Contributions to Discrete Mathematics

Volume 20, Number 2, Pages 311–336
ISSN 1715-0868

CAYLEY GRAPHS OF ORDER $8pq$ ARE HAMILTONIAN

FATEME ABEDI, DAVE WITTE MORRIS, JAVANSHIR REZAEE,
AND M. REZA SALARIAN

Abstract. We give a computer-assisted proof that if G is a finite group of order $8pq$, where p and q are distinct primes, then every connected Cayley graph on G has a hamiltonian cycle.

1. Introduction

Numerous papers show that all connected Cayley graphs of certain orders are hamiltonian. (See Eq. (2.2) for a definition of the term "Cayley graph.") Several of these results are collected in the following theorem, which is an updated version of [12, Thm. 1.2].

Theorem 1.1 (cf. [14, Thm. 1.2])**.** *If G is a finite group with $|G| > 2$, and $|G|$ has any of the following forms (where p, q, r and s are distinct primes, and k is a positive integer), then every connected Cayley graph on G has a hamiltonian cycle:*

(1) kp, *where* $k \leq 47$,
(2) kpq, *where* $k \leq 7$ *or* $k = 9$,
(3) pqr,
(4) $pqrs$ *if* p, q, r *and* s *are odd,*
(5) kp^2, *where* $k \leq 4$,
(6) kp^3, *where* $k \leq 2$,
(7) p^k.

Remark 1.2. The introduction of [14] provides a list of the papers that were combined to make Eq. (1.1), except that it does not have references for the two parts of the equation that do not appear in [14]'s statement of the result: see [16, Cor. 1.5] for the case $k = 9$ of part (2), and see [18] for part (4). A more detailed (but outdated, and therefore incomplete) explanation of the contribution from each paper is in [12, §2A].

The purpose of this paper is to add the case $k = 8$ to part (2) of the equation:

Received by the editors April 25, 2023, and in revised form February 26, 2024.
2010 *Mathematics Subject Classification.* 05C25, 05C45.
Key words and phrases. Cayley graphs, hamiltonian cycles.
The project of Reza Salarian, leading to this publication, has received funding from the European Research Council (ERC) under the European Union's Horizon 2020 research and innovation program (grant agreement No 741420).

Theorem 1.3. *If p and q are distinct primes, then every connected Cayley graph of order $8pq$ has a hamiltonian cycle.*

Remark 1.4. This means that part (2) of Eq. (1.1) can be replaced with:

(2′) kpq, where $k \leq 9$.

The proof of Eq. (1.3) relies on an exhaustive case-by-case analysis, like most other parts of Eq. (1.1). However, although almost all parts of that equation were proved by hand (so some of the papers are long and complicated — see, for example, the proof of the case $k = 6$ of part (2) of the equation in [14]), we will use a computer-assisted approach that is adapted from the method that was used to complete part (1) of the equation in [19]. Equation (2.11) is the main tool. See Section 3A for an explanation of the technique.

Here is an outline of the paper.

- Section 2 consists of preliminaries on several topics: hamiltonian cycles in Cayley graphs, the Factor Group Lemma, generalized dihedral groups, elementary number theory, and group theory.
- Section 3 describes how we use a computer to find hamiltonian cycles.
- Section 4 spells out assumptions and notation that will be in effect for all later sections of the paper.
- Sections 5 and 6 deal with two cases that cannot be handled by our computer programs. (However, Section 5 does use a computer program in the final subsubcase of the proof of Eq. (5.1).)
- Section 7 proves Eq. (1.3).

2. Preliminaries

Notation 2.1. G is always a finite group.

2A. Some basic results on hamiltonian cycles in Cayley graphs.

Definition 2.2 (cf. [5, p. 34])**.** Let S be a subset of G. The *Cayley graph* $\mathrm{Cay}(G; S)$ is the graph whose vertices are the elements of G, such that there is an edge joining two vertices g and h if and only if $h = gs$ for some $s \in S \cup S^{-1}$ (where $S^{-1} = \{\, s^{-1} \mid s \in S \,\}$.

Remark 2.3 ([19, Rem. 2.2])**.** Unlike most authors, we do not require S to be symmetric (i.e., closed under inverses). Instead, in our notation, $\mathrm{Cay}(G; S) = \mathrm{Cay}(G; S \cup S^{-1})$.

Theorem 2.4 ([13, Problem 12.17, pp. 89 and 505–506], [11], [17])**.** *Assume $|G| > 2$. Every connected Cayley graph on G has a hamiltonian cycle if any of the following are true:*

(1) *G is abelian (in other words, the commutator subgroup of G is trivial), or*
(2) *the commutator subgroup of G is a cyclic p-group, for some prime p, or*

(3) *the commutator subgroup of G has order $2p$, where p is an odd prime.*

The following elementary observation is well-known (and was used in the proofs of almost all parts of Eq. (1.1)). (A generating set S of a group G is *irredundant* if no proper subset of S generates G, so the result follows easily from the fact that every hamiltonian cycle of a spanning subgraph is a hamiltonian cycle of the ambient graph.) When proving that all connected Cayley graphs on a group G are hamiltonian, it allows us to consider only the Cayley graphs of generating sets that are irredundant.

Lemma 2.5. *If there is a hamiltonian cycle in the Cayley graph of every* irredundant *generating set of G, then every connected Cayley graph on G has a hamiltonian cycle.*

The following observation is also well-known.

Lemma 2.6 ([12, Lem. 2.27])**.** *Let S generate G and let $s \in S$, such that $\langle s \rangle \trianglelefteq G$. If*

- $\mathrm{Cay}(G/\langle s \rangle; S)$ *has a hamiltonian cycle, and*
- *either*
  (1) *$s \in Z(G)$, or*
  (2) *$Z(G) \cap \langle s \rangle = 1$, or*
  (3) *$|s|$ is prime,*

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

A slight modification of the proof of part (2) of the equation establishes the following generalization:

Lemma 2.7. *Let S generate G and let $s \in S$, such that $\langle s \rangle \trianglelefteq G$. If*

- $\mathrm{Cay}(G/\langle s \rangle; S)$ *has a hamiltonian cycle,*
- *$Z(G) \cap \langle s \rangle$ is a direct factor of $\langle s \rangle$, and*
- *$|Z(G) \cap \langle s \rangle|$ is a divisor of $|G : \langle s \rangle|$,*

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

2B. **Factor Group Lemma.** Because of the following equation, it is very useful to be able to lift hamiltonian cycles from a quotient graph to the original Cayley graph. Equation (2.11) is a fundamental result that often makes this possible.

Remark 2.8. Suppose N is any nontrivial, proper, normal subgroup of G, such that $|G/N| > 2$. By Eq. (1.1)(1,2), we know that every connected Cayley graph on G/N has a hamiltonian cycle.

Notation 2.9 (cf., e.g., [14, §2.1])**.** For $s_1, s_2, ..., s_n \in S \cup S^{-1}$:

- $(s_1, s_2, s_3, ..., s_n)$ denotes the walk in $\mathrm{Cay}(G; S)$ that visits (in order) the vertices

$$1,\ s_1,\ s_1s_2,\ s_1s_2s_3,\ ...,\ s_1s_2...s_n.$$

- $(s_1, s_2, s_3, ..., s_n)^k$ denotes the walk that is obtained from the concatenation of k copies of $(s_1, s_2, s_3, ..., s_n)$, and
- $(s_1, s_2, s_3, ..., s_n)\#$ denotes the walk $(s_1, s_2, s_3..., s_{n-1})$ that is obtained by deleting the last term of the sequence.

Definition 2.10 (cf. [6, §2.1.3, p. 61])**.** Suppose N is a normal subgroup of a group G and let $C = (s_1, s_2, ..., s_n)$ be a walk in $\mathrm{Cay}(G; S)$. If the walk $(s_1N, s_2N, ..., s_nN)$ in $\mathrm{Cay}(G/N; SN/N)$ is closed, then its *voltage* is the product $\mathbb{V}(C) = s_1s_2...s_n$. This is an element of N.

Lemma 2.11 (Factor Group Lemma [21, §2.2])**.** *Suppose that*

- *S is a generating set of G,*
- *N is a cyclic normal subgroup of G,*
- *$(s_1N, ..., s_nN)$ is a hamiltonian cycle in $\mathrm{Cay}(G/N; S)$, and*
- *the product $s_1s_2...s_n$ generates N.*

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

Corollary 2.12 ([12, Cor. 2.11])**.** *Suppose that*

- *N is a cyclic, normal subgroup of G, such that $|N|$ is prime,*
- *S is an irredundant generating set of G,*
- *there is a hamiltonian cycle in $\mathrm{Cay}(G/N; S)$, and*
- *$s \equiv t \pmod N$ for some $s, t \in S \cup S^{-1}$ with $s \neq t$.*

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

Notation 2.13.

(1) $[g, h] = g^{-1}h^{-1}gh$ is the *commutator* of two elements g and h of G.
(2) $G' = \langle\, [g, h] \mid g, h \in G \,\rangle$ is the *commutator subgroup* of G.
(3) We use $\mathcal{C}_n$ to denote a (multiplicative) cyclic group of order n.

Lemma 2.14 ([14, Cor. 2.14])**.** *If $G = \langle s, t\rangle$, G' is cyclic, and $\gcd\big(k, |G|\big) = 1$, then $G' = \langle [s^k, t]\rangle$.*

Corollary 2.15. *Assume G' is cyclic and $G/G' \cong \mathcal{C}_2 \times \mathcal{C}_2$. If S is any 2-element generating set of G, then $\mathrm{Cay}(G; S)$ has a hamiltonian cycle.*

Proof. Write $S = \{s, t\}$. Then (s^{-1}, t^{-1}, s, t) is a hamiltonian cycle in $\mathrm{Cay}(G/G'; S)$ whose voltage is $s^{-1}t^{-1}st = [s, t]$. This generates G' (by Eq. (2.14) with $k = 1$), so Eq. (2.11) applies. □

2C. **Generalized dihedral groups.**

Notation 2.16 (cf. [1, Defn. 1.2])**.** We use D_{2n} to denote the dihedral group of order $2n$. That is,

$$D_{2n} = \left\langle f, x \mid f^2 = x^n = 1, fxf = x^{-1} \right\rangle.$$

(In [1], this group is called D_n, instead of D_{2n}, but that is not consistent with the notation used in GAP [7].)

Definition 2.17 ([1, Defn. 1.3])**.** A group G is a *generalized dihedral group* if it has

- an abelian subgroup A of index 2, and
- an element f of order 2 (with $f \notin A$),

such that f inverts every element of A (i.e., $faf = a^{-1}$ for all $a \in A$).

Thus, dihedral groups are the generalized dihedral groups in which A is cyclic.

Theorem 2.18 (Alspach, Chen, and Dean [1, Thm. 1.8])**.** *If G is a generalized dihedral group, and $|G|$ is divisible by 4, then every connected Cayley graph on G has a hamiltonian cycle.*

Remark 2.19.

