# CAYLEY GRAPHS OF ORDER $6pq$ ARE HAMILTONIAN

**FARZAD MAGHSOUDI**
**Bachelor of Science, Shahid Beheshti University, 2017**

A thesis submitted
in partial fulfilment of the requirements for the degree of

**MASTER OF SCIENCE**

in

**MATHEMATICS**

Department of Mathematics and Computer Science
University of Lethbridge
LETHBRIDGE, ALBERTA, CANADA

CAYLEY GRAPHS OF ORDER $6pq$ ARE HAMILTONIAN

FARZAD MAGHSOUDI

Date of Defence: August 4, 2020

| | | |
|---|---|---|
| Dr. Joy Morris<br>Thesis Supervisor | Professor | Ph.D. |
| Dr. Dave Morris<br>Thesis Co-Supervisor | Professor | Ph.D. |
| Dr. Andrew Fiori<br>Thesis Examination Committee Member | Assistant Professor | Ph.D. |
| Dr. Shelly Wismath<br>Thesis Examination Committee Member | Professor | Ph.D. |
| Dr. John Sheriff<br>Chair, Thesis Examination Committee | Assistant Professor | Ph.D. |

# Dedication

I would like to dedicate my thesis to my mother, who always believed in me.

# Abstract

Assume $G$ is a finite group, such that $|G| = 6pq$ or $7pq$, where $p$ and $q$ are distinct prime numbers, and let $S$ be a generating set of $G$. We prove there is a Hamiltonian cycle in the corresponding Cayley graph $\mathrm{Cay}(G; S)$.

# Acknowledgments

I would like to express my sincere gratitude to my supervisor, professor Joy Morris who always supported me throughout my graduate journey. I am especially grateful to my co-supervisor, professor Dave Morris, for the patient guidance and advice he has provided during my graduate study. I have been extremely lucky to have a co-supervisor who cared so much about my research, and who responded to my questions so promptly.

I am also thankful to professor Hadi Kharaghani and professor Amir Akbary and cannot forget their valuable help and motivation during my graduate years.

I am truly grateful to my family for their immeasurable love and care.

# Contents

# List of Figures

# Chapter 1

# Introduction

## 1.1 Statement of the main result

Arthur Cayley [9] introduced the definition of Cayley graph in 1878. All graphs in this thesis are undirected.

**Definition 1.1.1** (cf. [23, p. 34])**.** Let $S$ be a subset of a finite group $G$. The *Cayley graph* $\mathrm{Cay}(G; S)$ is the graph whose vertices are elements of $G$, with an edge joining $g$ and $gs$, for every $g \in G$ and $s \in S$.

Since then, the theory of Cayley graphs has grown into a substantial branch in algebraic graph theory. It is an interesting topic to work on because not only is it related to pure mathematics problems, but it is connected to fascinating problems studied by computer scientists, molecular biologists, and coding theorists (see [30] for more information).

Recall that a *Hamiltonian cycle* is a cycle that visits every vertex of a graph. Finding Hamiltonian cycles is a fundamental question in graph theory, but in general, it is extremely difficult. To be precise, it is an NP-complete problem, which means most mathematicians do not believe there exists an efficient algorithm to determine whether an arbitrary graph contains such a cycle. (Finding a method would win a US$1,000,000 prize from the Clay Mathematics Institute [27].) Because the general case is so hard, it is natural to look at special cases.

Cayley graphs are one of these cases that mathematicians are interested in working on. There have been many papers on the topic, but it is still an open question whether every connected Cayley graph has a Hamiltonian cycle. (See survey papers [14, 50, 42] for more information. We ignore the trivial counterexamples on 1 or 2 vertices.) There are several different lines of research in the area. We mention some of the approaches that have been taken:

- Restrictions on $|G|$ that imply every connected Cayley graph on $G$ has a Hamiltonian cycle (see Theorem 1.1.2 below). The main results of this thesis are a contribution to this topic (see Theorem 1.1.3 and Proposition 1.1.4 below).
- Cayley graphs on groups that are almost abelian: commutator subgroup of prime order [17, 18, 37] (or cyclic of prime-power order [29]), commutator subgroup that is cyclic of order $pq$ (where $p$ and $q$ are prime) [40, 39], dihedral groups ([6] and [51, Proposition 5.5]), nilpotent groups [22, 38, 49].
- Existence of small-valency Cayley graphs that have a Hamiltonian cycle: [42, Theorem 1] and [51, Theorem 3.1].
- Random Cayley graphs: [31, Theorem 4.1].
- Hamiltonian paths (or cycles) in certain Cayley graphs on symmetric groups: These provide a list of all the permutations of a set. Several examples are described in [45, Section 3].
- Hamiltonian cycles in *vertex-transitive* graphs (graphs such that all vertices are in the same orbit of the automorphism group): See the survey [32]. Cayley graphs are examples of vertex-transitive graphs.
- Directed Hamiltonian paths or cycles in Cayley digraphs: [16, 38, 43, 44].
- Stronger or weaker results than Hamiltonian cycles (for Cayley graphs): Hamiltonian connected or Hamiltonian laceable: [4, 5, 13, 47], Hamiltonian decomposable [3, 8, 48], edge-Hamiltonian [10, 35, 36], Hamiltonian paths [38].

The following result combines the work of several authors (C. C. Chen and N. Quimpo [11], S. J. Curran, J. Morris and D. W. Morris [15], E. Ghaderpour and D. W. Morris [20, 21], D. Jungreis and E. Friedman [28], Kutnar et al. [33], K. Keating and D. Witte [29], D. Li [34], D. W. Morris and K. Wilk [41], and D. Witte [49]).

**Theorem 1.1.2** ([33, 41, 49])**.** *Let $G$ be a finite group. Every connected Cayley graph on $G$ has a Hamiltonian cycle if $|G|$ has any of the following forms (where $p$, $q$, and $r$ are distinct primes):*

1. *$kp$, where $1 \leqslant k \leqslant 47$,*
2. *$kpq$, where $1 \leqslant k \leqslant 5$,*
3. *$pqr$,*
4. *$kp^2$, where $1 \leqslant k \leqslant 4$,*
5. *$kp^3$, where $1 \leqslant k \leqslant 2$,*
6. *$p^k$, where $1 \leqslant k < \infty$.*

This thesis extends part (2) of Theorem 1.1.2 by improving the condition on $k$: we show that 5 can be replaced with 7. The hard part is when $k = 6$:

**Theorem 1.1.3.** *Assume $G$ is a finite group of order $6pq$, where $p$ and $q$ are distinct prime numbers. Then every connected Cayley graph on $G$ contains a Hamiltonian cycle.*

This generalizes [21], which considered only the case where $q = 5$. The proof takes up all of Chapter 3, after some preliminaries in Chapter 2.

Unlike Theorem 1.1.3, the following observation follows easily from known results, and may be known to experts. The proof is on page 35.

**Proposition 1.1.4.** *Assume $G$ is a finite group of order $7pq$, where $p$ and $q$ are distinct prime numbers. Then every connected Cayley graph on $G$ contains a Hamiltonian cycle.*

The remainder of this chapter explains some of the key ideas in the subject. Section 1.2 provides a brief description of the new part of the proof of Theorem 1.1.3, and gives a fairly complete proof of an illustrative special case. The other sections discuss results that are already in the literature. Section 1.3 explains the structure of groups of square-free order. Section 1.4 explains the key ideas in the proof of the previously known special case where the commutator subgroup has prime order. Section 1.5 explains the proof of parts (2) and (3) of Theorem 1.1.2. Section 1.6 describes a method that has been used to prove part (1) of Theorem 1.1.2.

The other chapters are devoted to the proof of Theorem 1.1.3: Chapter 2 covers preliminaries, and the proof is carried out in Chapter 3.

## 1.2 Basic methods

In this section we explain some of the key ideas in the proof of our main result (Theorem 1.1.3). We use standard terminology of graph theory and group theory that can be found in textbooks, such as [23, 25].

It is easy to see that $\mathrm{Cay}(G;S)$ is connected if and only if $S$ generates $G$ ([23, Lemma 3.7.4]). Also, if $S$ is a subset of $S_0$, then $\mathrm{Cay}(G;S)$ is a subgraph of $\mathrm{Cay}(G;S_0)$ that contains all of the vertices. Therefore, in order to show that every connected Cayley graph on $G$ contains a Hamiltonian cycle, it suffices to consider $\mathrm{Cay}(G;S)$, where $S$ is a generating set that is *minimal*, which means that no proper subset of $S$ generates $G$.

**Notation 1.2.1** ([21, Notation on page 3615])**.** For $S \subseteq G$, a sequence $(s_1, s_2, \ldots, s_n)$ of elements of $S \cup S^{-1}$ specifies the walk in $\mathrm{Cay}(G;S)$ that visits the vertices

$$e,\ s_1,\ s_1s_2, \ldots,\ s_1s_2 \cdots\ s_n.$$

Additional notation, terminology, and basic results can be found in Chapter 2. The following well known (and easy) result handles the case of Theorem 1.1.3 where $G$ is abelian.

Note $\mathrm{Cay}(\mathcal{C}_2; \{a\})$ is a Cayley graph with two vertices, where $\mathcal{C}_2 = \langle a \rangle$. We consider $(a, a)$ as its Hamiltonian cycle which is:

$$e \xrightarrow{a} a \xrightarrow{a} a^2 = e.$$

Although graph theorists would not typically consider this a cycle, it satisfies the basic property of visiting each vertex exactly once. In some of our inductive proofs, we require a Hamiltonian cycle in a Cayley graph on a quotient group. When this quotient group is $\mathcal{C}_2$, this Hamiltonian cycle provide the structure we need for our inductive arguments to work.

**Lemma 1.2.2** ([12, Corollary on page 257])**.** *Assume $G$ is an abelian group. Then every connected Cayley graph on $G$ has a Hamiltonian cycle.*

*Proof.* Let $S = \{s_1, s_2, \ldots, s_n\}$ be a minimal generating set for $G$. By induction on $n = |S|$, we prove that $\mathrm{Cay}(G; S)$ has a Hamiltonian cycle. If $n = 1$, then $G$ is cyclic and $\mathrm{Cay}(G; S)$ has a Hamiltonian cycle:

$$e \xrightarrow{s_1} s_1 \xrightarrow{s_1} s_1^2 \xrightarrow{s_1} \cdots \xrightarrow{s_1} s_1^{|G|} = e.$$

Now assume $n > 1$, and let $\overline{G} = G/\langle s_1 \rangle$. Then $|\overline{S \backslash \{s_1\}}| \leqslant n - 1$, so by the induction hypothesis $\mathrm{Cay}(\overline{G}; \overline{S})$ has a Hamiltonian cycle $(\bar{t}_1, \bar{t}_2, \ldots, \bar{t}_m)$. Clearly, $|G/\langle s_1 \rangle| = m$. Let $|s_1| = k$. If $m$ is even, then by considering $\{t_1, t_2, \ldots, t_m\}$ as the horizontal edges and $s_1$ as the vertical edges, we can see in Figure 1.1 that

$$(t_1, t_2, \ldots, t_{m-1}, s_1^{k-1}, t_{m-1}^{-1}, s_1^{-(k-2)}, t_{m-2}^{-1}, s_1^{k-2}, \ldots, t_1^{-1}, s_1^{-(k-1)})$$

is a Hamiltonian cycle in $\mathrm{Cay}(G; S)$. If $m$ is odd, then with the same understanding

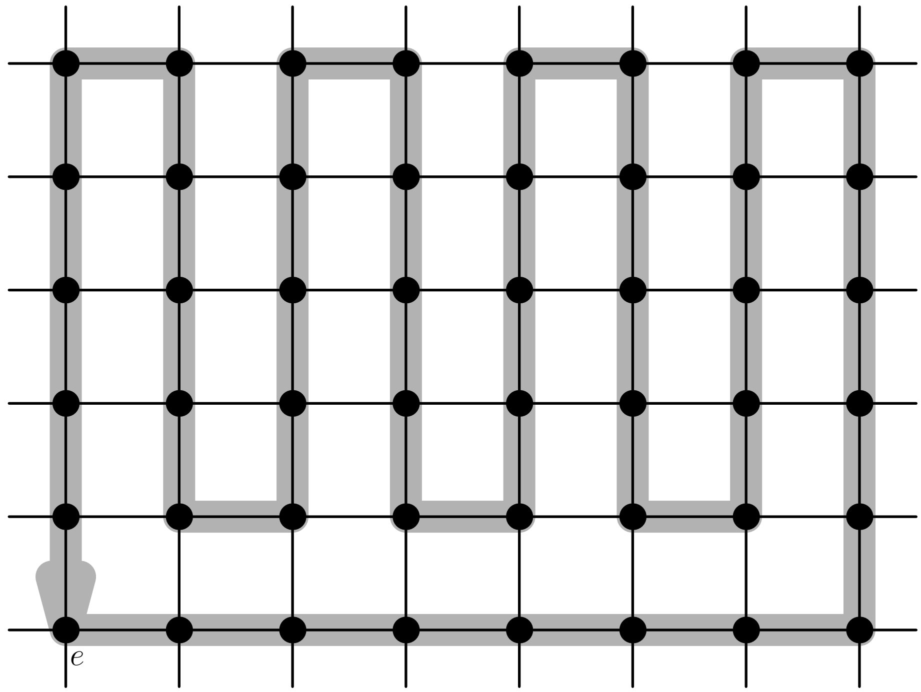


Figure 1.1: A zig-zag Hamiltonian cycle when the number of columns is even

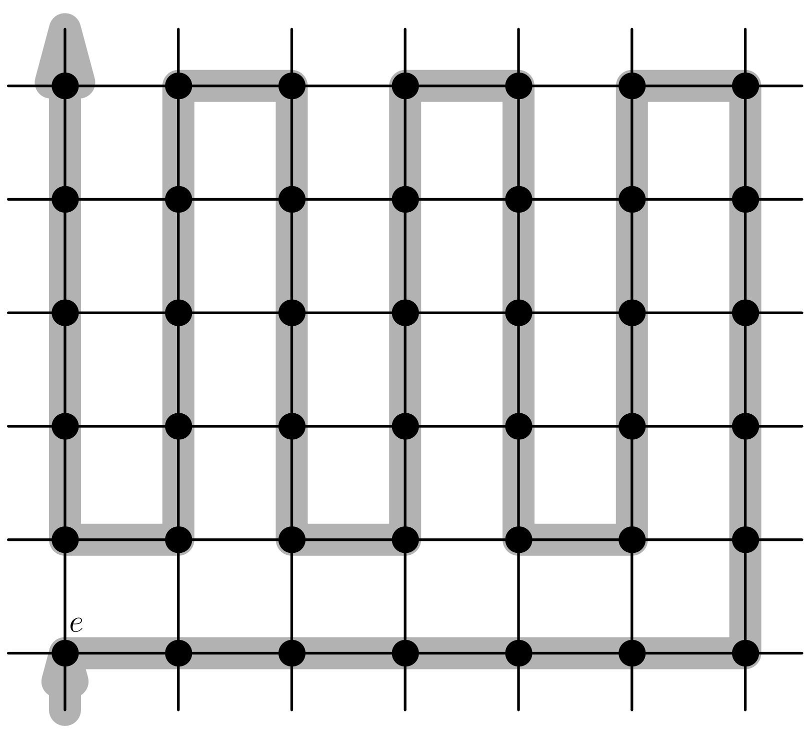


Figure 1.2: A zig-zag Hamiltonian cycle when the number of columns is odd

of the edges, we can see in Figure 1.2 that

$$(t_1, t_2, \ldots, t_{m-1}, s_1^{k-1}, t_{m-1}^{-1}, s_1^{-(k-2)}, t_{m-2}^{-1}, s_1^{k-2}, \ldots, t_1^{-1}, s_1^{(k-1)})$$

is a Hamiltonian cycle in $\mathrm{Cay}(G; S)$. □

**Theorem 1.2.3** (Marušič [37], Durnberger [17, 18], and Keating-Witte [29])**.** *If the commutator subgroup $G'$ of $G$ is a cyclic $p$-group, then every connected Cayley graph on $G$ has a Hamiltonian cycle.*

**Theorem 1.2.4** (Chen-Quimpo [13])**.** *Let $v$ and $w$ be two distinct vertices of a connected Cayley graph* $\mathrm{Cay}(G; S)$*. Assume $G$ is abelian, $|G|$ is odd, and the valency of* $\mathrm{Cay}(G; S)$ *is at least* 3*. Then* $\mathrm{Cay}(G; S)$ *has a Hamiltonian path that starts at $v$ and ends at $w$.*

We will always let $G' = [G, G]$ be the commutator subgroup of $G$. Then $\overline{G} = G/G'$ is always abelian, so Lemma 1.2.2 provides a Hamiltonian cycle in $\mathrm{Cay}(\overline{G}; \overline{S})$. The following lemma (and its corollary) often provide a way to lift this Hamiltonian cycle to a Hamiltonian cycle in $\mathrm{Cay}(G; S)$. Before stating the results, we introduce a useful piece of notation.

**Notation 1.2.5.** Let $N$ be a normal subgroup of $G$, and $\overline{G} = G/N$. For a Hamiltonian cycle $C = (\overline{s}_1, \overline{s}_2, \ldots, \overline{s}_n)$ in $\mathrm{Cay}(\overline{G}; \overline{S})$, $\mathbb{V}(C) = s_1 s_2 \cdots s_n$ is the *voltage* of $C$.

**Factor Group Lemma 1.2.6** ([50, Section 2.2])**.** *Suppose:*

- *$S$ is a generating set of $G$,*
- *$N$ is a cyclic normal subgroup of $G$,*
- *$\overline{G} = G/N$,*
- *$C = (\overline{s_1}, \overline{s_2}, \ldots, \overline{s_n})$ is a Hamiltonian cycle in* $\mathrm{Cay}(G/N; \overline{S})$*, and*
- *the voltage $\mathbb{V}(C)$ generates $N$.*

*Then there is a Hamiltonian cycle in* $\mathrm{Cay}(G; S)$.

*Proof.* Let $a = \mathbb{V}(C) = s_1 s_2 \cdots s_n$. We claim that $C^{|N|} = (s_1, s_2, \ldots, s_n)^{|N|}$ is a Hamiltonian cycle in $\mathrm{Cay}(G; S)$. Here is the walk $C^{|N|}$:

$$e \xrightarrow{s_1} s_1 \xrightarrow{s_2} s_1 s_2 \xrightarrow{s_3} \cdots \xrightarrow{s_n} s_1 s_2 \cdots s_n = a$$

$$\xrightarrow{s_1} a s_1 \xrightarrow{s_2} a s_1 s_2 \xrightarrow{s_3} \cdots \xrightarrow{s_n} a s_1 s_2 \cdots s_n = a^2$$

$$\vdots$$

$$\xrightarrow{s_1} a^{|N|-1} s_1 \xrightarrow{s_2} a^{|N|-1} s_1 s_2 \xrightarrow{s_3} \cdots \xrightarrow{s_n} a^{|N|-1} s_1 s_2 \cdots s_n = a^{|N|}.$$

Since $a^{|N|} = (s_1 s_2 \cdots s_n)^{|N|} = e$, then the walk is closed. Also, since $C$ is a Hamiltonian cycle in $\mathrm{Cay}(G/N; \overline{S})$, then its length is $|G|/|N|$. So the length of the walk $C^{|N|}$ is equal to $(|G|/|N|) \cdot |N| = |G|$, which is the correct length for a Hamiltonian cycle in $\mathrm{Cay}(G; S)$.

Therefore, if the walk is not a Hamiltonian cycle, then there must be a repeated vertex, which means

$$a^i (s_1 s_2 \cdots s_k) = a^j (s_1 s_2 \cdots s_l),$$

and $(i, j) \neq (k, l)$ where $0 \leqslant i, j \leqslant |N| - 1$ and $1 \leqslant k, l \leqslant n - 1$. If $k \neq l$, then they are in two different cosets of $N$ which is a contradiction, so $k = l$. Now we may assume $j \geqslant i$, then multiplying by $a^{-i}$ from the left side we have

$$a^{j-i} (s_1 s_2 \cdots s_k) = (s_1 s_2 \cdots s_k).$$

Therefore,

$$a^{j-i}(s_1s_2\cdots s_k)(s_k^{-1}s_{k-1}^{-1}\cdots s_1^{-1}) = (s_1s_2\cdots s_k)(s_k^{-1}s_{k-1}^{-1}\cdots s_1^{-1}).$$

This implies that $a^{j-i} = e$, which means $a^i = a^j$, so $i = j$. Therefore, $C^{|N|}$ is a Hamiltonian cycle in $\mathrm{Cay}(G; S)$. □

**Corollary 1.2.7** ([21, Corollary 2.3])**.** *Suppose:*

- *$S$ is a generating set of $G$,*
- *$N$ is a normal subgroup of $G$, such that $|N|$ is prime,*
- *$sN = tN$ for some $s, t \in S$ with $s \neq t$, and*
- *there is a Hamiltonian cycle in $\mathrm{Cay}(G/N; \overline{S})$ that uses at least one edge labeled $\overline{s}$.*

*Then there is a Hamiltonian cycle in $\mathrm{Cay}(G; S)$.*

*Proof.* Let $C = (\overline{s}_1, \overline{s}_2, \ldots, \overline{s}_n)$ be a Hamiltonian cycle in $\mathrm{Cay}(G/N; S)$, such that $s_i = s$ for some $i$, and assume, for simplicity, that $i = n$. If $\mathbb{V}(C) \neq e$, then since $|N|$ is a prime number, the subgroup generated by $\mathbb{V}(C)$ is $N$. Thus, Factor Group Lemma 1.2.6 applies. Now if $\mathbb{V}(C) = e$, then let $C_1 = (\overline{s}_1, \overline{s}_2, \ldots, \overline{s}_{n-1}, \overline{t})$. Since $\overline{t} = tN = sN = s_nN$, this is another representation of the Hamiltonian cycle $C$. However,

$$\mathbb{V}(C_1) = s_1s_2\cdots s_{n-1}t = s_1s_2\cdots s_{n-1}s_n \cdot (s_n)^{-1}t = e \cdot (s^{-1}t) \neq e$$

since $s \neq t$. So Factor Group Lemma 1.2.6 applies. □

**Definition 1.2.8.** The *Cartesian product* $X_1 \square X_2$ of graphs $X_1$ and $X_2$ is a graph such that the vertex set of $X_1 \square X_2$ is $V(X_1) \times V(X_2) = \{(v, v'); v \in V(X_1), v' \in V(X_2)\}$, and two vertices $(v_1, v_2)$ and $(v_1', v_2')$ are adjacent in $X_1 \square X_2$ if and only if either

- $v_1 = v_1'$ and $v_2$ is adjacent to $v_2'$ in $X_2$ or

- $v_2 = v_2'$ and $v_1$ is adjacent to $v_1'$ in $X_1$.

**Lemma 1.2.9** ([13, Lemma 5 on page 28])**.** *The Cartesian product of a path and a cycle is Hamiltonian.*

*Proof.* Let $L_n \,\square\, C_m$ be a Cartesian product of a path and a cycle, where $m \geqslant 3$. ($L_n$ is a path and $C_m$ is a cycle of length $m$.) Figures 1.1 on page 6 and 1.2 on page 6 show a Hamiltonian cycle in $L_n \,\square\, C_m$ depending on whether $n$ is even or not. □

**Corollary 1.2.10** (cf. [13, Corollary on page 29])**.** *The Cartesian product of two Hamiltonian graphs is Hamiltonian.*

*Proof.* Let $X_n \,\square\, X_m$ be a Cartesian product of two Hamiltonian graphs. Assume $C_n$ and $C_m$ are Hamiltonian cycles of $X_n$ and $X_m$, respectively. Then $C_n \square C_m$ is a spanning subgraph of $X_n \,\square\, X_m$. Also, since $C_n$ is a Hamiltonian cycle, then clearly there is a Hamiltonian path $L_n$ of $C_n$, so $L_n \,\square\, C_m$ is a spanning subgraph of $C_n \,\square\, C_m$. This implies that $L_n \,\square\, C_m$ is a spanning subgraph of $X_n \,\square\, X_m$, so Lemma 1.2.9 applies. □

**Lemma 1.2.11** ([33, Lemma 2.27])**.** *Let $S$ generate the finite group $G$, and let $s \in S$, such that $\langle s \rangle \lhd G$. If $\mathrm{Cay}(G/\langle s \rangle; \overline{S})$ has a Hamiltonian cycle, and either*

1. *$s \in Z(G)$ , or*
2. *$Z(G) \cap \langle s \rangle = \{e\}$,*

*then $\mathrm{Cay}(G; S)$ has a Hamiltonian cycle.*

*Proof.* ([33, Lemma 2.27]) Let $(\overline{s}_1, \overline{s}_2, \ldots, \overline{s}_n)$ be a Hamiltonian cycle in $\mathrm{Cay}(G/\langle s \rangle; \overline{S})$, and let $k = |s_1 s_2 \cdots s_n|$, so $(s_1, s_2, \ldots, s_n)^k$ is a cycle in $\mathrm{Cay}(G; S)$.

(1) Since $s \in Z(G)$, by considering a Cartesian coordinate system such that the vertical axis has vertices labeled

$$(e, s, s^2, \ldots, s^{|s|-1})$$

and the horizontal axis has vertices labeled

$$(e, s_1, s_1 s_2, \ldots, s_1 s_2 \cdots s_{n-1})$$

it is easy to see that $\mathrm{Cay}(G; S)$ contains a spanning subgraph isomorphic to the Cartesian product $P_n \square C_{|s|}$ of a path with $n$ vertices and a cycle with $|s|$ vertices. By Lemma 1.2.9 this Cartesian product is Hamiltonian, so we conclude that $\mathrm{Cay}(G; S)$ has a Hamiltonian cycle.

(2) Let $m = |G|/(nk)$. We claim that

$$(s^{m-1}, s_1, s^{m-1}, s_2, ..., s^{m-1}, s_n)^k$$

is a Hamiltonian cycle in $\mathrm{Cay}(G; S)$. Let

$$g_i = (s_1 s_2 ... s_i)^{-1} \text{ for } 0 \leqslant i \leqslant n, \text{ so } g_i g_{i+1}^{-1} = s_{i+1}$$

and note that, since $(s_1, s_2, \ldots, s_n)$ is a Hamiltonian cycle in $\mathrm{Cay}(G/\langle s \rangle; \overline{S})$, we know that $\{1, g_1, g_2, \ldots, g_{n-1}\}$ is a complete set of coset representatives for $\langle s \rangle$ in $G$. Then for any $h \in G$,

$$\{h, g_1 h, g_2 h, \ldots, g_{n-1} h\}$$

is also a set of coset representatives. Also, since $\langle s \rangle$ is abelian, we know that if $x$ and $y$ are elements in the same coset of $\langle s \rangle$, then $s^x = s^y$. Thus, for any $t \in \langle s \rangle$, we have

$$\{t, t^{g_1}, t^{g_2}, \ldots, t^{g_{n-1}}\} = \{t^h, t^{g_1 h}, t^{g_2 h}, \ldots, t^{g_{n-1} h}\}$$

so

$$t t^{g_1} t^{g_2} \cdots t^{g_{n-1}} = t^h t^{g_1 h} t^{g_2 h} \cdots t^{g_{n-1} h}$$

because both products have exactly the same factors (but possibly in a different order) and all factors are in the abelian group $\langle s\rangle$. Since the right-hand product is $(tt^{g_1}t^{g_2}\cdots t^{g_{n-1}})^h$, and $h$ is an arbitrary element of $G$, we conclude that $tt^{g_1}t^{g_2}\cdots t^{g_{n-1}} \in Z(G)$. Since $Z(G)$ has trivial intersection with $\langle s\rangle$, this implies that

$$tt^{g_1}t^{g_2}\cdots t^{g_{n-1}} = e.$$

Therefore, by letting $t = s^{m-1}$, we see that

$$(s^{m-1})s_1(s^{m-1})s_2\cdots(s^{m-1})s_n = ((s^{m-1})(s^{m-1})^{g_1}(s^{m-1})^{g_2}\cdots(s^{m-1})^{g_{n-1}})g_n^{-1} = g_n^{-1}.$$

Then,

$$((s^{m-1})s_1(s^{m-1})s_2\cdots(s^{m-1})s_n)^k = g_n^{-k} = (s_1s_2\cdots s_n)^k = e,$$

so the walk is closed. Furthermore, since $m = |\langle s\rangle/\langle g_n\rangle|$, it is clear that the walk visits every element of $\langle s\rangle$, and it is similarly easy to see that it visits every element of all of the other cosets. So it visits every element of $G$. Since it is also a closed walk of the correct length, we conclude that it is a Hamiltonian cycle. □

Known results easily imply many cases of our main theorem. Almost all of the remaining cases are proved by using the Factor Group Lemma 1.2.6 (or its corollary). In most of these cases, we apply the Factor Group Lemma 1.2.6 to $\overline{G} = G/G'$.

Let $S$ be a minimal generating set of $G$. As explained in Lemma 1.2.2, it is easy to find Hamiltonian cycles in $\mathrm{Cay}(\overline{G};\overline{S})$ since $\overline{G} = G/G'$ is abelian. However, we need to find a Hamiltonian cycle whose voltage generates $G'$. This requires a careful choice of the Hamiltonian cycle, and also requires calculating the product $s_1s_2\ldots s_n$, to show that it generates $G'$. This calculation can be rather complicated. Also, there are many different possibilities for the generating set $S$, so we need to find Hamiltonian cycles in many different Cayley graphs $\mathrm{Cay}(\overline{G};\overline{S})$, and calculating the voltage $s_1s_2\ldots s_n$ depends on the particular generating set $S$, not only on its image in $\overline{G}$. In a few cases, there does not exist a Hamiltonian cycle in $\mathrm{Cay}(\overline{G};\overline{S})$ whose voltage generates $G'$. In these situations, we apply Factor Group Lemma 1.2.6 to a Cayley graph on a quotient $G/N$, where $N$ is a proper subgroup of $G'$ that has prime order. Since $G/N$ is not abelian, it is more difficult to find Hamiltonian cycles in this Cayley graph.

We now describe the main ideas of our proof, which is in Chapter 3. We may assume $|G|$ is square-free, for otherwise $\{p,q\}\cap\{2,3\} \neq \varnothing$, so Theorem 1.1.2(1) applies (because $|G| \in \{12p, 12q, 18p, 18q\}$). Now elementary group theory implies that $G'$ is cyclic (see Proposition 1.3.12(1)). Now, known results apply unless $G'$ is either $\mathcal{C}_p \times \mathcal{C}_q$ or $\mathcal{C}_3 \times \mathcal{C}_p$, perhaps after interchanging $p$ and $q$ (see Proposition 2.3.2). (We use $\mathcal{C}_n$ to denote the cyclic group of order $n$.) The proof is divided into three parts, depending on the cardinality of $S$: $|S| = 2$, $|S| = 3$ or $|S| \geqslant 4$. (Note if $|S| = 1$, then $G$ is abelian and Lemma 1.2.2 applies.) This is the same general argument as in [21], which is the case where $q = 5$ and we use similar techniques. However, one of the reasons that our result is harder to prove is that $\mathcal{C}_3$ does not need to centralize $\mathcal{C}_q$ in our situation unlike when $q = 5$. Thus, the arguments of [21] did not apply to any of the cases we consider in which $\mathcal{C}_3$ does not centralize $\mathcal{C}_q$.

The easiest part of our proof is when $|S| \geqslant 4$. Section 3.9 (which is very short) shows that if we make some additional assumptions to rule out cases that are already known, then $\mathrm{Cay}(G;S)$ is a Cartesian product of smaller connected Cayley graphs. Each of these smaller Cayley graphs is known to have a Hamiltonian cycle (by Theorem 1.1.2), and it is well known that the Cartesian product of Hamiltonian graphs is Hamiltonian (see Lemma 1.2.10).

The hardest part of our proof is when $|S| = 3$. This part of the argument is in Sections 3.3–3.8. Since there are many different possible minimal generating sets, it is broken into many cases and subcases. (See Figures 3.1, 3.2 and 3.3 on pages 51 and 52 for a list of the cases.) In most situations, we apply Factor Group Lemma 1.2.6 to $G/G'$. Indeed, there are only three cases where this is not possible. These are in

Cases 2, 3, and 4 of Section 3.4, where we apply the Factor Group Lemma 1.2.6 to $G/\mathcal{C}_p$ or $G/\mathcal{C}_q$.

The other part is when $|S| = 2$. This part of the argument is in Sections 3.1 and 3.2. To give the flavour of the general arguments, we provide some details of one special case here.

We remark that in our notation for cycles, if $|a| = n$ we use $a^{n-i}$ to indicate $n - i$ copies of $a$, while $a^{-i}$ indicates $i$ copies of $a^{-1}$. Additionally, even when $|\overline{a}| = 2$, we may write $\overline{a}^{-1}$ in a cycle, if $|a| \neq 2$. This is used to indicate that when calculating the voltage, we will using $a^{-1}$ rather than $a$.

**Proposition 1.2.12.** *Assume*

- $G = (\mathcal{C}_2 \times \mathcal{C}_3) \ltimes G'$,
- $G' = \mathcal{C}_p \times \mathcal{C}_q$, *where $p$ and $q$ are distinct primes greater than* 3,
- $\overline{G} = G/G'$,
- $S = \{a, b\}$,
- $|\overline{a}| = 6$ *and* $|\overline{b}| = 2$.

*Then* $\mathrm{Cay}(G; S)$ *contains a Hamiltonian cycle.*

*Proof.* Since $|\overline{a}| = 6$, then $|a| \in \{6, 6p, 6q, 6pq\}$. If $|a| = 6pq$, then $G = \langle a \rangle$, which contradicts the minimality of $S$. If $|a| = 6p$, then $\mathcal{C}_p \subseteq \langle a \rangle$, so $\mathcal{C}_p$ centralizes $\mathcal{C}_2 \times \mathcal{C}_3$, and we already know that $\mathcal{C}_p$ centralizes $\mathcal{C}_q$. Therefore, $\mathcal{C}_p \subseteq Z(G)$, which contradicts the fact that $Z(G) \cap G' = \{e\}$ (see Proposition 1.3.12(2)). If $|a| = 6q$, then the same argument as when $|a| = 6p$ works, by interchanging $p$ and $q$. Thus, $|a| = 6$. So we have $\overline{b} = \overline{a}^3$, then $b = a^3\gamma$, where $G' = \langle \gamma \rangle$ (otherwise $\langle a, b \rangle = \langle a, a^3\gamma \rangle = \langle a, \gamma \rangle \neq G$ which contradicts the fact that $G = \langle a, b \rangle$).

Now by Proposition 1.3.12(4), we have $\tau \in \mathbb{Z}^+$ such that $a\gamma a^{-1} = \gamma^\tau$ and $\tau^6 \equiv 1 \pmod{pq}$, and $\gcd(\tau - 1, pq) = 1$. This implies that $\gcd(\tau - 1, p) = 1$ and $\gcd(\tau - 1, q) =$

1. Therefore, $\tau \not\equiv 1 \pmod p$ and $\tau \not\equiv 1 \pmod q$. Since $\tau^6 \equiv 1 \pmod{pq}$, then

$$0 \equiv \tau^6 - 1 = (\tau^3 - 1)(\tau^3 + 1) = (\tau - 1)(\tau^2 + \tau + 1)(\tau + 1)(\tau^2 - \tau + 1) \pmod{pq}.$$

Since $\tau \not\equiv 1 \pmod p$ and $\tau \not\equiv 1 \pmod q$, then we conclude that

$$0 \equiv (\tau^2 + \tau + 1)(\tau + 1)(\tau^2 - \tau + 1) \pmod{pq}. \tag{eq.1}$$

Up to automorphisms, there are only three different Hamiltonian cycles in $\mathrm{Cay}(\overline{G}; \overline{S})$, which are: $C_1 = (\overline{a}^6)$, $C_2 = ((\overline{a}, \overline{b})^3)$ and $C_3 = (\overline{a}^2, \overline{b}, \overline{a}^{-2}, \overline{b})$. Now we calculate their voltages. We have $\mathbb{V}(C_1) = a^6 = e$, so clearly it does not generate $G'$. We have

$$\begin{aligned}
\mathbb{V}(C_2) &= (ab)^3 = (a \cdot a^3\gamma)^3 = (a^4\gamma)^3 = a^4\gamma \cdot a^4\gamma \cdot a^4\gamma = \gamma^{\tau^4} a^4 \cdot a^4\gamma \cdot a^4\gamma \\
&= \gamma^{\tau^4} \cdot a^8\gamma \cdot a^4\gamma = \gamma^{\tau^4} \cdot a^2\gamma \cdot a^4\gamma = \gamma^{\tau^4} \cdot \gamma^{\tau^2} a^2 \cdot a^4\gamma = \gamma^{\tau^4} \cdot \gamma^{\tau^2} \cdot a^6\gamma \\
&= \gamma^{\tau^4+\tau^2} \cdot \gamma = \gamma^{\tau^4+\tau^2+1} = \gamma^{(\tau^2+\tau+1)(\tau^2-\tau+1)}.
\end{aligned}$$

We may assume the subgroup generated by $\mathbb{V}(C_2)$ does not contain $G'$, for otherwise Factor Group Lemma 1.2.6 applies. Therefore,

$$\gcd((\tau^2 + \tau + 1)(\tau^2 - \tau + 1), pq) \neq 1,$$

which by looking into eq.1, we see is possible. Assume, without loss of generality, that either $\tau^2 + \tau + 1 \equiv 0 \pmod p$ or $\tau^2 - \tau + 1 \equiv 0 \pmod p$. Note that this implies $\tau \not\equiv \pm 1 \pmod p$.

We can now calculate the voltage of $C_3$.

$$\mathbb{V}(C_3) = a^2ba^{-2}b = a^2 \cdot a^3\gamma \cdot a^{-2} \cdot a^3\gamma = a^5\gamma a\gamma = \gamma^{\tau^5+1}.$$

We may assume this does not generate $G'$, for otherwise Factor Group Lemma 1.2.6

applies. So $\gcd(\tau^5+1, pq) \neq 1$. This implies that $\tau^5+1 \equiv 0 \pmod{p}$ or $\tau^5+1 \equiv 0 \pmod{q}$. Therefore, $\tau \equiv -1 \pmod{p}$ or $\tau \equiv -1 \pmod{q}$. Since $\tau \not\equiv -1 \pmod{p}$, this implies $\tau \equiv -1 \pmod{q}$.

We are now in a situation where the voltages of $C_1$, $C_2$ and $C_3$ do not generate $G'$. Since $|\overline{b}| = 2$, we could try to obtain different voltages by replacing some occurrences of $\overline{b}$ with $\overline{b}^{-1}$. However, if $\tau^2 - \tau + 1 \equiv 0 \pmod{p}$, then $\tau^3 \equiv -1 \pmod{p}$. Since $\tau^3 \equiv (-1)^3 = -1 \pmod{q}$, this implies that $b$ has order 2, so $b = b^{-1}$. Hence replacing $\overline{b}$ with $\overline{b}^{-1}$ will not change the voltages of Hamiltonian cycles in this case. Thus, the Factor Group Lemma 1.2.6 cannot be applied to $G/G'$. In this situation, we will therefore look at $\widehat{G} = G/\mathcal{C}_p$.

Consider $\widehat{G} = G/\mathcal{C}_p = (\mathcal{C}_2 \times \mathcal{C}_3) \ltimes \mathcal{C}_q$. Since $b = a^3\gamma$, where $\langle \gamma \rangle = G'$, we have $\widehat{b} = \widehat{a}^3 a_q$, where $\langle a_q \rangle = \mathcal{C}_q$. Since $\tau \equiv -1 \pmod{q}$, then $a^2$ centralizes $\gamma$ and $a^3$ inverts $\gamma$, so $\mathcal{C}_3$ centralizes $\mathcal{C}_q$ and $\mathcal{C}_2$ does not centralize $\mathcal{C}_q$. Therefore, $\widehat{G} \cong D_{2q} \times \mathcal{C}_3$, where $D_{2q}$ is the dihedral group of order $2q$. Now we have

$$C_4 = ((\widehat{a}^5, \widehat{b}, \widehat{a}^{-5}, \widehat{b})^{(q-3)/2}, (\widehat{a}^5, \widehat{b})^3)$$

as a Hamiltonian cycle in $\mathrm{Cay}(\widehat{G}; \widehat{S})$. The picture in Figure 3.4 shows the Hamiltonian cycle when $q = 7$.

If in $C_4$ we change one occurrence of $(\widehat{a}^5, \widehat{b}, \widehat{a}^{-5}, \widehat{b})$ to $(\widehat{a}^{-5}, \widehat{b}, \widehat{a}^5, \widehat{b})$ we have another Hamiltonian cycle. Note that,

$$a^5 b a^{-5} b = a^5 \cdot a^3\gamma \cdot a^{-5} \cdot a^3\gamma = a^2\gamma a^{-2}\gamma = \gamma^{\tau^2+1},$$

and

$$a^{-5} b a^5 b = a^{-5} \cdot a^3\gamma \cdot a^5 \cdot a^3\gamma = a^{-2}\gamma a^2\gamma = \gamma^{\tau^{-2}+1}.$$

Since $\tau^4 \not\equiv 0 \pmod{p}$ we see that $\tau^2 + 1 \not\equiv \tau^{-2} + 1 \pmod{p}$. Therefore, the voltages of these two Hamiltonian cycles are different, so one of these Hamiltonian cycles has a nontrivial voltage. Thus, Factor Group Lemma 1.2.6 applies. □

## 1.3 Groups of square-free order

In this section we describe the structure of groups of square-free order. We start the section by stating the following proposition about the solvability of groups of square-free order.

**Proposition 1.3.1** ([19, Proposition 17])**.** *Every group of square-free order is solvable.*

The proof of this proposition needs a concept in group theory named *transfer homomorphism.* Since the goal of this thesis is to prove Theorem 1.1.3 in which the order of the group is $6pq$ ($p$ and $q$ are distinct primes which can be assumed to be greater than 7 by Assumption 3.0.1(1)), then it suffices for our purposes to prove the following special case, which does not require the transfer homomorphism.

**Proposition 1.3.2.** *Assume $|G| = 2pqr$, where $p$, $q$ and $r$ are distinct odd prime numbers. Then $G$ is solvable.*

Before proving this proposition, we establish several well known lemmas.

**Lemma 1.3.3.** *Assume $|G| = pq$, where $p$ and $q$ are distinct prime numbers and $p > q$. Then $G$ has a unique subgroup of order $p$ (this subgroup is normal) and $G$ is solvable.*

*Proof.* By the Sylow existence theorem, there exists a Sylow $p$-subgroup of $G$. Let $n_p$ be the number of Sylow $p$-subgroups of $G$. Then by Sylow's theorem we have $n_p \equiv 1 \pmod{p}$ and $n_p | q$. Since $p > q$, then $n_p = 1$, which implies that there is a unique $P$ as the Sylow $p$-subgroup of $G$. This implies that $P \lhd G$, where $|P| = p$.

