AUSTRALASIAN JOURNAL OF COMBINATORICS
Volume **83(3)** (2022), Pages 124–166

On Hamiltonicity of Cayley graphs of order $pqrs$

Farzad Maghsoudi

School of Mathematics and Statistics
Carleton University, Ottawa
Ontario K1S 5B6, Canada
farzadmaghsoudi@cmail.carleton.ca

Abstract

Assume G is a finite group such that $|G| = pqrs$, where p, q, r and s are distinct prime numbers, and let S be a minimal generating set of G, such that $|S| \geqslant 3$. We prove there is a Hamiltonian cycle in the corresponding Cayley graph $\mathrm{Cay}(G; S)$.

1 Introduction

In 1878 Arthur Cayley [1] introduced the definition of a Cayley graph. All graphs in this paper are undirected and simple. (The graphs have no loops or multiple edges or directions on the edges.)

Definition 1.1 ([11, Definition 1.1], cf. [7, 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 $s \in S$.

The field of Cayley graphs has become a significant branch of algebraic graph theory (see [10] for more information). Finding Hamiltonian cycles in Cayley graphs is a fundamental question in graph theory, but in general it is extremely difficult. There are many papers on the topic, but it is still an open question whether every connected Cayley graph has a Hamiltonian cycle. (See survey papers [3, 12] for more information.) In particular, a number of papers have shown that all connected Cayley graphs of specific orders are Hamiltonian:

Theorem 1.2 ([11, 13, 16, 18]) *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* $1 \leqslant k \leqslant 7$*,*
(3) pqr*,*
(4) kp^2*, where* $1 \leqslant k \leqslant 4$*,*
(5) kp^3*, where* $1 \leqslant k \leqslant 2$*,*
(6) p^k*, where* $1 \leqslant k < \infty$*.*

ISSN: 2202-3518

By the following theorem, every connected Cayley graph of order the product of four distinct odd primes has a Hamiltonian cycle.

Theorem 1.3 ([15, Theorem 1.3]) *If p, q, r, and s are distinct odd primes, then every connected Cayley graph of order $pqrs$ has a Hamiltonian cycle.*

The theorem above requires all four primes to be odd. The goal of this paper is to make progress toward removing this restriction, by proving certain cases where one of the primes is 2. However, we add the assumption that the generating set of the group contains a minimal generating set whose cardinality is greater than or equal to 3.

Theorem 1.4 *Assume G is a finite group of order $pqrs$ with the generating set S, where p, q, r, and s are distinct primes. If no 2-element subset of S generates G, then $\mathrm{Cay}(G; S)$ contains a Hamiltonian cycle.*

Remark 1.5 The case where p, q, r, and s are not distinct primes is still an open problem. For instance, it is not known whether all connected Cayley graphs of order $9p^2$ or $3p^3$ are Hamiltonian.

Remark 1.6 To remove the restriction on the generating set of our result (Theorem 1.4) and to complete the proof of the following problem "Every connected Cayley graph of order $pqrs$ (where p, q, r and s are distinct primes) are Hamiltonian", it would suffice to show that every connected Cayley graph of order $2pqr$ (where p, q, and r are distinct odd primes) which has a minimal generating set of order 2, has a Hamiltonian cycle.

2 Preliminaries

The purpose of this section is to introduce terminology and notation and to establish some results that will be used in the proof of Theorem 1.4.

2.1 Notation and definitions

Throughout the paper, we have used standard terminology of graph theory and group theory that can be found in textbooks, such as [7, 8].

The following notation is used in the paper:

- The commutator $ghg^{-1}h^{-1}$ of g and h is denoted by $[g, h]$.
- We will always let $G' = [G, G]$ be the commutator subgroup of G.
- We define $\overline{G} = G/G'$, $\overline{g} = gG'$ for any $g \in G$, and $\overline{S} = \{\overline{g}; g \in S\}$ for any $S \subseteq G$.
- We define $\overline{\overline{G}} = G/N$, $\overline{\overline{g}} = gN$ for any $g \in G$, and $\overline{\overline{S}} = \{\overline{\overline{g}}; g \in S\}$ for any $S \subseteq G$.
- $C_{G'}(S)$ denotes the centralizer of S in G'.
- $G \ltimes H$ denotes a semidirect product of groups G and H, where H is normal.
- D_{2n} denotes the dihedral group of order $2n$.

- e denotes the identity element of 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: $e, s_1, s_1 s_2, \ldots, s_1 s_2 \cdots s_n$. Also, $(s_1, s_2, \ldots, s_n)^{-1} = (s_n^{-1}, s_{n-1}^{-1}, \ldots, s_1^{-1})$.
- We use $(\overline{s_1}, \overline{s_2}, \ldots, \overline{s_n})$ to denote the image of the walk $(s_1, s_2, \ldots, s_n)$ in $\mathrm{Cay}(G/G'; \overline{S})$ $= \mathrm{Cay}(\overline{G}; \overline{S})$ which is a Cayley graph on the quotient group G/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 $(s_1, s_2, \ldots, s_m)$.
- p, q, and r are distinct prime numbers.
- $\mathcal{C}_n$ denotes the cyclic group of order n.
- $\widehat{G} = G/\mathcal{C}_p$, when $\mathcal{C}_p$ is a normal subgroup of G, we also let $\breve{G} = G/\mathcal{C}_q$ when $\mathcal{C}_q$ is a normal subgroup. Also, $\widehat{g} = g\mathcal{C}_p$, $\breve{g} = g\mathcal{C}_q$, for any $g \in G$, and $\widehat{S} = \{\widehat{g}; g \in S\}$, $\breve{S} = \{\breve{g}; g \in S\}$ for any $S \subseteq G$.
- If $G = (\mathcal{C}_2 \times \mathcal{C}_r) \ltimes (\mathcal{C}_p \times \mathcal{C}_q)$, we let a_2, a_r, γ_p, and γ_q be elements of G that generate $\mathcal{C}_2$, $\mathcal{C}_r$, $\mathcal{C}_p$, and $\mathcal{C}_q$, respectively.

2.2 Basic methods

In this subsection, we will see some of the key ideas used to prove Theorem 1.4 which is our main result.

The following well-known result handles the case of Theorem 1.4 where G is abelian.

Lemma 2.2.1 ([2, Corollary on p. 257]) *Assume G is an abelian group. Then every connected Cayley graph on G has a Hamiltonian cycle.*

Theorem 2.2.2 (Marušič [14], Durnberger [4, 5], and Keating-Witte [9]) *If the commutator subgroup G' of G is a cyclic p-group, then every connected Cayley graph on G has a Hamiltonian cycle.*

The following lemma (and its corollary) often provide a way to lift a Hamiltonian cycle in $\mathrm{Cay}(\overline{\overline{G}}; \overline{\overline{S}})$ to a Hamiltonian cycle in $\mathrm{Cay}(G; S)$. We introduce some useful notation before stating the results.

Notation 2.2.3 Suppose N is a normal subgroup of G, and $C = (s_1, s_2, \ldots, s_n)$ is a walk in $\mathrm{Cay}(G; S)$. If the walk $(s_1 N, s_2 N, \ldots, s_n N)$ in $\mathrm{Cay}(G/N; SN/N)$ is closed, then its *voltage* is the product $\mathbb{V}(C) = s_1 s_2 \cdots s_n$. This is an element of N. In particular, if $C = (\overline{\overline{s}}_1, \overline{\overline{s}}_2, \ldots, \overline{\overline{s}}_n)$ is a Hamiltonian cycle in $\mathrm{Cay}(\overline{\overline{G}}; \overline{\overline{S}})$, then $\mathbb{V}(C) = s_1 s_2 \cdots s_n$.

Factor Group Lemma 2.2.4 ([19, Section 2.2]) *Suppose:*

- *S is a generating set of G,*
- *N is a cyclic normal subgroup of G,*

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

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

Corollary 2.2.5 ([6, 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* $\mathrm{Cay}(\overline{\overline{G}}; \overline{\overline{S}})$ *that uses at least one edge labeled $\overline{\overline{s}}$.*

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

Lemma 2.2.6 [13, Lemma 2.8] *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 $\mathcal{C}_p$.*

Lemma 2.2.7 ([11, Lemma 2.27]) *Let S generate the finite group G, and let $s \in S$, such that $\langle s \rangle \lhd G$. If* $\mathrm{Cay}(G/\langle s \rangle; S)$ *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.*

2.3 Facts from group theory

Throughout this subsection we state some facts in group theory, which are used to prove our main result.

Lemma 2.3.1 ([17, Exercise 19 on page 43]) *Assume $|G| = 2k$, where k is odd. Then G has a subgroup of index* 2*.*

Corollary 2.3.2 *Assume $|G| = 2k$, where k is odd. Then $|G'|$ is odd.*

Proof. By Lemma 2.3.1, there is a normal subgroup H of G such that $[G : H] = 2$. Now since G/H has order 2, it follows that G/H is abelian, so $G' \subseteq H$. Therefore, $|G'|$ is odd. □

Proposition 2.3.3 ([8, Theorem 9.4.3 on page 146], cf. [6, 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 γ 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 τ, such that $|\gamma| = m$, $|b| = n$, $b\gamma b^{-1} = \gamma^\tau$, $mn = |G|$, $\gcd(\tau - 1, m) = 1$, and $\tau^n \equiv 1 \pmod{m}$.

Notation 2.3.4 For τ as defined in Proposition 2.3.3 (4),we use τ^{-1} to denote the inverse of τ modulo m (so $\tau^{-1} \equiv \tau^{n-1} \pmod{m}$).

2.4 Cayley graphs that contain a Hamiltonian cycle

Within this subsection, we show that there exists a Hamiltonian cycle in some specific Cayley graphs. The following proposition shows that in the proof of Theorem 1.4 we can assume $|G|$ is square-free, because the cases where $|G|$ is not square-free have been already proved.

Proposition 2.4.1 *Assume:*

- $|G| = 2pqr$*, where* p*,* q *and* r *are distinct prime numbers, and*
- $|G|$ *is not square-free.*

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

Proof. Without loss of generality we may assume $r = 2$. Then $|G| = 4pq$. Therefore, Theorem 1.2 (2) applies. □

Proposition 2.4.2 ([20, Proposition 5.5]) *If* n *is divisible by at most three distinct primes, then every connected Cayley graph on* D_{2n} *has a Hamiltonian cycle.*

The following proposition demonstrates that we can assume $|G'|$ in Theorem 1.4 is a product of two distinct prime numbers.

Proposition 2.4.3 [13, Proposition 2.22] *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.*

According to the following proposition we can assume $|S| = 3$ to prove Theorem 1.4.

Proposition 2.4.4 ([13, Proposition 3.10]) *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.*

Lemma 2.4.5 (cf. [6, Case 2 of proof of Theorem 1.1, pp. 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 $\mathrm{Cay}(G; S)$ *contains a Hamiltonian cycle.*

Lemma 2.4.6 ([6, 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.*

2.5 Specific sets that generate G

This subsection 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 2.5.1 *Assume $G = (\mathcal{C}_2 \times \mathcal{C}_r) \ltimes G'$, and $G' = \mathcal{C}_p \times \mathcal{C}_q$. Also, assume $C_{G'}(\mathcal{C}_r) = \mathcal{C}_q$ and $\mathcal{C}_q \nsubseteq C_{G'}(\mathcal{C}_2)$. If (a, b) is one of the following ordered pairs*

(1) $(a_2 a_r^m \gamma_q, a_2 a_r^j \gamma_q^k \gamma_p)$, where $m \not\equiv 0 \pmod r$ and $k \not\equiv 1 \pmod q$,
(2) $(a_2 a_r^m \gamma_q, a_r^j \gamma_q^k \gamma_p)$, where $m \not\equiv 0 \pmod r$ and $k \not\equiv 0 \pmod q$,
(3) $(a_2 a_r^m, a_2^i a_r^j \gamma_q^k \gamma_p)$, where $m \not\equiv 0 \pmod r$ and $k \not\equiv 0 \pmod q$,
(4) $(a_r^m \gamma_q, a_2 a_r^j \gamma_q^k \gamma_p)$, where $m \not\equiv 0 \pmod r$,

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 $\breve{G} = G/(\mathcal{C}_r \ltimes \mathcal{C}_p) \cong D_{2q}$ and $\breve{G} = G/C_q$.

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

The pair $(\breve{a}, \breve{b})$ is $(a_2\gamma_q, a_2\gamma_q^k)$ where $k \not\equiv 1 \pmod q$, or $(a_2\gamma_q, \gamma_q^k)$ where $k \not\equiv 0 \pmod q$, or $(a_2, a_2^i\gamma_q^k)$ where $k \not\equiv 0 \pmod q$, or $(\gamma_q, a_2\gamma_q^k)$. 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 2.5.2 *Assume $G = (\mathcal{C}_2 \times \mathcal{C}_r) \ltimes G'$, and $G' = \mathcal{C}_p \times \mathcal{C}_q$. Also, assume $C_{G'}(\mathcal{C}_r) = \{e\}$. If (a, b) is one of the following ordered pairs:*

(1) $(a_2 a_r, a_2^i a_r^j \gamma_q^k \gamma_p)$, where $k \not\equiv 0 \pmod q$,
(2) $(a_r^m \gamma_q, a_2 a_r^j \gamma_p)$, where $m \not\equiv 0 \pmod r$, and $j \not\equiv 0 \pmod r$,
(3) $(a_r, a_2 a_r^j \gamma_q^k \gamma_p)$, where $k \not\equiv 0 \pmod q$,
(4) $(a_2 a_r^m \gamma_q, a_2^i a_r^j \gamma_p)$, where $m \not\equiv 0 \pmod r$ and $j \not\equiv 0 \pmod r$,

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 2.5.1, since a_r does not centralize $\mathcal{C}_p$, it is clear in each of (1)–(4) that $\breve{a}$ does not centralize γ_p (and γ_p is one of the factors in $\breve{b}$), so $\breve{G}$ is not abelian.

In (1)–(4), γ_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_r. Since a_r does not centralize γ_q, it follows that $\widehat{G}$ is not abelian. □

Lemma 2.5.3 *Assume*

- $G = (\mathcal{C}_2 \times \mathcal{C}_r) \ltimes (\mathcal{C}_p \times \mathcal{C}_q)$, *where* p, q, *and* r *are distinct odd primes,*
- $a_r \gamma_p a_r^{-1} = \gamma_p^{\widehat{\tau}}$, *where* $\widehat{\tau}^r \equiv 1 \pmod{p}$, *and*
- $a_r \gamma_q a_r^{-1} = \gamma_q^{\check{\tau}}$, *where* $\check{\tau}^r \equiv 1 \pmod{q}$.

If $\widehat{\tau}^j \equiv \pm 1 \pmod{p}$ *(or* $\check{\tau}^k \equiv \pm 1 \pmod{q}$*), where* $1 \leqslant j, k \leqslant r-1$, *then* $\widehat{\tau} \equiv 1 \pmod{p}$ *(or* $\check{\tau} \equiv 1 \pmod{q}$*).*

Proof. Assume $\widehat{\tau}^j \equiv \pm 1 \pmod{p}$; then $\widehat{\tau}^{2j} \equiv 1 \pmod{p}$. We also know that $\widehat{\tau}^r \equiv 1 \pmod{p}$. So $\widehat{\tau}^d \equiv 1 \pmod{p}$, where $d = \gcd(2j, r)$. Since $1 \leqslant j \leqslant r-1$ and r is an odd prime, it follows that $d = 1$. Thus $\widehat{\tau} \equiv 1 \pmod{p}$. A similar argument works when $\check{\tau}^k \equiv \pm 1 \pmod{q}$ to show $\check{\tau} \equiv 1 \pmod{q}$. □

3 Proof of the Main Result

In this section we prove Theorem 1.4, which is the main result. When p, q, r, and s are distinct odd primes, then Theorem 1.3 applies. Therefore we may assume without loss of generality that $s = 2$. We are given a generating set S of a finite group G of order $2pqr$, where p, q and r are distinct odd prime numbers, and $|S| \geqslant 3$. We prove that $\mathrm{Cay}(G; S)$ has a Hamiltonian cycle. The proof is a long case-by-case analysis. (See Figure 1 for outlines of the cases that are considered.) Here are our main assumptions.

Assumption 3.0.1 We assume:

(1) $p, q, r \geqslant 5$, for otherwise Theorem 1.2 (2) applies.
(2) $|G|$ is square-free; otherwise Proposition 2.4.1 applies.
(3) $G' \cap Z(G) = \{e\}$, by Proposition 2.3.3 (2).
(4) $G \cong \mathcal{C}_n \ltimes G'$, by Proposition 2.3.3 (3).
(5) $|G'|$ is odd by Corollary 2.3.2. If $|G'| = 1$, then Lemma 2.2.1 applies. If $|G'| = pqr$, then Proposition 2.4.2 applies. So we can assume $|G'| \in \{pq, pr, qr\}$. Without loss of generality we may assume $|G'| = pq$, so $G' = \mathcal{C}_p \times \mathcal{C}_q$.
(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 1.2. By Assumption 3.0.1 (3), $\langle s \rangle \cap Z(G) = \{e\}$, and therefore Lemma 2.2.7 (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, i.e. removal of any element from the generating set S leaves a set which does not generate G.)
(8) When $|S| \geqslant 4$, Proposition 2.4.4 applies, so we assume $|S| = 3$.

$|S| = 3$.

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

i. $C_{G'}(\mathcal{C}_r) \neq \{e\}$ (Section 3.1).

1. $a = a_2$ and $b = a_r\gamma_q$.
2. $a = a_2$ and $b = a_2a_r\gamma_q$.
3. $a = a_2a_r$ and $b = a_2\gamma_q$.
4. $a = a_2a_r$ and $b = a_r^m\gamma_q$.
5. $a = a_2a_r$ and $b = a_2a_r^m\gamma_q$.

ii. $\widehat{S}$ is minimal (Section 3.2).

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

i. $C_{G'}(\mathcal{C}_2) = \mathcal{C}_p \times \mathcal{C}_q$ (Section 3.3).

1. $a = a_r$ and $b = a_2\gamma_q$.
2. $a = a_r$ and $b = a_2a_r^m\gamma_q$.
3. $a = a_2a_r$ and $b = a_r^m\gamma_q$.
4. $a = a_2a_r$ and $b = a_2\gamma_q$.
5. $a = a_2a_r$ and $b = a_2a_r^m\gamma_q$.

ii. $C_{G'}(\mathcal{C}_2) \neq \{e\}$ (Section 3.4).

1. $a = a_2a_r$ and $b = a_2a_r^m\gamma_q$.
2. $a = a_2a_r$ and $b = a_2\gamma_q$.
3. $a = a_2a_r$ and $b = a_r^m\gamma_q$.
4. $a = a_r$ and $b = a_2\gamma_q$.

iii. $C_{G'}(\mathcal{C}_2) = \{e\}$ (Section 3.5).

1. $a = a_2a_r$ and $b = a_2a_r^m\gamma_q$.
2. $a = a_2a_r$ and $b = a_2\gamma_q$.
3. $a = a_2a_r$ and $b = a_r^m\gamma_q$.
4. $a = a_r$ and $b = a_2\gamma_q$.

Figure 1: Outline of the cases in the proof of Theorem 1.4

3.1 Assume $|S| = 3$ and $C_{G'}(\mathcal{C}_r) \neq \{e\}$

In this subsection we prove the part of Theorem 1.4 where $|S| = 3$, and $C_{G'}(\mathcal{C}_r) \neq \{e\}$. Recall that $\overline{G} = G/G'$, $\breve{G} = G/\mathcal{C}_q$ and $\widehat{G} = G/\mathcal{C}_p$.

Proposition 3.1.1 *Assume*

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

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

Proof. Let $S = \{a, b, c\}$. If $C_{G'}(\mathcal{C}_r) = \mathcal{C}_p \times \mathcal{C}_q$, then since $G' \cap Z(G) = \{e\}$ (see Proposition 2.3.3 (2)), we conclude that $C_{G'}(\mathcal{C}_2) = \{e\}$. So we have

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

Therefore Lemma 2.4.6 applies.