(1) We only need the special case of Eq. (2.18) in which the valency of the graph is 3, which is much easier (cf. [3]).
(2) Alspach, Chen, and Dean [1] actually proved not only that there is a hamiltonian cycle, but that the Cayley graph is hamiltonian connected (or hamiltonian laceable if it is bipartite), if the valency is at least 3.

2D. **Elementary number theory.** We will use the following two very easy and elementary observations:

Lemma 2.20. *If p and q are prime numbers, and there exist $i, j \in \{0, 1, 2\}$, such that*

$$2^i p - 1 \equiv 0 \pmod{q} \quad \textit{and} \quad 2^j q - 1 \equiv 0 \pmod{p},$$

then $\min(p, q) \leq 5$.

Proof. Write $2^i p - 1 = kq$ and $2^j q - 1 = \ell p$. Then

(2.21)
$$0 \equiv \ell k q = \ell(2^i p - 1) = 2^i \ell p - \ell = 2^i(2^j q - 1) - \ell \equiv -(2^i + \ell) \pmod{q}.$$

Assuming, without loss of generality, that $q < p$, we also have

$$\ell p = 2^j q - 1 < 2^j p \leq 4p,$$

so $\ell \leq 4$. Since $i \leq 2$, we also have $2^i \leq 4$, so $2^i + \ell \leq 8$. So (2.21) implies $q \leq 7$.

This obviously implies

$$p \leq 2^2 q - 1 \leq 2^2 \cdot 7 - 1 = 27.$$

Therefore, it is easy to see by exhaustive search that

$$(p, q) \in \{(3, 2), (7, 2), (5, 3), (11, 3), (19, 5)\}.$$

By inspection, we conclude that $\min(p, q) \leq 5$, as desired. □

Lemma 2.22. *Assume $p, q > 3$ are distinct prime numbers. If $x, a_1, a_2, a_3 \in \mathbb{Z}$, such that $\gcd(a_i, pq) = 1$ for all i, then there is a subset I of $\{1, 2, 3\}$ (possibly empty), such that $x + \sum_{i \in I} a_i$ is relatively prime to pq.*

Proof. Note that:

- If $\gcd(x, pq) = 1$, then we may let $I = \emptyset$.
- If $x \equiv 0 \pmod{pq}$, then we may let $I = \{1\}$.

Therefore, we may assume (after interchanging p and q, if necessary) that $\gcd(x, pq) = p$.

Now, for all i, we have

$$x + a_i \equiv 0 + a_i = a_i \not\equiv 0 \pmod{p}.$$

Therefore, if there is some i, such that $x + a_i \not\equiv 0 \pmod{q}$, then we may let $I = \{i\}$. So we may assume, for all i, that

$$a_i \equiv -x \pmod{q}.$$

Since $a_3 \not\equiv 0 \pmod{p}$, we have

$$x + a_1 + a_2 \not\equiv x + a_1 + a_2 + a_3 \pmod{p},$$

so, by letting I be either $\{1, 2\}$ or $\{1, 2, 3\}$, we may arrange that

$$x + \sum_{i \in I} a_i \not\equiv 0 \pmod{p}.$$

Note that we also have

$$x + a_1 + a_2 \equiv x + (-x) + (-x) = -x \not\equiv 0 \pmod{q}$$

and

$$x + a_1 + a_2 + a_3 \equiv x + (-x) + (-x) + (-x) = -2x \not\equiv 0 \pmod{q}.$$

Therefore $x + \sum_{i \in I} a_i$ is relatively prime to pq, as desired. □

Equation (2.12) requires $|N|$ to be prime, but Eq. (2.22) yields the following analogous result that allows the cyclic normal subgroup N to have order pq, which is usually the case in the proof of the main theorem.

Corollary 2.23. *Suppose that*

- *$p, q > 3$ are two distinct prime numbers,*
- *N is a cyclic, normal subgroup of G, such that $|N| = pq$,*
- *S is a generating set of G,*
- *$C = (s_1, s_2, \ldots, s_n)$ is a hamiltonian cycle in $\mathrm{Cay}(G/N; S)$,*
- *$\langle s^{-1}t \rangle = N$ for some $s, t \in S \cup S^{-1}$, and*
- *$|\{\, i \mid s_i \in \{s^{\pm 1}\}\,\}| \geq 3$.*

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

Proof. We have $t = sa$, for some $a \in N$, such that $\langle a \rangle = N$. Let $J = \{\, i \mid s_i \in \{s^{\pm 1}\}\,\}$. For each subset I of J, let C_I be the hamiltonian cycle in $\mathrm{Cay}(G/N; S)$ that is obtained by replacing s_i with t, if $s_i = s$ (or by t^{-1}, if $s_i = s^{-1}$), for each $i \in I$. For each $i \in J$, let

$$a_i = \mathbb{V}(C_{\{i\}})\,\mathbb{V}(C^{-1}) = \begin{cases} s_1 s_2 \cdots s_i a (s_1 s_2 \cdots s_i)^{-1} & \text{if } s_i = s, \\ s_1 s_2 \cdots s_{i-1} a^{-1} (s_1 s_2 \cdots s_{i-1})^{-1} & \text{if } s_i = s^{-1}. \end{cases}$$

In either case, a_i is a conjugate of a or a^{-1}, and therefore generates N.

We claim that if $j \in J$ and $I \subseteq J$, such that $j \notin I$, then

$$\mathbb{V}(C_{I\cup\{j\}}) = a_j \cdot \mathbb{V}(C_I).$$

In fact, we only need this fact in the special case where $j < I$ (i.e., $j < i$, for all $i \in I$), so let us prove only this special case. (The general case uses the fact that N is abelian, because it is a cyclic group, but we will not rely on this fact.) For definiteness, let us assume $s_j = s$. (The other case is similar.) Letting $C_I = (s'_1, s'_2, \ldots, s'_n)$, we have

$$\begin{aligned}
\mathbb{V}(C_{I\cup\{j\}}) &= s'_1 s'_2 \cdots s'_j a s'_{j+1} \cdots s'_n \\
&= s'_1 s'_2 \cdots s'_j a (s'_1 s'_2 \cdots s'_j)^{-1} \cdot (s'_1 s'_2 \cdots s'_n) \\
&= s_1 s_2 \cdots s_j a (s_1 s_2 \cdots s_j)^{-1} \cdot (s'_1 s'_2 \cdots s'_n) \qquad (j < I) \\
&= a_j \cdot \mathbb{V}(C_I).
\end{aligned}$$

This completes the proof of the claim.

Letting $x = \mathbb{V}(C)$, repeated application of the claim implies $\mathbb{V}(C_I) = x \prod_{i\in I} a_i$. By identifying N with $\mathbb{Z}_{pq}$ in the natural way, we can now conclude from Eq. (2.22) that there is a subset I of J, such that $\mathbb{V}(C_I)$ generates N. So Eq. (2.11) provides a hamiltonian cycle in $\mathrm{Cay}(G; S)$. □

2E. **Some facts from group theory.**

Proposition 2.24 (Hall's Theorem on solvable groups [8, Thm. 9.3.1(1), p. 141])**.** *If G is a solvable group of order mn, and $\gcd(m, n) = 1$, then G has at least one subgroup of order m.*

Lemma 2.25 (well-known)**.** *If $p, q > 5$ are distinct primes, then every group of order $8pq$ is solvable.*

Proof. Equivalently, we wish to show that no divisor of $8pq$ is the order of a nonabelian simple group. Burnside's 2-prime theorem [8, Thm. 9.3.2, p. 143] tells us that the order of every nonabelian finite simple group is divisible by at least three distinct primes, so it suffices to show that the order of a simple group cannot be $2pq$, $4pq$, or $8pq$. Here are two different ways to establish this.

First proof. It was proved by J. G. Thompson [20, Cor. 4, p. 388] that if the order of a simple group G is divisible by precisely three distinct primes, then $|G|$ is divisible by 2 and 3 (and one other prime). (In fact, there are only eight nonabelian simple groups whose order is divisible by only three distinct primes, and they are listed in [10, Table I, p. 3].) Since $3 \notin \{p, q\}$, this implies that $|G|$ is not a divisor of $8pq$.

Second proof. The conclusion can easily be derived from facts that appear in standard textbooks on group theory. Suppose G is a simple group of order $2^m pq$, with $m \in \{1, 2, 3\}$.

Let P be a Sylow p-subgroup of G. We know from Sylow's Theorem that

- $|G : N_G(P)| \equiv 1 \pmod{p}$, and
- $|G : N_G(P)|$ is a divisor of $|G : P| = 2^m q$.

Furthermore, P is abelian (indeed, it is cyclic of prime order), and Sylow subgroups of a nonabelian simple group cannot be in the centre of their normalizer [8, Thm. 14.3.1, p. 203], so $N_G(P) \neq P$, which means $|G : N_G(P)| \neq 2^m q$.

Suppose $|G : N_G(P)| = 8$. (This will lead to a contradiction.) Since $p > 5$ and $|G : N_G(P)| \equiv 1 \pmod{p}$, this implies $p = 7$. Also, since $|G : N_G(P)| = 8$, we have $|N_G(P)| = pq$. However, since $p, q > 5$ are distinct primes, and $p = 7$, we know that $q > p$. Therefore, any group of order pq that has a normal subgroup of order p must be abelian; thus, we conclude that $N_G(P)$ is abelian. This contradicts the above-mentioned fact that Sylow subgroups of a nonabelian simple group cannot be in the centre of their normalizer.

We can now conclude that

$$2^i q \equiv 1 \pmod{p}, \text{ for some } i \in \{0, 1, 2\}.$$

By the same argument, we also have $2^j p \equiv 1 \pmod{q}$, for some $j \in \{0, 1, 2\}$. So we see from Eq. (2.20) that $\min(p, q) \leq 5$, which contradicts the assumption that $p, q > 5$. □

Remark 2.26. The hypothesis that $p, q > 5$ in Eq. (2.25) can be weakened, because the first proof only requires $p, q > 3$. However, Eq. (4.3) easily handles the case where one of the primes is 5, so this strengthening of Eq. (2.25) would not shorten the proof of our main theorem.

We will use the following fact in the proof of Eq. (2.28), and also in Section 4.

