Also available at http://amc-journal.eu
ISSN 1855-3966 (printed edn.), ISSN 1855-3974 (electronic edn.)
ARS MATHEMATICA CONTEMPORANEA 8 (2015) 1–28

Odd-order Cayley graphs with commutator subgroup of order pq are hamiltonian*

Dave Witte Morris

Department of Mathematics and Computer Science, University of Lethbridge, Lethbridge, Alberta, T1K 3M4, Canada

Received 1 May 2012, accepted 8 August 2013, published online 11 April 2014

Abstract

We show that if G is a nontrivial, finite group of odd order, whose commutator subgroup $[G, G]$ is cyclic of order $p^\mu q^\nu$, where p and q are prime, then every connected Cayley graph on G has a hamiltonian cycle.

Keywords: Cayley graph, hamiltonian cycle, commutator subgroup.

Math. Subj. Class.: 05C25, 05C45

1 Introduction

It has been conjectured that there is a hamiltonian cycle in every connected Cayley graph on any finite group, but all known results on this problem have very restrictive hypotheses (see [2, 13, 15] for surveys). One approach is to assume that the group is close to being abelian, in the sense that its commutator subgroup is small. This is illustrated by the following theorem that was proved in a series of papers by Marušič [12], Durnberger [3, 4], and Keating-Witte [10]:

Theorem 1.1 (D. Marušič, E. Durnberger, K. Keating, and D. Witte, 1985)**.** If G is a nontrivial, finite group, whose commutator subgroup $[G, G]$ is cyclic of order p^μ, where p prime and $\mu \in \mathbb{N}$, then every connected Cayley graph on G has a hamiltonian cycle.

Under the additional assumption that G has odd order, we extend this theorem, by allowing the order of $[G, G]$ to be the product of two prime-powers:

Theorem 1.2. If G is a nontrivial, finite group of odd order, whose commutator subgroup $[G, G]$ is cyclic of order $p^\mu q^\nu$, where p and q are prime, and $\mu, \nu \in \mathbb{N}$, then every connected Cayley graph on G has a hamiltonian cycle.

*To Dragan Marušič on his 60th birthday.

E-mail address: Dave.Morris@uleth.ca, http://people.uleth.ca/∼dave.morris/ (Dave Witte Morris)

This work is licensed under http://creativecommons.org/licenses/by/3.0/

Remark 1.3. Of course, we would like to prove the conclusion of Theorem 1.2 without the assumption that $|G|$ is odd, or with a weaker assumption on the order of $[G, G]$.

If $\mu, \nu \leq 1$, then there is no need to assume that $[G, G]$ is cyclic:

Corollary 1.4. If G is a nontrivial, finite group of odd order, whose commutator subgroup $[G, G]$ has order pq, where p and q are distinct primes, then every connected Cayley graph on G has a hamiltonian cycle.

This yields the following contribution to the ongoing search [11] for hamiltonian cycles in Cayley graphs on groups whose order has few prime factors:

Corollary 1.5. If p and q are distinct primes, then every connected Cayley graph of order $9pq$ has a hamiltonian cycle.

Here is an outline of the paper. Miscellaneous definitions and preliminary results are collected in Section 2. (Also, Corollaries 1.4 and 1.5 are derived from Theorem 1.2 in §2E.) The paper's main tool is a technique known as "Marušič's Method." A straightforward application of this method is given in Section 3, and some other consequences are in Section 4. The proof of Theorem 1.2 is in Section 5, except that one troublesome case is postponed to Section 6.

Acknowledgments. I thank D. Marušič for suggesting this research problem. I also thank him, K. Kutnar, and other members of the Faculty of Mathematics, Natural Sciences, and Information Technologies of the University of Primorska (Koper, Slovenia), for their excellent hospitality that supported the early stages of this work. Furthermore, I am grateful to an anonymous referee for helpful comments on an earlier version of this manuscript.

2 Preliminaries

2A Assumptions, definitions, and notation

Assumption 2.1.

(1) G is always a finite group.

(2) S is a generating set for G.

Definition 2.2. The *Cayley graph* $\mathrm{Cay}(G; S)$ is the graph whose vertex set is G, with an edge from g to gs and an edge from g to gs^{-1}, for every $g \in G$ and $s \in S$.

Notation 2.3.

- We let $G' = [G, G]$ and $\overline{G} = G/G'$. Also, for $g \in G$, we let $\overline{g} = gG'$ be the image of g in $\overline{G}$.
- For $g, h \in G$, we let $g^h = h^{-1}gh$ and $[g, h] = g^{-1}h^{-1}gh$.
- If H is an abelian subgroup of G and $k \in \mathbb{Z}$, we let

$$H^k = \{\, h^k \mid h \in H \,\}.$$

This is a subgroup of H (because H is abelian).

Notation 2.4. For $g \in G$ and $s_1, \ldots, s_n \in S \cup S^{-1}$, we use $[g](s_1, \ldots, s_n)$ to denote the walk in $\mathrm{Cay}(G; S)$ that visits (in order), the vertices

$$g,\ gs_1,\ gs_1s_2,\ gs_1s_2s_3,\ \ldots,\ gs_1s_2\cdots s_n.$$

We often write $(s_1, \ldots, s_n)$ for $[e](s_1, \ldots, s_n)$.

Definition 2.5. Suppose

- N is a normal subgroup of G, and
- $C = (s_i)_{i=1}^n$ is a hamiltonian cycle in $\mathrm{Cay}(G/N; S)$.

The *voltage* of C is $\prod_{i=1}^n s_i$. This is an element of N, and it may be denoted ΠC.

Remark 2.6. If $C = [g](s_1, \ldots, s_n)$, and N is abelian, then $\prod_{i=1}^n s_i = (\Pi C)^g$.

Proof. There is some ℓ with $(s_1s_2\cdots s_\ell)g \in N$. Then

$$C = (s_{\ell+1}, s_{\ell+2}, \ldots, s_n, s_1, s_2, \ldots, s_\ell),$$

so

$$\begin{aligned}(\Pi C)^g &= g^{-1}(s_{\ell+1}s_{\ell+2}\cdots s_n\, s_1s_2\cdots s_\ell)g \\ &= \big[(s_1s_2\cdots s_\ell)g\big]^{-1}\,(s_1s_2\cdots s_\ell)(s_{\ell+1}s_{\ell+2}\cdots s_n)\,\big[(s_1s_2\cdots s_\ell)g\big] \\ &= (s_1s_2\cdots s_n)^{(s_1s_2\cdots s_\ell)g} \\ &= s_1s_2\cdots s_n.\end{aligned}$$

□

2B Factor Group Lemma and Marušič's Method

Lemma 2.7 ("Factor Group Lemma" [15, §2.2])**.** Suppose

- N is a cyclic, normal subgroup of G,
- $(s_i)_{i=1}^m$ is a hamiltonian cycle in $\mathrm{Cay}(G/N; S)$, and
- the product $s_1s_2\cdots s_m$ generates N.

Then $(s_1, s_2, \ldots, s_m)^{|N|}$ is a hamiltonian cycle in $\mathrm{Cay}(G; S)$.

The following simple observation allows us to assume $|N|$ is square-free whenever we apply the Factor Group Lemma (2.7).

Lemma 2.8 ([10, Lem. 3.2])**.** Suppose

- N is a cyclic, normal subgroup of G,
- $\underline{N} = N/\Phi$ is the maximal quotient of N that has square-free order,
- $\underline{G} = G/\Phi$,
- $(s_1, s_2, \ldots, s_m)$ is a hamiltonian cycle in $\mathrm{Cay}(\underline{G}/\underline{N}; S)$, and
- the product $\underline{s_1}\,\underline{s_2}\cdots\underline{s_m}$ generates $\underline{N}$.

Then $s_1s_2\cdots s_m$ generates N, so $(s_1, s_2, \ldots, s_m)^{|N|}$ is a hamiltonian cycle in $\mathrm{Cay}(G; S)$.

Remark 2.9 (cf. [7, Thm. 5.1.1])**.** When applying Lemma 2.8, it is sometimes helpful to know that if

- N, $\underline{N} = N/\Phi$, and $\underline{G} = G/\Phi$ are as in Lemma 2.8, and
- S is a minimal generating set of G.

Then $\underline{S}$ is a minimal generating set of $\underline{G}$.

Lemma 2.10 ("Marušič's Method" [12], cf. [10, Lem. 3.1])**.** Suppose

- $S_0 \subseteq S$,
- $\langle S_0 \rangle$ contains G',
- there are hamiltonian cycles $C_1, \ldots, C_r$ in $\mathrm{Cay}(\langle S_0 \rangle / G'; S_0)$ that all have an oriented edge in common, and

$*$ for every $\gamma \in G'$, there is some i, such that $\langle \gamma \cdot \Pi C_i \rangle = G'$.

Then there is a hamiltonian cycle in $\mathrm{Cay}(G/G'; S)$ whose voltage generates G'. Hence, the Factor Group Lemma (2.7) provides a hamiltonian cycle in $\mathrm{Cay}(G; S)$.

Corollary 2.11. Assume $G' = \mathbb{Z}_p \times \mathbb{Z}_q$, where p and q are distinct primes. Then, in the situation of Marušič's Method (2.10), the final condition $(*)$ can be replaced with either of the following:

(1) $r = 3$, and $\langle (\Pi C_i)^{-1}(\Pi C_j) \rangle = G'$ whenever $1 \le i < j \le 3$.

(2) $r = 4$, and

- $\langle (\Pi C_1)^{-1}(\Pi C_2) \rangle$ contains $\mathbb{Z}_p$, and
- $\langle (\Pi C_1)^{-1}(\Pi C_3) \rangle = \langle (\Pi C_2)^{-1}(\Pi C_4) \rangle = \mathbb{Z}_q$.

Proof. Let $\gamma \in G'$.

(1) Consider the three elements $\gamma \cdot \Pi C_1$, $\gamma \cdot \Pi C_2$, and $\gamma \cdot \Pi C_3$ of $\mathbb{Z}_p \times \mathbb{Z}_q$. By assumption, no two have the same projection to $\mathbb{Z}_p$, so only one of them can have trivial projection. Similarly for the projection to $\mathbb{Z}_q$. Therefore, there is some i, such that $\gamma \cdot \Pi C_i$ projects nontrivially to both $\mathbb{Z}_p$ and $\mathbb{Z}_q$. Therefore $\langle \gamma \cdot \Pi C_i \rangle = G'$.

(2) There is some $i \in \{1, 2\}$, such that $\gamma \cdot \Pi C_i$ projects nontrivially to $\mathbb{Z}_p$. We may assume the projection of $\gamma \cdot \Pi C_i$ to $\mathbb{Z}_q$ is trivial (otherwise, we have $\langle \gamma \cdot \Pi C_i \rangle = G'$, as desired). Then $\gamma \cdot \Pi C_{i+2}$ has the same (nontrivial) projection to $\mathbb{Z}_p$, but has a different (hence, nontrivial) projection to $\mathbb{Z}_q$. So $\langle \gamma \cdot \Pi C_{i+2} \rangle = G'$. □

2C Some known results

We recall a few results that provide hamiltonian cycles in $\mathrm{Cay}(G; S)$ under certain assumptions.

Theorem 2.12 (Witte [14])**.** If $|G| = p^\mu$, where p is prime and $\mu > 0$, then every connected Cayley digraph on G has a directed hamiltonian cycle.

Theorem 2.13 (Ghaderpour-Morris [6])**.** If G is a nontrivial, nilpotent, finite group, and the commutator subgroup of G is cyclic, then every connected Cayley graph on G has a hamiltonian cycle.

Theorem 2.14 (Ghaderpour-Morris [5])**.** If $|G| = 27p$, where p is prime, then every connected Cayley graph on G has a hamiltonian cycle.

The proof of the preceding theorem has the following consequence.

Corollary 2.15. If G is a finite group, such that $|G/G'| = 9$ and G' is cyclic of order $p^\mu \cdot 3^\nu$, where $p \geq 5$ is prime, then every connected Cayley graph on G has a hamiltonian cycle.

Proof. Let $\underline{G} = G/(G')^{3p}$. Then $|\underline{G}| = 27p$ and $|\underline{G}'| = 3p$, so the proof of [5, Props. 3.4 and 3.6] provides a hamiltonian cycle in $\mathrm{Cay}\big(\underline{G}/\underline{G}'; \underline{S}\big)$ whose voltage generates $\underline{G}'$. Then Lemma 2.8 provides a hamiltonian cycle in $\mathrm{Cay}(G; S)$. □

Theorem 2.16 (Alspach [1, Thm. 3.7])**.** Suppose

- $s \in S$,
- $\langle s \rangle \triangleleft G$,
- $|G/\langle s \rangle|$ is odd, and
- there is a hamiltonian cycle in $\mathrm{Cay}\big(G/\langle s \rangle; S\big)$.