Since we have $\langle e \rangle \lhd P \lhd G$ as a normal series with abelian quotients, then $G$ is solvable. □

**Lemma 1.3.4.** *Assume $|G| = pqr$, where $p$, $q$ and $r$ are distinct prime numbers and $p > q > r$. Then $G$ contains a normal subgroup of order either $p$, $q$ or $r$.*

*Proof.* Let $n_p$, $n_q$ and $n_r$ be the number of Sylow $p$-subgroups, Sylow $q$-subgroups and Sylow $r$-subgroups of $G$, respectively. We may assume $n_p > 1$, for otherwise we have a unique Sylow $p$-subgroup of $G$, which is normal and we are done. Similarly, assume $n_q > 1$ and $n_r > 1$. By Sylow's theorem, we have $n_p \equiv 1 \pmod{p}$ and $n_p | qr$. This implies that $n_p \in \{1, r, q, qr\}$. Since $n_p > 1$ and $p > q, r$, then $n_p = qr$. Also, by Sylow's theorem, we have $n_q \equiv 1 \pmod{q}$ and $n_q | pr$. This implies that $n_q \in \{1, p, r, pr\}$. Since $n_q > 1$ and $q > r$, then $n_q \geqslant p$. By applying Sylow's theorem we also have, $n_r \equiv 1 \pmod{r}$ and $n_r | pq$. This implies that $n_r \in \{1, p, q, pq\}$. Since $n_r > 1$, then we have $n_r \geqslant q$. Each Sylow $p$-subgroup contains $p-1$ elements of order $p$. Since distinct Sylow $p$-subgroups intersect trivially, there are $(p-1)n_p = (p-1)qr$ elements of order $p$ in $G$. By a similar argument, the number of elements of order either $p$, $q$ or $r$ is greater than or equal to

$$(r-1)q + (q-1)p + (p-1)qr = qr - q + pq - p + pqr - qr = pqr + pq - q - p.$$

Clearly, this number must be less than or equal to $|G| = pqr$. Therefore,

$$pqr + pq - q - p \leqslant pqr.$$

This implies that (since $p > q > r \geqslant 2$)

$$q \leqslant p/(p-1) < 2,$$

which is a contradiction. $\square$

**Lemma 1.3.5.** *Assume $|G| = pqr$, where $p$, $q$ and $r$ are distinct prime numbers and $p > q > r$. Then the Sylow $p$-subgroup of $G$ is normal.*

*Proof.* By Lemma 1.3.4 we know that there exists a normal subgroup of order either $p$, $q$ or $r$. If the normal subgroup of $G$ has order $p$, then we are done. So we may assume $N \lhd G$, where the order of $N$ is either $q$ or $r$. Now $G/N$ has order either $pr$ or $pq$. Thus, by Lemma 1.3.3 we have $M$ as a Sylow $p$-subgroup of $G/N$, which is normal. Since $M \lhd G/N$, then by the Correspondence Theorem, it corresponds to a normal subgroup $N_1$ of $G$ of order $pr$ or $pq$ (depending on whether $|N| = q$ or $|N| = r$). Now by applying Lemma 1.3.3 to $N_1$, we conclude that there exists $M_1 \lhd N_1$ as a unique Sylow $p$-subgroup of $N_1$. Let $g \in G$ be an arbitrary element. Then $gM_1g^{-1} \leqslant gN_1g^{-1} = N_1$. Since $|gM_1g^{-1}| = |M_1|$, and we know that $M_1$ is a unique Sylow $p$-subgroup of $N_1$, then $gM_1g^{-1} = M_1$. This implies that $M_1 \lhd G$. $\square$

**Lemma 1.3.6.** *Assume $|G| = pqr$, where $p$, $q$ and $r$ are distinct prime numbers and $p > q > r$. Then $G$ is solvable.*

*Proof.* By Lemma 1.3.5 we know $M \lhd G$ as a Sylow $p$-subgroup of $G$. We have $|G/M| = qr$, so by Lemma 1.3.3, there exists $Q \lhd G/M$ as a Sylow $q$-subgroup of $G/M$. By the Correspondence Theorem, $Q$ corresponds to $N \lhd G$ with $|N| = pq$. Therefore, $\langle e\rangle \lhd Q \lhd N \lhd G$ is a subnormal series of $G$ with abelian quotients. This implies that $G$ is solvable. $\square$

**Lemma 1.3.7.** *Assume $|G| = 2k$, where $k$ is odd. Then $G$ has a subgroup of index 2.*

*Proof.* Let $\Phi : G \to S_{2k}$, by $\Phi(g) = \sigma_g$ for every $g \in G$, where $\sigma_g$ is the permutation in $S_{2k}$ defined by $\sigma_g(g') = gg'$ for every $g' \in G$. For arbitrary $g_1, g_2 \in G$, we have

$$\Phi(g_1g_2) = \sigma_{g_1g_2} = \sigma_{g_1}\sigma_{g_2} = \Phi(g_1)\Phi(g_2).$$

So $\Phi$ is a group homomorphism. Since $|G| = 2k$, then there is an element of order 2 in $G$, say $a$. Note that $\sigma_a(ag) = a^2g = g$. So for every $g \in G$, $(g, ag)$ is a transposition in $\sigma_a$. Thus, $\sigma_a$ is a product of transpositions. Since every $g \in G$ belongs to exactly one transposition, and $|G| = 2k$, then $\sigma_a$ has $k$ transpositions, so $\sigma_a$ is an odd permutation.

Now define $\Psi : S_{2k} \to \{1, -1\}$ by $\Psi(\sigma) = 1$ if the permutation $\sigma$ is even, and $\Psi(\sigma) = -1$ if the permutation $\sigma$ is odd. We claim that $\Psi$ is a group homomorphism. Suppose not, then there exists $\sigma_1, \sigma_2 \in S_{2k}$, such that $\Psi(\sigma_1\sigma_2) \neq \Psi(\sigma_1)\Psi(\sigma_2)$. Without loss of generality assume $\Psi(\sigma_1\sigma_2) = 1$ and $\Psi(\sigma_1)\Psi(\sigma_2) = -1$. Since $\Psi(\sigma_1\sigma_2) = 1$, then either both $\sigma_1$ and $\sigma_2$ are even or both $\sigma_1$ and $\sigma_2$ are odd. So $\Psi(\sigma_1)\Psi(\sigma_2) = 1$, which is a contradiction. Now since $\Phi$ and $\Psi$ are group homomorphisms, then $\Psi \circ \Phi : G \to \{1, -1\}$ is a group homomorphism. Since

$$\Psi \circ \Phi(a) = \Psi(\Phi(a)) = \Psi(\sigma_a) = -1$$

and $\Psi \circ \Phi(e) = 1$, then $\Psi \circ \Phi$ is onto. Now by the First Isomorphism Theorem, we have $G/\mathrm{Ker}(\Psi \circ \Phi) \cong \{1, -1\}$. This implies that $\mathrm{Ker}(\Psi \circ \Phi)$ is a subgroup of index 2. □

**Lemma 1.3.8.** *Assume $|G| = 2k$, where $k$ is odd. Then $|G'|$ is odd.*

*Proof.* By Lemma 1.3.7, there is a normal subgroup $H$ of $G$ such that $[G : H] = 2$. Now since $G/H$ has order 2, then $G/H$ is abelian, so $G' \subseteq H$. Therefore, $|G'|$ is odd. □

**Lemma 1.3.9.** *If $N$ is a normal subgroup of $G$, such that $N$ and $G/N$ are solvable, then $G$ is solvable.*

*Proof.* By induction on $r$, we see that $(G/N)^{(r)} = G^{(r)}N$. (Note that $G^{(r)}$ is the $r^{\text{th}}$ derived subgroup of $G$.) However, since $G/N$ is solvable, there is some $r$, such that $(G/N)^{(r)}$ is trivial. Therefore, we must have $G^{(r)} \subseteq N$. By induction on $s$, we see that $G^{(r+s)} = (G^{(r)})^{(s)}$ for all $s \in \mathbb{Z}^+$. However, since $N$ is solvable, there is some $s \in \mathbb{Z}^+$, such that $N^{(s)} = \{e\}$. Then $G^{(r+s)} = (G^{(r)})^{(s)} \subseteq N^{(s)} = \{e\}$. □

*Proof of Proposition 1.3.2.* Since $|G| = 2 \times odd$, then by Lemma 1.3.7 there is a subgroup $N$ of index 2 in $G$. Since $|G : N| = 2$, then $N \lhd G$. Since $|N| = pqr$, then by Lemma 1.3.6 $N$ is solvable. Also, clearly $|G/N| = 2$ and $G/N$ is solvable. Therefore, by Lemma 1.3.9 $G$ is solvable. □

**Lemma 1.3.10.** *If $N \lhd G$, $N \subseteq Z(G)$, and $G/N$ is cyclic, then $G$ is abelian.*

*Proof.* By the Third Isomorphism Theorem, we have $G/Z(G) \cong (G/N)/(Z(G)/N)$. Since $(G/N)/(Z(G)/N)$ is a quotient of $G/N$ (which is cyclic), then $(G/N)/(Z(G)/N)$ is cyclic. This implies that $G/Z(G)$ is cyclic. Let $gZ(G)$ be a generator of $G/Z(G)$, where $g \in G$. Now let $g_1 \in G$ be an arbitrary element in $G$. So $g_1Z(G) = g^nZ(G)$ for some $n \in \mathbb{Z}^+$. Therefore, $g^{-n}g_1 \in Z(G)$, so there exists $z_1 \in Z(G)$ such that $z_1 = g^{-n}g_1$. Thus, $g_1 = g^nz_1$. Let $g_2 \in G$ be another arbitrary element in $G$, by the same argument we have $g_2 = g^mz_2$, where $z_2 \in Z(G)$, and $m \in \mathbb{Z}^+$. Now we have

$$g_1g_2 = g^nz_1 \cdot g^mz_2 = g^{n+m}z_1z_2 = g^mg^nz_2z_1 = g^mz_2 \cdot g^nz_1 = g_2g_1.$$

This implies that $G$ is abelian. ☐

**Lemma 1.3.11** ([46, 12.6.16 on page 356])**.** *If $G$ is a group and $G^{(i-1)}/G^{(i)}$ and $G^{(i)}/G^{(i+1)}$ are cyclic for some $i \geqslant 2$, then $G^{(i)}/G^{(i+1)} = \{e\}$.*

*Proof.* Let $H = G^{(i-2)}/G^{(i+1)}$. Then $H'/H'' \cong G^{(i-1)}/G^{(i)}$ and $H'' = G^{(i)}/G^{(i+1)}$ are cyclic and $H''' = G^{(i+1)}/G^{(i+1)} = \{e\}$. Define $\Phi : N_H(H'') \to \mathrm{Aut}(H'')$, where $\Phi(h) = \Psi_h$ for every $h \in H$, and $\Psi_h = hh''h^{-1}$ for every $h'' \in H''$. Let $h_1, h_2 \in N_H(H'')$ be arbitrary elements. Then

$$\Phi(h_1h_2) = \Psi_{h_1h_2} = \Psi_{h_1}\Psi_{h_2} = \Phi(h_1)\Phi(h_2).$$

This implies that $\Phi$ is a homomorphism. We claim that $\mathrm{Ker}(\Phi) = C_H(H'')$. Assume $h \in \mathrm{Ker}(\Phi)$, then $\Phi(h) = \Psi_h = hh''h^{-1} = h'' = \Psi_e$, for every $h'' \in H''$. This implies that $h \in C_H(H'')$. So $\mathrm{Ker}(\Phi) \subseteq C_H(H'')$. Now assume $h \in C_H(H'')$, then $\Phi(h) = \Psi_h = hh''h^{-1} = h'' = \Psi_e$. This implies that $h \in \mathrm{Ker}(\Phi)$. Therefore, $C_H(H'') \subseteq \mathrm{Ker}(\Phi)$. We conclude that $\mathrm{Ker}(\Phi) = C_H(H'')$. By the First Isomorphism Theorem

$$N_H(H'')/C_H(H'') = N_H(H'')/\mathrm{Ker}(\Phi) \cong \Phi(N_H(H''))$$

which is a subgroup of $\mathrm{Aut}(H'')$. Now it is clear that $N_H(H'')/C_H(H'') = H/C_H(H'')$. So $H/C_H(H'')$ is isomorphic to a subgroup of $\mathrm{Aut}(H'')$. We know that $H''$ is cyclic. So $H'' = \langle h'' \rangle$. Now let $\Phi_1, \Phi_2 \in \mathrm{Aut}(H'')$. Since $H''$ is cyclic, then $\Phi_1(h'') = (h'')^a$ and $\Phi_2(h'') = (h'')^b$ for some $a, b \in \mathbb{Z}^+$. Thus,

$$\Phi_1 \circ \Phi_2(h'') = \Phi_1(\Phi_2(h'')) = \Phi_1((h'')^b) = (h'')^{ba} = ((h'')^a)^b = \Phi_2 \circ \Phi_1(h'').$$

This implies that $\mathrm{Aut}(H'')$ is abelian. So $H/C_H(H'')$ is abelian. Therefore, $H' \subseteq C_H(H'')$. Thus, $H'' \subseteq Z(H')$. Now since $H'/H''$ is cyclic and $H'' \subseteq Z(H')$, then $H'$ is abelian (see Lemma 1.3.10). Since $H'$ is abelian, then $H'' = \{e\}$, which means $G^{(i)}/G^{(i+1)} = \{e\}$ as desired. □

We can now prove the main result of this section.

**Proposition 1.3.12** ([25, Theorem 9.4.3 on page 146], cf. [21, Lemma 2.11])**.** *Assume $|G|$ is square-free. Then:*

1. *$G'$ and $G/G'$ are cyclic,*
2. *$Z(G) \cap G' = \{e\}$,*
3. *$G \cong C_n \ltimes G'$, for some $n \in \mathbb{Z}^+$,*
4. *If $b$ and $\gamma$ are elements of $G$ such that $\langle bG' \rangle = G/G'$ and $\langle \gamma \rangle = G'$, then $\langle b, \gamma \rangle = G$, and there are integers $m$, $n$, and $\tau$, such that $|\gamma| = m$, $|b| = n$, $b\gamma b^{-1} = \gamma^\tau$, $mn = |G|$, $\gcd(\tau - 1, m) = 1$, and $\tau^n \equiv 1 \pmod{m}$.*

*Proof.* Since $|G|$ is square-free, then by Proposition 1.3.1 $G$ is solvable. (We proved in Proposition 1.3.2 that the group we are working on in Theorem 1.1.3 is solvable.) Since $G/G'$ is an abelian group of square-free order, then $G/G'$ is cyclic. By the same argument, $G'/G''$ and $G''/G'''$ are also cyclic. Now by Lemma 1.3.11 (with $i = 2$), $G'' = G'''$. Since $G$ is solvable, then there exists $r \in \mathbb{Z}^+$ such that $G^{(r)} = \{e\}$. By

Lemma 1.3.11 (with $i \in \{3, 4, \ldots, r-1\}$) we have

$$G'' = G''' = G^{(4)} = \ldots = G^{(r-1)} = G^{(r)} = \{e\}.$$

This implies that $G'' = \{e\}$. Since $G'/G''$ is cyclic, this implies $G'$ is cyclic. Thus we have shown that $G'$ and $G/G'$ are cyclic, as desired.

Let $G' = \langle \gamma \rangle$, $m = |\gamma| = |G'|$, and let $G/G' = \langle bG' \rangle$. Hence $b$ and $\gamma$ generate $G$ and $b\gamma b^{-1} = \gamma^{\tau}$ for some $\tau \in \mathbb{Z}^+$. If $G/G'$ is of order $n$, then $b^n \in G' = \langle \gamma \rangle$ so $b^n$ centralizes $\gamma$. Therefore, $b^n \gamma b^{-n} = \gamma$. Since $b\gamma b^{-1} = \gamma^{\tau}$, then

$$\gamma^{\tau^n} = (b\gamma b^{-1})^n = b^n \gamma b^{-n} = \gamma.$$

So $\tau^n \equiv 1 \pmod{m}$. Note that $G = \langle b, \gamma \rangle$ and $[b, \gamma] = b\gamma b^{-1}\gamma^{-1} = \gamma^{\tau-1}$. Hence $\gamma^{\tau-1}$ generates $G'$ (see Lemma 2.2.1), therefore, $\gcd(\tau - 1, m) = 1$. Also, we know that $b^n \in G'$, so there exists $k \in \mathbb{Z}^+$ such that $b^n = \gamma^k$. We have

$$\gamma^{k+\tau} = \gamma^k \gamma^{\tau} = b^n \gamma^{\tau} = b^n (b\gamma b^{-1}) = b b^n \gamma b^{-1} = b\gamma^{k+1} b^{-1} = \gamma^{(k+1)\tau}.$$

This implies that $k + \tau \equiv (k+1)\tau \pmod{m}$, so $k\tau - k \equiv 0 \pmod{m}$. Therefore, $k(\tau - 1) \equiv 0 \pmod{m}$. Since $\gcd(\tau - 1, m) = 1$, then $k \equiv 0 \pmod{m}$, so $b^n = \gamma^k = e$.

Assume $Z(G) \cap G' \neq \{e\}$. Then there exists $z \in Z(G)$ such that $z \in G'$. Since $G' = \langle \gamma \rangle$, then $z = \gamma^{\ell}$ for some $\ell \in \mathbb{Z}^+$. We have

$$\gamma^{\ell+\tau} = \gamma^{\ell} \gamma^{\tau} = z\gamma^{\tau} = z(b\gamma b^{-1}) = b(z\gamma b^{-1}) = b\gamma^{\ell}\gamma b^{-1} = b\gamma^{\ell+1} b^{-1} = \gamma^{(\ell+1)\tau}.$$

This implies that $\ell + \tau \equiv (\ell + 1)\tau \pmod{m}$. Therefore, $\ell(\tau - 1) \equiv 0 \pmod{m}$, which implies that $\ell \equiv 0 \pmod{m}$ (because $\gcd(\tau - 1, m) = 1$). So $Z(G) \cap G' = \{e\}$.

Since $G = \langle b, \gamma \rangle$, then every element in $G$ can be written in the form of $b^i \gamma^j \in \langle b \rangle \langle \gamma \rangle$, so $G \subseteq \langle b \rangle \langle \gamma \rangle$, and every element in $\langle b \rangle \langle \gamma \rangle$ belongs to $G$, therefore, $G = \langle b \rangle \langle \gamma \rangle$.

Since $\langle b\rangle \cap \langle\gamma\rangle \subseteq Z(G)$, $\langle\gamma\rangle = G'$, and $Z(G) \cap G' = \{e\}$ we see that $\langle b\rangle \cap \langle\gamma\rangle = \{e\}$. Since $G = \langle b\rangle\langle\gamma\rangle$ and $\langle b\rangle \cap \langle\gamma\rangle = \{e\}$, then $G = \langle b\rangle \ltimes \langle\gamma\rangle$. Also, since $|b| = n$ and $\langle\gamma\rangle = G'$, then $G \cong \mathcal{C}_n \ltimes G'$. □

**Notation 1.3.13.** For $\tau$ as defined in Proposition 1.3.12(4), we use $\tau^{-1}$ to denote the inverse of $\tau$ modulo $m$ (so $\tau^{-1} \equiv \tau^{n-1} \pmod{m}$).

## 1.4 Marušič's method and an application

Throughout this section, firstly, we state and prove Marušič's method, which is a fundamental technique that was introduced in [37]. Then we see an application of this method in proving a case of our main result.

**Lemma 1.4.1** (Marušič's method [29, Lemma 3.1])**.** *Let $G = \langle S\rangle$ with $|G'| = p$, where $p$ is prime. Choose a subset $T$ of $S$ with $H = \langle T\rangle$ non-abelian. Suppose there are Hamiltonian cycles $(y_1, y_2, \ldots, y_m)$ and $(y_1^*, y_2^*, \ldots, y_m^*)$ in* $\mathrm{Cay}(H/H'; T)$ *such that $y_m = y_m^*$ and $y_1 y_2 \cdots y_m \neq y_1^* y_2^* \cdots y_m^*$. Then there is a Hamiltonian cycle $(x_1, x_2, \ldots, x_n)$ in* $\mathrm{Cay}(G/G'; S)$ *such that $(x_1, x_2, \ldots, x_n)^{|G'|}$ is a Hamiltonian cycle in* $\mathrm{Cay}(G; S)$*.*

*Proof.* ([29, Proof of Lemma 3.1]) Since $|G'|$ is prime, we must have $H' = G'$ so $(y_1, y_2, \ldots, y_m)$ and $(y_1^*, y_2^*, \ldots, y_m^*)$ are Hamiltonian cycles in $\mathrm{Cay}(H/G'; T)$. Since $G' \subseteq H$, then $G/H$ is an abelian group. Let $(z_1, z_2, \ldots, z_k)$ be a Hamiltonian path in $\mathrm{Cay}(G/H; S\backslash T)$, and let $L = (y_1, y_2, \ldots, y_{m-1})$. If $m$ is even we have

$$C = (z_1, z_2, \ldots, z_k, L, z_k^{-1}, y_{m-1}^{-1}, y_{m-2}^{-1} \ldots, y_2^{-1}, z_{k-1}^{-1}, \ldots, z_1^{-1}, y_{m-1}^{-1}, y_{m-2}^{-1}, \ldots, y_1^{-1})$$

as a Hamiltonian cycle in $\mathrm{Cay}(G/G'; S)$ (see Figure 1.1 on page 6). If $m$ is odd we have

$$C = (z_1, z_2, \ldots, z_k, L, z_k^{-1}, y_{m-1}^{-1}, y_{m-2}^{-1}, \ldots, y_2^{-1}, z_{k-1}^{-1}, \ldots, z_1^{-1}, y_2, y_3, \ldots, y_m)$$

as a Hamiltonian cycle in $\mathrm{Cay}(G/G';S)$ (see Figure 1.2 on page 6). Now we construct another Hamiltonian cycle $C^*$ in $\mathrm{Cay}(G/G';S)$ by replacing $L$ with $(y_1^*, y_2^*, \ldots, y_{m-1}^*)$ in $C$. Since $y_1 y_2 \cdots y_m \neq y_1^* y_2^* \cdots y_m^*$, then $\mathbb{V}(C) \neq V(C^*)$. Since $|G'|$ is prime, then one of $\mathbb{V}(C)$ or $V(C^*)$ must be nontrivial, therefore, this voltage generates $G'$. So Factor Group Lemma 1.2.6 applies. This means that either $C^{|G'|}$ or $C^{*|G'|}$ is a Hamiltonian cycle in $\mathrm{Cay}(G;S)$. $\square$

**Corollary 1.4.2** (cf. [29, Case 5.3])**.** *Assume $S$ is a minimal generating set of $G$ such that $|G'| = p$ where $p$ is prime, and let $\overline{G} = G/G'$. Also, assume $a, b \in S$ with $a \notin C_G(G')$, $ab \neq ba$, and either $|\overline{a}| > 2$ and $\overline{b} \notin \langle \overline{a} \rangle$ or $a\gamma a^{-1} \neq \gamma^{-1}$ for some generator $\gamma$ of $G'$. Then* $\mathrm{Cay}(G;S)$ *has a Hamiltonian cycle.*

*Proof.* (cf. [29, Case 5.3]) Let $T = \{a, b\}$ and $H = \langle a, b \rangle$.

**Case 1.** Assume $|\overline{a}| > 2$ and $\overline{b} \notin \langle \overline{a} \rangle$. Then one of the following is a Hamiltonian cycle in $\mathrm{Cay}(H/H';\overline{T})$, depending on whether $k = |H : \langle a, G' \rangle|$ is even or odd (see Figures 1.1, and 1.2 on page 6):

$$C = (\overline{b}^{k-1}, \overline{a}, (\overline{a}^{|\overline{a}|-2}, \overline{b}^{-1}, \overline{a}^{-(|\overline{a}|-2)}, \overline{b}^{-1})^{(k-2)/2}, \overline{a}^{|\overline{a}|-1}, \overline{b}^{-1}, \overline{a}^{-(|\overline{a}|-1)})$$

or

$$C = (\overline{b}^{k-1}, \overline{a}, (\overline{a}^{|\overline{a}|-2}, \overline{b}^{-1}, \overline{a}^{-(|\overline{a}|-2)}, \overline{b}^{-1})^{(k-1)/2}, \overline{a}^{|\overline{a}|-1}).$$

Since $|\overline{a}| > 2$ and $k > 1$, then each of the above Hamiltonian cycles contains the string $(\overline{b}, \overline{a}^{|\overline{a}|-1}, \overline{b}^{-1}, \overline{a}^{-1})$ (This is at the right end of Figures 1.1 and 1.2). Now we form a new Hamiltonian cycle by replacing this string with $(\overline{a}^{-1}, \overline{b}, \overline{a}^{|\overline{a}|-1}, \overline{b}^{-1})$. This Hamiltonian cycle has a different voltage than the original, for otherwise if we let

$\gamma = [b, a^{-1}]$, then

$$\gamma a^{-1} = (ba^{-1}b^{-1}a)a^{-1} = (ba^{-1}b^{-1}a^{-1})a = (a^{-1}ba^{-1}b^{-1})a = a^{-1}[b, a^{-1}] = a^{-1}\gamma.$$

This contradicts the fact that $a \notin C_G(G')$. Therefore, Lemma 1.4.1 applies.

**Case 2.** Assume $a\gamma a^{-1} \neq \gamma^{-1}$. Then $|\overline{a}| > 2$. So we may assume $\overline{b} \in \langle \overline{a} \rangle$, for otherwise the Case 1 applies. Thus, $\overline{b} = \overline{a}^i$, where $0 \leqslant i \leqslant |\overline{a}| - 1$. By Proposition 1.3.12(2) $G' \cap Z(G) = \{e\}$, so we may assume $S \cap G' = \varnothing$, for otherwise Lemma 1.2.11(2) applies since $G/\langle s \rangle$ is abelian, so $\mathrm{Cay}(G/\langle s \rangle; \overline{S})$ has a Hamiltonian cycle. Therefore, $i \neq 0$. Also, we may assume $i \neq 1, |\overline{a}| - 1$, for otherwise Corollary 1.2.7 applies with $s = a$ and $t = b^{\pm 1}$. Since $\overline{b} = \overline{a}^i$, then $b = a^i\gamma$, where $\gamma \in G'$, and $G' = \langle \gamma \rangle$, for otherwise $b = a^i$ which contradicts the fact that $ba \neq ab$. We have $(\overline{a}^{|\overline{a}|})$ and $(\overline{b}, \overline{a}^{-(i-1)}, \overline{b}, \overline{a}^{(|\overline{a}|-i-1)})$ as Hamiltonian cycles in $\mathrm{Cay}(H/H'; \overline{T})$. We may assume they have the same voltage, for otherwise Lemma 1.4.1 applies. Therefore,

$$e = a^{|\overline{a}|} = ba^{-(i-1)}ba^{|\overline{a}|-i-1} = ba^{-i+1}ba^{-i-1} = a^i\gamma \cdot a^{-i+1} \cdot a^i\gamma \cdot a^{-i-1} = a^i\gamma a\gamma a^{-i-1}.$$

Multiplying by $a^{i+1}$ on the right side and by $a^{-i}$ on the left side we have

$$a = \gamma a \gamma.$$

This implies that $a$ inverts $\gamma$ which is a contradiction. □

**Corollary 1.4.3.** *Assume $|G|$ is odd and $|G'| = p$, where $p$ is prime. Then every connected Cayley graph on $G$ has a Hamiltonian cycle.*

*Proof.* Let $S$ be a minimal generating set of $G$. Since $|G'| \neq 1$, then $C_G(G') \neq G$. So there exists $a \in S$ such that $a \notin C_G(G')$. We choose $b \in S$ such that $b$ does not commute with $a$. Since $|a|$ is odd, it does not invert $G'$, so Corollary 1.4.2 applies. □

**Corollary 1.4.4** (cf. [11]). *Assume $|G| = pq$, where $p$ and $q$ are distinct prime numbers. Then every connected Cayley graph on $G$ has a Hamiltonian cycle.*

*Proof.* If $G$ is abelian, then Lemma 1.2.2 applies. Additionally, if $|G|$ is odd, then Corollary 1.4.3 applies. So we may assume $|G|$ is even and $G$ is not abelian. By Proposition 1.3.12 we have $G \cong \mathcal{C}_2 \ltimes \mathcal{C}_p \cong D_{2p}$. Let $S$ be a minimal generating set of $G$. For all $s \in S$, we may assume $|s| = 2$. (Note that if $|s| = 2p$, then $G$ is abelian. Also, if $|s| = p$, then Lemma 1.2.11(2) applies.) Let $a, b \in S$ such that $a = a_2$ and $b = a_2\gamma_p$, where $a_2$ and $\gamma_p$ are generators of $\mathcal{C}_2$ and $\mathcal{C}_p$, respectively. Then we have $(a, b)^p$ as a Hamiltonian cycle in $\mathrm{Cay}(G; S)$. □

**Corollary 1.4.5.** *Assume $|G| = 2pqr$, where $p$, $q$ and $r$ are distinct odd primes, and $|G'|$ is prime. Then every connected Cayley graph on $G$ has a Hamiltonian cycle.*

*Proof.* (cf. [29, Case 5.3]) Let $S$ be a minimal generating set of $G$. We consider two cases.

**Case 1.** Assume $|G : C_G(G')| \neq 2$. Then there exists $a \in S$ such that $a \notin C_G(G')$ and $|a|$ is odd. (Note that since $|G'|$ is prime, then $|G : C_G(G')| \neq 1$.) Choose $b \in S$ such that $ab \neq ba$. Since $|a|$ is odd, then $a$ does not invert $G'$, so Corollary 1.4.2 applies.

**Case 2.** Assume $|G : C_G(G')| = 2$. This implies that $G = D_{2p} \times \mathcal{C}_q \times \mathcal{C}_r$ (up to permuting $p$, $q$, and $r$).

**Subcase 2.1.** Assume $S$ has no elements of odd order. Let $a$ and $b$ be two elements of $S$ whose orders are divisible by $q$ and $r$, respectively. (So $|a|$ is divisible by $2q$ and $|b|$ is divisible by $2r$.) Now if $|a| = 2q$, $|b| = 2r$ and $\langle a, b\rangle = G$, then by Theorem 1.1.2(2) there is a Hamiltonian cycle in $\mathrm{Cay}(\breve{G}; \{\breve{a}, \breve{b}\})$, and since $\langle \breve{a}, \breve{b}\rangle = G$ any such cycle uses both $\breve{a}$ and $\breve{b}$, so Corollary 1.2.7 applies with $N = \mathcal{C}_q$, $s = a$ and $t = a^{-1}$. If $\langle a, b\rangle \neq G$, then there should be another element $c \in S$ such that $\langle a, b, c\rangle = G$. Then there is a Hamiltonian cycle in $\mathrm{Cay}(\breve{G}; \{\breve{a}, \breve{b}, \breve{c}\})$ and since $\breve{c}$ cannot be the only element in the Hamiltonian cycle, it must use either $\breve{a}$ or $\breve{b}$, so Corollary 1.2.7 applies with

$N = \mathcal{C}_q$ and (by interchanging $q$ and $r$ if necessary), $s = a$ and $t = a^{-1}$. So we may assume $|a| = 2qr$. We may write $G = (\mathcal{C}_2 \ltimes \mathcal{C}_p) \times \mathcal{C}_q \times \mathcal{C}_r$. Let $a_2$, $\gamma_p$, $a_q$, and $a_r$ be generators of $\mathcal{C}_2$, $\mathcal{C}_p$, $\mathcal{C}_q$, and $\mathcal{C}_r$, respectively. Now, let $b$ be another element of $S$. Write $a = a_2 a_q a_r$ and $b = a_2 \gamma_p a_q^i a_r^j$, where $0 \leqslant i \leqslant q-1$ and $0 \leqslant j \leqslant r-1$.

Let $\breve{G} = G/(\mathcal{C}_q \times \mathcal{C}_r)$, then $\breve{a} = a_2$ and $\breve{b} = a_2\gamma_p$. We have $C_1 = (\breve{a}, \breve{b})^p$ is a Hamiltonian cycle in $\mathrm{Cay}(\breve{G}; \{\breve{a}, \breve{b}\})$. Now we calculate its voltage modulo $\mathcal{C}_p$.

$$\begin{aligned} \mathbb{V}(C_1) = (ab)^p &\equiv (a_2 a_q a_r \cdot a_2 a_q^i a_r^j)^p \pmod{\mathcal{C}_p} \\ &= (a_q^{i+1} a_r^{j+1})^p \\ &= a_q^{(i+1)p} a_r^{(j+1)p}. \end{aligned}$$

We may assume this does not generate $\mathcal{C}_q \times \mathcal{C}_r$, for otherwise Factor Group Lemma 1.2.6 applies. Therefore, either $i = -1$ or $j = -1$. We may assume $j = -1$. (Note that since $p$, $q$ and $r$ are distinct primes, then $p \not\equiv 0 \pmod r$ and $p \not\equiv 0 \pmod q$.)

We also have $C_2 = (\breve{a}, \breve{b}^{-1})^p$ as a Hamiltonian cycle in $\mathrm{Cay}(\breve{G}; \{\breve{a}, \breve{b}\})$. By a similar argument and calculating the voltage of $C_2$, we see that if $i \neq 1$, then the Factor Group Lemma 1.2.6 applies. Therefore, we may assume $i = 1$. Then $b = a_2\gamma_p a_q a_r^{-1}$.

We consider $\widehat{G} = G/(\mathcal{C}_p \times \mathcal{C}_r) \cong \mathcal{C}_2 \times \mathcal{C}_q$. So we have $\widehat{a} = \widehat{b} = a_2 a_q$. We have $C_3 = (\widehat{a}^q, \widehat{b}, \widehat{a}, \widehat{b}^{q-2})$ as a Hamiltonian cycle in $\mathrm{Cay}((\mathcal{C}_2 \times \mathcal{C}_q); \{\widehat{a}, \widehat{b}\})$. Now we calculate its voltage modulo $\mathcal{C}_p$ and modulo $\mathcal{C}_r$.

$$\begin{aligned} \mathbb{V}(C_3) &= a^q b a b^{q-2} \\ &\equiv (a_2 a_q a_r)^q \cdot a_2 a_q a_r^{-1} \cdot a_2 a_q a_r \cdot (a_2 a_q a_r^{-1})^{q-2} \pmod{\mathcal{C}_p} \\ &= a_2 a_q^q a_r^q \cdot a_2 a_q a_r^{-1} \cdot a_2 a_q a_r \cdot a_2 a_q^{q-2} a_r^{-(q-2)} \\ &= a_r^{q-1+1-q+2} a_q^{q+2+q-2} \\ &= a_r^2 \end{aligned}$$

which generates $\mathcal{C}_r$. So $\langle \mathbb{V}(C_3) \rangle$ contains $\mathcal{C}_r$ (cf. Lemma 2.5.1). Also,

$$
\begin{aligned}
\mathbb{V}(C_3) &= a^q bab^{q-2} \\
&\equiv (a_2a_q)^q \cdot a_2\gamma_p a_q \cdot a_2a_q \cdot (a_2\gamma_p a_q)^{q-2} \pmod{\mathcal{C}_r} \\
&= a_2a_q^q \cdot a_2\gamma_p a_q \cdot a_2a_q \cdot a_2\gamma_p a_q^{q-2} \\
&= a_q^{q+2+q-2}\gamma_p^2 \\
&= \gamma_p^2
\end{aligned}
$$

which generates $\mathcal{C}_p$. So $\langle \mathbb{V}(C_3) \rangle$ contains $\mathcal{C}_p$ (cf. Lemma 2.5.1). Therefore, the subgroup generated by $\mathbb{V}(C_3)$ is $\mathcal{C}_p \times \mathcal{C}_r$. So Factor Group Lemma 1.2.6 applies.

**Subcase 2.2.** Assume $S$ has exactly one element of odd order. Let $b$ be the element of odd order. If $|b| = pqr$, then there exists $a \in S$ such that $|a|$ is divisible by 2. Let $n = |b| = pqr$. Since $\langle b \rangle$ is normal in $G$ (because $|G : \langle b \rangle| = 2$), there is some $k \in \mathbb{Z}^+$, such that $aba^{-1} = b^k$. For $0 \leqslant i < n$, let $v_i = b^i$ and $w_i = b^i a$, so $V(G) = \{v_i\} \cup \{w_i\}$. Then, for each $i$, $\mathrm{Cay}(G; S)$ contains edges (labeled $b^{\pm 1}$) from $v_i$ to $v_{i\pm 1}$ and from $w_i$ to $w_i b^{\pm 1} = b^i a b^{\pm 1} = b^i b^{\pm k} a = b^{i \pm k} a = w_{i \pm k}$. It also contains the edge (labeled $a$) from $v_i$ to $v_i a = w_i$. This means that $\mathrm{Cay}(G; S)$ contains a copy of the generalized Petersen graph $\mathrm{GP}(n, k)$. Work of Bannai [7] and Alspach [1] has determined precisely which generalized Petersen graphs are Hamiltonian. Since $\langle b \rangle$ is of index 2, then $a^2 \in \langle b \rangle$, so $a^2 b = ba^2$. This implies that $k^2 \equiv 1 \pmod{n}$. Therefore, $\gcd(n, k) = 1$, and $k \neq \pm 2, \pm(n-1)/2$. Therefore, $\mathrm{GP}(n, k)$ has a Hamiltonian cycle. This Hamiltonian cycle is also a Hamiltonian cycle in $\mathrm{Cay}(G; S)$.

So we may assume $|b| \neq pqr$. Also, we can assume $b \notin Z(G)$ and $\langle b \rangle \cap Z(G) \neq \{e\}$, for otherwise since $\langle b \rangle \lhd G$, then Lemma 1.2.11(2) applies. (A Hamiltonian cycle in $\mathrm{Cay}(G/\langle b \rangle; \overline{S})$ exists by Theorem 1.1.2(2) or Theorem 1.2.3 depending on $|b|$.) So $|b|$ is either $pq$ or $pr$. Without loss of generality we may assume $|b| = pq$. Then there is $a \in S$ such that $|a|$ is divisible by $r$. Since $b$ is the only element in $S$ of odd order, $|a|$

is divisible by $2r$. We can assume $|a| \neq 2r$, for otherwise Corollary 1.2.7 applies with $N = \mathcal{C}_r$, $s = a$ and $t = a^{-1}$ (since $S$ is minimal and $G = \langle a, b \rangle$, a Hamiltonian cycle in $\mathrm{Cay}(G/N; \{\widehat{a}, \widehat{b}\})$ must use $\widehat{a}$). So we have $|a| = 2qr$. We may assume $a = a_2 a_q a_r$ and $b = \gamma_p a_q^i$, where $i \neq 0$. Let $\breve{G} = G/(\mathcal{C}_q \times \mathcal{C}_r) \cong D_{2p}$. Then $\breve{a} = a_2$ and $\breve{b} = \gamma_p$. We have $C_1 = (\breve{b}^{p-1}, \breve{a}, \breve{b}^{p-1}, \breve{a})$ as a Hamiltonian cycle in $\mathrm{Cay}(\breve{G}; \{\breve{a}, \breve{b}\})$. Now we calculate its voltage modulo $\mathcal{C}_p$.

$$\begin{aligned}
\mathbb{V}(C_1) &= b^{p-1} a b^{p-1} a \\
&\equiv (a_q^i)^{p-1} \cdot a_2 a_q a_r \cdot (a_q^i)^{p-1} \cdot a_2 a_q a_r \pmod{\mathcal{C}_p} \\
&= a_q^{2(i(p-1)+1)} a_r^2
\end{aligned}$$

We may assume this does not generate $\mathcal{C}_q \times \mathcal{C}_r$, for otherwise Factor Group Lemma 1.2.6 applies. Therefore,

$$0 \equiv i(p-1) + 1 \pmod{q}. \tag{2.2.A}$$

By replacing $\breve{a}$ with $\breve{a}^{-1}$ in $C_1$, we have $C_2 = (\breve{b}^{p-1}, \breve{a}^{-1}, \breve{b}^{p-1}, \breve{a}^{-1})$ as a Hamiltonian cycle in $\mathrm{Cay}(G/(\mathcal{C}_q \times \mathcal{C}_r); \{\breve{a}, \breve{b}\})$. By the same argument above and calculating $\mathbb{V}(C_2)$ modulo $\mathcal{C}_p$, we have

$$\mathbb{V}(C_2) \equiv a_q^{2(i(p-1)-1)} a_r^{-2} \pmod{\mathcal{C}_p}.$$

We may assume this does not generate $\mathcal{C}_q \times \mathcal{C}_r$, for otherwise Factor Group Lemma 1.2.6 applies. Therefore,

$$0 \equiv i(p-1) - 1 \pmod{q}.$$

By subtracting the above equation from 2.2.A, we have $0 \equiv 2 \pmod{q}$ which is a contradiction.

**Subcase 2.3.** Assume $S$ has more than 1 element of odd order. Assume $b$ and $c$ have odd order. Now since $\langle b, c\rangle$ is abelian, $|\langle b, c\rangle|$ is odd, and the valency of the Cayley graph $\mathrm{Cay}(\langle b, c\rangle; \{b, c\})$ is at least 3 (in fact it is 4). If either $\langle b\rangle$ or $\langle c\rangle$ does not contain $\mathcal{C}_p$, then we claim that $\mathrm{Cay}(G; S)$ has a Hamiltonian cycle. Without loss of generality we may assume $\langle b\rangle$ does not contain $\mathcal{C}_p$. We know $\langle b\rangle \lhd G$, $\mathrm{Cay}(G/\langle b\rangle; \overline{S})$ has a Hamiltonian cycle ($G/\langle b\rangle$ is isomorphic to either $D_{2p}$ or $D_{2p} \times \mathcal{C}_q$ or $D_{2p} \times \mathcal{C}_r$, so Theorem 1.1.2(2) or Theorem 1.1.2(3) applies), and $b \in Z(G)$, so Lemma 1.2.11(1) applies.

So we may assume both $\langle b\rangle$ and $\langle c\rangle$ contain $\mathcal{C}_p$. Then clearly $\mathcal{C}_p \lhd \langle b, c\rangle$, and $\mathcal{C}_p \cap Z(G) = \{e\}$ (see Proposition 1.3.12(2)). Let $a \in S$ be an element of even order. Now by Theorem 1.2.4 we can choose $L = (s_1, s_2, \ldots, s_m)$ as a Hamiltonian path in $\mathrm{Cay}(\langle b, c\rangle; \{b, c\})$ such that $s_1 s_2 \cdots s_m \in \mathcal{C}_p$. So $(L, a, L, a^{-1})$ is a Hamiltonian cycle in $\mathrm{Cay}(G; S)$. □

## 1.5 Proof of some parts of Theorem 1.1.2

In this section, we prove most cases in Theorem 1.1.2(2). Then we prove Theorem 1.1.2(3), and Proposition 1.1.4. In order to prove these results, firstly, we state some well known lemmas and propositions.

