CAYLEY GRAPHS OF ORDER $pqrs$ ARE HAMILTONIAN

FLORIAN LEHNER, FARZAD MAGHSOUDI, AND BOBBY MIRAFTAB

ABSTRACT. Assume G is a finite group with order $|G| = pqrs$, where p, q, r, and s are distinct prime numbers. We prove that every connected Cayley graph of G contains a hamiltonian cycle. Our result drops all restrictions of all previously known results on hamiltonian cycles in Cayley graphs of groups of order $pqrs$.

1. INTRODUCTION

A well-known conjecture by Lovász states that every finite connected vertex-transitive graph contains a hamiltonian path [2]. So far, there are numerous papers about this conjecture in finite and infinite settings (see [5, 8, 9, 10, 16, 19]), but no counterexample to this conjecture has been found.

A related and extensively studied problem concerns the existence of hamiltonian cycles in vertex-transitive graphs. Thomassen [4, 14] conjectured that there are only finitely many connected vertex-transitive graphs without a hamiltonian cycle. In contrast, Babai proposed that there are infinitely many such graphs [2, 3]. Currently, only five connected vertex-transitive graphs are known to lack a hamiltonian cycle: the complete graph K_2, the Petersen graph, the Coxeter graph, and two graphs obtained by replacing each vertex of the Petersen and Coxeter graphs with a triangle.

The problem has also been extensively studied in the context of Cayley graphs. For instance, it is known that Cayley graphs of specific orders contain hamiltonian cycles.

Theorem 1.1 ([1, 15, 17, 20, 21, 22])**.** *Let G be a finite group. If $|G|$ has any of the following forms (where p, q, r, s are distinct primes), then every connected Cayley graph of G contains a hamiltonian cycle:*

(1) kp, where $1 \leqslant k \leqslant 47$,
(2) kpq, where $1 \leqslant k \leqslant 9$,
(3) pqr,
(4) $pqrs$, where p, q, r, and s are odd distinct primes,
(5) kp^2, where $1 \leqslant k \leqslant 4$,
(6) kp^3, where $1 \leqslant k \leqslant 2$,
(7) p^k, where $1 \leqslant k < \infty$.

Furthermore, in [18], the hamiltonicity of Cayley graphs of groups of order $pqrs$, where p, q, r, and s are distinct prime numbers, was studied. More specifically,

Theorem 1.2 ([18, Theorem 1.4])**.** *Assume G is a finite group of order $pqrs$ with a minimal generating set S, where p, q, r, and s are distinct primes. If $|S| \geqslant 3$, then $\mathrm{Cay}(G; S)$ contains a hamiltonian cycle.*

2010 *Mathematics Subject Classification.* 05C25, 05C45 .
Key words and phrases. Cayley graphs, hamiltonian cycles.

In this paper, we drop the condition on the size of S, and we prove the following.

Theorem 1.3. *Assume $G = \langle S \rangle$ is a finite group of order $pqrs$, where p, q, r, and s are distinct primes. Then $\mathrm{Cay}(G; S)$ has a hamiltonian cycle.*

An overview of the proof techniques: The case $|S| = 1$ is trivial. Moreover, we may apply parts (2) and (4) of Theorem 1.1, and Theorem 1.2, so we only need to prove the following.

Theorem 1.4. *Assume $G = \langle S \rangle$ is a finite group of order $2pqr$, such that $|S| = 2$, where p, q, and r are distinct primes, and $p, q, r \geqslant 5$. Then $\mathrm{Cay}(G; S)$ has a hamiltonian cycle.*

Since the group G is generated by two elements, a and b, we analyze three distinct cases based on the orders of a and b. In each case, we first consider the quotient group $\overline{G} = G/G'$, where G' is the commutator subgroup of G. Using the images $\overline{a}$ and $\overline{b}$ in this quotient group, we attempt to construct a hamiltonian cycle in $\mathrm{Cay}(\overline{G}; \{\overline{a}, \overline{b}\})$. If this hamiltonian cycle lifts to a hamiltonian cycle in the Cayley graph of G, we are done.

If there is no such hamiltonian cycle that can be lifted, we consider the quotient groups $\widehat{G} = G/\langle \gamma_p \rangle$ or $\check{G} = G/\langle \gamma_q \rangle$, where γ_p and γ_q are generators of cyclic subgroups of G of orders p and q, respectively. In these quotient groups, we again aim to identify at least one hamiltonian cycle that can successfully be lifted. A key ingredient to our proof is identifying spanning generalized Petersen graphs contained in Cayley graphs of these quotient groups; hamiltonian cycles inside such a spanning subgraph can be shown to lift to hamiltonian cycles of $\mathrm{Cay}(G; S)$.

2. Preliminaries

This section establishes basic terminology and notation, and states a number of results that will be used in the proof of Theorem 1.4. All graphs in this paper are undirected and do not contain loops, but may contain parallel edges; all groups are finite.

Following [15, Definition 1.1] and [12, p. 34], if $G = \langle S \rangle$, 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 commutator $ghg^{-1}h^{-1}$ of g and h is denoted by $[g, h]$. The derived subgroup G' is the subgroup of G generated by all commutators, and we write $\overline{G} = G/G'$. Moreover, we write $\overline{g} = gG'$ for any $g \in G$, and $\overline{S} = \{\overline{g}; g \in S\}$ for any $S \subseteq G$.

The notation $G \ltimes H$ denotes a semidirect product of groups G and H, where H is normal. We write D_{2n} for the dihedral group of order $2n$, and e for the identity element of G. The symbol $\mathcal{C}_n$ denotes the cyclic group of order n.

For $S \subseteq G$, a sequence $(s_1, s_2, \ldots, s_n)$ of elements of $S \cup S^{-1}$ specifies the walk in $\mathrm{Cay}(G; S)$ that visits the vertices $e, s_1, s_1s_2, \ldots, s_1s_2 \cdots s_n$. Its inverse is $(s_1, s_2, \ldots, s_n)^{-1} = (s_n^{-1}, s_{n-1}^{-1}, \ldots, s_1^{-1})$. For $k \in \mathbb{Z}^+$, the notation $(s_1, s_2, \ldots, s_m)^k$ denotes the concatenation of k copies of the sequence $(s_1, s_2, \ldots, s_m)$, and by extension also the walk corresponding to this sequence. We use $(\overline{s_1}, \overline{s_2}, \ldots, \overline{s_n})$ to denote the image of this walk in $\mathrm{Cay}(G/G'; \overline{S}) = \mathrm{Cay}(\overline{G}; \overline{S})$. When a power s^k appears as one entry of a sequence defining a walk, we tacitly assume that it denotes $|k|$ consecutive steps labelled s if $k > 0$, $|k|$ consecutive steps labelled s^{-1} if $k < 0$, and the empty sequence if $k = 0$.

Fix a group $G = \langle a, b \rangle$ of order $2pqr$, and let a_2, a_r, γ_p, and γ_q denote elements of G of orders 2, r, p, and q, respectively. We denote the subgroups of G generated by these elements by $\mathbb{Z}_2$, $\mathbb{Z}_r$, $\mathbb{Z}_p$, and $\mathbb{Z}_q$. If $\mathbb{Z}_p$ is normal, we write $\widehat{G} = G/\mathbb{Z}_p$; if $\mathbb{Z}_q$ is normal, we

write $\breve{G} = G/\mathbb{Z}_q$. Moreover, in these cases we define $\widehat{g} = g\mathbb{Z}_p$, $\breve{g} = g\mathbb{Z}_q$ for any $g \in G$, and $\widehat{S} = \{\widehat{g}; g \in S\}$, $\breve{S} = \{\breve{g}; g \in S\}$ for any $S \subseteq G$.

In the remainder of this section we provide some known results which will be used in the proof of Theorem 1.4. The following well-known result handles the special case where G is abelian.

Lemma 2.1 ([6, Corollary on page 257]). *Assume G is a non-trivial abelian group. Then every connected Cayley graph on G has a hamiltonian cycle.*

The next lemma (and its corollary) often provides a way to lift a hamiltonian cycle in $\mathrm{Cay}(G/N; SN)$ to a hamiltonian cycle in $\mathrm{Cay}(G; S)$. Before stating the results, we introduce a useful piece of notation.

Notation 2.2. Suppose N is a normal subgroup of G, and let $(s_1, s_2, \ldots, s_n)$ be a sequence of elements in $S \cup S^{-1}$. If the walk $(s_1N, s_2N, \ldots, s_nN)$ in $\mathrm{Cay}(G/N; SN/N)$ is closed, then its *voltage* is the product $\mathsf{Volt}(C) = s_1s_2\cdots s_n$. This is an element of N. In particular, if $C = (\overline{s}_1, \overline{s}_2, \ldots, \overline{s}_n)$ is a hamiltonian cycle in $\mathrm{Cay}(\overline{G}; \overline{S})$, then $\mathsf{Volt}(C) = s_1s_2\cdots s_n$.