Lemma 2.27 (cf. [8, Thm. 9.4.2, p. 146])**.** *If G is a finite group, and $|G'|$ is square-free, then G' is cyclic.*

Equation (4.7) will place restrictive conditions on G. We conclude our discussion of group theory with a two-part elementary observation about such groups:

Lemma 2.28. *Assume*

- *G is a group of order $8pq$, where p and q are distinct odd primes, and*
- *$G = P_2 \ltimes \mathcal{C}_{pq}$, where $|P_2| = 8$ and $\mathcal{C}_{pq}$ is a cyclic, normal subgroup of order pq that is contained in G'.*

Then:

(1) *$\mathcal{C}_{pq} \cap Z(G)$ is trivial, and*
(2) *if S is a generating set of G, such that $S \cap G' \neq \emptyset$, then $\mathrm{Cay}(G; S)$ has a hamiltonian cycle.*

Proof. (1) This is a standard fact about relatively prime actions, but we provide a short proof. Suppose $\mathcal{C}_{pq} \cap Z(G)$ is nontrivial. We may write $\mathcal{C}_{pq} = \mathcal{C}_p \times \mathcal{C}_q$ (uniquely) where $\mathcal{C}_p$ and $\mathcal{C}_q$ are cyclic subgroups of order p and q, respectively. (Note that $\mathcal{C}_p$ and $\mathcal{C}_q$ are normal subgroups of G, because

every subgroup of a cyclic, normal subgroup is normal.) For definiteness, let us assume that the subgroup $\mathcal{C}_q$ is contained in $Z(G)$. Let $\widehat{G} = G/\mathcal{C}_p \cong P_2 \times \mathcal{C}_q$. It is obvious from this direct-product decomposition that $\mathcal{C}_q \not\subseteq G'$, which contradicts the assumption that $\mathcal{C}_{pq}$ is contained in G'.

(2) Let $s \in S \cap G'$. Since $|P_2| = 8$, we know that $|P_2'| \in \{1, 2\}$. Therefore $|G'|$ is a divisor of $2pq$, so $|G'|$ is square-free, which implies that G' is cyclic (see Eq. (2.27)). Then $\langle s \rangle$ is a subgroup of a cyclic, normal subgroup, so it is normal.

Also note that $|\langle s \rangle|$, like $|G'|$, must be a divisor of $2pq$. This immediately implies that $|G : \langle s \rangle|$ is even (in fact, it is a multiple of 4). By (1), it also implies that $|\langle s \rangle \cap Z(G)| \leq 2$. Therefore, $|\langle s \rangle \cap Z(G)|$ is a divisor of $|G : \langle s \rangle|$. So, by Eq. (2.8), Eq. (2.7) applies. □

3. Using a computer to find hamiltonian cycles

3A. **Using a computer to apply the Factor Group Lemma.** In the proof of the main theorem (1.3), we are given a group G of order $8pq$, and we wish to show that $\mathrm{Cay}(G; S)$ has a hamiltonian cycle, for every irredundant generating set S of G. This is accomplished by an extensive case-by-case analysis. However, as in [15, 19], we will use a computer to do the vast majority of the work.

Remark 3.1. Our computer programs are written in GAP [7]. The source code is available online at

`https://arxiv.org/src/2304.03348/anc/`

but this code relies on some of the programs of Morris–Wilk [19] that are available at

`https://arxiv.org/src/1805.00149/anc/`

So a reader who wishes to reproduce our results should combine all of the `.gap` files from both locations into a single directory.

In most cases, the group G is a semidirect product. More precisely, $G = \overline{G} \ltimes (\mathcal{C}_p \times \mathcal{C}_q)$, where $\overline{G}$ is a subgroup of order 8, and $\mathcal{C}_p$ and $\mathcal{C}_q$ are cyclic, normal subgroups of order p and q, respectively (see Eq. (4.7)). The quotient $G/(\mathcal{C}_p \times \mathcal{C}_q)$ can be naturally identified with $\overline{G}$. By Eq. (2.11), it suffices to find a hamiltonian cycle C in $\mathrm{Cay}(\overline{G}; S)$ whose voltage generates $\mathcal{C}_p \times \mathcal{C}_q$. The graph $\mathrm{Cay}(\overline{G}; S)$ has only 8 vertices, so it is easy to have a computer find all of its hamiltonian cycles, calculate their voltages, and determine whether there is a good one.

The key difficulty is that there are infinitely many possibilities for the primes p and q, but a computer can only do finitely many calculations. A method that addresses this issue can be found in [19, Lem. 3.3]. The idea is to let Z be the subring of $\mathbb{C}$ that is generated by the roots of unity and let μ be the group of all roots of unity. Any semidirect product $\overline{G} \ltimes (\mathcal{C}_p \times \mathcal{C}_q)$ arises from a pair of twist homomorphisms $\zeta_p \colon \overline{G} \to \mathrm{Aut}\, \mathcal{C}_p$ and

$\zeta_q\colon \overline{G} \to \operatorname{Aut}\mathcal{C}_q$. Since $\operatorname{Aut}\mathcal{C}_p$ and $\operatorname{Aut}\mathcal{C}_q$ are cyclic, they can be identified with subgroups of μ. Therefore, ζ_p and ζ_q correspond to homomorphisms $\widehat{\zeta}_p\colon \overline{G} \to \mu$ and $\widehat{\zeta}_q\colon \overline{G} \to \mu$. After constructing the corresponding semidirect products $G_p = \overline{G} \ltimes_{\widehat{\zeta}_p} Z$ and $G_q = \overline{G} \ltimes_{\widehat{\zeta}_q} Z$, a computer program can calculate the voltages π_p and π_q of any hamiltonian cycle C in both of these groups. These voltages are algebraic integers, so they have a "norm," which is an element of $\mathbb{Z}$. It is not difficult to see that if $\operatorname{Norm}\pi_p \not\equiv 0 \pmod{p}$ and $\operatorname{Norm}\pi_q \not\equiv 0 \pmod{q}$, then $\mathbb{V}(C)$ generates $\mathcal{C}_p \times \mathcal{C}_q$ (see the proof of [19, Lem. 3.3], with $n = 1$). Therefore, it suffices to show, for every pair of distinct primes p and q, that there exists a hamiltonian cycle in $\operatorname{Cay}(\overline{G}; S)$, such that $\operatorname{lcm}(\operatorname{Norm}\pi_p, \operatorname{Norm}\pi_q)$ is relatively prime to pq. Actually, by Eq. (4.4), we will only need to consider primes that are greater than 5.

Here is a bit more explanation of how the computer programs work. Write $S = \{s_1, \ldots, s_k\}$, and fix generators x_p and x_q of $\mathcal{C}_p$ and $\mathcal{C}_q$, respectively. Each element s of S can be written uniquely in the form $\overline{s}\, x_p^i\, x_q^j$, with $\overline{s} \in \overline{G}$. Let us say that s *involves* x_p if $x_p^i \neq 0$; similarly, s *involves* x_q if $x_q^j \neq 0$.

Case 1. *The simplest case for computation is when we know that only one element s_m involves x_p, and only one element s_n involves x_q.* (It is possible that $m = n$.) Every nontrivial element of a cyclic group of prime order is a generator, so we may assume $s_m = \overline{s_m}\, x_p$ and $s_n = \overline{s_n}\, x_q$ (unless $m = n$, in which case we have $s_m = s_n = \overline{s_m} x_p x_q$). To consider all possibilities, we have the computer:

- loop through all groups $\overline{G}$ of order 8,
- loop through all generating sets $\overline{S}$ of $\overline{G}$,
- loop through all hamiltonian cycles $\overline{C}$ in $\operatorname{Cay}(\overline{G}; \overline{S})$, and
- loop through all homomorphisms $\zeta_p\colon \overline{G} \to \mu$ and $\zeta_q\colon \overline{G} \to \mu$ (these homomorphisms are called *abelian characters* of $\overline{G}$).

Actually, the program must allow $\overline{S}$ to be a multiset, because two different elements of S may have the same image in $\overline{G}$. (However, we will see in Eq. (7.2) that the cardinality of S is at most 5, so this is still a finite problem.) Then each hamiltonian cycle $\overline{C}$ in $\operatorname{Cay}(\overline{G}; \overline{S})$ may have many different possible lifts to a walk in $\operatorname{Cay}(G; S)$. We refer to these walks as "coded" hamiltonian cycles, because we encode each walk as a sequence of numbers, by making a list of the elements of $S \cup S^{-1}$, and specifying each edge of the walk by recording the index of the corresponding element of the list.

Now, for each coded hamiltonian cycle C in $\operatorname{Cay}(\overline{G}; S)$, the computer calculates the voltages π_p and π_q of the corresponding walks in $\operatorname{Cay}(\overline{G} \ltimes_{\widehat{\zeta}_p} Z; S_p)$ and $\operatorname{Cay}(\overline{G} \ltimes_{\widehat{\zeta}_q} Z; S_q)$, where

- S_p is obtained from $\overline{S}$ by replacing s_m with $s_m x_p$, and
- S_q is obtained from $\overline{S}$ by replacing s_n with $s_n x_q$.

(Here, x_p and x_q are represented by the element $(0,1)$ of $\overline{G} \ltimes_{\widehat{\zeta_p}} Z$ or $\overline{G} \ltimes_{\widehat{\zeta_q}} Z$. However, in order to be consistent with the conventions used in the Morris–Wilk programs, the order of the factors needs to be reversed: to be precise, the programs compute in the groups $Z \rtimes_{\zeta_p} \overline{G}$ and $Z \rtimes_{\zeta_q} \overline{G}$, so x_p and x_q are actually represented by the element $(1,0)$.)

If the computer finds a hamiltonian cycle, such that the least common multiple of $\mathrm{Norm}(\pi_p)$ and $\mathrm{Norm}(\pi_q)$ has no prime divisors greater than 5, then we know that $\mathrm{Cay}(G;S)$ has a hamiltonian cycle for all p and q (greater than 5), so the computer can move on to the next iteration of the loop. On the other hand, the program will raise an error if there is no such hamiltonian cycle. It is important to note that this never happens in our calculations, because all cases where the computer search would fail are handled separately (see Sections 5 and 6).

Case 2. *The situation is more complicated when x_p or x_q may be involved in more than one element of S.* In all cases of the proof, we are able to use theoretical arguments to reduce to a situation where x_p and x_q are not *both* involved in more than one element of S. Therefore, let us assume that

- x_p is involved in only one element of S, but
- x_q is involved in s_1, and may (or may not) be involved in s_2 (and is certainly not involved in any other element of S).

For each coded hamiltonian cycle C, we calculate the voltage π_p of C in $\overline{G} \ltimes_{\widehat{\zeta_p}} Z$, exactly as in Case 1. If no prime divisor of $\mathrm{Norm}\,\pi_p$ is greater than 5, then we know that the voltage of C generates $\mathcal{C}_p$, so checking whether the voltage generates $\mathcal{C}_q$ is the only remaining issue. (On the other hand, if some prime divisor is greater than 5, then we discard this hamiltonian cycle as being useless.)

We deal with the prime q by a different approach that was introduced in [19, Lem. 3.3]. Namely, we calculate the voltage of C in $\overline{G} \ltimes_{\widehat{\zeta_q}} Z$ with respect to two different connection sets $S'_q = \{s'_1, \ldots, s'_k\}$ and $S''_q = \{s''_1, \ldots, s''_k\}$. In S'_q, the generator s'_1 is the only element that involves x_q; in S''_q, it is s''_2 that involves x_q. Let us use $\pi'_q(C)$ and $\pi''_q(C)$ to denote the corresponding voltages (in $\overline{G} \ltimes_{\widehat{\zeta_q}} Z$).