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

This has the following immediate consequence, since every subgroup of a cyclic, normal subgroup is normal:

Corollary 2.17. Suppose

- G' is cyclic,
- $s \in S \cap G'$,
- $|G/\langle s \rangle|$ is odd, and
- there is a hamiltonian cycle in $\mathrm{Cay}(G/\langle s \rangle; S)$.

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

2D Group theoretic preliminaries

We recall a few elementary facts about finite groups.

Lemma 2.18 ([6, Lem. 3.4])**.** Suppose

- $\langle a, b \rangle = G$,
- G' is cyclic of square-free order, and
- $G' \subseteq Z(G)$.

Then $|[a, b]|$ is a divisor of both $\langle \overline{a} \rangle$ and $|\overline{G}/\langle \overline{a} \rangle|$.

Lemma 2.19 ([6, Lem. 3.5])**.** If $G = \langle a, b \rangle$, and G' is cyclic, then $G' = \langle [a, b] \rangle$.

Corollary 2.20. Suppose

- $\langle a, G' \rangle = G$, and
- G' is cyclic of square-free order.

Then a does not centralize any nontrivial subgroup of G'.

Proof. Let γ be a generator of the cyclic group G', and let $\underline{G} = G/\langle [a,\gamma]\rangle$, so $\underline{a}$ centralizes $\underline{\gamma}$. Then $\underline{G}' = \langle\underline{\gamma}\rangle \subseteq Z(\underline{G})$, so Lemma 2.18 tells us that $|\underline{G}'| = |[\underline{a},\underline{\gamma}]|$ is a divisor of $|\overline{G}/\langle\overline{a}\rangle| = 1$. This means $\underline{G}$ is abelian, so $\langle [a,\gamma]\rangle = G' = \langle\gamma\rangle$. This implies that a does not centralize any nontrivial power of γ. In other words, a does not centralize any nontrivial subgroup of G'. □

Lemma 2.21. Suppose

- $G' = \mathbb{Z}_{3^\mu}$ is cyclic of order 3^μ, for some $\mu \in \mathbb{N}$, and
- $G/(G')^3$ is a nonabelian group of order 27.

Then

(1) $\mu = 1$ (so $|G| = 27$),

(2) $(ab)^3 = a^3b^3$ for all $a, b \in G$, and

(3) the elements of order 3 (together with e) form a subgroup of G.

Proof. Note that $|G| = 3^{\mu+2}$, so G is a 3-group. Since G' is cyclic (and 3 is odd), it is not difficult to show

$$(ab)^3 \in a^3b^3(G')^3, \text{ for all } a, b \in G. \tag{2.21A}$$

(This is a special case of [9, Satz III.10.2(c), p. 322].)

(1) Since $G/G' \cong \mathbb{Z}_3 \times \mathbb{Z}_3$, there is a 2-element generating set $\{a, b\}$ of G. (In fact, every minimal generating set has exactly two elements [9, 3.15, p. 273].) Since $a^3, b^3 \in G'$, we see from (2.21A) that we may assume $b^3 \in (G')^3$ (by replacing b with ba or ba^{-1}, if necessary). Furthermore, by modding out $(G')^9$, there is no harm in assuming $\mu \leq 2$, so $(G')^3 \subseteq Z(G)$. Therefore $[a, b^3] = e$, so [9, Satz 10.6(b), p. 326] tells us that $[a, b]^3 = e$. Since $\langle [a, b]\rangle = G'$ (see Lemma 2.19), this implies $\mu = 1$.

(2) Since $\mu = 1$, we have $(G')^3 = \{e\}$, so this is immediate from (2.21A).

(3) This is immediate from (2). (Also, it is a special case of [9, Satz III.10.6(a), p. 326].) □

2E Proofs of Corollaries 1.4 and 1.5

Proof of Corollary 1.4. Assume, without loss of generality, that $p < q$. Then Sylow's Theorem implies that G' has a unique Sylow q-subgroup Q, so $Q \lhd G$. Therefore G acts on Q by conjugation. Since $Q \cong \mathbb{Z}_q$, we know that the automorphism group of Q is abelian (more precisely, it is cyclic of order $q - 1$), so this implies that G' centralizes Q. So $Q \subseteq Z(G')$. Since G'/Q is cyclic (indeed, it is of prime order, namely, p), this implies that G' is abelian. Since $p \neq q$, we know that every abelian group of order pq is cyclic, so we conclude that G' is cyclic. Therefore Theorem 1.2 applies. □

Proof of Corollary 1.5. Assume $|G| = 9pq$. We may assume p and q are odd, for otherwise $|G|$ is of the form $18p$, so [11, Prop. 9.1] applies. Therefore $|G|$ is odd, so it suffices to show $|G'|$ is a divisor of pq, for then Corollary 1.4 (or Theorem 1.1) applies.

Note that we may assume $3 \notin \{p, q\}$, for otherwise $|G|$ is of the form $27p$, so Theorem 2.14 applies. Therefore, neither $|\mathrm{Aut}(\mathbb{Z}_9)| = 6$ nor $|\mathrm{Aut}(\mathbb{Z}_3 \times \mathbb{Z}_3)| = 48$ is divisible

by either p or q, so Burnside's Transfer Theorem [7, Thm. 7.4.3, p. 252] implies that G has a normal subgroup N of order pq. Since $|G/N| = 9$, and every group of order 9 is abelian, we know that $G' \subseteq N$, so $|G'|$ is a divisor of $|N| = pq$, as desired. □

Let us also record the fact that almost all cases of Theorem 1.2 will be proved by using Marušič's Method (2.10):

Theorem 2.22. Assume

- S is a minimal generating set for a nontrivial, finite group G of odd order,
- G' is cyclic of order $p^\mu q^\nu$, where p and q are prime, and $\mu, \nu \in \mathbb{N}$,
- for all $s \in S$, we have $s \notin G'$ and $G' \not\subseteq \langle s \rangle$,
- $G/(G')^3$ is **not** the nonabelian group of order 27 and exponent 3, and
- either $G/G' \ncong \mathbb{Z}_3 \times \mathbb{Z}_3$, or $\#S \neq 2$.

Then, for every $\gamma \in G'$, there exists a hamiltonian cycle C in $\mathrm{Cay}\big(G/G'; S\big)$, such that $\gamma \Pi C$ generates G'.

3 The usual application of Marušič's Method

Applying Marušič's Method (2.10) requires the existence of more than one hamiltonian cycle in a quotient of $\mathrm{Cay}(G; S)$. In practice, one usually starts with a single hamiltonian cycle and modifies it in various ways to obtain the others that are needed. The following result describes a modification that will be used repeatedly in the proof of Theorem 1.2.

Lemma 3.1 (cf. Durnberger [3] and Marušič [12])**.** Assume:

- C_0 is an oriented hamiltonian cycle in $\mathrm{Cay}(\overline{G}; S)$,
- $a, b \in S^{\pm 1}$, $g \in G$, and $m \in \mathbb{Z}^+$,
- C_0 contains:
  - the oriented path $[ga^{-(m+1)}](a^m, b, a^{-m})$, and
  - either the oriented edge $[g](b)$ or the oriented edge $[gb](b^{-1})$.

Then there are hamiltonian cycles $C_0, C_1, \ldots, C_m$ in $\mathrm{Cay}(\overline{G}; S)$, such that

$$\Big(\big(\Pi C_0\big)^{-1}\big(\Pi C_k\big)\Big)^g = \begin{cases} [a^k, b^{-1}]\,[a^k, b^{-1}]^a & \text{if } C_0 \text{ contains } [g](b), \\ [b^{-1}, a^k]\,[a^k, b^{-1}]^a & \text{if } C_0 \text{ contains } [gb](b^{-1}). \end{cases}$$

Proof. Note that $[ga^{-(m+1)}](a^m, b, a^{-m})$ contains the subpath $[ga^{-(k+1)}](a^k, b, a^{-k})$ for $0 \leq k \leq m$.

Case 1. Assume that C_0 contains $[g](b)$. Construct C_k by:

- replacing the oriented edge $[g](b)$ with the oriented path $[g](a^{-k}, b, a^k)$, and
- replacing the oriented path $[ga^{-(k+1)}](a^k, b, a^{-k})$ with the oriented edge $[ga^{-(k+1)}](b)$

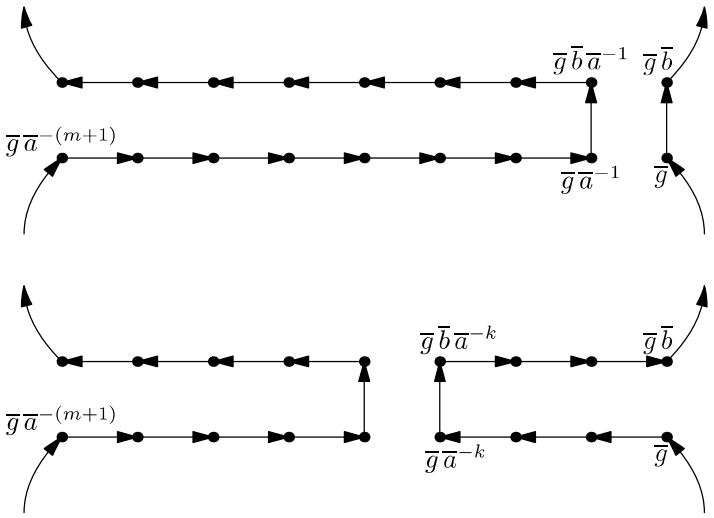

Figure 1: A portion of the hamiltonian cycles C_0 (top) and C_k (bottom).

(see Figure 1).

To calculate the voltage of C_k, write $C_0 = [g](s_1, \ldots, s_n)$. There is some ℓ with $\overline{s_1} \cdots \overline{s_\ell} = \overline{a}^{-1}$, so

$$C_k = [g]\big(a^{-k}, b, a^k,\ (s_i)_{i=2}^{\ell-k},\ b, (s_i)_{i=\ell+k+2}^{n}\big).$$

For convenience, let

$$h = \prod_{i=\ell+1}^{n} s_i \equiv \left(\prod_{i=1}^{\ell} s_i\right)^{-1} \equiv a \ (\mathrm{mod}\, G').$$

Then, from Remark 2.6 (and the fact that G' is commutative), we have

$$\begin{aligned}
\big(\Pi C_k\big)^g &= (a^{-k}ba^k)\left(\prod_{i=2}^{\ell-k} s_i\right) b \left(\prod_{i=\ell+k+2}^{n} s_i\right) \\
&= (a^{-k}ba^kb^{-1})\left(\prod_{i=1}^{\ell} s_i\right) a^{-k}ba^kb^{-1} \left(\prod_{i=\ell+1}^{n} s_i\right) \\
&= [a^k, b^{-1}] \cdot \left(\prod_{i=1}^{\ell} s_i\right)\left(\prod_{i=\ell+1}^{n} s_i\right) \cdot [a^k, b^{-1}]^h \\
&= [a^k, b^{-1}] \cdot \big(\Pi C_0\big)^g \cdot [a^k, b^{-1}]^a \\
&= \big(\Pi C_0\big)^g \cdot [a^k, b^{-1}]\,[a^k, b^{-1}]^a.
\end{aligned}$$

Case 2. Assume that C_0 contains $[gb](b^{-1})$. This is similar. Construct C_k by:

- replacing the oriented edge $[gb](b^{-1})$ with the oriented path $[gb](a^{-k}, b^{-1}, a^k)$, and

- replacing the oriented path $[ga^{-(k+1)}](a^k, b, a^{-k})$ with the oriented edge $[ga^{-(k+1)}](b)$.

(See Figure 1, but reverse the orientation of the paths in the right half of the figure.)

To calculate the voltage of C_k, write $C_0 = [gb](s_1, \dots, s_n)$. There is some ℓ with $\overline{s_1} \cdots \overline{s_\ell} = \overline{ab}^{-1}$, so

$$C_k = [gb]\big(a^{-k}, b^{-1}, a^k,\ (s_i)_{i=2}^{\ell-k},\ b, (s_i)_{i=\ell+k+2}^{n}\big).$$

For convenience, let

$$h = \prod_{i=\ell+1}^{n} s_i \equiv \left(\prod_{i=1}^{\ell} s_i\right)^{-1} \equiv ab \pmod{G'}.$$

Then

$$\begin{aligned}
\big(\Pi C_k\big)^{gb} &= (a^{-k}b^{-1}a^k)\left(\prod_{i=2}^{\ell-k} s_i\right) b \left(\prod_{i=\ell+k+2}^{n} s_i\right) \\
&= (a^{-k}b^{-1}a^k b)\left(\prod_{i=1}^{\ell} s_i\right) a^{-k}ba^kb^{-1}\left(\prod_{i=\ell+1}^{n} s_i\right) \\
&= b^{-1}(ba^{-k}b^{-1}a^k)b \cdot \left(\prod_{i=1}^{\ell} s_i\right)\left(\prod_{i=\ell+1}^{n} s_i\right) \cdot [a^k, b^{-1}]^h \\
&= [b^{-1}, a^k]^b \cdot \big(\Pi C_0\big)^{gb} \cdot [a^k, b^{-1}]^{ab} \\
&= \big(\Pi C_0\big)^{gb} \cdot [b^{-1}, a^k]^b\,[a^k, b^{-1}]^{ab}. \qquad \square
\end{aligned}$$

Remark 3.2. In the situation of Lemma 3.1, we have $\Big\langle \big(\Pi C_0\big)^{-1}\big(\Pi C_k\big) \Big\rangle = \langle [a^k, b^{-1}] \rangle$ if either

(1) C_0 contains $[g](b)$ and a does not invert any nontrivial element of $\langle [a^k, b^{-1}] \rangle$, or

(2) C_0 contains $[gb](b^{-1})$ and a does not centralize any nontrivial element of $\langle [a^k, b^{-1}] \rangle$.