Since $C_{G'}(\mathcal{C}_r) \neq \{e\}$, we may assume $C_{G'}(\mathcal{C}_r) = \mathcal{C}_q$ by interchanging q and p if necessary. Since $\mathcal{C}_r$ centralizes $\mathcal{C}_q$ and $Z(G) \cap G' = \{e\}$ (by Proposition 2.3.3 (2)), this implies $\mathcal{C}_2$ inverts $\mathcal{C}_q$. Thus,

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

Now if $\widehat{S}$ is minimal, then Lemma 2.4.5 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 $\langle a, b\rangle = D_{2q} \times \mathcal{C}_r$ after replacing a and b by conjugates. The projection of (a, b) to D_{2q} must be of the form (a_2, γ_q) or $(a_2, a_2\gamma_q)$, where a_2 is reflection and γ_q is a rotation. (Also note that $\widehat{b} \neq \gamma_q$ because $S \cap G' = \varnothing$ by Assumption 3.0.1 (6).) Therefore (a, b) must have one of the following forms:

(1) $(a_2, a_r\gamma_q)$,
(2) $(a_2, a_2a_r\gamma_q)$,
(3) $(a_2a_r, a_2\gamma_q)$,
(4) $(a_2a_r, a_r^m\gamma_q)$, where $1 \leqslant m \leqslant r-1$,
(5) $(a_2a_r, a_2a_r^m\gamma_q)$, where $1 \leqslant m \leqslant r-1$.

Let c be the third element of S. We may write $c = a_2^i a_r^j \gamma_q^k \gamma_p$ with $0 \leqslant i \leqslant 1$, $0 \leqslant j \leqslant r-1$ 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 $a_r\gamma_p a_r^{-1} = \gamma_p^{\widehat{\tau}}$ where $\widehat{\tau}^r \equiv 1 \pmod{p}$. Also, $\widehat{\tau} \not\equiv 1 \pmod{p}$ since $C_{G'}(\mathcal{C}_r) = \mathcal{C}_q$. Therefore, we conclude that $\widehat{\tau}^{r-1} + \widehat{\tau}^{r-2} + \cdots + 1 \equiv 0 \pmod{p}$. Note that this implies $\widehat{\tau} \not\equiv -1 \pmod{p}$.

Case 3.1.1 Assume $a = a_2$ and $b = a_r\gamma_q$.

Subcase 3.1.1.1 Assume $i \neq 0$. Then $c = a_2 a_r^j \gamma_q^k \gamma_p$. Thus, by Lemma 2.5.1 (4), $\langle b, c\rangle = G$, which contradicts the minimality of S.

Subcase 3.1.1.2 Assume $i = 0$. So, $j \neq 0$. We have $c = a_r^j \gamma_q^k \gamma_p$. We may assume j is even by replacing c with its inverse and j with $r-j$ if necessary. Consider $\overline{G} = \mathcal{C}_2 \times \mathcal{C}_r$. We have $\overline{a} = a_2$, $\overline{b} = a_r$ and $\overline{c} = a_r^j$. We have

$$C_1 = (\overline{c}, (\overline{a}, \overline{b})^{r-j}, \overline{b}^{j-1}, \overline{a}, \overline{b}^{-(j-1)})$$

and

$$C_2 = (\overline{c}, \overline{b}^{r-j-1}, \overline{c}, \overline{b}^{-(j-2)}, \overline{a}, \overline{b}^{r-1}, \overline{a})$$

and

$$C_3 = (\overline{c}, \overline{a}, \overline{b}^{r-j-1}, \overline{a}, \overline{b}^{-(r-j-2)}, \overline{c}^{-1}, \overline{b}^{j-2}, \overline{a}, \overline{b}^{-(j-1)}, \overline{a})$$

as Hamiltonian cycles in $\mathrm{Cay}(\overline{G}; \overline{S})$. Now since there is one occurrence of c in C_1, by Lemma 2.2.6 the subgroup generated by $\mathbb{V}(C_1)$ contains $\mathcal{C}_p$. Also,

$$\begin{aligned}
\mathbb{V}(C_1) &= c(ab)^{r-j} b^{j-1} a b^{-(j-1)} \\
&\equiv \gamma_q^k \cdot (a_2 \cdot \gamma_q)^{r-j} \cdot \gamma_q^{j-1} \cdot a_2 \cdot \gamma_q^{-(j-1)} \pmod{\mathcal{C}_r \ltimes \mathcal{C}_p} \\
&= \gamma_q^k a_2 \gamma_q \gamma_q^{j-1} a_2 \gamma_q^{-j+1} \\
&= \gamma_q^{k-2j+1}.
\end{aligned}$$

We can assume this does not generate $\mathcal{C}_q$, for otherwise Factor Group Lemma 2.2.4 applies. Therefore,

$$0 \equiv k - 2j + 1 \pmod q. \tag{3.1.A}$$

Now we calculate the voltage of C_2.

$$\begin{aligned}
\mathbb{V}(C_2) &= cb^{r-j-1}cb^{-(j-2)}ab^{r-1}a \\
&\equiv a_r^j\gamma_p \cdot a_r^{r-j-1} \cdot a_r^j\gamma_p \cdot a_r^{-(j-2)} \cdot a_2 \cdot a_r^{r-1} \cdot a_2 \pmod{\mathcal{C}_q} \\
&= a_r^j\gamma_p a_r^{-1}\gamma_p a_r^{-j+1} \\
&= \gamma_p^{\hat{\tau}^j - \hat{\tau}^{j-1}} \\
&= \gamma_p^{\hat{\tau}^{j-1}(\hat{\tau}-1)},
\end{aligned}$$

which generates $\mathcal{C}_p$. Also, we have

$$\begin{aligned}
\mathbb{V}(C_2) &= cb^{r-j-1}cb^{-(j-2)}ab^{r-1}a \\
&\equiv \gamma_q^k \cdot \gamma_q^{r-j-1} \cdot \gamma_q^k \cdot \gamma_q^{-(j-2)} \cdot a_2 \cdot \gamma_q^{r-1} \cdot a_2 \pmod{\mathcal{C}_r \ltimes \mathcal{C}_p} \\
&= \gamma_q^{2k-2j+2}.
\end{aligned}$$

We may assume this does not generate $\mathcal{C}_q$, for otherwise Factor Group Lemma 2.2.4 applies. Thus,

$$0 \equiv 2k - 2j + 2 \pmod q.$$

Dividing by 2 yields

$$k - j + 1 \equiv 0 \pmod q.$$

By replacing the above equation in (3.1.A), we have

$$j \equiv 0 \pmod q. \tag{3.1.B}$$

Now we calculate the voltage of C_3.

$$\begin{aligned}
\mathbb{V}(C_3) &= cab^{r-j-1}ab^{-(r-j-2)}c^{-1}b^{j-2}ab^{-(j-1)}a \\
&\equiv a_r^j\gamma_p \cdot a_2 \cdot a_r^{r-j-1} \cdot a_2 \cdot a_r^{-(r-j-2)} \cdot \gamma_p^{-1}a_r^{-j} \cdot a_r^{j-2} \cdot a_2 \cdot a_r^{-(j-1)} \cdot a_2 \pmod{\mathcal{C}_q} \\
&= a_r^j\gamma_p a_r \gamma_p^{-1} a_r^{-j-1} \\
&= \gamma_p^{\hat{\tau}^j - \hat{\tau}^{j+1}} \\
&= \gamma_p^{\hat{\tau}^j(1-\hat{\tau})},
\end{aligned}$$

which generates $\mathcal{C}_p$. Also, we have

$$\begin{aligned}
\mathbb{V}(C_3) &= cab^{r-j-1}ab^{-(r-j-2)}c^{-1}b^{j-2}ab^{-(j-1)}a \\
&\equiv \gamma_q^k \cdot a_2 \cdot \gamma_q^{r-j-1} \cdot a_2 \cdot \gamma_q^{-(r-j-2)} \cdot \gamma_q^{-k} \cdot \gamma_q^{j-2} \cdot a_2 \cdot \gamma_q^{-(j-1)} \cdot a_2 \pmod{\mathcal{C}_r \ltimes \mathcal{C}_p}
\end{aligned}$$

$$= \gamma_q^{4j-2r}.$$

We can assume this does not generate $\mathcal{C}_q$, for otherwise Factor Group Lemma 2.2.4 applies. Therefore,

$$0 \equiv 4j - 2r \pmod{q}.$$

Dividing by 2 yields

$$2j - r \equiv 0 \pmod{q}.$$

By replacing (3.1.B) in the above equation, we have $r \equiv 0 \pmod{q}$, which contradicts the assumption that q and r are distinct primes.

Case 3.1.2 Assume $a = a_2$ and $b = a_2 a_r \gamma_q$.

Subcase 3.1.2.1 Assume $j = 0$. Then $i \neq 0$. If $k \neq 1$, then $c = a_2 \gamma_q^k \gamma_p$. Thus, by Lemma 2.5.1 (1), $\langle b, c \rangle = G$, which contradicts the minimality of S. We may therefore assume $k = 1$. Then $c = a_2 \gamma_q \gamma_p$.

Consider $\overline{G} = \mathcal{C}_2 \times \mathcal{C}_r$. Then $\overline{a} = \overline{c} = a_2$ and $\overline{b} = a_2 a_r$. We have $C = (\overline{c}, \overline{b}^{r-1}, \overline{a}, \overline{b}^{-(r-1)})$ as a Hamiltonian cycle in $\mathrm{Cay}(\overline{G}; \overline{S})$. Since there is one occurrence of c in C, by Lemma 2.2.6 the subgroup generated by $\mathbb{V}(C)$ contains $\mathcal{C}_p$. Also,

$$\begin{aligned}
\mathbb{V}(C) &= c b^{r-1} a b^{-(r-1)} \\
&\equiv a_2 \gamma_q \cdot (a_2 \gamma_q)^{r-1} \cdot a_2 \cdot (a_2 \gamma_q)^{-(r-1)} \pmod{\mathcal{C}_r \ltimes \mathcal{C}_p} \\
&= \gamma_q^{-1},
\end{aligned}$$

which generates $\mathcal{C}_q$. Therefore the subgroup generated by $\mathbb{V}(C)$ is G'. So Factor Group Lemma 2.2.4 applies.

Subcase 3.1.2.2 Assume $i \neq 0$ and $j \neq 0$. If $k \neq 1$, then $c = a_2 a_r^j \gamma_q^k \gamma_p$. So, by Lemma 2.5.1 (1), $\langle b, c \rangle = G$, which contradicts the minimality of S. Therefore we may assume $k = 1$. Then $c = a_2 a_r^j \gamma_q \gamma_p$. We may also assume that j is odd by replacing c with its inverse and j with $r - j$ if necessary. Consider $\overline{G} = \mathcal{C}_2 \times \mathcal{C}_r$.

Subsubcase 3.1.2.2.1 Assume $j = 1$. Then $c = a_2 a_r \gamma_q \gamma_p$. So $\overline{b} = \overline{c} = a_2 a_r$. We have $C_1 = (\overline{c}, \overline{a}, (\overline{b}, \overline{a})^{r-1})$ as a Hamiltonian cycle in $\mathrm{Cay}(\overline{G}; \overline{S})$. Since there is one occurrence of c in C_1, by Lemma 2.2.6 the subgroup generated by $\mathbb{V}(C_1)$ contains $\mathcal{C}_p$. Also,

$$\begin{aligned}
\mathbb{V}(C_1) &= c a (ba)^{r-1} \\
&\equiv a_2 \gamma_q \cdot a_2 \cdot (a_2 \gamma_q \cdot a_2)^{r-1} \pmod{\mathcal{C}_r \ltimes \mathcal{C}_p} \\
&= \gamma_q^{-r}.
\end{aligned}$$

Since $\gcd(q, r) = 1$, this implies that γ_q^{-r} generates $\mathcal{C}_q$. Therefore the subgroup generated by $\mathbb{V}(C_1)$ is G'. So Factor Group Lemma 2.2.4 applies.

Subsubcase 3.1.2.2.2 Assume $j \geqslant 3$. Then $\overline{a} = a_2$, $\overline{b} = a_2 a_r$, and $\overline{c} = a_2 a_r^j$. We have

$$C_2 = (\overline{c}, (\overline{a}, \overline{b})^{r-j-1}, \overline{a}, \overline{c}, (\overline{a}, \overline{b}^{-1})^{j-1}, \overline{a})$$

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

$$\begin{aligned}
\mathbb{V}(C_2) &= c(ab)^{r-j-1} ac(ab^{-1})^{j-1} a \\
&\equiv a_2\gamma_q \cdot (a_2 \cdot a_2\gamma_q)^{r-j-1} \cdot a_2 \cdot a_2\gamma_q \cdot (a_2 \cdot \gamma_q^{-1} a_2)^{j-1} \cdot a_2 \pmod{\mathcal{C}_r \ltimes \mathcal{C}_p} \\
&= a_2\gamma_q\gamma_q^{r-j-1}\gamma_q\gamma_q^{j-1}a_2 \\
&= a_2\gamma_q^r a_2 \\
&= \gamma_q^{-r},
\end{aligned}$$

which generates $\mathcal{C}_q$, since $\gcd(q, r) = 1$. Also,

$$\begin{aligned}
\mathbb{V}(C_2) &= c(ab)^{r-j-1} ac(ab^{-1})^{j-1} a \\
&\equiv a_2 a_r^j \gamma_p \cdot (a_2 \cdot a_2 a_r)^{r-j-1} \cdot a_2 \cdot a_2 a_r^j \gamma_p \cdot (a_2 \cdot a_r^{-1} a_2)^{j-1} \cdot a_2 \pmod{\mathcal{C}_q} \\
&= a_2 a_r^j \gamma_p a_r^{-1} \gamma_p a_r^{-j+1} a_2 \\
&= a_2 \gamma_p^{\hat{\tau}^j + \hat{\tau}^{j-1}} a_2 \\
&= \gamma_p^{\pm\hat{\tau}^{j-1}(\hat{\tau}-1)},
\end{aligned}$$

which generates $\mathcal{C}_p$. Therefore the subgroup generated by $\mathbb{V}(C_2)$ is G'. So Factor Group Lemma 2.2.4 applies.

Subcase 3.1.2.3 Assume $i = 0$, then $j \neq 0$. If $k \neq 0$, then $c = a_r^j \gamma_q^k \gamma_p$. Thus, by Lemma 2.5.1(2.5.1) $\langle b, c\rangle = G$ which contradicts the minimality of S. Therefore, we may assume $k = 0$. We may also assume j is odd, by replacing c with its inverse and j with $r - j$ if necessary. Then $c = a_r^j \gamma_p$. Consider $\overline{G} = \mathcal{C}_2 \times \mathcal{C}_r$, then $\overline{a} = a_2$, $\overline{b} = a_2 a_r$, and $\overline{c} = a_r^j$.

Subsubcase 3.1.2.3.1 Assume $j = 1$. Then $c = a_r \gamma_p$.

Suppose, for the moment, that $\mathcal{C}_2$ centralizes $\mathcal{C}_p$. We have $C_1 = ((\overline{a}, \overline{c})^{r-1}, \overline{a}, \overline{b})$ as a Hamiltonian cycle in $\mathrm{Cay}(\overline{G}; \overline{S})$. Since there is one occurrence of b in C_1, by Lemma 2.2.6 the subgroup generated by $\mathbb{V}(C_1)$ contains $\mathcal{C}_q$. Also,

$$\begin{aligned}
\mathbb{V}(C_1) &= (ac)^{r-1} ab \\
&\equiv (a_r\gamma_p)^{r-1} \cdot a_r \pmod{\mathcal{C}_2 \ltimes \mathcal{C}_q} \\
&= \gamma_p^{\hat{\tau} + \hat{\tau}^2 + \ldots + \hat{\tau}^{r-1}} \\
&= \gamma_p^{-1},
\end{aligned}$$

which generates $\mathcal{C}_p$. Therefore the subgroup generated by $\mathbb{V}(C_1)$ is G'. So Factor Group Lemma 2.2.4 applies.

Now we assume $\mathcal{C}_2$ does not centralize $\mathcal{C}_p$. We have

$$C_2 = (\overline{b}^{r-2}, \overline{a}, \overline{b}^{-(r-2)}, \overline{c}^{-1}, \overline{a}, \overline{c})$$

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

$$\begin{aligned}
\mathbb{V}(C_2) &= b^{r-2}ab^{-(r-2)}c^{-1}ac \\
&\equiv (a_2a_r)^{r-2} \cdot a_2 \cdot (a_2a_r)^{-(r-2)} \cdot \gamma_p^{-1}a_r^{-1} \cdot a_2 \cdot a_r\gamma_p \pmod{\mathcal{C}_q} \\
&= a_2a_r^{r-2}a_2a_r^{-r+2}a_2\gamma_p^{-1}a_r^{-1}a_2a_r\gamma_p \\
&= \gamma_p^2,
\end{aligned}$$

since $\gcd(2,p) = 1$, this implies γ_p^2 generates $\mathcal{C}_p$. Also,

$$\begin{aligned}
\mathbb{V}(C_2) &= b^{r-2}ab^{-(r-2)}c^{-1}ac \\
&\equiv (a_2\gamma_q)^{r-2} \cdot a_2 \cdot (a_2\gamma_q)^{-(r-2)} \cdot a_2 \pmod{\mathcal{C}_r \ltimes \mathcal{C}_p} \\
&= a_2\gamma_q a_2\gamma_q^{-1}a_2a_2 \\
&= \gamma_q^{-2},
\end{aligned}$$

since $\gcd(2,q) = 1$, this implies γ_q^{-2} generates $\mathcal{C}_q$. Therefore, the subgroup generated by $\mathbb{V}(C_2)$ is G'. So, Factor Group Lemma 2.2.4 applies.

Subsubcase 3.1.2.3.2 Assume $j \neq 1$. We have

$$C_3 = (\overline{c}, \overline{b}^{-1}, \overline{a}, \overline{b}^2, \overline{a}, \overline{c}^{-1}, \overline{b}^{j-3}, \overline{a}, \overline{b}^{-(r-4)}, \overline{a}, \overline{b}^{r-j-2})$$

as a Hamiltonian cycle in $\mathrm{Cay}(\overline{G};\overline{S})$. Considering the fact that $\mathcal{C}_2$ might centralize $\mathcal{C}_p$ or not, we calculate the voltage of C_3.

$$\begin{aligned}
\mathbb{V}(C_3) &= cb^{-1}ab^2ac^{-1}b^{j-3}ab^{-(r-4)}ab^{r-j-2} \\
&\equiv a_r^j\gamma_p \cdot a_r^{-1}a_2 \cdot a_2 \cdot (a_2a_r)^2 \cdot a_2 \cdot \gamma_p^{-1}a_r^{-j} \\
&\quad \cdot (a_2a_r)^{j-3} \cdot a_2 \cdot (a_2a_r)^{-(r-4)} \cdot a_2 \cdot (a_2a_r)^{r-j-2} \pmod{\mathcal{C}_q} \\
&= a_r^j\gamma_p a_r^{-1}a_r^2a_2\gamma_p^{-1}a_r^{-j}a_r^{j-3}a_2a_2a_r^{-r+4}a_2a_r^{r-j-2} \\
&= a_r^j\gamma_p a_r\gamma_p^{\mp 1}a_r^{-j-1} \\
&= \gamma_p^{\hat{\tau}^j \mp \hat{\tau}^{j+1}} \\
&= \gamma_p^{\hat{\tau}^j(1\mp\hat{\tau})},
\end{aligned}$$

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

$$\begin{aligned}
\mathbb{V}(C_3) &= cb^{-1}ab^2ac^{-1}b^{j-3}ab^{-(r-4)}ab^{r-j-2} \\
&\equiv \gamma_q^{-1}a_2 \cdot a_2 \cdot (a_2\gamma_q)^2 \cdot a_2 \cdot (a_2\gamma_q)^{j-3} \cdot a_2 \cdot (a_2\gamma_q)^{-(r-4)} \cdot a_2 \cdot (a_2\gamma_q)^{r-j-2} \pmod{\mathcal{C}_r \ltimes \mathcal{C}_p} \\
&= \gamma_q^{-2}.
\end{aligned}$$

Since $\gcd(2,q) = 1$, this implies γ_q^{-2} generates $\mathcal{C}_q$. Therefore the subgroup generated by $\mathbb{V}(C_3)$ is G'. So Factor Group Lemma 2.2.4 applies.