Note that it is possible that there are elements $s, t \in S$ such that $sN = tN$, so the voltage indeed depends on the elements s_i, not just on the cosets s_iN.

Factor Group Lemma 2.3 ([23, Section 2.2]). *Let $G = \langle S\rangle$ and let N be a cyclic normal subgroup of G. If $C = (s_1N, \ldots s_nN)$ is a hamiltonian cycle in $\mathrm{Cay}(G/N; SN/N)$ such that $\mathsf{Volt}(C)$ generates N, then there is a hamiltonian cycle in $\mathrm{Cay}(G; S)$.*

Corollary 2.4 ([11, Corollary 2.3]). *Let $G = \langle S\rangle$ and let N be a normal subgroup of G of prime order. Assume that there are $s, t \in S$ such that $sN = tN$. If there is a hamiltonian cycle in $\mathrm{Cay}(G/N; SN/N)$ which uses at least one edge corresponding to the generator sN, then there is a hamiltonian cycle in $\mathrm{Cay}(G; S)$.*

Lemma 2.5 ([17, Lemma 2.16]). *Assume $G = (\mathbb{Z}_p \times \mathbb{Z}_q) \ltimes G'$, where $G' = (\mathbb{Z}_r \times \mathbb{Z}_s)$, and p, q, r and s are distinct primes such that $(\mathbb{Z}_r \times \mathbb{Z}_s) \cap Z(G) = \{e\}$. If $|\overline{a}| = pq$, then $|a| = pq$.*

The following proposition demonstrates that we can assume $|G'|$ in Theorem 1.4 is a product of two distinct odd prime numbers. Because if $\mathbb{Z}_2 \subseteq G'$, then $G' \cong \mathbb{Z}_\ell \times \mathbb{Z}_2$, where $\ell \in \{p, q, r, pq, rq, pr\}$. Then the quotient $G/\mathbb{Z}_\ell$ is isomorphic to $\mathbb{Z}_m \ltimes \mathbb{Z}_2$, where $|G| = 2\ell m$. Since $\mathbb{Z}_m$ is normal, we have $G/\mathbb{Z}_\ell \cong \mathbb{Z}_m \times \mathbb{Z}_2$.

Proposition 2.6 ([17, 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.*

The following lemmas show that some special Cayley graphs have a hamiltonian cycle, and we use these facts in Section 4 in order to prove our main result.

Lemma 2.7. [17, Lemma 2.23] *Assume $G = (\mathbb{Z}_2 \times \mathbb{Z}_r) \ltimes G'$, and $G' = \mathbb{Z}_p \times \mathbb{Z}_q$, where p, q and r are distinct prime numbers and let $S = \{a, b\}$ be a generating set of G. Additionally, assume $|\overline{b}| \in \{2, 2r\}$, $|\overline{a}| = r$ and $\gcd(|a|, r-1) = 1$. Then $\mathrm{Cay}(G; S)$ contains a hamiltonian cycle.*

Lemma 2.8 (cf. [11, Case 2 of proof of Theorem 1.1, pages 3619–3620]). *Assume that*

$$G = (\mathbb{Z}_2 \times \mathbb{Z}_r) \ltimes (\mathbb{Z}_p \times \mathbb{Z}_q),$$

that $|S| = 3$*, that* $\widehat{S}$ *is a minimal generating set of* $\widehat{G} = G/\mathbb{Z}_p$*, that* $\mathbb{Z}_r$ *centralizes* $\mathbb{Z}_q$*, and that* $\mathbb{Z}_2$ *inverts* $\mathbb{Z}_q$*. Then,* $\mathrm{Cay}(G; S)$ *contains a hamiltonian cycle.*

Lemma 2.9. [11, Lemma 2.9] *If* $G = D_{2pq} \times \mathbb{Z}_r$*, where* p, q *and* r *are distinct odd primes, then every connected Cayley graph on* G *has a hamiltonian cycle.*

Lemma 2.10. [15, Lemma 2.27] *Let* S *generate the finite group* G*, and let* $s \in S$*, such that* $\langle s \rangle \lhd G$*. If* $\mathrm{Cay}(G/\langle s \rangle; \overline{S})$ *has a hamiltonian cycle, and either*

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

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

Lemma 2.11 ([7, Corollary 4.4])**.** *Assume* $G = \langle a, b \rangle$ *and* G' *is cyclic. Then* $G' = \langle [a, b] \rangle$*.*

Corollary 2.12. *Assume* $G = \langle a, b \rangle$ *and* $\gcd(k, |a|) = 1$*, where* $k \in \mathbb{Z}$*, and* G' *is cyclic. Then* $G' = \langle [a^k, b] \rangle$*.*

Proposition 2.13 ([13, Theorem 9.4.3 on page 146], cf. [11, Lemma 2.11])**.** *Assume* $|G|$ *is square-free. Then:*

(1) G' *and* G/G' *are cyclic,*
(2) $Z(G) \cap G' = \{e\}$*,*
(3) $G \cong \mathbb{Z}_n \ltimes G'$*, 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* $\tau^n \equiv 1 \pmod{m}$*.*

3. Generalized Petersen graphs

Definition 3.1. Let n and ℓ be coprime positive integers with $1 \leqslant \ell < n$. The *generalized Petersen graph* $GP(n, \ell)$ has vertex set

$$\{0, 1, \ldots, n-1\} \cup \{0', 1', \ldots, (n-1)'\},$$

and edge set consisting of

$$(i, i+1), \qquad (i', (i+1)'), \qquad (i, (i\ell)')$$

for $0 \leqslant i < n$, where all indices are taken modulo n. The edges $(i, i+1)$ are called the *outer rim*, the edges $(i', (i+1)')$ are called the *inner rim*, and the edges $(i, (i\ell)')$ are called the *spokes*.

Lemma 3.2. *Let* $H = \langle a, b \rangle$ *be a group of order* $2n$*. Assume that*

$$|a| = n, \qquad b \notin \langle a \rangle, \qquad b^{-1}ab = a^\ell,$$

where $\gcd(n, \ell) = 1$*. Then* $\mathrm{Cay}(H; \{a, b\})$ *contains a spanning subgraph isomorphic to* $GP(n, \ell)$ *given by the bijection*

$$a^j \longleftrightarrow j, \qquad ba^j \longleftrightarrow j', \qquad 0 \leqslant j < n.$$

Proof. Since $|a| = n$, $|H| = 2n$, and $b \notin \langle a \rangle$, the vertices of H are precisely

$$a^j, \qquad ba^j \qquad (0 \leqslant j < n).$$

The edges $a^j \sim a^{j+1}$ give the outer rim, and the edges $ba^j \sim ba^{j+1}$ give the inner rim. Finally, $a^j b = b(b^{-1}a^j b) = ba^{j\ell}$, so the edge labelled b from a^j gives the spoke $j \sim (j\ell)'$. Thus the displayed correspondence gives a spanning copy of $GP(n, \ell)$. □

Lemma 3.3. *For coprime integers n and ℓ with $1 \leqslant \ell < n$, we have $GP(n,\ell) \cong GP(n,n-\ell)$. One such isomorphism is $\varphi(i) = i$, $\varphi(j') = (-j)'$.*

Proof. The outer-rim edge $(i, i+1)$ maps to $(i, i+1)$, which is again an outer-rim edge. The inner-rim edge $(j', (j+1)')$ maps to $((-j)', (-(j+1))')$, which is an inner-rim edge with the orientation reversed. Finally, the spoke $(i, (i\ell)')$ maps to $(i, (-i\ell)')$. But in $GP(n, n-\ell)$, the spoke at i is

$$(i, (i(n-\ell))') = (i, (-i\ell)').$$

Thus φ preserves adjacency and is a bijection, so it is an isomorphism. □

Proposition 3.4. *Let p, r be odd primes with $p > 5$ and $r \equiv 1 \pmod p$. Define*

$$n = rp, \qquad \ell = r(p-2)+1, \qquad k = n-\ell = 2r-1, \qquad m = n-3k-1.$$

Suppose $H = \langle a, b\rangle$ satisfies the hypotheses of Lemma 3.2. Then the spanning copy of $GP(n,\ell)$ in $\mathrm{Cay}(H;\{a,b\})$ contains the following hamiltonian cycle:

$$\begin{aligned} C_0 = \big(&a^{-m}, b, a^{-(k-3)}, b^{-1}, a^{-1}, b, a^{k-3}, b^{-1}, a^{-(k-1)}, b, a, b^{-1}, a, b, a^{-(k-1)}, b^{-1}, \\ &a^{k-3}, b, a^{-1}, b^{-1}, a^{-(k-3)}, b, a^{-m}, b^{-1}\big). \end{aligned} \tag{1}$$

Moreover, we can construct further hamiltonian cycles as follows. For $t \in \{1,2\}$, let $i = tp$. Then, with all indices taken modulo n,

$$D_t = \big(i-1,\ i,\ i',\ (i-1)',\ k+i,\ k+i-1,\ (k+i-1)',\ (k+i)',\ i-1\big) \tag{2}$$

is an 8-cycle in $GP(n,\ell)$. Its four rim edges lie in C_0, and its four spoke edges do not. Hence the (edge-wise) symmetric difference $C_t = C_0 \triangle D_t$ is also a hamiltonian cycle in $GP(n,\ell)$, and therefore also in $\mathrm{Cay}(H;\{a,b\})$.