A key observation in the proof of [19, Lem. 3.3] is that there is a homomorphism $\Phi\colon Z \to \mathcal{C}_q$, such that if we write $s_1 = \overline{s_1} x_q$ and $s_2 = \overline{s_2} x_q^i$ (modulo $\mathcal{C}_p$), and let $\pi_q(C)$ be the voltage of C in $\overline{G} \ltimes_{\zeta_q} \mathcal{C}_q$, then

$$\pi_q(C) = \Phi\big(\pi'_q(C)\big) + i\,\Phi\big(\pi''_q(C)\big).$$

In particular, if it happens to be the case that $\pi''_q(C) = 0$, then $\pi_q(C) = \pi'_q(C)$. Therefore, if it is also true that $\mathrm{Norm}\big(\pi'_q(C)\big)$ does not have any prime divisors greater than 5, then $\pi_q(C)$ generates $\mathcal{C}_q$. Since we already know from above that $\pi_p(C)$ generates $\mathcal{C}_p$, this implies that $\mathrm{Cay}(G;S)$ has a hamiltonian cycle. So we can pass to the next iteration of the loop. The program refers to this as finding a "single" hamiltonian cycle.

Another key observation in the proof of [19, Lem. 3.3] is a consequence of undergraduate-level linear algebra: if C_1 and C_2 are two coded hamiltonian cycles, and the norm of

$$\det \begin{bmatrix} \pi'_q(C_1) & \pi''_q(C_1) \\ \pi'_q(C_2) & \pi''_q(C_2) \end{bmatrix}$$

is not divisible by q, then C_1 and C_2 cannot both have trivial voltage in $\overline{G} \ltimes_{\widehat{\zeta_q}} Z$. Hence, Eq. (2.11) applies to at least one of them, so $\mathrm{Cay}(G; S)$ has a hamiltonian cycle. Therefore, when a "single" is not found, the program searches through all pairs of hamiltonian cycles C_1 and C_2, to find a case where the norm of the determinant is not divisible by any prime greater than 5.

Remark 3.2.

(1) We said above that the computer loops through all groups, all generating sets, and all abelian characters, but that is not actually true. Slightly different computer programs were written for different cases of the proof, and each case puts restrictions on the groups, generating sets, or abelian characters that need to be considered.
(2) The programs in 8pq-Prop-4-1.gap, 8pq-Prop-7-4.gap, and 8pq-Prop-7-7.gap use the method of Case 1, but the program in 8pq-Prop-7-9.gap deals with Case 2.

3B. **An anomalous case with $q = 7$.** The programs described in Section 3A assume that G is a semidirect product $\overline{G} \ltimes (\mathcal{C}_p \times \mathcal{C}_q)$, but this is not always the case. In this section, we deal with a situation where that assumption is not true, by using some of the computer programs that accompany the Morris–Wilk paper [19]. As was already mentioned in Eq. (3.1), these programs are online at

`https://arxiv.org/src/1805.00149/anc/`

The programs that are used in this section make extensive use of K. Helsgaun's program LKH [9], which implements a very effective heuristic for finding hamiltonian cycles. (So LKH must also be installed.)

Lemma 3.3 (cf. [19, Rem. 1.4(4)])**.** *If H is the unique nonabelian semidirect product of the form $\mathcal{C}_7 \ltimes (\mathcal{C}_2)^3$, then every connected Cayley graph on G is hamiltonian connected.*

Proof. The Morris–Wilk program 1-3-HamConnOrLaceable.gap verifies that every connected Cayley graph of order less than 64 (and valency at least 3) is either hamiltonian connected or hamiltonian laceable. However, it takes a long time to run, and the official report in [19, Prop. 1.3] only states the result for orders less than 48.

The program loops through all orders from 3 to 63, and loops through all groups of each order. (See [19, §2C] for more explanation.) To quickly prove the case we need, change two lines in the program:

- change `for k in [3..63] do`
  to `for k in [56] do`
- change `for GapId in [1..NumberSmallGroups(k)] do`
  to `for GapId in [11] do`

This modified program will print

```
G = SmallGroup(56,11) = (C2 x C2 x C2) : C7
```

which confirms that the correct group is being considered, then will print a few lines of progress reports, followed by a statement that all of the Cayley graphs are hamiltonian connected or hamiltonian laceable.

However, the group H has no subgroup of index 2, so none of its connected Cayley graphs are bipartite; therefore, none of its connected Cayley graphs are hamiltonian laceable. Hence, all of them must be hamiltonian connected. □

Proposition 3.4. *Let H be the unique nonabelian semidirect product of the form $\mathcal{C}_7 \ltimes (\mathcal{C}_2)^3$. If $G = H \ltimes \mathcal{C}_p$, for some prime $p > 5$, then every connected Cayley graph on G has a hamiltonian cycle.*

Proof. In [19], it is proved that every connected Cayley graph of order kp is hamiltonian when $1 \le k < 48$ (and p is prime). In the current situation, we have $k = 56$, but it is easy to adapt the argument. Actually, we do not need the entire argument, just two short parts of it.

Let S be a generating set of G; we wish to show $\mathrm{Cay}(G; S)$ has a hamiltonian cycle. By Eq. (2.5), we may assume that S is irredundant. Let $\overline{G} = G/\mathcal{C}_p \cong H$.

Case 1. *Assume $\overline{S}$ is a redundant generating set of $\overline{G}$.* This case follows from the proof of [19, Lem. 4.2]. For the reader's convenience, we sketch the argument.

Choose a (proper) subset S_0 of S, such that $\overline{S_0}$ is an irredundant generating set of $\overline{G}$. Since $\overline{S_0}$ generates $\overline{G}$, we know that $|\langle S_0\rangle|$ is divisible by $|\overline{G}| = 56$. However, we also know $\langle S_0\rangle \ne G$, since the generating set S is irredundant. We conclude that $|\langle S_0\rangle| = 56$, so, after passing to a conjugate, $\langle S_0\rangle = H$.

Since $|G|/|\overline{G} = p$ is prime, it is easy to see that $|S| = |S_0| + 1$; hence, we have $S = S_0 \cup \{a\}$ for some $a \in S$. By Eq. (2.6)(3), we may assume $\overline{a}$ is nontrivial. Therefore Eq. (3.3) provides a hamiltonian path $(\overline{s_1}, \ldots, \overline{s_{55}})$ from $\overline{1}$ to $\overline{a^{-1}}$ in $\mathrm{Cay}(\overline{G}; \overline{S_0})$. Then

$$C = (\overline{s_1}, \ldots, \overline{s_{55}}, \overline{a})$$

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

Write $a = hz$ with $h \in H$ and $z \in \mathcal{C}_p$. Since $\langle S_0, h\rangle = H \ne G$, it must be the case that z is nontrivial. Since $\mathcal{C}_p$ has prime order, this implies that z generates $\mathcal{C}_p$. The voltage of the hamiltonian cycle is

$$\mathbb{V}(C) = s_1 s_2 \cdots s_{55} a = s_1 s_2 \cdots s_{55} hz.$$

However, since

$$\overline{s_1 s_2 \cdots s_{55} h} = \overline{s_1 s_2 \cdots s_{55} a} = \overline{1}$$

and $s_1 s_2 \cdots s_{55} h \in H$, we must have $s_1 s_2 \cdots s_{55} h = 1$. Therefore $\mathbb{V}(C) = z$ generates $\mathcal{C}_p$. So Eq. (2.11) applies.

Case 2. *Assume $\overline{S}$ is an irredundant generating set of $\overline{G}$.* For every nontrivial group H of order less than 48, the Morris–Wilk program 3-4-IrredundantSBar.gap verifies that if

- p is a prime number,
- G is any semidirect product $H \ltimes \mathcal{C}_p$, and
- S is any irredundant generating set of G, such that the projection of S to H is an irredundant generating set,

then $\mathrm{Cay}(G; S)$ has a hamiltonian cycle. It does this by looping through all orders from 1 to 47, then looping through all possible groups of each order.

This computer program can easily be modified to consider the case here. Instead of looping through all groups of many different orders, we just want to look at a single group of order 56. As in the proof of Eq. (3.3), it suffices to change two lines in the program. Specifically:

- change `for k in [1..47] do`
  to `for k in [56] do`
- change `for GapId in [1..NumberSmallGroups(k)] do`
  to `for GapId in [11] do`

The modified program should take less than a minute to run. Since it completes successfully, rather than raising an error, we conclude that $\mathrm{Cay}(G; S)$ has a hamiltonian cycle. □

4. Assumptions and notation

This short section establishes that we may make some simplifying assumptions when proving the main theorem (1.3). All later sections will make use of the assumptions and notation that are introduced here.

Notation 4.1. Let G be a finite group, such that

$$|G| = 8pq \text{ where } p \text{ and } q \text{ are distinct prime numbers,}$$

and let S be a generating set of G.

To prove Eq. (1.3), we wish to show that $\mathrm{Cay}(G; S)$ has a hamiltonian cycle. By Eq. (2.5), the following causes no loss of generality:

Assumption 4.2. The generating set S is irredundant.

We first consider the case where (at least) one of the primes is small:

Lemma 4.3. *If $\min(p, q) \leq 5$, then every connected Cayley graph on G has a hamiltonian cycle.*

Proof. Assume, without loss of generality, that $\min(p, q) = q$, so $q \leq 5$. Then $8q < 48$, so Eq. (1.1)(1) applies with $k = 8q$. □

In view of this equation, we henceforth make the following assumption:

Assumption 4.4. $\min(p, q) > 5$.

With these assumptions, the following result is an easy (but crucial!) consequence of Eq. (2.25).

Proposition 4.5. *One of the following is true: either*

(1) $G = P_2 \ltimes H$, *where* P_2 *is a Sylow* 2*-subgroup* (*so* $|P_2| = 8$) *and* H *is a normal subgroup of order* pq, *or*
(2) *the assumptions of Eq.* (3.4) *are satisfied* (*perhaps after interchanging* p *and* q), *so every connected Cayley graph on* G *has a hamiltonian cycle.*

Proof. This is a standard argument. Let P_2 be a Sylow 2-subgroup of G. The group G is solvable (see Eq. (2.25)), so Eq. (2.24) tells us there is a subgroup H of order pq. Assume, without loss of generality, that $p > q$, and let P be a Sylow p-subgroup of H. Then it is easy to see from Sylow's Theorem (and is well-known [8, p. 49]) that P is a normal subgroup of H, so $H \subseteq N_G(P)$. Hence, if we let n_p be the number of Sylow p-subgroups of G, then (by Sylow's Theorem) we see that

$$n_p = |G : N_G(P)| \text{ is a divisor of } |G : H| = 8, \text{ so } n_p \in \{1, 2, 4, 8\}.$$

However, we also know from Sylow's Theorem that $n_p \equiv 1 \pmod{p}$. Since $p > q > 5$, we have $p > 7$, so we can conclude that $n_p = 1$. This means that P is the unique Sylow p-subgroup of G, so P is a normal subgroup of G.