**Lemma 1.5.1** (cf. [33, Corollary 2.16])**.** *Every connected Cayley graph on the alternating group $A_4$ has a Hamiltonian cycle.*

**Proposition 1.5.2** ([28, Theorem 5.4])**.** *If $G = \mathcal{C}_2 \ltimes A$ such that $Z(G) = \{e\}$, $A$ is abelian, and $|A|$ is the product of at most three primes (not necessarily distinct), then every connected Cayley graph on $G$ has a Hamiltonian cycle.*

**Lemma 1.5.3** ([33, Corollary 2.3])**.** *If $|G| = pq^2$, where $p$ and $q$ are distinct primes with $q^2 \not\equiv 1 \pmod{p}$, then every connected Cayley graph on $G$ has a Hamiltonian* *cycle.*

*Proof.* ([33, Corollary 2.3]) Let $P$ be a Sylow $p$-subgroup of $G$. By Sylow's Theorem we have $n_p|q^2$, and $n_p \equiv 1 \pmod{p}$, where $n_p$ is the number of Sylow $p$-subgroups in $G$. Since $q^2 \not\equiv 1 \pmod{p}$, this implies that $q \not\equiv 1 \pmod{p}$, we must have $n_p = 1$. Therefore, $P \lhd G$. Now $|G/P| = q^2$, so $G/P$ is abelian. Therefore, $G' \subseteq P$. This implies that $|G'|$ is either 1 or $p$. If $|G'| = 1$, then $G$ is abelian, so Lemma 1.2.2 applies. If $|G'| = p$, then Theorem 1.2.3 applies. □

**Lemma 1.5.4** ([33, Corollary 2.24]). *If $|G| = 2p^2$, where $p$ is odd, then every connected Cayley graph on $G$ has a Hamiltonian cycle.*

*Proof.* ([33, Corollary 2.24]) By Lemma 1.3.8 $|G'|$ is odd. If $|G'| = 1$, then Lemma 1.2.2 applies. If $|G'|$ is cyclic of order $p$, then Theorem 1.2.3 applies. If $|G'| = p^2$, then Proposition 1.5.2 applies. □

**Proposition 1.5.5** ([33, Proposition 4.1]). *If $|G| = 3p^2$, where $p$ is prime, then every connected Cayley graph on $G$ has a Hamiltonian cycle.*

**Proposition 1.5.6** ([33, Proposition 6.1]). *Assume $|G| = 2pq$, where $p$ and $q$ are prime numbers. Then every Cayley graph on $G$ has a Hamiltonian cycle.*

*Proof.* ([33, Proposition 6.1]) Let $S$ be a minimal generating set of $G$. We may assume $p$ and $q$ are distinct, for otherwise $|G| = 2p^2$, so Proposition 1.5.4 applies. Without loss of generality assume $p > q$. If $q = 2$, then $|G| = 4p$. By Sylow's Theorem we have $n_p|4$, and $n_p \equiv 1 \pmod{p}$, where $n_p$ is the number of Sylow $p$-subgroups in $G$. Since $p > q$, then $p \geqslant 3$. Now if $p \geqslant 5$, then Lemma 1.5.3 applies. Now we may assume $p = 3$. If a Sylow 3-subgroup $P$ is normal in $G$, then $|G/P| = 4$, so $G/P$ is abelian. (Since $P$ is normal it is the unique Sylow 3-subgroup.) This implies that $G' \subseteq P$, therefore, $|G'| \in \{1, 3\}$. If $|G'| = 1$, then Lemma 1.2.2 applies, and if $|G'| = 3$, then Theorem 1.2.3 applies. So we may assume a Sylow 3-subgroup of $G$ is not normal. Then $G \cong A_4$, so Lemma 1.5.1 applies. Thus, we may assume $p, q \geqslant 3$.

Now we may assume $|G|$ is square-free. By Lemma 1.3.8 $|G'|$ is odd and by Proposition 1.3.12(1) $G'$ is cyclic. If $|G'| = 1$, then $G$ is abelian, so Lemma 1.2.2 applies. If $|G'|$ is prime, then Theorem 1.2.3 applies. If $|G'| = pq$, then $G \cong \mathcal{C}_2 \ltimes (\mathcal{C}_{pq}) \cong D_{2pq}$, so Proposition 1.5.2 applies. □

**Proposition 1.5.7** ([33, Proposition 6.2]). *Assume $|G| = pqr$, where $p$, $q$ and $r$ are distinct prime numbers. Then every connected Cayley graph on $G$ has a Hamiltonian cycle.*

*Proof.* (cf. [33, Proposition 6.2]) Since $|G|$ is square-free, then by Proposition 1.3.12(1) $G'$ is cyclic. If $|G| = 2pq$, then Proposition 1.5.6 applies. So we may assume $|G|$ is odd.

If $|G'| = 1$, then $G$ is abelian, so Lemma 1.2.2 applies. If $|G'|$ is prime, then Corollary 1.4.3 applies. So we may assume $G = \mathcal{C}_r \ltimes (\mathcal{C}_p \times \mathcal{C}_q)$ (up to permuting $p$, $q$, and $r$), where $G' = \mathcal{C}_p \times \mathcal{C}_q$. By Proposition 1.3.12(2) we know $G' \cap Z(G) = \{e\}$, so $C_{G'}(\mathcal{C}_r) = \{e\}$. Let $S$ be a minimal generating set of $G$. We may assume $S \cap G' = \varnothing$, for otherwise Lemma 1.2.11(2) applies. Therefore, every element of $S$ has order $r$. (Note since $G' \cap Z(G) = \{e\}$ (see Proposition 1.3.12(2)), $\mathcal{C}_r$ cannot commute with $\mathcal{C}_p$ or $\mathcal{C}_q$, so no element belonging to $S$ can have order $rp$ or $rq$.)

**Case 1.** Assume $|S| = 2$. We may write $S = \{a, b\}$. Consider $\overline{G} = G/G' = \mathcal{C}_r$. Then $|\overline{a}| = |\overline{b}| = r$. So $\overline{b} = \overline{a}^k$, where $1 \leqslant k \leqslant r-1$. Therefore, $b = a^k\gamma$, where $G' = \langle \gamma \rangle$, for otherwise

$$\langle a, b \rangle = \langle a, a^k\gamma \rangle = \langle a, \gamma \rangle \neq G$$

which contradicts our assumption that $G = \langle S \rangle$. We also have $a\gamma a^{-1} = \gamma^\tau$, where $\tau^r \equiv 1 \pmod{pq}$ (see Proposition 1.3.12(4)). So $\gcd(\tau, p) = 1$ and $\gcd(\tau, q) = 1$. Also, since $|a| = r$ is odd, $a$ cannot invert $\gamma^p$ or $\gamma^q$, so $\tau \not\equiv -1 \pmod{p}$ and $\tau \not\equiv -1 \pmod{q}$.

We have $C = (\overline{b}, \overline{a}^{-(k-1)}, \overline{b}, \overline{a}^{r-k-1})$ as a Hamiltonian cycle in $\mathrm{Cay}(\overline{G}; \overline{S})$. Now we calculate its voltage.

$$\begin{aligned}\mathbb{V}(C) &= ba^{-(k-1)}ba^{r-k-1} \\ &= a^k\gamma \cdot a^{-k+1} \cdot a^k\gamma \cdot a^{r-k-1} \\ &= a^k\gamma a\gamma a^{-k-1} \\ &= \gamma^{\tau^k(1+\tau)}\end{aligned}$$

which generates $G'$. So Factor Group Lemma 1.2.6 applies.

**Case 2.** Assume $|S| = 3$. We may write $S = \{a, b, c\}$ with $|\overline{a}| = |\overline{b}| = |\overline{c}| = r$. Also, since $S$ is minimal, then $|a| = |b| = |c| = r$. So we may assume $b = a^j a_q$ and $c = a^k\gamma_p$, where $1 \leqslant j, k \leqslant r-1$. Therefore, $\langle b, c\rangle = G$ which contradicts the minimality of $S$. $\square$

**Proposition 1.5.8** ([33, Corollary 6.3])**.** *Assume $|G| = 3pq$, where $p$ and $q$ are prime numbers. Then every connected Cayley graph on $G$ has a Hamiltonian cycle.*

*Proof.* ([33, Corollary 6.3]) We may assume $p, q \geqslant 3$, for otherwise $|G|$ is of the form $2pq$ or $2p^2$, so Proposition 1.5.6 or Lemma 1.5.4 applies. We may also assume $p, q > 3$, for otherwise $|G|$ is of the form $pq^2$ with $q^2 \not\equiv 1 \pmod p$, so Lemma 1.5.3 applies. Thus, $|G|$ is a product of three distinct primes, so Proposition 1.5.7 applies. $\square$

**Proposition 1.5.9** ([33, Corollary 6.4])**.** *Assume $|G| = 5pq$, where $p$ and $q$ are distinct prime numbers. Then every Cayley graph on $G$ has a Hamiltonian cycle.*

*Proof.* ([33, Corollary 6.4]) We may assume $p, q \geqslant 5$, for otherwise $|G|$ is of the form $2pq$ or $2p^2$ or $3pq$ or $3p^2$, so Proposition 1.5.6 or Lemma 1.5.4 or Proposition 1.5.8 or Proposition 1.5.5 applies. We may also assume $p, q \neq 5$, for otherwise $|G|$ is of the form $pq^2$ with $q^2 \not\equiv 1 \pmod p$, so Lemma 1.5.3 applies. Thus, $|G|$ is a product of three distinct primes, so Proposition 1.5.7 applies. $\square$

*Proof of Proposition 1.1.4.* If $p \neq 7$ and $q \neq 7$, then Theorem 1.1.2(3) applies. So we may assume $q = 7$, which means $|G| = 49p$ (and $p \neq 7$). We may also assume that $G$ is not abelian, for otherwise Lemma 1.2.2 applies.

If a Sylow $p$-subgroup $P$ of $G$ is normal, then $|G/P| = 49$, so the quotient $G/P$ is abelian. (Because if $q$ is prime, then every group of order $q^2$ is abelian). Therefore, since $P$ is normal and $G/P$ is abelian, then $G'$ is contained in $P$. So $|G'| = p$. Therefore, Theorem 1.2.3 applies.

Now we may assume $P$ is not normal in $G$. Then by Sylow's Theorem, $n_p|49$ and $n_p \equiv 1 \pmod{p}$, where $n_p$ is the number of Sylow $p$-subgroups in $G$. Thus, $p \in \{2, 3\}$, so $|G| \in \{14q, 21q\}$. Therefore, Theorem 1.1.2(1) applies. □

## 1.6 Description of the proof of part (1) of Theorem 1.1.2

In this section we provide a very brief description of methods that D. Morris and K. Wilk have used in [41] to prove Theorem 1.1.2 (1).

In a series of papers published in 2011 and 2012 [15, 20, 21, 33], it has been proved that every connected Cayley graph on $G$ of order $kp$ has a Hamiltonian cycle (unless $kp = 2$), where $1 \leqslant k \leqslant 31$ ($k \neq 24$) and $p$ is prime. These results were verified by hand and the proofs contain many calculations and other details that are not very easy to check quickly. On the other hand, most of the results in Morris-Wilk's paper are established by using a computer, instead of being verified by hand. In fact, they used the computer algebra system GAP [24] for group-theoretic calculations, and used G. Helsgaun's computer program LKH [26] to find Hamiltonian cycles in many thousands of Cayley graphs. In the following paragraph we state the Schur-Zassenhaus Theorem, then we describe Morris-Wilk's method.

**Theorem 1.6.1** (Schur-Zassenhaus Theorem [25, Theorem 15.2.2 on page 224])**.** *If $G$ is a finite group, and $N$ is a normal subgroup whose order is coprime to the order of the quotient group $G/N$, then $G$ is semidirect product of $N$ and $G/N$.*

*Idea of proof of Theorem 1.1.2(1)[41, page 2].* If $kp$ is not too large, then the computer program LKH can find a Hamiltonian cycle in any Cayley graph of order $kp$. So large primes are the main problem. If $G$ is a group of order $kp$, where $p > k$, then Sylow's Theorem implies $G$ has a unique Sylow $p$-subgroup which can be identified with $\mathcal{C}_p$. The uniqueness implies $\mathcal{C}_p \lhd G$. Let $\overline{G} = G/\mathcal{C}_p$, so $|\overline{G}| = k$. Since $\mathcal{C}_p$ is cyclic, then by Factor Group Lemma 1.2.6, it suffices to find a Hamiltonian cycle in $\mathrm{Cay}(\overline{G}; \overline{S})$ whose voltage generates $\mathcal{C}_p$.

The problem is that there are infinitely many primes $p$ so a given group $\overline{G}$ of order $k$ is the quotient of infinitely many different groups $G$ of order $kp$. By Theorem 1.6.1 $G = \overline{G} \ltimes \mathcal{C}_p$. Using this fact, Morris and Wilk construct finitely many semidirect products of the form $\widetilde{G} = \overline{G} \ltimes Z$ (where $Z$ is a finitely generated abelian group), such that, for every $p > k$, every group $G$ of order $kp$ is a quotient of some $\widetilde{G}$. In almost all of the cases, they used a computer search to find a Hamiltonian cycle whose voltage in $Z$ is non-trivial. Then if $p$ is not a divisor of that voltage, they could apply Factor Group Lemma 1.2.6. Finally, they verified the exceptional cases by hand to complete the proof of their result. $\square$

# Chapter 2

# Preliminaries

This chapter establishes basic terminology and notation, and proves a number of technical results that will be used in the proof of Theorem 1.1.3. In particular, it is shown we may assume that $|G|$ is square-free, so the Sylow subgroups of $G$ are $\mathcal{C}_2$, $\mathcal{C}_3$, $\mathcal{C}_p$, and $\mathcal{C}_q$, and that $|G'|$ has precisely 2 prime factors, so $G'$ is either $\mathcal{C}_p \times \mathcal{C}_q$ or $\mathcal{C}_3 \times \mathcal{C}_p$.

## 2.1 Basic notation and definitions

Throughout the thesis, as already mentioned in Section 1.2, we have used standard terminology of graph theory and group theory that can be found in textbooks, such as [23, 25].

The following notation is used through the thesis:

- The commutator of $g$ and $h$ is denoted by $[g, h] = ghg^{-1}h^{-1}$.
- $C_{G'}(S)$ denotes the centralizer of $S$ in $G'$.
- $G \ltimes H$ denotes a semidirect product of groups $G$ and $H$.
- $D_{2n}$ denotes the dihedral group of order $2n$.
- $e$ denotes the identity element of $G$.
- Given a fixed normal subgroup $N$ of $G$, we define $\overline{G} = G/N$, $\overline{g} = gN$ for any $g \in G$, and $\overline{S} = \{\overline{g}; g \in S\}$ for any $S \subseteq G$.
- For $S \subseteq G$, a sequence $(s_1, s_2, \ldots, s_n)$ of elements of $S \cup S^{-1}$ specifies the walk in the Cayley graph $\mathrm{Cay}(G; S)$ that visits the vertices: $e, s_1, s_1s_2, \ldots, s_1s_2 \cdots s_n$.

Also, $(s_1, s_2, \ldots, s_n)^{-1} = (s_n^{-1}, s_{n-1}^{-1}, \ldots, s_1^{-1})$.

- We use $(\overline{s_1}, \overline{s_2}, \overline{s_3}, \ldots, \overline{s_n})$ to denote the image of this walk in the quotient $\mathrm{Cay}(G/G'; \overline{S}) = \mathrm{Cay}(\overline{G}; \overline{S})$.
- If the walk $C = (\overline{s_1}, \overline{s_2}, \ldots, \overline{s_n})$ in $\mathrm{Cay}(G/G'; \overline{S})$ is closed, then its *voltage* is the product $\mathbb{V}(C) = s_1 s_2 \cdots s_n$. This is an element of $G'$.
- For $k \in \mathbb{Z}^+$, we use $(s_1, s_2, \ldots, s_m)^k$ to denote the concatenation of $k$ copies of the sequence $(s_1, s_2, \ldots, s_m)$.
- $\mathcal{C}_n$ denotes the cyclic group of order $n$. When $|G| = 6pq$ (as is usually the case in Chapter 3), the Sylow subgroups are $\mathcal{C}_2$, $\mathcal{C}_3$, $\mathcal{C}_p$, and $\mathcal{C}_q$. Also, the commutator subgroup $G'$ will usually be either $\mathcal{C}_p \times \mathcal{C}_q$ or $\mathcal{C}_3 \times \mathcal{C}_p$, so $\mathcal{C}_p$ is a normal subgroup and either $\mathcal{C}_q$ or $\mathcal{C}_3$ is also a normal subgroup.
- $\overline{G} = G/G'$ and $\widehat{G} = G/\mathcal{C}_p$. Also, we let $\check{G} = G/\mathcal{C}_q$ when $\mathcal{C}_q$ is a normal subgroup, and let $\widehat{G} = G/\mathcal{C}_3$ when $\mathcal{C}_3$ is a normal subgroup.
- We let $a_2$, $a_3$, $\gamma_p$, and $a_q$ be elements of $G$ that generate $\mathcal{C}_2$, $\mathcal{C}_3$, $\mathcal{C}_p$, and $\mathcal{C}_q$, respectively.

## 2.2 Some facts from group theory

In this section we state some facts in group theory, which are used to prove our main result. The following lemmas often makes it possible to use Factor Group Lemma 1.2.6 for finding Hamiltonian cycles in connected Cayley graphs of $G$.

**Lemma 2.2.1** ([15, Corollary 4.4])**.** *Assume $G = \langle a, b \rangle$ and $G'$ is cyclic. Then $G' = \langle [a, b] \rangle$.*

*Proof.* Since every subgroup of a cyclic, normal subgroup is normal in the larger group, we know $\langle [a, b] \rangle \lhd G$. Since $\langle a, b \rangle = G$, and $a$ commutes with $b$ in $G/\langle [a, b] \rangle$, then $G/\langle [a, b] \rangle$ is abelian. So $G' \subseteq \langle [a, b] \rangle$. Also, clearly $\langle [a, b] \rangle \subseteq G'$. Therefore, $G' = \langle [a, b] \rangle$. □

**Corollary 2.2.2.** *Assume* $G = \langle a, b\rangle$ *and* $\gcd(k, |a|) = 1$*, where* $k \in \mathbb{Z}$*, and* $G'$ *is cyclic. Then* $G' = \langle [a^k, b]\rangle$*.*

**Lemma 2.2.3.** *Assume* $G = (\mathcal{C}_p \times \mathcal{C}_q) \ltimes (\mathcal{C}_r \times \mathcal{C}_t)$*, where* $p, q, r$ *and* $t$ *are distinct primes. If* $|\overline{a}| = pq$*, then* $|a| = pq$*.*

*Proof.* Suppose $|a| \neq pq$. Without loss of generality, assume $|a|$ is divisible by $r$. Then (after replacing $a$ by a conjugate) the abelian group $\langle a\rangle$ contains $\mathcal{C}_p \times \mathcal{C}_q$ and $\mathcal{C}_r$, so $\mathcal{C}_r$ centralizes $\mathcal{C}_p \times \mathcal{C}_q$. Since $\mathcal{C}_r$ also centralizes $\mathcal{C}_t$, this implies that $\mathcal{C}_r \subseteq Z(G)$. This contradicts the fact that $G' \cap Z(G) = \{e\}$ (see Proposition 1.3.12(2)). □

## 2.3 Cayley graphs that contain a Hamiltonian cycle

In this section we show that there exists a Hamiltonian cycle in some special connected Cayley graphs. The following proposition shows that in our proof of Theorem 1.1.3 we can assume $|G|$ is square-free, since the cases where $|G|$ is not square-free have already been dealt with.

**Proposition 2.3.1.** *Assume:*

- $|G| = 6pq$*, where* $p$ *and* $q$ *are distinct prime numbers, and*
- $|G|$ *is not square-free (i.e.* $\{p, q\} \cap \{2, 3\} \neq \varnothing$*).*

*Then every connected Cayley graph on* $G$ *has a Hamiltonian cycle.*

*Proof.* Without loss of generality we may assume $q \in \{2, 3\}$. Then $|G| \in \{12p, 18p\}$. Therefore, Theorem 1.1.2(1) applies. □

The following proposition demonstrates that we can assume $|G'|$ in Theorem 1.1.3 is a product of two distinct prime numbers.

**Proposition 2.3.2.** *Assume* $|G| = 2pqr$*, where* $p$*,* $q$ *and* $r$ *are distinct odd prime numbers. Now if* $|G'| \in \{1, pqr\}$ *or* $|G'|$ *is prime, then every connected Cayley graph on* $G$ *has a Hamiltonian cycle.*

*Proof.* If $|G'| = 1$, then $G' = \{e\}$. So $G$ is an abelian group. Therefore, Lemma 1.2.2 applies. Now if $|G'|$ is prime, then Corollary 1.4.5 applies. Finally, if $|G'| = pqr$, then

$$G = \mathcal{C}_2 \ltimes (\mathcal{C}_p \times \mathcal{C}_q \times \mathcal{C}_r) \cong D_{2pqr}.$$

So Proposition 1.5.2 applies. □

The next theorem tells us that if we have a finite group that can be broken into a semidirect product of two cyclic subgroups, then there is a Hamiltonian cycle in the connected Cayley graph of this group that comes from the generators of the factors.

**Theorem 2.3.3** (B. Alspach [2, Corollary 5.2])**.** *If $G = \langle s \rangle \ltimes \langle t \rangle$, for some elements $s$ and $t$ of $G$, then* $\mathrm{Cay}(G; \{s, t\})$ *has a Hamiltonian cycle.*

The following lemmas show that some special Cayley graphs have a Hamiltonian cycle, and we use these facts in Chapter 3 in order to prove our main result.

**Lemma 2.3.4.** *Assume $G = (\mathcal{C}_2 \times \mathcal{C}_r) \ltimes G'$, and $G' = \mathcal{C}_p \times \mathcal{C}_q$, where $p$, $q$ and $r$ are distinct prime numbers and let $S = \{a, b\}$ be a generating set of $G$. Additionally, assume $|\overline{a}| \in \{2, 2r\}$, $|\overline{b}| = r$ and* $\gcd(|b|, r-1) = 1$. *Then* $\mathrm{Cay}(G; S)$ *contains a Hamiltonian cycle.*

*Proof.* We have $C = (\overline{b}^{r-1}, \overline{a}, \overline{b}^{-(r-1)}, \overline{a}^{-1})$ as a Hamiltonian cycle in $\mathrm{Cay}(\overline{G}; \overline{S})$. Now we calculate its voltage

$$\mathbb{V}(C) = b^{r-1} a b^{-(r-1)} a^{-1} = [b^{r-1}, a].$$

Since $\gcd(|b|, r-1) = 1$, then by Lemma 2.2.2 we have $[b^{r-1}, a] = G'$. Therefore, Factor Group Lemma 1.2.6 applies. □

**Lemma 2.3.5** (cf. [21, Case 2 of proof of Theorem 1.1, pages 3619-3620])**.** *Assume*

- $G = (\mathcal{C}_2 \times \mathcal{C}_r) \ltimes (\mathcal{C}_p \times \mathcal{C}_q)$,

- $|S| = 3$,
- $\widehat{S}$ *is a minimal generating set of* $\widehat{G} = G/\mathcal{C}_p$,
- $\mathcal{C}_r$ *centralizes* $\mathcal{C}_q$,
- $\mathcal{C}_2$ *inverts* $\mathcal{C}_q$.

*Then,* $\operatorname{Cay}(G; S)$ *contains a Hamiltonian cycle.*

**Lemma 2.3.6** ([21, Lemma 2.6])**.** *Assume:*

- $G = \langle a \rangle \ltimes \langle S_0 \rangle$, *where* $\langle S_0 \rangle$ *is an abelian subgroup of odd order,*
- $|(S_0 \cup S_0^{-1})| \geqslant 3$, *and*
- $\langle S_0 \rangle$ *has a nontrivial subgroup* $H$, *such that* $H \lhd G$ *and* $H \cap Z(G) = \{e\}$.

*Then* $\operatorname{Cay}(G; S_0 \cup \{a\})$ *has a Hamiltonian cycle.*

*Proof.* ([21, Lemma 2.6]) Since $\langle S_0 \rangle$ is abelian of odd order, and $|(S_0 \cup S_0^{-1})| \geqslant 3$, by Theorem 1.2.4 $\operatorname{Cay}(\langle S_0 \rangle; S_0)$ has a Hamiltonian path $(s_1, s_2, \ldots, s_m)$, such that $s_1 s_2 \cdots s_m \in H$. Note that

$$\begin{aligned}(s_1 s_2 \cdots s_m a)^{|a|} &= (a a^{-1} s_1 s_2 \cdots s_m a)^{|a|} = (a (s_1 s_2 \cdots s_m)^a)^{|a|} \\ &= (s_1 s_2 \cdots s_m)^{a^{|a|-1} + a^{|a|-2} + \cdots + a + 1}.\end{aligned}$$

Since this is a product of all possible $\langle a \rangle$-conjugation of $s_1 s_2 \cdots s_m$ and it is abelian, then it commutes with $a$ and $\langle S_0 \rangle$. So

$$(s_1 s_2 \cdots s_m)^{a^{|a|-1} + a^{|a|-2} + \cdots + a + 1} \in Z(G) \cap H.$$

Therefore,

$$(s_1 s_2 \cdots s_m)^{a^{|a|-1} + a^{|a|-2} + \cdots + a + 1} = e.$$

Therefore, we have $(s_1, s_2, \ldots, s_m, a)^{|a|}$ as a Hamiltonian cycle in $\operatorname{Cay}(G; S_0 \cup \{a\})$. $\square$

**Lemma 2.3.7** ([21, Lemma 2.9]). *If $G = D_{2pq} \times \mathcal{C}_r$, where $p, q$ and $r$ are distinct odd primes, then every connected Cayley graph on $G$ has a Hamiltonian cycle.*

*Proof.* ([21, Lemma 2.9]) Let $S$ be a minimal generating set of $G$, let $\varphi : G \to D_{2pq}$ be the projection such that $\varphi(F, i) = F$, where $F \in D_{2pq}$ and $i \in \mathcal{C}_r$, and let $T$ be the group of rotations in $D_{2pq}$, so it is obvious that $T = \mathcal{C}_p \times \mathcal{C}_q$.

For $s \in S$ we may assume that $\varphi(s)$ is nontrivial, because otherwise $s \in \mathcal{C}_r \subseteq Z(G)$, therefore Lemma 1.2.11 applies.

Suppose there exists $s \in S$ such that $\varphi(s)$ has order 2, but $|s| \neq 2$. Then we may assume $\varphi(S)$ is not minimal, for otherwise Corollary 1.2.7 applies with $N = \mathcal{C}_r$ and $t = s^{-1}$. Therefore, if we let $S' = S \backslash \{s\}$, then $\langle S' \rangle = D_{2pq} = \mathcal{C}_2 \ltimes (\mathcal{C}_p \times \mathcal{C}_q)$. We may assume $S' \cap (\mathcal{C}_p \times \mathcal{C}_q) = \varnothing$, for otherwise there is an element $s'_1 \in S'$ such that $s'_1 \in \mathcal{C}_p \times \mathcal{C}_q$, and there is a Hamiltonian cycle in $\mathrm{Cay}(D_{2pq}/\langle s'_1 \rangle; S')$ (see Proposition 1.5.2), so Lemma 1.2.11(2) applies. Thus, $|s'| = 2$ for all $s' \in S'$.

We may now assume $a_2 \in S'$. Let $b = a_2 a_p^i a_q^j$ be another element of $S'$. Since $i$ and $j$ cannot both be 0, we may assume $i = 1$.

We claim that $\langle a_2, b \rangle = D_{2pq}$. If not, then $j = 0$. There is some $c = a_2 a_p^k a_q^\ell \in S'$ with $\ell \neq 0$. The minimality of $S$ implies $\langle a_2, c \rangle \neq D_{2pq}$, so $k = 0$. Then $\langle b, c \rangle = D_{2pq}$, which contradicts the minimality of $S$. This completes the proof of the claim.

This claim means $j \neq 0$, so we may assume $j = 1$, which means $b = a_2 a_p a_q$. Write $s = a_2 a_p^m a_q^n a_r$. The minimality of $S$ implies that $\langle a_2, s \rangle \neq G$, so either $m = 0$ or $n = 0$. Assume, without loss of generality, that $n = 0$. Now, the minimality of $S$ implies that $\langle b, s \rangle \neq G$, so we must have $m = 1$. This means $s = a_2 a_p a_r$. So $s \equiv b$ (mod $\mathcal{C}_q \times \mathcal{C}_r$).

Let $\breve{G} = G/(\mathcal{C}_q \times \mathcal{C}_r) \cong D_{2p}$, so $\breve{s} = \breve{b}$. We have the following two Hamiltonian cycles in $\mathrm{Cay}(\breve{G}; \breve{S})$:

$$C_1 = ((\breve{a}_2, \breve{b})^{p-1}, (\breve{a}_2, \breve{s})),$$

$$C_2 = ((\breve{a}_2, \breve{b})^{p-2}, (\breve{a}_2, \breve{s})^2).$$

Their voltages are:

$$V(C_1) = (a_2 b)^{p-1}(a_2 s) = (a_2 \cdot a_2 a_p a_q)^{p-1}(a_2 \cdot a_2 a_p a_r) = a_q^{p-1} a_r,$$
$$V(C_2) = (a_2 b)^{p-2}(a_2 s)^2 = (a_2 \cdot a_2 a_p a_q)^{p-2}(a_2 \cdot a_2 a_p a_r)^2 = a_q^{p-2} a_r^2.$$

Since at least one of $p-1$ and $p-2$ is relatively prime to $q$ (and 1 and 2 are relatively prime to $r$), we know that at least one of these voltages generates $\mathcal{C}_q \times \mathcal{C}_r$. So Factor Group Lemma 1.2.6 applies.

Thus, we may assume that for any $s \in S$, if $\varphi(s)$ has order 2, then $s = \varphi(s)$ has order 2.

Since $\varphi(S)$ generates $D_{2pq}$, it must contain at least one reflection (which is an element of order 2). So $S \cap D_{2pq}$ contains a reflection.

**Case 1.** Assume $S \cap D_{2pq}$ contains only one reflection. Let $a \in S \cap D_{2pq}$, such that $a$ is a reflection. Let $S_0 = S \backslash \{a\}$. Since $\langle S_0 \rangle$ is a subgroup of the cyclic, normal subgroup $T \times \mathcal{C}_r$, we know $\langle S_0 \rangle$ is normal. Therefore $G = \langle a \rangle \ltimes \langle S_0 \rangle$, so:

- If $|S_0| = 1$, then Theorem 2.3.3 applies.
- If $|S_0| \geqslant 2$, then 2.3.6 applies with $H = T$, because $T \times \mathcal{C}_r$ is an abelian subgroup of odd order.

**Case 2.** Assume $S \cap D_{2pq}$ contains at least two reflections. Since no minimal generating set of $D_{2pq}$ contains three reflections, the minimality of $S$ implies that $S \cap D_{2pq}$ contains exactly two reflections; $a$ and $b$ are reflections. Let $c \in S \backslash \{D_{2pq}\}$, so $\mathcal{C}_r \subseteq \langle c \rangle$. Since $|c| > 2$, we know $\varphi(c)$ is not a reflection, so $\varphi(c) \in T$. The minimality of $S$ and the fact that $|S| > 2$ implies $\langle \varphi(c) \rangle \neq T$. Since $\varphi(c)$ is nontrivial, this implies we may assume $\langle \varphi(c) \rangle = \mathcal{C}_p$ (by interchanging $p$ and $q$ if necessary). Hence, we may write $c = wz$ with $\langle w \rangle = \mathcal{C}_p$ and $\langle z \rangle = \mathcal{C}_r$. We now use the argument of ([29, Case

5.3, p. 96]), which is based on ideas of Marušič [37] that are explained in Section 1.4. Let $\overline{G} = G/\mathcal{C}_p = \overline{D_{2pq}} \times \mathcal{C}_r = \overline{D_{2pq}} \times \langle \overline{c} \rangle$. Then $\overline{D_{2pq}} \equiv D_{2q}$, so $(a, b)^q$ is a Hamiltonian cycle in $\mathrm{Cay}(\overline{D_{2pq}}; \{a, b\})$. With this in mind it is easy to see that

$$(c^{r-1}, a, ((b, a)^{q-1}, c^{-1}, (a, b)^{q-1}, c^{-1})^{(r-1)/2}, (b, a)^{q-1}, b)$$

is a Hamiltonian cycle in $\mathrm{Cay}(\overline{G}; S)$. This contains the string

$$(c, a, (b, a)^{q-1}, c^{-1}, a),$$

which can be replaced with the string

$$(b, c, (b, a)^{q-1}, b, c^{-1})$$

to obtain another Hamiltonian cycle. Since $ba \in T$ is inverted by $a$

$$ca(ba)^{q-1}c^{-1}a = (cac^{-1}a)(ba)^{-(q-1)}$$

$c = wz$, therefore

$$(cac^{-1}a)(ba)^{-(q-1)} = ((wz)a(wz)^{-1}a)(ba)^{-(q-1)}$$

now $a$ inverts $w$ and centralizes $z$, then

$$((wz)a(wz)^{-1}a)(ba)^{-(q-1)} = (w^2)(ba)^{-(q-1)},$$

clearly

$$(w^2)(ba)^{-(q-1)} \neq (w^{-2})(ba)^{-(q-1)}$$

we know that $b$ inverts $w$ and centralizes $z$, so

$$(w^{-2})(ba)^{-(q-1)} = (b(wz)b(wz)^{-1})(ba)^{-(q-1)} = (bcbc^{-1})(ba)^{-(q-1)},$$

since $ba \in T$ is inverted by $b$, then

$$(bcbc^{-1})(ba)^{-(q-1)} = bc(ba)^{q-1}bc^{-1}.$$

Therefore,

$$(cac^{-1}a)(ba)^{-(q-1)} \neq bc(ba)^{q-1}bc^{-1}.$$

And this implies that we have two Hamiltonian cycles that have different voltages. Therefore at least one of them must have a nontrivial voltage. This nontrivial voltage must generate $\mathcal{C}_p$, so Factor Group Lemma 1.2.6 applies and there is a Hamiltonian cycle in $\mathrm{Cay}(G; S)$. □

## 2.4 Some specific sets that generate $G$

This section presents a few results that provide conditions under which certain 2-element subsets generate $G$. Obviously, no 3-element minimal generating set can contain any of these subsets.

**Lemma 2.4.1.** *Assume $G = (\mathcal{C}_2 \times \mathcal{C}_3) \ltimes G'$, and $G' = \mathcal{C}_p \times \mathcal{C}_q$. Also, assume $C_{G'}(\mathcal{C}_3) = \mathcal{C}_q$ and $\mathcal{C}_q \nsubseteq C_{G'}(\mathcal{C}_2)$. If $(a, b)$ is one of the following ordered pairs*

1. $(a_3 a_q, a_2 a_3^j a_q^k \gamma_p)$,
2. $(a_2 a_3, a_3^j a_q^k \gamma_p)$, *where* $k \not\equiv 0 \pmod{q}$,
3. $(a_2 a_3 a_q, a_3^j a_q^k \gamma_p)$, *where* $k \not\equiv 0 \pmod{q}$,
4. $(a_2 a_3 a_q, a_2 a_3^j a_q^k \gamma_p)$, *where* $k \not\equiv 1 \pmod{q}$,

*then* $\langle a, b \rangle = G$.

*Proof.* It is easy to see that $(\overline{a}, \overline{b}) = \overline{G}$, so it suffices to show that $\langle a, b\rangle$ contains $\mathcal{C}_p$ and $\mathcal{C}_q$. Thus, it suffices to show that $\breve{G}$ and $\breve{G}$ are nonabelian, where $\breve{G} = G/(\mathcal{C}_3 \ltimes \mathcal{C}_p) \cong D_{2q}$ and $\breve{G} = G/C_q$.

Since $a_3$ does not centralize $\mathcal{C}_p$, it is clear in each of $(1) - (4)$ that $\breve{a}$ does not centralize $\gamma_p$ (and $\gamma_p$ is one of the factors in $\breve{b}$), so $\breve{G}$ is not abelian.

The pair $(\breve{a}, \breve{b})$ is either $(a_q, a_2 a_q^k)$, $(a_2, a_q^k)$ where $k \not\equiv 0 \pmod q$, $(a_2 a_q, a_q^k)$ where $k \not\equiv 0 \pmod q$, or $(a_2 a_q, a_2 a_q^k)$ where $k \not\equiv 1 \pmod q$. Each of these is either a reflection and a nontrivial rotation or two different reflections, and therefore generates the (nonabelian) dihedral group $D_{2q} = \breve{G}$. □

**Lemma 2.4.2.** *Assume $G = (\mathcal{C}_2 \times \mathcal{C}_3) \ltimes G'$, and $G' = \mathcal{C}_p \times \mathcal{C}_q$. Also, assume $C_{G'}(\mathcal{C}_3) = \{e\}$. If $(a, b)$ is one of the following ordered pairs*

1. $(a_2 a_3, a_2^i a_3^j a_q^k \gamma_p)$, *where* $k \not\equiv 0 \pmod q$,
2. $(a_3 a_q, a_2 a_3^j \gamma_p)$, *where* $j \not\equiv 0 \pmod 3$,
3. $(a_3, a_2 a_3^j a_q^k \gamma_p)$, *where* $k \not\equiv 0 \pmod q$,
4. $(a_2 a_3 a_q, a_2^i a_3^j \gamma_p)$, *where* $j \not\equiv 0 \pmod 3$,

*then* $\langle a, b\rangle = G$.

*Proof.* It is easy to see that $(\overline{a}, \overline{b}) = \overline{G}$, so it suffices to show that $\langle a, b\rangle$ contains $\mathcal{C}_p$ and $\mathcal{C}_q$. we need to show that $\widehat{G}$ and $\breve{G}$ are nonabelian, where $\widehat{G} = G/\mathcal{C}_p$ and $\breve{G} = G/\mathcal{C}_q$, as usual.

As in the proof of Lemma 2.4.1, since $a_3$ does not centralize $\mathcal{C}_p$, it is clear in each of $(1) - (4)$ that $\breve{a}$ does not centralize $\gamma_p$ (and $\gamma_p$ is one of the factors in $\breve{b}$), so $\breve{G}$ is not abelian.

In $(1) - (4)$, $a_q$ appears in one of the generators in $(\widehat{a}, \widehat{b})$, but not the other, and the other generator does have an occurrence of $a_3$. Since $a_3$ does not centralize $a_q$, this implies that $\widehat{G}$ is not abelian. □

**Lemma 2.4.3.** *Assume* $G = (\mathcal{C}_2 \times \mathcal{C}_q) \ltimes G'$*, and* $G' = \mathcal{C}_3 \times \mathcal{C}_p$*. Also, assume* $C_{G'}(\mathcal{C}_q) = \mathcal{C}_3$ *and* $\mathcal{C}_3 \nsubseteq C_{G'}(\mathcal{C}_2)$*. If* $(a, b)$ *is one of the following ordered pairs*

1. $(a_2 a_q, a_2^i a_q^j a_3^k \gamma_p)$*, where* $k \not\equiv 0 \pmod q$*,*
2. $(a_q a_3, a_2 a_q^j a_3^k \gamma_p)$*,*
3. $(a_2^i a_q^m a_3, a_2 a_q^j \gamma_p)$*, where* $m \not\equiv 0 \pmod q$*,*

*then* $G = \langle a, b \rangle$*.*

*Proof.* It is easy to see that $(\overline{a}, \overline{b}) = \overline{G}$, so it suffices to show that $\langle a, b\rangle$ contains $\mathcal{C}_p$ and $\mathcal{C}_3$. We need to show that $\breve{G}$ and $\widehat{G}$ are nonabelian, where $\breve{G} = G/(\mathcal{C}_q \ltimes \mathcal{C}_p) \cong D_6$ and $\widehat{G} = G/\mathcal{C}_3$.

In each of $(1) - (4)$, $a_q$ appears in $\widehat{a}$, and $\gamma_p$ appears in $\widehat{b}$ (but not in $\widehat{a}$). Since $a_q$ does not centralize $\gamma_p$, this implies that $\widehat{G}$ is not abelian.

In each of $(1) - (4)$, $(\widehat{a}, \widehat{b})$ consists of either a reflection and a nontrivial rotation or two different reflections, so it generates the (nonabelian) dihedral group $D_6 = \widehat{G}$. □

## 2.5 Methods of calculating voltage

In this section, we present some methods of calculating the voltage of a Hamiltonian cycle. These techniques will be used repeatedly in Chapter 3.

**Lemma 2.5.1.** *Assume* $G = H \ltimes (\mathcal{C}_p \times \mathcal{C}_q)$*, where* $G' = \mathcal{C}_p \times \mathcal{C}_q$*, and let* $S$ *be a generating set of* $G$*. As usual, let* $\widehat{G} = G/\mathcal{C}_p$ *and* $\breve{G} = G/\mathcal{C}_q$*. If* $\widehat{\mathbb{V}(C)}$ *and* $\breve{\mathbb{V}(C)}$ *are nontrivial elements of* $G'$*, then* $\mathbb{V}(C)$ *generates* $G'$*.*

*Proof.* Since $\mathbb{V}(C)$ is contained in $G'$, then $\mathbb{V}(C) = a_q^i \gamma_p^j$, where $0 \leqslant i \leqslant q-1$ and $0 \leqslant j \leqslant p-1$. Then $a_q^i = \widehat{\mathbb{V}(C)}$ is nontrivial, so $i \neq 0$. Similarly, $\gamma_p^j = \breve{\mathbb{V}(C)}$ is nontrivial, so $j \neq 0$. Therefore $a_q^i \gamma_p^j$ generates $\mathcal{C}_p \times \mathcal{C}_q = G'$. □

The above lemma means that if $\mathbb{V}(C)$ is nontrivial modulo $\mathcal{C}_p$ and is also nontrivial modulo $\mathcal{C}_q$, then $\mathbb{V}(C)$ generates $G'$. This observation will be used repeatedly in Chapter 3.

**Lemma 2.5.2.** *Assume $G = H \ltimes (\mathcal{C}_p \times \mathcal{C}_q)$, where $G' = \mathcal{C}_p \times \mathcal{C}_q$, and let $S$ be a generating set of $G$. As usual, let $\overline{G} = G/G' \cong H$. Assume there is a unique element $c$ of $S$ that is not in $H \ltimes \mathcal{C}_q$, and $C$ is a Hamiltonian cycle in $\mathrm{Cay}(\overline{G}; \overline{S})$ such that $c$ occurs precisely once in $C$. Then the subgroup generated by $\mathbb{V}(C)$ contains $\mathcal{C}_p$.*

*Proof.* Write $C = (\overline{s}_1, \overline{s}_2, \cdots, \overline{s}_n)$, and let $H^+ = H \ltimes \mathcal{C}_q$. By assumption, there is a unique $k$, such that $s_k = c$, and all other elements of $S$ are in $H^+$. Therefore,

$$\mathbb{V}(C) = s_1 s_2 ... s_n \in H^+ \cdot H^+ \cdots H^+ \cdot c \cdot H^+ \cdot H^+ \cdots H^+ = H^+ c H^+.$$

Since $c \notin H^+$, we conclude that $\mathbb{V}(C) \notin H^+$.

On the other hand, since $\mathbb{V}(C)$ is an element of $G' = \mathcal{C}_p \times \mathcal{C}_q$, we have $\mathbb{V}(C) = a_q^i \gamma_p^j \in H^+ \gamma_p^j$. Since $\mathbb{V}(C) \notin H^+$, this implies $j \not\equiv 0 \pmod{p}$, so $\langle a_q^i \gamma_p^j \rangle$ contains $\mathcal{C}_p$. □

**Lemma 2.5.3.** *Assume $a, \gamma \in G$, and there exists $\tau \in \mathbb{Z}$, such that $a\gamma a^{-1} = \gamma^\tau$. If $\tau^k \neq 1$, then*

$$(a^k \gamma^m)^n = \gamma^{m\tau^k(\tau^{nk}-1)/(\tau^k-1)} a^{nk}.$$

*Proof.* For all $i \in \mathbb{Z}$, we have $a^{ik}\gamma^m = \gamma^{m\tau^{ik}} a^{ik}$. Therefore,

$$\begin{aligned}
(a^k\gamma^m)^n &= a^k\gamma^m \cdot (a^k\gamma^m)^{(n-1)} \\
&= \gamma^{m\tau^k} a^k \cdot a^k\gamma^m \cdot (a^k\gamma^m)^{(n-2)} \\
&= \gamma^{m\tau^k + m\tau^{2k}} a^{2k} \cdot a^k\gamma^m \cdot (a^k\gamma^m)^{(n-3)} \\
&\;\;\vdots \\
&= \gamma^{m\tau^k + m\tau^{2k} + \cdots + m\tau^{nk}} \cdot a^{nk} \\
&= \gamma^{m\tau^k(1 + \tau^k + \tau^{2k} + \cdots + \tau^{(n-1)k})} \cdot a^{nk} \\
&= \gamma^{m\tau^k(\tau^{nk}-1)/(\tau^k-1)} \cdot a^{nk}.
\end{aligned}$$

□

**Remark 2.5.4.** In the situation of Lemma 2.5.3, if $\tau^k = 1$, then $a^k$ commutes with $\gamma$. So $(a^k\gamma^m)^n = \gamma^{nm}a^{nk}$.