Proof. Since $r \equiv 1 \pmod p$, we have $k \equiv -1 \pmod r$, and $k \equiv 1 \pmod p$. Hence $k^2 \equiv 1 \pmod n$. Also $\ell = n-k$, so $\ell \equiv -k \pmod n$ and $\ell^2 \equiv 1 \pmod n$. Since $p > 5$, we have $m = n-3k-1 = r(p-6)+2 > 0$.

We identify the spanning Petersen subgraph with $GP(n,\ell)$ as in Lemma 3.2. Under this identification, the word C_0 in (1) visits the outer vertices in the following order:

$$\begin{aligned} &0, -1, \ldots, 3k+1; \\ &2, 1; \\ &3k, 3k-1, \ldots, 2k+1; \\ &k+1, k+2; \\ &3, 4, \ldots, k; \\ &2k, 2k-1, \ldots, k+3. \end{aligned}$$

These are all residues modulo n, each appearing exactly once. Similarly, it visits the inner vertices in the following order:

$$\begin{aligned} &-(k+3)', -(k+4)', \ldots, -(2k)'; \\ &-k', -(k-1)', \ldots, -3'; \\ &-(k+2)', -(k+1)'; \\ &-(2k+1)', -(2k+2)', \ldots, -3k'; \\ &-1', -2'; \\ &-(3k+1)', -(3k+2)', \ldots, 0'. \end{aligned}$$

These are also all residues modulo n, each appearing exactly once. Thus C_0 is a hamiltonian cycle.

It remains to verify the local cycles D_t. Fix $t \in \{1, 2\}$, and put $i = tp$. Since

$$i\ell - i = i(\ell - 1) = tp \cdot r(p-2) \equiv 0 \pmod{n},$$

we have $i\ell \equiv i \pmod{n}$. Using $\ell \equiv -k \pmod{n}$ and $\ell^2 \equiv 1 \pmod{n}$, we obtain

$$(i-1)\ell \equiv i\ell - \ell \equiv i + k \pmod{n},$$

$$(k+i)\ell \equiv k\ell + i\ell \equiv -\ell^2 + i \equiv i - 1 \pmod{n},$$

and

$$(k+i-1)\ell \equiv (k+i)\ell - \ell \equiv i - 1 + k \equiv k + i - 1 \pmod{n}.$$

These congruences give the four spoke edges

$$i \sim i', \qquad i-1 \sim (k+i)', \qquad k+i \sim (i-1)', \qquad k+i-1 \sim (k+i-1)'.$$

The remaining four consecutive pairs in D_t are rim edges. Hence D_t is a closed walk in $GP(n, \ell)$. Since $r \equiv 1 \pmod{p}$ and r is prime, we have $r \geqslant 2p + 1$, so

$$0 < i - 1 < i < k + i - 1 < k + i < n.$$

Therefore, the four vertices of D_t are distinct, and likewise for the four primed vertices. It follows that D_t is an 8-cycle.

From the displayed order of C_0, the outer rim edges

$$(i-1, i) \qquad \text{and} \qquad (k+i, k+i-1)$$

belong to C_0. The inner rim edge $(i', (i-1)')$ belongs to the final inner segment of C_0. The other inner rim edge $((k+i-1)', (k+i)')$ also belongs to C_0: if $p \geqslant 11$, it lies in the final inner segment, while if $p = 7$, it lies in the segment

$$-(2k+1)', -(2k+2)', \ldots, -3k'.$$

Thus the four rim edges of D_t lie in C_0.

The spokes of C_0 have outer endpoints

$$0,\ 1,\ 2,\ 3,\ k,\ k+1,\ k+2,\ k+3,\ 2k,\ 2k+1,\ 3k,\ 3k+1.$$

The four spoke endpoints of D_t are

$$i-1,\ i,\ k+i-1,\ k+i.$$

None of these is in the preceding list, because

$$3 < i - 1 < i < k \qquad \text{and} \qquad k + 3 < k + i - 1 < k + i < 2k.$$

Hence $D_t \cap C_0$ consists exactly of the four rim edges of D_t.

Therefore $C_0 \triangle D_t$ is obtained from C_0 by deleting those four rim edges and inserting the four spoke edges of D_t. A direct trace from any one of the affected vertices shows that these four inserted spokes reconnect the four resulting paths into a single cycle through the same vertex set. Hence $C_t = C_0 \triangle D_t$ is again a hamiltonian cycle. $\square$

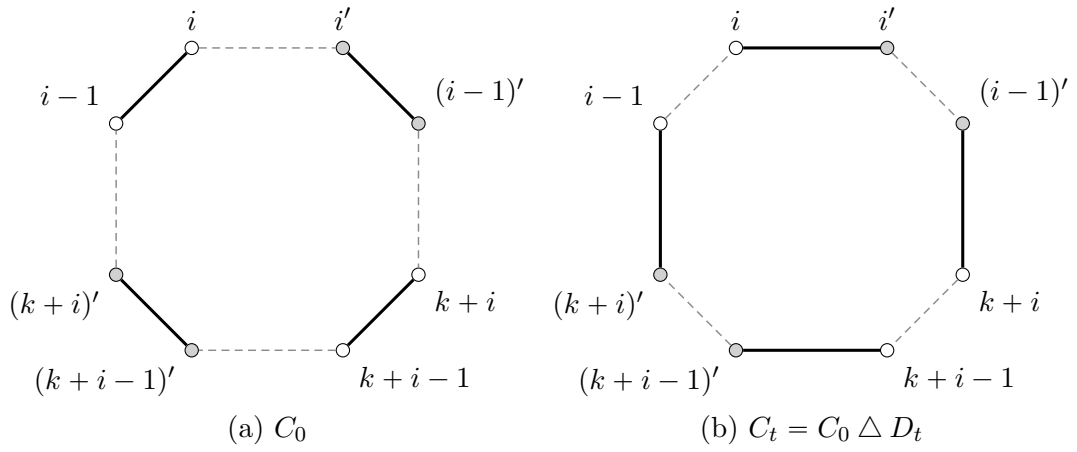

FIGURE 1. The local symmetric-difference switch in Proposition 3.4. Only the eight edges of D_t are shown. In C_0, the four rim edges of D_t are used and its four spokes are not; passing to $C_t = C_0 \triangle D_t$ reverses these choices.

4. Proof of the Main Result

In this section, we prove Theorem 1.4. The proof is a case-by-case analysis. Here are our main assumptions.

Assumption 4.1. We assume:

(1) $G' \cap Z(G) = \{e\}$, by Proposition 2.13(2).
(2) $G \cong \mathbb{Z}_n \ltimes G'$, by Proposition 2.13(3).
(3) By Proposition 2.6, we can assume $|G'| \in \{pq, pr, qr\}$. Without loss of generality we may assume $|G'| = pq$, so $G' = \mathbb{Z}_p \times \mathbb{Z}_q$ by Proposition 2.13(1).
(4) 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 Theorem 1.1(2) and Theorem 1.1(3). By Assumption 4.1(1), $\langle s \rangle \cap Z(G) = \{e\}$, therefore, Lemma 2.10(2) applies.

By Theorem 1.1(2), Theorem 1.1(3), and Theorem 1.2, it remains to treat the case where $|G| = 2pqr$ and $|S| \leqslant 2$. The following theorem settles exactly this remaining case.