Case 3.1.3 Assume $a = a_2 a_r$ and $b = a_2\gamma_q$. Since $b = a_2\gamma_q$ is conjugate to a_2 via an element of $\mathcal{C}_q$ (which centralizes $\mathcal{C}_r$), this implies $\{a, b\}$ is conjugate to $\{a_2 a_r \gamma_q^m, a_2\}$ for some nonzero m. So Case 3.1.2 applies (after replacing γ_q with γ_q^m, and interchanging a and b).

Case 3.1.4 Assume $a = a_2 a_r$ and $b = a_r^m \gamma_q$, where $1 \leqslant m \leqslant r-1$.

Subcase 3.1.4.1 Assume $i \neq 0$. Then $c = a_2 a_r^j \gamma_q^k \gamma_p$. Thus, by Lemma 2.5.1 (4), $\langle b, c\rangle = G$, which contradicts the minimality of S.

Subcase 3.1.4.2 Assume $i = 0$. Then $j \neq 0$ and $c = a_r^j \gamma_q^k \gamma_p$. If $k \neq 0$, then by Lemma 2.5.1 (3), $\langle a, c\rangle = G$ which contradicts the minimality of S. So we may assume $k = 0$. Then $c = a_r^j \gamma_p$. We may also assume m and j are even, by replacing $\{b, c\}$ with their inverses, m with $r - m$, and j with $r - j$ if necessary. Consider $\overline{G} = \mathcal{C}_2 \times \mathcal{C}_r$. Then $\overline{a} = a_2 a_r$, $\overline{b} = a_r^m$, and $\overline{c} = a_r^j$.

Subsubcase 3.1.4.2.1 Assume $m = j$. Then $\overline{b} = \overline{c}$. We have

$$C_1 = (\overline{c}^{-(r-1)}, \overline{a}^{-1}, \overline{b}^{r-1}, \overline{a})$$

as a Hamiltonian cycle in $\mathrm{Cay}(\overline{G}; \overline{S})$. Since $c^r = e$, this implies $c^{-(r-1)} = c = a_r^j \gamma_p$. This is the only occurrence of γ_p in $\mathbb{V}(C_1)$. So the subgroup generated by $\mathbb{V}(C_1)$ contains $\mathcal{C}_p$. Similarly, since $b^r = e$, this implies $b^{r-1} = b^{-1} = \gamma_q^{-1} a_r^{-m}$. This is the only occurrence of γ_q in $\mathbb{V}(C_1)$. So the subgroup generated by $\mathbb{V}(C_1)$ contains $\mathcal{C}_q$. Hence the subgroup generated by $\mathbb{V}(C_1)$ contains G'. Therefore, Factor Group Lemma 2.2.4 applies.

Subsubcase 3.1.4.2.2 Assume $m \neq j$, and $j = 2$. Then we have $c = a_r^2 \gamma_p$. We also have

$$C_2 = (\overline{b}, \overline{c}^{-(m-2)/2}, \overline{a}^{-1}, \overline{c}^{m/2}, \overline{a}^{2r-m-1})$$

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 γ_q, by Lemma 2.2.6 we conclude that the subgroup generated by $\mathbb{V}(C_2)$ contains $\mathcal{C}_q$. Now by considering the fact that $\mathcal{C}_2$ might centralize $\mathcal{C}_p$ or not, we have

$$\begin{aligned}
\mathbb{V}(C_2) &= b c^{-(m-2)/2} a^{-1} c^{m/2} a^{2r-m-1} \\
&\equiv a_r^m \cdot (a_r^2\gamma_p)^{-(m-2)/2} \cdot a_r^{-1} a_2 \cdot (a_r^2 \gamma_p)^{m/2} \cdot (a_2 a_r)^{2r-m-1} \pmod{\mathcal{C}_q} \\
&= a_r^m (a_r^2\gamma_p)^{-(m-2)/2} a_r^{-1} a_2 (a_r^2\gamma_p)^{m/2} a_2 a_r^{-m-1} \\
&= a_r^m (\gamma_p^{\widehat{\tau}^2 + (\widehat{\tau}^2)^2 + \cdots + (\widehat{\tau}^2)^{(m-2)/2}} a_r^{(m-2)})^{-1} a_r^{-1} a_2 (\gamma_p^{\widehat{\tau}^2 + (\widehat{\tau}^2)^2 + \cdots + (\widehat{\tau}^2)^{m/2}} a_r^m) a_2 a_r^{-m-1} \\
&= a_r^m a_r^{-(m-2)} \gamma_p^{-\widehat{\tau}^2(1 + \widehat{\tau}^2 + \cdots + (\widehat{\tau}^2)^{(m-4)/2})} a_r^{-1} \gamma_p^{\pm\widehat{\tau}^2(1+\widehat{\tau}^2 + \cdots + (\widehat{\tau}^2)^{(m-2)/2})} a_r^m a_r^{-m-1}.
\end{aligned}$$

Since $\widehat{\tau}^2 - 1 \not\equiv 0 \pmod{p}$, this implies

$$\begin{aligned}\mathbb{V}(C_2) &= a_r^2 \gamma_p^{-\widehat{\tau}^2(\widehat{\tau}^{m-2}-1)/(\widehat{\tau}^2-1)} a_r^{-1} \gamma_p^{\pm\widehat{\tau}^2(\widehat{\tau}^{m}-1)/(\widehat{\tau}^2-1)} a_r^{-1} \\ &= \gamma_p^{-\widehat{\tau}^4(\widehat{\tau}^{m-2}-1)/(\widehat{\tau}^2-1) \pm \widehat{\tau}^3(\widehat{\tau}^{m}-1)/(\widehat{\tau}^2-1)} \\ &= \gamma_p^{\widehat{\tau}^3(1\mp\widehat{\tau})(-\widehat{\tau}^{m-1}\mp 1)/(\widehat{\tau}^2-1)}.\end{aligned}$$

We may assume that this does not generate $\mathcal{C}_p$, for otherwise the Factor Group Lemma 2.2.4 applies. Therefore $\widehat{\tau} \equiv \pm 1 \pmod{p}$ or $\widehat{\tau}^{m-1} \equiv \pm 1 \pmod{p}$. The first case is impossible. So we may assume $\widehat{\tau}^{m-1} \equiv \pm 1 \pmod{p}$. Thus $\widehat{\tau}^{2(m-1)} \equiv 1 \pmod{p}$. We also know that $\widehat{\tau}^r \equiv 1 \pmod{p}$. So we have $\widehat{\tau}^d \equiv 1 \pmod{p}$, where $d = \gcd(2(m-1), r)$. Since $\gcd(2, r) = 1$ and $2 \leqslant m \leqslant r-1$, it follows that $d = 1$, which contradicts the fact that $\widehat{\tau} \not\equiv 1 \pmod{p}$.

Subsubcase 3.1.4.2.3 Assume $m \neq j$, and $j \neq 2$. We have

$$C_3 = (\overline{b}, \overline{c}, \overline{a}, \overline{c}^{-1}, \overline{b}^{-1}, \overline{a}^{m-2}, \overline{c}, \overline{a}^{-(j-3)}, \overline{c}, \overline{a}^{2r-m-j-2})$$

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

$$\begin{aligned}\mathbb{V}(C_3) &= bcac^{-1}b^{-1}a^{m-2}ca^{-(j-3)}ca^{2r-m-j-2} \\ &\equiv \gamma_q \cdot a_2 \cdot \gamma_q^{-1} \cdot a_2^{m-2} \cdot a_2^{-j+3} \cdot a_2^{2r-m-j-2} \pmod{\mathcal{C}_r \ltimes \mathcal{C}_p} \\ &= \gamma_q^2\end{aligned}$$

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

$$\begin{aligned}\mathbb{V}(C_3) &= bcac^{-1}b^{-1}a^{m-2}ca^{-(j-3)}ca^{2r-m-j-2} \\ &\equiv a_r^m \cdot a_r^j \gamma_p \cdot a_2 a_r \cdot \gamma_p^{-1} a_r^{-j} \cdot a_r^{-m} \cdot (a_2 a_r)^{m-2} \\ &\cdot a_r^j \gamma_p \cdot a_r^{-j+3} a_2^{-j+3} \cdot a_r^j \gamma_p \cdot (a_2 a_r)^{2r-m-j-2} \pmod{\mathcal{C}_q} \\ &= a_r^{m+j} \gamma_p a_2 a_r \gamma_p^{-1} a_r^{-2} \gamma_p a_r^3 a_2 \gamma_p a_r^{-m-j-2} \\ &= a_r^{m+j} \gamma_p a_r \gamma_p^{\mp 1} a_r^{-2} \gamma_p^{\pm 1} a_r^3 \gamma_p a_r^{-m-j-2} \\ &= \gamma_p^{\widehat{\tau}^{m+j} \mp \widehat{\tau}^{m+j+1} \pm \widehat{\tau}^{m+j-1} + \widehat{\tau}^{m+j+2}} \\ &= \gamma_p^{\widehat{\tau}^{m+j-1}(\widehat{\tau}^3 \mp \widehat{\tau}^2 + \widehat{\tau} \pm 1)}.\end{aligned}$$

We may assume this does not generate $\mathcal{C}_p$, for otherwise Factor Group Lemma 2.2.4 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

$$0 \equiv \widehat{\tau}^3 - \widehat{\tau}^2 + \widehat{\tau} + 1 \pmod{p}. \tag{3.1.C}$$

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 3.1.C 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

$$0 \equiv \widehat{\tau}^3 + \widehat{\tau}^2 + \widehat{\tau} - 1 \pmod{p}. \tag{3.1.D}$$

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 (3.1.D) 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 3.1.5 Assume $a = a_2 a_r$, $b = a_2 a_r^m \gamma_q$, where $1 \leqslant m \leqslant r - 1$.

Subcase 3.1.5.1 Assume $i \neq 0$. Then $c = a_2 a_r^j \gamma_q^k \gamma_p$. If $k \neq 1$, then, by Lemma 2.5.1 (1), $\langle b, c \rangle = G$, which contradicts the minimality of S. So we may assume $k = 1$. Then $c = a_2 a_r^j \gamma_q \gamma_p$. Thus, by Lemma 2.5.1 (3), $\langle a, c \rangle = G$, which contradicts the minimality of S.

Subcase 3.1.5.2 Assume $i = 0$. Then $j \neq 0$ and $c = a_r^j \gamma_q^k \gamma_p$. If $k \neq 0$, then by Lemma 2.5.1 (2), $\langle b, c \rangle = G$, which contradicts the minimality of S. So we may assume $k = 0$. Then $c = a_r^j \gamma_p$.

Consider $\overline{G} = \mathcal{C}_2 \times \mathcal{C}_r$. Then $\overline{a} = a_2 a_r$, $\overline{b} = a_2 a_r^m$, and $\overline{c} = a_r^j$. We may assume m is odd by replacing b with b^{-1} (and m with $r - m$) if necessary. Note that this implies $\overline{b} = \overline{a}^m$. Also, we have $|\overline{a}| = |\overline{b}| = 2r$ and $|\overline{c}| = r$.

Subsubcase 3.1.5.2.1 Assume $m = 1$. Then $\overline{a} = \overline{b}$. We have

$$C_1 = (\overline{c}^{r-1}, \overline{b}, \overline{c}^{-(r-1)}, \overline{a}^{-1})$$

as a Hamiltonian cycle in $\mathrm{Cay}(\overline{G}; \overline{S})$. Since there is one occurrence of b in C_1, and it is the only generator of G that contains γ_q, by Lemma 2.2.6 we conclude that the subgroup generated by $\mathbb{V}(C_1)$ contains $\mathcal{C}_q$. Also, since $c^r = e$, this implies $c^{r-1} = c^{-1} = \gamma_p^{-1} a_r^{-j}$, and $c^{-(r-1)} = c = a_r^j \gamma_p$. Now by considering the fact that $\mathcal{C}_2$ might centralize $\mathcal{C}_p$ or not we have

$$\begin{aligned}
\mathbb{V}(C_1) &= c^{r-1} b c^{-(r-1)} a^{-1} \\
&\equiv \gamma_p^{-1} a_r^{-j} \cdot a_2 a_r \cdot a_r^j \gamma_p \cdot a_r^{-1} a_2 \pmod{\mathcal{C}_q} \\
&= \gamma_p^{-1} a_r \gamma_p^{\pm 1} a_r^{-1} \\
&= \gamma_p^{-1 \pm \widehat{\tau}},
\end{aligned}$$

which generates $\mathcal{C}_p$. Therefore, the subgroup generated by $\mathbb{V}(C_1)$ is G'. So Factor Group Lemma 2.2.4 applies.

Subsubcase 3.1.5.2.2 Assume $m \neq 1$ and $j = 2$. Then $c = a_r^2 \gamma_p$. We have

$$C_2 = (\overline{b}, \overline{c}^{-(m-1)/2}, \overline{a}, \overline{c}^{(m-1)/2}, \overline{a}^{2r-m-1})$$

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 γ_q, by Lemma 2.2.6 we conclude that the subgroup generated by $\mathbb{V}(C_2)$ contains $\mathcal{C}_q$. Considering the fact that $\mathcal{C}_2$ might centralize $\mathcal{C}_p$ or not we have

$$\begin{aligned}
\mathbb{V}(C_2) &= b c^{-(m-1)/2} a c^{(m-1)/2} a^{2r-m-1} \\
&\equiv a_2 a_r^m \cdot (a_r^2 \gamma_p)^{-(m-1)/2} \cdot a_2 a_r \cdot (a_r^2 \gamma_p)^{(m-1)/2} \cdot (a_2 a_r)^{2r-m-1} \pmod{\mathcal{C}_q} \\
&= a_2 a_r^m (\gamma_p^{\widehat{\tau}^2 + (\widehat{\tau}^2)^2 + \cdots + (\widehat{\tau}^2)^{(m-1)/2}} a_r^{(m-1)})^{-1} a_2 a_r (\gamma_p^{\widehat{\tau}^2 + (\widehat{\tau}^2)^2 + \cdots + (\widehat{\tau}^2)^{(m-1)/2}} a_r^{(m-1)}) a_r^{-m-1} \\
&= a_2 a_r^m a_r^{-m+1} \gamma_p^{-\widehat{\tau}^2(1 + \widehat{\tau}^2 + \cdots + (\widehat{\tau}^2)^{(m-3)/2})} a_2 a_r \gamma_p^{\widehat{\tau}^2(1 + \widehat{\tau}^2 + \cdots + (\widehat{\tau}^2)^{(m-3)/2})} a_r^{-2} \\
&= a_r \gamma_p^{\pm \widehat{\tau}^2(1 + \widehat{\tau}^2 + \cdots + \widehat{\tau}^2)^{(m-3)/2}} a_r \gamma_p^{\widehat{\tau}^2(1 + \widehat{\tau}^2 + \cdots + \widehat{\tau}^2)^{(m-3)/2}} a_r^{-2} \\
&= \gamma_p^{\pm \widehat{\tau}^3(\widehat{\tau}^{m-1} - 1)/(\widehat{\tau}^2 - 1) + \widehat{\tau}^4(\widehat{\tau}^{m-1} - 1)/(\widehat{\tau}^2 - 1)} \\
&= \gamma_p^{\widehat{\tau}^3(\widehat{\tau}^{m-1} - 1)(\pm 1 + \widehat{\tau})/(\widehat{\tau}^2 - 1)}.
\end{aligned}$$

We may assume this does not generate $\mathcal{C}_p$, for otherwise Factor Group Lemma 2.2.4 applies. Therefore, $\widehat{\tau}^{m-1} \equiv 1 \pmod{p}$. We also know that $\widehat{\tau}^r \equiv 1 \pmod{p}$. So $\widehat{\tau}^d \equiv 1 \pmod{p}$, where $d = \gcd(m-1, r)$. Since $2 \leqslant m \leqslant r-1$, this implies $d = 1$, which contradicts the fact that $\widehat{\tau} \not\equiv 1 \pmod{p}$.

Subsubcase 3.1.5.2.3 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 $r - j$ if necessary. This implies that $\overline{c} = \overline{a}^j$. We have

$$C_3 = (\overline{b}, \overline{c}, \overline{a}, \overline{c}^{-1}, \overline{b}^{-1}, \overline{a}^{m-2}, \overline{c}, \overline{a}^{-(j-3)}, \overline{c}, \overline{a}^{2r-m-j-2})$$

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

$$\begin{aligned}
\mathbb{V}(C_3) &= bcac^{-1}b^{-1}a^{m-2}ca^{-(j-3)}ca^{2r-m-j-2} \\
&\equiv a_2\gamma_q \cdot a_2 \cdot \gamma_q^{-1}a_2 \cdot a_2^{m-2} \cdot a_2^{-(j-3)} \cdot a_2^{2r-m-j-2} \pmod{\mathcal{C}_r \ltimes \mathcal{C}_p} \\
&= a_2\gamma_q a_2 \gamma_q^{-1} \\
&= \gamma_q^{-2}
\end{aligned}$$

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

$$\begin{aligned}
\mathbb{V}(C_3) &= bcac^{-1}b^{-1}a^{m-2}ca^{-(j-3)}ca^{2r-m-j-2} \\
&\equiv a_2a_r^m \cdot a_r^j\gamma_p \cdot a_2a_r \cdot \gamma_p^{-1}a_r^{-j} \cdot a_r^{-m}a_2 \\
&\quad \cdot a_2a_r^{m-2} \cdot a_r^j\gamma_p \cdot a_r^{-j+3}a_2 \cdot a_r^j\gamma_p \cdot a_2a_r^{2r-m-j-2} \pmod{\mathcal{C}_q} \\
&= a_r^{m+j}\gamma_p^{\pm1}a_r\gamma_p^{-1}a_r^{-2}\gamma_p a_r^3\gamma_p^{\pm1}a_r^{-m-j-2} \\
&= \gamma_p^{\pm\widehat{\tau}^{m+j} - \widehat{\tau}^{m+j+1} + \widehat{\tau}^{m+j-1} \pm \widehat{\tau}^{m+j+2}} \\
&= \gamma_p^{\widehat{\tau}^{m+j-1}(\pm\widehat{\tau}^3 - \widehat{\tau}^2 \pm \widehat{\tau} + 1)}.
\end{aligned}$$

So we may assume this does not generate $\mathcal{C}_p$, for otherwise Factor Group Lemma 2.2.4 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

$$0 \equiv t^3 - t^2 + t + 1 \pmod{p}. \tag{3.1.E}$$

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 (3.1.E) 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 $\widehat{\tau} \not\equiv \pm1 \pmod{p}$.

□

3.2 Assume $|S| = 3$ and $\widehat{S}$ is minimal

In this subsection we prove the part of Theorem 1.4 where $|S| = 3$, and $\widehat{S}$ is minimal. Recall that $\overline{G} = G/G'$ and $\widehat{G} = G/\mathcal{C}_p$.

Proposition 3.2.1 *Assume*

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

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

Proof. Let $S = \{a, b, c\}$. If $C_{G'}(\mathcal{C}_r) \neq \{e\}$, then Proposition 3.1.1 applies. Hence we may assume $C_{G'}(\mathcal{C}_r) = \{e\}$. Then we have four different cases.

Case 3.2.1 Assume $C_{G'}(\mathcal{C}_2) = \mathcal{C}_p \times \mathcal{C}_q$; thus $G = \mathcal{C}_2 \times (\mathcal{C}_r \ltimes \mathcal{C}_{pq})$. Since $\widehat{S}$ is minimal, it follows that all three elements of $\widehat{S}$ 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 2.2.5 applies with $s = a$ and $t = a^{-1}$, because there is a Hamiltonian cycle in $\mathrm{Cay}(\widehat{G}; \widehat{S})$ (see Theorem 1.2 (3)) which uses at least one edge labeled $\widehat{a}$ because $\widehat{S}$ is minimal.