# Chapter 3

# Proof of the Main Result

In this chapter we prove Theorem 1.1.3, which is the main result. We are given a generating set $S$ of a finite group $G$ of order $6pq$, where $p$ and $q$ are distinct prime numbers, and we wish to show $\mathrm{Cay}(G;S)$ contains a Hamiltonian cycle. The proof is a long case-by-case analysis. (See Figures 3.1, 3.2 and 3.3 on pages 51−53 for outlines of the many cases that are considered.) Here are our main assumptions through the whole chapter.

**Assumption 3.0.1.** We assume:

1. $p, q > 7$, otherwise Theorem 1.1.2(1) applies.
2. $|G|$ is square-free, otherwise Proposition 2.3.1 applies.
3. $G' \cap Z(G) = \{e\}$, by Proposition 1.3.12(2).
4. $G \cong \mathcal{C}_n \ltimes G'$, by Proposition 1.3.12(3).
5. $|G'| \in \{pq, 3p\}$, by Lemma 1.3.8.
6. For every element $\overline{s} \in \overline{S}$, $|\overline{s}| \neq 1$. Otherwise, if $|\overline{s}| = 1$, then $s \in G'$, so $G' = \langle s \rangle$ or $|s|$ is prime. In each case $\mathrm{Cay}(G/\langle s \rangle; \overline{S})$ has a Hamiltonian cycle by part 2 or 3 of Theorem 1.1.2. By Assumption 3.0.1(3), $\langle s \rangle \cap Z(G) = \{e\}$, therefore, Lemma 1.2.11(2) applies.
7. $S$ is a minimal generating set of $G$. (Note that $S$ must generate $G$, for otherwise $\mathrm{Cay}(G;S)$ is not connected. Also, in order to show that every connected Cayley graph on $G$ contains a Hamiltonian cycle, it suffices to consider $\mathrm{Cay}(G;S)$, where $S$ is a generating set that is minimal.)

See Figures 3.1, 3.2 and 3.3 for outlines of the cases that are considered.

## 3.1 Assume $|S| = 2$ and $G' = \mathcal{C}_p \times \mathcal{C}_q$

In this section we prove the part of Theorem 1.1.3 where, $|S| = 2$ and $G' = \mathcal{C}_p \times \mathcal{C}_q$. Recall $\overline{G} = G/G'$ and $\widehat{G} = G/\mathcal{C}_p$.

I. $|S| = 2$.

A. $G' = \mathcal{C}_p \times \mathcal{C}_q$ (Section 3.1).

1. $\overline{S}$ is a minimal generating set.

2. $\overline{S}$ is not a minimal generating set.

B. $G' = \mathcal{C}_3 \times \mathcal{C}_p$ (Section 3.2).

1. $|\overline{a}| = |\overline{b}| = 2q$.

2. $|\overline{a}| = q$.

3. $|\overline{a}| = 2q$ and $|\overline{b}| = 2$.

4. None of the previous cases apply.

Figure 3.1: Outline of the cases in the proof of Theorem 1.1.3 where $|S| = 2$

**Proposition 3.1.** *Assume*

- $G = (\mathcal{C}_2 \times \mathcal{C}_3) \ltimes (\mathcal{C}_p \times \mathcal{C}_q)$,
- $|S| = 2$.

*Then* $\mathrm{Cay}(G; S)$ *contains a Hamiltonian cycle.*

*Proof.* Let $S = \{a, b\}$. For every $s \in S$, $|\overline{s}| \neq 1$, by Assumption 3.0.1(6).

**Case 1.** Assume $\overline{S}$ is minimal. Then $|\overline{a}|, |\overline{b}| \in \{2, 3\}$. When $|\overline{a}| = |\overline{b}| = 2$ or $|\overline{a}| = |\overline{b}| = 3$, then $\overline{G} \neq \langle \overline{a}, \overline{b} \rangle$. Therefore, $G \neq \langle a, b \rangle$ which contradicts the fact that $G = \langle a, b \rangle$. So we may assume $|\overline{a}| = 2$ and $|\overline{b}| = 3$. Since $|b| \in \{3, 3p, 3q, 3pq\}$, then $\gcd(|b|, 2) = 1$. Thus, Lemma 2.3.4 applies.

II. $|S| = 3$.

A. $G' = \mathcal{C}_p \times \mathcal{C}_q$.

a. $C_{G'}(\mathcal{C}_3) \neq \{e\}$ or $\widehat{S}$ is minimal.

i. $C_{G'}(\mathcal{C}_3) \neq \{e\}$ (Section 3.3).

1. $a = a_2$ and $b = a_q a_3$.
2. $a = a_2$ and $b = a_2 a_q a_3$.
3. $a = a_2 a_3$ and $b = a_2 a_q$.
4. $a = a_2 a_3$ and $b = a_q a_3$.
5. $a = a_2 a_3$ and $b = a_2 a_3 a_q$.

ii. $\widehat{S}$ is minimal (Section 3.4).

1. $C_{G'}(\mathcal{C}_2) = \mathcal{C}_p \times \mathcal{C}_q$.
2. $C_{G'}(\mathcal{C}_2) = \mathcal{C}_q$.
3. $C_{G'}(\mathcal{C}_2) = \mathcal{C}_p$.
4. $C_{G'}(\mathcal{C}_2) = \{e\}$.

b. $C_{G'}(\mathcal{C}_3) = \{e\}$ and $\widehat{S}$ is not minimal.

i. $C_{G'}(\mathcal{C}_2) = \mathcal{C}_p \times \mathcal{C}_q$ (Section 3.5).

1. $a = a_3$ and $b = a_2 a_q$.
2. $a = a_3$ and $b = a_2 a_3 a_q$.
3. $a = a_2 a_3$ and $b = a_3 a_q$.
4. $a = a_2 a_3$ and $b = a_2 a_q$.
5. $a = a_2 a_3$ and $b = a_2 a_3 a_q$.

ii. $C_{G'}(\mathcal{C}_2) \neq \{e\}$ (Section 3.6).

1. $a = a_2 a_3$ and $b = a_2 a_3 a_q$.
2. $a = a_2 a_3$ and $b = a_2 a_q$.
3. $a = a_2 a_3$ and $b = a_3 a_q$.
4. $a = a_3$ and $b = a_2 a_q$.

iii. $C_{G'}(\mathcal{C}_2) = \{e\}$ (Section 3.7).

1. $a = a_2 a_3$ and $b = a_2 a_3 a_q$.
2. $a = a_2 a_3$ and $b = a_2 a_q$.
3. $a = a_2 a_3$ and $b = a_3 a_q$.
4. $a = a_3$ and $b = a_2 a_q$.

B. $G' = \mathcal{C}_3 \times \mathcal{C}_p$. (Section 3.8).

1. $a = a_2 a_q$ and $b = a_2 a_q^m a_3$.
2. $a = a_2 a_q$ and $b = a_2 a_3$.
3. $a = a_2 a_q$ and $b = a_q^m a_3$.
4. $a = a_2$ and $b = a_q a_3$.

Figure 3.2: Outline of the cases in the proof of Theorem 1.1.3 where $|S| = 3$

**Case 2.** Assume $\overline{S}$ is not minimal. Then $\{|\overline{a}|, |\overline{b}|\}$ is either $\{6, 2\}$, $\{6, 3\}$, or $\{6\}$. We may assume $|\overline{a}| = 6$.

**Subcase 2.1.** Assume $|\overline{b}| = 2$. So we have $\overline{b} = \overline{a}^3$, then $b = a^3\gamma$, where $G' = \langle\gamma\rangle$

III. $|S| \geqslant 4$ (Section 3.9). This part of the proof applies whenever $|G| = pqrt$ with $p$, $q$, $r$, and $t$ distinct primes.

1. $|G'|$ has only two prime factors.

2. $|G'|$ has three prime factors.

Figure 3.3: Outline of the cases in the proof of Theorem 1.1.3 where $|S| \geqslant 4$

(otherwise $\langle a, b\rangle = \langle a, a^3\gamma\rangle = \langle a, \gamma\rangle \neq G$ which contradicts the fact that $G = \langle a, b\rangle$). Now by Proposition 1.3.12(4), we have $\tau \in \mathbb{Z}^+$ such that $a\gamma a^{-1} = \gamma^\tau$ and $\tau^6 \equiv 1 \pmod{pq}$, also $\gcd(\tau - 1, pq) = 1$. This implies that $\tau \not\equiv 1 \pmod{p}$ and $\tau \not\equiv 1 \pmod{q}$. We have $C_1 = (\overline{a}^2, \overline{b}, \overline{a}^{-2}, \overline{b}^{-1})$ as a Hamiltonian cycle in $\mathrm{Cay}(\overline{G}; \overline{S})$. Now we calculate its voltage.

$$\mathbb{V}(C_1) = a^2ba^{-2}b^{-1} = a^2a^3\gamma a^{-2}\gamma^{-1}a^{-3} = \gamma^{\tau^5 - \tau^3} = \gamma^{\tau^3(\tau^2-1)}.$$

We may assume $\gcd(\tau^2 - 1, pq) \neq 1$ (otherwise Factor Group Lemma 1.2.6 applies). Without loss of generality let $\tau^2 \equiv 1 \pmod{q}$, then $\tau \equiv -1 \pmod{q}$. We may assume $\tau \not\equiv -1 \pmod{p}$, for otherwise $G \cong D_{2pq} \times \mathcal{C}_3$, so Lemma 2.3.7 applies.

Consider $\widehat{G} = G/\mathcal{C}_p = \mathcal{C}_6 \ltimes \mathcal{C}_q$. Since $|\overline{a}| = 6$, then by Lemma 2.2.3 $|a| = 6$, so $|\widehat{a}| = 6$. We may assume $|\widehat{b}| = 2$, for otherwise Corollary 1.2.7 applies with $s = b$ and $t = b^{-1}$ since $\langle \widehat{a}\rangle \neq \widehat{G}$, so any Hamiltonian cycle must use an edge labeled $\widehat{b}$. Thus, $\widehat{b} = \widehat{a}^3 a_q$, where $\langle a_q\rangle = \mathcal{C}_q$. Since $\tau \equiv -1 \pmod{q}$, then $\mathcal{C}_3$ centralizes $\mathcal{C}_q$ and $\mathcal{C}_2$ inverts $\mathcal{C}_q$. Therefore, $\widehat{G} \cong D_{2q} \times \mathcal{C}_3$. Now we have

$$C_2 = ((\widehat{a}^5, \widehat{b}, \widehat{a}^{-5}, \widehat{b})^{(q-3)/2}, (\widehat{a}^5, \widehat{b})^3)$$

as a Hamiltonian cycle in $\mathrm{Cay}(\widehat{G}; \widehat{S})$. The picture in Figure 3.4 on page 55 shows the Hamiltonian cycle when $q = 7$. If in $C_2$ we change one occurrence of $(\widehat{a}^5, \widehat{b}, \widehat{a}^{-5}, \widehat{b})$ to

$(\widehat{a}^{-5}, \widehat{b}, \widehat{a}^{5}, \widehat{b})$ we have another Hamiltonian cycle. Note that,

$$a^5ba^{-5}b = a^5 \cdot a^3\gamma \cdot a^{-5} \cdot a^3\gamma = a^2\gamma a^{-2}\gamma = \gamma^{\tau^2+1},$$

and

$$a^{-5}ba^5b = a^{-5} \cdot a^3\gamma \cdot a^5 \cdot a^3\gamma = a^{-2}\gamma a^2\gamma = \gamma^{\tau^{-2}+1}.$$

Since $\tau^4 \not\equiv 0 \pmod{p}$ we see that $\tau^2 + 1 \not\equiv \tau^{-2} + 1 \pmod{p}$. Therefore, the voltages of these two Hamiltonian cycles are different, so one of these Hamiltonian cycles has a nontrivial voltage. Thus, Factor Group Lemma 1.2.6 applies.

**Subcase 2.2.** Assume $|\overline{b}| = 3$. Since $|\overline{b}| = 3$, then $|b| \in \{3, 3p, 3q, 3pq\}$. Since $|\overline{a}| = 6$, then by 2.2.3 $|a| = 6$. Since $\gcd(|b|, 2) = 1$, then Lemma 2.3.4 applies.

**Subcase 2.3.** Assume $|\overline{b}| = 6$. Then we have $\overline{a} = \overline{b}$ or $\overline{a} = \overline{b}^{-1}$. Additionally, by Lemma 2.2.3 we have $|a| = |b| = 6$. We may assume $\overline{a} = \overline{b}$ by replacing $b$ with its inverse if necessary. Then $b = a\gamma$, where $G' = \langle\gamma\rangle$, because $G = \langle a, b\rangle$. We have $C = (\overline{a}^5, \overline{b})$ as a Hamiltonian cycle in $\mathrm{Cay}(\overline{G}, \overline{S})$. Now we calculate its voltage

$$\mathbb{V}(C) = a^5b = a^5a\gamma = a^6\gamma = \gamma$$

which generates $G'$. Therefore, Factor Group Lemma 1.2.6 applies. □

## 3.2 Assume $|S| = 2$ and $G' = \mathcal{C}_3 \times \mathcal{C}_p$

In this section we prove the part of Theorem 1.1.3 where, $|S| = 2$ and $G' = \mathcal{C}_3 \times \mathcal{C}_p$. Recall $\overline{G} = G/G'$ and $\widehat{G} = G/\mathcal{C}_p$.

**Proposition 3.2.** *Assume*

- $G = (\mathcal{C}_2 \times \mathcal{C}_q) \ltimes (\mathcal{C}_3 \times \mathcal{C}_p)$,

- $|S| = 2$.

*Then* $\mathrm{Cay}(G;S)$ *contains a Hamiltonian cycle.*

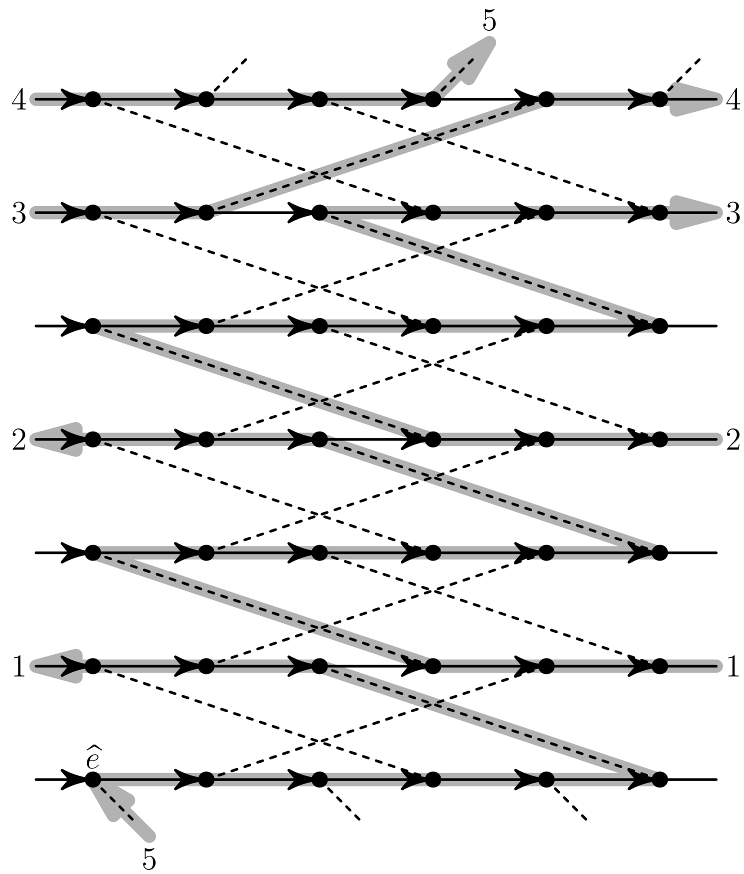


Figure 3.4: The Hamiltonian cycle $C_1$: $\widehat{a}$ edges are solid and $\widehat{b}$ edges are dashed.

*Proof.* Let $S = \{a, b\}$. Since the only non-trivial automorphism of $\mathcal{C}_3$ is inversion, $\mathcal{C}_q$ centralizes $\mathcal{C}_3$. Since $G' \cap Z(G) = \{e\}$ (see Proposition 1.3.12(4)), $\mathcal{C}_2$ does not centralize $\mathcal{C}_3$.

**Case 1.** Assume $|\overline{a}| = |\overline{b}| = 2q$. Then $\overline{b} = \overline{a}^m$, where $1 \leqslant m \leqslant q-1$ by replacing $b$ with its inverse if needed. Therefore, $b = a^m\gamma$, where $G' = \langle\gamma\rangle$. Also, $\gcd(m, 2q) = 1$. So, by Proposition 1.3.12(4) we have $a\gamma a^{-1} = \gamma^{\tau}$ where $\tau^{2q} \equiv 1 \pmod{3p}$ and $\gcd(\tau - 1, 3p) = 1$. Consider $\overline{G} = \mathcal{C}_{2q}$.

**Subcase 1.1.** Assume $m > 3$. Then we have

$$C = (\overline{b}^{-2}, \overline{a}^{-2}, \overline{b}, \overline{a}, \overline{b}, \overline{a}^{-(m-2)}, \overline{b}^{-1}, \overline{a}^{m-4}, \overline{b}^{-1}, \overline{a}^{-(2q-2m-3)})$$

as a Hamiltonian cycle in $\mathrm{Cay}(\overline{G}; \overline{S})$. Now we calculate its voltage.

$$\begin{aligned}
\mathbb{V}(C) &= b^{-2}a^{-2}baba^{-(m-2)}b^{-1}a^{m-4}b^{-1}a^{-(2q-2m-3)} \\
&= \gamma^{-1}a^{-m}\gamma^{-1}a^{-m}a^{-2}a^{m}\gamma a a^{m}\gamma a^{-m+2}\gamma^{-1}a^{-m}a^{m-4}\gamma^{-1}a^{-m}a^{-2q+2m+3} \\
&= \gamma^{-1}a^{-m}\gamma^{-1}a^{-2}\gamma a^{m+1}\gamma a^{-m+2}\gamma^{-1}a^{-4}\gamma^{-1}a^{m+3} \\
&= \gamma^{-1-\tau^{-m}+\tau^{-m-2}+\tau^{-1}-\tau^{-m+1}-\tau^{-m-3}} \\
&= \gamma^{-1+\tau^{-1}-\tau^{-m+1}-\tau^{-m}+\tau^{-m-2}-\tau^{-m-3}}.
\end{aligned}$$

We may assume $\mathbb{V}(C)$ does not generate $G' = \mathcal{C}_3 \times \mathcal{C}_p$. Therefore, the subgroup generated by $\mathbb{V}(C)$ either does not contain $\mathcal{C}_3$, or does not contain $\mathcal{C}_p$. We already know $\tau \equiv -1 \pmod 3$, then we have

$$\begin{aligned}
-1+\tau^{-1}-\tau^{-m+1}-\tau^{-m}+\tau^{-m-2}-\tau^{-m-3} &\equiv -1-1-1+1-1-1 \pmod 3 \\
&= -4 = -1.
\end{aligned}$$

This implies that the subgroup generated by $\mathbb{V}(C)$ contains $\mathcal{C}_3$. So we may assume the subgroup generated by $\mathbb{V}(C)$ does not contain $\mathcal{C}_p$, then

$$0 \equiv -1+\tau^{-1}-\tau^{-m+1}-\tau^{-m}+\tau^{-m-2}-\tau^{-m-3} \pmod p. \tag{1.1A}$$

Multiplying by $-\tau^{m+3}$ we have

$$0 \equiv \tau^{m+3}-\tau^{m+2}+\tau^{4}+\tau^{3}-\tau+1 \pmod p. \tag{1.1B}$$

Replacing $\{\overline{a}, \overline{b}\}$ with $\{\overline{a}^{-1}, \overline{b}^{-1}\}$ replaces $\tau$ with $\tau^{-1}$. Therefore, applying the above argument to $\{\overline{a}^{-1}, \overline{b}^{-1}\}$ establishes that 1.1A holds with $\tau^{-1}$ in the place of $\tau$, which means we have

$$0 \equiv -\tau^{m+3} + \tau^{m+2} - \tau^{m} - \tau^{m-1} + \tau - 1 \pmod p. \tag{1.1C}$$

By adding 1.1B and 1.1C we have

$$0 \equiv -\tau^{m} - \tau^{m-1} + \tau^4 + \tau^3 = \tau^3(\tau + 1)(1 - \tau^{m-4}) \pmod p.$$

If $\tau \equiv -1 \pmod p$, then $\mathcal{C}_{2q}$ inverts $\mathcal{C}_{3p}$, so $\mathcal{C}_q$ centralizes $\mathcal{C}_p$. This implies that $G \cong D_{6p} \times \mathcal{C}_q$, so Lemma 2.3.7 applies. The only other possibility is $\tau^{m-4} \equiv 1 \pmod p$. Multiplying by $\tau^4$, we have $\tau^m \equiv \tau^4 \pmod p$. We also know that $\tau^{2q} \equiv 1 \pmod p$. So $\tau^d \equiv 1 \pmod p$, where $d = \gcd(m-4, 2q)$. Since $m$ is odd and $m < q$, then $d = 1$. This contradicts the fact that $\gcd(\tau - 1, 3p) = 1$.

**Subcase 1.2.** Assume $m \leqslant 3$. Therefore, either $m = 1$ or $m = 3$. If $m = 1$, then $\overline{a} = \overline{b}$ and $b = a\gamma$. So we have $C_1 = (\overline{a}^{2q-1}, \overline{b})$ as a Hamiltonian cycle in $\mathrm{Cay}(\overline{G}; \overline{S})$. Now we calculate its voltage.

$$\mathbb{V}(C_1) = a^{2q-1}b = a^{2q-1}a\gamma = \gamma$$

which generates $G'$. Therefore, Factor Group Lemma 1.2.6 applies. Now if $m = 3$, then $b = a^3\gamma$ and we have

$$C_2 = (\overline{b}^2, \overline{a}^{-1}, \overline{b}^{-1}, \overline{a}^{-1}, \overline{b}^3, \overline{a}^{-2}, \overline{b}, \overline{a}^{2q-11})$$

as a Hamiltonian cycle in $\mathrm{Cay}(\overline{G}; \overline{S})$. We calculate its voltage.

$$\begin{aligned}
\mathbb{V}(C_2) &= b^2a^{-1}b^{-1}a^{-1}b^3a^{-2}ba^{2q-11} \\
&= a^3\gamma a^3\gamma a^{-1}\gamma^{-1}a^{-3}a^{-1}a^3\gamma a^3\gamma a^3\gamma a^{-2}a^3\gamma a^{-11} \\
&= a^3\gamma a^3\gamma a^{-1}\gamma^{-1}a^{-1}\gamma a^3\gamma a^3\gamma a\gamma a^{-11} \\
&= \gamma^{\tau^3+\tau^6-\tau^5+\tau^4+\tau^7+\tau^{10}+\tau^{11}} \\
&= \gamma^{\tau^{11}+\tau^{10}+\tau^7+\tau^6-\tau^5+\tau^4+\tau^3}
\end{aligned}$$

We may assume $\mathbb{V}(C_2)$ does not generate $G' = \mathcal{C}_3 \times \mathcal{C}_p$. Therefore, the subgroup generated by $\mathbb{V}(C)$ does not contain either $\mathcal{C}_3$, or $\mathcal{C}_p$. We already know $\tau \equiv -1 \pmod 3$, then

$$\tau^{11}+\tau^{10}+\tau^7+\tau^6-\tau^5+\tau^4+\tau^3 \equiv -1+1-1+1+1+1-1 = 1 \pmod 3.$$

This implies that the subgroup generated by $\mathbb{V}(C_2)$ contains $\mathcal{C}_3$. So we may assume the subgroup generated by $\mathbb{V}(C_2)$ does not contain $\mathcal{C}_p$, for otherwise Factor Group Lemma 1.2.6 applies. Then we have

$$\begin{aligned}
0 &\equiv \tau^{11}+\tau^{10}+\tau^7+\tau^6-\tau^5+\tau^4+\tau^3 \pmod p \\
&= \tau^3(\tau^8+\tau^7+\tau^4+\tau^3-\tau^2+\tau+1).
\end{aligned}$$

This implies that

$$0 \equiv \tau^8+\tau^7+\tau^4+\tau^3-\tau^2+\tau+1 \pmod p. \tag{1.2A}$$

We can replace $\tau$ with $\tau^{-1}$ in the above equation, by replacing $\{\overline{a}, \overline{b}\}$ with $\{\overline{a}^{-1}, \overline{b}^{-1}\}$

if necessary. Then we have

$$0 \equiv \tau^{-8} + \tau^{-7} + \tau^{-4} + \tau^{-3} - \tau^{-2} + \tau^{-1} + 1 \pmod{p}.$$

Multiplying $\tau^8$, then we have

$$\begin{aligned} 0 &\equiv 1 + \tau + \tau^4 + \tau^5 - \tau^6 + \tau^7 + \tau^8 \pmod{p} \\ &= \tau^8 + \tau^7 - \tau^6 + \tau^5 + \tau^4 + \tau + 1. \end{aligned}$$

Now by subtracting the above equation from 1.2A we have

$$\begin{aligned} 0 &\equiv \tau^6 - \tau^5 + \tau^3 - \tau^2 \pmod{p} \\ &= \tau^2(\tau - 1)(\tau^3 + 1). \end{aligned}$$

This implies that $\tau \equiv 1 \pmod{p}$ or $\tau^3 \equiv -1 \pmod{p}$. If $\tau \equiv 1 \pmod{p}$, then it contradicts the fact that $\gcd(\tau - 1, 3p) = 1$. Now if $\tau^3 \equiv -1 \pmod{p}$, then $\tau^6 \equiv 1 \pmod{p}$. We already know $\tau^{2q} \equiv 1 \pmod{p}$. Then $\tau^d \equiv 1 \pmod{p}$, where $d = \gcd(2q, 6)$. Since $\gcd(2, 6) = 2$ and $\gcd(q, 6) = 1$, then $d = 2$. This implies that $\tau^2 \equiv 1 \pmod{p}$, which means $\mathcal{C}_q$ centralizes $\mathcal{C}_p$. Then we have

$$G = \mathcal{C}_q \times (\mathcal{C}_2 \ltimes \mathcal{C}_{3p}) \cong \mathcal{C}_q \times D_{6p}.$$

So Lemma 2.3.7 applies.

**Case 2.** Assume $|\overline{a}| = q$. Then $|\overline{b}| \in \{2, 2q\}$. Thus $|b| \in \{2, 2q, 2p, 2pq\}$. If $|b| = 2pq$, then $\mathcal{C}_q$ centralizes $\mathcal{C}_p$. This implies that

$$G = \mathcal{C}_q \times (\mathcal{C}_2 \ltimes \mathcal{C}_{3p}) \cong \mathcal{C}_q \times D_{6p}$$

so, Lemma 2.3.7 applies. Therefore, we may assume $\mathcal{C}_q$ does not centralize $\mathcal{C}_p$, so $|a|$ is not divisible by $p$. If $|b| = 2p$, then Corollary 1.2.7 applies with $s = b$ and $t = b^{-1}$, because we have a Hamiltonian cycle in $\mathrm{Cay}(\widehat{G}; \widehat{S})$ by Theorem 1.1.2(3). (Since $b$ is the only generator whose order is even, then any Hamiltonian cycle in $\mathrm{Cay}(\widehat{G}; \widehat{S})$ must use some edge labeled $\widehat{b}$.)

We may now assume $|b| \in \{2, 2q\}$. We have $C = (\overline{a}^{q-1}, \overline{b}, \overline{a}^{-(q-1)}, \overline{b}^{-1})$ as a Hamiltonian cycle in $\mathrm{Cay}(\overline{G}; \overline{S})$. Now if $|a| = q$, then by Lemma 2.2.2 we have $G' = \langle [a^{q-1}, b] \rangle$. Therefore, Factor Group Lemma 1.2.6 applies. So, we may assume $|a| = 3q$. Since $\mathcal{C}_q$ does not centralize $\mathcal{C}_p$, then after conjugation we can assume $a = a_3 a_q$ and $b = a_2 a_q^j \gamma_p$, where $0 \leqslant j \leqslant q-1$. We already know that $C$ is a Hamiltonian cycle in $\mathrm{Cay}(\overline{G}; \overline{S})$. So we can assume $\gcd(3q, q-1) \neq 1$ (otherwise Lemma 2.2.2 applies, which implies that Factor Group Lemma 1.2.6 applies). This implies that $\gcd(3, q-1) \neq 1$ which means $q \equiv 1 \pmod 3$.

Consider $\widehat{G} = G/\mathcal{C}_p$. Then $\widehat{a} = a_3 a_q$ and $\widehat{b} = a_2 a_q^j$. Therefore, there exists $0 \leqslant k \leqslant 3q-1$ such that $\widehat{b}^{-1} \widehat{a} \widehat{b} = \widehat{a}^k$. Since $\widehat{b}$ inverts $a_3$ and centralizes $a_q$, then we must have $\widehat{a} = \widehat{b} \widehat{a}^k \widehat{b}^{-1} = a_3^{-k} a_q^k$, so $k \equiv -1 \pmod 3$ and $k \equiv 1 \pmod q$. Since $q \equiv 1 \pmod 3$, then $k = q+1$. Additionally, we have $a \gamma_p a^{-1} = \gamma_p^{\widehat{\tau}}$, where $\widehat{\tau}^q \equiv 1 \pmod p$. We also have $\widehat{\tau} \not\equiv 1 \pmod p$, because $\mathcal{C}_q$ does not centralize $\mathcal{C}_p$. Now we have

$$b^{-1} a b = \gamma_p^{-1} a_q^{-j} a_2 a a_2 a_q^j \gamma_p = \gamma_p^{-1} a^{q+1} \gamma_p.$$

This implies that

$$b^{-1} a^i b = (b^{-1} a b)^i = (\gamma_p^{-1} a^{q+1} \gamma_p)^i = \gamma_p^{-1} a^{i(q+1)} \gamma_p.$$

Therefore,

$$b^{-1} a^i b = \gamma_p^{-1} a^{i(q+1)} \gamma_p \equiv \gamma_p^{-1} a^i \gamma_p \pmod{\mathcal{C}_3}.$$

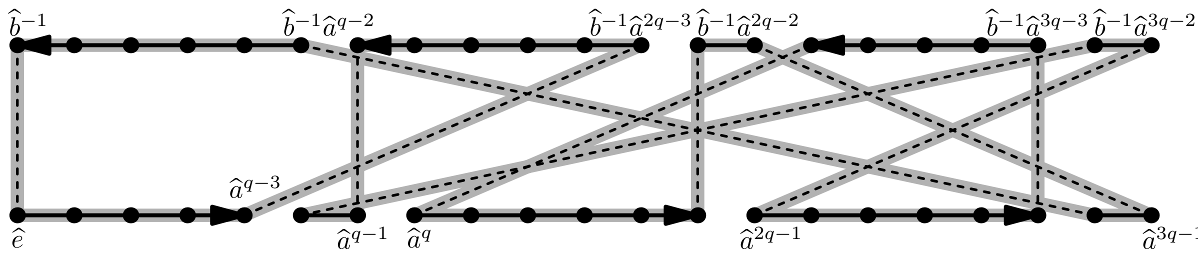


Figure 3.5: The Hamiltonian cycle $C_1$: $\widehat{a}$ edges are solid and $\widehat{b}$ edges are dashed.

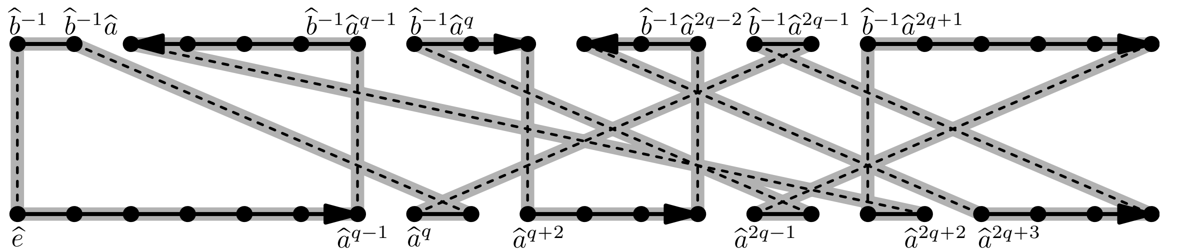


Figure 3.6: The Hamiltonian cycle $C_2$: $\widehat{a}$ edges are solid and $\widehat{b}$ edges are dashed.

We have

$$\begin{aligned} C_1 = (&\widehat{a}^{q-3}, \widehat{b}^{-1}, \widehat{a}^{-(q-2)}, \widehat{b}, \widehat{a}^{-1}, \widehat{b}^{-1}, \widehat{a}, \widehat{b}, \widehat{a}^{q-2}, \widehat{b}^{-1}, \\ &\widehat{a}^{-(q-3)}, \widehat{b}, \widehat{a}^{q-2}, \widehat{b}^{-1}, \widehat{a}, \widehat{b}, \widehat{a}^{-1}, \widehat{b}^{-1}, \widehat{a}^{-(q-2)}, \widehat{b}) \end{aligned}$$

as our first Hamiltonian cycle in $\mathrm{Cay}(\widehat{G}; \widehat{S})$. The picture in Figure 3.5 on page 61 shows the Hamiltonian cycle. In addition,

$$\begin{aligned} C_2 = (&\widehat{a}^{q-1}, \widehat{b}^{-1}, \widehat{a}^{-(q-3)}, \widehat{b}, \widehat{a}^{-1}, \widehat{b}^{-1}, \widehat{a}^{q-2}, \widehat{b}, \widehat{a}, \widehat{b}^{-1}, \widehat{a}^{2}, \widehat{b}, \\ &\widehat{a}^{q-4}, \widehat{b}^{-1}, \widehat{a}^{-(q-5)}, \widehat{b}, \widehat{a}^{q-4}, \widehat{b}^{-1}, \widehat{a}, \widehat{b}, \widehat{a}, \widehat{b}^{-1}, \widehat{a}^{-1}, \widehat{b}) \end{aligned}$$

is the second Hamiltonian cycle in $\mathrm{Cay}(\widehat{G}; \widehat{S})$. The picture in Figure 3.6 on page 61 shows the Hamiltonian cycle. We calculate the voltage of $C_1$ in $\widehat{G} = G/\mathcal{C}_3$. Since $a^q \equiv e \pmod{\mathcal{C}_3}$, we have

$$\mathbb{V}(C_1) \equiv a^{-3}(b^{-1}a^2b)a^{-1}(b^{-1}ab)a^{-2}(b^{-1}a^3b)a^{-2}(b^{-1}ab)a^{-1}(b^{-1}a^2b) \pmod{\mathcal{C}_3}$$

$$
\begin{aligned}
&= a^{-3}(\gamma_p^{-1}a^2\gamma_p)a^{-1}(\gamma_p^{-1}a\gamma_p)a^{-2}(\gamma_p^{-1}a^3\gamma_p)a^{-2}(\gamma_p^{-1}a\gamma_p)a^{-1}(\gamma_p^{-1}a^2\gamma_p)\\
&= a^{-3}(\gamma_p^{\widehat{\tau}^2-1}a^2)a^{-1}(\gamma_p^{\widehat{\tau}-1}a)a^{-2}(\gamma_p^{\widehat{\tau}^3-1}a^3)a^{-2}(\gamma_p^{\widehat{\tau}-1}a)a^{-1}(\gamma_p^{\widehat{\tau}^2-1}a^2)\\
&= a^{-3}\gamma_p^{\widehat{\tau}^2-1}a\gamma_p^{\widehat{\tau}-1}a^{-1}\gamma_p^{\widehat{\tau}^3-1}a\gamma_p^{\widehat{\tau}^2+\widehat{\tau}-2}a^2\\
&= \gamma_p^{\widehat{\tau}^{-3}(\widehat{\tau}^2-1)+\widehat{\tau}^{-2}(\widehat{\tau}-1)+\widehat{\tau}^{-3}(\widehat{\tau}^3-1)+\widehat{\tau}^{-2}(\widehat{\tau}^2+\widehat{\tau}-2)}\\
&= \gamma_p^{-2\widehat{\tau}^{-3}-3\widehat{\tau}^{-2}+3\widehat{\tau}^{-1}+2}.
\end{aligned}
$$

We may assume this does not generate $\mathcal{C}_p$, so

$$0 \equiv -2\widehat{\tau}^{-3} - 3\widehat{\tau}^{-2} + 3\widehat{\tau}^{-1} + 2 \pmod{p}.$$

Multiplying by $\widehat{\tau}^3$, we have

$$0 \equiv 2\widehat{\tau}^3 + 3\widehat{\tau}^2 - 3\widehat{\tau} - 2 = (\widehat{\tau} - 1)(\widehat{\tau} + 2)(2\widehat{\tau} + 1) \pmod{p}.$$

Since $\widehat{\tau} \not\equiv 1 \pmod{p}$, then we may assume $\widehat{\tau} \equiv -2 \pmod{p}$, by replacing $\widehat{a}$ with $\widehat{a}^{-1}$ if needed.

Now we calculate the voltage of $C_2$ in $\widehat{G} = G/\mathcal{C}_3$.

$$
\begin{aligned}
\mathbb{V}(C_2) &\equiv a^{-1}(b^{-1}a^3b)a^{-1}(b^{-1}a^{-2}b)a(b^{-1}a^2b)a^{-4}(b^{-1}a^5b)a^{-4}(b^{-1}ab)a(b^{-1}a^{-1}b) \pmod{\mathcal{C}_3}\\
&= a^{-1}(\gamma_p^{-1}a^3\gamma_p)a^{-1}(\gamma_p^{-1}a^{-2}\gamma_p)a(\gamma_p^{-1}a^2\gamma_p)\\
&\qquad \cdot a^{-4}(\gamma_p^{-1}a^5\gamma_p)a^{-4}(\gamma_p^{-1}a\gamma_p)a(\gamma_p^{-1}a^{-1}\gamma_p)\\
&= a^{-1}(\gamma_p^{\widehat{\tau}^3-1}a^3)a^{-1}(\gamma_p^{\widehat{\tau}^{-2}-1}a^{-2})a(\gamma_p^{\widehat{\tau}^2-1}a^2)\\
&\qquad \cdot a^{-4}(\gamma_p^{\widehat{\tau}^5-1}a^5)a^{-4}(\gamma_p^{\widehat{\tau}-1}a)a(\gamma_p^{\widehat{\tau}^{-1}-1}a^{-1})\\
&= a^{-1}\gamma_p^{\widehat{\tau}^3-1}a^2\gamma_p^{\widehat{\tau}^{-2}-1}a^{-1}\gamma_p^{\widehat{\tau}^2-1}a^{-2}\gamma_p^{\widehat{\tau}^5-1}a\gamma_p^{\widehat{\tau}-1}a^2\gamma_p^{\widehat{\tau}^{-1}-1}a^{-1}\\
&= \gamma_p^{\widehat{\tau}^{-1}(\widehat{\tau}^3-1)+\widehat{\tau}(\widehat{\tau}^{-2}-1)+\widehat{\tau}^2-1+\widehat{\tau}^{-2}(\widehat{\tau}^5-1)+\widehat{\tau}^{-1}(\widehat{\tau}-1)+\widehat{\tau}(\widehat{\tau}^{-1}-1)}\\
&= \gamma_p^{\widehat{\tau}^3+2\widehat{\tau}^2-2\widehat{\tau}+1-\widehat{\tau}^{-1}-\widehat{\tau}^{-2}}.
\end{aligned}
$$

We may assume this does not generate $\mathcal{C}_p$, so

$$0 \equiv \widehat{\tau}^3 + 2\widehat{\tau}^2 - 2\widehat{\tau} + 1 - \widehat{\tau}^{-1} - \widehat{\tau}^{-2} \pmod{p}.$$

Multiplying by $\widehat{\tau}^2$, we have

$$0 \equiv \widehat{\tau}^5 + 2\widehat{\tau}^4 - 2\widehat{\tau}^3 + \widehat{\tau}^2 - \widehat{\tau} - 1 \pmod{p}.$$

We already know $\widehat{\tau} \equiv -2 \pmod{p}$. By substituting this in the equation above, we have

$$0 \equiv (-2)^5 + 2(-2)^4 - 2(-2)^3 + (-2)^2 - (-2) - 1 = 21 = 3 \cdot 7 \pmod{p}.$$

Since $p > 7$, then $21 \not\equiv 0 \pmod{p}$. This is a contradiction.

**Case 3.** Assume $|\overline{a}| = 2q$ and $|\overline{b}| = 2$. Since $|\overline{a}| = 2q$, then by Lemma 2.2.3 $|a| = 2q$. We have $b = a^q\gamma$ where $G' = \langle\gamma\rangle$.

By Proposition 1.3.12(4) we have $a\gamma a^{-1} = \gamma^\tau$, where $\tau^{2q} \equiv 1 \pmod{3p}$ and $\gcd(\tau - 1, 3p) = 1$. This implies that $\tau \not\equiv 0, 1 \pmod{p}$ and $\tau \equiv -1 \pmod{3}$.

Suppose, for the moment, that $\tau \equiv -1 \pmod{p}$. Then $G \cong D_{6p} \times \mathcal{C}_q$, so $\mathrm{Cay}(G; S)$ has a Hamiltonian cycle by Lemma 2.3.7.