Theorem 1.4. *Assume $G = \langle S \rangle$ is a finite group of order $2pqr$, such that $|S| = 2$, where p, q, and r are distinct primes, and $p, q, r \geqslant 5$. Then $\mathrm{Cay}(G; S)$ has a hamiltonian cycle.*

Proof. Let $G = \langle a, b \rangle$. If G is abelian, then the result follows from Lemma 2.1. So assume G is non-abelian. Moreover, assume the conditions in Assumption 4.1 are satisfied. Since $|\overline{G}| = 2r$, Proposition 2.13 implies that $\overline{G}$ is cyclic of order $2r$. Therefore $|\overline{a}|,\ |\overline{b}| \in \{2, r, 2r\}$.

The cases $|\overline{a}| = |\overline{b}| = 2$ and $|\overline{a}| = |\overline{b}| = r$ are impossible, because then $\langle \overline{a}, \overline{b} \rangle \neq \overline{G}$. So, after interchanging a and b if necessary, we are left with three cases:

(1) $|\overline{a}| = r$ and $|\overline{b}| \in \{2, 2r\}$,
(2) $|\overline{a}| = 2r$ and $|\overline{b}| = 2$,
(3) $|\overline{a}| = |\overline{b}| = 2r$.

Case 1. Assume $|\overline{a}| = r$ and $|\overline{b}| \in \{2, 2r\}$.

Then $|a| \in \{r, rp, rq, rpq\}$.

- If $|a| = r$, then $\gcd(|a|, r-1) = 1$, so Lemma 2.7 applies.
- If $|a| = rpq$, then $\mathbb{Z}_r$ centralizes $\mathbb{Z}_p \times \mathbb{Z}_q$. Since $G' \cap Z(G) = \{e\}$, the subgroup $\mathbb{Z}_2$ inverts $\mathbb{Z}_p \times \mathbb{Z}_q$. Hence
$$G \cong \mathbb{Z}_r \times (\mathbb{Z}_2 \ltimes \mathbb{Z}_{pq}) \cong \mathbb{Z}_r \times D_{2pq},$$
so Lemma 2.9 applies.
- Assume $|a| \in \{rp, rq\}$. Without loss of generality, let $|a| = rp$. Then $\mathbb{Z}_r$ centralizes $\mathbb{Z}_p$. Since $G' \cap Z(G) = \{e\}$, the subgroup $\mathbb{Z}_2$ acts non-trivially on $\mathbb{Z}_p$, and hence inverts $\mathbb{Z}_p$. Therefore $|b| \in \{2, 2q, 2r\}$. We note that $|b| = 2qr$ is already ruled out. If $|b| = 2q$, then Corollary 2.4 applies. So assume $|b| \in \{2, 2r\}$. If $\gcd(rp, r-1) = 1$, then Lemma 2.7 applies. Hence we may assume $\gcd(p, r-1) \neq 1$, so $r \equiv 1 \pmod{p}$.

  Consider
$$\breve{G} = G/\mathbb{Z}_q \cong \mathbb{Z}_r \times D_{2p} \cong (\mathbb{Z}_2 \times \mathbb{Z}_r) \ltimes \mathbb{Z}_p.$$
After conjugation, we may assume $\breve{a} = a_r\gamma_p\mathbb{Z}_q$, $\breve{b} = a_2a_r^j\mathbb{Z}_q$ for some j satisfying $0 \leqslant j \leqslant r-1$, where $\langle a_r\rangle = \mathbb{Z}_r$ and $\langle\gamma_p\rangle = \mathbb{Z}_p$. Since $\breve{b}$ centralizes $a_r\mathbb{Z}_q$ and inverts $\gamma_p\mathbb{Z}_q$, we have $\breve{b}^{-1}\breve{a}\breve{b} = \breve{a}^{k_0}$, whenever $k_0 \equiv 1 \pmod{r}$ and $k_0 \equiv -1 \pmod{p}$. Because $r \equiv 1 \pmod{p}$, we may choose $k_0 = r(p-2)+1$. Let $n = rp$ and $k = n - k_0$.

Subcase 1.1. Assume $p > 5$. We know $\breve{a} = a\mathbb{Z}_q$, and $\breve{b} = b\mathbb{Z}_q$. Since
$$|\breve{G}| = 2rp = 2n, \qquad |\breve{a}| = n, \qquad \breve{b} \notin \langle\breve{a}\rangle, \qquad \breve{b}^{-1}\breve{a}\breve{b} = \breve{a}^{k_0},$$
Proposition 3.4 applies. Hence $\mathrm{Cay}(\breve{G}; \breve{S})$ contains hamiltonian cycles
$$C_0, \qquad C_1 = C_0 \triangle D_1, \qquad C_2 = C_0 \triangle D_2,$$
where C_0 is the cycle in (1) and D_t is the 8-cycle in (2).

We now compute the voltage with respect to the normal subgroup $\mathbb{Z}_q$. For simplicity let $\gamma = \gamma_q$ and write $a_r\gamma a_r^{-1} = \gamma^\tau$. If $\tau = 1$, then $\mathbb{Z}_r$ centralizes both $\mathbb{Z}_p$ and $\mathbb{Z}_q$. Since $\mathbb{Z}_2$ inverts $\mathbb{Z}_p$ and $G' \cap Z(G) = \{e\}$, the subgroup $\mathbb{Z}_2$ must also act non-trivially on $\mathbb{Z}_q$, hence it inverts $\mathbb{Z}_q$. Therefore $G \cong D_{2pq} \times \mathbb{Z}_r$, so Lemma 2.9 applies. Hence we may assume $\tau \neq 1$. Since r is prime and $\tau^r = 1$ i.e. $\tau^r \equiv 1 \mod q$, the element τ has order r modulo q. We note that by repeatedly multiplying the identity $a_r\gamma a_r^{-1} = \gamma^\tau$ on the left by a_r and on the right by a_r^{-1}, we obtain $a_r^i\gamma a_r^{-i} = \gamma^{\tau^i}$ for every integer $i \geqslant 1$.

After conjugating by an element of $\mathbb{Z}_q$, we may assume, modulo $\mathbb{Z}_p$, that $a \equiv a_r$. After simultaneously conjugating a and b by an element of $\mathbb{Z}_q$, we may assume that $a\mathbb{Z}_p = a_r\mathbb{Z}_p$. Since $G/\mathbb{Z}_p \cong (\mathbb{Z}_2 \times \mathbb{Z}_r) \ltimes \mathbb{Z}_q$ and $b\mathbb{Z}_q = a_2a_r^j\mathbb{Z}_q$, there is some $u \in \mathbb{Z}/q\mathbb{Z}$ such that $b\mathbb{Z}_p = a_2a_r^j\gamma^u\mathbb{Z}_p$. We must have $u \not\equiv 0 \pmod{q}$, because otherwise the images of a and b would generate no element of the normal subgroup $\mathbb{Z}_q$ in $G/\mathbb{Z}_p$, contradicting $\langle a\mathbb{Z}_p, b\mathbb{Z}_p\rangle = G/\mathbb{Z}_p$. Since q is prime, γ^u is a generator of $\mathbb{Z}_q$. Replacing γ by γ^u, we may therefore write $b\mathbb{Z}_p = a_2a_r^j\gamma\mathbb{Z}_p$ and so $b \equiv a_2a_r^j\gamma \pmod{\mathbb{Z}_p}$. Also write
$$a_2\gamma a_2^{-1} = \gamma^\varepsilon, \qquad \varepsilon \in \{1, -1\}.$$
A direct multiplication, using
$$a_r^x\gamma a_r^{-x} = \gamma^{\tau^x},$$
gives
$$\mathrm{Volt}(C_0) \equiv \gamma^{\varepsilon\tau^j V_0} \pmod{\mathbb{Z}_p},$$

where

$$V_0 = -\tau^3 + 2\tau - 2 + 2\tau^{-1} - \tau^{-3}.$$

Equivalently, we obtain $V_0 = -\tau^{-3}(\tau-1)^2\big(\tau^4+2\tau^3+\tau^2+2\tau+1\big)$. If $V_0 \not\equiv 0 \pmod q$, then the voltage generates $\mathbb{Z}_q$, so the Factor Group Lemma 2.3 applies. Thus assume $V_0 \equiv 0 \pmod q$.

