ISSN 2590-9770
The Art of Discrete and Applied Mathematics 5 (2022) #P3.12
https://doi.org/10.26493/2590-9770.1442.cb1
(Also available at http://adam-journal.eu)

On hamiltonian cycles in Cayley graphs of order $pqrs$

Dave Witte Morris*
Department of Mathematics and Computer Science, University of Lethbridge, 4401 University Drive, Lethbridge, Alberta, T1K 3M4, Canada

Received 18 August 2021, accepted 29 June 2022, published online 5 August 2022

Abstract

Let G be a finite group. We show that if $|G| = pqrs$, where p, q, r, and s are distinct odd primes, then every connected Cayley graph on G has a hamiltonian cycle.

Keywords: Cayley graph, hamiltonian cycle.

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

1 Introduction

Definition 1.1 (cf. [4, page 34]). If A is a subset of a finite group G, then the corresponding *Cayley graph* $\mathrm{Cay}(G; A)$ is the undirected graph whose vertices are the elements of G, and such that vertices g and h are adjacent if and only if $g^{-1}h \in A \cup A^{-1}$, where $A^{-1} = \{ a^{-1} \mid a \in A \}$.

It is easy to see (and well known) that $\mathrm{Cay}(G; A)$ is connected if and only if A is a generating set of G. Several papers show that all connected Cayley graphs of certain orders are hamiltonian:

Theorem 1.2 (see [6, 7, 9] and references therein). Let A be a generating set of a finite group G. If $|G|$ has any of the following forms (where p, q, and r are distinct primes, and k is a positive integer), then $\mathrm{Cay}(G; A)$ has a hamiltonian cycle:

1. kp, where $k \leq 47$,
2. kpq, where $k \leq 7$,
3. pqr,
4. kp^2, where ≤ 4,
5. kp^3, where $k \leq 2$.
6. p^k.

*I thank an anonymous referee for carefully reading the original version of the paper, and pointing out some serious deficiencies in the exposition.

E-mail address: dmorris@deductivepress.ca (Dave Witte Morris)

This work is licensed under https://creativecommons.org/licenses/by/4.0/

The purpose of this note is to add $pqrs$ to the list when it is odd:

Theorem 1.3. If p, q, r, and s are distinct odd primes, then every connected Cayley graph of order $pqrs$ has a hamiltonian cycle.

Remark 1.4.

1. To remove Theorem 1.3's assumption that the primes are odd, it would suffice to show that every connected Cayley graph of order $2pqr$ is hamiltonian (where p, q, and r are distinct odd primes). An important first step in this direction was taken by F. Maghsoudi [7], who handled the case where one of the primes is 3.

2. Theorem 1.3 implies that if p, q, and r are distinct primes, then every connected Cayley graph of order $3pqr$ is hamiltonian. Namely:

   - If $r = 2$, then $3pqr = 6pq$, so the main theorem of [7] applies.
   - If $r = 3$, then $3pqr = 9pq$, so [11, Corollary 1.5] applies.
   - If $\{p, q, r\} \cap \{2, 3\} \neq \emptyset$, then the theorem applies (because 3, p, q, and r are distinct odd primes).

3. Unfortunately, current methods do not seem to be sufficient to remove the assumption that p, q, r, and s are distinct. For example, it is not known that all Cayley graphs of order $9p^2$ or $3p^3$ are hamiltonian (cf. [6]).

2 Preliminaries

We use the following fairly standard notation.

Notation 2.1. Let A be a subset of a finite group G.

1. e is the identity element of G,

2. $|g|$ is the order of an element g of G.

3. $G' = [G, G]$ is the *commutator subgroup* of G.

4. $Z(G) = \{ z \in G \mid zg = gz \text{ for all } g \in G \}$ is the *centre* of G.

5. A sequence $(a_i)_{i=1}^m = (a_1, a_2, \ldots, a_m)$ of elements of $A \cup A^{-1}$ represents the walk in $\mathrm{Cay}(G; A)$ that visits the vertices

$$e, a_1, a_1a_2, \ldots, a_1a_2 \cdots a_m.$$

   Also, we use a^k and a^{-k} to represent the sequences

$$(a, a, \ldots, a) \text{ and } (a^{-1}, a^{-1}, \ldots, a^{-1})$$

   of length k.

Most cases of Theorem 1.3 are easy consequences of three known results that are collected in the following theorem.

Theorem 2.2 ([1, page 257], Durnberger [2], Morris [11]). Let A be a generating set of a nontrivial finite group G, and assume that $|G|$ is odd. If either

(0) $|G'| = 1$, or

(1) $|G'|$ is prime, or

(2) $|G'|$ is the product of 2 distinct primes,

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

Remark 2.3. The assumption that G has odd order is not necessary in parts (0) and (1) of Theorem 2.2. Steps toward removing this assumption from part (2) were taken in [3] and [8].