We may now assume that $\tau \not\equiv -1 \pmod{p}$. Recall that $\widehat{G} = G/\mathcal{C}_p = \mathcal{C}_{2q} \ltimes \mathcal{C}_3$. We may assume $\widehat{a} = a_2 a_q$ and $\widehat{b} = a_2 a_3$. We have

$$\begin{aligned} C_1 = ((&\widehat{a}, \widehat{b}, \widehat{a}, \widehat{b}, \widehat{a}^{-1}, \widehat{b}, \widehat{a}, \widehat{b}, \widehat{a}^{-1}, \widehat{b}, \widehat{a}, \widehat{b})^{(q-5)/2}, \widehat{a}, \widehat{b}, \widehat{a}^4, \\ &\widehat{b}, \widehat{a}^{-3}, \widehat{b}, \widehat{a}^{-1}, \widehat{b}, \widehat{a}^2, \widehat{b}, \widehat{a}^2, \widehat{b}, \widehat{a}^{-1}, \widehat{b}, \widehat{a}^{-3}, \widehat{b}, \widehat{a}^4, \widehat{b}) \end{aligned}$$

as the first Hamiltonian cycle in $\mathrm{Cay}(\widehat{G}; \widehat{S})$. The picture in Figure 3.7 on page 65 shows the Hamiltonian cycle. We also have

$$C_2 = ((\widehat{a}, \widehat{b}, \widehat{a}^{-1}, \widehat{b}, \widehat{a}, \widehat{b})^{q-5}, \widehat{a}^3, \widehat{b}, \widehat{a}^2, \widehat{b}, \widehat{a}^{-1}, \widehat{b}, \widehat{a}^{-3}, \widehat{b}, \widehat{a}^3, \widehat{b}, \widehat{a}^{-3}, \widehat{b}, \widehat{a}^{-1}, \widehat{b}, \widehat{a}^2, \widehat{b}, \widehat{a}^3, \widehat{b})$$

as the second Hamiltonian cycle in $\mathrm{Cay}(\widehat{G}; \widehat{S})$. The picture in Figure 3.8 on page 67 shows the Hamiltonian cycle. Now we calculate the voltage of $C_1$.

$$\begin{aligned}
\mathbb{V}(C_1) &= ((ababa^{-1}b)(aba^{-1}bab))^{(q-5)/2}(aba^4ba^{-3}ba^{-1}ba^2ba^2ba^{-1}ba^{-3}ba^4b) \\
&= ((aa^q\gamma aa^q\gamma a^{-1}a^q\gamma)(aa^q\gamma a^{-1}a^q\gamma aa^q\gamma))^{(q-5)/2} \\
&\qquad \cdot (aa^q\gamma a^4a^q\gamma a^{-3}a^q\gamma a^{-1}a^q\gamma a^2a^q\gamma a^2a^q\gamma a^{-1}a^q\gamma a^{-3}a^q\gamma a^4a^q\gamma) \\
&= ((a^{q+1}\gamma a^{q+1}\gamma a^{q-1}\gamma)(a^{q+1}\gamma a^{q-1}\gamma a^{q+1}\gamma))^{(q-5)/2} \\
&\qquad \cdot (a^{q+1}\gamma a^{q+4}\gamma a^{q-3}\gamma a^{q-1}\gamma a^{q+2}\gamma a^{q+2}\gamma a^{q-1}\gamma a^{q-3}\gamma a^{q+4}\gamma) \\
&= ((\gamma^{\tau^{q+1}+\tau^2+\tau^{q+1}}a^{q+1})(\gamma^{\tau^{q+1}+1+\tau^{q+1}}a^{q+1}))^{(q-5)/2} \\
&\qquad \cdot (\gamma^{\tau^{q+1}+\tau^5+\tau^{q+2}+\tau+\tau^{q+3}+\tau^5+\tau^{q+4}+\tau+\tau^{q+5}}a^{q+5}) \\
&= ((\gamma^{2\tau^{q+1}+\tau^2}a^{q+1})(\gamma^{2\tau^{q+1}+1}a^{q+1}))^{(q-5)/2} \\
&\qquad \cdot (\gamma^{\tau^{q+5}+\tau^{q+4}+\tau^{q+3}+\tau^{q+2}+\tau^{q+1}+2\tau^5+2\tau}a^{q+5}) \\
&= ((\gamma^{2\tau^{q+1}+\tau^2+\tau^{q+1}(2\tau^{q+1}+1)}a^2))^{(q-5)/2} \\
&\qquad \cdot (\gamma^{\tau^{q+5}+\tau^{q+4}+\tau^{q+3}+\tau^{q+2}+\tau^{q+1}+2\tau^5+2\tau}a^{q+5}) \\
&= (\gamma^{3\tau^{q+1}+3\tau^2}a^2)^{(q-5)/2}(\gamma^{\tau^{q+5}+\tau^{q+4}+\tau^{q+3}+\tau^{q+2}+\tau^{q+1}+2\tau^5+2\tau}a^{q+5}) \\
&= (\gamma^{(3\tau^{q+1}+3\tau^2)(\tau^{q-5}-1)/(\tau^2-1)}a^{q-5})(\gamma^{\tau^{q+5}+\tau^{q+4}+\tau^{q+3}+\tau^{q+2}+\tau^{q+1}+2\tau^5+2\tau}a^{q+5}) \\
&= \gamma^{(3\tau^{q+1}+3\tau^2)(\tau^{q-5}-1)/(\tau^2-1)+\tau^{q-5}(\tau^{q+5}+\tau^{q+4}+\tau^{q+3}+\tau^{q+2}+\tau^{q+1}+2\tau^5+2\tau)}.
\end{aligned}$$

Since $\tau^{2q} \equiv 1 \pmod p$, we have $\tau^q \equiv \pm 1 \pmod p$.

Let us now consider the case where $\tau^q \equiv 1 \pmod p$, then by substituting this in

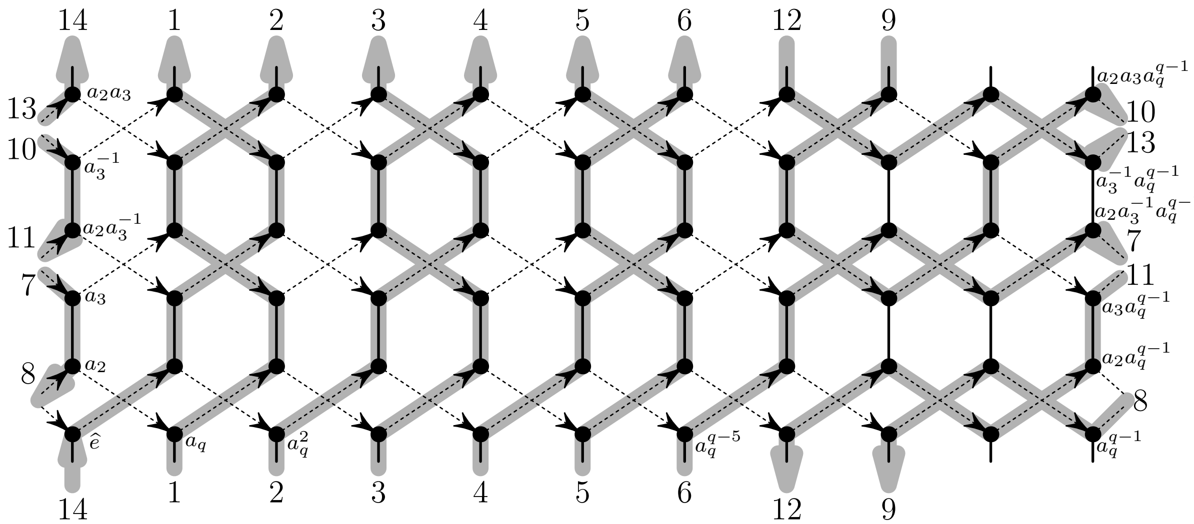


Figure 3.7: The Hamiltonian cycle $C_1$: $\widehat{b}$ edges are solid and $\widehat{a}$ edges are dashed.

the formula for the voltage of $C_1$ we have

$$\begin{aligned}
\mathbb{V}(C_1) &= \gamma^{(3\tau+3\tau^2)(\tau^{-5}-1)/(\tau^2-1)+\tau^{-5}(\tau^5+\tau^4+\tau^3+\tau^2+\tau+2\tau^5+2\tau)} \\
&= \gamma^{3\tau(1+\tau)(\tau^{-5}-1)/(\tau+1)(\tau-1)+(1+\tau^{-1}+\tau^{-2}+\tau^{-3}+\tau^{-4}+2+2\tau^{-4})} \\
&= \gamma^{3\tau(\tau^{-5}-1)/(\tau-1)+(3+\tau^{-1}+\tau^{-2}+\tau^{-3}+3\tau^{-4})} \\
&= \gamma^{(-2+2\tau^{-3})/(\tau-1)}.
\end{aligned}$$

We may assume this does not generate $\mathcal{C}_p$, then

$$0 \equiv -2 + 2\tau^{-3} \pmod{p}.$$

Multiplying by $\tau^3$, we have

$$0 \equiv -2\tau^3 + 2 \pmod{p}.$$

This implies that $\tau^3 \equiv 1 \pmod{p}$, which contradicts the fact that $\tau^q \equiv 1 \pmod{p}$ but $\tau \not\equiv 1 \pmod{p}$.

Now we may assume $\tau^q \equiv -1 \pmod{p}$, then substituting this in the formula for the voltage of $C_1$ we have

$$\begin{aligned}
\mathbb{V}(C_1) &= \gamma^{(-3\tau+3\tau^2)(-\tau^{-5}-1)/(\tau^2-1)-\tau^{-5}(-\tau^5-\tau^4-\tau^3-\tau^2-\tau+2\tau^5+2\tau)} \\
&= \gamma^{3\tau(\tau-1)(-\tau^{-5}-1)/(\tau+1)(\tau-1)+(1+\tau^{-1}+\tau^{-2}+\tau^{-3}+\tau^{-4}-2-2\tau^{-4})} \\
&= \gamma^{3\tau(-\tau^{-5}-1)/(\tau+1)+(-1+\tau^{-1}+\tau^{-2}+\tau^{-3}-\tau^{-4})} \\
&= \gamma^{(-4\tau+2\tau^{-1}+2\tau^{-2}-4\tau^{-4})/(\tau+1)}.
\end{aligned}$$

We may assume this does not generate $\mathcal{C}_p$, then

$$0 \equiv -4\tau + 2\tau^{-1} + 2\tau^{-2} - 4\tau^{-4} \pmod{p}.$$

Multiplying by $(-\tau^4)/2$, we have

$$\begin{aligned}
0 &\equiv 2\tau^5 - \tau^3 - \tau^2 + 2 \\
&= (\tau+1)(2\tau^4 - 2\tau^3 + \tau^2 - 2\tau + 2) \pmod{p}.
\end{aligned}$$

Since we assumed $\tau \not\equiv -1 \pmod{p}$, then the above equation implies that

$$0 \equiv 2\tau^4 - 2\tau^3 + \tau^2 - 2\tau + 2 \pmod{p}. \tag{3A}$$

Now we calculate the voltage of $C_2$.

$$\begin{aligned}
\mathbb{V}(C_2) &= (aba^{-1}bab)^{(q-5)}(a^3ba^2ba^{-1}ba^{-3}ba^3ba^{-3}ba^{-1}ba^2ba^3b) \\
&= (aa^q\gamma a^{-1}a^q\gamma aa^q\gamma)^{(q-5)}(a^3a^q\gamma a^2a^q\gamma a^{-1}a^q\gamma a^{-3}a^q\gamma a^3a^q\gamma a^{-3}a^q\gamma a^{-1}a^q\gamma a^2a^q\gamma a^3a^q\gamma) \\
&= (a^{q+1}\gamma a^{q-1}\gamma a^{q+1}\gamma)^{(q-5)}(a^{q+3}\gamma a^{q+2}\gamma a^{q-1}\gamma a^{q-3}\gamma a^{q+3}\gamma a^{q-3}\gamma a^{q-1}\gamma a^{q+2}\gamma a^{q+3}\gamma) \\
&= (\gamma^{\tau^{q+1}+1+\tau^{q+1}}a^{q+1})^{(q-5)}(\gamma^{\tau^{q+3}+\tau^5+\tau^{q+4}+\tau+\tau^{q+4}+\tau+\tau^q+\tau^2+\tau^{q+5}}a^{q+5}) \\
&= (\gamma^{2\tau^{q+1}+1}a^{q+1})^{(q-5)}(\gamma^{\tau^{q+5}+2\tau^{q+4}+\tau^{q+3}+\tau^q+\tau^5+\tau^2+2\tau}a^{q+5}) \\
&= (\gamma^{(2\tau^{q+1}+1)((\tau^{q+1})^{(q-5)}-1)/(\tau^{q+1}-1)}a^{(q+1)(q-5)})(\gamma^{\tau^{q+5}+2\tau^{q+4}+\tau^{q+3}+\tau^q+\tau^5+\tau^2+2\tau}a^{q+5})
\end{aligned}$$

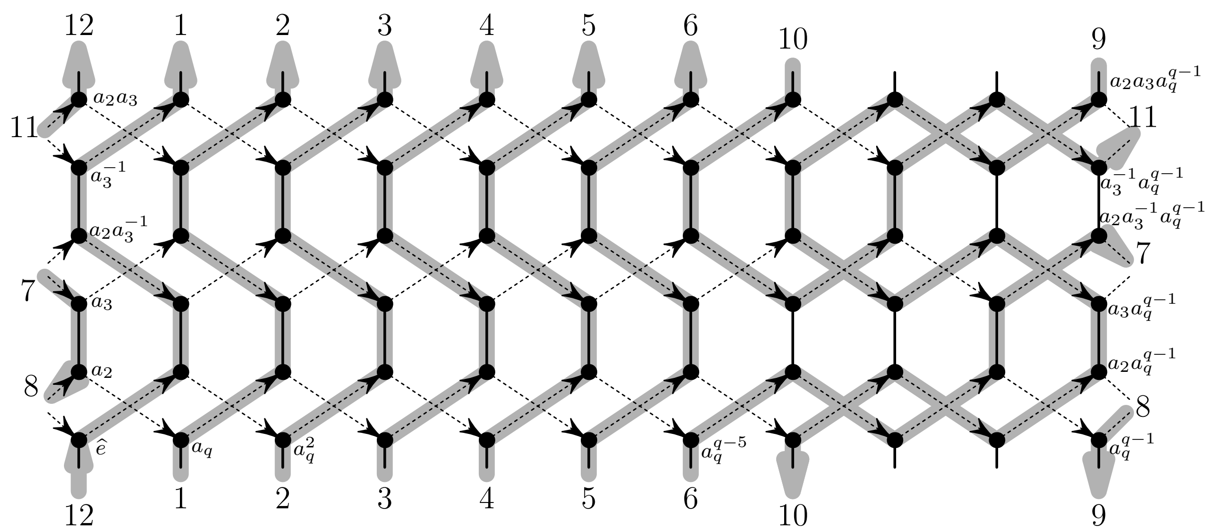


Figure 3.8: The Hamiltonian cycle $C_2$: $\widehat{b}$ edges are solid and $\widehat{a}$ edges are dashed.

$$= \gamma^{(2\tau^{q+1}+1)((\tau^{q+1})^{(q-5)}-1)/(\tau^{q+1}-1)+\tau^{(q+1)(q-5)}(\tau^{q+5}+2\tau^{q+4}+\tau^{q+3}+\tau^{q}+\tau^{5}+\tau^{2}+2\tau)}.$$

Since we are assuming $\tau^q \equiv -1 \pmod{p}$, then by substituting this in the above formula we have

$$\begin{aligned}
\mathbb{V}(C_2) &= \gamma^{(-2\tau+1)((-\tau)^{-5}-1)/(-\tau-1)-\tau^{-5}(-\tau^5-2\tau^4-\tau^3-1+\tau^5+\tau^2+2\tau)} \\
&= \gamma^{(2\tau^{-4}+2\tau-\tau^{-5}-1)/(-\tau-1)+1+2\tau^{-1}+\tau^{-2}+\tau^{-5}-1-\tau^{-3}-2\tau^{-4}} \\
&= \gamma^{(2\tau-3-3\tau^{-1}+3\tau^{-3}+3\tau^{-4}-2\tau^{-5})/(-\tau-1)}.
\end{aligned}$$

We may assume this does not generate $\mathcal{C}_p$, then

$$2\tau - 3 - 3\tau^{-1} + 3\tau^{-3} + 3\tau^{-4} - 2\tau^{-5} \equiv 0 \pmod{p}.$$

Multiplying by $\tau^5$, we have

$$0 \equiv 2\tau^6 - 3\tau^5 - 3\tau^4 + 3\tau^2 + 3\tau - 2 = (\tau^2-1)(2\tau^4 - 3\tau^3 - \tau^2 - 3\tau + 2) \pmod{p}.$$

Since $\tau^2 \not\equiv 1 \pmod{p}$, then the above equation implies that

$$0 \equiv 2\tau^4 - 3\tau^3 - \tau^2 - 3\tau + 2 \pmod{p}.$$

Therefore, by subtracting the above equation from 3A, we have

$$0 \equiv (\tau^3 + 2\tau^2 + \tau) = \tau(\tau + 1)^2 \pmod{p}.$$

This is a contradiction.

**Case 4.** Assume none of the previous cases apply. Since $\langle \overline{a}, \overline{b} \rangle = \overline{G}$, we may assume $|\overline{a}|$ is divisible by $q$, which means $|\overline{a}|$ is either $q$ or $2q$. Since Case 2 applies when $|\overline{a}| = q$, we must have $|\overline{a}| = 2q$. Then $|\overline{b}| = q$, since Cases 1 and 3 do not apply. So Case 2 applies after interchanging $a$ and $b$. □

## 3.3 Assume $|S| = 3$, $G' = \mathcal{C}_p \times \mathcal{C}_q$ and $C_{G'}(\mathcal{C}_3) \neq \{e\}$

In this section we prove the part of Theorem 1.1.3 where, $|S| = 3$, $G' = \mathcal{C}_p \times \mathcal{C}_q$ and $C_{G'}(\mathcal{C}_3) \neq \{e\}$. Recall $\overline{G} = G/G'$, $\check{G} = G/\mathcal{C}_q$ and $\widehat{G} = G/\mathcal{C}_p$.

**Proposition 3.3.** *Assume*

- $G = (\mathcal{C}_2 \times \mathcal{C}_3) \ltimes (\mathcal{C}_p \times \mathcal{C}_q)$,
- $|S| = 3$,
- $C_{G'}(\mathcal{C}_3) \neq \{e\}$.

*Then* $\mathrm{Cay}(G; S)$ *contains a Hamiltonian cycle.*

*Proof.* Let $S = \{a, b, c\}$. If $C_{G'}(\mathcal{C}_3) = \mathcal{C}_p \times \mathcal{C}_q$, then since $G' \cap Z(G) = \{e\}$ (see Proposition 1.3.12(2)), we conclude that $C_{G'}(\mathcal{C}_2) = \{e\}$. So we have

$$G = \mathcal{C}_3 \times (\mathcal{C}_2 \ltimes \mathcal{C}_{pq}) \cong \mathcal{C}_3 \times D_{2pq}.$$

Therefore, Lemma 2.3.7 applies.

Since $C_{G'}(\mathcal{C}_3) \neq \{e\}$, then we may assume $C_{G'}(\mathcal{C}_3) = \mathcal{C}_q$ by interchanging $q$ and $p$ if necessary. Since $G' \cap Z(G) = \{e\}$, then $\mathcal{C}_2$ inverts $\mathcal{C}_q$. Since $\mathcal{C}_3$ centralizes $\mathcal{C}_q$ and $Z(G) \cap G' = \{e\}$ (by Proposition 1.3.12(2)), then $\mathcal{C}_2$ inverts $\mathcal{C}_q$. Thus,

$$\widehat{G} = (\mathcal{C}_2 \times \mathcal{C}_3) \ltimes \mathcal{C}_q \cong (\mathcal{C}_2 \ltimes \mathcal{C}_q) \times \mathcal{C}_3 = D_{2q} \times \mathcal{C}_3.$$

Now if $\widehat{S}$ is minimal, then Lemma 2.3.5 applies. Therefore, we may assume $\widehat{S}$ is not minimal. Choose a 2-element subset $\{a, b\}$ of $S$ that generates $\widehat{G}$. From the minimality of $S$, we see that $\langle a, b\rangle = D_{2q} \times \mathcal{C}_3$ after replacing $a$ and $b$ by conjugates. The projection of $(a, b)$ to $D_{2q}$ must be of the form $(a_2, a_q)$ or $(a_2, a_2a_q)$, where $a_2$ is reflection and $a_q$ is a rotation. (Also note that $\widehat{b} \neq a_q$ because $S \cap G' = \varnothing$ by Assumption 3.0.1(6).) Therefore, $(a, b)$ must have one of the following forms:

1. $(a_2, a_3a_q)$,
2. $(a_2, a_2a_3a_q)$,
3. $(a_2a_3, a_2a_q)$,
4. $(a_2a_3, a_3a_q)$,
5. $(a_2a_3, a_2a_3a_q)$.

Let $c$ be the third element of $S$. We may write $c = a_2^i a_3^j a_q^k \gamma_p$ with $0 \leqslant i \leqslant 1$, $0 \leqslant j \leqslant 2$ and $0 \leqslant k \leqslant q-1$. Note since $S \cap G' = \varnothing$, we know that $i$ and $j$ cannot both be equal to 0. Additionally, we have $a_3\gamma_p a_3^{-1} = \gamma_p^{\widehat{\tau}}$ where $\widehat{\tau}^3 \equiv 1 \pmod{\mathcal{C}_p}$. Also, $\widehat{\tau} \not\equiv 1 \pmod{p}$ since $C_{G'}(\mathcal{C}_3) = \mathcal{C}_q$. Therefore, we conclude that $\widehat{\tau}^2 + \widehat{\tau} + 1 \equiv 0 \pmod{p}$. Note that this implies $\widehat{\tau} \not\equiv -1 \pmod{p}$.

**Case 1.** Assume $a = a_2$ and $b = a_3a_q$.

**Subcase 1.1.** Assume $i \neq 0$. Then, $c = a_2a_3^j a_q^k \gamma_p$. Thus, by Lemma 2.4.1(1) $\langle b, c\rangle = G$ which contradicts the minimality of $S$.

**Subcase 1.2.** Assume $i = 0$. Then $j \neq 0$. We may assume $j = 1$, by replacing $c$ with $c^{-1}$ if necessary. Thus $c = a_3 a_q^k \gamma_p$. Consider $\overline{G} = \mathcal{C}_2 \times \mathcal{C}_3$. We have $\overline{a} = a_2$, $\overline{b} = a_3$ and $\overline{c} = a_3$. Therefore, $\overline{b} = \overline{c} = a_3$. We have $(\overline{a}, \overline{b}^2, \overline{a}, \overline{b}^{-2})$ as a Hamiltonian cycle in $\mathrm{Cay}(\overline{G}; \overline{S})$. Since we can replace each $\overline{b}$ by $\overline{c}$, then we consider $C_1 = (\overline{a}, \overline{b}^2, \overline{a}, \overline{b}^{-1}, \overline{c}^{-1})$ and $C_2 = (\overline{a}, \overline{b}^2, \overline{a}, \overline{c}^{-2})$ as Hamiltonian cycles in $\mathrm{Cay}(\overline{G}; \overline{S})$. Now since there is one occurrence of $c$ in $C_1$, then by Lemma 2.5.2 the subgroup generated by $\mathbb{V}(C_1)$ contains $\mathcal{C}_p$. Also,

$$\begin{aligned}
\mathbb{V}(C_1) &= ab^2ab^{-1}c^{-1} \\
&\equiv a_2 \cdot a_3^2 a_q^2 \cdot a_2 \cdot a_q^{-1} a_3^{-1} \cdot a_q^{-k} a_3^{-1} \pmod{\mathcal{C}_p} \\
&= a_q^{-2} a_3 a_q^{-1-k} a_3^{-1} \\
&= a_q^{-3-k}.
\end{aligned}$$

We can assume this does not generate $\mathcal{C}_q$, for otherwise Factor Group Lemma 1.2.6 applies. Therefore,

$$-3 - k \equiv 0 \pmod{q}.$$

Thus, $k \equiv -3 \pmod{q}$.

Now we calculate the voltage of $C_2$.

$$\begin{aligned}
\mathbb{V}(C_2) &= ab^2ac^{-2} \\
&\equiv a_2 \cdot a_3^2 \cdot a_2 \cdot \gamma_p^{-1} a_3^{-1} \gamma_p^{-1} a_3^{-1} \pmod{\mathcal{C}_q} \\
&= a_3^2 \gamma_p^{-1} a_3^{-1} \gamma_p^{-1} a_3^{-1} \\
&= \gamma_p^{-\widehat{\tau}^2 - \widehat{\tau}}.
\end{aligned}$$

Since $\widehat{\tau}^2 + \widehat{\tau} + 1 \equiv 0 \pmod{p}$, then $-\widehat{\tau}^2 - \widehat{\tau} \equiv 1 \pmod{p}$. Thus, $\gamma_p^{-\widehat{\tau}^2 - \widehat{\tau}} = \gamma_p$

generates $\mathcal{C}_p$.

$$\begin{aligned}
\mathbb{V}(C_2) &= ab^2ac^{-2} \\
&\equiv a_2 \cdot a_3^2 a_q^2 \cdot a_2 \cdot a_q^{-k} a_3^{-1} a_q^{-k} a_3^{-1} \pmod{\mathcal{C}_p} \\
&= a_q^{-2} a_3^2 a_q^{-k} a_3^{-1} a_q^{-k} a_3^{-1} \\
&= a_q^{-2(k+1)}.
\end{aligned}$$

We know $k \equiv -3 \pmod{q}$, therefore, $-2(k+1) \equiv 4 \pmod{q}$, so Factor Group Lemma 1.2.6 applies.

**Case 2.** Assume $a = a_2$ and $b = a_2a_3a_q$.

**Subcase 2.1.** Assume $i = 0$, then $j \neq 0$. If $k \neq 0$, then $c = a_3^j a_q^k \gamma_p$. Thus, by Lemma 2.4.1(3) $\langle b, c \rangle = G$ which contradicts the minimality of $S$. Therefore, we may assume $k = 0$. We may also assume $j = 1$, by replacing $c$ with $c^{-1}$ if necessary. Then $c = a_3\gamma_p$.

Consider $\overline{G} = \mathcal{C}_2 \times \mathcal{C}_3$, thus $\overline{a} = a_2$, $\overline{b} = a_2a_3$ and $\overline{c} = a_3$. Therefore, $|\overline{a}| = 2$, $|\overline{b}| = 6$ and $|\overline{c}| = 3$. Consider $C = (\overline{b}^2, \overline{c}, \overline{b}, \overline{c}^{-1}, \overline{a})$ as a Hamiltonian cycle in $\mathrm{Cay}(\overline{G}; \overline{S})$. Now we calculate its voltage.

$$\begin{aligned}
\mathbb{V}(C) &= b^2cbc^{-1}a \\
&\equiv a_2a_3a_qa_2a_3a_q \cdot a_3 \cdot a_2a_3a_q \cdot a_3^{-1} \cdot a_2 \pmod{\mathcal{C}_p} \\
&= a_q^{-1}
\end{aligned}$$

which generates $\mathcal{C}_q$. By considering the fact that $\mathcal{C}_2$ might centralize $\mathcal{C}_p$ or not, we have

$$\begin{aligned}
\mathbb{V}(C) &= b^2cbc^{-1}a \\
&\equiv a_2a_3a_2a_3 \cdot a_3\gamma_p \cdot a_2a_3 \cdot \gamma_p^{-1} a_3^{-1} \cdot a_2 \pmod{\mathcal{C}_q}
\end{aligned}$$

$$= \gamma_p a_3 \gamma_p^{\mp 1} a_3^{-1}$$
$$= \gamma_p^{1 \mp \hat{\tau}}.$$

which generates $\mathcal{C}_p$. Therefore, the subgroup generated by $\mathbb{V}(C)$ is $G'$. So, Factor Group Lemma 1.2.6 applies.

**Subcase 2.2.** Assume $j = 0$. Then $i \neq 0$. If $k \neq 1$, then $c = a_2 a_q^k \gamma_p$. Thus, by Lemma 2.4.1(4) $\langle b, c \rangle = G$ which contradicts the minimality of $S$. We may therefore assume $k = 1$. Then $c = a_2 a_q \gamma_p$.

Consider $\overline{G} = \mathcal{C}_2 \times \mathcal{C}_3$, then $\overline{a} = \overline{c} = a_2$ and $\overline{b} = a_2 a_3$. Thus, $|\overline{a}| = |\overline{c}| = 2$ and $|\overline{b}| = 6$. We have $C = (\overline{b}^2, \overline{c}, \overline{b}^{-2}, \overline{a})$ as a Hamiltonian cycle in $\mathrm{Cay}(\overline{G}; \overline{S})$. Since there is one occurrence of $c$ in $C$, and it is the only generator of $G$ that contains $\gamma_p$, then by Lemma 2.5.2 we conclude that the subgroup generated by $\mathbb{V}(C)$ contains $\mathcal{C}_p$. Also,

$$\begin{aligned}
\mathbb{V}(C) &= b^2 c b^{-2} a \\
&\equiv a_2 a_3 a_q a_2 a_3 a_q \cdot a_2 a_q \cdot a_q^{-1} a_3^{-1} a_2 a_q^{-1} a_3^{-1} a_2 \cdot a_2 \pmod{\mathcal{C}_p} \\
&= a_q^{-1} a_3 a_q a_3 a_q^{-1} a_3^{-1} a_q a_3^{-1} a_q^{-1} \\
&= a_q^{-1}.
\end{aligned}$$

which generates $\mathcal{C}_q$. Therefore, the subgroup generated by $\mathbb{V}(C)$ is $G'$. So, Factor Group Lemma 1.2.6 applies.

**Subcase 2.3.** Assume $i \neq 0$ and $j \neq 0$. We may assume $j = 1$, by replacing $c$ with $c^{-1}$ if necessary. So $c = a_2 a_3 a_q^k \gamma_p$. If $k \neq 1$, then by Lemma 2.4.1(4) $\langle b, c \rangle = G$ which contradicts the minimality of $S$. We may now assume $k = 1$. Then $c = a_2 a_3 a_q \gamma_p$.

Consider $\overline{G} = \mathcal{C}_2 \times \mathcal{C}_3$. Then $\overline{a} = a_2$ and $\overline{b} = \overline{c} = a_2 a_3$. Therefore, $|\overline{b}| = |\overline{c}| = 6$ and $|\overline{a}| = 2$. We have $C = (\overline{c}, \overline{a}, (\overline{b}, \overline{a})^2)$ as a Hamiltonian cycle in $\mathrm{Cay}(\overline{G}; \overline{S})$. Since there is one occurrence of $c$ in $C$, and it is the only generator of $G$ that contains $\gamma_p$, then by Lemma 2.5.2 we conclude that the subgroup generated by $\mathbb{V}(C)$ is $\mathcal{C}_p$. Also,

$$\begin{aligned}\mathbb{V}(C) &= ca(ba)^2 \\ &\equiv a_2a_3a_q \cdot a_2 \cdot a_2a_3a_q \cdot a_2 \cdot a_2a_3a_q \cdot a_2 \pmod{\mathcal{C}_p} \\ &= a_3a_q^{-2}a_3a_q^{-1}a_3 \\ &= a_q^{-3}\end{aligned}$$

which generates $\mathcal{C}_q$. Therefore, the subgroup generated by $\mathbb{V}(C)$ is $G'$. So, Factor Group Lemma 1.2.6 applies.

**Case 3.** Assume $a = a_2a_3$ and $b = a_2a_q$. Since $b = a_2a_q$ is conjugate to $a_2$ via an element of $\mathcal{C}_q$ (which centralizes $\mathcal{C}_3$), then $\{a, b\}$ is conjugate to $\{a_2a_3a_q^m, a_2\}$ for some nonzero $m$. So Case 2 applies (after replacing $a_q$ with $a_q^m$).

**Case 4.** Assume $a = a_2a_3$ and $b = a_3a_q$.

**Subcase 4.1.** Assume $i \neq 0$. Then $c = a_2a_3^ja_q^k\gamma_p$. Thus, by Lemma 2.4.1(1) $\langle b, c\rangle = G$ which contradicts the minimality of $S$.

**Subcase 4.2.** Assume $i = 0$. Then $j \neq 0$ and $c = a_3^ja_q^k\gamma_p$. If $k \neq 0$, then by Lemma 2.4.1(2) $\langle a, c\rangle = G$ which contradicts the minimality of $S$. So we may assume $k = 0$. We may also assume $j = 1$, by replacing $c$ with $c^{-1}$ if necessary. Then $c = a_3\gamma_p$.

Consider $\overline{G} = \mathcal{C}_2 \times \mathcal{C}_3$. Therefore, $\overline{a} = a_2a_3$ and $\overline{b} = \overline{c} = a_3$. In addition, $|\overline{a}| = 6$ and $|\overline{b}| = |\overline{c}| = 3$. We have $C = (\overline{c}, \overline{b}, \overline{a}, \overline{b}^{-2}, \overline{a}^{-1})$ as a Hamiltonian cycle in $\mathrm{Cay}(\overline{G}; \overline{S})$. Since there is one occurrence of $c$ in $C$, and it is the only generator of $G$ that contains $\gamma_p$, then by Lemma 2.5.2 we conclude that the subgroup generated by $\mathbb{V}(C)$ contains $\mathcal{C}_p$. Also,

$$\begin{aligned}\mathbb{V}(C) &= cbab^{-2}a^{-1} \\ &\equiv a_3 \cdot a_3a_q \cdot a_2a_3 \cdot a_q^{-2}a_3^{-2} \cdot a_3^{-1}a_2 \pmod{\mathcal{C}_p}\end{aligned}$$

$$= a_3 a_q a_3^2 a_q^2$$
$$= a_q^3$$

which generates $\mathcal{C}_q$. Therefore, the subgroup generated by $\mathbb{V}(C)$ is $G'$. Thus, Factor Group Lemma 1.2.6 applies.

**Case 5.** Assume $a = a_2 a_3$, $b = a_2 a_3 a_q$.

**Subcase 5.1.** Assume $i = 0$. Then $j \neq 0$ and $c = a_3^j a_q^k \gamma_p$. If $k \neq 0$, then by Lemma 2.4.1(3) $\langle b, c \rangle = G$ which contradicts the minimality of $S$. So we may assume $k = 0$. We may also assume $j = 1$, by replacing $c$ with $c^{-1}$ if necessary. Then $c = a_3 \gamma_p$.

Consider $\overline{G} = \mathcal{C}_2 \times \mathcal{C}_3$. Therefore, $\overline{a} = \overline{b} = a_2 a_3$ and $\overline{c} = a_3$. Thus, $|\overline{a}| = |\overline{b}| = 6$ and $|\overline{c}| = 3$. We have $C = (\overline{a}, \overline{c}^2, \overline{b}^{-1}, \overline{c}^{-2})$ as a Hamiltonian cycle in $\mathrm{Cay}(\overline{G}; \overline{S})$. Now we calculate its voltage.

$$\begin{aligned}
\mathbb{V}(C) &= ac^2b^{-1}c^{-2} \\
&\equiv a_2 a_3 \cdot a_3^2 \cdot a_q^{-1} a_3^{-1} a_2 \cdot a_3^{-2} \pmod{\mathcal{C}_p} \\
&= a_3^{-1} a_q a_3^{-2} \\
&= a_q
\end{aligned}$$

which generates $\mathcal{C}_q$. Also

$$\begin{aligned}
\mathbb{V}(C) &= ac^2b^{-1}c^{-2} \\
&\equiv ac^2a^{-1}c^{-2} \pmod{\mathcal{C}_q} \text{ (because } a \equiv b \pmod{\mathcal{C}_q}) \\
&= ac^{-1}a^{-1}c \text{ (because } |c| = 3) \\
&= [a, c^{-1}].
\end{aligned}$$

This generates $\mathcal{C}_p$, because $\{a, c\}$ generates $G/\mathcal{C}_q$. Therefore, the subgroup generated by $\mathbb{V}(C)$ is $G'$. So, Factor Group Lemma 1.2.6 applies.

**Subcase 5.2.** Assume $i \neq 0$. Then $c = a_2 a_3^j a_q^k \gamma_p$. If $k \neq 1$, then by Lemma 2.4.1(4) $\langle b, c \rangle = G$ which contradicts the minimality of $S$. So we may assume $k = 1$. Then $c = a_2 a_3^j a_q \gamma_p$. We show that $\langle a, c \rangle = G$. Now, we have

$$\begin{aligned}
\langle a, c \rangle &= \langle a_2, a_3, c \rangle \text{ (because } \langle a \rangle = \langle a_2 a_3 \rangle = \langle a_2, a_3 \rangle) \\
&= \langle a_2, a_3, a_2 a_3^j a_q \gamma_p \rangle \\
&= \langle a_2, a_3, a_q \gamma_p \rangle \\
&= \langle a_2, a_3, a_q, \gamma_p \rangle \\
&= G,
\end{aligned}$$

which contradicts the minimality of $S$. $\square$

## 3.4 Assume $|S| = 3$, $G' = \mathcal{C}_p \times \mathcal{C}_q$ and $\widehat{S}$ is minimal

In this section we prove the part of Theorem 1.1.3 where, $|S| = 3$, $G' = \mathcal{C}_p \times \mathcal{C}_q$ and $C_{G'}(\mathcal{C}_3) = \{e\}$. Recall $\overline{G} = G/G'$ and $\widehat{G} = G/\mathcal{C}_p$.

**Proposition 3.4.** *Assume*

- $G = (\mathcal{C}_2 \times \mathcal{C}_3) \ltimes (\mathcal{C}_p \times \mathcal{C}_q)$,
- $|S| = 3$,
- $\widehat{S}$ *is minimal.*

*Then* $\mathrm{Cay}(G; S)$ *contains a Hamiltonian cycle.*

*Proof.* Let $S = \{a, b, c\}$. If $C_{G'}(\mathcal{C}_3) \neq \{e\}$, then Proposition 3.3 applies. Hence we may assume $C_{G'}(\mathcal{C}_3) = \{e\}$. Then we have four different cases.

**Case 1.** Assume $C_{G'}(\mathcal{C}_2) = \mathcal{C}_p \times \mathcal{C}_q$, thus $G = \mathcal{C}_2 \times (\mathcal{C}_3 \ltimes \mathcal{C}_{pq})$. Since $\widehat{S}$ is minimal, then all three elements belonging to $\widehat{S}$ must have prime order. There is an element

$\widehat{a} \in \widehat{S}$, such that $|\widehat{a}| = 2$, otherwise all elements of $S$ belong to a subgroup of index 2 of $G$, so $\langle a, b, c\rangle \neq G$ which is a contradiction. If $|a| = 2p$, then Corollary 1.2.7 applies with $s = a$ and $t = a^{-1}$, because there is a Hamiltonian cycle in $\mathrm{Cay}(\widehat{G}; \widehat{S})$ (see Theorem 1.1.2(3)) which uses at least one labeled edge $\widehat{a}$ because $\widehat{S}$ is minimal.

Now we may assume $|a| = 2$. Replacing $a$ by a conjugate we may assume $\langle a\rangle = \mathcal{C}_2$. Thus, $\langle b, c\rangle = \mathcal{C}_3 \ltimes \mathcal{C}_{pq}$. By Theorem 1.1.2(3), there is a Hamiltonian path $L$ in $\mathrm{Cay}(\mathcal{C}_3 \ltimes \mathcal{C}_{pq}, \{b, c\})$. Therefore, $LaL^{-1}a^{-1}$ is a Hamiltonian cycle in $\mathrm{Cay}(G; S)$.

**Case 2.** Assume $C_{G'}(\mathcal{C}_2) = \mathcal{C}_q$. Therefore,

$$\widehat{G} = G/\mathcal{C}_p = \mathcal{C}_6 \ltimes \mathcal{C}_q \cong \mathcal{C}_2 \times (\mathcal{C}_3 \ltimes \mathcal{C}_q).$$

There is some $a \in S$ such that $|\widehat{a}| = 2$. Thus, we can assume $|a| = 2$, for otherwise Corollary 1.2.7 applies with $s = a$ and $t = a^{-1}$. (Note since $\widehat{S}$ is minimal, then $\widehat{a}$ must be used in any Hamiltonian cycle in $\mathrm{Cay}(\widehat{G}; \widehat{S})$.) We may assume $a = a_2$. Since $\widehat{S}$ is minimal, $S \cap G' = \varnothing$ (see Assumption 3.0.1(6)) and each element belonging to $\widehat{S}$ has prime order, then $|\widehat{b}| = |\widehat{c}| = 3$. We may assume $\widehat{a} = a_2$, $\widehat{b} = a_3$ and $\widehat{c} = a_3a_q$. We have the following two Hamiltonian paths in $\mathrm{Cay}(\mathcal{C}_3 \ltimes \mathcal{C}_q; \{\widehat{b}, \widehat{c}\})$:

$$L_1 = ((\widehat{c}, \widehat{b}^2)^{q-1}, \widehat{c}, \widehat{b})$$

and

$$L_2 = ((\widehat{b}, \widehat{c}, \widehat{b})^{q-1}, \widehat{b}, \widehat{c}).$$

These lead to the following two Hamiltonian cycles in $\mathrm{Cay}(\widehat{G}; \widehat{S})$:

$$C_1 = (L_1, \widehat{a}, L_1^{-1}, \widehat{a})$$

and

$$C_2 = (L_2, \widehat{a}, L_2^{-1}, \widehat{a}).$$

Then if we let

$$\prod L_1 = (cb^2)^{q-1}cb = (cb^2)^q b^{-1} \in a_3^{-1}\mathcal{C}_p$$

and

$$\prod L_2 = (bcb)^{q-1}bc = (bcb)^q b^{-1} = b(cb^2)^q b^{-2} = b(\prod L_1)b^{-1}$$

then it is clear that $V(C_i) = [\prod L_i, a]$ for $i = 1, 2$. Therefore, we may assume $a$ centralizes $\prod L_1$ and $\prod L_2$, for otherwise Factor Group Lemma 1.2.6 applies. Now, since $a$ centralizes $\prod L_1$, and $\prod L_1 \in a_3^{-1}\mathcal{C}_p$, we must have $\prod L_1 = a_3^{-1}$. So $\prod L_2 = ba_3^{-1}b^{-1}$. If $b$ does not centralize $a_3$, then $\mathbb{V}(C_1) \neq \mathbb{V}(C_2)$, so the voltage of $C_1$ or $C_2$ cannot both be equal to identity. Therefore, Factor Group Lemma 1.2.6 applies. Now if $b$ centralizes $a_3$, then we can assume $b = a_3$. Therefore, $c = a_3 a_q \gamma_p$. We calculate the voltage of $C_1$. We have

$$\begin{aligned}
\mathbb{V}(C_1) &= (cb^2)^q b^{-1} a((cb^2)^q b^{-1})^{-1} a \\
&= (a_3 a_q \gamma_p \cdot a_3^2)^q \cdot a_3^{-1} \cdot a_2 \cdot ((a_3 a_q \gamma_p \cdot a_3^2)^q \cdot a_3^{-1})^{-1} \cdot a_2 \\
&= (a_3 a_q \gamma_p a_3^{-1})^q a_3^{-1} a_2 ((a_3 a_q \gamma_p a_3^{-1}) a_3^{-1})^{-1} a_2 \\
&= a_3 a_q^q \gamma_p^q a_3^{-1} a_3^{-1} a_2 (a_3 a_q^q \gamma_p^q a_3^{-1} a_3^{-1})^{-1} a_2 \\
&= a_3 \gamma_p^q a_3^{-2} a_2 (a_3 \gamma_p^q a_3^{-2})^{-1} a_2 \\
&= a_3 \gamma_p^q a_3^{-2} a_2 a_3^2 \gamma_p^{-q} a_3^{-1} a_2 \\
&= a_3 \gamma_p^{2q} a_3^{-1}
\end{aligned}$$

which generates $\mathcal{C}_p$. Thus, Factor Group Lemma 1.2.6 applies.