Now H/P is a Sylow q-subgroup of G/P. If $H/P \lhd G/P$, then $H \lhd G$, so conclusion (1) holds.

We may therefore assume H/P is not normal, so G/P has more than one Sylow q-subgroup. By Eq. (2.24), we may let K be a subgroup of order $8q$ in G, so $G = K \ltimes P$. Then $K \cong G/P$ has more than one Sylow q-subgroup. Thus, if we let $\mathcal{C}_q$ be a Sylow q-subgroup of K, then $|K : N_K(\mathcal{C}_q)| > 1$. Since $|K : N_K(\mathcal{C}_q)| \leq |K : \mathcal{C}_q| = 8$ (and we know $|K : N_K(\mathcal{C}_q)| \equiv 1 \pmod{q}$ by Sylow's Theorem), we conclude that $q = 7$ and $N_K(\mathcal{C}_q) = \mathcal{C}_q$. So K has a normal q-complement [8, Thm. 14.3.1, p. 203]: $K = \mathcal{C}_q \ltimes P_2$ (after replacing P_2 by a conjugate, so it is contained in K).

The orders of the automorphism groups of $\mathcal{C}_8$, $\mathcal{C}_4 \times \mathcal{C}_2$, $(\mathcal{C}_2)^3$, D_8, and Q_8 are 4, 8, 168, 8, and 24 respectively. Thus, $(\mathcal{C}_2)^3$ is the only group of order 8 that has an automorphism group whose order is divisible by 7. Hence, $\mathcal{C}_7 \ltimes (\mathcal{C}_2)^3$ is the only semidirect product of the form $\mathcal{C}_7 \ltimes P_2$, such that P_2 has order 8 and is not centralized by $\mathcal{C}_7$. So G is as described in Eq. (3.4). □

We may assume it is the condition in part (1) of the equation that is satisfied. Now, $|G/H| = 8$, so $|(G/H)'| \in \{1, 2\}$. Therefore

$$|G'| \text{ is a divisor of } 2pq. \tag{4.6}$$

We may assume $|G'|$ is divisible by pq, for otherwise $|G'|$ is either 1 or prime or twice an odd prime, so Eq. (2.4) applies. This implies $H \subseteq G'$.

On the other hand, (4.6) implies that $|G'|$ is square-free. So G' is cyclic (see Eq. (2.27)). Since subgroups of cyclic groups are cyclic, we conclude that H is cyclic. Hence, the following condition is satisfied:

Assumption 4.7. We have

$$G = P_2 \ltimes \mathcal{C}_{pq},$$

where $|P_2| = 8$, and $\mathcal{C}_{pq}$ is a cyclic, normal subgroup of order pq that is contained in G'.

Notation 4.8. Let:

- $\overline{G} = G/\mathcal{C}_{pq} \cong P_2$,
- $\mathcal{C}_p$ be the subgroup of $\mathcal{C}_{pq}$ that has order p,
- $\mathcal{C}_q$ be the subgroup of $\mathcal{C}_{pq}$ that has order q,
- x_p be a generator of $\mathcal{C}_p$, and
- x_q be a generator of $\mathcal{C}_q$.

Then

$$\mathcal{C}_{pq} = \mathcal{C}_p \times \mathcal{C}_q = \langle x_p \rangle \times \langle x_q \rangle.$$

5. Some cases where $\overline{G} \cong (\mathcal{C}_2)^3$

Proposition 5.1. *The assumptions and notation of Section 4 are in effect. Also assume $\overline{G} \cong (\mathcal{C}_2)^3$, and either*

(1) $|S| = 3$, *or*
(2) $|S| = 4$ *and there does not exist a subset S_0 of S, such that $|\langle S_0 \rangle| = 8$.*

Then every connected Cayley graph on G has a hamiltonian cycle.

Proof. For convenience, let us recall some terminology from Section 3A for use in this proof. Every element g of G can be written in the form $\overline{g} x_p^i x_q^j$, where $\overline{g} \in P_2$ and $i, j \in \mathbb{Z}$. If x_p^i is nontrivial, we say that g *involves* x_p; similarly, if x_q^j is nontrivial, we say that g *involves* x_q.

Now, we consider each of the two possibilities for $|S|$ as a separate case.

Case 1. *Assume* $|S| = 3$. Write $S = \{a, b, c\}$. We have the following hamiltonian cycle in $\mathrm{Cay}(G/\mathcal{C}_{pq}; S)$:

$$C_{a,b,c} = (a^{-1}, b^{-1}, a, c^{-1}, a^{-1}, b, a, c).$$

Its voltage is

$$\mathbb{V}(C_{a,b,c}) = a^{-1}b^{-1}ac^{-1}a^{-1}bac = (b^a)^{-1}c^{-1}b^a c = [b^a, c],$$

where $b^a = a^{-1}ba$ denotes the *conjugate* of b by a.

Subcase 1.1. *Assume some element of S centralizes $\mathcal{C}_{pq}$.* For definiteness, assume that a centralizes $\mathcal{C}_{pq}$.

- If $|a| = 2$, then $a \in Z(G)$, so Eq. (2.6)(1) applies with $s = a$.
- If $|a| \in \{2p, 2q\}$, then Eq. (2.12) applies with $s = a$, $t = s^{-1}$, and $N = \langle a^2 \rangle$.

So we may assume $|a| = 2pq$. The hamiltonian cycle $C_{a,b,c}$ has 4 occurrences of a or a^{-1}. (In fact, 3 occurrences would be enough.) Therefore, we see from Eq. (2.23) that there is a hamiltonian cycle in $\mathrm{Cay}(G; S)$.

SUBCASE 1.2. *Assume every element of S inverts $\mathcal{C}_{pq}$.* This implies that $G \cong (\mathcal{C}_2)^2 \times D_{2pq}$ is a generalized dihedral group (with $A = (\mathcal{C}_2)^2 \times \mathcal{C}_{pq}$), so a hamiltonian cycle is provided by Eq. (2.18).

SUBCASE 1.3. *Assume two elements of S invert $\mathcal{C}_{pq}$.* For definiteness, let us say that b and c invert $\mathcal{C}_{pq}$ (but a does not, for otherwise Subcase 1.2 applies). We may assume a does not centralize all of $\mathcal{C}_{pq}$ (for otherwise Subcase 1.1 applies), so a inverts $\mathcal{C}_p$ and centralizes $\mathcal{C}_q$ (perhaps after interchanging p and q). Since c has trivial centralizer in $\mathcal{C}_{pq}$, we may conjugate by an element of $\mathcal{C}_{pq}$ to assume c is in $(\mathcal{C}_2)^3$. (So c does not involve x_p or x_q.) We may also assume that a does not involve x_q, for otherwise $|a| = 2q$, so Eq. (2.12) applies with $s = a$, $t = a^{-1}$, and $N = \mathcal{C}_q$. Write $a = e_1 x_p^i$ and $b = e_2 x_p^j x_q$, with $e_1, e_2 \in (\mathcal{C}_2)^3$. Note that e_1, like a, inverts x_p and centralizes x_q, whereas e_2 inverts both x_p and x_q. Therefore

$$b^a = a^{-1}ba = x_p^{-i} e_1 \cdot e_2 x_p^j x_q \cdot e_1 x_p^i = e_2 x_p^{2i-j} x_q,$$

so

$$\mathbb{V}(C_{a,b,c}) = [b^a, c] \text{ generates } \mathcal{C}_{pq} \text{ if and only if } 2i \not\equiv j \pmod{p}.$$

Therefore, we may assume $i = 1$ and $j = 2$, so $a = e_1 x_p$ and $b = e_2 x_p^2 x_q$.

Let $\widehat{G} = G/\mathcal{C}_p \cong \mathcal{C}_2 \times D_{4q}$, where $\langle \widehat{a} \rangle = \mathcal{C}_2 \times \{1\}$ and $\langle \widehat{b}, \widehat{c} \rangle = \{1\} \times D_{4q}$. Then

$$C_1 = \big((b,c)^{2q}\#, a\big)^2$$

is a hamiltonian cycle in $\mathrm{Cay}(\widehat{G}; a, b, c)$. Its voltage is

$$\begin{aligned}
\mathbb{V}(C_1) &= \big((bc)^{2q}\, ca\big)^2 \\
&= \big((e_2 x_p^2 x_q \cdot c)^{2q} \cdot c \cdot e_1 x_p\big)^2 \\
&= \big((e_2 c \cdot x_p^{-2} x_q^{-1})^{2q} \cdot c e_1 \cdot x_p\big)^2 \\
&= \big(x_p^{-4q}\, x_p\big)^2 \big(c e_1\big)^2 \\
&= x_p^{2(1-4q)}.
\end{aligned}$$

Therefore, if $\mathbb{V}(C_1)$ is trivial, then

$$4q \equiv 1 \pmod{p}.$$

Now, let $\breve{G} = G/\mathcal{C}_q \cong \mathcal{C}_2 \times D_{4p}$. We claim that the following is a hamiltonian cycle in $\mathrm{Cay}(\breve{G}; a, b, c)$:

$$C_2 = \big((b,c)^p\#, a, (c,b)^p\#, a\big)^2.$$

In fact, $\breve{G}$ is a generalized dihedral group, with $A = \mathbb{Z}_2 \times \mathbb{Z}_{2p}$, and C_2 is the hamiltonian cycle that is constructed in the proof of [3, Cor. 2.3] for this particular group. However, we provide a short proof for completeness. First,

note that the length $8p$ of this walk is correct for a hamiltonian cycle. Also note that the walk is closed, because, by using the fact that $(\breve{b}\breve{c})^p = (\breve{c}\breve{b})^p$ is an element of order 2 in the centre of $\breve{G}$, we see that

$$(bc)^p c \cdot a \cdot (cb)^p b \cdot a \equiv c \cdot a \cdot b \cdot a \equiv c \cdot e_1 x_p \cdot e_2 x_p^2 \cdot e_1 x_p = e_2 c \equiv (\breve{b}\breve{c})^p \pmod{\mathcal{C}_q}$$

has order 2, modulo $\mathcal{C}_q$. It therefore suffices to show that this cycle passes through all of the vertices of the Cayley graph. Let

$$\mathcal{V} = \{\, (\breve{b}\,\breve{c})^i\, \breve{b}^j \mid 0 \le i < p,\ 0 \le j \le 1 \,\}$$

and

$$\mathcal{W} = \{\, (\breve{c}\,\breve{b})^i\, \breve{c}^j \mid 0 \le i < p,\ 0 \le j \le 1 \,\}.$$

Then C_2 passes through the vertices in

$$\mathcal{V} \ \cup\ (\breve{b}\breve{c})^p\, \breve{c}\breve{a}\, \mathcal{W} \ \cup\ (\breve{b}\,\breve{c})^p\, \mathcal{V} \ \cup\ \breve{c}\breve{a}\, \mathcal{W} \ =\ \langle \breve{b}, \breve{c}\rangle \ \cup\ \breve{c}\breve{a}\langle \breve{b}, \breve{c}\rangle \ =\ \breve{G}.$$

This completes the proof of the claim.