For $t = 1, 2$, we use the hamiltonian cycle $C_t = C_0 \triangle D_t$ given by Proposition 3.4. A direct voltage calculation gives

$$\mathrm{Volt}(C_t) \equiv \gamma^{\varepsilon\tau^j V_t} \pmod{\mathbb{Z}_p}.$$

If $p \geqslant 11$, then

$$V_t = V_0 + \tau^{tp-2}(1 + 2\tau - \tau^2) - 2\tau^2, \qquad t = 1, 2.$$

If $p = 7$, then

$$V_t = V_0 + 2\tau^3 - \tau^{7t-2}(1 + \tau^2), \qquad t = 1, 2.$$

We now show that at least one of V_0, V_1, V_2 is non-zero modulo q. Suppose, for a contradiction, that

$$V_0 \equiv V_1 \equiv V_2 \equiv 0 \pmod q.$$

First assume $p \geqslant 11$. From $V_1 \equiv V_0 \equiv 0 \pmod q$ and $V_2 \equiv V_0 \equiv 0 \pmod q$, we obtain

$$\tau^{p-2}(1 + 2\tau - \tau^2) \equiv 2\tau^2 \pmod q$$

and

$$\tau^{2p-2}(1 + 2\tau - \tau^2) \equiv 2\tau^2 \pmod q.$$

The factor $1 + 2\tau - \tau^2$ is non-zero, because $2\tau^2 \not\equiv 0 \pmod q$. Dividing the two displayed equations gives $\tau^p \equiv 1 \pmod q$. But τ has order r, and $r \equiv 1 \pmod p$, so $r > p$. This is impossible.

It remains to consider $p = 7$. Then $V_1 \equiv V_0 \equiv 0 \pmod q$ and $V_2 \equiv V_0 \equiv 0 \pmod q$ imply

$$\tau^5(1 + \tau^2) \equiv 2\tau^3 \pmod q$$

and

$$\tau^{12}(1 + \tau^2) \equiv 2\tau^3 \pmod q.$$

Again $1 + \tau^2 \neq 0$, so division gives $\tau^7 = 1$. But τ has order r, and $r \equiv 1 \pmod 7$, so $r > 7$. This is impossible.

Therefore at least one of C_0, C_1, C_2 has non-trivial voltage modulo $\mathbb{Z}_q$. Since $|\mathbb{Z}_q| = q$ is prime, this voltage generates $\mathbb{Z}_q$. Thus, Factor Group Lemma 2.3 gives a hamiltonian cycle in $\mathrm{Cay}(G; S)$.

Subcase 1.2. Assume $p = 5$. Note that $r \geqslant 5$. Then $\mathrm{Cay}(\breve{G}; \breve{S})$ has the following hamiltonian cycle (see Figure 2):

$$C = \big(\breve{a}^{r-5}, \breve{b}^{-1}, \breve{a}^{-(2r-4)}, \breve{b}, \breve{a}^{-1}, \breve{b}^{-1}, \breve{a}^{r+1}, \breve{b}, \breve{a}^{2r-3}, \breve{b}^{-1}, \breve{a}, \breve{b}, \breve{a}, \breve{b}^{-1},$$
$$\breve{a}^{-1}, \breve{b}, \breve{a}^{r}, \breve{b}^{-1}, \breve{a}^{r-1}, \breve{b}, \breve{a}^{r}, \breve{b}^{-1}, \breve{a}^{-(r-4)}, \breve{b}\big).$$

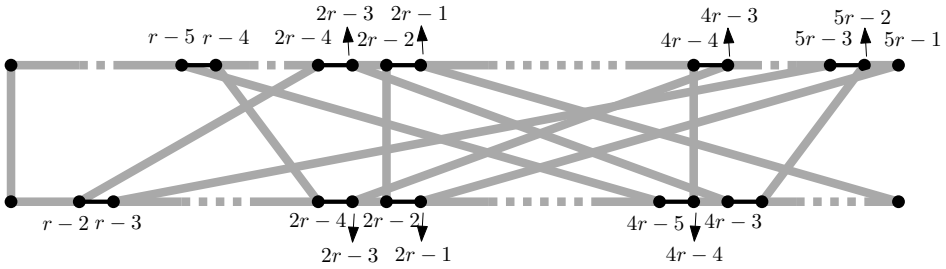

FIGURE 2. Hamiltonian cycle.

We compute the voltage with respect to the normal subgroup $\mathbb{Z}_q$. For simplicity let $\gamma = \gamma_q$, and write $a_r \gamma a_r^{-1} = \gamma^\tau$. If $\tau = 1$, then $\mathbb{Z}_r$ centralizes both $\mathbb{Z}_p$ and $\mathbb{Z}_q$. Since $\mathbb{Z}_2$ inverts $\mathbb{Z}_p$ and $G' \cap Z(G) = \{e\}$, the subgroup $\mathbb{Z}_2$ must act non-trivially on $\mathbb{Z}_q$, hence it inverts $\mathbb{Z}_q$. Therefore $G \cong D_{2pq} \times \mathbb{Z}_r$, so Lemma 2.9 applies. Hence we may assume $\tau \neq 1$. Since r is prime and $\tau^r = 1$, the element τ has order r modulo q.

After conjugating by an element of $\mathbb{Z}_q$, we may assume, modulo $\mathbb{Z}_p$, that $a \equiv a_r$. Since $\langle a, b \rangle = G$, the $\mathbb{Z}_q$-component of b is non-trivial. Replacing γ by a suitable generator of $\mathbb{Z}_q$, write

$$b \equiv a_2 a_r^j \gamma \pmod{\mathbb{Z}_p}.$$

Also write

$$a_2 \gamma a_2^{-1} = \gamma^\varepsilon, \qquad \varepsilon \in \{1, -1\}.$$

A direct multiplication in $G/\mathbb{Z}_p$, using

$$a_r^x \gamma a_r^{-x} = \gamma^{\tau^x},$$

gives

$$\mathrm{Volt}(C) \equiv \gamma^\ell \pmod{\mathbb{Z}_p},$$

where

$$\ell = -\tau^{-5} + 2\tau^{-1} - 2\tau^{-2} - \tau^{-4} + \tau^{-3} + 1.$$

If $\ell \not\equiv 0 \pmod{q}$, then the voltage generates $\mathbb{Z}_q$, so Factor Group Lemma 2.3 applies. Thus assume $\ell \equiv 0 \pmod{q}$. Multiplying by τ^5 gives

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

Since $\tau \neq 1$, we get

$$\tau^4 + 3\tau^3 + \tau^2 + 2\tau + 1 \equiv 0 \pmod{q}. \tag{3}$$

We can replace τ with τ^{-1} in Equation (3) by replacing $\{\breve{a}, \breve{b}\}$ with $\{\breve{a}^{-1}, \breve{b}^{-1}\}$. Hence, we have

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

Multiplying by τ^4, we have

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

By subtracting Equation (5) from Equation (3), we get $\tau(\tau^2 - 1) \equiv 0 \pmod{q}$, which is a contradiction.

Case 2. Assume $|\overline{a}| = 2r$ and $|\overline{b}| = 2$. Then $\overline{b} = \overline{a}^r$, so $b = a^r\gamma$ for some $\gamma \in G'$. Since

$$G = \langle a, b\rangle = \langle a, a^r\gamma\rangle = \langle a, \gamma\rangle,$$

the element γ must generate G'. By Proposition 2.13(4), we have $|a| = 2r$ and

$$a\gamma a^{-1} = \gamma^\tau, \qquad \tau^{2r} \equiv 1 \pmod{pq}, \qquad \gcd(\tau - 1, pq) = 1.$$

In particular, $\tau \not\equiv 1 \pmod{p}$ and $\tau \not\equiv 1 \pmod{q}$. We have

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

as a hamiltonian cycle in $\mathrm{Cay}(\overline{G}; \overline{S})$. Its voltage is

$$\begin{aligned}\mathrm{Volt}(C_1) &= a^{r-1}ba^{-(r-1)}b \\ &= a^{r-1}a^r\gamma a^{-(r-1)}a^r\gamma \\ &= a^{-1}\gamma a\gamma = \gamma^{\tau^{-1}+1}.\end{aligned}$$

We may assume $\gcd(\tau^{-1} + 1, pq) \neq 1$, for otherwise Factor Group Lemma 2.3 applies. Without loss of generality, let $\tau^{-1} \equiv -1 \pmod{q}$, so $\tau \equiv -1 \pmod{q}$. We may also assume $\tau \not\equiv -1 \pmod{p}$, for otherwise $G \cong D_{2pq} \times \mathbb{Z}_r$, so Lemma 2.9 applies. Next we consider $\widehat{G} = G/\mathbb{Z}_p = \mathbb{Z}_{2r} \ltimes \mathbb{Z}_q$.