For ease of reference, we record a few other known facts:

Lemma 2.4 ("Factor Group Lemma" [10, §2.2]). *Suppose*

- *A is a subset of the group G,*
- *N is a cyclic, normal subgroup of G,*
- *$C = (a_i)_{i=1}^m$ is a hamiltonian cycle in $\mathrm{Cay}(G/N; A)$, and*
- *the voltage $\mathbb{V}(C) = \prod_{i=1}^m a_i$ generates N.*

Then $(a_1, a_2, \ldots, a_m)^{|N|}$ is a hamiltonian cycle in $\mathrm{Cay}(G; A)$.

Lemma 2.5 ([6, Lemma 2.27]). *Let A generate a finite group G and let $b \in A$, such that the subgroup generated by b is normal in G. If $\mathrm{Cay}\big(G/\langle b \rangle; A\big)$ has a hamiltonian cycle, and $\langle b \rangle \cap Z(G) = \{e\}$, then $\mathrm{Cay}(G; A)$ has a hamiltonian cycle.*

Lemma 2.6 (cf. [5, Theorem 9.4.3, p. 146] and [7, Lemma 2.16]). *Assume G is a finite group of square-free order. Then*

(1) *G' and G/G' are cyclic,*

(2) *$G' \cap Z(G) = \{e\}$, and*

(3) *if $a \in G$, such that $\langle a, G' \rangle = G$, then*

  (a) *a does not commute with any nontrivial element of G', and*

  (b) *$|a| = |G/G'|$.*

Proposition 2.7 (Maghsoudi [7, Proposition 3.1]). Assume G is a finite group, such that $|G|$ is a product of four distinct primes. If A is an irredundant generating set of G, such that $|A| \geq 4$, then $\mathrm{Cay}(G; A)$ has a hamiltonian cycle.

3 Proof of Theorem 1.3

Let A be an irredundant generating set of a finite group G, such that $|G| = pqrs$. We wish to show that $\mathrm{Cay}(G; A)$ has a hamiltonian cycle. Although some of the details are new, the line of argument here is quite standard. (See the proofs in [7], for example.)

Let

$$\overline{G} = G/G'.$$

Note that G is solvable by Lemma 2.6(1), so $G' \neq G$. Therefore $|G'|$ has at most 3 prime factors. We may assume it has exactly 3, for otherwise Theorem 2.2 applies. Hence, we may assume $|G'| = qrs$ (so $|\overline{G}| = p$). Since G' is cyclic (see Lemma 2.6(1)), we have

$$G' = \mathcal{C}_q \times \mathcal{C}_r \times \mathcal{C}_s,$$

where $\mathcal{C}_n$ denotes a (multiplicative) cyclic group of order n. Then each element γ of G' can be written uniquely in the form

$$\gamma = \gamma_q \, \gamma_r \, \gamma_s, \text{ where } \gamma_q \in \mathcal{C}_q, \gamma_r \in \mathcal{C}_r, \text{ and } \gamma_s \in \mathcal{C}_s.$$

Let $a \in A$, such that $\langle \overline{a} \rangle = \overline{G}$. Then $|a| = p$ by Lemma 2.6(3)(b). Let b be another element of A, so we may write $b = a^k \gamma$, where $\gamma \in G'$ (and $0 \leq k < p$).

Case 1. *Assume* $A \cap G' \neq \emptyset$. Then we may assume $b \in G'$. Since G' is cyclic (see Lemma 2.6(1)), and it is a standard exercise in undergraduate abstract algebra to show that every subgroup of a cyclic normal subgroup is normal, we know that $\langle b \rangle \triangleleft G$. Let $\widehat{G} = G/\langle b \rangle$. Since $|G| = pqrs$ has only 4 prime factors, we know that $|\widehat{G}|$ has at most 3 prime factors, so we see from part (1), (2), or (3) of Theorem 1.2 that $\operatorname{Cay}(\widehat{G}; A)$ has a hamiltonian cycle. Since

$$\langle b \rangle \cap Z(G) \subseteq G' \cap Z(G) = \{e\}$$

(see Lemma 2.6(2)), we can now conclude from Lemma 2.5 that $\operatorname{Cay}(G; S)$ has a hamiltonian cycle, as desired.