Note that if $|G|$ is odd, then the hypothesis on a in (1) is automatically satisfied (because no element of odd order can ever invert a nontrivial element).

Corollary 3.3 (cf. [4, Case iv] and [10, Case 4.3])**.** Assume

- $a \in S$ with $\langle \overline{a} \rangle \neq \overline{G}$,
- $(s_i)_{i=1}^{d}$ is a hamiltonian cycle in $\mathrm{Cay}\big(\overline{G}/\langle \overline{a} \rangle; S\big)$,
- $a^r \prod_{i=1}^{d} s_i \in G'$, with $0 \leq r \leq |\overline{a}| - 2$, and
- $0 \leq k \leq |\overline{a}| - 3$.

Then the walk

$$\begin{aligned}
C_k = \big(&a^k, s_1, a^{-(k+1)}, (s_{2i}, a^{|\overline{a}|-2}, s_{2i+1}, a^{-(|\overline{a}|-2)})_{i=1}^{(d-3)/2}, \\
&s_{d-1}, a^r, s_d, a^{-(|\overline{a}|-k-2)}, s_1, a^{|\overline{a}|-k-3}, (s_i)_{i=2}^{d-1}, a^{-(|\overline{a}|-r-2)}, s_d\big)
\end{aligned}$$

is a hamiltonian cycle in $\mathrm{Cay}(\overline{G}; S)$ (see Figure 2), and we have

$$\Pi C_k = (\Pi C_0)[a^{-k}, s_1^{-1}][a^{-k}, s_1^{-1}]^{a^{-1}}.$$

Proof. C_0 contains the oriented edge (s_1) and the oriented path $[a^{|\overline{a}|-2}](a^{-(|\overline{a}|-3)}, s_1, a^{|\overline{a}|-3})$, so we may apply Lemma 3.1 with $g = e$, $b = s_1$, and a^{-1} in the role of a. □

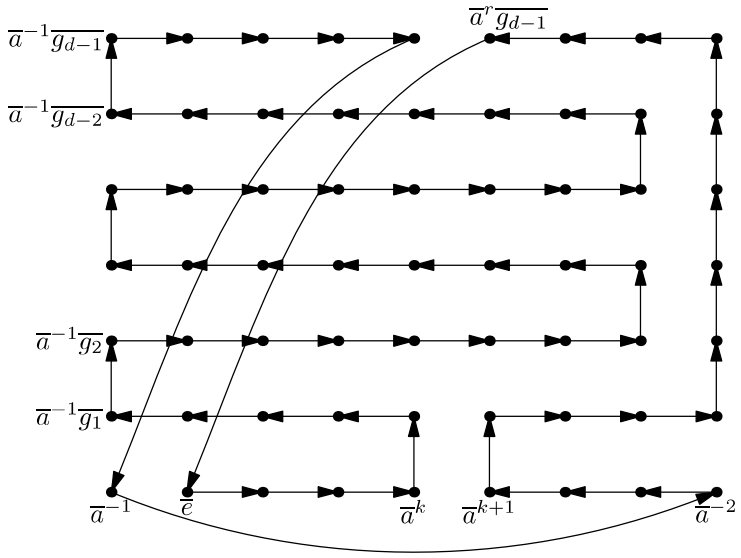

Figure 2: A hamiltonian cycle C_k in $\mathrm{Cay}(\overline{G}; S)$, where $g_j = \prod_{i=1}^{j} s_i$.

4 Other applications of Marušič's Method

Here are some other situations in which we can apply Marušič's Method (2.10).

Theorem 4.1 ([10, §4 and §5])**.** Suppose

- $|G|$ is odd,
- $G' = \mathbb{Z}_{p^\mu}$ is cyclic of prime-power order,
- S is a generating set of G,
- $S \cap G' = \emptyset$, and
- G is **not** the nonabelian group of order 27 with exponent 3.

Then there exist hamiltonian cycles C_1 and C_2 in $\mathrm{Cay}(G/G'; S)$ that have an oriented edge in common, such that $(\Pi C_1)^{-1}(\Pi C_2)$ generates G'.

Proof. Lemma 2.8 allows us to assume $|G'| = p$. Then the desired conclusion is implicit in [10, §4 and §5] unless $|G/G'| \cong \mathbb{Z}_3 \times \mathbb{Z}_3$ and $p = 3$.

Therefore $G/(G')^3$ is a nonabelian group of order 27, so Lemma 2.21(1) tells us $|G| = 27$. By assumption, the exponent of G is greater than 3, so we conclude from

Lemma 2.21(3) that S contains an element b with $|b| \geq 9$. We may assume S is minimal, so $\#S = 2$; write $S = \{a, b\}$. Then we have the following two hamiltonian cycles in $\mathrm{Cay}(\overline{G}; S)$:

$$C_1 = (a^2, b)^3 \text{ and } C_2 = (a^2, b^{-1})^3.$$

Since Lemma 2.21(2) tells us $(xy)^3 = x^3y^3$ for all $x, y \in G$, and we have $x^3 \in G' = Z(G)$ for all $x \in G$, we see that

$$(\Pi C_1)^{-1}(\Pi C_2) = \big((a^2b)^3\big)^{-1}\big(a^2b^{-1}\big)^3 = \big((a^2)^3b^3\big)^{-1}\big((a^2)^3(b^{-1})^3\big) = b^{-6} \neq e,$$

since $|b| \geq 9$. □

We will use the following version of this result in Subcase ii of Case 5.12.

Proposition 4.2. Suppose

- $|G|$ is odd,
- $G' = \mathbb{Z}_p$ has prime order,
- Z is a subgroup of $Z(G)$,
- $S \cap G'Z = \emptyset$, and
- G is not nilpotent.

Then there exist hamiltonian cycles C_1 and C_2 in $\mathrm{Cay}\big(G/(G'Z); S\big)$ that have an oriented edge in common, such that $\big\langle (\Pi C_1)^{-1}(\Pi C_2)\big\rangle = G'$.

Proof. Choose $a, b \in S$ with $[a, b] \neq e$. Since G is not nilpotent, we may assume a does not centralize G'. Furthermore, since we are using Marušič's Method (2.10), there is no harm in assuming $S = \{a, b\}$.

If $b \notin \langle a, G', Z\rangle$, then the proof of [10, Case 5.3] provides two hamiltonian cycles $C_1 = (s_i)_{i=1}^n$ and $C_2 = (t_i)_{i=1}^n$ in $\mathrm{Cay}\big(G/(G'Z); a, b\big)$, such that $\Pi C_1 \neq \Pi C_2$ (and the two cycles have an oriented edge in common). From the construction, it is clear that $(s_i)_{i=1}^n$ is a permutation of $(t_i)_{i=1}^n$, so $(\Pi C_1)^{-1}(\Pi C_2) \in G'$.

We may now assume $b \in \langle a, G', Z\rangle$. Then, letting $n = |G : \langle a, G', Z\rangle|$, there is some i, such that $b^i \in a^iG'Z$ and $0 < i < n$. Therefore, we have the following two hamiltonian cycles in $\mathrm{Cay}\big(G/(G'Z); S\big)$ that both contain the oriented edge (b):

$$C_1 = (b, a^{-(i-1)}, b, a^{n-i-1}),$$
$$C_2 = (b, a^{n-i-1}, b, a^{-(i-1)}) = [a^{-1}]C_1.$$

The sequence of edges in C_2 is a permutation of the sequence of edges in C_1, therefore $(\Pi C_1)^{-1}(\Pi C_2) \in G'$. Also, since a does not centralize G', it is not difficult to see that $(\Pi C_1)^{-1}(\Pi C_2)$ is nontrivial, and therefore generates G'. □

Lemma 4.3. Assume

- $G' = \mathbb{Z}_{p^\mu} \times \mathbb{Z}_{q^\nu}$, where p and q are prime,
- $S \cap G' = \emptyset$,
- there exist $a, b \in S \cup S^{-1}$, with $a \neq b$, such that $aG' = bG'$,

- the generating set S is minimal, and
- $|G|$ is odd.

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

Proof. Write $b = a\gamma$, with $\gamma \in G'$.

Case 1. Assume $\langle\gamma\rangle = G'$. We apply Marušič's Method (2.10), so Lemma 2.8 allows us to assume $G' = \mathbb{Z}_p \times \mathbb{Z}_q$. Since $|\overline{a}| \geq 3$, it is easy to find an oriented hamiltonian cycle C_0 in $\mathrm{Cay}\big(\overline{G};S\big)$ that has (at least) 2 oriented edges α_1 and α_2 that are labeled a. We construct two more hamiltonian cycles C_1 and C_2 by replacing one or both of α_1 and α_2 with a b-edge. (Replace one a-edge to obtain C_1; replace both to obtain C_2.) Then there are conjugates γ_1 and γ_2 of γ, such that

$$(\Pi C_0)^{-1}(\Pi C_1) = \gamma_1, \quad (\Pi C_1)^{-1}(\Pi C_2) = \gamma_2, \quad (\Pi C_0)^{-1}(\Pi C_2) = \gamma_1\gamma_2.$$

By the assumption of this case, we know that γ_1 and γ_2 generate G'. Also, since $|G|$ is odd, we know that no element of G inverts any nontrivial element of G', so $\gamma_1\gamma_2$ also generates G'. Therefore, Marušič's Method 2.11(1) applies.

Case 2. Assume $\langle\gamma\rangle \neq G'$. Since S is minimal, we know $\langle\gamma\rangle$ contains either $\mathbb{Z}_{p^\mu}$ or $\mathbb{Z}_{q^\nu}$. By the assumption of this case, we know it does not contain both. So let us assume $\langle\gamma\rangle = N \times \mathbb{Z}_{q^\nu}$, where N is a proper subgroup of $\mathbb{Z}_{p^\mu}$.

Assume, for the moment, that $G/(G')^p$ is not the nonabelian group of order 27 and exponent 3. We use Marušič's Method (2.10), so Lemma 2.8 allows us to assume $G' = \mathbb{Z}_p \times \mathbb{Z}_q$. Applying Theorem 4.1 to $G/\mathbb{Z}_q$ provides us with hamiltonian cycles C_1 and C_2 in $\mathrm{Cay}\big(G/G';S\smallsetminus\{b\}\big)$, such that $\big\langle(\Pi C_1)^{-1}(\Pi C_2)\big\rangle$ contains $\mathbb{Z}_p$. (Furthermore, the two cycles have an oriented edge in common.) Since S is a minimal generating set, we know that C_i contains an edge labelled $a^{\pm1}$. (In fact, more than one, so we can take one that is not the edge in common with the other cycle.) Assume, without loss of generality, that it is labelled a. Replacing this edge with b results in a hamiltonian cycle C_i', such that $\big\langle(\Pi C_i)^{-1}(\Pi C_i')\big\rangle = \langle\gamma\rangle = \mathbb{Z}_q$. Then Marušič's Method 2.11(2) applies.

We may now assume that $G/(G')^p$ is the nonabelian group of order 27 and exponent 3. Then $G/\langle\gamma\rangle$ is a 3-group, so Theorem 2.12 tells us there is a directed hamiltonian cycle C_0 in the Cayley digraph $\overrightarrow{\mathrm{Cay}}\big(G/\langle\gamma\rangle;S\smallsetminus\{b\}\big)$. Since $S\smallsetminus\{b\}$ is a minimal generating set of $G/\langle\gamma\rangle$, there must be at least two edges α_1 and α_2 that are labeled a in C. Now the proof of Case 1 applies (but with $\langle\gamma\rangle$ in the place of G'). □

5 Proof of Theorem 1.2

Assumption 5.1. We always assume:

(1) The generating set S is minimal.

(2) $S \cap G' = \emptyset$ (see Corollary 2.17).

(3) p and q are distinct (see Theorem 1.1).

(4) G is not nilpotent (see Theorem 2.13). This implies $G/(G')^{pq}$ is not nilpotent [9, Satz 3.5, p. 270].

(5) There do not exist $a, b \in S \cup S^{-1}$ with $a \neq b$ and $aG' = bG'$ (see Lemma 4.3).

(6) There does not exist $s \in S$, such that $G' \subseteq \langle s\rangle$ (see Theorem 2.16).

Remark 5.2. We consider several cases that are exhaustive up to permutations of the variables a, b, and c, and interchanging p and q. Here is an outline of the cases:

- There exist $a, b \in S$, such that $\langle [a,b] \rangle = G'$.