Now we may assume $|a| = 2$. So $\langle a\rangle = \mathcal{C}_2$. Thus $\langle b, c\rangle = \mathcal{C}_r \ltimes \mathcal{C}_{pq}$. By Theorem 1.2 (3), there is a Hamiltonian path L in $\mathrm{Cay}(\mathcal{C}_r \ltimes \mathcal{C}_{pq}, \{b, c\})$. Therefore $LaL^{-1}a^{-1}$ is a Hamiltonian cycle in $\mathrm{Cay}(G; S)$.

Case 3.2.2 Assume $C_{G'}(\mathcal{C}_2) = \mathcal{C}_q$. Therefore,

$$\widehat{G} = G/\mathcal{C}_p = \mathcal{C}_{2r} \ltimes \mathcal{C}_q \cong \mathcal{C}_2 \times (\mathcal{C}_r \ltimes \mathcal{C}_q).$$

There is some $a \in S$ such that $|\widehat{a}| = 2$. Thus, we can assume $|a| = 2$, for otherwise Corollary 2.2.5 applies with $s = a$ and $t = a^{-1}$. (Note since $\widehat{S}$ is minimal, it follows that $\widehat{a}$ 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(3.0.1)) and each element belonging to $\widehat{S}$ has prime order, this implies $|\widehat{b}| = |\widehat{c}| = r$. We may assume $\widehat{b} = a_r$ and $\widehat{c} = a_r^j \gamma_q$, where $1 \leqslant j \leqslant r - 1$. We can also assume $b = a_r\gamma_p$, and $c = a_r^j \gamma_q \gamma_p^k$, where $0 \leqslant k \leqslant p - 1$. Since $C_{G'}(\mathcal{C}_r) = \{e\}$, we have $a_r\gamma_p a_r^{-1} = \gamma_p^{\widehat{\tau}}$ where $\widehat{\tau}^r \equiv 1 \pmod p$ and $\widehat{\tau} \not\equiv 1 \pmod p$. Thus $\widehat{\tau}^{r-1} + \widehat{\tau}^{r-2} + \ldots + 1 \equiv 0 \pmod p$. Note that this implies $\widehat{\tau} \not\equiv -1 \pmod p$. Also, we have $a_r\gamma_q a_r^{-1} = \gamma_q^{\check{\tau}}$. By using the same argument we can conclude that $\check{\tau} \not\equiv 1 \pmod q$ and $\check{\tau}^{r-1} + \check{\tau}^{r-2} + \ldots + 1 \equiv 0 \pmod q$. Note that this implies $\check{\tau} \not\equiv -1 \pmod q$.

Consider $\overline{G} = \mathcal{C}_2 \times \mathcal{C}_r$. Then $\overline{a} = a_2$, $\overline{b} = a_r$, and $\overline{c} = a_r^j$. We may assume j is odd by replacing c with its inverse and j with $r - j$ if necessary. We have

$$C_1 = (\overline{c}, (\overline{a}, \overline{b}^{-1})^j, \overline{b}^{-(r-j-1)}, \overline{a}, \overline{b}^{r-j-1})$$

and

$$C_2 = (\overline{c}, \overline{b}^{r-j-1}, \overline{a}, \overline{b}^{-(r-j-1)}, (\overline{b}^{-1}, \overline{a})^j)$$

as Hamiltonian cycles in $\mathrm{Cay}(\overline{G}; \overline{S})$. Now we calculate the voltage of C_1. Since there is one occurrence of c in C_1, and it is the only generator of G that contains γ_q, by Lemma 2.2.6 we conclude that the subgroup generated by $\mathbb{V}(C_1)$ contains $\mathcal{C}_q$. Also,

$$\begin{aligned}
\mathbb{V}(C_1) &= c(ab^{-1})^j b^{-(r-j-1)} ab^{r-j-1} \\
&\equiv a_r^j \gamma_p^k \cdot (a_2 \cdot \gamma_p^{-1} a_r^{-1})^j \cdot (a_r \gamma_p)^{-(r-j-1)} \cdot a_2 \cdot (a_r \gamma_p)^{r-j-1} \pmod{\mathcal{C}_q} \\
&= a_r^j \gamma_p^k (\gamma_p^{1-\widehat{\tau}^{-1}+\widehat{\tau}^{-2}-\cdots+\widehat{\tau}^{-(j-1)}} a_r^{-j} a_2) \\
&\cdot (\gamma_p^{\widehat{\tau}+\widehat{\tau}^2+\cdots+\widehat{\tau}^{r-j-1}} a_r^{r-j-1})^{-1} a_2 (\gamma_p^{\widehat{\tau}+\widehat{\tau}^2+\cdots+\widehat{\tau}^{r-j-1}} a_r^{r-j-1}) \\
&= a_r^j \gamma_p^{k+(1-\widehat{\tau}^{-1}+\widehat{\tau}^{-2}-\cdots+\widehat{\tau}^{-(j-1)})} a_r^{-j} a_r^{j+1} \gamma_p^{2(\widehat{\tau}+\widehat{\tau}^2+\cdots+\widehat{\tau}^{r-j-1})} a_r^{-j-1} \\
&= \gamma_p^{k\widehat{\tau}^j+\widehat{\tau}^j(1-\widehat{\tau}^{-1}+\widehat{\tau}^{-2}-\cdots+\widehat{\tau}^{-(j-1)})+2\widehat{\tau}^{j+1}(\widehat{\tau}+\widehat{\tau}^2+\cdots+\widehat{\tau}^{r-j-1})}.
\end{aligned}$$

We may assume this does not generate $\mathcal{C}_p$, for otherwise Factor Group Lemma 2.2.4 applies. Therefore,

$$\begin{aligned}
0 \equiv k\widehat{\tau}^j + \widehat{\tau}^j(1 - \widehat{\tau}^{-1} + \widehat{\tau}^{-2} - \cdots + \widehat{\tau}^{-(j-1)}) + \\
2\widehat{\tau}^{j+1}(\widehat{\tau} + \widehat{\tau}^2 + \cdots + \widehat{\tau}^{r-j-1}) \pmod{p}. \qquad (3.2.A)
\end{aligned}$$

Now we calculate the voltage of C_2. Since there is one occurrence of c in C_2, and it is the only generator of G that contains γ_q, by Lemma 2.2.6 we conclude that the subgroup generated by $\mathbb{V}(C_2)$ contains $\mathcal{C}_q$. Also,

$$\begin{aligned}
\mathbb{V}(C_2) &= cb^{r-j-1} ab^{-(r-j-1)} (b^{-1}a)^j \\
&\equiv a_r^j \gamma_p^k \cdot (a_r \gamma_p)^{r-j-1} \cdot a_2 \cdot (a_r \gamma_p)^{-(r-j-1)} \cdot (\gamma_p^{-1} a_r^{-1} \cdot a_2)^j \pmod{\mathcal{C}_q} \\
&= a_r^j \gamma_p^k (\gamma_p^{\widehat{\tau}+\widehat{\tau}^2+\cdots+\widehat{\tau}^{r-j-1}} a_r^{r-j-1}) a_2 \\
&\quad \cdot (\gamma_p^{\widehat{\tau}+\widehat{\tau}^2+\cdots+\widehat{\tau}^{r-j-1}} a_r^{r-j-1})^{-1} (\gamma_p^{-1+\widehat{\tau}^{-1}-\widehat{\tau}^{-2}+\cdots-\widehat{\tau}^{-(j-1)}} a_r^{-j} a_2) \\
&= a_r^j \gamma_p^{k+(\widehat{\tau}+\widehat{\tau}^2+\cdots+\widehat{\tau}^{r-j-1})} a_r^{-j-1} a_r^{j+1} \gamma_p^{\widehat{\tau}+\widehat{\tau}^2+\cdots+\widehat{\tau}^{r-j-1}} \gamma_p^{1-\widehat{\tau}^{-1}+\widehat{\tau}^{-2}-\cdots+\widehat{\tau}^{-(j-1)}} a_r^{-j} \\
&= a_r^j \gamma_p^{k+2(\widehat{\tau}+\widehat{\tau}^2+\cdots+\widehat{\tau}^{r-j-1})+(1-\widehat{\tau}^{-1}+\widehat{\tau}^{-2}-\cdots+\widehat{\tau}^{-(j-1)})} a_r^{-j} \\
&= \gamma_p^{k\widehat{\tau}^j+2\widehat{\tau}^j(\widehat{\tau}+\widehat{\tau}^2+\cdots+\widehat{\tau}^{r-j-1})+\widehat{\tau}^j(1-\widehat{\tau}^{-1}+\widehat{\tau}^{-2}-\cdots+\widehat{\tau}^{-(j-1)})}.
\end{aligned}$$

We can assume this does not generate $\mathcal{C}_p$, for otherwise Factor Group Lemma 2.2.4 applies. Therefore,

$$0 \equiv k\widehat{\tau}^j + 2\widehat{\tau}^j(\widehat{\tau} + \widehat{\tau}^2 + \cdots + \widehat{\tau}^{r-j-1}) + \widehat{\tau}^j(1 - \widehat{\tau}^{-1} + \widehat{\tau}^{-2} - \cdots + \widehat{\tau}^{-(j-1)}) \pmod{p}. \qquad (3.2.B)$$

Subtracting (3.2.B) from (3.2.A) we have

$$0 \equiv 2\widehat{\tau}^{j+1}(\widehat{\tau} + \widehat{\tau}^2 + \cdots + \widehat{\tau}^{r-j-1}) - 2\widehat{\tau}^j(\widehat{\tau} + \widehat{\tau}^2 + \cdots + \widehat{\tau}^{r-j-1}) \pmod{p}$$

$$= 2\hat{\tau}^r - 2\hat{\tau}^{j+1}$$
$$= 2(1 - \hat{\tau}^{j+1}).$$

This implies that $\hat{\tau}^{j+1} \equiv 1 \pmod{p}$. Since j is odd, and $1 \leqslant j \leqslant r-1$, this implies $\gcd(j+1, r) = 1$. So $\hat{\tau} \equiv 1 \pmod{p}$, which is not possible.

Case 3.2.3 Assume $C_{G'}(\mathcal{C}_2) = \mathcal{C}_p$. Therefore,

$$\breve{G} = G/\mathcal{C}_q = \mathcal{C}_{2r} \ltimes \mathcal{C}_p \cong \mathcal{C}_2 \times (\mathcal{C}_r \ltimes \mathcal{C}_p).$$

Now since $S \cap G' = \varnothing$ (see Assumption 3.0.1(3.0.1)) and $\mathcal{C}_r$ does not centralize $\mathcal{C}_p$, this implies for all $a \in S$, we have $|\breve{a}| \in \{2, r, 2r, 2p\}$. If $|\breve{a}| = 2r$, then $|\hat{a}|$ is divisible by $2r$ which contradicts the minimality of $\widehat{S}$. (Note that every element of $\widehat{S}$ has prime order.) If $|\breve{a}| = 2p$, then $|\hat{a}| = 2$ (because $\widehat{S}$ is minimal). Therefore, Corollary 2.2.5 applies with $s = a$ and $t = a^{-1}$ (Note that since $\widehat{S}$ is minimal, it follows that there is a Hamiltonian cycle in $\mathrm{Cay}(\widehat{G}; \widehat{S})$ that uses at least one labeled edge $\hat{a}$.) Thus, $|\breve{a}| \in \{2, r\}$ for all $a \in S$. This implies that $\breve{S}$ is minimal, because we need an a_2 and an a_r to generate $\mathcal{C}_2 \times \mathcal{C}_r$ and two elements whose order is divisible by 2 or r to generate $\mathcal{C}_p$. So by interchanging p and q the proof in Case 3.2.2 applies.

Case 3.2.4 Assume $C_{G'}(\mathcal{C}_2) = \{e\}$. Consider

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

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

Subcase 3.2.4.1 Assume $|c| = 2$. Then $c = a\gamma$, where $\gamma \in G'$.

Suppose, for the moment, that $\langle \gamma \rangle \neq G'$. Since $\langle \gamma \rangle \lhd G$, this implies 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', it follows that $\langle \gamma \rangle = \mathcal{C}_q$. Thus, we may assume that $a = a_2$ (by conjugation if necessary), $b = a_r\gamma_p$ and $c = a_2\gamma_q$. So $\langle b, c \rangle = \langle a_r\gamma_p, a_2\gamma_q \rangle = G$ (since $a_r\gamma_p$ and $a_2\gamma_q$ clearly generate $\overline{G}$ and do not commute modulo $\mathcal{C}_p$ or modulo $\mathcal{C}_q$, they must generate G). This contradicts the minimality of S. Therefore $\langle \gamma \rangle = G'$.

Consider $\overline{G} = \mathcal{C}_2 \times \mathcal{C}_r$. Then $\overline{a} = \overline{c}$. We have $|\overline{a}| = |\overline{c}| = 2$ and $|\overline{b}| = r$. We also have $C_1 = (\overline{c}^{-1}, \overline{b}^{-(r-1)}, \overline{a}, \overline{b}^{r-1})$ and $C_2 = (\overline{c}, \overline{b}^{r-1}, \overline{a}^{-1}, \overline{b}^{-(r-1)})$ as Hamiltonian cycles in $\mathrm{Cay}(\overline{G}; \overline{S})$. Now we calculate its voltage.

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

and

$$\mathbb{V}(C_2) = cb^{r-1}a^{-1}b^{-(r-1)} = a\gamma b^{r-1}a^{-1}b^{-(r-1)} = \gamma^{-1}ab^{r-1}a^{-1}b^{-(r-1)}.$$

We have

$$\{a^{-1}b^{-(r-1)}ab^{r-1}, ab^{r-1}a^{-1}b^{-(r-1)}\} \in G'.$$

Since $\langle a, b\rangle \neq G$, this implies that $a^{-1}b^{-(r-1)}ab^{r-1} = \gamma_p^j$ and $ab^{r-1}a^{-1}b^{-(r-1)} = \gamma_p^k$ (perhaps after interchanging p and q), where $0 \leqslant j, k \leqslant p-1$. If $j = 0$, then $a^{-1}b^{-(r-1)}ab^{r-1} = e$, so a and b^{r-1} commute. Thus a and b commute. Hence $b = a_r$, so $\langle b, c\rangle = G$, a contradiction. A similar argument works for $ab^{r-1}a^{-1}b^{-(r-1)} = e$. So $a^{-1}b^{-(r-1)}ab^{r-1} = \gamma_p^j$, and $ab^{r-1}a^{-1}b^{-(r-1)} = \gamma_p^k$, where $1 \leqslant j, k \leqslant p-1$. Thus $\mathbb{V}(C_1) = \gamma^{-1}\gamma_p^j$ and $\mathbb{V}(C_2) = \gamma^{-1}\gamma_p^k$. In this case, $\gamma_p^j \neq \gamma_p^k$ since $a^{-1}b^{-(r-1)}ab^{r-1} \neq ab^{r-1}a^{-1}b^{-(r-1)}$. Hence at least one of $\mathbb{V}(C_1)$ or $\mathbb{V}(C_2)$ generates G'. Therefore, Factor Group Lemma 2.2.4 applies.

Subcase 3.2.4.2 Assume $|c| = r$. Then $c = b^j\gamma$, where $1 \leqslant j \leqslant r-1$ and $\gamma \in G'$ (after replacing c with its conjugate if necessary).

Suppose, for the moment, that $\langle\gamma\rangle \neq G'$. Since $\langle\gamma\rangle \lhd G$, this implies 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, it follows that $\langle a, b\rangle$ 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', this implies $\langle\gamma\rangle = \mathcal{C}_q$. Therefore, we may assume that $a = a_2\gamma_p$ (by conjugation if necessary), $b = a_r$ and $c = a_r^j\gamma_q$, where $1 \leqslant j \leqslant r-1$. So $\langle a, c\rangle = \langle a_2\gamma_p, a_r^j\gamma_q\rangle = G$ (since $a_2\gamma_p$ and $a_r^j\gamma_q$ clearly generate $\overline{G}$ and do not commute modulo $\mathcal{C}_p$ or modulo $\mathcal{C}_q$, they must generate G). This contradicts the minimality of S. So $\langle\gamma\rangle = G'$.

Consider $\overline{G} = \mathcal{C}_2 \times \mathcal{C}_r$. Then $\overline{c} = \overline{b}^j$. We have $|\overline{a}| = 2$ and $|\overline{b}| = |\overline{c}| = r$. We may assume $a = a_2\gamma_p$, $b = a_r$, and $c = a_r^j\gamma_q\gamma_p^k$, where $1 \leqslant j \leqslant r-1$, and $1 \leqslant k \leqslant p-1$. We may also assume j is odd by replacing c with its inverse and j with $r-j$ if necessary.

Since $C_{G'}(\mathcal{C}_r) = \{e\}$, we have $a_r\gamma_p a_r^{-1} = \gamma_p^{\widehat{\tau}}$ where $\widehat{\tau}^r \equiv 1 \pmod p$ and $\widehat{\tau} \not\equiv 1 \pmod p$. Thus, $\widehat{\tau}^{r-1} + \widehat{\tau}^{r-2} + \ldots + 1 \equiv 0 \pmod p$. Note that this implies $\widehat{\tau} \not\equiv -1 \pmod p$. Also, we have $a_r\gamma_q a_r^{-1} = \gamma_q^{\check{\tau}}$. By using the same argument we can conclude that $\check{\tau} \not\equiv 1 \pmod q$ and $\check{\tau}^{r-1} + \check{\tau}^{r-2} + \ldots + 1 \equiv 0 \pmod q$. Note that this implies $\check{\tau} \not\equiv -1 \pmod q$. Also, $C_{G'}(\mathcal{C}_2) = \{e\}$, so $\mathcal{C}_2$ inverts $\mathcal{C}_p$ and it inverts $\mathcal{C}_q$. We have

$$C_1 = (\overline{c}, \overline{b}^{-(j-1)}, \overline{c}, \overline{b}^{r-j-2}, \overline{a}, \overline{b}^{-(r-1)}, \overline{a}^{-1})$$

and

$$C_2 = (\overline{c}, \overline{b}^{r-j-1}, \overline{c}, \overline{a}, \overline{b}^{r-1}, \overline{a}^{-1}, \overline{b}^{-(j-2)})$$

as Hamiltonian cycles in $\mathrm{Cay}(\overline{G}; \overline{S})$. Now we calculate the voltage of C_1.

$$\mathbb{V}(C_1) = cb^{-(j-1)}cb^{r-j-2}ab^{-(r-1)}a$$

$$
\begin{aligned}
&\equiv a_r^j \gamma_q \cdot a_r^{-(j-1)} \cdot a_r^j \gamma_q \cdot a_r^{r-j-2} \cdot a_2 \cdot a_r^{-(r-1)} \cdot a_2 \pmod{\mathcal{C}_p} \\
&= a_r^j \gamma_q a_r \gamma_q a_r^{-j-1} \\
&= \gamma_q^{\check{\tau}^j + \check{\tau}^{j+1}} \\
&= \gamma_q^{\check{\tau}^j (1+\check{\tau})},
\end{aligned}
$$

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

$$
\begin{aligned}
\mathbb{V}(C_1) &= cb^{-(j-1)} cb^{r-j-2} ab^{-(r-1)} a \\
&\equiv a_r^j \gamma_p^k \cdot a_r^{-(j-1)} \cdot a_r^j \gamma_p^k \cdot a_r^{r-j-2} \cdot a_2 \gamma_p \cdot a_r^{-(r-1)} \cdot \gamma_p^{-1} a_2 \pmod{\mathcal{C}_q} \\
&= a_r^j \gamma_p^k a_r \gamma_p^k a_r^{-j-2} a_2 \gamma_p a_r \gamma_p^{-1} a_2 \\
&= a_r^j \gamma_p^k a_r \gamma_p^k a_r^{-j-2} \gamma_p^{-1} a_r \gamma_p \\
&= \gamma_p^{k\hat{\tau}^j + k\hat{\tau}^{j+1} - \hat{\tau}^{-1} + 1}.
\end{aligned}
$$