**Case 3.** Assume $C_{G'}(\mathcal{C}_2) = \mathcal{C}_p$. Therefore,

$$\breve{G} = G/\mathcal{C}_q = \mathcal{C}_6 \ltimes \mathcal{C}_p \cong \mathcal{C}_2 \times (\mathcal{C}_3 \ltimes \mathcal{C}_p).$$

Now since $S \cap G' = \varnothing$ (see Assumption 3.0.1(6)) and $\mathcal{C}_3$ does not centralize $\mathcal{C}_p$, then for all $a \in S$, we have $|\breve{a}| \in \{2, 3, 6, 2p\}$. If $|\breve{a}| = 6$, then $|\widehat{a}|$ is divisible by 6 which contradicts the minimality of $\widehat{S}$. (Note that every element belong to $\widehat{S}$ has prime order.) If $|\breve{a}| = 2p$, then $|\widehat{a}| = 2$ (because $\widehat{S}$ is minimal). Therefore, Corollary 1.2.7 applies with $s = a$ and $t = a^{-1}$ (Note that since $\widehat{S}$ is minimal, then there is a Hamiltonian cycle in $\mathrm{Cay}(\widehat{G}; \widehat{S})$ uses at least one labeled edge $\widehat{a}$.) Thus, $|\breve{a}| \in \{2, 3\}$ for all $a \in S$. This implies that $\breve{S}$ is minimal, because we need an $a_2$ and an $a_3$ to generate $\mathcal{C}_2 \times \mathcal{C}_3$ and two elements whose order divisible by 2 or 3 to generate $\mathcal{C}_p$. So by interchanging $p$ and $q$ the proof in Case 2 applies.

**Case 4.** Assume $C_{G'}(\mathcal{C}_2) = \{e\}$. Consider

$$\widehat{G} = G/\mathcal{C}_p = (\mathcal{C}_2 \times \mathcal{C}_3) \ltimes \mathcal{C}_q.$$

Now since $\widehat{S}$ is minimal, every element of $\widehat{S}$ has prime order. Since $S \cap G' = \varnothing$ (see Assumption 3.0.1(6)), then for every $\widehat{s} \in \widehat{S}$, we have $|\widehat{s}| \in \{2, 3\}$. Since $C_{G'}(\mathcal{C}_2) = \{e\}$ and $C_{G'}(\mathcal{C}_3) = \{e\}$, this implies that for every $s \in S$, we have $|s| \in \{2, 3\}$. From our assumption we know that $S = \{a, b, c\}$. Now we may assume $|a| = 2$ and $|b| = 3$. Also, we know that $|c| \in \{2, 3\}$.

If $|c| = 2$, then $c = a\gamma$, where $\gamma \in G'$. Suppose, for the moment, $\langle\gamma\rangle \neq G'$. Since $\langle\gamma\rangle \lhd G$, then we have

$$G = \langle a, b, c\rangle = \langle a, b, \gamma\rangle = \langle a, b\rangle\langle\gamma\rangle.$$

Now since $\widehat{S}$ is minimal, $\langle a, b\rangle$ does not contain $\mathcal{C}_q$. So this implies that $\langle\gamma\rangle$ contains $\mathcal{C}_q$. Since $\langle\gamma\rangle$ does not contain $G'$, then $\langle\gamma\rangle = \mathcal{C}_q$. Thus, we may assume that $a = a_2$ (by conjugation if necessary), $b = a_3\gamma_p$ and $c = a_2a_q$. So $\langle b, c\rangle = \langle a_3\gamma_p, a_2a_q\rangle = G$ (since $a_3\gamma_p$ and $a_2a_q$ clearly generate $\overline{G}$ and do not commute modulo $p$ or modulo $q$, they must generate $G$). This contradicts the minimality of $S$. Therefore, $\langle\gamma\rangle = G'$.

Consider $\overline{G} = \mathcal{C}_2 \times \mathcal{C}_3$. Then $\overline{a} = \overline{c}$. We have $|\overline{a}| = |\overline{c}| = 2$ and $|\overline{b}| = 3$. We also have $C_1 = (\overline{c}^{-1}, \overline{b}^{-2}, \overline{a}, \overline{b}^{2})$ as a Hamiltonian cycle in $\mathrm{Cay}(\overline{G}; \overline{S})$. Now we calculate its voltage.

$$\mathbb{V}(C_1) = c^{-1}b^{-2}ab^2 = \gamma^{-1}a^{-1}b^{-2}ab^2.$$

Now, $a^{-1}b^{-2}ab^2 \in G'$. Since $\langle a, b\rangle \neq G$, we have $a^{-1}b^{-2}ab^2 \in \{e, \gamma_p\}$. If $a^{-1}b^{-2}ab^2 = e$, then $a$ and $b^2$ commute, so $a$ and $b$ commute. Hence $b = a_3$, so $\langle b, c\rangle = G$, a contradiction. So $a^{-1}b^{-2}ab^2 = \gamma_p$, and $\mathbb{V}(C_1) = \gamma^{-1}\gamma_p$ which generates $G'$. Therefore, Factor Group Lemma 1.2.6 applies.

Now we can assume $|c| = 3$. Then $c = b\gamma$, where $\gamma \in G'$ (after replacing $c$ with its inverse if necessary). Suppose, for the moment, $\langle\gamma\rangle \neq G'$. Since $\langle\gamma\rangle \lhd G$, then we have

$$G = \langle a, b, c\rangle = \langle a, b, \gamma\rangle = \langle a, b\rangle\langle\gamma\rangle.$$

Now since $\widehat{S}$ is minimal, then $\langle a, b\rangle$ does not contain $\mathcal{C}_q$. So this implies that $\langle\gamma\rangle$ contains $\mathcal{C}_q$. Since $\langle\gamma\rangle$ does not contain $G'$, then $\langle\gamma\rangle = \mathcal{C}_q$. Therefore, we may assume that $a = a_2\gamma_p$ (by conjugation if necessary), $b = a_3$ and $c = a_3a_q$. So $\langle a, c\rangle = \langle a_2\gamma_p, a_3a_q\rangle = G$ (since $a_2\gamma_p$ and $a_3a_q$ clearly generate $\overline{G}$ and do not commute modulo $p$ or modulo $q$, they must generate $G$). This contradicts the minimality of $S$. So $\langle\gamma\rangle = G'$.

Consider $\overline{G} = \mathcal{C}_2 \times \mathcal{C}_3$. Then $\overline{b} = \overline{c}$. We have $|\overline{a}| = 2$ and $|\overline{b}| = |\overline{c}| = 3$. We also have $C_2 = (\overline{c}^{-1}, \overline{b}^{-1}, \overline{a}^{-1}, \overline{b}^{2}, \overline{a})$ as a Hamiltonian cycle in $\mathrm{Cay}(\overline{G}; \overline{S})$. Now we calculate its voltage.

$$\mathbb{V}(C_2) = c^{-1}b^{-1}a^{-1}b^2a = \gamma^{-1}b^{-1}b^{-1}a^{-1}b^2a.$$

Now, $b^{-2}a^{-1}b^2a \in G'$. Since $\langle a, b\rangle \neq G$, we have $b^{-2}a^{-1}b^2a \in \{e, \gamma_p\}$. If $b^{-2}a^{-1}b^2a = e$, then $a$ and $b^2$ commute, so $a$ and $b$ commute. Hence $a = a_2$, so $\langle a, c\rangle = G$, a contradiction. So $b^{-2}a^{-1}b^2a = \gamma_p$, and $\mathbb{V}(C_2) = \gamma^{-1}\gamma_p$ which generates $G'$. Therefore, Factor Group Lemma 1.2.6 applies. □

## 3.5 Assume $|S| = 3$, $G' = \mathcal{C}_p \times \mathcal{C}_q$ and $C_{G'}(\mathcal{C}_2) = \mathcal{C}_p \times \mathcal{C}_q$

In this section we prove the part of Theorem 1.1.3 where, $|S| = 3$, $G' = \mathcal{C}_p \times \mathcal{C}_q$, $C_{G'}(\mathcal{C}_2) = \mathcal{C}_p \times \mathcal{C}_q$, and neither $C_{G'}(\mathcal{C}_3) \neq \{e\}$ nor $\widehat{S}$ is minimal holds. Recall $\overline{G} = G/G'$, $\breve{G} = G/\mathcal{C}_q$ and $\widehat{G} = G/\mathcal{C}_p$.

**Proposition 3.5.** *Assume*

- $G = (\mathcal{C}_2 \times \mathcal{C}_3) \ltimes (\mathcal{C}_p \times \mathcal{C}_q)$,
- $|S| = 3$,
- $C_{G'}(\mathcal{C}_2) = \mathcal{C}_p \times \mathcal{C}_q$.

*Then* $\mathrm{Cay}(G; S)$ *contains a Hamiltonian cycle.*

*Proof.* Let $S = \{a, b, c\}$. If $C_{G'}(\mathcal{C}_3) \neq \{e\}$, then Proposition 3.3 applies. So we may assume $C_{G'}(\mathcal{C}_3) = \{e\}$. Now if $\widehat{S}$ is minimal, then Proposition 3.4 applies. So we may assume $\widehat{S}$ is not minimal. Consider

$$\widehat{G} = G/\mathcal{C}_p = (\mathcal{C}_2 \times \mathcal{C}_3) \ltimes \mathcal{C}_q \cong (\mathcal{C}_3 \ltimes \mathcal{C}_q) \times \mathcal{C}_2.$$

Choose a 2-element $\{a, b\}$ subset of $S$ that generates $\widehat{G}$. From the minimality of $S$, we see that

$$\langle a, b \rangle = (\mathcal{C}_3 \ltimes \mathcal{C}_q) \times \mathcal{C}_2,$$

after replacing $a$ and $b$ by conjugates. The projection of $(a, b)$ to $\mathcal{C}_3 \ltimes \mathcal{C}_q$ must be of the form $(a_3, a_q)$ or $(a_3, a_3 a_q)$ (perhaps after replacing $a$ and/or $b$ with its inverse; also note that $\widehat{b} \neq a_q$ because $S \cap G' = \varnothing$). Therefore, $(a, b)$ must have one of the following forms:

1. $(a_3, a_2 a_q)$,
2. $(a_3, a_2 a_3 a_q)$,
3. $(a_2 a_3, a_3 a_q)$,
4. $(a_2 a_3, a_2 a_q)$,
5. $(a_2 a_3, a_2 a_3 a_q)$.

Let $c$ be the third element of $S$. We may write $c = a_2^i a_3^j a_q^k \gamma_p$ with $0 \leqslant i \leqslant 1$, $0 \leqslant j \leqslant 2$ and $0 \leqslant k \leqslant q-1$. Note since $S \cap G' = \varnothing$, we know that $i$ and $j$ cannot both be equal to 0. Additionally, we have $a_3 \gamma_p a_3^{-1} = \gamma_p^{\widehat{\tau}}$ where $\widehat{\tau}^3 \equiv 1 \pmod{p}$ and $\widehat{\tau} \not\equiv 1 \pmod{p}$. Thus $\widehat{\tau}^2 + \widehat{\tau} + 1 \equiv 0 \pmod{p}$. Note that this implies $\widehat{\tau} \not\equiv -1 \pmod{p}$. Also we have $a_3 a_q a_3^{-1} = a_q^{\check{\tau}}$. By using the same argument we can conclude that $\check{\tau} \not\equiv 1 \pmod{q}$ and $\check{\tau}^2 + \check{\tau} + 1 \equiv 0 \pmod{q}$. Note that this implies $\check{\tau} \not\equiv -1 \pmod{q}$. Combining these facts with $\widehat{\tau}^3 \equiv 1 \pmod{p}$ and $\check{\tau}^3 \equiv 1 \pmod{q}$, we conclude that $\widehat{\tau}^2 \not\equiv \pm 1 \pmod{p}$, and $\check{\tau}^2 \not\equiv \pm 1 \pmod{q}$.

**Case 1.** Assume $a = a_3$ and $b = a_2 a_q$.

**Subcase 1.1.** Assume $i = 0$. Then $j \neq 0$ and $c = a_3^j a_q^k \gamma_p$. For future reference in Subcase 4.1 of Proposition 3.6, we note that the argument here does not require our current assumption that $\mathcal{C}_2$ centralizes $\mathcal{C}_p$. We may assume $j = 1$, by replacing $c$ with $c^{-1}$ if necessary. Then $c = a_3 a_q^k \gamma_p$. Consider $\overline{G} = \mathcal{C}_2 \times \mathcal{C}_3$. Then we have $\overline{a} = \overline{c} = a_3$, $\overline{b} = a_2$. We have $C_1 = (\overline{c}, \overline{a}, \overline{b}, \overline{a}^{-2}, \overline{b})$ and $C_2 = (\overline{c}^2, \overline{b}, \overline{a}^{-2}, \overline{b})$ as Hamiltonian cycles in

$\mathrm{Cay}(\overline{G}; \overline{S})$. Since there is one occurrence of $c$ in $C_1$, then by Lemma 2.5.2 we conclude that the subgroup generated by $\mathbb{V}(C_1)$ contains $\mathcal{C}_p$. Also,

$$\begin{aligned}
\mathbb{V}(C_1) &= caba^{-2}b \\
&\equiv a_3 a_q^k \cdot a_3 \cdot a_2 a_q \cdot a_3^{-2} \cdot a_2 a_q \pmod{\mathcal{C}_p} \\
&= a_q^{k\check{\tau} + \check{\tau}^2 + 1} \\
&= a_q^{\check{\tau}^2 + k\check{\tau} + 1}.
\end{aligned}$$

We may assume this does not generate $\mathcal{C}_q$, for otherwise Factor Group Lemma 1.2.6 applies. Therefore,

$$0 \equiv \check{\tau}^2 + k\check{\tau} + 1 \pmod{q}. \tag{1.1A}$$

We also have

$$0 \equiv \check{\tau}^2 + \check{\tau} + 1 \pmod{q}. \tag{1.1B}$$

By subtracting the above equation from 1.1A, we have $0 \equiv (k-1)\check{\tau} \pmod{q}$. This implies that $k = 1$.

Now we calculate the voltage of $C_2$.

$$\begin{aligned}
\mathbb{V}(C_2) &= c^2ba^{-2}b \\
&\equiv a_3 \gamma_p a_3 \gamma_p \cdot a_2 \cdot a_3^{-2} \cdot a_2 \pmod{\mathcal{C}_q} \\
&= \gamma_p^{\hat{\tau} + \hat{\tau}^2}
\end{aligned}$$

which generates $\mathcal{C}_p$. Also

$$\mathbb{V}(C_2) = c^2ba^{-2}b$$

$$\begin{aligned}
&\equiv a_3 a_q \cdot a_3 a_q \cdot a_2 a_q \cdot a_3^{-2} \cdot a_2 a_q \pmod{\mathcal{C}_p} \\
&= a_q^{\check{\tau}+\check{\tau}^2+\check{\tau}^2+1} \\
&= a_q^{2\check{\tau}^2+\check{\tau}+1}.
\end{aligned}$$

We may assume this does not generate $\mathcal{C}_q$, for otherwise Factor Group Lemma 1.2.6 applies. Then

$$0 \equiv 2\check{\tau}^2 + \check{\tau} + 1 \pmod{q}.$$

By subtracting 1.1B from the above equation we have

$$0 \equiv \check{\tau}^2 \pmod{q}$$

which is a contradiction.

**Subcase 1.2.** Assume $j = 0$. Then $i \neq 0$ and $c = a_2 a_q^k \gamma_p$. For future reference in Subcase 4.2 of Proposition 3.6, we note that the argument here does not require our current assumption that $\mathcal{C}_2$ centralizes $\mathcal{C}_p$. If $k \neq 0$, then by Lemma 2.4.2(3) $\langle a, c \rangle = G$ which contradicts the minimality of $S$.

So we can assume $k = 0$. Then $c = a_2\gamma_p$. Consider $\overline{G} = \mathcal{C}_2 \times \mathcal{C}_3$. Then we have $\overline{a} = a_3$ and $\overline{b} = \overline{c} = a_2$. This implies that $|\overline{a}| = 3$ and $|\overline{b}| = |\overline{c}| = 2$. We have $C = (\overline{c}^{-1}, \overline{a}^2, \overline{b}, \overline{a}^{-2})$ as a Hamiltonian cycle in $\mathrm{Cay}(\overline{G}; \overline{S})$. Since there is one occurrence of $c$ in $C$, and it is the only generator of $G$ that contains $\gamma_p$, then by Lemma 2.5.2 we conclude that the subgroup generated by $\mathbb{V}(C)$ contains $\mathcal{C}_p$. Similarly, since there is one occurrence of $b$ in $C$, and it is the only generator of $G$ that contains $a_q$, then by Lemma 2.5.2 we conclude that the subgroup generated by $\mathbb{V}(C)$ contains $\mathcal{C}_q$. Therefore, the subgroup generated by $\mathbb{V}(C)$ is $G'$. So, Factor Group Lemma 1.2.6 applies.

**Subcase 1.3.** Assume $i \neq 0$ and $j \neq 0$. Then $c = a_2 a_3^j a_q^k \gamma_p$. If $k \neq 0$, then by Lemma 2.4.2(3) $\langle a, c\rangle = G$ which contradicts the minimality of $S$.

So we can assume $k = 0$. We may also assume $j = 1$, by replacing $c$ with $c^{-1}$ if necessary. Then $c = a_2 a_3 \gamma_p$. Consider $\overline{G} = \mathcal{C}_2 \times \mathcal{C}_3$. Then we have $\overline{a} = a_3$, $\overline{b} = a_2$ and $\overline{c} = a_2 a_3$. This implies that $|\overline{a}| = 3$, $|\overline{b}| = 2$ and $|\overline{c}| = 6$. We have $C = (\overline{c}, \overline{b}, \overline{a}, \overline{c}, \overline{a}^{-1}, \overline{c})$ as a Hamiltonian cycle in $\mathrm{Cay}(\overline{G}; \overline{S})$. Now we calculate its voltage.

$$\begin{aligned}
\mathbb{V}(C) &= cbaca^{-1}c \\
&\equiv a_2a_3 \cdot a_2a_q \cdot a_3 \cdot a_2a_3 \cdot a_3^{-1} \cdot a_2a_3 \pmod{\mathcal{C}_p} \\
&= a_3a_qa_3^2 \\
&= a_q^{\check{\tau}}
\end{aligned}$$

which generates $\mathcal{C}_q$. Also

$$\begin{aligned}
\mathbb{V}(C) &= cbaca^{-1}c \\
&\equiv a_2a_3\gamma_p \cdot a_2 \cdot a_3 \cdot a_2a_3\gamma_p \cdot a_3^{-1} \cdot a_2a_3\gamma_p \pmod{\mathcal{C}_q} \\
&= a_3\gamma_pa_3^2\gamma_p^2 \\
&= \gamma_p^{\hat{\tau}+2}.
\end{aligned}$$

We may assume this does not generate $\mathcal{C}_p$, for otherwise Factor Group Lemma 1.2.6 applies. Then $\hat{\tau} \equiv -2 \pmod{p}$. By substituting this in

$$0 \equiv \hat{\tau}^2 + \hat{\tau} + 1 \pmod{p},$$

we have

$$0 \equiv 4 - 2 + 1 \pmod{p}$$

$$= 3.$$

This contradicts the fact that $p > 3$.

**Case 2.** Assume $a = a_3$ and $b = a_2a_3a_q$.

**Subcase 2.1.** Assume $i \neq 0$ and $j \neq 0$. Then $c = a_2a_3^ja_q^k\gamma_p$. If $k \neq 0$, then by Lemma 2.4.2(3) $\langle a, c\rangle = G$ which contradicts the minimality of $S$. So we can assume $k = 0$. Then $c = a_2a_3^j\gamma_p$. Thus, by Lemma 2.4.2(4) $\langle b, c\rangle = G$ which contradicts the minimality of $S$.

**Subcase 2.2.** Assume $i = 0$. Then $j \neq 0$. We may assume $j = 1$, by replacing $c$ with $c^{-1}$ if necessary. Then $c = a_3a_q^k\gamma_p$.

Suppose, for the moment, that $k \neq 1$. Then $c = a_3a_q^k\gamma_p$. We have $\langle \overline{b}, \overline{c}\rangle = \langle \overline{a}_2\overline{a}_3, \overline{a}_3\rangle = \overline{G}$. Consider $\{\widehat{b}, \widehat{c}\} = \{a_2a_3a_q, a_3a_q^k\}$. Since $\mathcal{C}_2$ centralizes $\mathcal{C}_q$, then

$$[a_2a_3a_q, a_3a_q^k] = [a_3a_q, a_3a_q^k] = a_3a_qa_3a_q^ka_q^{-1}a_3^{-1}a_q^{-k}a_3^{-1} = a_q^{\check{\tau}+k\check{\tau}^2-\check{\tau}^2-k\check{\tau}} = a_q^{\check{\tau}(k-1)(\check{\tau}-1)}$$

which generates $\mathcal{C}_q$. Now consider $\{\check{b}, \check{c}\} = \{a_2a_3, a_3\gamma_p\}$. Since $\mathcal{C}_2$ centralizes $\mathcal{C}_p$, then

$$[a_2a_3, a_3\gamma_p] = [a_3, a_3\gamma_p] = a_3a_3\gamma_pa_3^{-1}\gamma_p^{-1}a_3^{-1} = \gamma_p^{\hat{\tau}^2-\hat{\tau}} = \gamma_p^{\hat{\tau}(\hat{\tau}-1)}$$

which generates $\mathcal{C}_p$. Therefore, $\langle b, c\rangle = G$ which contradicts the minimality of $S$.

Now we can assume $k = 1$. Then $c = a_3a_q\gamma_p$. Consider $\overline{G} = \mathcal{C}_2 \times \mathcal{C}_3$. We have $\overline{a} = \overline{c} = a_3$ and $\overline{b} = a_2a_3$. This implies that $|\overline{a}| = |\overline{c}| = 3$ and $|\overline{b}| = 6$. We have $C = (\overline{c}, \overline{b}, \overline{a}^2, \overline{b}, \overline{a})$ as a Hamiltonian cycle in $\mathrm{Cay}(\overline{G}; \overline{S})$. Since there is one occurrence of $c$ in $C$, and it is the only generator of $G$ that contains $\gamma_p$, then by Lemma 2.5.2 we conclude that the subgroup generated by $\mathbb{V}(C)$ is $\mathcal{C}_p$. Also,

$$\mathbb{V}(C) = cba^2ba$$

$$\begin{aligned}
&\equiv a_3a_q \cdot a_2a_3a_q \cdot a_3^2 \cdot a_2a_3a_q \cdot a_3 \pmod{\mathcal{C}_p} \\
&= a_3a_qa_3a_q^2a_3 \\
&= a_q^{\breve{\tau}+2\breve{\tau}^2} \\
&= a_q^{\breve{\tau}(1+2\breve{\tau})}.
\end{aligned}$$

We may assume this does not generate $\mathcal{C}_q$, for otherwise Factor Group Lemma 1.2.6 applies. Therefore, $1 + 2\breve{\tau} \equiv 0 \pmod{q}$. This implies that $\breve{\tau} \equiv -1/2 \pmod{q}$. By substituting $\breve{\tau} \equiv -1/2 \pmod{q}$ in

$$\breve{\tau}^2 + \breve{\tau} + 1 \equiv 0 \pmod{q},$$

then we have $3/4 \equiv 0 \pmod{q}$, which contradicts Assumption 3.0.1(1).

**Subcase 2.3.** Assume $j = 0$. Then $i \neq 0$ and $c = a_2a_q^k\gamma_p$. If $k \neq 0$, then by Lemma 2.4.2(3) $\langle a, c\rangle = G$ which contradicts the minimality of $S$.

So we can assume $k = 0$. Then $c = a_2\gamma_p$. Consider $\overline{G} = \mathcal{C}_2 \times \mathcal{C}_3$. Then we have $\overline{a} = a_3$, $\overline{b} = a_2a_3$ and $\overline{c} = a_2$. This implies that $|\overline{a}| = 3$, $|\overline{b}| = 6$ and $|\overline{c}| = 2$. We have $C = (\overline{c}, \overline{a}, \overline{b}, \overline{a}^{-1}, \overline{b}^2)$ as a Hamiltonian cycle in $\mathrm{Cay}(\overline{G}; \overline{S})$. Since there is one occurrence of $c$ in $C$, and it is the only generator of $G$ that contains $\gamma_p$, then by Lemma 2.5.2 we conclude that the subgroup generated by $\mathbb{V}(C)$ contains $\mathcal{C}_p$. Also,

$$\begin{aligned}
\mathbb{V}(C) &= caba^{-1}b^2 \\
&\equiv a_2 \cdot a_3 \cdot a_2a_3a_q \cdot a_3^{-1} \cdot a_2a_3a_qa_2a_3a_q \pmod{\mathcal{C}_p} \\
&= a_3^2a_q^2a_3a_q \\
&= a_q^{2\breve{\tau}^2+1}.
\end{aligned}$$

We may assume this does not generate $\mathcal{C}_q$, for otherwise Factor Group Lemma 1.2.6

applies. Thus, $\check{\tau}^2 \equiv -1/2 \pmod{q}$. By substituting this in

$$\check{\tau}^2 + \check{\tau} + 1 \equiv 0 \pmod{q},$$

we have $\check{\tau} \equiv -1/2 \pmod{q}$ which contradicts $\check{\tau}^2 \equiv -1/2 \pmod{q}$.

**Case 3.** Assume $a = a_2a_3$ and $b = a_3a_q$. Since $b = a_3a_q$ is conjugate to $a_3$ via an element of $\mathcal{C}_q$, then $\{a, b\}$ is conjugate to $\{a_2a_3a_q^m, a_3\}$ for some nonzero $m$. So Case 2 applies (after replacing $a_q$ with $a_q^m$).

**Case 4.** Assume $a = a_2a_3$ and $b = a_2a_q$.

**Subcase 4.1.** Assume $i = 0$. Then $j \neq 0$ and $c = a_3^j a_q^k \gamma_p$. If $k \neq 0$, then by Lemma 2.4.2(1) $\langle a, c\rangle = G$ which contradicts the minimality of $S$.

So we can assume $k = 0$. We may also assume $j = 1$, by replacing $c$ with $c^{-1}$ if necessary. Then $c = a_3\gamma_p$. Consider $\overline{G} = \mathcal{C}_2 \times \mathcal{C}_3$. Thus, $\overline{a} = a_2a_3$, $\overline{b} = a_2$ and $\overline{c} = a_3$. This implies that $|\overline{a}| = 6$, $|\overline{b}| = 2$ and $|\overline{c}| = 3$. We have $C = (\overline{a}^2, \overline{b}, \overline{c}, \overline{a}, \overline{c}^{-1})$ as a Hamiltonian cycle in $\mathrm{Cay}(\overline{G}; \overline{S})$. Since there is one occurrence of $b$ in $C$, and it is the only generator of $G$ that contains $a_q$, then by Lemma 2.5.2 we conclude that the subgroup generated by $\mathbb{V}(C)$ contains $\mathcal{C}_q$. Also,

$$\begin{aligned}
\mathbb{V}(C) &= a^2bcac^{-1} \\
&\equiv a_3^2 \cdot a_2 \cdot a_3\gamma_p \cdot a_2a_3 \cdot \gamma_p^{-1}a_3^{-1} \pmod{\mathcal{C}_q} \\
&= \gamma_p a_3 \gamma_p^{-1} a_3^{-1} \\
&= \gamma_p^{1-\hat{\tau}}
\end{aligned}$$

which generates $\mathcal{C}_p$. Therefore, the subgroup generated by $\mathbb{V}(C)$ is $G'$. So, Factor Group Lemma 1.2.6 applies.

**Subcase 4.2.** Assume $j = 0$. Then $i \neq 0$ and $c = a_2a_q^k\gamma_p$. If $k \neq 0$, then by Lemma 2.4.2(1) $\langle a, c\rangle = G$ which contradicts the minimality of $S$.

So we can assume $k = 0$. Then $c = a_2\gamma_p$. Consider $\overline{G} = \mathcal{C}_2 \times \mathcal{C}_3$, then $\overline{a} = a_2a_3$ and $\overline{b} = \overline{c} = a_2$. This implies that $|\overline{a}| = 6$ and $|\overline{b}| = |\overline{c}| = 2$. We have $C = ((\overline{a}, \overline{b})^2, \overline{a}, \overline{c})$ as a Hamiltonian cycle in $\mathrm{Cay}(\overline{G}; \overline{S})$. Since there is one occurrence of $c$ in $C$, and it is the only generator of $G$ that contains $\gamma_p$, then by Lemma 2.5.2 we conclude that the subgroup generated by $\mathbb{V}(C)$ contains $\mathcal{C}_p$. Also,

$$\begin{aligned}
\mathbb{V}(C) &= (ab)^2 ac \\
&\equiv (a_2a_3 \cdot a_2a_q)^2 \cdot a_2a_3 \cdot a_2 \pmod{\mathcal{C}_p} \\
&= a_3a_qa_3a_qa_3 \\
&= a_q^{\check{\tau}+\check{\tau}^2}.
\end{aligned}$$

which generates $\mathcal{C}_q$. Therefore, the subgroup generated by $\mathbb{V}(C)$ is $G'$. Thus, Factor Group Lemma 1.2.6 applies.

**Subcase 4.3.** Assume $i \neq 0$ and $j \neq 0$. Then $c = a_2a_3^ja_q^k\gamma_p$. If $k \neq 0$, then by Lemma 2.4.2(1) $\langle a, c\rangle = G$ which contradicts the minimality of $S$.

So we can assume $k = 0$. We may also assume $j = 1$, by replacing $c$ with $c^{-1}$ if necessary. Then $c = a_2a_3\gamma_p$. Consider $\overline{G} = \mathcal{C}_2 \times \mathcal{C}_3$. Thus, $\overline{a} = \overline{c} = a_2a_3$ and $\overline{b} = a_2$. This implies that $|\overline{a}| = |\overline{c}| = 6$ and $|\overline{b}| = 2$. We have $C = (\overline{a}, \overline{c}, \overline{b}, \overline{a}^{-2}, \overline{b})$ as a Hamiltonian cycle in $\mathrm{Cay}(\overline{G}; \overline{S})$. Since there is one occurrence of $c$ in $C$, and it is the only generator of $G$ that contains $\gamma_p$, then by Lemma 2.5.2 we conclude that the subgroup generated by $\mathbb{V}(C)$ contains $\mathcal{C}_p$. Also,

$$\begin{aligned}
\mathbb{V}(C) &= acba^{-2}b \\
&\equiv a_2a_3 \cdot a_2a_3 \cdot a_2a_q \cdot a_3^{-2} \cdot a_2a_q \pmod{\mathcal{C}_p} \\
&= a_3^2a_qa_3^{-2}a_q \\
&= a_q^{\check{\tau}^2+1}
\end{aligned}$$

which generates $\mathcal{C}_q$, because $\check{\tau}^2 \not\equiv -1 \pmod q$. Therefore, the subgroup generated by $\mathbb{V}(C)$ is $G'$. So, Factor Group Lemma 1.2.6 applies.

**Case 5.** Assume $a = a_2 a_3$ and $b = a_2 a_3 a_q$. If $k \neq 0$, then by Lemma 2.4.2(1) $\langle a, c \rangle = G$ which contradicts the minimality of $S$. So we can assume $k = 0$. Also, if $j \neq 0$, then by Lemma 2.4.2(4) $\langle b, c \rangle = G$ which contradicts the minimality of $S$. So we may also assume $j = 0$. Then $i \neq 0$. Therefore, $c = a_2 \gamma_p$. So Case 4 applies, after interchanging $b$ and $c$, and interchanging $p$ and $q$. □

## 3.6 Assume $|S| = 3$, $G' = \mathcal{C}_p \times \mathcal{C}_q$ and $C_{G'}(\mathcal{C}_2) \neq \{e\}$

In this section we prove the part of Theorem 1.1.3 where, $|S| = 3$, $G' = \mathcal{C}_p \times \mathcal{C}_q$, $C_{G'}(\mathcal{C}_2) \neq \{e\}$, and neither $C_{G'}(\mathcal{C}_2) = \mathcal{C}_p \times \mathcal{C}_q$ nor $C_{G'}(\mathcal{C}_3) \neq \{e\}$ nor $\widehat{S}$ is minimal holds. Recall $\overline{G} = G/G'$, $\check{G} = G/\mathcal{C}_q$ and $\widehat{G} = G/\mathcal{C}_p$.

**Proposition 3.6.** *Assume*

- $G = (\mathcal{C}_2 \times \mathcal{C}_3) \ltimes (\mathcal{C}_p \times \mathcal{C}_q)$,
- $|S| = 3$,
- $C_{G'}(\mathcal{C}_2) \neq \{e\}$.

*Then* $\mathrm{Cay}(G; S)$ *contains a Hamiltonian cycle.*

*Proof.* Let $S = \{a, b, c\}$. If $C_{G'}(\mathcal{C}_3) \neq \{e\}$, then Proposition 3.3 applies. Therefore, we may assume $C_{G'}(\mathcal{C}_3) = \{e\}$. Now if $C_{G'}(\mathcal{C}_2) = \mathcal{C}_p \times \mathcal{C}_q$, then Proposition 3.5 applies. Since $C_{G'}(\mathcal{C}_2) \neq \{e\}$, then we may assume $C_{G'}(\mathcal{C}_2) = \mathcal{C}_q$, by interchanging $q$ and $p$ if necessary. This implies that $\mathcal{C}_2$ inverts $\mathcal{C}_p$. Now if $\widehat{S}$ is minimal, then Proposition 3.4 applies. So we may assume $\widehat{S}$ is not minimal. Consider

$$\widehat{G} = G/\mathcal{C}_p = (\mathcal{C}_2 \times \mathcal{C}_3) \ltimes \mathcal{C}_q.$$

Choose a 2-element subset $\{a, b\}$ in $S$ that generates $\widehat{G}$. From the minimality of $S$, we see that

$$\langle a, b \rangle = (\mathcal{C}_2 \times \mathcal{C}_3) \ltimes \mathcal{C}_q$$

after replacing $a$ and $b$ by conjugates. We may assume $|\overline{a}| \geqslant |\overline{b}|$ and (by conjugating if necessary) $a$ is an element of $\mathcal{C}_2 \times \mathcal{C}_3$. Then the projection of $(a, b)$ to $\mathcal{C}_2 \times \mathcal{C}_3$ has one of the following forms after replacing $a$ and $b$ with their inverses if necessary.

- $(a_2a_3, a_2a_3)$,
- $(a_2a_3, a_2)$,
- $(a_2a_3, a_3)$,
- $(a_3, a_2)$.

So there are four possibilities for $(a, b)$:

1. $(a_2a_3, a_2a_3a_q)$,
2. $(a_2a_3, a_2a_q)$,
3. $(a_2a_3, a_3a_q)$,
4. $(a_3, a_2a_q)$.

Let $c$ be the third element of $S$. We may write $c = a_2^i a_3^j a_q^k \gamma_p$ with $0 \leqslant i \leqslant 1$, $0 \leqslant j \leqslant 2$ and $0 \leqslant k \leqslant q-1$. Note since $S \cap G' = \varnothing$, we know that $i$ and $j$ cannot both be equal to 0. Additionally, we have $a_3\gamma_p a_3^{-1} = \gamma_p^{\widehat{\tau}}$ where $\widehat{\tau}^3 \equiv 1 \pmod{p}$ and $\widehat{\tau} \not\equiv 1 \pmod{p}$. Thus $\widehat{\tau}^2 + \widehat{\tau} + 1 \equiv 0 \pmod{p}$. Note that this implies $\widehat{\tau} \not\equiv -1 \pmod{p}$. Also we have $a_3a_qa_3^{-1} = a_q^{\check{\tau}}$. By using the same argument we can conclude that $\check{\tau} \not\equiv 1 \pmod{q}$ and $\check{\tau}^2 + \check{\tau} + 1 \equiv 0 \pmod{q}$. Note that this implies $\check{\tau} \not\equiv -1 \pmod{q}$. Therefore, we conclude that $\widehat{\tau}^2 \not\equiv \pm 1 \pmod{p}$, and $\check{\tau}^2 \not\equiv \pm 1 \pmod{q}$.

**Case 1.** Assume $a = a_2a_3$ and $b = a_2a_3a_q$. If $k \neq 0$, then by Lemma 2.4.2(1), $\langle a, c \rangle = G$ which contradicts the minimality of $S$. So we can assume $k = 0$. Now if $j \neq 0$, then by Lemma 2.4.2(4), $\langle b, c \rangle = G$ which contradicts the minimality of $S$.

Therefore, we may assume $j = 0$. Then $i \neq 0$ and $c = a_2\gamma_p$. Consider $\overline{G} = \mathcal{C}_2 \times \mathcal{C}_3$. Thus $\overline{a} = \overline{b} = a_2a_3$ and $\overline{c} = a_2$. Therefore, $|\overline{a}| = |\overline{b}| = 6$ and $|\overline{c}| = 2$. We have $C = (\overline{a}, \overline{b}, \overline{c}, \overline{a}^{-2}, \overline{c})$ as a Hamiltonian cycle in $\mathrm{Cay}(\overline{G}; \overline{S})$. Since there is one occurrence of $b$ in $C$, and it is the only generator of $G$ that contains $a_q$, then by Lemma 2.5.2 we conclude that the subgroup generated by $\mathbb{V}(C)$ contains $\mathcal{C}_q$. Also,

$$\begin{aligned}
\mathbb{V}(C) &= abca^{-2}c \\
&\equiv a_2a_3 \cdot a_2a_3 \cdot a_2\gamma_p \cdot a_3^{-2} \cdot a_2\gamma_p \pmod{\mathcal{C}_q} \\
&= a_3^2\gamma_p^{-1}a_3^{-2}\gamma_p \\
&= \gamma_p^{-\hat{\tau}^2+1}
\end{aligned}$$

which generates $\mathcal{C}_p$. Therefore, the subgroup generated by $\mathbb{V}(C)$ is $G'$. So, Factor Group Lemma 1.2.6 applies.

**Case 2.** Assume $a = a_2a_3$ and $b = a_2a_q$.

**Subcase 2.1.** Assume $i = 0$. Then $j \neq 0$ and $c = a_3^j a_q^k \gamma_p$. If $k \neq 0$, then by Lemma 2.4.2(1), $\langle a, c \rangle = G$ which contradicts the minimality of $S$.

So we can assume $k = 0$. We may also assume $j = 1$, by replacing $c$ with $c^{-1}$ if necessary. Then $c = a_3\gamma_p$. Consider $\overline{G} = \mathcal{C}_2 \times \mathcal{C}_3$. Thus, $\overline{a} = a_2a_3$, $\overline{b} = a_2$ and $\overline{c} = a_3$. Therefore, $|\overline{a}| = 6$, $|\overline{b}| = 2$ and $|\overline{c}| = 3$. We have $C = (\overline{a}^2, \overline{b}, \overline{c}, \overline{a}, \overline{c}^{-1})$ as a Hamiltonian cycle in $\mathrm{Cay}(\overline{G}; \overline{S})$. Since there is one occurrence of $b$ in $C$, and it is the only generator of $G$ that contains $a_q$, then by Lemma 2.5.2 we conclude that the subgroup generated by $\mathbb{V}(C)$ contains $\mathcal{C}_q$. Also,

$$\begin{aligned}
\mathbb{V}(C) &= a^2bc^{-1}ac \\
&\equiv a_3^2 \cdot a_2 \cdot a_3\gamma_p \cdot a_2a_3 \cdot \gamma_p^{-1}a_3^{-1} \pmod{\mathcal{C}_q} \\
&= \gamma_p^{-1}a_3\gamma_p^{-1}a_3^{-1}
\end{aligned}$$

$$= \gamma_p^{-1-\hat{\tau}}$$

which generates $\mathcal{C}_p$. Therefore, the subgroup generated by $\mathbb{V}(C)$ is $G'$. So, Factor Group Lemma 1.2.6 applies.

**Subcase 2.2.** Assume $j = 0$. Then $i \neq 0$ and $c = a_2 a_q^k \gamma_p$. If $k \neq 0$, then by Lemma 2.4.2(1), $\langle a, c \rangle = G$ which contradicts the minimality of $S$.

So we can assume $k = 0$. Then $c = a_2\gamma_p$. Consider $\overline{G} = \mathcal{C}_2 \times \mathcal{C}_3$, then $\overline{a} = a_2 a_3$ and $\overline{b} = \overline{c} = a_2$. We have $C = ((\overline{a}, \overline{b})^2, \overline{a}, \overline{c})$ as a Hamiltonian cycle in $\mathrm{Cay}(\overline{G}; \overline{S})$. Since there is one occurrence of $c$ in $C$, and it is the only generator of $G$ that contains $\gamma_p$, then by Lemma 2.5.2 we conclude that the subgroup generated by $\mathbb{V}(C)$ contains $\mathcal{C}_p$. Now we calculate its voltage. Also,

$$\begin{aligned}
\mathbb{V}(C) &= (ab)^2 ac \\
&\equiv (a_2 a_3 \cdot a_2 a_q)^2 \cdot a_2 a_3 \cdot a_2 \pmod{\mathcal{C}_p} \\
&= a_3 a_q a_3 a_q a_3 \\
&= a_q^{\check{\tau} + \check{\tau}^2}.
\end{aligned}$$

which generates $\mathcal{C}_q$. Therefore, the subgroup generated by $\mathbb{V}(C)$ generates $G'$. So, Factor Group Lemma 1.2.6 applies.

**Subcase 2.3.** Assume $i \neq 0$ and $j \neq 0$. If $k \neq 0$, then $c = a_2 a_3^j a_q^k \gamma_p$. Thus, by Lemma 2.4.2(1), $\langle a, c \rangle = G$ which contradicts the minimality of $S$.

So we can assume $k = 0$. We may also assume $j = 1$, by replacing $c$ with $c^{-1}$ if necessary. Then $c = a_2 a_3 \gamma_p$. Consider $\overline{G} = \mathcal{C}_2 \times \mathcal{C}_3$. Thus, $\overline{a} = \overline{c} = a_2 a_3$ and $\overline{b} = a_2$. Therefore, $|\overline{a}| = |\overline{c}| = 6$ and $|\overline{b}| = 2$. We have $C = (\overline{a}, \overline{c}, \overline{b}, \overline{a}^{-2}, \overline{b})$ as a Hamiltonian cycle in $\mathrm{Cay}(\overline{G}; \overline{S})$. Since there is one occurrence of $c$ in $C$, and it is the only generator of $G$ that contains $\gamma_p$, then by Lemma 2.5.2 we conclude that the subgroup generated by $\mathbb{V}(C)$ contains $\mathcal{C}_p$. Also,

$$\begin{aligned}\mathbb{V}(C) &= acba^{-2}b \\ &\equiv a_2a_3 \cdot a_2a_3 \cdot a_2a_q \cdot a_3^{-2} \cdot a_2a_q \pmod{\mathcal{C}_p} \\ &= a_3^2a_qa_3^{-2}a_q \\ &= a_q^{\check{\tau}^2+1}.\end{aligned}$$

Since $\check{\tau}^2 \not\equiv -1 \pmod q$, Factor Group Lemma 1.2.6 applies.

**Case 3.** Assume $a = a_2a_3$ and $b = a_3a_q$.

**Subcase 3.1.** Assume $i \neq 0$ and $j \neq 0$. If $k = 0$, then $c = a_2a_3^j\gamma_p$. Thus, by Lemma 2.4.2(2), $\langle b, c\rangle = G$ which contradicts the minimality of $S$. So we can assume $k \neq 0$. Then $c = a_2a_3^ja_q^k\gamma_p$. Thus, by Lemma 2.4.2(1), $\langle a, c\rangle = G$ which contradicts the minimality of $S$.

**Subcase 3.2.** Assume $i = 0$. Then $j \neq 0$ and $c = a_3^ja_q^k\gamma_p$. If $k \neq 0$, then by Lemma 2.4.2(1), $\langle a, c\rangle = G$ which contradicts the minimality of $S$.