  (5.3) $\overline{b} \in \langle \overline{a} \rangle$.
  (5.4) $\overline{b} \notin \langle \overline{a} \rangle$ and $|\overline{a}| \geq 5$.
  (5.5) $|\overline{a}| = |\overline{b}| = 3$ and $\langle \overline{a} \rangle \neq \langle \overline{b} \rangle$.

- There exist $a, b, c \in S$, such that $\mathbb{Z}_{p^\mu} \subseteq \langle [a,b] \rangle$ and $\mathbb{Z}_{q^\nu} \subseteq \langle [a,c] \rangle$.

  (5.7) $\overline{b}, \overline{c} \in \langle \overline{a} \rangle$.
  (5.8) $\langle \overline{a} \rangle \subsetneq \langle \overline{a}, \overline{b} \rangle \subsetneq \langle \overline{a}, \overline{b}, \overline{c} \rangle$.
  (5.9) a centralizes $G'/(G')^{pq}$.
  (5.10) $\overline{b}, \overline{c} \notin \langle \overline{a} \rangle$.
  (5.11) $\overline{c} \in \langle \overline{a} \rangle$ and $\overline{b} \notin \langle \overline{a} \rangle$.

- There do not exist $a, b, c \in S$, such that $\langle [a,b], [a,c] \rangle = G'$. (5.12)

Case 5.3. Assume there exist $a, b \in S$, such that $\langle [a,b] \rangle = G'$ and $\overline{b} \in \langle \overline{a} \rangle$.

Proof. We use Marušič's Method (2.11), so there is no harm in assuming $S = \{a, b\}$. Then $\langle \overline{a} \rangle = \langle \overline{a}, \overline{b} \rangle = \overline{G}$. Furthermore, Lemma 2.8 allows us to assume $G' = \mathbb{Z}_{pq}$. Let $n = |\overline{a}| = |\overline{G}|$, fix k with $\overline{b} = \overline{a}^k$, and choose $\gamma \in G'$, such that $b = a^k\gamma$. Note that

- $a^n = e$ (since Corollary 2.20 implies that a cannot centralize a nontrivial subgroup of G'), and
- $\langle \gamma \rangle = G'$ (since $\langle a \rangle \ltimes \langle \gamma \rangle = \langle a, b \rangle = G$).

We may assume $1 \leq k < n/2$, by replacing b with its inverse if necessary. We may also assume $n \geq 5$ (otherwise, we must have $k = 1$, contrary to Assumption 5.1(5)). Therefore $n - k - 2 > 0$.

We have the following three hamiltonian cycles in $\mathrm{Cay}(\overline{G}; a, b)$:

$$C_1 = (a^n), \qquad C_2 = (a^{n-k-1}, b, a^{-(k-1)}, b), \qquad C_3 = (a^{n-k-2}, b, a^{-(k-1)}, b, a).$$

Their voltages are

$$\Pi C_1 = a^n = e,$$
$$\Pi C_2 = a^{n-k-1}ba^{-(k-1)}b = a^{n-k-1}(a^k\gamma)a^{-(k-1)}(a^k\gamma) = a^n \cdot a^{-1}\gamma a\gamma = \gamma^a\gamma,$$
$$\Pi C_3 = a^{n-k-2}ba^{-(k-1)}ba = a^{-1}(a^{n-k-1}ba^{-(k-1)}b)a = (\Pi C_2)^a.$$

Since $|G|$ is odd, we know that a does not invert $\mathbb{Z}_p$ or $\mathbb{Z}_q$. Therefore ΠC_2 generates G'. Hence, the conjugate ΠC_3 must also generate G'. Furthermore, as was mentioned above, we know that a does not centralize any nontrivial element of G', so $(\Pi C_2)(\Pi C_3)^{-1}$ also generates G'. (Also note that all three hamiltonian cycles contain the oriented edge (a).) Hence, Marušič's Method 2.11(1) applies. □

Case 5.4. Assume there exist $a, b \in S$, such that $\langle [a,b] \rangle = G'$ and $\overline{b} \notin \langle \overline{a} \rangle$. Also assume $|\overline{a}| \geq 5$.

Proof (cf. proof of [10, Case 4.3]). We use Marušič's Method (2.11), so there is no harm in assuming $S = \{a, b\}$. Furthermore, Lemma 2.8 allows us to assume $G' = \mathbb{Z}_{pq}$. Let $d = |\overline{G}/\langle\overline{a}\rangle|$, so there is some r with $\overline{b}^d\overline{a}^r = \overline{e}$ and $0 \le r < |\overline{a}|$. We may assume $r \le |\overline{a}| - 2$, by replacing b with its inverse if necessary.

Applying Corollary 3.3 to the hamiltonian cycle (b^{-d}) yields hamiltonian cycles C_0, C_1, and C_2 (since $2 = 5 - 3 \le |\overline{a}| - 3$). Note that all of these contain the oriented edge $\overline{b}(b^{-1})$. Furthermore, the voltage of C_k is

$$\Pi C_k = \pi[a^{-k}, b]\,[a^{-k}, b]^{a^{-1}},$$

where $\pi = \Pi C_0$ is independent of k.

Since $[a^{-1}, b]$ generates G', and a does not invert any nontrivial element of G' (recall that $|G|$ is odd), it is easy to see that G' is generated by the difference of any two of

$$e,\ [a^{-1}, b],\ \text{and}\ [a^{-2}, b] = [a^{-1}, b][a^{-1}, b]^{a^{-1}}.$$

Using again the fact that a does not invert any element of G', this implies that G' is generated by the difference of any two of the three voltages, so Marušič's Method 2.11(1) applies. □

Case 5.5. Assume there exist $a, b \in S$, such that $\langle[a, b]\rangle = G'$, $|\overline{a}| = |\overline{b}| = 3$ and $\langle\overline{a}\rangle \ne \langle\overline{b}\rangle$.

Proof. This proof is rather lengthy. It can be found in Section 6. □

Assumption 5.6. Henceforth, we assume there do not exist $a, b \in S \cup S^{-1}$, such that $\langle[a, b]\rangle = G'$.

Case 5.7. Assume $\mathbb{Z}_{p^\mu} \subseteq \langle[a, b]\rangle$, $\mathbb{Z}_{q^\nu} \subseteq \langle[a, c]\rangle$, and $\langle\overline{b}, \overline{c}\rangle \subseteq \langle\overline{a}\rangle$.

Proof. We use Marušič's Method (2.11), so there is no harm in assuming $S = \{a, b, c\}$. (Furthermore, Lemma 2.8 allows us to assume $G' = \mathbb{Z}_{pq}$, so $\langle[a, b]\rangle = \mathbb{Z}_p$ and $\langle[a, c]\rangle = \mathbb{Z}_q$.) Then, since $\overline{b}, \overline{c} \in \langle\overline{a}\rangle$, we must have $\langle\overline{a}\rangle = \overline{G}$. Therefore, Corollary 2.20 tells us that a does not centralize any nonidentity element of G'. Fix k and ℓ with $\overline{b} = \overline{a}^k$ and $\overline{c} = \overline{a}^\ell$. We may write $b = a^k\gamma_1$ and $c = a^\ell\gamma_2$, for some $\gamma_1 \in \mathbb{Z}_p$ and $\gamma_2 \in \gamma_q$.

Since 1, k, and ℓ are distinct (see Assumption 5.1(5)), we may assume $1 < k < \ell < n/2$, by interchanging b and c and/or replacing b and/or c with its inverse if necessary. Therefore $\ell \ge 3$ and $k + \ell \le n - 2$, so we have the following three hamiltonian cycles in $\mathrm{Cay}(\overline{G}; a, b, c)$:

$$\begin{aligned}
C_1 &= (a^{-n})\\
C_2 &= (a^{-(\ell-1)}, c,\ b, a^{-(k-1)}, b,\ a^{n-k-\ell-2},\ c)\\
C_3 &= (a^{-(\ell-2)}, c,\ b, a^{-(k-1)}, b,\ a^{n-k-\ell-2},\ c, a^{-1}).
\end{aligned}$$

Note that each of these contains the oriented edge (a^{-1}).

Since a does not centralize any nonidentity element of G', we know $\Pi C_1 = e$. A straightforward calculation shows

$$\Pi C_2 = (\gamma_1\gamma_1^{a^{-1}})^{a^{-k-1}}(\gamma_2^{a^{-1}}\gamma_2),$$

which generates G'. Therefore, $\Pi C_3 = (\Pi C_2)^{a^{-1}}$ and $(\Pi C_2)^{-1}(\Pi C_3)$ also generate G'. (For the latter, note that a^{-1} does not centralize any nonidentity element of G'.) Therefore Marušič's Method 2.11(1) applies. □

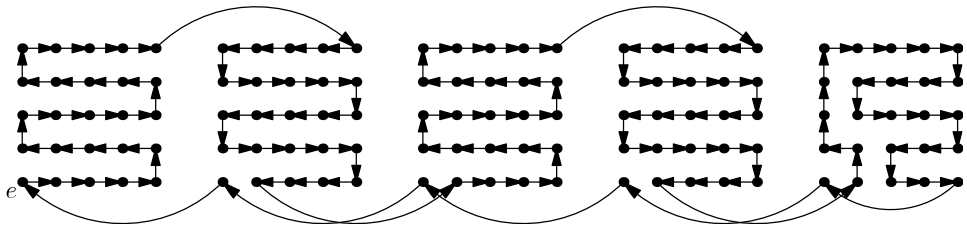

Figure 3: A hamiltonian cycle X.

Case 5.8. Assume $\mathbb{Z}_{p^\mu} \subseteq \langle [a,b] \rangle$, $\mathbb{Z}_{q^\nu} \subseteq \langle [a,c] \rangle$, and there exists $s \in \{a,b\}$, such that $\langle \overline{a} \rangle \subsetneq \langle \overline{a}, \overline{s} \rangle \subsetneq \langle \overline{a}, \overline{b}, \overline{c} \rangle$.

Proof. We use Marušič's Method (2.11), so there is no harm in assuming $S = \{a,b,c\}$. Furthermore, Lemma 2.8 allows us to assume $G' = \mathbb{Z}_{pq}$, so $\langle [a,b] \rangle = \mathbb{Z}_p$ and $\langle [a,c] \rangle = \mathbb{Z}_q$. Choose $A, B, C \geq 3$, such that $\overline{a}^A = \overline{e}$, and every element of $\overline{G}$ can be written uniquely in the form

$$\overline{a}^x \overline{b}^y \overline{c}^z \text{ with } \begin{array}{r} 0 \leq x < A, \\ 0 \leq y < B, \\ 0 \leq z < C. \end{array}$$

More precisely, we may let

$$\begin{cases} A = |\overline{a}|, B = |\langle \overline{a}, \overline{b} \rangle : \langle \overline{a} \rangle|, C = |\overline{G} : \langle \overline{a}, \overline{b} \rangle| & \text{if } s = b, \\ A = |\overline{a}|, C = |\langle \overline{a}, \overline{c} \rangle : \langle \overline{a} \rangle|, B = |\overline{G} : \langle \overline{a}, \overline{c} \rangle| & \text{if } s = c. \end{cases}$$

Then we have the following hamiltonian cycle X in $\mathrm{Cay}(\overline{G}; a, b, c)$ (see Figure 3):

$$\begin{aligned} X = \Big(a, \Big(& a^{A-2}, (b, a^{-(A-1)}, b, a^{A-1})^{(B-1)/2}, c, \\ & (a^{-(A-1)}, b^{-1}, a^{A-1}, b^{-1})^{(B-1)/2}, a^{-(A-2)}, c \Big)^{(C-1)/2}, \\ & b, a^{-1}, b^{B-2}, a, (a^{A-2}, b^{-1}, a^{-(A-2)}, b^{-1})^{(B-3)/2}, \\ & a^{A-2}, b^{-1}, a^{-(A-3)}, b^{-1}, a^{A-2}, c^{-(C-1)} \Big). \end{aligned}$$

We obtain a new hamiltonian cycle X^p by replacing a subpath of the form $[g](a^{A-1}, b, a^{-(A-1)})$ with $[g](a^{-(A-1)}, b, a^{A-1})$. Then $(\Pi X)^{-1}(\Pi X^p)$ is a conjugate of

$$(a^{A-1} b a^{-(A-1)})^{-1} (a^{-(A-1)} b a^{A-1}) = [b, a^{A-1}]^a [b, a^{A-1}].$$

Similarly, replacing a subpath of the form $[g](a^{A-1}, c, a^{-(A-1)})$ with $[g](a^{-(A-1)}, c, a^{A-1})$ results in a hamiltonian cycle X_q, such that $(\Pi X)^{-1}(\Pi X_q)$ is a conjugate of $[c, a^{A-1}]^a [c, a^{A-1}]$. Furthermore, doing both replacements results in a hamiltonian cycle X_q^p, such that $(\Pi X^p)^{-1}(\Pi X_q^p)$ is also a conjugate of $[c, a^{A-1}]^a [c, a^{A-1}]$. Note that all four of these hamiltonian cycles contain the oriented edge $c(c^{-1})$.