We may assume this does not generate $\mathcal{C}_p$, for otherwise Factor Group Lemma 2.2.4 applies. Therefore,

$$
\begin{aligned}
0 &\equiv k\hat{\tau}^j + k\hat{\tau}^{j+1} - \hat{\tau}^{-1} + 1 \pmod{p} \\
&= k\hat{\tau}^{j+1} + k\hat{\tau}^j + 1 - \hat{\tau}^{-1}.
\end{aligned}
$$

Multiplying by $\hat{\tau}$, we have

$$
0 \equiv k\hat{\tau}^{j+2} + k\hat{\tau}^{j+1} + \hat{\tau} - 1 \pmod{p}. \tag{3.2.C}
$$

Now we calculate the voltage of C_2.

$$
\begin{aligned}
\mathbb{V}(C_2) &= cb^{r-j-1} cab^{r-1} a^{-1} b^{-(j-2)} \\
&\equiv a_r^j \gamma_q \cdot a_r^{r-j-1} \cdot a_r^j \gamma_q \cdot a_2 \cdot a_r^{r-1} \cdot a_2 \cdot a_r^{-(j-2)} \pmod{\mathcal{C}_p} \\
&= a_r^j \gamma_q a_r^{-1} \gamma_q a_r^{-j+1} \\
&= \gamma_q^{\check{\tau}^j + \check{\tau}^{j-1}} \\
&= \gamma_q^{\check{\tau}^{j-1} (\check{\tau}-1)},
\end{aligned}
$$

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

$$
\begin{aligned}
\mathbb{V}(C_2) &= cb^{r-j-1} cab^{r-1} a^{-1} b^{-(j-2)} \\
&\equiv a_r^j \gamma_p^k \cdot a_r^{r-j-1} \cdot a_r^j \gamma_p^k \cdot a_2 \gamma_p \cdot a_r^{r-1} \cdot \gamma_p^{-1} a_2 \cdot a_r^{-(j-2)} \pmod{\mathcal{C}_q} \\
&= a_r^j \gamma_p^k a_r^{-1} \gamma_p^k \gamma_p^{-1} a_r^{-1} \gamma_p a_r^{-j+2} \\
&= \gamma_p^{k\hat{\tau}^j + k\hat{\tau}^{j-1} - \hat{\tau}^{j-1} + \hat{\tau}^{j-2}}.
\end{aligned}
$$

We may assume this does not generate $\mathcal{C}_p$, for otherwise Factor Group Lemma 2.2.4 applies. Therefore,

$$
0 \equiv k\hat{\tau}^j + k\hat{\tau}^{j-1} - \hat{\tau}^{j-1} + \hat{\tau}^{j-2} \pmod{p}.
$$

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

$$0 \equiv k\widehat{\tau}^{j+2} + k\widehat{\tau}^{j+1} - \widehat{\tau}^{j+1} + \widehat{\tau}^{j} \pmod{p}. \tag{3.2.D}$$

Subtracting (3.2.D) from (3.2.C), we have

$$\begin{aligned} 0 &\equiv \widehat{\tau}^{j+1} - \widehat{\tau}^{j} + \widehat{\tau} - 1 \pmod{p} \\ &= (\widehat{\tau}^{j} + 1)(\widehat{\tau} - 1) \end{aligned}$$

This implies that $\widehat{\tau}^j \equiv -1 \pmod{p}$. Thus, by Lemma 2.5.3, $\widehat{\tau} \equiv 1 \pmod{p}$, which is not possible.

□

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

In this subsection we prove the part of Theorem 1.4 where $|S| = 3$, and $C_{G'}(\mathcal{C}_2) = \mathcal{C}_p \times \mathcal{C}_q$.

Proposition 3.3.1 *Assume*

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

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

Proof. Let $S = \{a, b, c\}$. If $C_{G'}(\mathcal{C}_r) \neq \{e\}$, then Proposition 3.1.1 applies. So we may assume $C_{G'}(\mathcal{C}_r) = \{e\}$. Now if $\widehat{S}$ is minimal, then Proposition 3.2.1 applies. So we may assume $\widehat{S}$ is not minimal. Consider

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

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

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

after replacing a and b by conjugates. The projection of (a, b) to $\mathcal{C}_r \ltimes \mathcal{C}_q$ must be of the form (a_r, γ_q) or $(a_r, a_r^m\gamma_q)$, where $1 \leqslant m \leqslant r-1$ (note that $\widehat{b} \neq \gamma_q$ because $S \cap G' = \varnothing$). Therefore (a, b) must have one of the following forms:

(1) $(a_r, a_2\gamma_q)$,
(2) $(a_r, a_2a_r^m\gamma_q)$, where $1 \leqslant m \leqslant r-1$,
(3) $(a_2a_r, a_r^m\gamma_q)$, where $1 \leqslant m \leqslant r-1$,
(4) $(a_2a_r, a_2\gamma_q)$,
(5) $(a_2a_r, a_2a_r^m\gamma_q)$, where $1 \leqslant m \leqslant r-1$.

Let c be the third element of S. We may write $c = a_2^i a_r^j \gamma_q^k \gamma_p$ with $0 \leqslant i \leqslant 1$, $0 \leqslant j \leqslant r-1$ 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 $a_r \gamma_p a_r^{-1} = \gamma_p^{\widehat{\tau}}$ where $\widehat{\tau}^r \equiv 1 \pmod p$ and $\widehat{\tau} \not\equiv 1 \pmod p$. Thus $\widehat{\tau}^{r-1} + \widehat{\tau}^{r-2} + \ldots + 1 \equiv 0 \pmod p$. Note that this implies $\widehat{\tau} \not\equiv -1 \pmod p$. Also we have $a_r \gamma_q a_r^{-1} = \gamma_q^{\check{\tau}}$. By using the same argument we can conclude that $\check{\tau} \not\equiv 1 \pmod q$ and $\check{\tau}^{r-1} + \check{\tau}^{r-2} + \ldots + 1 \equiv 0 \pmod q$. Note that this implies $\check{\tau} \not\equiv -1 \pmod q$.

Case 3.3.1 Assume $a = a_r$ and $b = a_2\gamma_q$.

Subcase 3.3.1.1 Assume $i = 0$. Then $j \neq 0$ and $c = a_r^j \gamma_q^k \gamma_p$. By part (1.2) of Theorem 1.2 $\mathrm{Cay}(\breve{G}; \breve{S})$ contains a Hamiltonian cycle. There must be an occurrence of $\breve{b}$ because it is the only generator that contains a_2. So Corollary 2.2.5 applies with $s = b$ and $t = b^{-1}$.

Subcase 3.3.1.2 Assume $j = 0$. Then $i \neq 0$ and $c = a_2 \gamma_q^k \gamma_p$. If $k \neq 0$, then by Lemma 2.5.2(2.5.2) $\langle a, c \rangle = G$ which contradicts the minimality of S.

So we may assume $k = 0$. Then $c = a_2\gamma_p$. Consider $\overline{G} = \mathcal{C}_2 \times \mathcal{C}_r$. Then $\overline{a} = a_r$, 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 b in C, and it is the only generator of G that contains γ_q, by Lemma 2.2.6 we conclude that the subgroup generated by $\mathbb{V}(C)$ contains $\mathcal{C}_q$. Similarly, since there is one occurrence of c in C, and it is the only generator of G that contains γ_p, by Lemma 2.2.6 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 2.2.4 applies.

Subcase 3.3.1.3 Assume $i \neq 0$ and $j \neq 0$. Then $c = a_2 a_r^j \gamma_q^k \gamma_p$. If $k \neq 0$, then by Lemma 2.5.2 (3), $\langle a, c \rangle = G$, which contradicts the minimality of S.

So we can assume $k = 0$. Then $c = a_2 a_r^j \gamma_p$. We may also assume j is odd by replacing c with its inverse and j with $r - j$ if necessary. Consider $\overline{G} = \mathcal{C}_2 \times \mathcal{C}_r$. Then $\overline{a} = a_r$, $\overline{b} = a_2$, and $\overline{c} = a_2 a_r^j$. We have

$$C_1 = (\overline{c}, (\overline{b}, \overline{a})^{r-j}, \overline{a}^{j-1}, \overline{b}, \overline{a}^{-(j-1)})$$

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 γ_p, by Lemma 2.2.6 we conclude that the subgroup generated by $\mathbb{V}(C_1)$ contains $\mathcal{C}_p$. By the Factor Group Lemma 2.2.4 this implies that C_1 lifts to $\tilde{C_1}$ in $\mathrm{Cay}(\breve{G}; \breve{S})$. Since C_1 contains an occurrence of b, Corollary 2.2.5 applies with $s = b$ and $t = b^{-1}$.

Case 3.3.2 Assume $a = a_r$ and $b = a_2 a_r^m \gamma_q$, where $1 \leqslant m \leqslant r-1$.

Subcase 3.3.2.1 Assume $i \neq 0$ and $j \neq 0$. Then $c = a_2 a_r^j \gamma_q^k \gamma_p$. If $k \neq 0$, then by Lemma 2.5.2 (3), $\langle a, c\rangle = G$, which contradicts the minimality of S. So we can assume $k = 0$. Then $c = a_2 a_r^j \gamma_p$. Thus, by Lemma 2.5.2(2.5.2) $\langle b, c\rangle = G$ which contradicts the minimality of S.

Subcase 3.3.2.2 Assume $i = 0$. Then $j \neq 0$ and $c = a_r^j \gamma_q^k \gamma_p$. We may assume j is odd by replacing c with its inverse and j with $r - j$ if necessary. If $k = 0$, then, by Lemma 2.5.2 (4), $\langle b, c\rangle = G$, which contradicts the minimality of S. So, we may also assume $k \neq 0$. Consider $\overline{G} = \mathcal{C}_2 \times \mathcal{C}_r$. Then $\overline{a} = a_r$, $\overline{b} = a_2 a_r^m$ and $\overline{c} = a_r^j$.

Subsubcase 3.3.2.2.1 Assume $j = 1$. Then $\overline{a} = \overline{c} = a_r$. We have $C_1 = (\overline{c}, \overline{a}^{r-2}, \overline{b}, \overline{a}^{-(r-1)}, \overline{b}^{-1})$ and $C_2 = (\overline{c}^2, \overline{a}^{r-3}, \overline{b}, \overline{a}^{-(r-1)}, \overline{b}^{-1})$ as Hamiltonian cycles 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 γ_p, by Lemma 2.2.6 we conclude that the subgroup generated by $\mathbb{V}(C_1)$ contains $\mathcal{C}_p$. We also have

$$\begin{aligned}
\mathbb{V}(C_1) &= c a^{r-2} b a^{-(r-1)} b^{-1} \\
&\equiv a_r \gamma_q^k \cdot a_r^{r-2} \cdot a_r^m \gamma_q \cdot a_r^{-(r-1)} \cdot \gamma_q^{-1} a_r^{-m} \pmod{\mathcal{C}_2 \times \mathcal{C}_p} \\
&= a_r \gamma_q^k a_r^{m-2} \gamma_q a_r \gamma_q^{-1} a_r^{-m} \\
&= \gamma_q^{k\breve{\tau} + \breve{\tau}^{m-1} - \breve{\tau}^m}.
\end{aligned}$$

We can assume this does not generate $\mathcal{C}_q$, for otherwise Factor Group Lemma 2.2.4 applies. So, we have

$$0 \equiv k\breve{\tau} + \breve{\tau}^{m-1} - \breve{\tau}^m \pmod{q}. \tag{3.3.A}$$

Now we calculate the voltage of C_2.

$$\begin{aligned}
\mathbb{V}(C_2) &= c^2 a^{r-3} b a^{-(r-1)} b^{-1} \\
&\equiv a_r \gamma_p a_r \gamma_p \cdot a_r^{r-3} \cdot a_r^m \cdot a_r^{-(r-1)} \cdot a_r^{-m} \pmod{\mathcal{C}_2 \times \mathcal{C}_q} \\
&= a_r \gamma_p a_r \gamma_p a_r^{-2} \\
&= \gamma_p^{\hat{\tau} + \hat{\tau}^2} \\
&= \gamma_p^{\hat{\tau}(1+\hat{\tau})},
\end{aligned}$$

which generates $\mathcal{C}_p$. Also, we have

$$\begin{aligned}
\mathbb{V}(C_2) &= c^2 a^{r-3} b a^{-(r-1)} b^{-1} \\
&\equiv a_r \gamma_q^k a_r \gamma_q^k \cdot a_r^{r-3} \cdot a_r^m \gamma_q \cdot a_r^{-(r-1)} \cdot \gamma_q^{-1} a_r^{-m} \pmod{\mathcal{C}_2 \times \mathcal{C}_p} \\
&= a_r \gamma_q^k a_r \gamma_q^k a_r^{m-3} \gamma_q a_r \gamma_q^{-1} a_r^{-m} \\
&= \gamma_q^{k\breve{\tau} + k\breve{\tau}^2 + \breve{\tau}^{m-1} - \breve{\tau}^m}.
\end{aligned}$$

We can assume this does not generate $\mathcal{C}_q$, for otherwise Factor Group Lemma 2.2.4 applies. Thus, we have

$$0 \equiv k\breve{\tau} + k\breve{\tau}^2 + \breve{\tau}^{m-1} - \breve{\tau}^m \pmod{q}.$$

By subtracting (3.3.A) from the above equation, we have $k\check{\tau}^2 \equiv 0 \pmod{q}$; this is not possible.

Subsubcase 3.3.2.2.2 Assume $j \neq 1$. We have

$$C_3 = (\overline{b}, \overline{c}^{-1}, \overline{a}^{j-1}, \overline{c}^{-1}, \overline{a}^{-(r-j-2)}, \overline{b}^{-1}, \overline{a}^{r-1})$$

and

$$C_4 = (\overline{c}^{-1}, \overline{a}^{-(r-j-1)}, \overline{c}^{-1}, \overline{b}^{-1}, \overline{a}^{-(r-1)}, \overline{b}, \overline{a}^{j-2})$$

as Hamiltonian cycles in $\mathrm{Cay}(\overline{G}; \overline{S})$. Now we calculate the voltage of C_3.

$$\begin{aligned}
\mathbb{V}(C_3) &= bc^{-1}a^{j-1}c^{-1}a^{-(r-j-2)}b^{-1}a^{r-1} \\
&\equiv a_r^m \cdot \gamma_p^{-1}a_r^{-j} \cdot a_r^{j-1} \cdot \gamma_p^{-1}a_r^{-j} \cdot a_r^{-(r-j-2)} \cdot a_r^{-m} \cdot a_r^{r-1} \pmod{\mathcal{C}_2 \times \mathcal{C}_q} \\
&= a_r^m\gamma_p^{-1}a_r^{-1}\gamma_p^{-1}a_r^{-m+1} \\
&= \gamma_p^{-\hat{\tau}^m - \hat{\tau}^{m-1}} \\
&= \gamma_p^{-\hat{\tau}^{m-1}(\hat{\tau}+1)},
\end{aligned}$$

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

$$\begin{aligned}
\mathbb{V}(C_3) &= bc^{-1}a^{j-1}c^{-1}a^{-(r-j-2)}b^{-1}a^{r-1} \\
&\equiv a_r^m\gamma_q \cdot \gamma_q^{-k}a_r^{-j} \cdot a_r^{j-1} \cdot \gamma_q^{-k}a_r^{-j} \cdot a_r^{-(r-j-2)} \cdot \gamma_q^{-1}a_r^{-m} \cdot a_r^{r-1} \pmod{\mathcal{C}_2 \times \mathcal{C}_p} \\
&= a_r^m\gamma_q^{1-k}a_r^{-1}\gamma_q^{-k}a_r^2\gamma_q^{-1}a_r^{-m-1} \\
&= \gamma_q^{(1-k)\check{\tau}^m - k\check{\tau}^{m-1} - \check{\tau}^{m+1}} \\
&= \gamma_q^{-\check{\tau}^{m-1}((k-1)\check{\tau}+k+\check{\tau}^2)}.
\end{aligned}$$

We can assume this does not generate $\mathcal{C}_q$, for otherwise Factor Group Lemma 2.2.4 applies. Therefore,

$$\begin{aligned}
0 &\equiv (k-1)\check{\tau} + k + \check{\tau}^2 \pmod{q} \\
&= k(\check{\tau}+1) + \check{\tau}(\check{\tau}-1).
\end{aligned} \tag{3.3.B}$$

Now we calculate the voltage of C_4.

$$\begin{aligned}
\mathbb{V}(C_4) &= c^{-1}a^{-(r-j-1)}c^{-1}b^{-1}a^{-(r-1)}ba^{j-2} \\
&\equiv \gamma_p^{-1}a_r^{-j} \cdot a_r^{-(r-j-1)} \cdot \gamma_p^{-1}a_r^{-j} \cdot a_r^{-m} \cdot a_r^{-(r-1)} \cdot a_r^m \cdot a_r^{j-2} \pmod{\mathcal{C}_2 \times \mathcal{C}_q} \\
&= \gamma_p^{-1}a_r\gamma_p^{-1}a_r^{-1} \\
&= \gamma_p^{-1-\hat{\tau}},
\end{aligned}$$

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

$$\mathbb{V}(C_4) = c^{-1}a^{-(r-j-1)}c^{-1}b^{-1}a^{-(r-1)}ba^{j-2}$$

$$\begin{aligned}&\equiv \gamma_q^{-k} a_r^{-j} \cdot a_r^{-(r-j-1)} \cdot \gamma_q^{-k} a_r^{-j} \cdot \gamma_q^{-1} a_r^{-m} \cdot a_r^{-(r-1)} \cdot a_r^{m} \gamma_q \cdot a_r^{j-2} \pmod{\mathcal{C}_2 \times \mathcal{C}_p} \\ &= \gamma_q^{-k-k\check{\tau}-\check{\tau}^{-j+1}+\check{\tau}^{-j+2}}.\end{aligned}$$

We may assume this does not generate $\mathcal{C}_q$, for otherwise Factor Group Lemma 2.2.4 applies. Therefore,

$$\begin{aligned}0 &\equiv -k - k\check{\tau} - \check{\tau}^{-j+1} + \check{\tau}^{-j+2} \pmod q \\ &= -k(\check{\tau}+1) + \check{\tau}^{-j+1}(\check{\tau}-1).\end{aligned} \tag{3.3.C}$$

Adding (3.3.B) and (3.3.C), we have

$$\begin{aligned}0 &\equiv \check{\tau}(\check{\tau}-1) + \check{\tau}^{-j+1}(\check{\tau}-1) \pmod q \\ &= \check{\tau}(\check{\tau}-1)(1+\check{\tau}^{-j}).\end{aligned}$$

This implies that $\check{\tau}^{-j} \equiv -1 \pmod q$. So $\check{\tau}^{j} \equiv -1 \pmod q$. Thus, by Lemma 2.5.3, $\check{\tau} \equiv 1 \pmod q$, which is not possible.

Subcase 3.3.2.3 Assume $j = 0$. Then $i \neq 0$ and $c = a_2 \gamma_q^k \gamma_p$. If $k \neq 0$, then by Lemma 2.5.2 (3), $\langle a, c\rangle = G$, which contradicts the minimality of S.

So we may assume $k = 0$. Then $c = a_2\gamma_p$. We may also assume m is odd by replacing b with its inverse and m with $r-m$ if necessary. Consider $\overline{G} = \mathcal{C}_2 \times \mathcal{C}_r$. Then $\overline{a} = a_r$, $\overline{b} = a_2 a_r^m$, and $\overline{c} = a_2$. We have

$$C_1 = (\overline{b}, (\overline{c}, \overline{a})^{r-m}, \overline{a}^{m-1}, \overline{c}, \overline{a}^{-(m-1)})$$

as a Hamiltonian cycle in $\mathrm{Cay}(\overline{G}; \overline{S})$. Since there is one occurrence of b in C_1, and it is the only generator of G that contains γ_q, by Lemma 2.2.6 we conclude that the subgroup generated by $\mathbb{V}(C_1)$ contains $\mathcal{C}_q$. By the Factor Group Lemma 2.2.4 this implies that C_1 lifts to a Hamiltonian cycle $\tilde{C}_1$ in $\mathrm{Cay}(\widehat{G}; \widehat{S})$. Since C_1 contains an occurrence of c, Corollary 2.2.5 applies with $s = c$ and $t = c^{-1}$.