So we can assume $k = 0$. We may also assume $j = 1$, by replacing $c$ with $c^{-1}$ if necessary. Then $c = a_3\gamma_p$. Consider $\overline{G} = \mathcal{C}_2 \times \mathcal{C}_3$, then $\overline{a} = a_2a_3$, $\overline{b} = \overline{c} = a_3$. Therefore, $|\overline{a}| = 6$ and $|\overline{b}| = |\overline{c}| = 3$. We have $C = (\overline{c}, \overline{b}, \overline{a}, \overline{b}^{-2}, \overline{a}^{-1})$ as a Hamiltonian cycle in $\mathrm{Cay}(\overline{G}; \overline{S})$. Since there is one occurrence of $c$ in $C$, and it is the only generator of $G$ that contains $\gamma_p$, then by Lemma 2.5.2 we conclude that the subgroup generated by $\mathbb{V}(C)$ contains $\mathcal{C}_p$. Also,

$$\begin{aligned}\mathbb{V}(C) &= cbab^{-2}a^{-1} \\ &\equiv a_3 \cdot a_3a_q \cdot a_2a_3 \cdot a_q^{-1}a_3^{-1}a_q^{-1}a_3^{-1} \cdot a_3^{-1}a_2 \pmod{\mathcal{C}_p} \\ &= a_3^2a_qa_3a_q^{-1}a_3^{-1}a_q^{-1}a_3^{-2} \\ &= a_q^{\check{\tau}^2-1-\check{\tau}^{-1}}\end{aligned}$$

$$= a_q^{\check{\tau}^2 - 1 - \check{\tau}^2}$$
$$= a_q^{-1}$$

which generates $\mathcal{C}_q$. Therefore, the subgroup generated by $\mathbb{V}(C)$ is $G'$. So, Factor Group Lemma 1.2.6 applies.

**Subcase 3.3.** Assume $j = 0$. Then $i \neq 0$ and $c = a_2 a_q^k \gamma_p$. If $k \neq 0$, then by Lemma 2.4.2(1), $\langle a, c \rangle = G$ which contradicts the minimality of $S$.

So we can assume $k = 0$. Then $c = a_2 \gamma_p$. Consider $\overline{G} = \mathcal{C}_2 \times \mathcal{C}_3$, then $\overline{a} = a_2 a_3$, $\overline{b} = a_3$ and $\overline{c} = a_2$. Therefore, $|\overline{a}| = 6$, $|\overline{b}| = 3$ and $|\overline{c}| = 2$. We have $C = (\overline{a}, \overline{c}, \overline{b}, \overline{a}, \overline{b}^{-1}, \overline{a})$ as a Hamiltonian cycle in $\mathrm{Cay}(\overline{G}; \overline{S})$. Since there is one occurrence of $c$ in $C$, and it is the only generator of $G$ that contains $\gamma_p$, then by Lemma 2.5.2 we conclude that the subgroup generated by $\mathbb{V}(C)$ contains $\mathcal{C}_p$. Also,

$$\begin{aligned}
\mathbb{V}(C) &= acbab^{-1}a \\
&\equiv a_2 a_3 \cdot a_2 \cdot a_3 a_q \cdot a_2 a_3 \cdot a_q^{-1} a_3^{-1} \cdot a_2 a_3 \pmod{\mathcal{C}_p} \\
&= a_3^2 a_q a_3 a_q^{-1} \\
&= a_q^{\check{\tau}^2 - 1}.
\end{aligned}$$

Since $\check{\tau}^2 \not\equiv 1 \pmod{q}$, Factor Group Lemma 1.2.6 applies.

**Case 4.** Assume $a = a_3$ and $b = a_2 a_q$.

**Subcase 4.1.** Assume $i = 0$. Then $j \neq 0$ and $c = a_3^j a_q^k \gamma_p$. Thus, the argument in Subcase 1.1 of Proposition 3.5 applies.

**Subcase 4.2.** Assume $j = 0$. Then $i \neq 0$ and $c = a_2 a_q^k \gamma_p$. Thus, the argument in Subcase 1.2 of Proposition 3.5 applies.

**Subcase 4.3.** Assume $i \neq 0$ and $j \neq 0$. Then $c = a_2 a_3^j a_q^k \gamma_p$. If $k \neq 0$, then by Lemma 2.4.2(3) $\langle a, c \rangle = G$ which contradicts the minimality of $S$.

So we can assume $k = 0$. We may also assume $j = 1$, by replacing $c$ with $c^{-1}$ if necessary. Then $c = a_2 a_3 \gamma_p$. Consider $\overline{G} = \mathcal{C}_2 \times \mathcal{C}_3$. Then we have $\overline{a} = a_3$, $\overline{b} = a_2$ and $\overline{c} = a_2 a_3$. This implies that $|\overline{a}| = 3$, $|\overline{b}| = 2$ and $|\overline{c}| = 6$. We have $C = (\overline{c}, \overline{b}, \overline{a}, \overline{c}, \overline{a}^{-1}, \overline{c})$ as a Hamiltonian cycle in $\mathrm{Cay}(\overline{G}; \overline{S})$. Since there is one occurrence of $b$ in $C$, and it is the only generator of $G$ that contains $a_q$, then by Lemma 2.5.2 we conclude that the subgroup generated by $\mathbb{V}(C)$ contains $\mathcal{C}_q$. Also, since $a_2$ inverts $\mathcal{C}_p$

$$\begin{aligned}
\mathbb{V}(C) &= cbaca^{-1}c \\
&\equiv a_2 a_3 \gamma_p \cdot a_2 \cdot a_3 \cdot a_2 a_3 \gamma_p \cdot a_3^{-1} \cdot a_2 a_3 \gamma_p \pmod{\mathcal{C}_q} \\
&= a_3 \gamma_p^{-1} a_3^2 \\
&= \gamma_p^{-\hat{\tau}}
\end{aligned}$$

which generates $\mathcal{C}_p$. Therefore, the subgroup generated by $\mathbb{V}(C)$ is $G'$. So, Factor Group Lemma 1.2.6 applies. $\square$

## 3.7 Assume $|S| = 3$, $G' = \mathcal{C}_p \times \mathcal{C}_q$ and $C_{G'}(\mathcal{C}_2) = \{e\}$

In this section we prove the part of Theorem 1.1.3 where, $|S| = 3$, $G' = \mathcal{C}_p \times \mathcal{C}_q$, $C_{G'}(\mathcal{C}_2) = \{e\}$, and neither $C_{G'}(\mathcal{C}_3) \neq \{e\}$ nor $\widehat{S}$ is minimal holds. Recall $\overline{G} = G/G'$, $\breve{G} = G/\mathcal{C}_q$ and $\widehat{G} = G/\mathcal{C}_p$.

**Proposition 3.7.** *Assume*

- $G = (\mathcal{C}_2 \times \mathcal{C}_3) \ltimes (\mathcal{C}_p \times \mathcal{C}_q)$,
- $|S| = 3$,
- $C_{G'}(\mathcal{C}_2) = \{e\}$.

*Then* $\mathrm{Cay}(G; S)$ *contains a Hamiltonian cycle.*

*Proof.* Let $S = \{a, b, c\}$. If $C_{G'}(\mathcal{C}_3) \neq \{e\}$, then Proposition 3.3 applies. So we may assume $C_{G'}(\mathcal{C}_3) = \{e\}$. Now if $\widehat{S}$ is minimal, then Proposition 3.4 applies. So we may assume $\widehat{S}$ is not minimal. Consider

$$\widehat{G} = G/\mathcal{C}_p = (\mathcal{C}_2 \times \mathcal{C}_3) \ltimes \mathcal{C}_q.$$

Choose a 2-element subset $\{a, b\}$ in $S$ that generates $\widehat{G}$. From the minimality of $S$, we see

$$\langle a, b \rangle = (\mathcal{C}_2 \times \mathcal{C}_3) \ltimes \mathcal{C}_q.$$

after replacing $a$ and $b$ by conjugates. We may assume $|a| \geqslant |b|$ and (by conjugating if necessary) $a$ is in $\mathcal{C}_2 \times \mathcal{C}_3$. Then the projection of $(a, b)$ to $\mathcal{C}_2 \times \mathcal{C}_3$ is one of the following forms after replacing $a$ and $b$ with their inverses if necessary.

- $(a_2 a_3, a_2 a_3)$,
- $(a_2 a_3, a_2)$,
- $(a_2 a_3, a_3)$,
- $(a_3, a_2)$.

There are four possibilities for $(a, b)$:

1. $(a_2 a_3, a_2 a_3 a_q)$,
2. $(a_2 a_3, a_2 a_q)$,
3. $(a_2 a_3, a_3 a_q)$,
4. $(a_3, a_2 a_q)$.

Let $c$ be the third element of $S$. We may write $c = a_2^i a_3^j a_q^k \gamma_p$ with $0 \leqslant i \leqslant 1$, $0 \leqslant j \leqslant 2$ and $0 \leqslant k \leqslant q-1$. Note since $S \cap G' = \varnothing$, we know that $i$ and $j$ cannot both be equal to 0. Additionally, we have $a_3 \gamma_p a_3^{-1} = \gamma_p^{\widehat{\tau}}$ where $\widehat{\tau}^3 \equiv 1 \pmod{p}$ and $\widehat{\tau} \not\equiv 1 \pmod{p}$. Thus $\widehat{\tau}^2 + \widehat{\tau} + 1 \equiv 0 \pmod{p}$. Note that this implies $\widehat{\tau} \not\equiv -1 \pmod{p}$. We have $a_3 a_q a_3^{-1} = a_q^{\check{\tau}}$. By using the same argument we can conclude that $\check{\tau} \not\equiv 1 \pmod{q}$ and $\check{\tau}^2 + \check{\tau} + 1 \equiv 0 \pmod{q}$. Note that this implies $\check{\tau} \not\equiv -1 \pmod{q}$. Therefore, we conclude that $\widehat{\tau}^2 \not\equiv \pm 1 \pmod{p}$, and $\check{\tau}^2 \not\equiv \pm 1 \pmod{q}$.

**Case 1.** Assume $a = a_2a_3$ and $b = a_2a_3a_q$. If $k \neq 0$, then by Lemma 2.4.2(1) $\langle a, c\rangle = G$ which contradicts the minimality of $S$. So we can assume $k = 0$. Now if $j \neq 0$, then by Lemma 2.4.2(4), $\langle b, c\rangle = G$ which contradicts the minimality of $S$. Therefore, we may assume $j = 0$. Then $i \neq 0$ and $c = a_2\gamma_p$. We have $\langle \overline{b}, \overline{c}\rangle = \langle \overline{a}_2\overline{a}_3, \overline{a}_2\rangle = \overline{G}$. Consider $\{\check{b}, \check{c}\} = \{a_2a_3, a_2\gamma_p\}$. Therefore,

$$[a_2a_3, a_2\gamma_p] = a_2a_3a_2\gamma_p a_3^{-1}a_2\gamma_p^{-1}a_2 = a_3\gamma_p a_3^{-1}\gamma_p = \gamma_p^{\widehat{\tau}+1}.$$

which generates $\mathcal{C}_p$. Now consider $\{\widehat{b}, \widehat{c}\} = \{a_2a_3a_q, a_2\}$, then

$$[a_2a_3a_q, a_2] = a_2a_3a_qa_2a_q^{-1}a_3^{-1}a_2a_2 = a_3a_q^{-2}a_3^{-1} = a_q^{-2\check{\tau}}$$

which generates $\mathcal{C}_q$. Therefore, $\langle b, c\rangle = G$ which contradicts the minimality of $S$.

**Case 2.** Assume $a = a_2a_3$ and $b = a_2a_q$. If $k \neq 0$, then by Lemma 2.4.2(1), $\langle a, c\rangle = G$ which contradicts the minimality of $S$. So we can assume $k = 0$.

**Subcase 2.1.** Assume $j \neq 0$. We may also assume $j = 1$, by replacing $c$ with $c^{-1}$ if necessary. Then $c = a_2^ia_3\gamma_p$. We have $\langle \overline{b}, \overline{c}\rangle = \langle \overline{a}_2, \overline{a}_2^i\overline{a}_3\rangle = \overline{G}$. Consider $\{\widehat{b}, \widehat{c}\} = \{a_2a_q, a_2^ia_3\}$. We have

$$\begin{aligned}[a_2a_q, a_2^ia_3] &= a_2a_qa_2^ia_3a_q^{-1}a_2a_3^{-1}a_2^i = a_q^{-1}a_2^{i+1}a_3a_q^{-1}a_3^{-1}a_2^{i+1}\\ &= a_q^{-1}a_3a_q^{\mp 1}a_3^{-1} = a_q^{-1\mp\check{\tau}}\end{aligned}$$

which generates $\mathcal{C}_q$. Now consider $\{\check{b}, \check{c}\} = \{a_2, a_2^ia_3\gamma_p\}$. We have

$$[a_2, a_2^ia_3\gamma_p] = a_2a_2^ia_3\gamma_pa_2\gamma_p^{-1}a_3^{-1}a_2^i = a_2^{i+1}a_3\gamma_p^2a_3^{-1}a_2^{i+1} = \gamma_p^{\pm 2\widehat{\tau}}$$

which generates $\mathcal{C}_p$. Therefore, $\langle b, c\rangle = G$ which contradicts the minimality of $S$.

**Subcase 2.2.** Assume $j = 0$. Then $i \neq 0$ and $c = a_2\gamma_p$. Consider $\overline{G} = \mathcal{C}_2 \times \mathcal{C}_3$, then $\overline{a} = a_2a_3$ and $\overline{b} = \overline{c} = a_2$. Thus, $|\overline{a}| = 6$ and $|\overline{b}| = |\overline{c}| = 2$. We have $C = ((\overline{a}, \overline{b})^2, \overline{a}, \overline{c})$ as a Hamiltonian cycle in $\mathrm{Cay}(\overline{G}; \overline{S})$. Since there is one occurrence of $c$ in $C$, and it is the only generator of $G$ that contains $\gamma_p$, then by Lemma 2.5.2 we conclude that the subgroup generated by $\mathbb{V}(C)$ contains $\mathcal{C}_p$. Also,

$$\begin{aligned}
\mathbb{V}(C) &= (ab)^2(ac) \\
&\equiv a_2a_3 \cdot a_2a_q \cdot a_2a_3 \cdot a_2a_q \cdot a_2a_3 \cdot a_2 \pmod{\mathcal{C}_p} \\
&= a_3a_qa_3a_qa_3 \\
&= a_q^{\check{\tau}+\check{\tau}^2}
\end{aligned}$$

which generates $\mathcal{C}_q$. Therefore, the subgroup generated by $\mathbb{V}(C)$ is $G'$. So, Factor Group Lemma 1.2.6 applies.

**Case 3.** Assume $a = a_2a_3$ and $b = a_3a_q$. If $k \neq 0$, then by Lemma 2.4.2(1), $\langle a, c\rangle = G$ which contradicts the minimality of $S$. So we can assume $k = 0$.

**Subcase 3.1.** Assume $i \neq 0$ and $j \neq 0$. Then $c = a_2a_3^j\gamma_p$. Thus, by Lemma 2.4.2(2), $\langle b, c\rangle = G$ which contradicts the minimality of $S$.

**Subcase 3.2.** Assume $j = 0$. Then $i \neq 0$ and $c = a_2\gamma_p$. We have $\langle \overline{b}, \overline{c}\rangle = \langle \overline{a}_3, \overline{a}_2\rangle = \overline{G}$. Consider $\{\check{b}, \check{c}\} = \{a_3, a_2\gamma_p\}$. Then we have

$$[a_3, a_2\gamma_p] = a_3a_2\gamma_pa_3^{-1}\gamma_p^{-1}a_2 = a_3\gamma_p^{-1}a_3^{-1}\gamma_p = \gamma_p^{-\hat{\tau}+1}$$

which generates $\mathcal{C}_p$. Now consider $\{\widehat{b}, \widehat{c}\} = \{a_3a_q, a_2\}$. Thus,

$$[a_3a_q, a_2] = a_3a_qa_2a_q^{-1}a_3^{-1}a_2 = a_3a_q^2a_3^{-1} = a_q^{2\check{\tau}}$$

which generates $\mathcal{C}_q$. Therefore, $\langle b, c\rangle = G$ which contradicts the minimality of $S$.

**Subcase 3.3.** Assume $i = 0$. Then $j \neq 0$. We may also assume $j = 1$, by replacing $c$ with $c^{-1}$ if necessary. Then $c = a_3\gamma_p$. Consider $\overline{G} = \mathcal{C}_2 \times \mathcal{C}_3$, then we have $\overline{a} = a_2a_3$, $\overline{b} = \overline{c} = a_3$. Thus, $|\overline{a}| = 6$ and $|\overline{b}| = |\overline{c}| = 3$. We have $C = (\overline{c}, \overline{b}, \overline{a}, \overline{b}^{-2}, \overline{a}^{-1})$ as a Hamiltonian cycle in $\mathrm{Cay}(\overline{G}; \overline{S})$. Since there is one occurrence of $c$ in $C$, and it is the only generator of $G$ that contains $\gamma_p$, then by Lemma 2.5.2 we conclude that the subgroup generated by $\mathbb{V}(C)$ contains $\mathcal{C}_p$. Also,

$$\begin{aligned}
\mathbb{V}(C) &= cbab^{-2}a^{-1} \\
&\equiv a_3 \cdot a_3a_q \cdot a_2a_3 \cdot a_q^{-1}a_3^{-1}a_q^{-1}a_3^{-1} \cdot a_3^{-1}a_2 \pmod{\mathcal{C}_p} \\
&= a_3^2a_qa_3a_qa_3^{-1}a_qa_3^{-2} \\
&= a_q^{\check{\tau}^2+1+\check{\tau}^{-1}} \\
&= a_q^{\check{\tau}^2+1-\check{\tau}^2} \\
&= a_q
\end{aligned}$$

which generates $\mathcal{C}_q$. Therefore, the subgroup generated by $\mathbb{V}(C)$ is $G'$. So, Factor Group Lemma 1.2.6 applies.

**Case 4.** Assume $a = a_3$ and $b = a_2a_q$.

**Subcase 4.1.** Assume $i = 0$. Then $j \neq 0$. We may also assume $j = 1$, by replacing $c$ with $c^{-1}$ if necessary. Then $c = a_3a_q^k\gamma_p$. Consider $\overline{G} = \mathcal{C}_2 \times \mathcal{C}_3$. Then we have $\overline{a} = \overline{c} = a_3$ and $\overline{b} = a_2$. This implies that $|\overline{a}| = |\overline{c}| = 3$ and $|\overline{b}| = 2$. We have $C = (\overline{c}^{-2}, \overline{b}, \overline{a}^2, \overline{b})$ as a Hamiltonian cycle in $\mathrm{Cay}(\overline{G}; \overline{S})$. Now we calculate its voltage.

$$\begin{aligned}
\mathbb{V}(C) &= c^{-2}ba^2b \\
&\equiv \gamma_p^{-1}a_3^{-1}\gamma_p^{-1}a_3^{-1} \cdot a_2 \cdot a_3^2 \cdot a_2 \pmod{\mathcal{C}_q} \\
&= \gamma_p^{-1}a_3^{-1}\gamma_p^{-1}a_3 \\
&= \gamma_p^{-1-\hat{\tau}^{-1}}
\end{aligned}$$

which generates $\mathcal{C}_p$. Also

$$\begin{aligned}
\mathbb{V}(C) &= c^{-2}ba^2b \\
&\equiv a_q^{-k}a_3^{-1}a_q^{-k}a_3^{-1} \cdot a_2a_q \cdot a_3^2 \cdot a_2a_q \pmod{\mathcal{C}_p} \\
&= a_q^{-k}a_3^{-1}a_q^{-k}a_3^{-1}a_q^{-1}a_3^2a_q \\
&= a_q^{-k-k\breve{\tau}^{-1}-\breve{\tau}^{-2}+1}.
\end{aligned}$$

If $k = 2$, then

$$a_q^{-k-k\breve{\tau}^{-1}-\breve{\tau}^{-2}+1} = a_q^{-2-2\breve{\tau}^{-1}-\breve{\tau}^{-2}+1} = a_q^{-(\breve{\tau}^{-1}+1)^2}$$

which generates $\mathcal{C}_q$. So we may assume $k \neq 2$ and the subgroup generated by $\mathbb{V}(C)$ does not contain $\mathcal{C}_q$, for otherwise Factor Group Lemma 1.2.6 applies. Therefore,

$$\begin{aligned}
0 &\equiv -k - k\breve{\tau}^{-1} - \breve{\tau}^{-2} + 1 \pmod{q} \\
&= (1-k) - k\breve{\tau}^{-1} - \breve{\tau}^{-2}.
\end{aligned}$$

Multiplying by $\breve{\tau}^2$, we have

$$0 \equiv (1-k)\breve{\tau}^2 - k\breve{\tau} - 1 \pmod{q}. \tag{4.1A}$$

We can replace $\breve{\tau}$ with $\breve{\tau}^{-1}$ in the above equation, by replacing $a_3$,$a$ and $c$ with their inverses.

$$0 \equiv (1-k)\breve{\tau}^{-2} - k\breve{\tau}^{-1} - 1 \pmod{q}.$$

Multiplying by $\breve{\tau}^2$, then

$$0 \equiv (1-k) - k\breve{\tau} - \breve{\tau}^2 \pmod{q}.$$

By subtracting 4.1A from the above equation, we have

$$0 \equiv (k-2)\check{\tau}^2 + (2-k) \pmod{q}.$$

This implies that $\check{\tau}^2 \equiv 1 \pmod{q}$, a contradiction.

**Subcase 4.2.** Assume $j = 0$. Then $i \neq 0$. If $k \neq 0$, then $c = a_2 a_q^k \gamma_p$. Thus, by Lemma 2.4.2(3), $\langle a, c \rangle = G$ which contradicts the minimality of $S$. So we can assume $k = 0$. Then $c = a_2\gamma_p$. Consider $\overline{G} = \mathcal{C}_2 \times \mathcal{C}_3$, then $\overline{a} = a_3$ and $\overline{b} = \overline{c} = a_2$. We have $C = (\overline{a}^2, \overline{b}, \overline{a}^{-2}, \overline{c})$ as a Hamiltonian cycle in $\mathrm{Cay}(\overline{G}; \overline{S})$. Since there is one occurrence of $c$ in $C$, and it is the only generator of $G$ that contains $\gamma_p$, then by Lemma 2.5.2 we conclude that the subgroup generated by $\mathbb{V}(C)$ contains $\mathcal{C}_p$. Similarly, since there is one occurrence of $b$ in $C$, and it is the only generator of $G$ that contains $a_q$, then by Lemma 2.5.2 we conclude that the subgroup generated by $\mathbb{V}(C)$ contains $\mathcal{C}_q$. Therefore, the subgroup generated by $\mathbb{V}(C)$ is $G'$. So, Factor Group Lemma 1.2.6 applies.

**Subcase 4.3.** Assume $i \neq 0$ and $j \neq 0$. If $k \neq 0$, then $c = a_2 a_3^j a_q^k \gamma_p$. Thus, by Lemma 2.4.2(3), $\langle a, c \rangle = G$ which contradicts the minimality of $S$. So we can assume $k = 0$. We may also assume $j = 1$, by replacing $c$ with $c^{-1}$ if necessary. Then $c = a_2 a_3 \gamma_p$. We have $\langle \overline{b}, \overline{c} \rangle = \langle \overline{a}_2, \overline{a}_2\overline{a}_3 \rangle = \overline{G}$. Consider $\{\widehat{b}, \widehat{c}\} = \{a_2 a_q, a_2 a_3\}$. Then we have

$$[a_2 a_q, a_2 a_3] = a_2 a_q a_2 a_3 a_q^{-1} a_2 a_3^{-1} a_2 = a_q^{-1} a_3 a_q^{-1} a_3^{-1} = a_q^{-1-\check{\tau}}$$

which generates $\mathcal{C}_q$. Now consider $\{\check{b}, \check{c}\} = \{a_2, a_2 a_3 \gamma_p\}$. Then

$$[a_2, a_2 a_3 \gamma_p] = a_2 a_2 a_3 \gamma_p a_2 \gamma_p^{-1} a_3^{-1} a_2 = a_3 \gamma_p^2 a_3^{-1} = \gamma_p^{2\hat{\tau}}$$

which generates $\mathcal{C}_p$. Therefore, $\langle b, c \rangle = G$ which contradicts the minimality of $S$. $\square$

## 3.8 Assume $|S| = 3$ and $G' = \mathcal{C}_3 \times \mathcal{C}_p$

In this section we prove the part of Theorem 1.1.3 where, $|S| = 3$ and $G' = \mathcal{C}_3 \times \mathcal{C}_p$. Recall $\overline{G} = G/G'$, $\widehat{G} = G/\mathcal{C}_p$ and $\widehat{G} = G/\mathcal{C}_3$.

**Proposition 3.8.** *Assume*

- $G = (\mathcal{C}_2 \times \mathcal{C}_q) \ltimes (\mathcal{C}_3 \times \mathcal{C}_p)$,
- $|S| = 3$.

*Then* $\mathrm{Cay}(G; S)$ *contains a Hamiltonian cycle.*

*Proof.* Let $S = \{a, b, c\}$. Since $\mathcal{C}_q$ centralizes $\mathcal{C}_3$ and $Z(G) \cap G' = \{e\}$ (by Proposition 1.3.12(2)), then $\mathcal{C}_2$ inverts $\mathcal{C}_3$. Now if $\widehat{S}$ is minimal, then Lemma 2.3.5 applies. So we may assume $\widehat{S}$ is not minimal. Consider

$$\widehat{G} = G/\mathcal{C}_p = (\mathcal{C}_2 \times \mathcal{C}_q) \ltimes \mathcal{C}_3.$$

Choose a 2-element subset $\{a, b\}$ in $S$ that generates $\widehat{G}$. From the minimality of $S$ we see

$$\langle a, b \rangle = (\mathcal{C}_2 \times \mathcal{C}_q) \ltimes \mathcal{C}_3.$$

after replacing $a$ and $b$ with conjugates. Then the projection of $(a, b)$ to $\mathcal{C}_2 \times \mathcal{C}_q$ has one of the following forms:

- $(a_2 a_q, a_2 a_q^m)$, where $1 \leqslant m \leqslant q - 1$,
- $(a_2 a_q, a_2)$,
- $(a_2 a_q, a_q^m)$, where $1 \leqslant m \leqslant q - 1$,
- $(a_2, a_q)$.

Thus, there are four different possibilities for $(a, b)$ after assuming, without loss of generality, that $a \in \mathcal{C}_2 \times \mathcal{C}_q$:

1. $(a_2 a_q, a_2 a_q^m a_3)$,

2. $(a_2a_q, a_2a_3)$,
3. $(a_2a_q, a_q^m a_3)$,
4. $(a_2, a_qa_3)$.

Let $c$ be the third element of $S$. We may write $c = a_2^i a_q^j a_3^k \gamma_p$ with $0 \leqslant i \leqslant 1$, $0 \leqslant j \leqslant q-1$ and $0 \leqslant k \leqslant 2$. Since $\mathcal{C}_q$ centralizes $\mathcal{C}_3$, we may assume $\mathcal{C}_q$ does not centralize $\mathcal{C}_p$, for otherwise Lemma 2.3.7 applies. Now we have $a_q\gamma_p a_q^{-1} = \gamma_p^{\widehat{\tau}}$, where $\widehat{\tau}^q \equiv 1 \pmod p$. We also have $\widehat{\tau} \not\equiv 1 \pmod p$. Since $\widehat{\tau}^q \equiv 1 \pmod p$, this implies

$$\widehat{\tau}^{q-1} + \widehat{\tau}^{q-2} + \cdots + 1 \equiv 0 \pmod p.$$

Note that this implies $\widehat{\tau} \not\equiv -1 \pmod p$.

**Case 1.** Assume $a = a_2a_q$ and $b = a_2a_q^m a_3$. If $k \neq 0$, then by Lemma 2.4.3(1) $\langle a, c\rangle = G$ which contradicts the minimality of $S$. So we can assume $k = 0$. Now if $i \neq 0$, then by Lemma 2.4.3(3) $\langle b, c\rangle = G$ which contradicts the minimality of $S$. Therefore, we may assume $i = 0$. Then $j \neq 0$ and $c = a_q^j\gamma_p$.

Consider $\overline{G} = \mathcal{C}_2 \times \mathcal{C}_q$. Then we have $\overline{a} = a_2a_q$, $\overline{b} = a_2a_q^m$ and $\overline{c} = a_q^j$. We may assume $m$ is odd by replacing $b$ with $b^{-1}$ (and $m$ with $q-m$) if necessary. Note that this implies $\overline{b} = \overline{a}^m$. Also, we have $|\overline{a}| = |\overline{b}| = 2q$ and $|\overline{c}| = q$.

**Subcase 1.1.** Assume $m = 1$. Then $\overline{a} = \overline{b}$. We have

$$C = (\overline{c}^{q-1}, \overline{b}, \overline{c}^{-(q-1)}, \overline{a}^{-1})$$

as a Hamiltonian cycle in $\mathrm{Cay}(\overline{G}; \overline{S})$. Since there is one occurrence of $b$ in $C$, and it is the only generator of $G$ that contains $a_3$, then by Lemma 2.5.2 we conclude that the subgroup generated by $\mathbb{V}(C)$ contains $\mathcal{C}_3$. Now by considering the fact that $\mathcal{C}_2$ might centralize $\mathcal{C}_p$ or not we have

$$\begin{aligned}
\mathbb{V}(C) &= c^{q-1} b c^{-(q-1)} a^{-1} \\
&\equiv (a_q^j \gamma_p)^{q-1} \cdot a_2 a_q \cdot (a_q^j \gamma_p)^{-(q-1)} \cdot a_q^{-1} a_2 \pmod{\mathcal{C}_3} \\
&= \gamma_p^{\widehat{\tau}^j + \widehat{\tau}^{2j} + \cdots + \widehat{\tau}^{(q-1)j}} a_q^{(q-1)j} a_2 a_q a_q^{-(q-1)j} \gamma_p^{-(\widehat{\tau}^j + \widehat{\tau}^{2j} + \cdots + \widehat{\tau}^{(q-1)j})} a_q^{-1} a_2 \\
&= \gamma_p^{\widehat{\tau}^j (1 + \widehat{\tau}^j + \cdots + \widehat{\tau}^{(q-2)j})} a_q \gamma_p^{\mp \widehat{\tau}^j (1 + \widehat{\tau}^j + \cdots + \widehat{\tau}^{(q-2)j})} a_q^{-1}.
\end{aligned}$$

Now if $\widehat{\tau}^j \not\equiv 1 \pmod{p}$, then

$$\begin{aligned}
\mathbb{V}(C) &= \gamma_p^{\widehat{\tau}^j (1 + \widehat{\tau}^j + \cdots + \widehat{\tau}^{(q-2)j})} a_q \gamma_p^{\mp \widehat{\tau}^j (1 + \widehat{\tau}^j + \cdots + \widehat{\tau}^{(q-2)j})} a_q^{-1} \\
&= \gamma_p^{\widehat{\tau}^j ((\widehat{\tau}^j)^{q-1} - 1)/(\widehat{\tau}^j - 1) \mp \widehat{\tau}^{j+1} ((\widehat{\tau}^j)^{q-1} - 1)/(\widehat{\tau}^j - 1)} \\
&= \gamma_p^{\widehat{\tau}^j ((\widehat{\tau}^{-j}) - 1)/(\widehat{\tau}^j - 1) \mp \widehat{\tau}^{j+1} ((\widehat{\tau}^{-j}) - 1)/(\widehat{\tau}^j - 1)} \\
&= \gamma_p^{(1 - \widehat{\tau}^j)(1 \mp \widehat{\tau})/(\widehat{\tau}^j - 1)} \\
&= \gamma_p^{-(1 \mp \widehat{\tau})}.
\end{aligned}$$

We may assume this does not generate $\mathcal{C}_p$, for otherwise Factor Group Lemma 1.2.6 applies. Therefore, $\widehat{\tau}^j \equiv 1 \pmod{p}$ or $\widehat{\tau} \equiv \pm 1 \pmod{p}$. The second case is impossible. So we must have $\widehat{\tau}^j \equiv 1 \pmod{p}$. We also know that $\widehat{\tau}^q \equiv 1 \pmod{p}$. So $\widehat{\tau}^d \equiv 1 \pmod{p}$, where $d = \gcd(j, q)$. Since $1 \leqslant j \leqslant q - 1$, then $d = 1$, which contradicts the fact that $\widehat{\tau} \not\equiv 1 \pmod{p}$.

**Subcase 1.2.** Assume $m \neq 1$ and $j = 2$. Then $c = a_q^2 \gamma_p$. We have

$$C = (\overline{b}, \overline{c}^{-(m-1)/2}, \overline{a}, \overline{c}^{(m-1)/2}, \overline{a}^{2q-m-1})$$

as a Hamiltonian cycle in $\mathrm{Cay}(\overline{G}; \overline{S})$. Since there is one occurrence of $b$ in $C$, and it is the only generator of $G$ that contains $a_3$, then by Lemma 2.5.2 we conclude that the subgroup generated by $\mathbb{V}(C)$ contains $\mathcal{C}_3$. Considering the fact that $\mathcal{C}_2$ might centralize $\mathcal{C}_p$ or not we have

$$\begin{aligned}
\mathbb{V}(C) &= bc^{-(m-1)/2}ac^{(m-1)/2}a^{2q-m-1} \\
&\equiv a_2a_q^m \cdot (a_q^2\gamma_p)^{-(m-1)/2} \cdot a_2a_q \cdot (a_q^2\gamma_p)^{(m-1)/2} \cdot a_q^{2q-m-1} \pmod{\mathcal{C}_3} \\
&= a_2a_q^m(\gamma_p^{\hat{\tau}^2+(\hat{\tau}^2)^2+\cdots+(\hat{\tau}^2)^{(m-1)/2}}a_q^{(m-1)})^{-1}a_2a_q(\gamma_p^{\hat{\tau}^2+(\hat{\tau}^2)^2+\cdots+(\hat{\tau}^2)^{(m-1)/2}}a_q^{(m-1)})a_q^{-m-1} \\
&= a_2a_q^m a_q^{-m+1}\gamma_p^{-\hat{\tau}^2(1+\hat{\tau}^2+\cdots+(\hat{\tau}^2)^{(m-3)/2})}a_2a_q\gamma_p^{\hat{\tau}^2(1+\hat{\tau}^2+\cdots+(\hat{\tau}^2)^{(m-3)/2})}a_q^{-2} \\
&= a_q\gamma_p^{\pm\hat{\tau}^2(1+\hat{\tau}^2+\cdots+\hat{\tau}^2)^{(m-3)/2}}a_q\gamma_p^{\hat{\tau}^2(1+\hat{\tau}^2+\cdots+\hat{\tau}^2)^{(m-3)/2}}a_q^{-2} \\
&= \gamma_p^{\pm\hat{\tau}^3(\hat{\tau}^{m-1}-1)/(\hat{\tau}^2-1)+\hat{\tau}^4(\hat{\tau}^{m-1}-1)/(\hat{\tau}^2-1)} \\
&= \gamma_p^{\hat{\tau}^3(\hat{\tau}^{m-1}-1)(\pm1+\hat{\tau})/(\hat{\tau}^2-1)}.
\end{aligned}$$

We may assume this does not generate $\mathcal{C}_p$, for otherwise Factor Group Lemma 1.2.6 applies. Therefore, $\hat{\tau}^{m-1} \equiv 1 \pmod{p}$. We also know that $\hat{\tau}^q \equiv 1 \pmod{p}$. So $\hat{\tau}^d \equiv 1 \pmod{p}$, where $d = \gcd(m-1, q)$. Since $2 \leqslant m \leqslant q-1$, then $d = 1$, which contradicts the fact that $\hat{\tau} \not\equiv 1 \pmod{p}$.

**Subcase 1.3.** Assume $m \neq 1$ and $j \neq 2$. We may also assume $j$ is an even number, by replacing $c$ with its inverse and $j$ with $q - j$ if necessary. This implies that $\overline{c} = \overline{a}^j$. We have

$$C = (\overline{b}, \overline{c}, \overline{a}, \overline{c}^{-1}, \overline{b}^{-1}, \overline{a}^{m-2}, \overline{c}, \overline{a}^{-(j-3)}, \overline{c}, \overline{a}^{2q-m-j-2})$$

as a Hamiltonian cycle in $\mathrm{Cay}(\overline{G}; \overline{S})$. Now we calculate its voltage.

$$\begin{aligned}
\mathbb{V}(C) &= bcac^{-1}b^{-1}a^{m-2}ca^{-(j-3)}ca^{2q-m-j-2} \\
&\equiv a_2a_3 \cdot a_2 \cdot a_3^{-1}a_2 \cdot a_2^{m-2} \cdot a_2^{-(j-3)} \cdot a_2^{2q-m-j-2} \pmod{\mathcal{C}_q \ltimes \mathcal{C}_p} \\
&= a_2a_3a_2a_3^{-1} \\
&= a_3^{-2}
\end{aligned}$$

which generates $\mathcal{C}_3$. Also considering the fact that $\mathcal{C}_2$ might centralize $\mathcal{C}_p$ or not we have

$$\begin{aligned}
\mathbb{V}(C) &= bcac^{-1}b^{-1}a^{m-2}ca^{-(j-3)}ca^{2q-m-j-2} \\
&\equiv a_2 a_q^m \cdot a_q^j \gamma_p \cdot a_2 a_q \cdot \gamma_p^{-1} a_q^{-j} \cdot a_q^{-m} a_2 \\
&\qquad \cdot a_2 a_q^{m-2} \cdot a_q^j \gamma_p \cdot a_q^{-j+3} a_2 \cdot a_q^j \gamma_p \cdot a_2 a_q^{2q-m-j-2} \pmod{\mathcal{C}_3} \\
&= a_q^{m+j} \gamma_p^{\pm 1} a_q \gamma_p^{-1} a_q^{-2} \gamma_p a_q^3 \gamma_p^{\pm 1} a_q^{-m-j-2} \\
&= \gamma_p^{\pm \widehat{\tau}^{m+j} - \widehat{\tau}^{m+j+1} + \widehat{\tau}^{m+j-1} \pm \widehat{\tau}^{m+j+2}} \\
&= \gamma_p^{\widehat{\tau}^{m+j-1}(\pm \widehat{\tau}^3 - \widehat{\tau}^2 \pm \widehat{\tau} + 1)}.
\end{aligned}$$

So we may assume this does not generate $\mathcal{C}_p$, for otherwise Factor Group Lemma 1.2.6 applies. Then we have

$$0 \equiv \pm \widehat{\tau}^3 - \widehat{\tau}^2 \pm \widehat{\tau} + 1 \pmod{p}.$$

Let $t = \widehat{\tau}$ if $\mathcal{C}_2$ centralizes $\mathcal{C}_p$ and $t = -\widehat{\tau}$ if $\mathcal{C}_2$ inverts $\mathcal{C}_p$. Then

$$0 \equiv t^3 - t^2 + t + 1 \pmod{p}. \tag{1.3A}$$

We can replace $t$ with $t^{-1}$ in the above equation after replacing $\{a, b, c\}$ with their inverses, then

$$0 \equiv t^{-3} - t^{-2} + t^{-1} + 1 \pmod{p}.$$

Multiplying by $t^3$, we have

$$\begin{aligned}
0 &\equiv 1 - t + t^2 + t^3 \pmod{p} \\
&= t^3 + t^2 - t + 1.
\end{aligned}$$

By subtracting 1.3A from the above equation, we have

$$\begin{aligned} 0 &\equiv 2t^2 - 2t \pmod{p} \\ &= 2t(t-1) \end{aligned}$$

This implies that $t \equiv 1 \pmod{p}$ which contradicts the fact that $\widehat{\tau} \not\equiv \pm 1 \pmod{p}$.

**Case 2.** Assume $a = a_2 a_q$ and $b = a_2 a_3$. If $k \neq 0$, then by Lemma 2.4.3(1) $\langle a, c \rangle = G$ which contradicts the minimality of $S$. So we can assume $k = 0$.

**Subcase 2.1.** Assume $i = 0$. Then $j \neq 0$ and $c = a_q^j \gamma_p$. We may assume $j$ is an odd number, by replacing $c$ with its inverse and $j$ with $q - j$ if necessary. Consider $\overline{G} = \mathcal{C}_2 \times \mathcal{C}_q$. Then we have $\overline{a} = a_2 a_q$, $\overline{b} = a_2$ and $\overline{c} = a_q^j$. Also, we have $|\overline{a}| = 2q$, $|\overline{b}| = 2$ and $|\overline{c}| = q$. Now if $j \neq 1$, then we have

$$C = (\overline{c}, \overline{a}^{-1}, \overline{b}, \overline{a}^2, \overline{b}, \overline{c}^{-1}, \overline{a}^{j-3}, \overline{b}, \overline{a}^{-(q-4)}, \overline{b}, \overline{a}^{q-j-2})$$

as a Hamiltonian cycle in $\mathrm{Cay}(\overline{G}; \overline{S})$. Now we calculate the voltage of $C$.

$$\begin{aligned} \mathbb{V}(C) &= ca^{-1}ba^2bc^{-1}a^{j-3}ba^{-(q-4)}ba^{q-j-2} \\ &\equiv a_2 \cdot a_2a_3 \cdot a_2^2 \cdot a_2a_3 \cdot a_2^{j-3} \cdot a_2a_3 \cdot a_2^{-(q-4)} \cdot a_2a_3 \cdot a_2^{q-j-2} \pmod{\mathcal{C}_q \ltimes \mathcal{C}_p} \\ &= a_3a_2a_3a_2a_3a_2a_2a_3 \\ &= a_3^2 \end{aligned}$$

which generates $\mathcal{C}_3$. By considering the fact that $\mathcal{C}_2$ might centralize $\mathcal{C}_p$ or not, we have

$$\begin{aligned} \mathbb{V}(C) &= ca^{-1}ba^2bc^{-1}a^{j-3}ba^{-(q-4)}ba^{q-j-2} \\ &\equiv a_q^j\gamma_p \cdot a_q^{-1}a_2 \cdot a_2 \cdot a_q^2 \cdot a_2 \cdot \gamma_p^{-1}a_q^{-j} \cdot a_q^{j-3} \cdot a_2 \cdot a_2a_q^{-q+4} \cdot a_2 \cdot a_q^{q-j-2} \pmod{\mathcal{C}_3} \end{aligned}$$

$$= a_q^j \gamma_p a_q \gamma_p^{\mp 1} a_q^{-j-1}$$

$$= \gamma_p^{\hat{\tau}^j \mp \hat{\tau}^{j+1}}$$

$$= \gamma_p^{\hat{\tau}^j (1 \mp \hat{\tau})}$$

which generates $\mathcal{C}_p$. Therefore, the subgroup generated by $\mathbb{V}(C)$ is $G'$. Thus, Factor Group Lemma 1.2.6 applies.

So we may assume $j = 1$, then $c = a_q \gamma_p$ and $\bar{c} = a_q$. We have

$$C_1 = ((\bar{b}, \bar{c})^{q-1}, \bar{b}, \bar{a})$$

as a Hamiltonian cycle in $\mathrm{Cay}(\overline{G}; \overline{S})$. Now we calculate its voltage.

$$\begin{aligned}
\mathbb{V}(C_1) &= (bc)^{q-1} ba \\
&\equiv (a_2 a_3)^{q-1} \cdot a_2 a_3 \cdot a_2 \pmod{\mathcal{C}_q \ltimes \mathcal{C}_p} \\
&= a_3^{-1}
\end{aligned}$$

which generates $\mathcal{C}_3$. If $\mathcal{C}_2$ centralizes $\mathcal{C}_p$, then

$$\begin{aligned}
\mathbb{V}(C_1) &= (bc)^{q-1} ba \\
&\equiv (a_2 \cdot a_q \gamma_p)^{q-1} \cdot a_2 \cdot a_2 a_q \pmod{\mathcal{C}_3} \\
&= (a_q \gamma_p)^{q-1} a_q \\
&= \gamma_p^{\hat{\tau} + \hat{\tau}^2 + \cdots + \hat{\tau}^{q-1}} \\
&= \gamma_p^{-1}
\end{aligned}$$

which generates $\mathcal{C}_p$. So in this case, the subgroup generated by $\mathbb{V}(C_1)$ is $G'$. Thus, Factor Group Lemma 1.2.6 applies.