Since $G' \not\subseteq \langle a \rangle$ (see Assumption 5.1(6)), we may assume $a^A \in \mathbb{Z}_p$ (by interchanging p and q if necessary). Since $[c,a] \in \mathbb{Z}_q$, this implies that c centralizes a^A, so $[c, a^{A-1}] =$

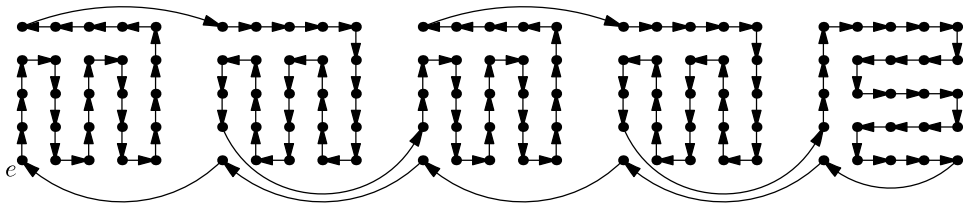

Figure 4: A hamiltonian cycle Y_1.

$[c, a^{-1}]$ generates $\mathbb{Z}_q$. Since a does not invert any nontrivial element of $\mathbb{Z}$ (recall that G has odd order), this implies that $[c, a^{A-1}]^a[c, a^{A-1}]$ generates $\mathbb{Z}_q$.

Assume, for the moment, that $[b, a^{A-1}]$ generates $\mathbb{Z}_p$. Since a does not invert any nontrivial element of $\mathbb{Z}_p$, this implies that $[b, a^{A-1}]^a[b, a^{A-1}]$ generates $\mathbb{Z}_p$. Therefore, Marušič's Method 2.11(2) applies.

We may now assume $[b, a^{A-1}]$ does not generate $\mathbb{Z}_p$. This means $[b, a^{A-1}] = e$. Since $[b, a^{-1}] \neq e$, we conclude that $[b, a^A] \neq e$, so

$$b \text{ does not centralize } \mathbb{Z}_p.$$

We have the following hamiltonian cycle Y_1 in $\mathrm{Cay}(\overline{G}; a, b, c)$ (see Figure 4):

$$\begin{aligned} Y_1 = \Big(b, \Big(b^{B-3}, (a, b^{-(B-2)}, a, b^{B-2})^{(A-1)/2}, b, a^{-(A-1)}, c,\\ a^{A-1}, b^{-1}, (b^{-(B-2)}, a^{-1}, b^{B-2}, a^{-1})^{(A-1)/2}, b^{-(B-3)}, c\Big)^{(C-1)/2},\\ b^{B-2}, a, (a^{A-2}, b^{-1}, a^{-(A-2)}, b^{-1})^{(B-1)/2}, a^{A-1}, c^{-(C-1)}\Big). \end{aligned}$$

We create a new hamiltonian cycle Y_2 by replacing a subpath of the form $[g](a^{-(A-1)}, c, a^{A-1})$ with $[g](a^{A-1}, c, a^{-(A-1)})$. This is the same as the construction of X_q from X, but with a and a^{-1} interchanged, so the same calculation shows

$$(\Pi Y_1)^{-1}(\Pi Y_2) \text{ is a conjugate of } [c, a^{-(A-1)}]^{a^{-1}}[c, a^{-(A-1)}], \text{ which generates } \mathbb{Z}_q.$$

Furthermore, since Y_1 and Y_2 both contain the oriented path $[b^{B-3}](b, a, b^{-1})$, and either the oriented edge $[b^{B-2}](a)$ or the oriented edge $[b^{B-2}a](a^{-1})$, Remark 3.2 provides hamiltonian cycles Y_1' and Y_2', such that $(\Pi Y_i)^{-1}(\Pi Y_i')$ generates $\mathbb{Z}_p$. Since all four hamiltonian cycles contain the oriented edge $[c](c^{-1})$, Marušič's Method 2.11(2) applies. □

Case 5.9. Assume $\mathbb{Z}_{p^\mu} \subseteq \langle [a, b] \rangle$, $\mathbb{Z}_{q^\nu} \subseteq \langle [a, c] \rangle$, and a centralizes $G'/(G')^{pq}$.

Proof. We use Marušič's Method (2.11), so there is no harm in assuming $S = \{a, b, c\}$. Furthermore, Lemma 2.8 allows us to assume $G' = \mathbb{Z}_{pq}$, so $\langle [a, b] \rangle = \mathbb{Z}_p$ and $\langle [a, c] \rangle = \mathbb{Z}_q$.

Note that $[a, b^{-1}, c] \in \mathbb{Z}_p$, $[c, a^{-1}, b] \in \mathbb{Z}_q$, and $[b, c^{-1}, a] = e$ (because a centralizes G'). Since $\mathbb{Z}_p \cap \mathbb{Z}_q = \{e\}$, and the Three-Subgroup Lemma [7, Thm. 2.3, p. 19] tells us

$$[a, b^{-1}, c]^b[b, c^{-1}, a]^c[c, a^{-1}, b]^a = e,$$

we conclude that $[a, b^{-1}, c] = [c, a^{-1}, b] = e$, so

$$c \text{ centralizes } \mathbb{Z}_p \text{ and } b \text{ centralizes } \mathbb{Z}_q.$$

We know $G' \not\subseteq Z(G)$, because G is not nilpotent (see Assumption 5.1(4)). Since a centralizes G', this implies we may assume c does not centralize G' (by interchanging b and c if necessary). So c does not centralize $\mathbb{Z}_q$. Since a, b, and G' all centralize $\mathbb{Z}_q$, this implies $c \notin \langle a, b, G' \rangle$. In other words, $\overline{c} \notin \langle \overline{a}, \overline{b} \rangle$. Furthermore, applying Corollary 2.20 to the group $\langle a, b \rangle$ tells us that $\langle \overline{a} \rangle \neq \langle \overline{a}, \overline{b} \rangle$. Therefore $\langle \overline{a} \rangle \subsetneq \langle \overline{a}, \overline{b} \rangle \subsetneq \langle \overline{a}, \overline{b}, \overline{c} \rangle$, so Case 5.8 applies. □

Case 5.10. Assume $\mathbb{Z}_{p^\mu} \subseteq \langle [a, b] \rangle$, $\mathbb{Z}_{q^\nu} \subseteq \langle [a, c] \rangle$, and $\overline{b}, \overline{c} \notin \langle \overline{a} \rangle$.

Proof. We use Marušič's Method (2.11), so there is no harm in assuming $S = \{a, b, c\}$. Furthermore, Lemma 2.8 allows us to assume $G' = \mathbb{Z}_{pq}$, so $\langle [a, b] \rangle = \mathbb{Z}_p$ and $\langle [a, c] \rangle = \mathbb{Z}_q$. We may assume $\langle \overline{a}, \overline{b} \rangle = \langle \overline{a}, \overline{c} \rangle = \overline{G}$, for otherwise Case 5.8 applies.

Let us begin by showing that a does not centralize any nontrivial element of G'. Suppose not. Then we may assume that a centralizes $\mathbb{Z}_p$. Let $\underline{G} = G/\mathbb{Z}_q = G/\langle [a, c] \rangle$. Since $\langle a, c, G' \rangle = G$, we know that $\langle \underline{a}, \underline{c}, \underline{\mathbb{Z}_p} \rangle = \underline{G}$, so $\underline{a}$ is in the center of $\underline{G}$. This contradicts the fact that $\langle [\underline{a}, \underline{b}] \rangle = \underline{\mathbb{Z}_p}$ is nontrivial.

Since $\overline{G}$ is abelian (and because $\overline{b}, \overline{c} \notin \langle \overline{a} \rangle$), it is easy to choose a hamiltonian cycle $(s_i)_{i=1}^d$ in $\mathrm{Cay}(\overline{G}/\langle \overline{a} \rangle; S)$ that contains both an edge labeled b (or b^{-1}) and an edge labeled c (or c^{-1}). Note that

$$C_0 = \big((s_i)_{i=1}^{d-1}, a^{|\overline{a}|-1}, (s_{d-2i+1}^{-1}, a^{-(|\overline{a}|-2)}, s_{d-2i}^{-1}, a^{|\overline{a}|-2})_{i=1}^{(d-1)/2}, a\big)$$

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

Subcase i. *Assume* $|\overline{a}| > 3$. We may assume $s_1 = b^{-1}$ and $s_2 = c^{-1}$. Then C_0 contains the four subpaths

$$(b^{-1}), \quad [b^{-1}a^2](a^{-1}, b, a), \quad [b^{-1}](c^{-1}), \quad [b^{-1}c^{-1}a^{-2}](a, c, a^{-1}).$$

Therefore, we may let g be either b^{-1} or $b^{-1}c^{-1}$ in Lemma 3.1, so Remark 3.2(2) tells us we have hamiltonian cycles C^b and C^c, such that $(\Pi C_0)^{-1}(\Pi C^b)$ is a generator of $\mathbb{Z}_p$, and $(\Pi C_0)^{-1}(\Pi C^c)$ is a generator of $\mathbb{Z}_q$. Since $|\overline{a}| > 3$, we see that

$$C^b, \text{ like } C_0, \text{ contains } [b^{-1}](c^{-1}) \text{ and } [b^{-1}c^{-1}a^{-2}](a, c, a^{-1}),$$

so Remark 3.2(2) provides a hamiltonian cycle C_c^b, such that $(\Pi C^b)^{-1}(\Pi C_c^b)$ is a generator of $\mathbb{Z}_q$. Therefore, Marušič's Method 2.11(2) applies (since each of these four hamiltonian cycles contains the oriented edge $[a^{-1}](a)$).

Subcase ii. *Assume* $d > 3$. We may assume $s_1 = b^{-1}$ and $s_3 = c^{-1}$. Then C_0 contains the four subpaths

$$(b^{-1}), \ [b^{-1}a^2](a^{-1}, b, a), \quad [s_1 s_2](c^{-1}), \ [s_1 s_2 c^{-1}a^2](a^{-1}, c, a).$$

Therefore, we may let g be either b^{-1} or $s_1 s_2 c^{-1}$ in Lemma 3.1, so Remark 3.2(2) tells us we have hamiltonian cycles C^b and C^c, such that $(\Pi C_0)^{-1}(\Pi C^b)$ is a generator of $\mathbb{Z}_p$, and $(\Pi C_0)^{-1}(\Pi C^c)$ is a generator of $\mathbb{Z}_q$. It is clear that C^b, like C_0, contains $[s_1 s_2](c^{-1})$

and $[s_1s_2c^{-1}a^2](a^{-1},c,a)$, so Remark 3.2(2) provides a hamiltonian cycle C_c^b, such that $(\Pi C^b)^{-1}(\Pi C_c^b)$ is a generator of $\mathbb{Z}_q$. Therefore, Marušič's Method 2.11(2) applies (since each of these four hamiltonian cycles contains the oriented edge $[a^{-1}](a)$).

Subcase iii. *Assume* $|\overline{a}|=3$ *and* $d=3$. Since $d=3$, we may assume $\overline{b}\equiv\overline{c}\pmod{\langle\overline{a}\rangle}$ (by replacing c with its inverse if necessary). Let

$$C_0=(b^{-1},c^{-1},a^2,c,a^{-1},b,a^2),$$

so C_0 is a hamiltonian cycle in $\mathrm{Cay}(\overline{G};S)$. Then C_0 contains the four subpaths

$$(b^{-1}),\ [b^{-1}a^2](a^{-1},b,a),\quad [b^{-1}](c^{-1}),\ [b^{-1}c^{-1}a^{-2}](a,c,a^{-1}).$$

Therefore, we may let g be either b^{-1} or $b^{-1}c^{-1}$ in Lemma 3.1, so Remark 3.2(2) tells us we have hamiltonian cycles

$$C^b=(a,b^{-1},a^{-1},c^{-1},a^2,c,b,a)$$

and

$$C^c=(b^{-1},a^{-1},c^{-1},a^2,c,b,a^2),$$

such that $(\Pi C_0)^{-1}(\Pi C^b)$ is a generator of $\mathbb{Z}_p$, and $(\Pi C_0)^{-1}(\Pi C^c)$ is a generator of $\mathbb{Z}_q$. Furthermore, C^c contains the oriented paths $[ab^{-1}](b)$ and $[a^{-1}](a,b^{-1},a^{-1})$, so, by letting $g=a$ in Lemma 3.1 (and replacing b with b^{-1}), Remark 3.2(2) tells us we have a hamiltonian cycle

$$C_b^c=(a^2,b^{-1},c^{-1},a^2,c,a^{-1},b),$$

such that $(\Pi C^c)^{-1}(\Pi C_b^c)$ is a generator of $\mathbb{Z}_p$. Therefore Marušič's Method 2.11(2) applies (since all four of these hamiltonian cycles contain the oriented edge $[b^{-1}c^{-1}](a)$). □

Case 5.11. Assume $\mathbb{Z}_{p^\mu}\subseteq\langle[a,b]\rangle$, $\mathbb{Z}_{q^\nu}\subseteq\langle[a,c]\rangle$, $\overline{c}\in\langle\overline{a}\rangle$, and $\overline{b}\notin\langle\overline{a}\rangle$.