Case 3.3.3 Assume $a = a_2 a_r$ and $b = a_r^m \gamma_q$, where $1 \leqslant m \leqslant r-1$. Since $b = a_r^m \gamma_q$ is conjugate to a_r^m via an element of $\mathcal{C}_q$, this implies $\{a, b\}$ is conjugate to $\{a_2 a_r \gamma_q^n, a_r^m\}$ for some nonzero n. So Case 3.3.2 applies (after replacing γ_q with γ_q^m and switching a_r with a_r^m).

Case 3.3.4 Assume $a = a_2 a_r$ and $b = a_2 \gamma_q$.

Subcase 3.3.4.1 Assume $i = 0$. Then $j \neq 0$ and $c = a_r^j \gamma_q^k \gamma_p$. If $k \neq 0$, then by Lemma 2.5.2 (1), $\langle a, c\rangle = G$, which contradicts the minimality of S.

So we can assume $k = 0$. Then $c = a_r^j \gamma_p$. Consider $\overline{G} = \mathcal{C}_2 \times \mathcal{C}_r$. Then $\overline{a} = a_2 a_r$, $\overline{b} = a_2$, and $\overline{c} = a_r^j$. We have

$$C = (\overline{c}, (\overline{a}^{-1}, \overline{b})^{j-1}, \overline{a}^{-1}, \overline{c}, (\overline{a}, \overline{b})^{r-j-1}, \overline{a})$$

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

$$\begin{aligned}\mathbb{V}(C) &= c(a^{-1}b)^{j-1}a^{-1}c(ab)^{r-j-1}a \\ &\equiv a_r^j\gamma_p \cdot a_r^{-(j-1)} \cdot a_r^{-1} \cdot a_r^j\gamma_p \cdot a_r^{r-j-1} \cdot a_r \pmod{\mathcal{C}_2 \times \mathcal{C}_q} \\ &= a_r^j\gamma_p^2 a_r^{-j} \\ &= \gamma_p^{2\hat{\tau}^j},\end{aligned}$$

which generates $\mathcal{C}_p$. By the Factor Group Lemma 2.2.4 this implies that C lifts to a Hamiltonian cycle $\tilde{C}$ in $\operatorname{Cay}(\breve{G};\breve{S})$. Since C contains an occurrence of b, Corollary 2.2.5 applies with $s = b$ and $t = b^{-1}$.

Subcase 3.3.4.2 Assume $j = 0$. Then $i \neq 0$ and $c = a_2\gamma_q^k\gamma_p$. If $k \neq 0$, then by Lemma 2.5.2(2.5.2) $\langle a, c\rangle = G$ which contradicts the minimality of S.

So we can assume $k = 0$. Then $c = a_2\gamma_p$. Consider $\overline{G} = \mathcal{C}_2 \times \mathcal{C}_r$. Then $\overline{a} = a_2a_r$, and $\overline{b} = \overline{c} = a_2$. We have $C = (\overline{c}, \overline{a}^{r-1}, \overline{b}^{-1}, \overline{a}^{-(r-1)})$ as a Hamiltonian cycle in $\operatorname{Cay}(\overline{G};\overline{S})$. Since there is one occurrence of b in C, and it is the only generator of G that contains γ_q, by Lemma 2.2.6 we conclude that the subgroup generated by $\mathbb{V}(C)$ contains $\mathcal{C}_q$. Similarly, since there is one occurrence of c in C, and it is the only generator of G that contains γ_p, by Lemma 2.2.6 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 2.2.4 applies.

Subcase 3.3.4.3 Assume $i \neq 0$ and $j \neq 0$. Then $c = a_2a_r^j\gamma_q^k\gamma_p$. If $k \neq 0$, then by Lemma 2.5.2(2.5.2) $\langle a, c\rangle = G$ which contradicts the minimality of S.

So we can assume $k = 0$. Then $c = a_2a_r^j\gamma_p$. We may also assume j is odd by replacing c with its inverse and j with $r-j$ if necessary. Consider $\overline{G} = \mathcal{C}_2 \times \mathcal{C}_r$. Then $\overline{a} = a_2a_r$, $\overline{b} = a_2$, and $c = a_2a_r^j$. We have

$$C = (\overline{c}, \overline{a}^{-(j-1)}, \overline{c}, \overline{a}^{r-j-2}, \overline{b}, \overline{a}^{-(r-1)}, \overline{b})$$

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

$$\begin{aligned}\mathbb{V}(C) &= ca^{-(j-1)}ca^{r-j-2}ba^{-(r-1)}b \\ &\equiv a_r^j\gamma_p \cdot a_r^{-(j-1)} \cdot a_r^j\gamma_p \cdot a_r^{r-j-2} \cdot a_r^{-(r-1)} \pmod{\mathcal{C}_2 \times \mathcal{C}_q} \\ &= a_r^j\gamma_p a_r \gamma_p a_r^{-j-1} \\ &= \gamma_p^{\hat{\tau}^j + \hat{\tau}^{j+1}} \\ &= \gamma_p^{\hat{\tau}^j(1+\hat{\tau})},\end{aligned}$$

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

$$\begin{aligned}\mathbb{V}(C) &= ca^{-(j-1)}ca^{r-j-2}ba^{-(r-1)}b \\ &\equiv a_r^j \cdot a_r^{-(j-1)} \cdot a_r^j \cdot a_r^{r-j-2} \cdot \gamma_q \cdot a_r^{-(r-1)} \cdot \gamma_q \pmod{\mathcal{C}_2 \times \mathcal{C}_p}\end{aligned}$$

$$= a_r^{-1}\gamma_q a_r \gamma_q$$
$$= \gamma_q^{\check{r}^{-1}+1},$$

which generates $\mathcal{C}_q$. Therefore the subgroup generated by $\mathbb{V}(C)$ is G'. So Factor Group Lemma 2.2.4 applies.

Case 3.3.5 Assume $a = a_2 a_r$ and $b = a_2 a_r^m \gamma_q$, where $1 \leqslant m \leqslant r-1$. If $k \neq 0$, then by Lemma 2.5.2(2.5.2) $\langle a, c\rangle = G$ which contradicts the minimality of S.

So we can assume $k = 0$. Also, if $j \neq 0$, then by Lemma 2.5.2 (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 3.3.4 applies, after interchanging b and c, and interchanging p and q. □

3.4 Assume $|S| = 3$ and $C_{G'}(\mathcal{C}_2) \neq \{e\}$

In this subsection we prove the part of Theorem 1.4 where $|S| = 3$, and $C_{G'}(\mathcal{C}_2) \neq \{e\}$.

Proposition 3.4.1 *Assume*

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

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

Proof. Let $S = \{a, b, c\}$. If $C_{G'}(\mathcal{C}_r) \neq \{e\}$, then Proposition 3.1.1 applies. Therefore, we may assume $C_{G'}(\mathcal{C}_r) = \{e\}$. Now if $C_{G'}(\mathcal{C}_2) = \mathcal{C}_p \times \mathcal{C}_q$, then Proposition 3.3.1 applies. Since $C_{G'}(\mathcal{C}_2) \neq \{e\}$, 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 3.2.1 applies. So we may assume $\widehat{S}$ is not minimal. Consider

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

Choose a 2-element subset $\{a, b\}$ in S that generates $\widehat{G}$. From the minimality of S, we see that $\langle a, b\rangle = \mathcal{C}_2 \times (\mathcal{C}_r \ltimes \mathcal{C}_q)$, 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 $\mathcal{C}_2 \times \mathcal{C}_r$. Then the projection of (a, b) to $\mathcal{C}_2 \times \mathcal{C}_r$ has one of the following forms.

- $(a_2 a_r, a_2 a_r^m)$, where $1 \leqslant m \leqslant r-1$,
- $(a_2 a_r, a_2)$,
- $(a_2 a_r, a_r^m)$, where $1 \leqslant m \leqslant r-1$,
- (a_r, a_2).

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

(1) $(a_2a_r, a_2a_r^m\gamma_q)$, where $1 \leqslant m \leqslant r-1$,
(2) $(a_2a_r, a_2\gamma_q)$,
(3) $(a_2a_r, a_r^m\gamma_q)$, where $1 \leqslant m \leqslant r-1$,
(4) $(a_r, a_2\gamma_q)$.

Let c be the third element of S. We may write $c = a_2^i a_r^j \gamma_q^k \gamma_p$ with $0 \leqslant i \leqslant 1$, $0 \leqslant j \leqslant r-1$ 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 $a_r\gamma_p a_r^{-1} = \gamma_p^{\widehat{\tau}}$ where $\widehat{\tau}^r \equiv 1 \pmod p$ and $\widehat{\tau} \not\equiv 1 \pmod p$. Thus, $\widehat{\tau}^{r-1} + \widehat{\tau}^{r-2} + \ldots + 1 \equiv 0 \pmod p$. Note that this implies $\widehat{\tau} \not\equiv -1 \pmod p$. Also we have $a_r\gamma_q a_r^{-1} = \gamma_q^{\check{\tau}}$. By using the same argument we can conclude that $\check{\tau} \not\equiv 1 \pmod q$ and $\check{\tau}^{r-1} + \check{\tau}^{r-2} + \ldots + 1 \equiv 0 \pmod q$. Note that this implies $\check{\tau} \not\equiv -1 \pmod q$.

Case 3.4.1 Assume $a = a_2a_r$ and $b = a_2a_r^m\gamma_q$, where $1 \leqslant m \leqslant r-1$. If $k \neq 0$, then by Lemma 2.5.2(2.5.2), $\langle a, c\rangle = G$ which contradicts the minimality of S. So we can assume $k = 0$. Now if $j \neq 0$, then by Lemma 2.5.2(2.5.2), $\langle b, c\rangle = G$ which contradicts the minimality of S.

Therefore, we may assume $j = 0$. Then $i \neq 0$ and $c = a_2\gamma_p$. We may also assume m is odd by replacing b with its inverse and m with $r - m$ if necessary. Consider $\overline{G} = \mathcal{C}_2 \times \mathcal{C}_r$. Then $\overline{a} = a_2a_r$, $\overline{b} = a_2a_r^m$, and $\overline{c} = a_2$. We have

$$C = (\overline{b}, \overline{a}^{-(m-1)}, \overline{b}, \overline{a}^{r-m-2}, \overline{c}, \overline{a}^{-(r-1)}, \overline{c})$$

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

$$\begin{aligned}
\mathbb{V}(C) &= ba^{-(m-1)}ba^{r-m-2}ca^{-(r-1)}c \\
&\equiv a_r^m\gamma_q \cdot a_r^{-(m-1)} \cdot a_r^m\gamma_q \cdot a_r^{r-m-2} \cdot a_r^{-(r-1)} \pmod{\mathcal{C}_2 \ltimes \mathcal{C}_p} \\
&= a_r^m\gamma_q a_r \gamma_q a_r^{-m-1} \\
&= \gamma_q^{\check{\tau}^m + \check{\tau}^{m+1}} \\
&= \gamma_q^{\check{\tau}^m(1+\check{\tau})},
\end{aligned}$$

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

$$\begin{aligned}
\mathbb{V}(C) &= ba^{-(m-1)}ba^{r-m-2}ca^{-(r-1)}c \\
&\equiv a_2a_r^m \cdot (a_2a_r)^{-(m-1)} \cdot a_2a_r^m \cdot (a_2a_r)^{r-m-2} \cdot a_2\gamma_p \cdot (a_2a_r)^{-(r-1)} \cdot a_2\gamma_p \pmod{\mathcal{C}_q} \\
&= a_2a_r^m a_r^{-m+1} a_2 a_r^m a_r^{-m-2} a_2\gamma_p a_r a_2 \gamma_p \\
&= a_r^{-1}\gamma_p^{-1} a_r \gamma_p \\
&= \gamma_p^{-\widehat{\tau}^{-1}+1},
\end{aligned}$$

which generates $\mathcal{C}_p$. Therefore, the subgroup generated by $\mathbb{V}(C)$ is G'. So Factor Group Lemma 2.2.4 applies.

Case 3.4.2 Assume $a = a_2a_r$ and $b = a_2\gamma_q$. If $k \neq 0$, then by Lemma 2.5.2 (1), $\langle a, c\rangle = G$, which contradicts the minimality of S. So we can assume $k = 0$. Then $c = a_2^i a_r^j \gamma_p$.

Subcase 3.4.2.1 Assume $i = 0$. Then $j \neq 0$ and $c = a_r^j \gamma_p$. We may also assume j is odd by replacing c with its inverse and j with $r-j$ if necessary. Consider $\overline{G} = \mathcal{C}_2 \times \mathcal{C}_r$. Then $\overline{a} = a_2 a_r$, $\overline{b} = a_2$, and $\overline{c} = a_r^j$. We have

$$C = (\overline{c}, \overline{a}^{r-j-1}, \overline{b}, \overline{a}^{-(r-j-1)}, \overline{c}^{-1}, \overline{a}^{j-1}, \overline{b}, \overline{a}^{-(j-1)})$$

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

$$\begin{aligned}
\mathbb{V}(C) &= ca^{r-j-1} b a^{-(r-j-1)} c^{-1} a^{j-1} b a^{-(j-1)} \\
&\equiv a_r^j \gamma_p \cdot (a_2 a_r)^{r-j-1} \cdot a_2 \cdot (a_2 a_r)^{-(r-j-1)} \cdot \gamma_p^{-1} a_r^{-j} \cdot (a_2 a_r)^{j-1} \cdot a_2 \cdot (a_2 a_r)^{-(j-1)} \pmod{\mathcal{C}_q} \\
&= a_r^j \gamma_p a_2 a_r^{r-j-1} a_2 a_r^{-(r-j-1)} a_2 \gamma_p^{-1} a_r^{-j} a_r^{j-1} a_2 a_r^{-(j-1)} \\
&= a_r^j \gamma_p a_2 \gamma_p^{-1} a_r^{-j} a_2 \\
&= a_r^j \gamma_p^2 a_r^{-j} \\
&= \gamma_p^{2\hat{\tau}^j},
\end{aligned}$$

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

$$\begin{aligned}
\mathbb{V}(C) &= ca^{r-j-1} b a^{-(r-j-1)} c^{-1} a^{j-1} b a^{-(j-1)} \\
&\equiv a_r^j \cdot a_r^{r-j-1} \cdot \gamma_q \cdot a_r^{-(r-j-1)} \cdot a_r^{-j} \cdot a_r^{j-1} \cdot \gamma_q \cdot a_r^{-(j-1)} \quad \pmod{\mathcal{C}_2 \ltimes \mathcal{C}_p} \\
&= a_r^{-1} \gamma_q a_r^j \gamma_q a_r^{-j+1} \\
&= \gamma_q^{\check{\tau}^{-1} + \check{\tau}^{j-1}}.
\end{aligned}$$

We can assume this does not generate $\mathcal{C}_q$, for otherwise Factor Group Lemma 2.2.4 applies. Therefore,

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

Multiplying by $\check{\tau}$, we have $0 \equiv 1 + \check{\tau}^j \pmod{q}$, so $\check{\tau}^j \equiv -1 \pmod{q}$. Thus, by Lemma 2.5.3, $\check{\tau} \equiv 1 \pmod{q}$, which is not possible.

Subcase 3.4.2.2 Assume $j = 0$. Then $i \neq 0$ and $c = a_2 \gamma_p$. Consider $\overline{G} = \mathcal{C}_2 \times \mathcal{C}_r$. Then $\overline{a} = a_2 a_r$, and $\overline{b} = \overline{c} = a_2$. We have $C = (\overline{c}, \overline{a}^{r-1}, \overline{b}^{-1}, \overline{a}^{-(r-1)})$ as a Hamiltonian cycle in $\operatorname{Cay}(\overline{G}; \overline{S})$. Since there is one occurrence of b in C, and it is the only generator of G that contains γ_q, by Lemma 2.2.6 we conclude that the subgroup generated by $\mathbb{V}(C)$ contains $\mathcal{C}_q$. Similarly, since there is one occurrence of c in C, and it is the only generator of G that contains γ_p, by Lemma 2.2.6 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 2.2.4 applies.

Subcase 3.4.2.3 Assume $i \neq 0$ and $j \neq 0$. Then $c = a_2 a_r^j \gamma_p$. We may also assume j is odd by replacing c with its inverse and j with $r-j$ if necessary. Consider $\overline{G} = \mathcal{C}_2 \times \mathcal{C}_r$. Then $\overline{a} = a_2 a_r$, $\overline{b} = a_2$, and $\overline{c} = a_2 a_r^j$. We have

$$C = (\overline{c}, \overline{a}^{-(j-1)}, \overline{c}, \overline{a}^{r-j-2}, \overline{b}, \overline{a}^{-(r-1)}, \overline{b})$$

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

$$\begin{aligned}\mathbb{V}(C) &= ca^{-(j-1)}ca^{r-j-2}ba^{-(r-1)}b \\ &\equiv a_r^j \cdot a_r^{-(j-1)} \cdot a_r^j \cdot a_r^{r-j-2} \cdot \gamma_q \cdot a_r^{-(r-1)} \cdot \gamma_q \pmod{\mathcal{C}_2 \ltimes \mathcal{C}_p} \\ &= a_r^{-1}\gamma_q a_r \gamma_q \\ &= \gamma_q^{\check{\tau}^{-1}+1},\end{aligned}$$

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

$$\begin{aligned}\mathbb{V}(C) &= ca^{-(j-1)}ca^{r-j-2}ba^{-(r-1)}b \\ &\equiv a_2a_r^j\gamma_p \cdot (a_2a_r)^{-(j-1)} \cdot a_2a_r^j\gamma_p \cdot (a_2a_r)^{r-j-2} \cdot a_2 \cdot (a_2a_r)^{-(r-1)} \cdot a_2 \pmod{\mathcal{C}_q} \\ &= a_2a_r^j\gamma_p a_r^{-j+1}a_2a_r^j\gamma_p a_r^{r-j-2}a_2a_r^{-r+1}a_2 \\ &= a_r^j\gamma_p^{-1}a_r\gamma_p a_r^{-j-1} \\ &= \gamma_p^{-\hat{\tau}^j+\hat{\tau}^{j+1}} \\ &= \gamma_p^{-\hat{\tau}^j(1-\hat{\tau})},\end{aligned}$$

which generates $\mathcal{C}_p$. Therefore the subgroup generated by $\mathbb{V}(C)$ is G'. So Factor Group Lemma 2.2.4 applies.