Since $|a| = 2r$, we have $|\widehat{a}| = 2r$. The image of γ in $G/\mathbb{Z}_p$ is a generator of $\mathbb{Z}_q$, which we denote by γ_q. Hence we have $\widehat{b} = \widehat{a}^r\gamma_q$. Since $\tau \equiv -1 \pmod{q}$, the subgroup $\mathbb{Z}_r$ centralizes $\mathbb{Z}_q$, while $\mathbb{Z}_2$ inverts $\mathbb{Z}_q$. Therefore we obtain $\widehat{G} \cong D_{2q} \times \mathbb{Z}_r$.

Subcase 2.1. If $q > r$, then

$$C_2 = \left((\widehat{a}^{2r-1}, \widehat{b}, \widehat{a}^{-(2r-1)}, \widehat{b})^{(q-r)/2}, (\widehat{a}^{2r-1}, \widehat{b})^r\right)$$

is a hamiltonian cycle in $\mathrm{Cay}(\widehat{G}; \widehat{S})$. The picture in Figure 3 shows the hamiltonian cycle when $q = 7$ and $r = 3$.

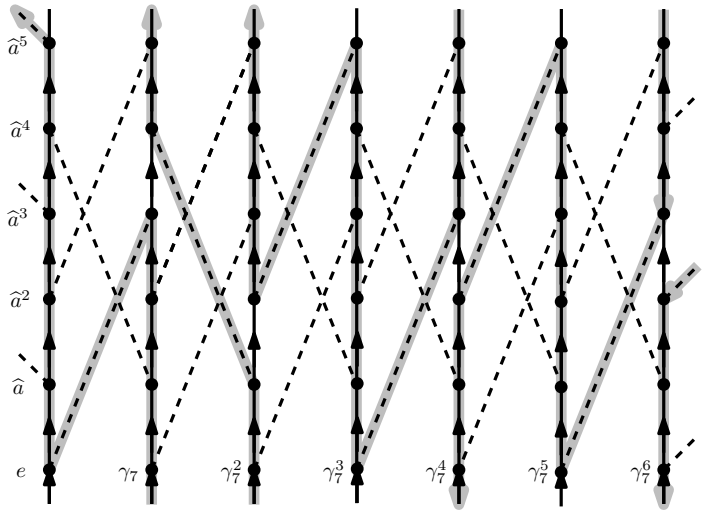

FIGURE 3. The union of the thick gray edges forms the hamiltonian cycle C_2 in $\mathrm{Cay}(\widehat{G}; \widehat{S})$.

If in C_2 we change one occurrence of $(\widehat{a}^{2r-1}, \widehat{b}, \widehat{a}^{-(2r-1)}, \widehat{b})$ to $(\widehat{a}^{-(2r-1)}, \widehat{b}, \widehat{a}^{2r-1}, \widehat{b})$, we obtain another hamiltonian cycle. Note that

$$a^{2r-1}ba^{-(2r-1)}b = a^{2r-1} \cdot a^r\gamma \cdot a^{-(2r-1)} \cdot a^r\gamma = a^{r-1}\gamma a^{-(r-1)}\gamma = \gamma^{\tau^{r-1}+1},$$

and

$$a^{-(2r-1)}ba^{2r-1}b = a^{-(2r-1)} \cdot a^r\gamma \cdot a^{2r-1} \cdot a^r\gamma = a^{-(r-1)}\gamma a^{r-1}\gamma = \gamma^{\tau^{-(r-1)}+1}.$$

We may assume $\tau^{r-1} + 1 \equiv \tau^{-(r-1)} + 1 \pmod p$, for otherwise the two hamiltonian cycles have different voltages, so one has non-trivial voltage and Factor Group Lemma 2.3 applies. Hence $\tau^{r-1} \equiv \tau^{-(r-1)} \pmod p$, so $\tau^{2r-2} \equiv 1 \pmod p$. Since $\tau^{2r} \equiv 1 \pmod p$, this implies $\tau^2 \equiv 1 \pmod p$, which is impossible because $\tau \not\equiv 1 \pmod p$ and $\tau \not\equiv -1 \pmod p$.

Subcase 2.2. If $r > q$, then

$$C_3 = \Big((\widehat{a}^r, \widehat{b}, \widehat{a}^{-r}, \widehat{b})^{(q-1)/2}, \widehat{a}^{-(r-1)}, \widehat{b}, (\widehat{a}^{r-2}, \widehat{b}, \widehat{a}^{-(r-2)}, \widehat{b})^{(q-1)/2}, \widehat{a}^{r-1}, \widehat{b}\Big)$$

is a hamiltonian cycle in $\mathrm{Cay}(\widehat{G}; \widehat{S})$. The picture in Figure 4 shows the hamiltonian cycle when $q = 3$ and $r = 7$.

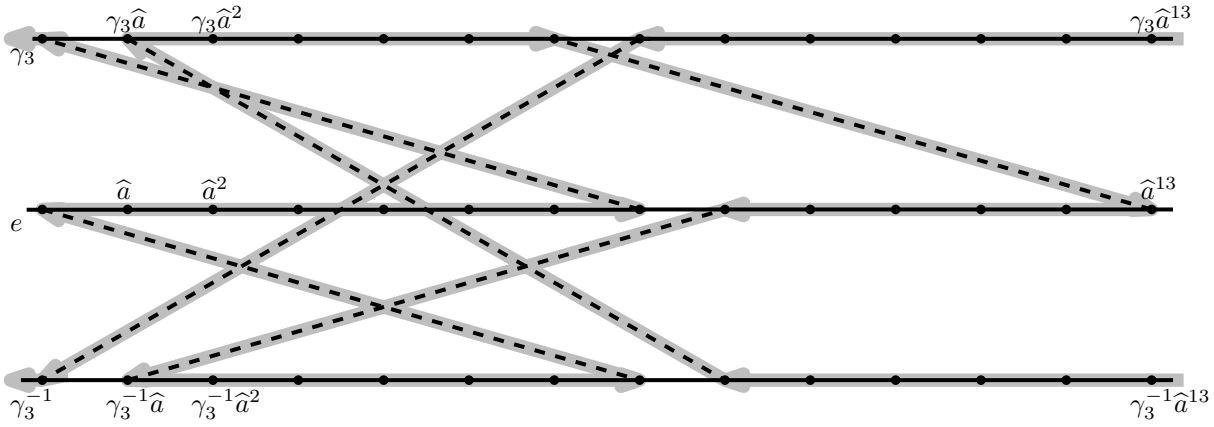

FIGURE 4. The union of the thick gray edges forms the hamiltonian cycle C_3 in $\mathrm{Cay}(\widehat{G}; \widehat{S})$.

Now we calculate its voltage:

$$\begin{aligned}
\mathrm{Volt}(C_3) &= (a^rba^{-r}b)^{(q-1)/2}a^{-(r-1)}b(a^{r-2}ba^{-(r-2)}b)^{(q-1)/2}a^{r-1}b \\
&= (a^r \cdot a^r\gamma \cdot a^{-r} \cdot a^r\gamma)^{(q-1)/2} \cdot a^{-(r-1)} \cdot a^r\gamma \\
&\qquad \cdot (a^{r-2} \cdot a^r\gamma \cdot a^{-(r-2)} \cdot a^r\gamma)^{(q-1)/2} \cdot a^{r-1} \cdot a^r\gamma \\
&= \gamma^{q-1}a\gamma(a^{-2}\gamma a^2\gamma)^{(q-1)/2}a^{-1}\gamma \\
&= \gamma^{q-1}a\gamma(\gamma^{\tau^{-2}+1})^{(q-1)/2}a^{-1}\gamma \\
&= \gamma^{(q-1)+\tau((\tau^{-2}+1)(q-1)/2+1)+1}.
\end{aligned}$$

We may assume this does not generate $\mathbb{Z}_p$, for otherwise Factor Group Lemma 2.3 applies. So

$$(q-1) + \tau((\tau^{-2}+1)(q-1)/2 + 1) + 1 \equiv 0 \pmod p,$$

which implies

$$\tau(q+1) + 2q + \tau^{-1}(q-1) \equiv 0 \pmod p. \tag{6}$$

Replacing a by a^{-1} in C_3 replaces τ by τ^{-1}, so we also have

$$\tau(q-1) + 2q + \tau^{-1}(q+1) \equiv 0 \pmod{p}. \tag{7}$$

Subtracting Equation (7) from Equation (6) gives $\tau^2 \equiv 1 \pmod{p}$, which is impossible.