Proof. We use Marušič's Method (2.10), so there is no harm in assuming $S=\{a,b,c\}$. Furthermore, Lemma 2.8 allows us to assume $G'=\mathbb{Z}_{pq}$, so $\langle[a,b]\rangle=\mathbb{Z}_p$ and $\langle[a,c]\rangle=\mathbb{Z}_q$. Also note that, from Assumption 5.1(5), we know $\overline{c}\notin\{\overline{a}^{\pm1}\}$, so we must have $|\overline{a}|>3$.

Let $d=|\overline{G}/\langle\overline{a}\rangle|$. Since $\overline{c}\in\langle\overline{a}\rangle$, we have $\langle\overline{a},\overline{b}\rangle=\overline{G}$, so (b^d) is a hamiltonian cycle in $\mathrm{Cay}(\overline{G}/\langle\overline{a}\rangle;S)$. Choose r such that $a^rb^d\in G'$ and $0\le r\le|\overline{a}|-1$. Assume $r<|\overline{a}|/2$ (so $r\le|\overline{a}|-3$), by replacing b with its inverse if necessary. Then letting $k=|\overline{a}|-3$ in Corollary 3.3 provides us with a hamiltonian cycle $C^0=C_{|\overline{a}|-3}$.

Choose ℓ with $\overline{c}=\overline{a}^\ell$, and write $c=a^\ell\gamma$, where $\mathbb{Z}_q\subseteq\langle\gamma\rangle$. We may assume $0\le\ell<|\overline{a}|/2$ (by replacing c with its inverse, if necessary). Then $\ell\le|\overline{a}|-3$, so we see from Figure 2 that $C_{|\overline{a}|-3}$ contains the path $[a^\ell b](a^{-(\ell+1)})$. Replacing this with the path $[a^\ell b](c^{-1},a^{\ell-1},c^{-1})$ results in a hamiltonian cycle C^1, such that $(\Pi C^0)^{-1}(\Pi C^1)$ is a conjugate of

$$c^{-1}a^{\ell-1}c^{-1}\cdot a^{\ell+1}=(a^\ell\gamma)^{-1}a^{\ell-1}(a^\ell\gamma)^{-1}\cdot a^{\ell+1}=\gamma^{-1}(\gamma^{-1})^a.$$

Since $|G|$ is odd, we know that a does not invert any nontrivial element of G', so this is a generator of $\langle\gamma\rangle$, which contains $\langle[a,c]\rangle=\mathbb{Z}_q$.

Furthermore, from Figure 2, we see that $C_{|\overline{a}|-3}$ contains both the oriented edge $[b^{-1}a^{-1}](b)$ and the oriented path $[b^{-1}a](a^{-1},b,a)$. Then, by construction, C^1 also contains these paths. Therefore, we may apply Lemma 3.1 with $g=b^{-1}a^{-1}$, so Remark 3.2(1)

tells us we have hamiltonian cycles $\widehat{C}^0$ and $\widehat{C}^1$, such that $(\Pi C^i)^{-1}(\Pi\widehat{C}^i)$ is a generator of $\mathbb{Z}_p$. Therefore Marušič's Method 2.11(2) applies (since there are many oriented edges, such as $[a^{-1}](a^{-1})$, that are in all four hamiltonian cycles). □

Case 5.12. Assume there do not exist $a, b, c \in S$, such that $\langle [a,b],[a,c]\rangle = G'$.

Proof. Let $\underline{G} = G/(G')^{pq}$, so $\underline{G'} = \mathbb{Z}_{pq}$. The assumption of this case implies that we may partition S into two nonempty sets S_p and S_q, such that

- $\underline{S_p}$ centralizes $\underline{S_q}$ in $\underline{G}$, and
- for $r \in \{p,q\}$, and $a, b \in S_r$, we have $[\underline{a},\underline{b}] \in \underline{\mathbb{Z}_r}$.

Let $G_p = \langle S_p\rangle$, $G_q = \langle S_q\rangle$, and $Z = \underline{G_p} \cap \underline{G_q} \subseteq Z(\underline{G})$.

Since $\underline{G}$ is not nilpotent (see Assumption 5.1(4)), we know that $\underline{G'} \not\subseteq Z(\underline{G})$. Therefore, we may assume $\mathbb{Z}_q \not\subseteq Z(\underline{G})$ (by interchanging p and q if necessary). Since $\underline{G_p} \cap \underline{G_q} \subseteq Z(\underline{G})$, this implies $\mathbb{Z}_q \not\subseteq \underline{G_p}$.

Subcase i. *Assume there exist $a_p, b_p, a_q, b_q \in S$, such that $\langle [\underline{a_p},\underline{b_p}]\rangle = \underline{\mathbb{Z}_p}$, $\langle [\underline{a_q},\underline{b_q}]\rangle = \underline{\mathbb{Z}_q}$, and $\{b_p, b_q\}$ is a minimal generating set of $\langle \overline{a_p}, \overline{b_p}, \overline{a_q}, \overline{b_q}\rangle / \langle \overline{a_p}, \overline{a_q}\rangle$.* We use Marušič's Method (2.10) with $S_0 = \{a_p, b_p, a_q, b_q\}$. Assume, for simplicity, that $S = S_0$. Lemma 2.8 allows us to assume $G' = \mathbb{Z}_{pq}$, so $G = \underline{G}$.

After perhaps replacing some generators with their inverses, it is easy to find:

- a hamiltonian cycle $(s_i)_{i=1}^m$ in $\mathrm{Cay}\big(\langle \overline{a_p}, \overline{a_q}\rangle; a_p, a_q\big)$, such that $s_{m-2} = a_p$ and $s_{m-1} = a_q$, and
- a hamiltonian cycle $(t_j)_{j=1}^n$ in $\mathrm{Cay}\big(\overline{G}/\langle \overline{a_p}, \overline{a_q}\rangle; b_p, b_q\big)$, such that $t_1 = b_p$ and $t_3 = b_q$.

We have the following hamiltonian cycle C_0 in $\mathrm{Cay}(G; S)$:

$$C_0 = \Big(\big((s_i)_{i=1}^{n-2}, t_{2j-1}, (s_{n-1-i}^{-1})_{i-1}^{n-2}, t_{2j}\big)_{j=1}^{(m-1)/2}, (s_i)_{i=1}^{n-1}, (t_{m-j}^{-1})_{j=1}^{m-1}, s_n \Big).$$

Much as in the proof of Lemma 3.1, we construct a hamiltonian cycle C_1 by

- replacing the oriented edge $[s_m^{-1}b_p](b_p^{-1})$ with the path $[s_m^{-1}b_p](a_q^{-1}, b_p^{-1}, a_q)$, and
- the oriented path $[s_m^{-1}a_q^{-1}a_p^{-1}](a_p, b_p, a_p^{-1})$ with $[s_m^{-1}a_q^{-1}a_p^{-1}](b_p)$.

Then there exist $g, h \in G$, such that

$$(\Pi C_0)^{-1}(\Pi C_1) = [b_p^{-1}, a_q]^g\,[a_p^{-1}, b_p]^h = e^g \cdot [a_p^{-1}, b_p]^h = [a_p^{-1}, b_p]^h,$$

which generates $\mathbb{Z}_p$.

Similarly, we may construct hamiltonian cycles C_0' and C_1' from C_0 and C_1 by

- replacing the oriented edge $[s_m^{-1}t_1t_2b_q](b_q^{-1})$ with the path $[s_m^{-1}t_1t_2b_q](a_q^{-1}, b_q^{-1}, a_q)$, and
- the oriented path $[s_m^{-1}a_q^{-1}a_p^{-1}t_1t_2](a_p, b_q, a_p^{-1})$ with $[s_m^{-1}a_q^{-1}a_p^{-1}t_1t_2](b_q)$.

Then, for $k \in \{0,1\}$, essentially the same calculation shows there exist $g', h' \in G$, such that

$$(\Pi C_k)^{-1}(\Pi C'_k) = [b_q^{-1}, a_q]^{g'}[a_p^{-1}, b_q]^{h'} = [b_q^{-1}, a_q]^{g'} \cdot e^{h'} = [b_q^{-1}, a_q]^{g'},$$

which generates $\mathbb{Z}_q$.

All four hamiltonian cycles contain the oriented edge (s_1), so Marušič's Method 2.11(2) applies.

Subcase ii. *Assume $\underline{G_p}$ is not the nonabelian group of order* 27 *and exponent* 3. We will apply Marušič's Method (2.11), so Lemma 2.8 allows us to assume $G' = \mathbb{Z}_{pq}$, which means $\underline{G} = G$.

Claim. We may assume $S_q \cap (G'Z) = \emptyset$. Suppose $a_q \in S_q \cap (G'Z)$. By the minimality of S, we know $a_q \notin G_p$. Since Z and $\mathbb{Z}_p$ are contained in G_p, this implies $G' \subseteq \langle G_p, a_q\rangle$. Therefore, the minimality of S implies that $S_q \smallsetminus \{a_q\}$ is a minimal generating set of $\overline{G}/\langle \overline{G_p}, \overline{a_q}\rangle$. So Subcase i applies. This completes the proof of the claim.

Now, applying Proposition 4.2 to G_q tells us there exist hamiltonian cycles C_q and C'_q in $\mathrm{Cay}\big(\overline{G_q}/\overline{Z}; S_q\big)$, such that C_q and C'_q have an oriented edge in common, and $\langle (\Pi C_q)^{-1}(\Pi C'_q)\rangle = \mathbb{Z}_q$.

Also, Theorem 4.1 provides hamiltonian cycles C_p and C'_p in $\mathrm{Cay}\big(\overline{G_p}; S_p\big)$, such that C_p and C'_p have an oriented edge in common, and $\langle (\Pi C_p)^{-1}(\Pi C'_p)\rangle = \mathbb{Z}_p$.

For $r \in \{p,q\}$, write $C_r = (s_{r,i})_{i=1}^{n_r}$ and $C'_r = (t_{r,i})_{i=1}^{n_r}$. Since C_r and C'_r have an edge in common, we may assume $s_{r,n_r} = t_{r,n_r}$.

Let

$$C = \Big((s_{p,i})_{i=1}^{n_p-1}, (s_{q,i})_{i=1}^{n_q-1}, \big(s_{p,n_p-2i+1}^{-1}, (s_{q,n_q-j}^{-1})_{j=1}^{n_q-2}, s_{p,n_p-2i}^{-1}, (s_{q,j})_{j=2}^{n_q-1}\big)_{i=1}^{(n_p-1)/2}, s_{q,n_q}\Big). \quad (5.12A)$$

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

For $r \in \{p,q\}$, a path of the form $[g](s_{r,i})_{i=1}^{n_r-1}$ appears near the start of C. We obtain a new hamiltonian cycle C^r in $\mathrm{Cay}\big(\overline{G}; S\big)$ by replacing this with $[g](t_{r,i})_{i=1}^{n_r-1}$. We can also construct a hamiltonian cycle $C^{p,q}$ by making both replacements. Then

$$\langle (\Pi C)^{-1}(\Pi C^r)\rangle = \langle (\Pi C_r)^{-1}(\Pi C'_r)\rangle = \mathbb{Z}_r,$$

and

$$\langle (\Pi C^q)^{-1}(\Pi C^{p,q})\rangle = \langle (\Pi C_p)^{-1}(\Pi C'_p)\rangle = \mathbb{Z}_p,$$

so Marušič's Method 2.11(2) applies (since all four hamiltonian cycles contain the oriented edge $[s_{q,n_q}^{-1}](s_{q,n_q})$).

Subcase iii. *Assume $\underline{G_p}$ is the nonabelian group of order* 27 *and exponent* 3. We have $p = 3$, and Lemma 2.21(1) tells us $\mu = 1$; i.e., $G' = \mathbb{Z}_3 \times \mathbb{Z}_{q^\nu}$. Therefore $\underline{G} = G/(G')^q$.