The voltage of this hamiltonian cycle is

$$\begin{aligned}
\mathbb{V}(C_2) &= \big((bc)^p c \cdot a \cdot (cb)^p b \cdot a\big)^2 \\
&\equiv \big((e_2 x_q c)^p c \cdot e_1 \cdot (c e_2 x_q)^p e_2 x_q \cdot e_1\big)^2 \qquad (\mathrm{mod}\ \mathcal{C}_p) \\
&= \big((e_2 c x_q^{-p}) c \cdot e_1 \cdot (c e_2 x_q^p) e_2 x_q \cdot e_1\big)^2 \\
&= (x_q^{1-2p} e_2 c)^2 \\
&= x_q^{2(1-2p)}.
\end{aligned}$$

If this voltage is trivial, then $2p \equiv 1 \pmod{q}$.

By Eq. (2.20), we know that either $4q \not\equiv 1 \pmod{p}$ or $2p \not\equiv 1 \pmod{q}$. So the above calculations show that either $\mathbb{V}(C_1)$ or $\mathbb{V}(C_2)$ is nontrivial. Hence, Eq. (2.11) applies.

Subcase 1.4. *Assume that precisely one element of S inverts $\mathcal{C}_{pq}$.* We may assume it is c that inverts $\mathcal{C}_{pq}$ and (after conjugating by an element of $\mathcal{C}_{pq}$) that c does not involve x_p or x_q. Then a and b each have a nontrivial centralizer in $\mathcal{C}_{pq}$. Note that if a and b both centralize $\mathcal{C}_p$, then we can assume that neither of them involves x_p (otherwise Eq. (2.12) applies with $s \in \{a, b\}$, $t = s^{-1}$, and $N = \mathcal{C}_p$), so no element of S involves x_p, which contradicts the fact that S generates G. Similarly, we can assume that a and b do not both centralize $\mathcal{C}_q$. Hence, we may assume that a centralizes $\mathcal{C}_q$ and b centralizes $\mathcal{C}_p$.

Then we have

$$a = e_1 x_p, \quad b = e_2 x_q, \quad c = e_3,$$

where $\langle e_1, e_2, e_3\rangle = (\mathcal{C}_2)^3$, and:

- e_1 inverts $\mathcal{C}_p$ and centralizes $\mathcal{C}_q$,
- e_2 centralizes $\mathcal{C}_p$ and inverts $\mathcal{C}_q$, and
- e_3 inverts $\mathcal{C}_p$ and $\mathcal{C}_q$.

As in Subcase 1.3, let $\widehat{G} = G/\mathcal{C}_p \cong \mathcal{C}_2 \times D_{4q}$, where $\langle \widehat{a} \rangle = \mathcal{C}_2 \times \{1\}$ and $\langle \widehat{b}, \widehat{c} \rangle = D_{4q}$. Then

$$C_1 = \big((b,c)^{2q}\#, a\big)^2$$

is again a hamiltonian cycle in $\mathrm{Cay}(\widehat{G}; a, b, c)$. Its voltage is

$$\mathbb{V}(C) = \big((bc)^{2q}\, ca\big)^2 = \big(1 \cdot ca\big)^2 = (ca)^2 = (e_3 \cdot e_1 x_p)^2 = (e_3 e_1)^2 x_p^2 = x_p^2 \neq 1.$$

So Eq. (2.11) applies.

Subcase 1.5. *Assume no element of S inverts $\mathcal{C}_{pq}$.* This means that every element of S has a nontrivial centralizer in $\mathcal{C}_{pq}$. However, we also know that $\mathcal{C}_{pq} \cap Z(G) = \{1\}$ (see Eq. (2.28)(1)), which means that no nontrivial subgroup of $\mathcal{C}_{pq}$ is centralized by every element of S. We may also assume that no element of S centralizes all of $\mathcal{C}_{pq}$ (for otherwise Subcase 1.1 applies). Therefore, we may assume a and b centralize $\mathcal{C}_p$, and c centralizes $\mathcal{C}_q$. Then we may also assume that a and b do not involve x_p (otherwise Eq. (2.12) applies with $s \in \{a, b\}$, $t = s^{-1}$, and $N = \mathcal{C}_p$). Conjugating by an element of $\mathcal{C}_p$, we may assume that c also does not involve x_p. Then no element of S involves x_p, which contradicts the fact that S generates G.

Case 2. *Assume $|S| = 4$.* Let S_0 be a 3-element subset of S that generates $G/\mathcal{C}_{pq}$. By Assumption (2) in the statement of the equation, we know that $|\langle S_0 \rangle| \neq 8$; therefore $|\langle S_0 \rangle| = 8p$ (perhaps after interchanging p and q). After conjugating, we may assume $\langle S_0 \rangle = (\mathcal{C}_2)^3 \ltimes \mathcal{C}_p$.

Let a be the fourth element of S, so a is the only element that involves x_q. Also choose $b \in S_0$, such that b does not centralize $\mathcal{C}_q$.

Let $\widehat{G} = G/\mathcal{C}_p = (\mathcal{C}_2)^3 \ltimes \mathcal{C}_q$. Then $\widehat{b} \in (\mathcal{C}_2)^3$, and $\widehat{a} = g x_q$, where $g \in (\mathcal{C}_2)^3$. Note that $\langle \widehat{a}, \widehat{b} \rangle$ is nonabelian, because $\widehat{b}$ commutes with g, but does not commute with x_q. So the commutator subgroup of $\langle \widehat{a}, \widehat{b} \rangle$ is nontrivial, and must therefore be all of $\mathcal{C}_q$. This implies that $\langle \widehat{a}, \widehat{b} \rangle$ contains $\mathcal{C}_q$, so $|\langle a, b \rangle|$ is divisible by q.

Subcase 2.1. *Assume $a \equiv b \pmod{\mathcal{C}_{pq}}$.* We may assume $|ab^{-1}| = pq$, for otherwise Eq. (2.12) applies with $s = a$, $t = b$, and $N = \langle a^{-1}b \rangle \in \{\mathcal{C}_p, \mathcal{C}_q\}$. If we write $S = \{a, b, c, d\}$, then the hamiltonian cycle $C_{a,c,d}$ has 4 occurrences of a or a^{-1}. Therefore, we see from Eq. (2.23) that there is a hamiltonian cycle in $\mathrm{Cay}(G; S)$.

Subcase 2.2. *Assume $a \not\equiv b \pmod{\mathcal{C}_{pq}}$.* Then we may choose an element c of S_0, such that $\{a, b, c\}$ generates $G/\mathcal{C}_{pq}$. So $|\langle a, b, c \rangle| = 8q$. (Recall that $|\langle a, b \rangle|$ is divisible by q.) Since $|\langle S_0 \rangle| = 8p$, we conclude that $|\langle S_0 \rangle \cap \langle a, b, c \rangle| = 8$. Since $b, c \in S_0$, then $|\langle b, c \rangle|$ is a divisor of 8, so, after conjugating by an element of $\mathcal{C}_p$, we may assume $\langle b, c \rangle \subseteq P_2$, which means that b and c do not involve x_p (and we already know that they do not involve x_q).

Subsubcase 2.2.1. *Assume a involves x_p.* Since $|\langle a, b, c \rangle| = 8q$, this implies that b and c centralize $\mathcal{C}_p$. Let d be the other element of S_0. Then

d cannot centralize $\mathcal{C}_p$, so, after conjugating by an element of $\mathcal{C}_p$, we may assume that $d \in P_2$. (This conjugation does not affect b and c, since they centralize $\mathcal{C}_p$.) Now b, c, and d all belong to P_2, so $|\langle S_0\rangle| \leq 8$. This contradicts the fact that $|\langle S_0\rangle| = 8p$.

SUBSUBCASE 2.2.2. *Assume a does not involve x_p.* This implies that $S = \{e_1x_q, e_2, e_3, gx_p\}$, where $\langle e_1, e_2, e_3\rangle = (\mathcal{C}_2)^3$, and g is a nontrivial element of $(\mathcal{C}_2)^3$. In this situation, the GAP computer program in 8pq-Prop-5-1.gap verifies that there is a hamiltonian cycle in $\mathrm{Cay}(\overline{G}; S)$ whose voltage generates $\mathcal{C}_{pq}$, unless (up to isomorphism) the Cayley graph is described in Eq. (5.2) below. □

Lemma 5.2. *Assume*

- $G = (\mathcal{C}_2)^3 \ltimes \mathcal{C}_{pq}$, *and*
- $S = \{e_1x_q, e_2, e_3, e_1e_2x_p\}$, *where* $\langle e_1, e_2, e_3\rangle = (\mathcal{C}_2)^3$, *such that*
  - e_1 *inverts* $\mathcal{C}_p$ *and* $\mathcal{C}_q$, *and*
  - e_2 *and* e_3 *centralize* $\mathcal{C}_p$, *and invert* $\mathcal{C}_q$.

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

Proof. Since e_2 and e_3 have the same action on $\mathcal{C}_{pq}$, we know that $e_2e_3^{-1} \in Z(G)$. Therefore Eq. (2.12) applies with $s = e_2$, $t = e_3$, and $N = \langle e_2e_3^{-1}\rangle \cong \mathcal{C}_2$. □

6. A CASE WHERE $\overline{G} \cong D_8$

Proposition 6.1. *Assume:*

1. $G = D_8 \ltimes \mathcal{C}_{pq}$,
2. $|S| = 3$,
3. $^-\colon G \to D_8$ *is the natural homomorphism with kernel* $\mathcal{C}_{pq}$,
4. $\overline{S} = \{f, fx_4, fx_4^{-1}\}$, *where f is a reflection, and x_4 is a rotation of order* 4,
5. f *centralizes* $\mathcal{C}_p$ *and inverts* $\mathcal{C}_q$,
6. x_4 *inverts* $\mathcal{C}_p$, *and centralizes* $\mathcal{C}_q$, *and*
7. *there does not exist a subset* S_0 *of* S, *such that* $|\langle S_0\rangle| = 8$.

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

Proof. Write $S = \{s, t, u\}$ with $\overline{s} = f$, $\overline{t} = fx_4$, and $\overline{u} = fx_4^{-1}$. Note that:

- s centralizes $\mathcal{C}_p$ and inverts $\mathcal{C}_q$, whereas
- t and u invert $\mathcal{C}_{pq}$.