Case 3.4.3 Assume $a = a_2a_r$ and $b = a_r^m\gamma_q$, where $1 \leqslant m \leqslant r-1$. If $k \neq 0$, then by Lemma 2.5.2 (1), $\langle a, c\rangle = G$, which contradicts the minimality of S. So we may assume $k = 0$. Then $c = a_2^i a_r^j \gamma_p$. If $j \neq 0$, then by Lemma 2.5.2 (2), $\langle b, c\rangle = G$, which contradicts the minimality of S. So we can assume $j = 0$. Then $i \neq 0$ and $c = a_2\gamma_p$. Consider $\overline{G} = \mathcal{C}_2 \times \mathcal{C}_r$. Then $\overline{a} = a_2a_r$, and $\overline{b} = a_r^m$, and $\overline{c} = a_2$. We may assume m is odd by replacing b with its inverse and m with $r-m$ if necessary. We have

$$C = (\overline{b}, (\overline{a}^{-1}, \overline{c})^{m-1}, \overline{a}^{-1}, \overline{b}, (\overline{a}, \overline{c})^{r-m-1}, \overline{a})$$

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

$$\begin{aligned}\mathbb{V}(C) &= b(a^{-1}c)^{m-1}a^{-1}b(ac)^{r-m-1}a \\ &\equiv a_r^m\gamma_q \cdot a_r^{-(m-1)} \cdot a_r^{-1} \cdot a_r^m\gamma_q \cdot a_r^{r-m-1} \cdot a_r \pmod{\mathcal{C}_2 \ltimes \mathcal{C}_p} \\ &= a_r^m\gamma_q^2a_r^{-m} \\ &= \gamma_q^{2\check{\tau}^m},\end{aligned}$$

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

$$\begin{aligned}\mathbb{V}(C) &= b(a^{-1}c)^{m-1}a^{-1}b(ac)^{r-m-1}a \\ &\equiv a_r^m \cdot (a_r^{-1}a_2 \cdot a_2\gamma_p)^{m-1} \cdot a_r^{-1}a_2 \cdot a_r^m \cdot (a_2a_r \cdot a_2\gamma_p)^{r-m-1} \cdot a_2a_r \pmod{\mathcal{C}_q} \\ &= a_r^m(a_r^{-1}\gamma_p)^{m-1}a_r^{m-1}a_2(a_r\gamma_p)^{r-m-1}a_2a_r \\ &= a_r^m(\gamma_p^{\hat{\tau}^{-1}+\hat{\tau}^{-2}+\ldots+\hat{\tau}^{m-1}}a_r^{-(m-1)})a_r^{m-1}a_2(\gamma_p^{\hat{\tau}+\hat{\tau}^2+\ldots+\hat{\tau}^{r-m-1}}a_r^{r-m-1})a_2a_r \\ &= a_r^m\gamma_p^{\hat{\tau}^{-1}+\hat{\tau}^{-2}+\ldots+\hat{\tau}^{m-1}}\gamma_p^{-(\hat{\tau}+\hat{\tau}^2+\ldots+\hat{\tau}^{r-m-1})}a_r^{-m}\end{aligned}$$

$$= \gamma_p^{\hat{\tau}^m(\hat{\tau}^{-1}+\hat{\tau}^{-2}+\ldots+\hat{\tau}^{m-1}-(\hat{\tau}+\hat{\tau}^2+\ldots+\hat{\tau}^{r-m-1}))}$$
$$= \gamma_p^{(\hat{\tau}+1)(1-\hat{\tau}^{-m})/(\hat{\tau}-1)}.$$

We can assume this does not generate $\mathcal{C}_p$, for otherwise Factor Group Lemma 2.2.4 applies. Therefore $0 \equiv 1-\hat{\tau}^{-m} \pmod p$, which implies $\hat{\tau}^{-m} \equiv 1 \pmod p$. Multiplying by $\hat{\tau}^m$, we have $\hat{\tau}^m \equiv 1 \pmod p$. Thus, by Lemma 2.5.3, $\hat{\tau} \equiv 1 \pmod p$, which is not possible.

Case 3.4.4 Assume $a = a_r$ and $b = a_2\gamma_q$.

Subcase 3.4.4.1 Assume $i = 0$. Then $j \neq 0$ and $c = a_r^j\gamma_q^k\gamma_p$. We show that $\langle b, c\rangle = G$, which contradicts the minimality of S. We have $\langle \overline{b}, \overline{c}\rangle = \langle a_2, a_r^j\rangle = \overline{G}$. We also have $\{\widehat{b}, \widehat{c}\} = \{a_2\gamma_q, a_r^j\gamma_q^k\}$. Since $\mathcal{C}_2$ centralizes $\mathcal{C}_q$, this implies

$$[\widehat{b}, \widehat{c}] = [a_2\gamma_q, a_r^j\gamma_q^k] = [\gamma_q, a_r^j\gamma_q^k] = \gamma_q a_r^j\gamma_q^k\gamma_q^{-1}\gamma_q^{-k}a_r^{-j} = \gamma_q a_r^j\gamma_q^{-1}a_r^{-j} = \gamma_q^{1-\check{\tau}^j}.$$

We may assume this does not generate $\mathcal{C}_q$, for otherwise $\widehat{G}$ contains $\mathcal{C}_q$. Therefore $0 \equiv 1-\check{\tau}^j \pmod q$, which implies $\check{\tau}^j \equiv 1 \pmod q$. So by Lemma 2.5.3, $\check{\tau} \equiv 1 \pmod q$, which is not possible.

Also, we have $\{\check{b}, \check{c}\} = \{a_2, a_r^j\gamma_p\}$. Since $\mathcal{C}_2$ inverts $\mathcal{C}_p$, this implies

$$[\check{b}, \check{c}] = [a_2, a_r^j\gamma_p] = a_2a_r^j\gamma_pa_2\gamma_p^{-1}a_r^{-j} = a_r^j\gamma_p^{-2}a_r^{-j} = \gamma_p^{-2\hat{\tau}^j},$$

which generates $\mathcal{C}_p$. Thus $\check{G}$ contains $\mathcal{C}_p$. So $G = \langle b, c\rangle$.

Subcase 3.4.4.2 Assume $j = 0$. Then $i \neq 0$ and $c = a_2\gamma_q^k\gamma_p$. If $k \neq 0$, then by Lemma 2.5.2 (3), $\langle a, c\rangle = G$, which contradicts the minimality of S. So we may assume $k = 0$. Thus $c = a_2\gamma_p$.

Consider $\overline{G} = \mathcal{C}_2 \times \mathcal{C}_r$. Then $\overline{a} = a_r$, $\overline{b} = \overline{c} = a_2$. We have $C = (\overline{c}, \overline{a}^{r-1}, \overline{b}^{-1}, \overline{a}^{-(r-1)})$ 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 γ_q, by Lemma 2.2.6 we conclude that the subgroup generated by $\mathbb{V}(C)$ contains $\mathcal{C}_q$. i Similarly, since there is one occurrence of c in C, and it is the only generator of G that contains γ_p, by Lemma 2.2.6 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 2.2.4 applies.

Subcase 3.4.4.3 Assume $i \neq 0$ and $j \neq 0$. Then $c = a_2a_r^j\gamma_q^k\gamma_p$. If $k \neq 0$, then by Lemma 2.5.2 (3), $\langle a, c\rangle = G$, which contradicts the minimality of S.

So we can assume $k = 0$. Then $c = a_2a_r^j\gamma_p$. We show that $\langle b, c\rangle = G$ which contradicts the minimality of S. We have $\langle \overline{b}, \overline{c}\rangle = \langle a_2, a_2a_r^j\rangle = \overline{G}$. Also, $\{\widehat{b}, \widehat{c}\} = \{a_2\gamma_q, a_2a_r^j\}$. Since $\mathcal{C}_2$ centralizes $\mathcal{C}_q$, we have

$$[\widehat{b}, \widehat{c}] = [a_2\gamma_q, a_2a_r^j] = [\gamma_q, a_r^j] = \gamma_q a_r^j\gamma_q^{-1}a_r^{-j} = \gamma_q^{1-\check{\tau}^j}.$$

We may assume this does not generate $\mathcal{C}_q$, for otherwise $\widehat{G}$ contains $\mathcal{C}_q$. Therefore, $0 \equiv 1 - \breve{\tau}^j \pmod{q}$, which implies $\breve{\tau}^j \equiv 1 \pmod{q}$. Thus, by Lemma 2.5.3, $\breve{\tau} \equiv 1 \pmod{q}$, which is not possible. Additionally, $\{\breve{b}, \breve{c}\} = \{a_2, a_2 a_r^j \gamma_p\}$. Since $\mathcal{C}_2$ inverts $\mathcal{C}_p$, we have

$$[\breve{b}, \breve{c}] = [a_2, a_2 a_r^j \gamma_p] = a_2 a_2 a_r^j \gamma_p a_2 \gamma_p^{-1} a_r^{-j} a_2 = a_r^j \gamma_p^2 a_r^{-j} = \gamma_p^{\hat{\tau}}$$

which generates $\mathcal{C}_p$. Thus $\breve{G}$ contains $\mathcal{C}_p$.

□

3.5 Assume $|S| = 3$ and $C_{G'}(\mathcal{C}_2) = \{e\}$

In this subsection we prove the part of Theorem 1.4 where $|S| = 3$ and $C_{G'}(\mathcal{C}_2) = \{e\}$.

Proposition 3.5.1 *Assume*

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

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

Proof. Let $S = \{a, b, c\}$. If $C_{G'}(\mathcal{C}_r) \neq \{e\}$, then Proposition 3.1.1 applies. So we may assume $C_{G'}(\mathcal{C}_r) = \{e\}$. Now if $\widehat{S}$ is minimal, then Proposition 3.2.1 applies. So we may assume $\widehat{S}$ is not minimal. Consider

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

Choose a 2-element subset $\{a, b\}$ in S that generates $\widehat{G}$. From the minimality of S, we see that $\langle a, b\rangle = (\mathcal{C}_2 \times \mathcal{C}_r) \ltimes \mathcal{C}_q$, after replacing a and b by conjugates. We may assume $|a| \geqslant |b|$ and (by conjugating if necessary) a is in $\mathcal{C}_2 \times \mathcal{C}_r$. Then the projection of (a, b) to $\mathcal{C}_2 \times \mathcal{C}_r$ is one of the following forms.

- $(a_2 a_r, a_2 a_r^m)$, where $1 \leqslant m \leqslant r - 1$,
- $(a_2 a_r, a_2)$,
- $(a_2 a_r, a_r^m)$, where $1 \leqslant m \leqslant r - 1$,
- (a_r, a_2).

There are four possibilities for (a, b):

(1) $(a_2 a_r, a_2 a_r^m \gamma_q)$, where $1 \leqslant m \leqslant r - 1$,
(2) $(a_2 a_r, a_2 \gamma_q)$,
(3) $(a_2 a_r, a_r^m \gamma_q)$, where $1 \leqslant m \leqslant r - 1$,
(4) $(a_r, a_2 \gamma_q)$.

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

Case 3.5.1 Assume $a = a_2 a_r$ and $b = a_2 a_r^m \gamma_q$, where $1 \leqslant m \leqslant r-1$. If $k \neq 0$, then by Lemma 2.5.2 (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 2.5.2 (4), $\langle b, c\rangle = G$, which contradicts the minimality of S. Therefore we may assume $j = 0$. Then $i \neq 0$ and $c = a_2\gamma_p$.

Now we show that $\langle b, c\rangle = G$, which contradicts the minimality of S. We have $\langle \overline{b}, \overline{c}\rangle = \langle a_2 a_r^m, a_2\rangle = \overline{G}$. Also, $\{\widehat{b}, \widehat{c}\} = \{a_2 a_r^m \gamma_q, a_2\}$. Since $\mathcal{C}_2$ inverts $\mathcal{C}_q$, this implies

$$[\widehat{b}, \widehat{c}] = [a_2 a_r^m \gamma_q, a_2] = a_2 a_r^m \gamma_q a_2 \gamma_q^{-1} a_r^{-m} a_2 a_2 = a_r^m \gamma_q^{-2} a_r^{-m} = \gamma_q^{-2\breve{\tau}^m},$$

which generates $\mathcal{C}_q$. So $\widehat{G}$ contains $\mathcal{C}_q$. We also have $\{\breve{b}, \breve{c}\} = \{a_2 a_r^m, a_2\gamma_p\}$. Since $\mathcal{C}_2$ inverts $\mathcal{C}_p$, this implies

$$[\breve{b}, \breve{c}] = [a_2 a_r^m, a_2\gamma_p] = a_2 a_r^m a_2 \gamma_p a_r^{-m} a_2 \gamma_p^{-1} a_2 = a_r^m \gamma_p a_r^{-m} \gamma_p = \gamma_p^{\widehat{\tau}^m + 1}.$$

We can assume this does not generate $\mathcal{C}_p$, for otherwise $\breve{G}$ contains $\mathcal{C}_p$. Therefore $0 \equiv \widehat{\tau}^m + 1 \pmod p$, which implies $\widehat{\tau}^m \equiv -1 \pmod p$. Thus, by Lemma 2.5.3, $\widehat{\tau} \equiv 1 \pmod p$, which is not possible.

Case 3.5.2 Assume $a = a_2 a_r$ and $b = a_2\gamma_q$. If $k \neq 0$, then by Lemma 2.5.2 (1), $\langle a, c\rangle = G$, which contradicts the minimality of S. So we can assume $k = 0$. Then $c = a_2^i a_r^j \gamma_p$.

If $j \neq 0$, then we show that $\langle b, c\rangle = G$ which contradicts the minimality of S. We have $\langle \overline{b}, \overline{c}\rangle = \langle a_2, a_2^i, a_r^j\rangle = \overline{G}$. Also, $\{\widehat{b}, \widehat{c}\} = \{a_2\gamma_q, a_2^i a_r^j\}$. Since $\mathcal{C}_2$ inverts $\mathcal{C}_q$, this implies

$$[\widehat{b}, \widehat{c}] = [a_2\gamma_q, a_2^i a_r^j] = a_2 \gamma_q a_2^i a_r^j \gamma_q^{-1} a_2 a_r^{-j} a_2^i = \gamma_q^{-1} a_2^{i+1} a_r^j \gamma_q^{-1} a_r^{-j} a_2^{i+1} = \gamma_q^{-1 \mp \breve{\tau}^j}.$$

We can assume this does not generate $\mathcal{C}_q$, for otherwise $\widehat{G}$ contains $\mathcal{C}_q$. Therefore $0 \equiv -1 \mp \breve{\tau}^j \pmod q$, which implies $\breve{\tau}^j \equiv \pm 1 \pmod q$. Thus, by Lemma 2.5.3, $\breve{\tau} \equiv 1 \pmod q$, which is not possible. We also have $\{\breve{b}, \breve{c}\} = \{a_2, a_2^i a_r^j \gamma_p\}$. Since $\mathcal{C}_2$ inverts $\mathcal{C}_p$, this implies

$$[\breve{b}, \breve{c}] = [a_2, a_2^i a_r^j \gamma_p] = a_2 a_2^i a_r^j \gamma_p a_2 \gamma_p^{-1} a_r^{-j} a_2^i = a_2^{i+1} a_r^j \gamma_p^2 a_r^{-j} a_2^{i+1} = \gamma_p^{\mp 2\widehat{\tau}^j}$$

which generates $\mathcal{C}_p$. Thus $\breve{G}$ contains $\mathcal{C}_p$.

So we can assume $j = 0$. Then $i \neq 0$ and $c = a_2\gamma_p$. Consider $\overline{G} = \mathcal{C}_2 \times \mathcal{C}_r$. Then $\overline{a} = a_2 a_r$, and $\overline{b} = \overline{c} = a_2$. We have $C = (\overline{c}, \overline{a}^{r-1}, \overline{b}^{-1}, \overline{a}^{-(r-1)})$ 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 γ_q, by Lemma 2.2.6 we conclude that the subgroup generated by $\mathbb{V}(C)$ contains $\mathcal{C}_q$. Similarly, since there is one occurrence of c in C, and it is the only generator of G that contains γ_p, by Lemma 2.2.6 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 2.2.4 applies.

Case 3.5.3 Assume $a = a_2a_r$ and $b = a_r^m\gamma_q$, where $1 \leqslant m \leqslant r-1$. If $k \neq 0$, then by Lemma 2.5.2 (1), $\langle a, c\rangle = G$, which contradicts the minimality of S. So we can assume $k = 0$.

If $i \neq 0$, then $c = a_2a_r^j\gamma_p$. Now we show that $\langle b, c\rangle = G$, which contradicts the minimality of S. We have $\langle \overline{b}, \overline{c}\rangle = \langle a_r^m, a_2a_r^j\rangle = \overline{G}$. Also $\{\widehat{b}, \widehat{c}\} = \{a_r^m\gamma_q, a_2a_r^j\}$. Since $\mathcal{C}_2$ inverts $\mathcal{C}_q$, this implies

$$\begin{aligned}[\widehat{b}, \widehat{c}] &= [a_r^m\gamma_q, a_2a_r^j] = a_r^m\gamma_q a_2 a_r^j \gamma_q^{-1} a_r^{-m} a_r^{-j} a_2 \\ &= a_r^m \gamma_q a_r^j \gamma_q a_r^{-m-j} = \gamma_q^{\check{\tau}^m + \check{\tau}^{m+j}} = \gamma_q^{\check{\tau}^m(1+\check{\tau}^j)}.\end{aligned}$$

We may assume this does not generate $\mathcal{C}_q$, for otherwise $\widehat{G}$ contains $\mathcal{C}_q$. Therefore $0 \equiv 1 + \check{\tau}^j \pmod q$, which implies $\check{\tau}^j \equiv -1 \pmod q$. Thus, by Lemma 2.5.3, $\check{\tau} \equiv 1 \pmod q$, which is not possible. We also have $\{\check{b}, \check{c}\} = \{a_r^m, a_2a_r^j\gamma_p\}$. Since $\mathcal{C}_2$ inverts $\mathcal{C}_p$, this implies

$$[\check{b}, \check{c}] = [a_r^m, a_2a_r^j\gamma_p] = a_r^m a_2 a_r^j \gamma_p a_r^{-m} \gamma_p^{-1} a_r^{-j} a_2 = a_r^{m+j} \gamma_p^{-1} a_r^{-m} \gamma_p a_r^{-j} = \gamma_p^{-\hat{\tau}^j(\hat{\tau}^m - 1)}.$$

We can assume this does not generate $\mathcal{C}_p$, for otherwise $\check{G}$ contains $\mathcal{C}_p$. Therefore $0 \equiv \hat{\tau}^m - 1 \pmod p$, which implies $\hat{\tau}^m \equiv 1 \pmod p$. Thus, by Lemma 2.5.3, $\hat{\tau} \equiv 1 \pmod p$, which is not possible.

So we may assume $i = 0$. Then $j \neq 0$ and $c = a_r^j\gamma_p$. Consider $\overline{G} = \mathcal{C}_2 \times \mathcal{C}_r$. Then $\overline{a} = a_2a_r$, $\overline{b} = a_r^m$, and $\overline{c} = a_r^j$.

Suppose, for the moment, that $m = j$. Then $\overline{b} = \overline{c}$. We have

$$C_1 = (\overline{c}^{-(r-1)}, \overline{a}^{-1}, \overline{b}^{r-1}, \overline{a})$$

as a Hamiltonian cycle in $\mathrm{Cay}(\overline{G};\overline{S})$. Since $c^r = e$, this implies $c^{-(r-1)} = c = a_r^j\gamma_p$. This is the only occurrence of γ_p in $\mathbb{V}(C_1)$. So the subgroup generated by $\mathbb{V}(C_1)$ contains $\mathcal{C}_p$. Similarly, since $b^r = e$, it follows that $b^{r-1} = b^{-1} = \gamma_q^{-1}a_r^{-m}$. This is the only occurrence of γ_q in $\mathbb{V}(C_1)$. So the subgroup generated by $\mathbb{V}(C_1)$ contains $\mathcal{C}_q$. Hence the subgroup generated by $\mathbb{V}(C_1)$ contains G'. Therefore Factor Group Lemma 2.2.4 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 $r - m$, and j with $r - j$, if necessary.