Let $C_p = (s_{p,i})_{i=1}^{27}$ be a hamiltonian cycle in $\mathrm{Cay}\big(\underline{G_p}; S_p\big)$. Also, for $r = q$, Theorem 4.1 provides hamiltonian cycles $C_q = (s_{q,i})_{i=1}^{n_q}$ and $C'_q = (t_{q,i})_{i=1}^{n_q}$ in $\mathrm{Cay}(\overline{G_q}; S_q)$, such that $s_{q,n_q} = t_{q,n_q}$ and $(\Pi C_q)^{-1}(\Pi C'_q)$ generates $\mathbb{Z}_{q^\nu}$. Define the hamiltonian cycle C as in (5.12A) (with $n_p = 27$). We obtain a new hamiltonian cycle C^q in $\mathrm{Cay}\big(\overline{G}; S\big)$ by

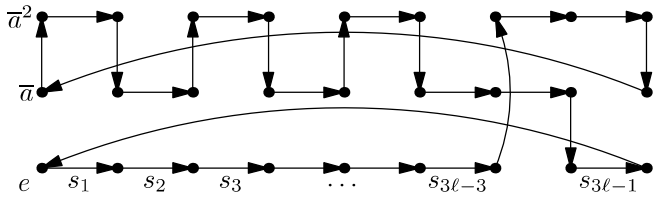

Figure 5: A hamiltonian cycle C_0.

replacing an occurrence of $(s_{q,i})_{i=1}^{n_q-1}$ with the path $(t_{q,i})_{i=1}^{n_q-1}$. Much as in Subcase ii, we have

$$\langle(\underline{\Pi C})^{-1}(\underline{\Pi C^q})\rangle = \langle(\underline{\Pi C_q})^{-1}(\underline{\Pi C'_q})\rangle = \underline{\mathbb{Z}_q},$$

so $\underline{\Pi C}$ and $\underline{\Pi C^q}$ cannot both be trivial. Therefore, applying the Factor Group Lemma (2.7) with $N = \mathbb{Z}_q$ provides a hamiltonian cycle in $\mathrm{Cay}(\underline{G}; S)$, and then Lemma 2.8 tells us there is a hamiltonian cycle in $\mathrm{Cay}(G; S)$. □

6 Proof of Case 5.5

In this section, we prove Case 5.5. Therefore, the following assumption is always in effect:

Assumption 6.1. Assume there exist $a, b \in S$, such that $\langle[a, b]\rangle = G'$, $|\overline{a}| = |\overline{b}| = 3$, and $\langle\overline{a}\rangle \neq \langle\overline{b}\rangle$.

The proof will consider two cases.

Case I. Assume $\#S > 2$.

Proof. Let c be a third element of S, and let $\ell = |\overline{G} : \langle\overline{a}, \overline{b}\rangle|$. (Since S is a minimal generating set, and $G' = \langle[a, b]\rangle \subseteq \langle a, b\rangle$, we must have $\ell > 1$.) We use Marušič's Method (2.10) with $S_0 = \{a, b, c\}$; assume, for simplicity, that $S = S_0$. Lemma 2.8 allows us to assume $G' = \mathbb{Z}_{pq}$. Let

$$(s_i)_{i=1}^{3\ell} = \big((b, c, b^{-1}, c)^{(\ell-1)/2}, b^2, c^{-(\ell-1)}, b\big),$$

so $(s_i)_{i=1}^{3\ell}$ is a hamiltonian cycle in $\mathrm{Cay}\big(\overline{G}/\langle\overline{a}\rangle; b, c\big)$. Note that

$$s_1 = s_5 = b.$$

From the definition of $(s_i)_{i=1}^{3\ell}$, it is easy to see that $\overline{\prod_{i=1}^{3\ell} s_i} = \overline{b}^3 = \overline{e}$, so we have the following hamiltonian cycle C_0 in $\mathrm{Cay}(\overline{G}; a, b, c)$ (see Figure 5):

$$C_0 = \big((s_j)_{j=1}^{3\ell-3}, a^{-1}, s_{3\ell-2}, s_{3\ell-1}, a^{-1}, s_{3\ell},$$
$$(a, s_{2j-1}, a^{-1}, s_{2j})_{j=1}^{3(\ell-1)/2}, s_{3\ell-2}, a^{-1}, s_{3\ell-1}, s_{3\ell}\big).$$

Since $s_1 = b$, we see that C_0 contains the oriented edge (b), and it also contains the oriented path $[a^{-2}](a, b, a^{-1})$, so Lemma 3.1 provides a hamiltonian cycle C_1, such that

$$(\Pi C_0)^{-1}(\Pi C_1) \text{ is a conjugate of } [a, b^{-1}][a, b^{-1}]^a.$$

Similarly, since $s_5 = b$ and $s_1s_2s_3s_4 = c^2$, we see that C_1 contains both the oriented edge $[c^2](b)$ and the oriented path $[c^2a^{-2}](a, b, a^{-1})$, so Lemma 3.1 provides a hamiltonian cycle C_2, such that

$$(\Pi C_1)^{-1}(\Pi C_2) \text{ is also a conjugate of } [a, b^{-1}][a, b^{-1}]^a.$$

Since no element of G inverts any nontrivial element of G' (recall that $|G|$ is odd), this implies that $(\Pi C_i)^{-1}(\Pi C_j)$ generates G' whenever $i \neq j$. So Marušič's Method 2.11(1) applies (since all three hamiltonian cycles contain the oriented edge $[s_1](s_2)$). □

Case II. Assume $\#S = 2$.

Proof. We have $S = \{a, b\}$, so $|G| = 9p^\mu q^\nu$. We may assume $p, q > 3$, for otherwise Corollary 2.15 applies (perhaps after interchanging p and q).

One very special case with a lengthy proof will be covered separately:

Assumption 6.2. Assume Proposition 6.4 below does not provide a hamiltonian cycle in $\mathrm{Cay}(G; S)$.

Under this assumption, we will always use the Factor Group Lemma (2.7) with $N = G'$, so Lemma 2.8 allows us to assume $G' = \mathbb{Z}_{pq}$.

Let

$$C = (a^{-2}, b^{-1}, a, b^{-1}, a^{-2}, b^2),$$

so C is a hamiltonian cycle in $\mathrm{Cay}(\overline{G}; a, b)$. We have

$$\Pi C = a^{-2}b^{-1}ab^{-1}a^{-2}b^2 = [a, b]^a[a, b][a, b]^b(a^{-3})^{b^2}. \tag{6.2A}$$

Let $\underline{G} = G/\mathbb{Z}_p$, so $\underline{G'} = \mathbb{Z}_q$. Since $p, q > 3$, we know $\gcd\big(|\overline{G}|, |G'|\big) = 1$, so $G \cong \overline{G} \ltimes G'$ [7, Thm. 6.2.1(i)]. Therefore $G' \cap Z(G)$ is trivial, so we may

$$\text{assume that } a \text{ does not centralize } \mathbb{Z}_q$$

(perhaps after interchanging a with b). Therefore a acts on $\mathbb{Z}_q$ via a nontrivial cube root of unity. Since the nontrivial cube roots of unity are the roots of the polynomial $x^2 + x + 1$, this implies that $\underline{[a, b]^{a^2}[a, b]^a[a, b]} = \underline{e}$, so

$$\underline{[a, b]^a[a, b]} = (\underline{[a, b]^{a^2}})^{-1} = (\underline{[a, b]^{a^{-1}}})^{-1}$$

(since $|\overline{a}| = 3$). Furthermore, $\underline{a^{-3}} = \underline{e}$ (since a has trivial centralizer in $\mathbb{Z}_q$). Hence,

$$\begin{aligned}\underline{\Pi C} &= \underline{[a, b]^a}\ \underline{[a, b]}\ \underline{[a, b]^b}(\underline{a}^{-3})^{b^2} \\ &= (\underline{[a, b]^{a^{-1}}})^{-1}\ \underline{[a, b]^b}\ \underline{e} \\ &= (\underline{[a, b]^{a^{-1}}})^{-1}\ \underline{[a, b]^b}.\end{aligned}$$

Therefore

$$\underline{\Pi C} \neq \underline{e} \text{ unless } y^b = y^{a^{-1}} \text{ for all } y \in \mathbb{Z}_q. \tag{6.2B}$$

Hence, we may assume $\langle \Pi C \rangle$ contains $\mathbb{Z}_q$ (by replacing b with its inverse if necessary).

Subcase i. *Assume a centralizes $\mathbb{Z}_p$.* Since $G' \cap Z(G)$ is trivial, we know that b does not centralize $\mathbb{Z}_p$. Also, we may assume $\langle \Pi C \rangle \neq G'$, for otherwise the Factor Group Lemma (2.7) applies. Therefore ΠC must project trivially to $\mathbb{Z}_p$. Fixing $r, k \in \mathbb{Z}$ with

$$[a,b]^b = [a,b]^r \text{ and } a^{-3} = [a,b]^k$$

(and using the fact that $r^2 + r + 1 \equiv 0 \pmod{p}$), we see from (6.2A) that this means

$$0 \equiv 1 + 1 + r + kr^2 \equiv 1 - r^2 + kr^2 \equiv r^2(r - 1 + k) \pmod{p},$$

so

$$k \equiv 1 - r \pmod{p}.$$

Therefore $k \not\equiv 0 \pmod{p}$ (since r is a primitive cube root of unity). Also, since a centralizes $\mathbb{Z}_p$, we have

$$[a^{-1}, b^{-1}]^{-kr} \equiv \big([a, b^{-1}]^{-1}\big)^{-kr} = \big([a,b]^{b^{-1}}\big)^{-kr} = [a,b]^{-k} = a^3 = (a^{-1})^{-3} \pmod{\mathbb{Z}_q}.$$

Therefore, replacing a and b with their inverses replaces k with $-kr$ (modulo p), and it obviously replaces r with r^2. Hence, we may assume that we also have

$$-kr \equiv 1 - r^2 \equiv r^3 - r^2 = -(1 - r)r^2 \equiv -kr^2 \pmod{p},$$

so $r \equiv 1 \pmod{p}$. This contradicts the fact that b does not centralize $\mathbb{Z}_p$.

Subcase ii. *Assume a does not centralize $\mathbb{Z}_p$.* We may assume that the preceding subcase does not apply when a and b are interchanged (and perhaps p and q are also interchanged). Therefore, we may assume that either

- b centralizes both $\mathbb{Z}_p$ and $\mathbb{Z}_q$, in which case, interchanging p and q in (6.2B) tells us that ΠC projects nontrivially to both $\mathbb{Z}_p$ and $\mathbb{Z}_q$, so the Factor Group Lemma (2.7) applies, or
- b has trivial centralizer in G'.

Henceforth, we assume a and b both have trivial centralizer in G'.

We may assume $y^b = y^a$ for $y \in \mathbb{Z}_q$, by replacing b with its inverse if necessary. We may also assume $\langle \Pi C \rangle \neq G'$ (for otherwise the Factor Group Lemma (2.7) applies). Since $\langle \Pi C \rangle$ contains $\mathbb{Z}_q$, this means that $\langle \Pi C \rangle$ does not contain $\mathbb{Z}_p$. By interchanging p and q in (6.2B), we conclude that $x^b = x^{a^{-1}}$ for $x \in \mathbb{Z}_p$. We are now in the situation where a hamiltonian cycle in $\mathrm{Cay}(G; a, b)$ is provided by Proposition 6.4 below. □

The remainder of this section proves Proposition 6.4, by applying the Factor Group Lemma (2.7) with $N = \mathbb{Z}_{q^\nu}$. To this end, the following lemma provides a hamiltonian cycle in $\mathrm{Cay}\big(G/\mathbb{Z}_{q^\nu}; S\big)$.

Lemma 6.3. Assume

- $G = \mathbb{Z}_{p^\mu} \rtimes (\mathbb{Z}_3 \times \mathbb{Z}_3) = \langle x \rangle \rtimes \big(\langle a \rangle \times \langle b_0 \rangle\big)$, with $p > 3$,
- $b = xb_0$,

- $x^b = x^{a^{-1}} = x^r$, where r is a primitive cube root of unity in $\mathbb{Z}_{p^\mu}$,
- $k \in \mathbb{Z}$, such that
  - $k \equiv 1 \pmod 3$,
  - $k \equiv r \pmod{p^\mu}$, and
  - $0 \le k < 3p^\mu$,
- ℓ is the multiplicative inverse of k, modulo $3p^\mu$ (and $0 \le \ell < 3p^\mu$),
- $C = \big(a, b^{-2}, (a^{-1}, b^2)^{k-1}, a^{-2}, b^2, (a, b^{-2})^{\ell-k-1}, a^{-2}, (b^{-2}, a)^{3p^\mu-\ell-1}\big)$, and
- $\widetilde{C}$ is the walk obtained from C by interchanging a and b, and also interchanging k and ℓ.

Then either C or $\widetilde{C}$ is a hamiltonian cycle in $\mathrm{Cay}(G; a, b)$.

Proof. Define

$$\begin{aligned} v_{2i+\epsilon} &= (ba)^i b^\epsilon && \text{for } \epsilon \in \{0, 1\}, \\ w_j &= (ba)^j b^{-1}, \end{aligned}$$

and let $V = \{v_i\}$ and $W = \{w_j\}$. Note that, since $x^{ab} = x$, we have $|ab| = 3p^\mu$, so $\#V = 6p^\mu$ and $\#W = 3p^\mu$, so G is the disjoint union of V and W. With this in mind, it is easy to see that $C_1 = (b^{-2}, a)^{3p^\mu}$ is a hamiltonian cycle in $\mathrm{Cay}(G; a, b)$.