We have $|t| = |u| = 2$. Since $|\overline{s}| = 2$, we may assume that s also has order 2 (otherwise Eq. (2.12) applies with $t = s^{-1}$ and $N = \mathcal{C}_p$), so we may assume

$$s = f \in D_8.$$

Since s centralizes $\mathcal{C}_p$, we know that $|\langle s, t\rangle|$ and $|\langle s, u\rangle|$ are not divisible by p. So we must have $|\langle s, t\rangle| = |\langle s, u\rangle| = 8q$ (by condition (7) in the statement

of the equation). Conjugating by an element of $\mathcal{C}_p$, we may then assume $\langle s, u\rangle = P_2 \ltimes \mathcal{C}_q$. Thus, we have

$$t = fx_4x_px_q^i \text{ and } u = fx_4^{-1}x_q \text{ for some } i \in \mathbb{Z} \text{ with } i \not\equiv 0 \pmod{q}.$$

Note that $\langle x_4^2\rangle = Z(G)$.

Let

$$\breve{G} = \frac{G}{\langle x_4^2\rangle \times \mathcal{C}_q} = \langle \breve{s}\rangle \times \langle \breve{t}, \breve{u}\rangle \cong \mathcal{C}_2 \times D_{2p},$$

so

$$C_1 = \big((t,u)^{2p}\#, s\big)^2 \quad \text{and} \quad C_2 = \big((u,t)^{2p}\#, s\big)^2$$

are hamiltonian cycles in $\mathrm{Cay}\big(\breve{G}; S\big)$ whose voltages are

$$\begin{aligned}
\mathbb{V}(C_1) &= \big((tu)^{2p}us\big)^2 \\
&= \big((fx_4x_px_q^i \cdot fx_4^{-1}x_q)^{2p} \cdot fx_4^{-1}x_q \cdot f\big)^2 \\
&= \big((x_4^2\, x_p^{-1}\, x_q^{1-i})^{2p}\, x_4x_q^{-1}\big)^2 \\
&= x_4^2\, x_q^{2\left(2p(1-i)-1\right)}
\end{aligned}$$

and

$$\begin{aligned}
\mathbb{V}(C_2) &= \big((ut)^{2p}ts\big)^2 \\
&= \big((fx_4^{-1}x_q \cdot fx_4x_px_q^i)^{2p} \cdot fx_4x_px_q^i \cdot f\big)^2 \\
&= \big((x_4^2\, x_p\, x_q^{i-1})^{2p}\, x_4^{-1}x_px_q^{-i}\big)^2 \\
&= x_4^2\, x_q^{2\left(2p(i-1)-i\right)}.
\end{aligned}$$

This shows that $\langle \mathbb{V}(C)\rangle$ contains $\langle x_4^2\rangle$. Hence, we may assume

$$2p(1-i) - 1 \equiv 0 \pmod{q} \quad \text{and} \quad 2p(i-1) - i \equiv 0 \pmod{q},$$

for otherwise either $\mathbb{V}(C_1)$ or $\mathbb{V}(C_2)$ generates $\langle x_4^2\rangle \times \mathcal{C}_q$, so Eq. (2.11) applies. Adding these two congruence's yields $-(1+i) \equiv 0$, so $i \equiv -1$, which means

$$t = fx_4x_px_q^{-1}.$$

Also, substituting $i = -1$ into the first congruence tells us that

$$4p \equiv 1 \pmod{q}.$$

Now, let $\widehat{G} = G/\mathcal{C}_p$. We have

$$tu = fx_4x_px_q^{-1} \cdot fx_4^{-1}x_q = x_4^2x_p^{-1}x_q^2 \equiv x_4^2x_q^2 \pmod{\mathcal{C}_p},$$

so $|\widehat{t}\,\widehat{u}| = 2q$. Since $|t| = |u| = 2$, this implies that $\langle \widehat{t}, \widehat{u}\rangle$ is isomorphic to D_{4q}, and is a subgroup of index 2 in $\widehat{G}$. Hence, we have the following hamiltonian cycle in $\mathrm{Cay}(\widehat{G}; S)$:

$$C = \big((t,u)^{2q}\#, s, (u,t)^{2q}\#, s\big).$$

(It may not be obvious that the walk C is closed, but that follows from the following calculation of its voltage, which establishes that the terminal vertex of the walk is in $\mathcal{C}_p$.) Its voltage is

$$\begin{aligned}\mathbb{V}(C) &= (tu)^{2q} us (ut)^{2q} ts \\ &= (f x_4 x_p x_q^{-1} \cdot f x_4^{-1} x_q)^{2q} \cdot f x_4^{-1} x_q \cdot f \\ &\qquad \cdot (f x_4^{-1} x_q \cdot f x_4 x_p x_q^{-1})^{2q} \cdot f x_4 x_p x_q^{-1} \cdot f \\ &= (x_4^2 x_p^{-1} x_q^2)^{2q} \cdot x_4 x_q^{-1} \cdot (x_4^2 x_p x_q^{-2})^{2q} \cdot x_4^{-1} x_p x_q \\ &= (x_p^{-2q}) \cdot x_4 x_q^{-1} \cdot (x_p^{2q}) \cdot x_4^{-1} x_p x_q \\ &= x_p^{1-4q}.\end{aligned}$$

We may assume this does not generate $\mathcal{C}_p$ (for otherwise Eq. (2.11) applies). So $4q \equiv 1 \pmod{p}$.

We have shown that $4p \equiv 1 \pmod{q}$ and $4q \equiv 1 \pmod{p}$. This contradicts Eq. (2.20). □

7. Proof of the main theorem

This section proves the main theorem (1.3). As described in Section 3A, most cases are handled by using a computer to do exhaustive case-by-case analysis that finds a hamiltonian cycle in a quotient group of order 8. However, some cases were handled in previous sections (especially Sections 5 and 6), and a small amount of additional work is done by hand in this section.

The assumptions and notation of Section 4 are in effect.

Notation 7.1. Let $d(\overline{G})$ be the cardinality of an irredundant generating set of $\overline{G}$. Since $\overline{G}$ has prime-power order, it is well-known that this is well-defined, independent of the choice of the irredundant generating set (by the Burnside Basis Theorem [8, Thm. 12.2.1, p. 176]). Specifically:

(1) $d(\mathcal{C}_8) = 1$,
(2) $d(\mathcal{C}_4 \times \mathcal{C}_2) = d(D_8) = d(Q_8) = 2$, and
(3) $d(\mathcal{C}_2 \times \mathcal{C}_2 \times \mathcal{C}_2) = 3$

(where $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$ is the quaternion group of order 8).

The following observation is elementary (and well-known):

Lemma 7.2. *We have*

$$d(\overline{G}) \leq |S| \leq d(\overline{G}) + 2.$$

Proof. Since S generates G, it must generate $G/\mathcal{C}_{pq} = \overline{G}$. Therefore, it contains a subset S_0 that is an irredundant generating set of $\overline{G}$. Since $|S_0| = d(\overline{G})$, this establishes that $d(\overline{G}) \leq |S|$.

To establish the other inequality, let $s_1, s_2, \ldots, s_k$ be a list of the elements of S that are not in S_0, so $|S| = d(\overline{G}) + k$. Since S is irredundant, we have

$$\langle S_0 \rangle \subsetneq \langle S_0, s_1 \rangle \subsetneq \langle S_0, s_1, s_2 \rangle \subsetneq \cdots \subsetneq \langle S_0, s_1, s_2, \ldots, s_k \rangle.$$

Thus, if we let

$$m_i = |\langle S_0, s_1, s_2, \ldots, s_i\rangle : \langle S_0, s_1, s_2, \ldots, s_{i-1}\rangle| \quad \text{for } i = 1, 2, \ldots, k,$$

then $m_i > 1$, and

$$m_1 m_2 \cdots m_k = |G : \langle S_0\rangle|.$$

However, since S_0 generates $\overline{G}$, we know that $|\langle S_0\rangle|$ is a multiple of $|\overline{G}| = 8$. Therefore, $|G : \langle S_0\rangle|$ is a divisor of $|G|/8 = pq$, so it cannot be written as a product of more than two nontrivial factors. We conclude that $k \leq 2$. □

We first handle the smallest value of $|S|$ that is consistent with Eq. (7.2):

Proposition 7.3. *If $|S| = d(\overline{G})$, then $\mathrm{Cay}(G; S)$ has a hamiltonian cycle.*

Proof. We know that $|S| \neq 1$ (because Eq. (4.7) implies that G is non-abelian), so $d(\overline{G}) \neq 1$. Also, Eq. (5.1)(1) applies if $|S| = 3$. Therefore, we may assume $d(\overline{G}) = 2$. We may also assume $\overline{G}$ is abelian, for otherwise $G/G' \cong \mathcal{C}_2 \times \mathcal{C}_2$, so Eq. (2.15) applies. Since the only abelian groups of order 8 are $\mathcal{C}_8$, $\mathcal{C}_4 \times \mathcal{C}_2$, and $(\mathcal{C}_2)^3$, we conclude that

$$\overline{G} \cong \mathcal{C}_4 \times \mathcal{C}_2 \text{ (and } |S| = 2).$$

Let $s \in S$, such that $|\overline{s}| = 4$, and let t be the other element of S. Then (s^{-3}, t^{-1}, s^3, t) is a hamiltonian cycle in $\mathrm{Cay}(\overline{G}; S)$. Its voltage is $[s^3, t]$, and, since $\gcd\big(3, |G|\big) = 1$, we know from (see Eq. (2.14)) that $\langle [s^3, t]\rangle = G'$. Therefore Eq. (2.11) applies. □

We now handle the largest possible value of $|S|$:

Proposition 7.4. *If $|S| = d(\overline{G}) + 2$, then $\mathrm{Cay}(G; S)$ has a hamiltonian cycle.*

Proof. Let S_0 be an irredundant generating set of $\overline{G}$ that is contained in S, so $|S_0| = d(\overline{G})$ and $|\langle S_0\rangle|$ is divisible by 8. Then we may assume that the Sylow 2-subgroup P_2 is contained in $|\langle S_0\rangle|$ (after replacing it by a conjugate).

We claim that $\langle S_0\rangle = P_2$, and that we may write $S = S_0 \cup \{ax_p, bx_q\}$, where a and b are elements of P_2. To see this, we argue much as in the proof of Eq. (7.2). Let s and t be the two elements of S that are not in S_0. Since S is irredundant, we know that

$$\langle S_0\rangle \subsetneq \langle S_0, s\rangle \subsetneq G \quad \text{and} \quad \langle S_0\rangle \subsetneq \langle S_0, t\rangle \subsetneq G.$$

On the other hand, any subgroup whose order is divisible by p must contain $\mathcal{C}_p$ (because, being normal, this is the only Sylow p-subgroup of G), and, similarly, any subgroup whose order is divisible by q must contain $\mathcal{C}_q$, so it is easy to see that the only proper subgroups of G that contain P_2 are

$$P_2,\ P_2 \ltimes \mathcal{C}_p, \text{ and } P_2 \ltimes \mathcal{C}_q.$$

We conclude (perhaps after interchanging p and q) that we have

$$\langle S_0\rangle = P_2,\ \langle S_0, s\rangle = P_2 \ltimes \mathcal{C}_p, \text{ and } \langle S_0, t\rangle = P_2 \ltimes \mathcal{C}_q.$$

This completes the proof of the claim.