Subcase 3.5.3.1 Assume $j = 2$. Then we have $c = a_r^2\gamma_p$. We also have

$$C_2 = (\overline{b}, \overline{c}^{-(m-2)/2}, \overline{a}^{-1}, \overline{c}^{m/2}, \overline{a}^{2r-m-1})$$

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 γ_q, by Lemma 2.2.6 we conclude that the subgroup generated by $\mathbb{V}(C_2)$ contains $\mathcal{C}_q$. Also,

$$\begin{aligned}
\mathbb{V}(C_2) &= bc^{-(m-2)/2}a^{-1}c^{m/2}a^{2r-m-1} \\
&\equiv a_r^m \cdot (a_r^2\gamma_p)^{-(m-2)/2} \cdot a_r^{-1}a_2 \cdot (a_r^2\gamma_p)^{m/2} \cdot (a_2a_r)^{2r-m-1} \pmod{\mathcal{C}_q} \\
&= a_r^m(\gamma_p^{\widehat{\tau}^2+(\widehat{\tau}^2)^2+\ldots+(\widehat{\tau}^2)^{(m-2)/2}}a_r^{m-2})^{-1}a_r^{-1}a_2(\gamma_p^{\widehat{\tau}^2+(\widehat{\tau}^2)^2+\ldots+(\widehat{\tau}^2)^{m/2}}a_r^m)a_2a_r^{2r-m-1} \\
&= a_r^2\gamma_p^{-(\widehat{\tau}^2+(\widehat{\tau}^2)^2+\ldots+(\widehat{\tau}^2)^{(m-2)/2})}a_r^{-1}\gamma_p^{-(\widehat{\tau}^2+(\widehat{\tau}^2)^2+\ldots+(\widehat{\tau}^2)^{m/2})}a_r^{-1} \\
&= \gamma_p^{-\widehat{\tau}^2(\widehat{\tau}^2+(\widehat{\tau}^2)^2+\ldots+(\widehat{\tau}^2)^{(m-2)/2})-\widehat{\tau}(\widehat{\tau}^2+(\widehat{\tau}^2)^2+\ldots+(\widehat{\tau}^2)^{m/2})} \\
&= \gamma_p^{-\widehat{\tau}^4(1+\widehat{\tau}^2+\ldots+(\widehat{\tau}^2)^{(m-4)/2})-\widehat{\tau}^3(1+\widehat{\tau}^2+\ldots+(\widehat{\tau}^2)^{(m-2)/2})} \\
&= \gamma_p^{-\widehat{\tau}^3(\widehat{\tau}(\widehat{\tau}^{m-2}-1)/(\widehat{\tau}^2-1)+(\widehat{\tau}^m-1)/(\widehat{\tau}^2-1))} \\
&= \gamma_p^{-\widehat{\tau}^3(\widehat{\tau}^{m-1}-\widehat{\tau}+\widehat{\tau}^m-1)/(\widehat{\tau}^2-1)}.
\end{aligned}$$

We can assume this does not generate $\mathcal{C}_p$, for otherwise Factor Group Lemma 2.2.4 applies. Therefore, either $0 \equiv \widehat{\tau}^2 - 1 \pmod{p}$ or

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

The first case is not possible, so we may assume

$$\begin{aligned}
0 &\equiv \widehat{\tau}^{m-1} - \widehat{\tau} + \widehat{\tau}^m - 1 \pmod{p} \\
&= (\widehat{\tau}^{m-1} - 1)(\widehat{\tau} + 1),
\end{aligned}$$

which implies $\widehat{\tau}^{m-1} \equiv 1 \pmod{p}$. We also know $\widehat{\tau}^r \equiv 1 \pmod{p}$. So $\widehat{\tau}^d \equiv 1 \pmod{p}$, where $d = \gcd(m-1, r)$. Since $2 \leqslant m \leqslant r-1$, this implies $d = 1$. Thus $\widehat{\tau} \equiv 1 \pmod{p}$, which is not possible.

Subcase 3.5.3.2 Assume $j \neq 2$. We have

$$C_3 = (\overline{b}, \overline{c}, \overline{a}, \overline{c}^{-1}, \overline{b}^{-1}, \overline{a}^{m-2}, \overline{c}, \overline{a}^{-(j-3)}, \overline{c}, \overline{a}^{2r-m-j-2})$$

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

$$\begin{aligned}
\mathbb{V}(C_3) &= bcac^{-1}b^{-1}a^{m-2}ca^{-(j-3)}ca^{2r-m-j-2} \\
&\equiv a_r^m\gamma_q \cdot a_r^j \cdot a_2a_r \cdot a_r^{-j} \cdot \gamma_q^{-1}a_r^{-m} \cdot (a_2a_r)^{m-2} \\
&\quad \cdot a_r^j \cdot (a_2a_r)^{-(j-3)} \cdot a_r^j \cdot (a_2a_r)^{2r-m-j-2} \pmod{\mathcal{C}_p} \\
&= a_r^m\gamma_q a_r^j a_2 a_r a_r^{-j}\gamma_q^{-1}a_r^{-m}a_r^{m-2}a_r^j a_r^{-j+3}a_2a_r^j a_r^{2r-m-j-2} \\
&= a_r^m\gamma_q a_r\gamma_q a_r^{-m-1}
\end{aligned}$$

$$\begin{aligned} &= \gamma_q^{\breve{\tau}^m + \breve{\tau}^{m+1}} \\ &= \gamma_q^{\breve{\tau}^m (1+\breve{\tau})}, \end{aligned}$$

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

$$\begin{aligned} \mathbb{V}(C_3) &= bcac^{-1}b^{-1}a^{m-2}ca^{-(j-3)}ca^{2r-m-j-2} \\ &\equiv a_r^m \cdot a_r^j\gamma_p \cdot a_2a_r \cdot \gamma_p^{-1}a_r^{-j} \cdot a_r^{-m} \cdot (a_2a_r)^{m-2} \cdot a_r^j\gamma_p \\ &\cdot (a_2a_r)^{-(j-3)} \cdot a_r^j\gamma_p \cdot (a_2a_r)^{2r-m-j-2} \pmod{\mathcal{C}_q} \\ &= a_r^{m+j}\gamma_p a_2 a_r \gamma_p^{-1} a_r^{-j-m} a_r^{m-2} a_r^j \gamma_p a_r^{-j+3} a_2 a_r^j \gamma_p a_r^{2r-m-j-2} \\ &= a_r^{m+j}\gamma_p a_r \gamma_p a_r^{-2}\gamma_p^{-1} a_r^3 \gamma_p a_r^{-m-j-2} \\ &= \gamma_p^{\widehat{\tau}^{m+j} + \widehat{\tau}^{m+j+1} - \widehat{\tau}^{m+j-1} + \widehat{\tau}^{m+j+2}} \\ &= \gamma_p^{\widehat{\tau}^{m+j-1}(\widehat{\tau}^3 + \widehat{\tau}^2 + \widehat{\tau} - 1)}. \end{aligned}$$

We can assume this does not generate $\mathcal{C}_p$, for otherwise Factor Group Lemma 2.2.4 applies. Therefore,

$$0 \equiv \widehat{\tau}^3 + \widehat{\tau}^2 + \widehat{\tau} - 1 \pmod{p}. \tag{3.5.A}$$

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. So we have

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

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

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

By adding (3.5.A) and 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 implies $\widehat{\tau} \equiv -1 \pmod{p}$, which is not possible.

Case 3.5.4 Assume $a = a_r$ and $b = a_2\gamma_q$.

Subcase 3.5.4.1 Assume $i = 0$. Then $j \neq 0$ and $c = a_r^j\gamma_q^k\gamma_p$.

Consider $\overline{G} = \mathcal{C}_2 \times \mathcal{C}_r$. Then $\overline{a} = a_r$, $\overline{b} = a_2$, and $\overline{c} = a_r^j$. We may assume j is odd by replacing c with its inverse and j with $r - j$ if necessary. We have

$$C_1 = (\overline{c}, \overline{a}^{r-j-1}, \overline{b}, \overline{a}^{-(r-j-1)}, \overline{c}^{-1}, \overline{a}^{j-1}, \overline{b}, \overline{a}^{-(j-1)})$$

and

$$C_2 = (\overline{a}^{r-j-1}, \overline{c}, \overline{a}^{-(j-1)}, \overline{b}, \overline{a}^{j-1}, \overline{c}^{-1}, \overline{a}^{-(r-j-1)}, \overline{b})$$

as Hamiltonian cycles in $\mathrm{Cay}(\overline{G};\overline{S})$. Now we calculate the voltage of C_1.

$$\begin{aligned}
\mathbb{V}(C_1) &= ca^{r-j-1}ba^{-(r-j-1)}c^{-1}a^{j-1}ba^{-(j-1)} \\
&\equiv a_r^j\gamma_p \cdot a_r^{r-j-1} \cdot a_2 \cdot a_r^{-(r-j-1)} \cdot \gamma_p^{-1}a_r^{-j} \cdot a_r^{j-1} \cdot a_2 \cdot a_r^{-(j-1)} \pmod{\mathcal{C}_q} \\
&= a_r^j\gamma_p a_r^{r-j-1}a_r^{-(r-j-1)}\gamma_p a_r^{-j}a_r^{j-1}a_r^{-(j-1)} \\
&= a_r^j\gamma_p^2 a_r^{-j} \\
&= \gamma_p^{2\hat{\tau}^j},
\end{aligned}$$

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

$$\begin{aligned}
\mathbb{V}(C_1) &= ca^{r-j-1}ba^{-(r-j-1)}c^{-1}a^{j-1}ba^{-(j-1)} \\
&\equiv a_r^j\gamma_q^k \cdot a_r^{r-j-1} \cdot a_2\gamma_q \cdot a_r^{-(r-j-1)} \cdot \gamma_q^{-k}a_r^{-j} \cdot a_r^{j-1} \cdot a_2\gamma_q \cdot a_r^{-(j-1)} \pmod{\mathcal{C}_p} \\
&= a_r^j\gamma_q^k a_r^{-j-1}\gamma_q^{-1}a_r^{j+1}\gamma_q^k a_r^{-1}\gamma_q a_r^{-j+1} \\
&= \gamma_q^{k\check{\tau}^j-\check{\tau}^{-1}+k\check{\tau}^j+\check{\tau}^{j-1}} \\
&= \gamma_q^{2k\check{\tau}^j+\check{\tau}^{j-1}-\check{\tau}^{-1}}.
\end{aligned}$$

We can assume this does not generate $\mathcal{C}_q$, for otherwise Factor Group Lemma 2.2.4 applies. Therefore,

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

Multiplying by $\check{\tau}$, we have

$$0 \equiv 2k\check{\tau}^{j+1} + \check{\tau}^j - 1 \pmod{q}. \tag{3.5.B}$$

Now we calculate the voltage of C_2.

$$\begin{aligned}
\mathbb{V}(C_2) &= a^{r-j-1}ca^{-(j-1)}ba^{j-1}c^{-1}a^{-(r-j-1)}b \\
&\equiv a_r^{r-j-1} \cdot a_r^j\gamma_p \cdot a_r^{-(j-1)} \cdot a_2 \cdot a_r^{j-1} \cdot \gamma_p^{-1}a_r^{-j} \cdot a_r^{-(r-j-1)} \cdot a_2 \pmod{\mathcal{C}_q} \\
&= a_r^{-1}\gamma_p a_2\gamma_p^{-1}a_r a_2 \\
&= a_r^{-1}\gamma_p^2 a_r \\
&= \gamma_p^{\hat{\tau}^{-1}},
\end{aligned}$$

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

$$\begin{aligned}
\mathbb{V}(C_2) &= a^{r-j-1}ca^{-(j-1)}ba^{j-1}c^{-1}a^{-(r-j-1)}b \\
&\equiv a_r^{r-j-1} \cdot a_r^j\gamma_q^k \cdot a_r^{-(j-1)} \cdot a_2\gamma_q \cdot a_r^{j-1} \cdot \gamma_q^{-k}a_r^{-j} \cdot a_r^{-(r-j-1)} \cdot a_2\gamma_q \pmod{\mathcal{C}_p} \\
&= a_r^{-1}\gamma_q^k a_r^{-j+1}a_2\gamma_q a_r^{j-1}\gamma_q^{-k}a_r a_2\gamma_q \\
&= a_r^{-1}\gamma_q^k a_r^{-j+1}\gamma_q^{-1}a_r^{j-1}\gamma_q^k a_r\gamma_q \\
&= \gamma_q^{k\check{\tau}^{-1}-\check{\tau}^{-j}+k\check{\tau}^{-1}+1} \\
&= \gamma_q^{1+2k\check{\tau}^{-1}-\check{\tau}^{-j}}.
\end{aligned}$$

We may assume this does not generate $\mathcal{C}_q$, for otherwise Factor Group Lemma 2.2.4 applies. Therefore,

$$0 \equiv 1 + 2k\breve{\tau}^{-1} - \breve{\tau}^{-j} \pmod q$$

Multiplying by $\breve{\tau}^{j+2}$, we have

$$0 \equiv \breve{\tau}^{j+2} + 2k\breve{\tau}^{j+1} - \breve{\tau}^{2} \pmod q.$$

By subtracting (3.5.B) from the above equation, we have

$$\begin{aligned} 0 &\equiv \breve{\tau}^{j+2} - \breve{\tau}^{j} - \breve{\tau}^{2} + 1 \pmod q \\ &= (\breve{\tau}^{j} - 1)(\breve{\tau}^{2} - 1). \end{aligned}$$

This implies that $\breve{\tau}^j \equiv 1 \pmod q$. Thus, by Lemma 2.5.3, $\breve{\tau} \equiv 1 \pmod q$, which is not possible.

Subcase 3.5.4.2 Assume $i \neq 0$. Then $c = a_2 a_r^j \gamma_q^k \gamma_p$. If $k \neq 0$, then by Lemma 2.5.2 (3), $\langle a, c \rangle = G$, which contradicts the minimality of S. So we may assume $k = 0$, and then $c = a_2 a_r^j \gamma_p$.

Suppose, for the moment, that $j \neq 0$; then we show that $\langle b, c \rangle = G$, which contradicts the minimality of S. We have $\langle \overline{b}, \overline{c} \rangle = \langle a_2, a_2 a_r^j \rangle = \overline{G}$. We also have $\{\widehat{b}, \widehat{c}\} = \{a_2\gamma_q, a_2 a_r^j\}$. Since $\mathcal{C}_2$ inverts $\mathcal{C}_q$, this implies

$$[\widehat{b}, \widehat{c}] = [a_2\gamma_q, a_2 a_r^j] = a_2\gamma_q a_2 a_r^j \gamma_q^{-1} a_2 a_r^{-j} a_2 = \gamma_q^{-1} a_r^j \gamma_q^{-1} a_r^{-j} = \gamma_q^{-1-\breve{\tau}^j}.$$

We can assume this does not generate $\mathcal{C}_q$, for otherwise $\widehat{G}$ contains $\mathcal{C}_q$. Therefore, $0 \equiv -1 - \breve{\tau}^j \pmod q$ which implies $\breve{\tau}^j \equiv -1 \pmod q$. So by Lemma 2.5.3 $\breve{\tau} \equiv 1 \pmod q$ which is not possible. Also, we have $\{\breve{b}, \breve{c}\} = \{a_2, a_2 a_r^j \gamma_p\}$. Since $\mathcal{C}_2$ inverts $\mathcal{C}_p$, this implies

$$[\breve{b}, \breve{c}] = [a_2, a_2 a_r^j \gamma_p] = a_2 a_2 a_r^j \gamma_p a_2 \gamma_p^{-1} a_r^{-j} a_2 = a_r^j \gamma_p^2 a_r^{-j} = \gamma_p^{2\hat{\tau}^j},$$

which generates $\mathcal{C}_p$. Thus, $\langle b, c \rangle = G$.

So we can assume $j = 0$. Then $c = a_2\gamma_p$. Consider $\overline{G} = \mathcal{C}_2 \times \mathcal{C}_r$. Then $\overline{a} = a_r$, and $\overline{b} = \overline{c} = a_2$. We have $C = (\overline{b}, \overline{a}^{r-1}, \overline{c}^{-1}, \overline{a}^{-(r-1)})$ 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 γ_q, by Lemma 2.2.6 we conclude that the subgroup generated by $\mathbb{V}(C)$ contains $\mathcal{C}_q$. Similarly, since there is one occurrence of c in C, and it is the only generator of G that contains γ_p, by Lemma 2.2.6 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 2.2.4 applies.

The proof of Theorem 1.4 is now completed by applying Propositions 3.1.1, 3.2.1, 3.3.1 and 3.4.1.

□

Acknowledgements

I am grateful to Professor Dave Morris for introducing me to this area of mathematics and for guiding me patiently.

References

[1] A. Cayley, Desiderata and Suggestions: No. 2, The Theory of Groups: Graphical Representation, *Amer. J. Math.* **1** (1878), 174–176. https://doi.org/10.2307/2369306.

[2] C. C. Chen and N. F. Quimpo, On some classes of hamiltonian graphs, *Southeast Asian Bull. Math.* (1979), 252–258. https://scopus.com/inward/record.url?eid=2-s2.0-0041913857&partnerID=10&rel=R3.0.0.

[3] S. J. Curran and J. A. Gallian, Hamiltonian cycles and paths in Cayley graphs and digraphs—a survey, *Discrete Math.* **156** (1996), 1–18. https://doi-org.proxy.library.carleton.ca/10.1016/0012-365X(95)00072-5.

[4] E. Durnberger, Connected Cayley graphs of semidirect products of cyclic groups of prime order by abelian groups are hamiltonian, *Discrete Math.* **46** (1983), 55–68. https://doi.org/10.1016/0012-365X(83)90270-4.

[5] E. Durnberger, Every connected Cayley graph of a group with prime order commutator group has a hamilton cycle, *North-Holland, Amsterdam* **115** (1985), 75–80. https://doi.org/10.1016/S0304-0208(08)72997-9.

[6] E. Ghaderpour and D. W. Morris, Cayley graphs of order $30p$ are hamiltonian, *Discrete Math.* **312** (2012), 3614–3625. https://doi.org/10.1016/j.disc.2012.08.017.

[7] C. Godsil and G. Royle, *Algebraic Graph Theory*, Springer, New York, 2001. https://doi.org/10.1007/978-1-4613-0163-9.

[8] M. Hall, *The Theory of Groups*, Macmillan Company, New York, N.Y., 1959.

[9] K. Keating and D. W. Morris, On hamilton cycles in Cayley graphs in groups with cyclic commutator subgroup, *North-Holland, Amsterdam* **115** (1985), 89–102. https://doi.org/10.1016/S0304-0208(08)72999-2.

[10] E. Konstantinova, Some problems on Cayley graphs, *Linear Algebra Appl.* **429** (2008), 2754–2769. https://doi.org/10.1016/j.laa.2008.05.010.

[11] 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** (2012), 27–71. https://doi.org/10.26493/1855-3974.177.341.

[12] G. H. Lanel, H. K. Pallage, J. K. Ratnayake, S. Thevasha and B. A. K. Welihinda, A survey on hamiltonicity in Cayley graphs and digraphs on different groups, *Discrete Math. Algorithms Appl.* **11** (2019), 1930002. https://doi-org.proxy.library.carleton.ca/10.1142/s1793830919300029.

[13] F. Maghsoudi, Cayley graphs of order $6pq$ and $7pq$ are hamiltonian, *Art Discrete Appl. Math.* **53** (2022). https://doi.org/10.26493/2590-9770.1389.fa2.

[14] D. Marušič, Hamiltonian circuits in Cayley graphs, *Discrete Math.* **46** (1983), 49–54. https://doi.org/10.1016/0012-365X(83)90269-8.

[15] D.W. Morris, On hamiltonian cycles in Cayley graphs of order $pqrs$, *arxiv* (2021). https://arxiv.org/abs/2107.14787.

[16] D. W. Morris and K. Wilk, Cayley graphs of order kp are hamiltonian for $k < 48$, *Art Discrete Appl. Math.* **17** (2020). https://doi.org/10.26493/2590-9770.1250.763.

[17] D. J. S. Robinson, *A Course in the Theory of Groups*, Springer, New York, 1996. https://doi.org/10.1007/978-1-4419-8594-1.

[18] D. Witte, Cayley digraphs of prime-power order are hamiltonian, *J. Combin. Theory Ser. B.* **40** (1986), 107–112. https://doi.org/10.1016/0095-8956(86)90068-7.

[19] D. Witte and J. A. Gallian, A survey: Hamiltonian cycles in Cayley graphs, *Discrete Math.* **51** (1984), 293–304. https://doi.org/10.1016/0012-365X(84)90010-4.

[20] D. S. Witte, On hamiltonian circuits in Cayley diagrams, *Discrete Math.* **38** (1982), 99–108. https://doi.org/10.1016/0012-365X(82)90174-1.

(Received 15 Sep 2021; revised 21 Jan 2022, 21 June 2022)