Removing the edges of the subpaths (b^{-2}) and $[(ba)^k](b^{-2}, a, b^{-2})$ from C_1 results in two paths:

- path P_1 from $b^{-2} = b$ to $(ba)^k$, and
- path P_2 from $(ba)^{k+1}b$ to e (since $(ba)^k(b^{-2}ab^{-2}) = (ba)^k(bab) = (ba)^{k+1}b$).

The union of P_1 and P_2 covers all the vertices of G *except* the interior vertices of the removed subpaths, namely,

$$\text{all vertices except } b^{-1},\ (ba)^k b^{-1},\ (ba)^k b,\ (ba)^{k+1},\ \text{and } (ba)^{k+1}b^{-1}.$$

By ignoring y in calculation (6.4A) below, we see that $b^{-1}a^{-1} = (a^{-1}b^{-1})^k$, which means

$$ab = (ba)^k.$$

Since $b^{-2} = b$, this implies

$$ab^{-2} = (ba)^k.$$

Also, since $a^{-1} = a^2$, we have

$$ba^{-1}b^2 = ba^2b^2 = (ba)(ab)b = (ba)\big((ba)^k\big)b = (ba)^{k+1}b.$$

Therefore

$$Q_1 = (a, b^{-2}) \text{ is a path from the end of } P_2 \text{ to the end of } P_1,$$

and

$$Q_2 = [b](a^{-1}, b^2) \text{ is a path from the start of } P_1 \text{ to the start of } P_2.$$

So, letting $-P_1$ be the reverse of the walk P_1, we see that

$$C_2 = Q_1 \cup -P_1 \cup Q_2 \cup P_2$$

is a closed walk.

Note that the interior vertices of Q_1 are

$$a = (ab)b^{-1} = (ba)^k b^{-1}$$

and

$$ab^{-1} = (ab)b = (ba)^k b,$$

and the interior vertices of Q_2 are

$$ba^{-1} = ba^2 = (ba)(ab)b^{-1} = (ba)(ba)^k b^{-1} = (ba)^{k+1}b^{-1}$$

and

$$ba^{-1}b = \big((ba)^{k+1}b^{-1}\big)b = (ba)^{k+1}.$$

These are all but one of the vertices that are not in the union of P_1 and P_2, so

$$C_2 \text{ is a cycle that covers every vertex except } b^{-1}.$$

Notice that the only a-edge removed from C_1 is $[(ba)^k b^{-2}](a) = [(ba)^k b](a)$. Since

$$k^2 \equiv (r^2)^2 = r^4 \equiv r \not\equiv 1 \pmod{p^\mu},$$

and ℓ is the multiplicative inverse of k, modulo $3p^\mu$, we know $k \neq \ell$, so this removed edge is not equal to $[(ba)^\ell b](a)$. Therefore $[(ba)^\ell b](a)$ is an edge of C_2. Now, we create a walk C^* by removing this edge from C_2, and replacing it with the path $[(ba)^\ell b](a^{-2})$. Since

$$(ab)^\ell = \big((ba)^k\big)^\ell = (ba)^{k\ell} = ba,$$

we see that the interior vertex of this path is

$$[(ba)^\ell b]a^{-1} = [b(ab)^\ell]a^{-1} = [b(ba)]a^{-1} = b^2 = b^{-1}.$$

Therefore C^* covers every vertex, so it is a hamiltonian cycle.

Since $ab = (ba)^k$ and $ba = (ab)^\ell$, it is obvious that interchanging a and b will also interchange k and ℓ. Therefore, we may assume $k < \ell$, by interchanging a and b if necessary. Then the edge $[(ba)^\ell b](a)$ is in P_2, rather than being in P_1. If we let P_2' be the path obtained by removing this edge from P_2, and replacing it with $[(ba)^\ell b](a^{-2})$, then we have

$$\begin{aligned} C &= \big((a, b^{-2}),\ \ (a^{-1}, b^2)^{k-1}, a^{-1},\ \ (a^{-1}, b^2),\ \ (a, b^{-2})^{\ell-k-1}, a^{-2}, (b^{-2}, a)^{3p^\mu-\ell-1} \big) \\ &= Q_1 \cup -P_1 \cup Q_2 \cup P_2' \\ &= C^* \end{aligned}$$

is a hamiltonian cycle in $\mathrm{Cay}(G; a, b)$. □

Proposition 6.4. Assume

- $\overline{G} \cong \mathbb{Z}_3 \times \mathbb{Z}_3$,

- $G' = \mathbb{Z}_{p^\mu} \times \mathbb{Z}_{q^\nu}$, with $p \neq q$ and $p, q > 3$,
- $S = \{a, b\}$ has only two elements,
- a and b have trivial centralizer in G', and
- ab centralizes $\mathbb{Z}_{p^\mu}$ and ab^{-1} centralizes $\mathbb{Z}_{q^\nu}$.

Then $\mathrm{Cay}(G; a, b)$ has a hamiltonian cycle.

Proof. Since $\gcd\big(|\overline{G}|, |G'|\big) = 1$, we have

$$G \cong G' \rtimes \overline{G} \cong (\mathbb{Z}_{p^\mu} \times \mathbb{Z}_{q^\nu}) \rtimes (\mathbb{Z}_3 \times \mathbb{Z}_3).$$

Write $\mathbb{Z}_{p^\mu} = \langle x \rangle$ and $\mathbb{Z}_{q^\nu} = \langle y \rangle$. Since a does not centralize any nontrivial element of G', we may assume $a \in \mathbb{Z}_3 \times \mathbb{Z}_3$ (after replacing it by a conjugate). Write $b = \gamma b_0$, with $\gamma \in G'$ and $b_0 \in \mathbb{Z}_3 \times \mathbb{Z}_3$. Since $\langle a, b \rangle = G$, we must have $\langle \gamma \rangle = G'$, so we may assume $\gamma = xy$; therefore $b = xyb_0$.

Choose $r \in \mathbb{Z}$ with $x^{a^{-1}} = x^r$. Since $|a| = 3$ and a does not centralize any nontrivial element of $\mathbb{Z}_{p^\mu}$, we know that r is a primitive cube root of unity, modulo p^μ. Also, since ab centralizes $\mathbb{Z}_{p^\mu}$, we have $x^b = x^r$.

Define k and ℓ as in Lemma 6.3. Then, letting $\underline{G} = G/\mathbb{Z}_{q^\nu}$ (and perhaps interchanging a with b), Lemma 6.3 tells us that

$$C = \big(a, b^{-2}, (a^{-1}, b^2)^{k-1}, a^{-2}, b^2, (a, b^{-2})^{\ell-k-1}, a^{-2}, (b^{-2}, a)^{3p^\mu-\ell-1}\big)$$

is a hamiltonian cycle in $\mathrm{Cay}\big(\underline{G}; a, b\big)$.

To calculate the voltage of C, choose $s \in \mathbb{Z}$ with $y^a = y^s$, and let

$$y_1 = y^{s^2-(1+s+s^2+\cdots+s^{k-1})} = y^{s^2-1}$$

(since $1 + s + s^2 \equiv 0 \pmod q$ and $k \equiv 1 \pmod 3$), and note that

$$\begin{aligned}
(a^{-1}b^{-1})^k &= \big(a^{-1}(xyb_0)^{-1}\big)^k && (6.4A)\\
&= \big(a^{-1}b_0^{-1}y^{-1}x^{-1}\big)^k \\
&= x^{-k}\big(a^{-1}b_0^{-1}y^{-1}\big)^k && (x \text{ commutes with } a^{-1}b_0^{-1} \text{ and } y)\\
&= x^{-r}\big(a^{-1}b_0^{-1}\big)^k y^{-(1+s+s^2+\cdots+s^{k-1})} && \left(\begin{array}{c} k \equiv r \pmod{p^\mu} \text{ and} \\ y^{a^{-1}b_0^{-1}} = y^{a^2b_0^2} = y^{s^4} = y^s \end{array}\right)\\
&= x^{-r}b_0^{-1}a^{-1}y^{-s^2}y_1 && \left(\begin{array}{c} a \text{ and } b_0 \text{ commute, } k \equiv 1 \\ \pmod 3, \text{ and definition of } y_1 \end{array}\right)\\
&= b_0^{-1}x^{-1}y^{-1}a^{-1}y_1 && (x^r = x^{b_0} \text{ and } y^{s^2} = y^{a^2} = y^{a^{-1}})\\
&= b^{-1}a^{-1}y^{s^2-1} && (b = xyb_0 \text{ and } y_1 = y^{s^2-1}).
\end{aligned}$$

Therefore

$$\begin{aligned}
\Pi C &= ab^{-2}(a^{-1}b^2)^{k-1}a^{-2}b^2(ab^{-2})^{\ell-k-1}a^{-2}(b^{-2}a)^{3p^\mu-\ell-1} \\
&= ab(a^{-1}b^{-1})^{k-1}ab\big(b(ab)^{\ell-k-1}a\big)(ba)^{3p^\mu-\ell-1} && (|a|=|b|=3) \\
&= ab(a^{-1}b^{-1})^{k}(a^{-1}b^{-1})^{-1}ab\big(ba\big)^{\ell-k}(ba)^{-\ell-1} && (|ba|=3p^\mu) \\
&= ab(a^{-1}b^{-1})^{k}(ba)ab(ba)^{-k}(ba)^{-1} \\
&= ab\big(b^{-1}a^{-1}y^{s^2-1}\big)ba^2b\big(b^{-1}a^{-1}y^{s^2-1}\big)(a^{-1}b^{-1}) && \left(\begin{array}{r}(ba)^{-k}=(a^{-1}b^{-1})^k \\ =b^{-1}a^{-1}y^{s^2-1}\end{array}\right) \\
&= y^{s^2-1}bay^{s^2-1}a^{-1}b^{-1} \\
&= y^{s^2-1}y^{(s^2-1)s} && \left(\begin{array}{r}y^{a^{-1}b^{-1}}=y^{a^2b^2} \\ =y^{s^4}=y^s\end{array}\right) \\
&= y^{(s^2-1)(1+s)}.
\end{aligned}$$

Since s is a primitive cube root of unity modulo q^ν, we know $s \not\equiv \pm 1 \pmod q$. Therefore, the exponent of y is not divisible by q, which means $\Pi C \notin \langle y^q \rangle$, so ΠC generates $\mathbb{Z}_{q^\nu}$. Hence, the Factor Group Lemma (2.7) provides the desired hamiltonian cycle in $\mathrm{Cay}(G; a, b)$. □

References

[1] B. Alspach, Lifting Hamilton cycles of quotient graphs, *Discrete Math.* **78** (1989), 25–36. MR 1020643

[2] S. J. Curran and J. A. Gallian, Hamiltonian cycles and paths in Cayley graphs and digraphs—a survey, *Discrete Math.* **156** (1996), 1–18. MR 1405010

[3] 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. MR 0708162

[4] E. Durnberger, Every connected Cayley graph of a group with prime order commutator group has a Hamilton cycle, in: B. Alspach, C. Godsil (eds.), *Cycles in Graphs (Burnaby, B.C., 1982),* North-Holland, Amsterdam, 1985, 75–80. MR 0821506

[5] E. Ghaderpour and D. W. Morris, Cayley graphs of order $27p$ are hamiltonian, *Internat. J. Comb.* **2011** (2011), Article ID 206930, 16 pages. MR 2822405

[6] E. Ghaderpour and D. W. Morris, Cayley graphs on nilpotent groups with cyclic commutator subgroup are hamiltonian, *Ars Contemp. Math.* **7** (2014), 55–72. MR 3029452

[7] D. Gorenstein, *Finite Groups,* Chelsea, New York, 1980. MR 0569209

[8] M. J. Hall, *The Theory of Groups,* Macmillan, New York, 1959. MR 0103215

[9] B. Huppert, *Endliche Gruppen I,* Springer, Berlin, 1967. MR 0224703

[10] K. Keating and D. Witte, On Hamilton cycles in Cayley graphs with cyclic commutator subgroup, in: B. R. Alspach, C. D. Godsil (eds.), *Cycles in Graphs (Burnaby, B.C., 1982)*, North-Holland, Amsterdam, 1985, 89–102. MR 0821508

[11] K. Kutnar, D. Marušič, J. Morris, D. W. Morris, and P. Šparl, Hamiltonian cycles in Cayley graphs whose order has few prime factors, *Ars Math. Contemp.* **5** (2012), 27–71. MR 2853700

[12] D. Marušič, Hamiltonian circuits in Cayley graphs, *Discrete Math.* **46** (1983), 49–54. MR 0708161

[13] I. Pak and R. Radoičić, Hamiltonian paths in Cayley graphs, *Discrete Math.* **309** (2009), 5501–5508. MR 2548568

[14] D. Witte, Cayley digraphs of prime-power order are Hamiltonian, *J. Combin. Theory Ser. B* **40** (1986), 107–112. MR 0830597

[15] D. Witte and J. A. Gallian, A survey: Hamiltonian cycles in Cayley graphs, *Discrete Math.* **51** (1984), 293–304. MR 0762322