Case 3. Assume $|\overline{a}| = |\overline{b}| = 2r$. Then $\overline{b} = \overline{a}^m$ for some integer m with $\gcd(m, 2r) = 1$. Replacing a by a^{-1}, if necessary, we may assume $1 \leqslant m \leqslant r-1$. In particular, m is odd. Since $\overline{b} = \overline{a}^m$, we can write $b = a^m\gamma$ with $\gamma \in G'$. The equality $G = \langle a, b\rangle = \langle a, \gamma\rangle$ forces γ to generate G'. By Proposition 2.13(4), we have

$$a\gamma a^{-1} = \gamma^{\tau}, \qquad \tau^{2r} \equiv 1 \pmod{pq}, \qquad \gcd(\tau - 1, pq) = 1.$$

Consider $\overline{G} = \mathcal{C}_{2r}$. We have $C_4 = (\overline{b}, \overline{a}^{-(m-1)}, \overline{b}, \overline{a}^{2r-m-1})$ as a hamiltonian cycle in $\mathrm{Cay}(\overline{G}; \overline{S})$. Its voltage is

$$\begin{aligned}\mathrm{Volt}(C_4) &= ba^{-(m-1)}ba^{2r-m-1}\\ &= a^m\gamma \cdot a^{-m+1} \cdot a^m\gamma \cdot a^{2r-m-1}\\ &= \gamma^{\tau^m+\tau^{m+1}} = \gamma^{\tau^m(1+\tau)}.\end{aligned}$$

We may assume this does not generate G', for otherwise Factor Group Lemma 2.3 applies. Thus $\gcd(1+\tau, pq) \neq 1$. Without loss of generality, assume $\tau \equiv -1 \pmod{q}$.

Subcase 3.1. Assume $m > 3$. Since m is odd and $m < r$, we have $m \leqslant r-2$. Then

$$C_5 = (\overline{b}^{-2}, \overline{a}^{-2}, \overline{b}, \overline{a}, \overline{b}, \overline{a}^{-(m-2)}, \overline{b}^{-1}, \overline{a}^{m-4}, \overline{b}^{-1}, \overline{a}^{-(2r-2m-3)})$$

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

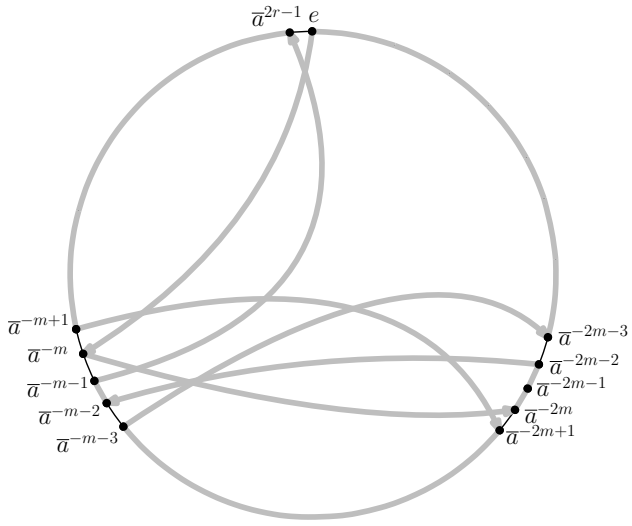

FIGURE 5. The union of the thick gray edges forms the hamiltonian cycle C_5 in $\mathrm{Cay}(\overline{G}; \overline{S})$.

Now we calculate its voltage:

$$\begin{aligned}\mathrm{Volt}(C_5) &= b^{-2}a^{-2}baba^{-(m-2)}b^{-1}a^{m-4}b^{-1}a^{-(2r-2m-3)}\\ &= \gamma^{-1}a^{-m}\gamma^{-1}a^{-m}a^{-2}a^m\gamma aa^m\gamma a^{-m+2}\gamma^{-1}a^{-m}a^{m-4}\gamma^{-1}a^{-m}a^{-2r+2m+3}\\ &= \gamma^{-1}a^{-m}\gamma^{-1}a^{-2}\gamma a^{m+1}\gamma a^{-m+2}\gamma^{-1}a^{-4}\gamma^{-1}a^{m+3}\end{aligned}$$

$$= \gamma^{-1-\tau^{-m}+\tau^{-m-2}+\tau^{-1}-\tau^{-m+1}-\tau^{-m-3}}$$
$$= \gamma^{-1+\tau^{-1}-\tau^{-m+1}-\tau^{-m}+\tau^{-m-2}-\tau^{-m-3}}.$$

We may assume $\mathrm{Volt}(C_5)$ does not generate $G' = \mathbb{Z}_p \times \mathbb{Z}_q$, for otherwise Factor Group Lemma 2.3 applies. Since $\tau \equiv -1 \pmod q$ and m is odd, the exponent of γ in $\mathrm{Volt}(C_5)$ is congruent to

$$-1-1-1+1-1-1 = -4 \pmod q.$$

Because $q \geqslant 5$, this is non-zero modulo q. Hence the voltage has non-trivial $\mathbb{Z}_q$-component, so the only remaining possibility is that its $\mathbb{Z}_p$-component is trivial. Thus

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

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

$$0 \equiv \tau^{m+3} - \tau^{m+2} + \tau^4 + \tau^3 - \tau + 1 \pmod p. \tag{9}$$

Replacing $\{\overline{a}, \overline{b}\}$ by $\{\overline{a}^{-1}, \overline{b}^{-1}\}$ replaces τ by τ^{-1}. Applying the same argument gives

$$0 \equiv -\tau^{m+3} + \tau^{m+2} - \tau^m - \tau^{m-1} + \tau - 1 \pmod p. \tag{10}$$

Adding Equation (9) and Equation (10) yields

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

If $\tau \equiv -1 \pmod p$, then, since also $\tau \equiv -1 \pmod q$, the quotient $\mathcal{C}_{2r}$ inverts $\mathbb{Z}_{pq}$. Hence $\mathbb{Z}_r$ centralizes G', so $G \cong D_{2pq} \times \mathbb{Z}_r$, and Lemma 2.9 applies. Therefore we may assume $\tau^{m-4} \equiv 1 \pmod p$. But $\tau^{2r} \equiv 1 \pmod p$, so the order of τ modulo p divides $\gcd(m-4, 2r)$. Since m is odd and $3 < m < r$, we have $\gcd(m-4, 2r) = 1$. This contradicts $\gcd(\tau - 1, pq) = 1$.

Subcase 3.2. Assume $m \leqslant 3$. Since m is odd, we have $m \in \{1, 3\}$.

First assume $m = 1$. Then $\overline{b} = \overline{a}$ and $b = a\gamma$. The quotient cycle $\overline{C}_6 = (\overline{a}^{2r-1}, \overline{b})$ is a hamiltonian cycle in $\mathrm{Cay}(\overline{G}; \overline{S})$. Indeed, it visits

$$e, \overline{a}, \overline{a}^2, \ldots, \overline{a}^{2r-1}, e.$$

Its lift is $C_6 = (a^{2r-1}, b)$, and its voltage is

$$\mathrm{Volt}(C_6) = a^{2r-1}b = a^{2r-1}a\gamma = \gamma.$$

Since γ generates G', Factor Group Lemma 2.3 applies.

Now assume $m = 3$. Thus $\overline{b} = \overline{a}^3$ and $b = a^3\gamma$. We claim that

$$\overline{C}_7 = (\overline{a}, \overline{b}^{-1}, \overline{a}, \overline{b}, \overline{a}^{2r-5}, \overline{b})$$

is a hamiltonian cycle in $\mathrm{Cay}(\overline{G}; \overline{S})$. Indeed, since $\overline{b} = \overline{a}^3$, the successive vertices of this walk are

$$e,\ \overline{a},\ \overline{a}^{-2},\ \overline{a}^{-1},\ \overline{a}^2,\ \overline{a}^3, \ldots, \overline{a}^{2r-3},\ e.$$

These are all $2r$ vertices of $\overline{G} = \langle \overline{a} \rangle$, before the final return to e. Therefore $\overline{C}_7$ is a hamiltonian cycle. Let

$$C_7 = (a, b^{-1}, a, b, a^{2r-5}, b)$$

be the corresponding lift to G. Since $b = a^3\gamma$, we have $b^{-1} = \gamma^{-1}a^{-3}$. Therefore

$$\begin{aligned}\mathrm{Volt}(C_7) &= ab^{-1}aba^{2r-5}b \\ &= a\gamma^{-1}a^{-3}a\, a^3\gamma a^{2r-5}a^3\gamma \\ &= a\gamma^{-1}a\gamma a^{2r-2}\gamma\end{aligned}$$

$$= \gamma^{-\tau+\tau^2+\tau^{2r}}$$
$$= \gamma^{\tau^2-\tau+1},$$

where the last equality uses $\tau^{2r} \equiv 1 \pmod{pq}$.