Now if $\mathcal{C}_2$ inverts $\mathcal{C}_p$, then

$$\begin{aligned}\mathbb{V}(C_1) &= (bc)^{q-1}ba \\ &\equiv (a_2 \cdot a_q\gamma_p)^{q-1} \cdot a_2 \cdot a_2a_q \pmod{\mathcal{C}_3} \\ &= \gamma_p^{-\widehat{\tau}+\widehat{\tau}^2-\cdots-\widehat{\tau}^{q-2}+\widehat{\tau}^{q-1}}.\end{aligned}$$

Since $\widehat{\tau} \not\equiv -1 \pmod{p}$, then

$$\begin{aligned}\mathbb{V}(C_1) &= \gamma_p^{-\widehat{\tau}+\widehat{\tau}^2-\cdots-\widehat{\tau}^{q-2}+\widehat{\tau}^{q-1}} \\ &= \gamma_p^{(\widehat{\tau}^q+1)/(\widehat{\tau}+1)-1}.\end{aligned}$$

We may assume this does not generate $\mathcal{C}_p$, for otherwise Factor Group Lemma 1.2.6 applies. Therefore, since $\widehat{\tau}^q \equiv 1 \pmod{p}$, then

$$\begin{aligned}0 &\equiv (\widehat{\tau}^q + 1)/(\widehat{\tau} + 1) - 1 \pmod{p} \\ &= 2/(\widehat{\tau} + 1) - 1.\end{aligned}$$

This implies that $\widehat{\tau} \equiv 1 \pmod{p}$, which is impossible.

**Subcase 2.2.** Assume $j = 0$. Then $i \neq 0$ and $c = a_2\gamma_p$. Consider $\overline{G} = \mathcal{C}_2 \times \mathcal{C}_q$. Then we have $\overline{a} = a_2a_q$ and $\overline{b} = \overline{c} = a_2$. This implies that $|\overline{a}| = 2q$ and $|\overline{b}| = |\overline{c}| = 2$. We have

$$C = (\overline{c}, \overline{a}^{q-1}, \overline{b}, \overline{a}^{-(q-1)})$$

as a Hamiltonian cycle in $\mathrm{Cay}(\overline{G}; \overline{S})$. Since there is one occurrence of $b$ in $C$, and it is the only generator of $G$ that contains $a_3$, then by Lemma 2.5.2 we conclude that the subgroup generated by $\mathbb{V}(C)$ contains $\mathcal{C}_3$. Similarly, since there is one occurrence of $c$ in $C$, and it is the only generator of $G$ that contains $\gamma_p$, then by Lemma 2.5.2 we conclude that the subgroup generated by $\mathbb{V}(C)$ contains $\mathcal{C}_p$. Therefore, the subgroup generated by $\mathbb{V}(C)$ is $G'$. So, Factor Group Lemma 1.2.6 applies.

**Subcase 2.3.** Assume $i \neq 0$ and $j \neq 0$. Then $c = a_2 a_q^j \gamma_p$. Consider $\overline{G} = \mathcal{C}_2 \times \mathcal{C}_q$. Then we have $\overline{a} = a_2 a_q$, $\overline{b} = a_2$ and $\overline{c} = a_2 a_q^j$. This implies that $|\overline{a}| = |\overline{c}| = 2q$ and $|\overline{b}| = 2$. We may assume $j$ is even by replacing $c$ with its inverse and $j$ with $q - j$ if necessary.

Suppose, for the moment, that $j = q-1$, then $c = a_2 a_q^{-1} \gamma_p$ and $\overline{c} = \overline{a}^{-1}$. We have

$$C_1 = (\overline{c}, \overline{b}, (\overline{a}^{-1}, \overline{b})^{q-1})$$

as a Hamiltonian cycle in $\mathrm{Cay}(\overline{G}; \overline{S})$. Since there is one occurrence of $c$ in $C$, and it is the only generator of $G$ that contains $\gamma_p$, then by Lemma 2.5.2 we conclude that the subgroup generated by $\mathbb{V}(C_1)$ contains $\mathcal{C}_p$. Also,

$$\begin{aligned}
\mathbb{V}(C_1) &= cb(a^{-1}b)^{q-1} \\
&\equiv a_2 \cdot a_2 a_3 \cdot (a_2 \cdot a_2 a_3)^{q-1} \pmod{\mathcal{C}_q \ltimes \mathcal{C}_p} \\
&= a_3^q
\end{aligned}$$

which generates $\mathcal{C}_3$. Therefore, the subgroup generated by $\mathbb{V}(C_1)$ contains $G'$. Thus, Factor Group Lemma 1.2.6 applies.

So we may assume $j \neq q-1$. Then we have

$$C_2 = (\overline{c}, \overline{a}^{q-j-1}, \overline{b}, \overline{a}^{-q+j+1}, (\overline{a}^{-1}, \overline{b})^j)$$

and

$$C_3 = (\overline{c}, \overline{a}^{q-j-2}, \overline{b}, \overline{a}^{-q+j+2}, (\overline{a}^{-1}, \overline{b})^{j-1}, \overline{a}^{-2}, \overline{b}, \overline{a})$$

as Hamiltonian cycles in $\mathrm{Cay}(\overline{G}; \overline{S})$. Since there is one occurrence of $c$ in $C_2$, and it is the only generator of $G$ that contains $\gamma_p$, then by Lemma 2.5.2 we conclude that the subgroup generated by $\mathbb{V}(C_2)$ contains $\mathcal{C}_p$. Also,

$$\begin{aligned}
\mathbb{V}(C_2) &= ca^{q-j-1}ba^{-q+j+1}(a^{-1}b)^j \\
&\equiv a_2 \cdot a_2^{q-j-1} \cdot a_2 a_3 \cdot a_2^{-q+j+1} \cdot a_3^j \pmod{\mathcal{C}_q \ltimes \mathcal{C}_p} \\
&= a_3^{j+1}.
\end{aligned}$$

We may assume this does not generate $\mathcal{C}_3$, for otherwise Factor Group Lemma 1.2.6 applies. Then $j \equiv -1 \pmod 3$.

Since there is one occurrence of $c$ in $C_3$, and it is the only generator of $G$ that contains $\gamma_p$, then by Lemma 2.5.2 we conclude that the subgroup generated by $\mathbb{V}(C_3)$ contains $\mathcal{C}_p$. Also,

$$\begin{aligned}
\mathbb{V}(C_3) &= ca^{q-j-2}ba^{-q+j+2}(a^{-1}b)^{j-1}a^{-2}ba \\
&\equiv a_2 \cdot a_2^{q-j-2} \cdot a_2 a_3 \cdot a_2^{-q+j+2} \cdot a_3^{j-1} \cdot a_2^{-2} \cdot a_2 a_3 \cdot a_2 \pmod{\mathcal{C}_q \ltimes \mathcal{C}_p} \\
&= a_2 a_3 a_2 a_3^{j-1} a_2 a_3 a_2 \\
&= a_3^{j-3} \\
&= a_3^j
\end{aligned}$$

Since $j \equiv -1 \pmod 3$, this generates $\mathcal{C}_3$. So, Factor Group Lemma 1.2.6 applies.

**Case 3.** Assume $a = a_2 a_q$ and $b = a_q^m a_3$. If $k \neq 0$, then by Lemma 2.4.3(1) $\langle a, c \rangle = G$ which contradicts the minimality of $S$. So we can assume $k = 0$. Now if $i \neq 0$, then by Lemma 2.4.3(3) $\langle b, c \rangle = G$ which contradicts the minimality of $S$. Therefore, we may assume $i = 0$. Then $j \neq 0$ and $c = a_q^j \gamma_p$. Consider $\overline{G} = \mathcal{C}_2 \times \mathcal{C}_q$. Then we have $\overline{a} = a_2 a_q$, $\overline{b} = a_q^m$ and $\overline{c} = a_q^j$.

Suppose, for the moment, that $m = j$. Then $\overline{b} = \overline{c}$. We have

$$C_1 = (\overline{c}^{-1}, \overline{b}^{-(q-2)}, \overline{a}^{-1}, \overline{b}^{q-1}, \overline{a})$$

as a Hamiltonian cycle in $\mathrm{Cay}(\overline{G}; \overline{S})$. Since there is one occurrence of $c$ in $C_1$, and it is the only generator of $G$ that contains $\gamma_p$, then by Lemma 2.5.2 we conclude that the subgroup generated by $\mathbb{V}(C_1)$ contains $\mathcal{C}_p$. Also,

$$\begin{aligned}
\mathbb{V}(C_1) &= c^{-1}b^{-(q-2)}a^{-1}b^{q-1}a \\
&\equiv a_3^{-(q-2)} \cdot a_2 \cdot a_3^{q-1} \cdot a_2 \pmod{\mathcal{C}_q \ltimes \mathcal{C}_p} \\
&= a_3^{-2q+3} \\
&= a_3^{-2q}
\end{aligned}$$

which generates $\mathcal{C}_3$, because $\gcd(2q, 3) = 1$. So, the subgroup generated by $\mathbb{V}(C_1)$ is $G'$. Therefore, Factor Group Lemma 1.2.6 applies.

So we may assume $m \neq j$. We may also assume $m$ and $j$ are even, by replacing $\{b, c\}$ with their inverses, $m$ with $q - m$, and $j$ with $q - j$ if necessary. Now suppose, for the moment, $j = 2$. Then we have $c = a_q^2\gamma_p$. We also have

$$C_2 = (\overline{b}, \overline{c}^{-(m-2)/2}, \overline{a}^{-1}, \overline{c}^{m/2}, \overline{a}^{2q-m-1})$$

as a Hamiltonian cycle in $\mathrm{Cay}(\overline{G}; \overline{S})$. Since there is one occurrence of $b$ in $C_2$, and it is the only generator of $G$ that contains $a_3$, then by Lemma 2.5.2 we conclude that the subgroup generated by $\mathbb{V}(C_2)$ contains $\mathcal{C}_3$. Now by considering the fact that $\mathcal{C}_2$ might centralize $\mathcal{C}_p$ or not, we have

$$\begin{aligned}
\mathbb{V}(C_2) &= bc^{-(m-2)/2}a^{-1}c^{m/2}a^{2q-m-1} \\
&\equiv a_q^m \cdot (a_q^2\gamma_p)^{-(m-2)/2} \cdot a_q^{-1}a_2 \cdot (a_q^2\gamma_p)^{m/2} \cdot a_2^{2q-m-1}a_q^{2q-m-1} \pmod{\mathcal{C}_3}
\end{aligned}$$

$$= a_q^m (\gamma_p^{\hat\tau^2+(\hat\tau^2)^2+\cdots+(\hat\tau^2)^{(m-2)/2}} a_q^{(m-2)})^{-1} a_q^{-1} a_2 (\gamma_p^{\hat\tau^2+(\hat\tau^2)^2+\cdots+(\hat\tau^2)^{m/2}} a_q^m) a_2 a_q^{-m-1}$$
$$= a_q^m a_q^{-(m-2)} \gamma_p^{-\hat\tau^2(1+\hat\tau^2+\cdots+(\hat\tau^2)^{(m-4)/2})} a_q^{-1} \gamma_p^{\pm\hat\tau^2(1+\hat\tau^2+\cdots+(\hat\tau^2)^{(m-2)/2})} a_q^m a_q^{-m-1}.$$

Since $\hat\tau^2 - 1 \not\equiv 0 \pmod p$, then

$$\begin{aligned}\mathbb{V}(C_2) &= a_q^2 \gamma_p^{-\hat\tau^2(\hat\tau^{m-2}-1)/(\hat\tau^2-1)} a_q^{-1} \gamma_p^{\pm\hat\tau^2(\hat\tau^m-1)/(\hat\tau^2-1)} a_q^{-1}\\ &= \gamma_p^{-\hat\tau^4(\hat\tau^{m-2}-1)/(\hat\tau^2-1)\pm\hat\tau^3(\hat\tau^m-1)/(\hat\tau^2-1)}\\ &= \gamma_p^{\hat\tau^3(1\mp\hat\tau)(-\hat\tau^{m-1}\mp1)/(\hat\tau^2-1)}.\end{aligned}$$

We may assume this does not generate $\mathcal{C}_p$, for otherwise Factor Group Lemma 1.2.6 applies. Therefore, $\hat\tau \equiv \pm1 \pmod p$ or $\hat\tau^{m-1} \equiv \pm1 \pmod p$. The first case is impossible. So we may assume $\hat\tau^{m-1} \equiv \pm1 \pmod p$. Thus, $\hat\tau^{2(m-1)} \equiv 1 \pmod p$. We also know that $\hat\tau^q \equiv 1 \pmod p$. So we have $\hat\tau^d \equiv 1 \pmod p$, where $d = \gcd(2(m-1), q)$. Since $\gcd(2, q) = 1$ and $2 \leqslant m \leqslant q-1$, then $d = 1$, which contradicts the fact that $\hat\tau \not\equiv 1 \pmod p$.

So we may assume $j \neq 2$. We have

$$C_3 = (\overline{b}, \overline{c}, \overline{a}, \overline{c}^{-1}, \overline{b}^{-1}, \overline{a}^{m-2}, \overline{c}, \overline{a}^{-(j-3)}, \overline{c}, \overline{a}^{2q-m-j-2})$$

as a Hamiltonian cycle in $\mathrm{Cay}(\overline{G}; \overline{S})$. Now we calculate its voltage.

$$\begin{aligned}\mathbb{V}(C_3) &= bcac^{-1}b^{-1}a^{m-2}ca^{-(j-3)}ca^{2q-m-j-2}\\ &\equiv a_3 \cdot a_2 \cdot a_3^{-1} \cdot a_2^{m-2} \cdot a_2^{-j+3} \cdot a_2^{2q-m-j-2} \pmod{\mathcal{C}_q \ltimes \mathcal{C}_p}\\ &= a_3^2\end{aligned}$$

which generates $\mathcal{C}_3$. Also, by considering the fact that $\mathcal{C}_2$ might centralize $\mathcal{C}_p$ or not, we have

$$\begin{aligned}
\mathbb{V}(C_3) &= bcac^{-1}b^{-1}a^{m-2}ca^{-(j-3)}ca^{2q-m-j-2} \\
&\equiv a_q^m \cdot a_q^j\gamma_p \cdot a_2 a_q \cdot \gamma_p^{-1}a_q^{-j} \cdot a_q^{-m} \cdot a_2^{m-2}a_q^{m-2} \\
&\qquad \cdot a_q^j\gamma_p \cdot a_q^{-j+3}a_2^{-j+3} \cdot a_q^j\gamma_p \cdot a_2^{2q-m-j-2}a_q^{2q-m-j-2} \pmod{\mathcal{C}_3} \\
&= a_q^{m+j}\gamma_p a_2 a_q \gamma_p^{-1} a_q^{-2}\gamma_p a_q^3 a_2 \gamma_p a_q^{-m-j-2} \\
&= a_q^{m+j}\gamma_p a_q \gamma_p^{\mp 1} a_q^{-2}\gamma_p^{\pm 1} a_q^3 \gamma_p a_q^{-m-j-2} \\
&= \gamma_p^{\widehat{\tau}^{m+j} \mp \widehat{\tau}^{m+j+1} \pm \widehat{\tau}^{m+j-1} + \widehat{\tau}^{m+j+2}} \\
&= \gamma_p^{\widehat{\tau}^{m+j-1}(\widehat{\tau}^3 \mp \widehat{\tau}^2 + \widehat{\tau} \pm 1)}.
\end{aligned}$$

We may assume this does not generate $\mathcal{C}_p$, for otherwise Factor Group Lemma 1.2.6 applies. Therefore,

$$0 \equiv \widehat{\tau}^3 \mp \widehat{\tau}^2 + \widehat{\tau} \pm 1 \pmod{p}.$$

If $\mathcal{C}_2$ centralizes $\mathcal{C}_p$, then

$$0 \equiv \widehat{\tau}^3 - \widehat{\tau}^2 + \widehat{\tau} + 1 \pmod{p}. \tag{3A}$$

We can replace $\widehat{\tau}$ with $\widehat{\tau}^{-1}$ in the above equation after replacing $\{a, b, c\}$ with their inverses in the Hamiltonian cycle, then

$$0 \equiv \widehat{\tau}^{-3} - \widehat{\tau}^{-2} + \widehat{\tau}^{-1} + 1 \pmod{p}.$$

Multiplying by $\widehat{\tau}^3$, we have

$$\begin{aligned}
0 &\equiv 1 - \widehat{\tau} + \widehat{\tau}^2 + \widehat{\tau}^3 \pmod{p} \\
&= \widehat{\tau}^3 + \widehat{\tau}^2 - \widehat{\tau} + 1.
\end{aligned}$$

Subtracting 3A from the above equation we have

$$\begin{aligned} 0 &\equiv 2\widehat{\tau}^2 - 2\widehat{\tau} \pmod{p} \\ &= 2\widehat{\tau}(\widehat{\tau} - 1) \end{aligned}$$

which is impossible, because $\widehat{\tau} \not\equiv 1 \pmod{p}$.

Now if $\mathcal{C}_2$ inverts $\mathcal{C}_p$, then

$$0 \equiv \widehat{\tau}^3 + \widehat{\tau}^2 + \widehat{\tau} - 1 \pmod{p}. \tag{3B}$$

We can replace $\widehat{\tau}$ with $\widehat{\tau}^{-1}$ in the above equation after replacing $\{a, b, c\}$ with their inverses. Then

$$0 \equiv \widehat{\tau}^{-3} + \widehat{\tau}^{-2} + \widehat{\tau}^{-1} - 1 \pmod{p}.$$

Multiplying by $\widehat{\tau}^3$, then

$$\begin{aligned} 0 &\equiv 1 + \widehat{\tau} + \widehat{\tau}^2 - \widehat{\tau}^3 \pmod{p} \\ &= -\widehat{\tau}^3 + \widehat{\tau}^2 + \widehat{\tau} + 1. \end{aligned}$$

By adding 3B and the above equation, we have

$$\begin{aligned} 0 &\equiv 2(\widehat{\tau}^2 + \widehat{\tau}) \pmod{p} \\ &= 2\widehat{\tau}(\widehat{\tau} + 1) \end{aligned}$$

which is also impossible, because $\widehat{\tau} \not\equiv -1 \pmod{p}$.

**Case 4.** Assume $a = a_2$ and $b = a_q a_3$.

**Subcase 4.1.** Assume $i \neq 0$. Then $c = a_2 a_q^j a_3^k \gamma_p$. By Lemma 2.4.3(2) $\langle b, c \rangle = G$

which contradicts the minimality of $S$.

**Subcase 4.2.** Assume $i = 0$. Then $j \neq 0$ and $c = a_q^j a_3^k \gamma_p$. We may assume $j$ is even by replacing $c$ with its inverse and $j$ with $q - j$ if necessary. Consider $\overline{G} = \mathcal{C}_2 \times \mathcal{C}_q$. Then we have $\overline{a} = a_2$, $\overline{b} = a_q$ and $\overline{c} = a_q^j$. This implies that $|\overline{a}| = 2$ and $|\overline{b}| = |\overline{c}| = q$. We have

$$C_1 = (\overline{c}, \overline{b}^{q-j-1}, \overline{c}, \overline{b}^{-(j-2)}, \overline{a}, \overline{b}^{q-1}, \overline{a})$$

as a Hamiltonian cycle in $\mathrm{Cay}(\overline{G}; \overline{S})$. Now we calculate its voltage.

$$\begin{aligned}
\mathbb{V}(C_1) &= cb^{q-j-1}cb^{-(j-2)}ab^{q-1}a \\
&\equiv a_q^j\gamma_p \cdot a_q^{q-j-1} \cdot a_q^j\gamma_p \cdot a_q^{-j+2} \cdot a_2 \cdot a_q^{q-1} \cdot a_2 \pmod{\mathcal{C}_3} \\
&= a_q^j\gamma_p a_q^{-1}\gamma_p a_q^{-j+1} \\
&= \gamma_p^{\hat{\tau}^{j-1}(\hat{\tau}+1)}
\end{aligned}$$

which generates $\mathcal{C}_p$. Also

$$\begin{aligned}
\mathbb{V}(C_1) &= cb^{q-j-1}cb^{-(j-2)}ab^{q-1}a \\
&\equiv a_3^k \cdot a_3^{q-j-1} \cdot a_3^k \cdot a_3^{-j+2} \cdot a_2 \cdot a_3^{q-1} \cdot a_2 \pmod{\mathcal{C}_q \ltimes \mathcal{C}_p} \\
&= a_3^{k+q-j-1+k-j+2-q+1} \\
&= a_3^{2(k-j+1)}.
\end{aligned}$$

We may assume this does not generate $\mathcal{C}_3$, for otherwise Factor Group Lemma 1.2.6 applies. Then

$$0 \equiv k - j + 1 \pmod{3}. \tag{4.2A}$$

We also have

$$C_2 = (\overline{c}, \overline{a}, (\overline{b}, \overline{a})^{q-j-1}, \overline{b}^j, \overline{a}, \overline{b}^{-(j-1)})$$

as a Hamiltonian cycle in $\mathrm{Cay}(\overline{G}; \overline{S})$. We calculate its voltage. Since there is one occurrence of $c$ in $C_2$, and it is the only generator of $G$ that contains $\gamma_p$, then by Lemma 2.5.2 we conclude that the subgroup generated by $\mathbb{V}(C_2)$ contains $\mathcal{C}_p$. Also,

$$\begin{aligned}
\mathbb{V}(C_2) &= ca(ba)^{q-j-1}b^j ab^{-(j-1)} \\
&\equiv a_3^k \cdot a_2 \cdot (a_3 a_2)^{q-j-1} \cdot a_3^j \cdot a_2 \cdot a_3^{-j+1} \pmod{\mathcal{C}_q \ltimes \mathcal{C}_p} \\
&= a_3^{k-2j+1}.
\end{aligned}$$

We may assume this does not generate $\mathcal{C}_3$, for otherwise Factor Group Lemma 1.2.6 applies. Therefore,

$$0 \equiv k - 2j + 1 \pmod 3.$$

By subtracting the above equation from 4.2A we have $j \equiv 0 \pmod 3$.

Now we have

$$C_3 = (\overline{c}, \overline{a}, \overline{b}^{q-j-1}, \overline{a}, \overline{b}^{-(q-j-2)}, \overline{c}^{-1}, \overline{b}^{j-2}, \overline{a}, \overline{b}^{-(j-1)}, \overline{a})$$

as a Hamiltonian cycle in $\mathrm{Cay}(\overline{G}; \overline{S})$. We calculate its voltage.

$$\begin{aligned}
\mathbb{V}(C_3) &= cab^{q-j-1}ab^{-(q-j-2)}c^{-1}b^{j-2}ab^{-(j-1)}a \\
&\equiv a_q^j \gamma_p \cdot a_2 \cdot a_q^{q-j-1} \cdot a_2 \cdot a_q^{-q+j+2} \cdot \gamma_p^{-1} a_q^{-j} \cdot a_q^{j-2} \cdot a_2 \cdot a_q^{-j+1} \cdot a_2 \pmod{\mathcal{C}_3} \\
&= a_q^j \gamma_p a_q \gamma_p^{-1} a_q^{-j-1} \\
&= \gamma_p^{\widehat{\tau}^j (1-\widehat{\tau})}.
\end{aligned}$$

which generates $\mathcal{C}_p$. Also

$$\begin{aligned}
\mathbb{V}(C_3) &= cab^{q-j-1}ab^{-(q-j-2)}c^{-1}b^{j-2}ab^{-(j-1)}a \\
&\equiv a_3^k \cdot a_2 \cdot a_3^{q-j-1} \cdot a_2 \cdot a_3^{-q+j+2} \cdot a_3^{-k} \cdot a_3^{j-2} \cdot a_2 \cdot a_3^{-j+1} \cdot a_2 \pmod{\mathcal{C}_q \ltimes \mathcal{C}_p} \\
&= a_3^{k-q+j+1-q+j+2-k+j-2+j-1} \\
&= a_3^{-2q+4j}.
\end{aligned}$$

We may assume this does not generate $\mathcal{C}_3$, for otherwise Factor Group Lemma 1.2.6 applies. Then

$$\begin{aligned}
0 &\equiv -2q + 4j \pmod 3 \\
&= q + j
\end{aligned}$$

We already know $j \equiv 0 \pmod 3$. By substituting this in the above equation, we have $q \equiv 0 \pmod 3$ which contradicts the fact that $\gcd(q, 3) = 1$. □

## 3.9 Assume $|S| \geqslant 4$

In this section we prove the following general result that includes the part of Theorem 1.1.3, where $|S| \geqslant 4$ (see Assumption 3.0.1). Unlike in the other sections of this chapter, we do not assume $|G| = 6pq$.

**Proposition 3.9.** *Assume $|G|$ is a product of four distinct primes and $S$ is a minimal generating set of $G$, where $|S| \geqslant 4$. Then $\mathrm{Cay}(G; S)$ contains a Hamiltonian cycle.*

*Proof.* Suppose $S = \{s_1, s_2, ..., s_k\}$ and let $G_i = \langle s_1, s_2, ..., s_i \rangle$ for $i = 1, 2, ..., k$. Since $S$ is minimal, we know $\{e\} \subset G_1 \subset G_2 \subset ...G_k = G$. Therefore, the number of prime factors of $|G_i|$ is at least $i$. Since $|G| = p_1p_2p_3q$ is the product of only 4 primes, and $k = |S| \geqslant 4$, we can conclude that $|G_i|$ has exactly $i$ prime factors, for all $i$. This implies that $|S| = 4$. This also implies every element of $S$ has prime order.

Since $|G|$ is square-free, we know that $G'$ is cyclic (see Proposition 1.3.12(1)), so $G' \neq G$. We may assume $|G'| \neq 1$, for otherwise $G$ is abelian, so Lemma 1.2.2 applies. Also, if $|G'|$ is equal to a prime number, then Theorem 1.2.3 applies. So we may assume $|G'|$ has at least two prime factors. Therefore, the number of prime factors of $|G'|$ is either 2 or 3.

**Case 1.** Assume $|G'|$ has only two prime factors. This implies $|\overline{G}| = p_1p_2$, where $p_1$ and $p_2$ are two distinct primes. Suppose $s \in S$, then $\overline{s} \in \overline{S}$. We know that $|\overline{s}| \neq 1$ (see Assumption 3.0.1(6)). Now since every element of $S$ has prime order, then $|s|$ is either $p_1$ or $p_2$. Also, every element of order $p_1$ must commute with every element of order $p_2$, because the subgroup $H$ generated by any element of $S$ that has order $p_1$, together with any element of $S$ that has order $p_2$ has exactly two prime factors, so $|H| = p_1p_2$, $H' \subseteq G'$, and $|G'| = p_3p_4$. Thus, $|H'| = 1$. Let $S_{p_1}$ be the elements of order $p_1$ in $S$, and let $S_{p_2}$ be the elements of order $p_2$. Also let $H_{p_1}$ and $H_{p_2}$ be the subgroups generated by $S_{p_1}$ and $S_{p_2}$, respectively. This implies that $\mathrm{Cay}(G; S) \cong \mathrm{Cay}(G_{p_1}; S_{p_1}) \square \mathrm{Cay}(G_{p_2}; S_{p_2})$. Therefore, $\mathrm{Cay}(G; S)$ contains a Hamiltonian cycle (see Corollary 1.2.10).

**Case 2.** Assume $|G'|$ has three prime factors. We may write (see Proposition 1.3.12(3))

$$G = \mathcal{C}_q \ltimes G' = \mathcal{C}_q \ltimes (\mathcal{C}_{p_1} \times \mathcal{C}_{p_2} \times \mathcal{C}_{p_3}),$$

where $p_1$, $p_2$, $p_3$ and $q$ are distinct primes. Note that $G' \cap Z(G) = \{e\}$ (see Proposition 1.3.12(2)). Now we may assume $\langle s_4 \rangle = \mathcal{C}_q$. Since $|\langle s_i, s_4 \rangle|$ has only two prime factors (for $1 \leqslant i \leqslant 3$), we must have $s_i = s_4^{k_i} a_{p_i}$ (after permuting $p_1$, $p_2$, $p_3$), where $a_{p_i}$ is a generator of $\mathcal{C}_{p_i}$. We may also assume $S \cap G' = \varnothing$ (see Lemma 1.2.11), so $k_i \not\equiv 0 \pmod q$. Now consider

$$G_2 = \langle s_1, s_2 \rangle = \langle s_4^{k_1} a_{p_1}, s_4^{k_2} a_{p_2} \rangle.$$

Since $\mathcal{C}_{p_1}$ is a normal subgroup in $G$, we can consider $\overline{G}_2 = G_2/\mathcal{C}_{p_1}$, then $\{\overline{s}_1, \overline{s}_2\} = \{\overline{s}_4^{k_1}, \overline{s}_4^{k_2}\overline{a}_{p_2}\}$. We have

$$\overline{s}_4^{k_2^{-1}} = (\overline{s}_4^{k_1})^{k_1^{-1}k_2^{-1}} = \overline{s}_1^{k_1^{-1}k_2^{-1}}.$$

Multiplying by $\overline{s}_2$, then

$$\overline{a}_{p_2} = \overline{s}_4^{k_2^{-1}} \cdot \overline{s}_4^{k_2} a_{p_2} = \overline{s}_1^{k_1^{-1}k_2^{-1}} \overline{s}_2 \in \overline{G}_2.$$

Since $a_{p_2}$ generates $\mathcal{C}_{p_2}$, this implies $|G_2|$ is divisible by $p_2$. Similarly, we can show that $|G_2|$ is divisible by $p_1$. Also, $|s_1| = q$, so $|G_2|$ is divisible by $q$. Therefore, $|G_2|$ has three prime factors, which is a contradiction. □

# Chapter 4

# Conclusion

Despite lots of papers published related to the topic of Hamiltonian cycles in Cayley graphs, there has been little progress in this area. In this chapter, we observe that we do not even know when $|G| = 144$ whether for every Cayley graph on $G$, there is a Hamiltonian cycle or not. We will also discuss a possible future direction for our research and some of the Hamiltonian cycles that will generalize.

When $|G| = 144 = 48 \times 3$, it means that $|G|$ is of the type $48p$, where $p$ is prime. By looking at Theorem 1.1.2(1) we see that the case where the order of $G$ is $48p$ is still open for arbitrary primes $p$. In fact, it has not been proven when $p = 3$, so 144 is the smallest number for which we do not know whether or not every connected Cayley graph of that order has a Hamiltonian cycle.

The most logical next step in this work would be to consider the following open problem.

**Problem 4.0.1.** *Assume $|G| = 2pqr$, where $p$,$q$ and $r$ are distinct primes. Show that every connected Cayley graph on $G$ has a Hamiltonian cycle.*

*Possible method of attack.* We can assume $|G|$ is square-free. Otherwise, without loss of generality we may assume $r = 2$, so $|G| = 4pq$, and Theorem 1.1.2(2) applies.

Let $S$ be a minimal generating set of $G$. By using the same strategy used to prove Theorem 1.1.3, we can divide this proof into three different parts depending on the cardinality of $|S|$. So $|S| = 2$ or $|S| = 3$ or $|S| \geqslant 4$. When $|S| \geqslant 4$, then Proposition 3.9 applies. (Note that if $|S| = 1$, then $G$ is abelian, so Lemma 1.2.2 applies.) Hence, there will be two main parts needed to prove that Hamiltonian cycles exist in all such graphs (the cases $|S| = 2$ or $|S| = 3$). $\square$

Some of the Hamiltonian cycles used in the proof of our main result (Theorem 1.1.3) will generalize to some cases of Problem 4.0.1. For instance, the Hamiltonian cycle in Subcase 2.2 on page 109 generalizes to the following case.

**Proposition 4.0.2.** *Assume*

- $G = (\mathcal{C}_2 \times \mathcal{C}_r) \ltimes (\mathcal{C}_p \times \mathcal{C}_q)$,
- $|S| = 3$ *and* $S = \{a_2 a_r, a_2 a_q, a_2 \gamma_p\}$,
- $C_{G'}(\mathcal{C}_2) = \{e\}$ *and* $C_{G'}(\mathcal{C}_r) = \{e\}$.

*Then* $\mathrm{Cay}(G; S)$ *has a Hamiltonian cycle.*

*Proof.* Let $a = a_2 a_r$, $b = a_2 a_q$ and $c = a_2 \gamma_p$. We have $a_r \gamma_p a_r^{-1} = \gamma_p^{\widehat{\tau}}$ and $a_r a_q a_r^{-1} = a_q^{\check{\tau}}$, where $\widehat{\tau}^r \equiv 1 \pmod p$ and $\check{\tau}^r \equiv 1 \pmod q$. Since $C_{G'}(\mathcal{C}_r) = \{e\}$, then $\widehat{\tau} \not\equiv 1 \pmod p$ and $\check{\tau} \not\equiv 1 \pmod q$.

Consider $\overline{G} \cong \mathcal{C}_2 \times \mathcal{C}_r$. Then $\overline{a} = a_2 a_r$ and $\overline{b} = \overline{c} = a_2$. We have $C = (\overline{c}, \overline{a}^{r-1}, \overline{b}, \overline{a}^{-(r-1)})$ as a Hamiltonian cycle in $\mathrm{Cay}(\overline{G}; \overline{S})$. Since there is one occurrence of $c$ in $C$, and it is the only generator that contains $\gamma_p$, then by Lemma 2.5.2 we conclude that the subgroup generated by $\mathbb{V}(C)$ contains $\mathcal{C}_p$. Similarly, since there is one occurrence of $b$ in $C$ and it is the only generator which contains $a_q$, then by Lemma 2.5.2 we conclude that the subgroup generated by $\mathbb{V}(C)$ contains $\mathcal{C}_q$. Therefore, the subgroup generated by $\mathbb{V}(C)$ is $G'$, so Factor Group Lemma 1.2.6 applies. $\square$

# Bibliography


[1] B. Alspach. The classification of Hamiltonian generalized Petersen graphs. *J. Combin. Theory Ser. B*, 34(3):293–312, 1983.

[2] B. Alspach. Lifting hamiltonian cycles of quotient graphs. *Discrete Math.*, 12(78):25–36, 1989.

[3] B. Alspach, J. C. Bermond, and D. Sotteau. Decomposition into cycles. I. Hamilton decompositions. In *Cycles and rays (Montreal, PQ, 1987)*, volume 301 of *NATO Adv. Sci. Inst. Ser. C Math. Phys. Sci.*, pages 9–18. Kluwer Acad. Publ., Dordrecht, 1990.

[4] B. Alspach, C. C. Chen, and K. McAvaney. On a class of Hamiltonian laceable 3-regular graphs. volume 151, pages 19–38. 1996. Graph theory and combinatorics (Manila, 1991).

[5] B. Alspach and Y. Qin. Hamilton-connected Cayley graphs on Hamiltonian groups. *European J. Combin.*, 22(6):777–787, 2001.

[6] B. Alspach and C. Q. Zhang. Hamilton cycles in cubic Cayley graphs on dihedral groups. *Ars Combin.*, 28:101–108, 1989.

[7] K. Bannai. Hamiltonian cycles in generalized Petersen graphs. *J. Combinatorial Theory Ser. B*, 24(2):181–188, 1978.

[8] D. Bryant and M. Dean. Vertex-transitive graphs that have no Hamilton decomposition. *J. Combin. Theory Ser. B*, 114:237–246, 2015.

[9] A. Cayley. The theory of groups: Graphical representation. *Amer. J. Math.*, 1(2):174–176, 1878.

[10] C. C. Chen. On edge-Hamiltonian property of Cayley graphs. In *Proceedings of the First Japan Conference on Graph Theory and Applications (Hakone, 1986)*, volume 72, pages 29–33, 1988.

[11] C. C. Chen and N. Quimpo. Hamiltonian Cayley graphs of order $pq$. In *Combinatorial mathematics, X (Adelaide, 1982)*, volume 1036 of *Lecture Notes in Math.*, pages 1–5. Springer, Berlin, 1983.

[12] C. C. Chen and N. F. Quimpo. On some classes of Hamiltonian graphs. *Southeast Asian Bull. Math.*, (Special Issue):252–258, 1979.

[13] C. C. Chen and N. F. Quimpo. On strongly Hamiltonian abelian group graphs. In *Combinatorial mathematics, VIII (Geelong, 1980)*, volume 884 of *Lecture Notes in Math.*, pages 23–34. Springer, Berlin-New York, 1981.

[14] S. J. Curran and J. A. Gallian. Hamiltonian cycles and paths in Cayley graphs and digraphs—a survey. *Discrete Math.*, 156(1-3):1–18, 1996.

[15] S. J. Curran, D. W. Morris, and J. Morris. Cayley graphs of order $16p$ are Hamiltonian. *Ars Math. Contemp.*, 5(2):185–211, 2012.

[16] S. J. Curran and D. Witte. Hamilton paths in Cartesian products of directed cycles. In *Cycles in graphs (Burnaby, B.C., 1982)*, volume 115 of *North-Holland Math. Stud.*, pages 35–74. North-Holland, Amsterdam, 1985.

[17] E. Durnberger. Connected Cayley graphs of semidirect products of cyclic groups of prime order by abelian groups are Hamiltonian. *Discrete Math.*, 46(1):55–68, 1983.

[18] E. Durnberger. Every connected Cayley graph of a group with prime order commutator group has a Hamilton cycle. In *Cycles in graphs (Burnaby, B.C., 1982)*, volume 115 of *North-Holland Math. Stud.*, pages 75–80. North-Holland, Amsterdam, 1985.

[19] I. Ganev. Groups of a square-free order. *Rose-Hulman Undergraduate Mathematics Journal.*, 11, 2010.

[20] E. Ghaderpour and D. W. Morris. Cayley graphs of order $27p$ are Hamiltonian. *Int. J. Comb.*, pages Art. ID 206930, 16, 2011.

[21] E. Ghaderpour and D. W. Morris. Cayley graphs of order $30p$ are Hamiltonian. *Discrete Math.*, 312(24):3614–3625, 2012.

[22] E. Ghaderpour and D. W. Morris. Cayley graphs on nilpotent groups with cyclic commutator subgroup are Hamiltonian. *Ars Math. Contemp.*, 7(1):55–72, 2014.

[23] C. Godsil and G. Royle. *Algebraic Graph Theory.* Springer New York., 2001.

[24] The GAP Group*, GAP-Groups, Algorithms, and Programming, Version 4.8.7 (2017) and 4.8.10 (2018).* `http://www.gap-system.org`.

[25] M. Hall. *The Theory of Groups.* American Mathematical Soc., 1959.

[26] K. Helsgaun. LKH - an effective implementation of the Lin-Kernighan heuristic, Version 2.0.7, 2012. `http://www.akira.ruc.dk/~keld/research/LKH/`.

[27] Clay Mathematics Institute. P vs NP problem. `https://www.claymath.org/millennium-problems/p-vs-np-problem`.

[28] D. Jungreis and E. Friedman. Cayley graphs on groups of low order are Hamiltonian (unpublished).

[29] K. Keating and D. W. Morris. On Hamilton cycles in Cayley graphs in groups with cyclic commutator subgroup. In *Cycles in graphs (Burnaby, B.C., 1982)*, volume 115 of *North-Holland Math. Stud.*, pages 89–102. North-Holland, Amsterdam, 1985.

[30] E. Konstantinova. Some problems on Cayley graphs. *Linear Algebra Appl.*, 429(11-12):2754–2769, 2008.

[31] M. Krivelevich and B. Sudakov. Sparse pseudo-random graphs are Hamiltonian. *J. Graph Theory*, 42(1):17–33, 2003.

[32] K. Kutnar and D. Marušič. Hamilton cycles and paths in vertex-transitive graphs—current directions. *Discrete Math.*, 309(17):5491–5500, 2009.

[33] K. Kutnar, D. Marušič, D. W. Morris, J. Morris, and P. Šparl. Hamiltonian cycles in Cayley graphs whose order has few prime factors. *Ars Math. Contemp.*, 5(1):27–71, 2012.

[34] D. Li. Cayley graphs of order $pqr$ are Hamiltonian (chinese). *Acta Math. Sinica*, 44(2):351–358, 2001.

[35] D. X. Li. On edge-Hamiltonian property of Cayley graphs. In *Combinatorics, graph theory, algorithms and applications (Beijing, 1993)*, pages 147–150. World Sci. Publ., River Edge, NJ, 1994.

[36] D. X. Li. A note on edge-Hamiltonian property of Cayley graphs of order $pqr$. *Sichuan Daxue Xuebao*, 41(4):697–699, 2004.

[37] D. Marušič. Hamiltonian circuits in Cayley graphs. *Discrete Math.*, 46(1):49–54, 1983.

[38] D. W. Morris. 2-generated Cayley digraphs on nilpotent groups have Hamiltonian paths. *Contrib. Discrete Math.*, 7(1):41–47, 2012.

[39] D. W. Morris. Odd-order Cayley graphs with commutator subgroup of order $pq$ are Hamiltonian. *Ars Math. Contemp.*, 8(1):1–28, 2015.

[40] D. W. Morris. Cayley graphs on groups with commutator subgroup of order $2p$ are hamiltonian. *Art Discrete Appl. Math.*, 1(1):#P1.04, 31, 2018.

[41] D. W. Morris and K. Wilk. Cayley graphs of order $kp$ are hamiltonian for $k < 48$. *Art Discrete Appl. Math.*, 17(3), 2020.

[42] I. Pak and R. Radoičić. Hamiltonian paths in Cayley graphs. *Discrete Math.*, 309(17):5501–5508, 2009.

[43] L. E. Penn and D. Witte. When the cartesian product of two directed cycles is hypohamiltonian. *J. Graph Theory.*, 7:441–443, 1983.

[44] R. A. Rankin. A campanological problem in group theory. *Proc Camb Phil Soc.*, 44:17–25, 1948.

[45] C. Savage. A survey of combinatorial Gray codes. *SIAM Rev.*, 39(4):605–629, 1997.

[46] W. R. Scott. *Group theory.* Dover Publications, Inc., New York, second edition, 1987.

[47] S. N. Thimmaraju and R. Murali. Decomposition of edge deleted complete graphs into Hamiltonian-2-laceable paths. *Far East J. Appl. Math.*, 18(1):59–87, 2005.

[48] E. E. Westlund, J. Liu, and D. L. Kreher. 6-regular Cayley graphs on abelian groups of odd order are Hamiltonian decomposable. *Discrete Math.*, 309(16):5106–5110, 2009.

[49] D. Witte. Cayley digraphs of prime-power order are Hamiltonian. *J. Combin. Theory Ser. B*, 40(1):107–112, 1986.

[50] D. Witte and J. A. Gallian. A survey: Hamiltonian cycles in Cayley graphs. *Discrete Math.*, 51(3):293–304, 1984.

[51] D. S. Witte. On Hamiltonian circuits in Cayley diagrams. *Discrete Math.*, 38(1):99–108, 1982.