Running the GAP computer program in 8pq-Prop-7-4.gap verifies in all cases that there is a hamiltonian cycle in $\mathrm{Cay}(\overline{G}; S)$ whose voltage generates $\mathcal{C}_{pq}$, so Eq. (2.11) applies. □

The preceding three results allow us to make the following assumption:

Assumption 7.5. Assume $|S| = d(\overline{G}) + 1$.

Let us now consider three additional special cases.

Lemma 7.6. *Assume* $G = (\mathcal{C}_2)^3 \ltimes \mathcal{C}_{pq}$, *and* $S = \{a, b, c, abx_px_q\}$, *where* $\langle a, b, c\rangle = (\mathcal{C}_2)^3$, *such that*

- a *inverts* $\mathcal{C}_p$ *and centralizes* $\mathcal{C}_q$, *and*
- b *and* c *centralize* $\mathcal{C}_p$ *and invert* $\mathcal{C}_q$.

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

Proof. Let $N = \langle b^{-1}c\rangle$. Since b and c have the same action on G', we know that $b^{-1}c \in Z(G)$, so N is a normal subgroup. Then, since N has order 2 (because it is a nontrivial, cyclic subgroup of $(\mathcal{C}_2)^3$), we see from Eq. (2.12) (with $s = a$ and $t = b$) that $\mathrm{Cay}(G; S)$ is hamiltonian. □

Proposition 7.7. *If* S *contains a subset* S_0, *such that* $|\langle S_0\rangle| = 8$, *then* $\mathrm{Cay}(G; S)$ *has a hamiltonian cycle.*

Proof. Let $P_2 = \langle S_0\rangle$, so P_2 is a Sylow 2-subgroup of G. By Eq. (7.5), we have $S = S_0 \cup \{gx_px_q\}$, for some $g \in P_2$. Also note that we may assume $g \notin P_2'$, for otherwise Eq. (2.28)(2) applies. In this situation, the computer program in 8pq-Prop-7-7.gap establishes that either Eq. (7.6) applies, or there is a hamiltonian cycle in $\mathrm{Cay}(G/\mathcal{C}_{pq}; S)$ whose voltage generates $\mathcal{C}_{pq}$ (so Eq. (2.11) applies). In either case, there is a hamiltonian cycle in $\mathrm{Cay}(G; S)$. □

Corollary 7.8. *If* $d(\overline{G}) = 1$, *then every connected Cayley graph on* G *has a hamiltonian cycle.*

Proof. Let S be an irredundant generating set of G, and let $S_0 \subseteq S$, such that S_0 is an irredundant generating set of $\overline{G}$. Then

$$|S_0| = d(\overline{G}) = 1,$$

so we may write $S_0 = \{s\}$.

Note that $s^8 \in \mathcal{C}_{pq}$ (because $|G/\mathcal{C}_{pq}| = 8$), and also $s \in \langle s\rangle$. Since cyclic groups are abelian, this implies that s^8 is centralized by $\langle \mathcal{C}_{pq}, s\rangle = G$. Since $Z(G) \cap \mathcal{C}_{pq}$ is trivial, we conclude that s^8 is trivial. On the other hand, we know that $|s| \geq 8$, since s generates $\overline{G}$. So we must have $|s| = 8$. Therefore Eq. (7.7) applies. □

Note that:

- if $d(\overline{G}) = 1$, then Eq. (7.8) applies, and
- if $d(\overline{G}) = 3$, then either Eq. (5.1)(2) or Eq. (7.7) applies.

Therefore, the following result completes the proof of the main theorem (1.3).

Proposition 7.9. *If $d(\overline{G}) = 2$, then $\mathrm{Cay}(G; S)$ has a hamiltonian cycle.*

Proof. Since $d(\overline{G}) = 2$, we may let $\{a, b\}$ be an irredundant generating set of $\overline{G}$ that is contained in S. By Eq. (7.5), we know that $S \neq \{a, b\}$, so the fact that S is irredundant implies $\langle a, b\rangle \neq G$. Therefore, we may assume $|\langle a, b\rangle| = 8q$ (perhaps after interchanging p and q), for otherwise Eq. (7.7) applies. So $\langle a, b\rangle = P_2 \ltimes \mathcal{C}_q$ (after passing to a conjugate). Since $\mathcal{C}_q \not\subseteq Z(G)$ (see Eq. (2.28)(1)), we may assume a does not centralize $\mathcal{C}_q$ (perhaps after interchanging a and b). Then, after conjugating by an element of $\mathcal{C}_q$, we may assume $a \in P_2$. Then $b = \overline{b}x_q$, for some $\overline{b} \in P_2$.

Let c be the third element of S. We may write $c = \overline{c}x_p x_q^i$, where $\overline{c} \in P_2$ and $i \in \mathbb{Z}$, and we may assume $c \notin G'$, for otherwise Eq. (2.28)(2) applies.

In this situation, the GAP computer program in 8pq-Prop-7-9.gap establishes that either Eq. (6.1) (or Eq. (7.7)) applies, or there is a hamiltonian cycle in $\mathrm{Cay}(G/\mathcal{C}_{pq}; S)$ whose voltage generates $\mathcal{C}_{pq}$ (so Eq. (2.11) applies). (See Case 2 of Section 3A for an explanation of the basic logic of the program.) In either case, there is a hamiltonian cycle in $\mathrm{Cay}(G; S)$. □

Acknowledgement

We thank an anonymous referee for reading the paper carefully, and providing several helpful comments and corrections.

References

1. B. Alspach, C. C. Chen and M. Dean, *Hamilton paths in Cayley graphs on generalized dihedral groups*, Ars Math. Contemp. **3** (2010) 29–47. MR 2592513, doi:10.26493/1855-3974.101.a37
2. B. Alspach, S. C. Locke, and D. Witte, *The Hamilton spaces of Cayley graphs on abelian groups*, Discrete Math. **82** (1990) 113–126. MR 1057481, doi:10.1016/0012-365X(90)90319-D
3. B. Alspach and C. Q. Zhang, *Hamilton cycles in cubic Cayley graphs on dihedral groups*, Ars Combin. **28** (1989) 101–108. MR 1039136
4. E. Ghaderpour and D. W. Morris, *Cayley graphs on nilpotent groups with cyclic commutator subgroup are hamiltonian*, Ars Math. Contemp. **7** (2014) 55–72. MR 3029452, doi:10.26493/1855-3974.280.8d3
5. C. Godsil and G. Royle, *Algebraic graph theory*, Grad. Texts in Math. 207, Springer, New York, 2001. MR 1829620, doi:10.1007/978-1-4613-0163-9
6. J. L. Gross and T. W. Tucker, *Topological graph theory*, Wiley, New York, 1987. MR 0898434, https://store.doverpublications.com/0486417417.html
7. The GAP Group, *GAP – Groups, Algorithms, and Programming, version 4.10.2*, 2019, https://www.gap-system.org.
8. M. Hall, Jr., *The theory of groups*, Macmillan, New York, 1959. MR 0103215, https://store.doverpublications.com/0486816907.html
9. K. Helsgaun, *LKH — an effective implementation of the Lin-Kernighan heuristic, Version 2.0.7*, 2012, http://webhotel4.ruc.dk/~keld/research/LKH/.
10. B. Huppert and W. Lempken, *Simple groups of order divisible by at most four primes*, preprint, 2000. http://www.iem.uni-due.de/preprints/Index00.html
11. K. Keating and D. Witte, *On Hamilton cycles in Cayley graphs with cyclic commutator subgroup*, Ann. Discrete Math. **27** (1985) 89–102. MR 0821508, doi:10.1016/S0304-0208(08)72999-2

12. 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, doi:10.26493/1855-3974.177.341
13. L. Lovász, *Combinatorial problems and exercises, 2nd ed.*, North-Holland, Amsterdam, 1993. MR 1265492, doi:10.1016/C2009-0-09109-0
14. F. Maghsoudi, *Cayley graphs of order 6pq or 7pq are hamiltonian*, Art Discrete Appl. Math. **5** (2022) #P1.10. MR 4423287, doi:10.26493/2590-9770.1389.fa2
15. D. W. Morris, *Infinitely many nonsolvable groups whose Cayley graphs are hamiltonian*, J. Algebra Comb. Discrete Struct. Appl. **3** (2016), no. 1, 13–30. MR 3450931, https://jacodesmath.com/index.php/jacodesmath/article/view/26
16. D. W. Morris, *Odd-order Cayley graphs with commutator subgroup of order pq are hamiltonian*, Ars Math. Contemp. **8** (2015), no. 1, 1–28. MR 3281117, doi:10.26493/1855-3974.330.0e6
17. D. W. Morris, *Cayley graphs on groups with commutator subgroup of order 2p are hamiltonian*, Art Discrete Appl. Math. **1** (2017) #P1.04. MR 3995535, doi:10.26493/2590-9770.1240.60e
18. D. W. Morris, *On hamiltonian cycles in Cayley graphs of order pqrs*, Art Discrete Appl. Math. **5** (2022), no. 3, Paper No. 3.12, 10 pp. MR 4475143, doi:10.26493/2590-9770.1442.cb1
19. D. W. Morris and K. Wilk, *Cayley graphs of order kp are hamiltonian for $k < 48$*, Art Discrete Appl. Math. **3** (2020) #P2.02. MR 4145949, doi:10.26493/2590-9770.1250.763
20. J. G. Thompson, *Nonsolvable finite groups all of whose local subgroups are solvable*, Bull. Amer. Math. Soc. **74** (1968) 383–437. MR 0230809, doi:10.1090/S0002-9904-1968-11953-6
21. D. Witte and J. A. Gallian, *A survey: Hamiltonian cycles in Cayley graphs*, Discrete Math. **51** (1984), no. 3, 293–304. MR 0762322, doi:10.1016/0012-365X(84)90010-4

Faculty of Mathematical Sciences and Computer, Kharazmi University, 50 Taleghani Ave., Tehran, 1561836314, I. R. Iran
E-mail address: std_f.abedi@khu.ac.ir

Department of Mathematics and Computer Science, University of Lethbridge, 4401 University Drive, Lethbridge, Alberta, T1K 3M4, Canada
E-mail address: dmorris@deductivepress.ca, https://deductivepress.ca/dmorris

Faculty of Mathematical Sciences and Computer, Kharazmi University, 50 Taleghani Ave., Tehran, 1561836314, I. R. Iran
E-mail address: jre927@gmail.com

Faculty of Mathematical Sciences and Computer, Kharazmi University, 50 Taleghani Ave., Tehran, 1561836314, I. R. Iran
A. Renyi Institute of Mathematics, Hungarian Academy of Sciences, P. O. Box 127, H-1364 Budapest, Hungary
E-mail address: salarian@khu.ac.ir, salarian78@gmail.com