We show that $\tau^2 - \tau + 1$ is relatively prime to pq. Since $\tau \equiv -1 \pmod{q}$, we have

$$\tau^2 - \tau + 1 = (-1)^2 - (-1) + 1 = 3 \not\equiv 0 \pmod{q},$$

because $q \geqslant 5$. It remains to show that $\tau^2 - \tau + 1 \not\equiv 0 \pmod{p}$. Suppose, for a contradiction, that

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

Then

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

Also $\tau \not\equiv -1 \pmod{p}$, because substituting $\tau = -1$ into $\tau^2 - \tau + 1$ gives $3 \not\equiv 0 \pmod{p}$. Hence $\tau^3 \equiv -1 \pmod{p}$, so τ has order 6 modulo p. But $\tau^{2r} \equiv 1 \pmod{p}$, so the order of τ modulo p must divide $2r$. This is impossible, because $r \geqslant 5$ is an odd prime, so $6 \nmid 2r$.

Therefore $\tau^2 - \tau + 1 \not\equiv 0 \pmod{p}$ and $\tau^2 - \tau + 1 \not\equiv 0 \pmod{q}$. Since $G' = \langle\gamma\rangle$ has order pq, it follows that $\gamma^{\tau^2-\tau+1}$ generates G'. Hence $\mathrm{Volt}(C_7)$ generates G', and Factor Group Lemma 2.3 applies. □

Proof of Theorem 1.3. Let $S_0 \subseteq S$ be a minimal generating subset of G. If $|S_0| \geqslant 3$, then Theorem 1.2 gives a hamiltonian cycle in $\mathrm{Cay}(G; S_0)$. Since $\mathrm{Cay}(G; S_0)$ is a spanning subgraph of $\mathrm{Cay}(G; S)$, this is also a hamiltonian cycle in $\mathrm{Cay}(G; S)$.

Thus we may assume $|S_0| \leqslant 2$. If all four prime divisors of $|G|$ are odd, then Theorem 1.1(4) applies. Hence we may assume that one of the prime divisors is 2, so $|G| = 2pqr$. If one of p, q, r is 3, then $|G| = 6uv$ for two distinct primes u, v, and Theorem 1.1(2) applies. Therefore the only remaining case is $|G| = 2pqr$ with $p, q, r \geqslant 5$. Applying Theorem 1.4 to the generating set S_0, we obtain a hamiltonian cycle in $\mathrm{Cay}(G; S_0)$. Since $\mathrm{Cay}(G; S_0)$ is a spanning subgraph of $\mathrm{Cay}(G; S)$, this is also a hamiltonian cycle in $\mathrm{Cay}(G; S)$. This completes the proof. □

Acknowledgments

We thank Dave Witte Morris for a discussion during the preparation of this paper.

References

[1] Fateme Abedi, Dave Witte Morris, Javanshir Rezaee, and Mohammad Reza Salarian. Cayley graphs of order $8pq$ are Hamiltonian. *Contributions to Discrete Mathematics*, 20(2):311–336, 2025. arXiv: 2304.03348, doi:10.55016/ojs/cdm.v20i2.77376.

[2] László Babai. Problem 17, unsolved problems. Summer Research Workshop in Algebraic Combinatorics, Simon Fraser University, 1979.

[3] László Babai. Automorphism groups, isomorphism, reconstruction. In Ronald L. Graham, Martin Grötschel, and László Lovász, editors, *Handbook of Combinatorics*, volume 2, chapter 27, pages 1447–1540. North-Holland, Amsterdam, 1995.

[4] Jean-Claude Bermond. Hamiltonian graphs. In Lowell W. Beineke and Robin J. Wilson, editors, *Selected Topics in Graph Theory*, pages 127–167. Academic Press, London, 1978.

[5] Darryn Bryant, Sarada Herke, Barbara Maenhaut, and Bridget S. Webb. On Hamilton decompositions of infinite circulant graphs. *Journal of Graph Theory*, 88(3):434–448, 2018. doi:10.1002/jgt.22223.

[6] Chuan Chong Chen and Norman F. Quimpo. On some classes of Hamiltonian graphs. *Southeast Asian Bulletin of Mathematics*, (Special Issue):252–258, 1979.

[7] Stephen J. Curran, Dave Witte Morris, and Joy Morris. Cayley graphs of order $16p$ are Hamiltonian. *Ars Mathematica Contemporanea*, 5(2):185–211, 2012. doi:10.26493/1855-3974.207.8e0.

[8] Iren Darijani, Babak Miraftab, and Dave Witte Morris. Arc-disjoint Hamiltonian paths in cartesian products of directed cycles. *Ars Mathematica Contemporanea*, 25(2):Article P2.10, 2025. doi:10.26493/1855-3974.3047.c2d.

[9] Joshua Erde and Florian Lehner. Hamiltonian decompositions of 4-regular Cayley graphs of infinite abelian groups. *Journal of Graph Theory*, 101(3):559–571, 2022. doi:10.1002/jgt.22840.

[10] Joshua Erde, Florian Lehner, and Max Pitz. Hamilton decompositions of one-ended Cayley graphs. *Journal of Combinatorial Theory, Series B*, 140:171–191, 2020. doi:10.1016/j.jctb.2019.05.005.

[11] Ebrahim Ghaderpour and Dave Witte Morris. Cayley graphs of order $30p$ are Hamiltonian. *Discrete Mathematics*, 312(24):3614–3625, 2012. doi:10.1016/j.disc.2012.08.017.

[12] Chris Godsil and Gordon Royle. *Algebraic Graph Theory*, volume 207 of *Graduate Texts in Mathematics*. Springer, New York, 2001. doi:10.1007/978-1-4613-0163-9.

[13] Marshall Hall, Jr. *The Theory of Groups*. Macmillan, New York, 1959.

[14] Klavdija Kutnar and Dragan Marušič. Hamilton cycles and paths in vertex-transitive graphs—current directions. *Discrete Mathematics*, 309(17):5491–5500, 2009. doi:10.1016/j.disc.2009.02.017.

[15] Klavdija Kutnar, Dragan Marušič, Dave Witte Morris, Joy Morris, and Primož Šparl. Hamiltonian cycles in Cayley graphs whose order has few prime factors. *Ars Mathematica Contemporanea*, 5(1):27–71, 2012. doi:10.26493/1855-3974.177.341.

[16] Florian Lehner, Farzad Maghsoudi, and Babak Miraftab. Hamiltonicity of transitive graphs whose automorphism group has $\mathbb{Z}_p$ as commutator subgroups. *Discrete Mathematics*, 349(3):114798, 2026. doi:10.1016/j.disc.2025.114798.

[17] Farzad Maghsoudi. Cayley graphs of order $6pq$ and $7pq$ are Hamiltonian. *The Art of Discrete and Applied Mathematics*, 5(1):Paper No. P1.10, 2022. 55 pages. doi:10.26493/2590-9770.1389.fa2.

[18] Farzad Maghsoudi. On Hamiltonicity of Cayley graphs of order $pqrs$. *Australasian Journal of Combinatorics*, 84:124–166, 2022. URL: https://ajc.maths.uq.edu.au/pdf/84/ajc_v84_p124.pdf.

[19] Babak Miraftab and Dave Witte Morris. On vertex-transitive graphs with a unique Hamiltonian cycle. *Journal of Graph Theory*, 108(1):65–99, 2025. doi:10.1002/jgt.23166.

[20] Dave Witte Morris. On Hamiltonian cycles in Cayley graphs of order $pqrs$. *The Art of Discrete and Applied Mathematics*, 5(3):Paper No. 3.12, 2022. 10 pages. doi:10.26493/2590-9770.1442.cb1.

[21] Dave Witte Morris and Kirsten Wilk. Cayley graphs of order kp are Hamiltonian for $k < 48$. *The Art of Discrete and Applied Mathematics*, 3(2):Paper No. P2.02, 2020. 17 pages. doi:10.26493/2590-9770.1250.763.

[22] David Witte. Cayley digraphs of prime-power order are Hamiltonian. *Journal of Combinatorial Theory, Series B*, 40(1):107–112, 1986. doi:10.1016/0095-8956(86)90068-7.

[23] David Witte and Joseph A. Gallian. A survey: Hamiltonian cycles in Cayley graphs. *Discrete Mathematics*, 51(3):293–304, 1984. doi:10.1016/0012-365X(84)90010-4.

Department of Mathematics, University of Auckland, 38 Princes Street, Auckland 1010, New Zealand

Email address: florian.lehner@auckland.ac.nz

Email address: farzad.maghsoudi93@gmail.com

School of Computer Science, Carleton University, Ottawa, ON, Canada

Email address: bobby.miraftab@gmail.com