Case 2. *Assume* $|A| = 2$ (*and* $A \cap G' = \emptyset$). This means that $A = \{a, b\}$, so $\langle a, b \rangle = G$. This implies $\langle \gamma \rangle = G'$, so γ_q, γ_r, and γ_s are nontrivial. Also, we have $k \geq 1$, since $A \cap G' = \emptyset$. Let

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

so C is a (well known) hamiltonian cycle in $\operatorname{Cay}(\overline{G}; \overline{A})$. The voltage of C is

$$\mathbb{V}(C) = ba^{-(k-1)}ba^{p-k-1} = a^k\gamma \cdot a^{-(k-1)} \cdot a^k\gamma \cdot a^{p-k-1} = a^k \cdot \gamma_q\gamma_r\gamma_s \cdot a \cdot \gamma_q\gamma_r\gamma_s \cdot a^{-k-1}.$$

Since $|G|$ is odd, we know that a does not invert any nontrivial element of G', so the two occurrences of γ_q in this product do not cancel each other, and similarly for the occurrences of γ_r and γ_s. Therefore, this voltage projects nontrivially to $\mathcal{C}_q$, $\mathcal{C}_r$, and $\mathcal{C}_s$, so it generates G'. Hence, the Factor Group Lemma 2.4 provides a hamiltonian cycle in $\operatorname{Cay}(G; A)$.

Case 3. *Assume* $|A| \geq 3$ (*and* $A \cap G' = \emptyset$). Let c be a third element of A. We may assume $|A| < 4$ (for otherwise Proposition 2.7 applies), so $A = \{a, b, c\}$. Write $c = a^\ell \gamma'$ (with $\gamma' \in G'$). Since $\langle a, b, c \rangle = G$, we must have $\langle \gamma, \gamma' \rangle = G'$, but the fact that A is irredundant implies $\langle \gamma \rangle \neq G'$ and $\langle \gamma' \rangle \neq G'$. If $|\gamma| = q$, then we must have $|\gamma'| = rs$. However, this implies $\langle b, c \rangle = G$, which contradicts the fact that the generating set A is irredundant. So $|\gamma|$ and $|\gamma'|$ must each have precisely two prime factors. Therefore, we may assume without loss of generality that $|\gamma| = qr$ and $|\gamma'| = rs$. Then

$$\gamma = \gamma_q \, \gamma_r \text{ and } \gamma' = \gamma'_r \, \gamma'_s,$$

and each of γ_q, γ_r, γ'_r, and γ'_s is nontrivial.

We may assume $k, \ell \leq (p-1)/2$ (by replacing some generators with their inverses, if necessary). We may also assume, without loss of generality, that $\ell \leq k$. (If $k \neq \ell$, this implies $\ell \leq (p-3)/2$.) Also note that $k, \ell \geq 1$, since $A \cap G' = \emptyset$.

Subcase 3.1. *Assume $p = 3$.* This implies $\overline{a} = \overline{b} = \overline{c}$, so we have the following two hamiltonian cycles in $\mathrm{Cay}(\overline{G}; A)$:

$$C_1 = (\overline{a}, \overline{b}, \overline{c}) \text{ and } C_2 = (\overline{a}, \overline{c}, \overline{b}).$$

Their voltages are

$$\mathbb{V}(C_1) = abc = a \cdot a\gamma \cdot a\gamma' = a^2\, \gamma_q\, \gamma_r\, a\, \gamma_r'\, \gamma_s'$$

and

$$\mathbb{V}(C_2) = acb = a \cdot a\gamma' \cdot a\gamma = a^2\, \gamma_r'\, \gamma_s'\, a\, \gamma_q\, \gamma_r.$$

In each of these voltages, there is nothing that could cancel the factor γ_q or the factor γ_s'. So both voltages project nontrivially to $\mathcal{C}_q$ and $\mathcal{C}_s$.

Therefore, we may assume that both voltages project trivially to $\mathcal{C}_r$, for otherwise we have a voltage that projects nontrivially to all three factors, and therefore generates G', so the Factor Group Lemma 2.4 applies. Hence

$$a^2\gamma_r a \gamma_r' = \mathbb{V}(C_1)_r = e = \mathbb{V}(C_2)_r = a^2\gamma_r' a \gamma_r,$$

so, letting $x = \gamma_r'\, \gamma_r^{-1}$, we have $ax = xa$, which means that x commutes with a. However, we also know from Lemma 2.6(3)(a) that a does not commute with any nontrivial element of G'. Therefore, we must have $x = e$, which means $\gamma_r' = \gamma_r$. Also, since a does not invert any nontrivial element of G' (since a has odd order), we know that $\gamma_r a \gamma_r \neq a$. Therefore

$$\mathbb{V}(C_1)_r = a^2 \cdot \gamma_r a \gamma_r' = a^2 \cdot \gamma_r a \gamma_r \neq a^2 \cdot a = e.$$

This voltage therefore projects nontrivially to all three factors of G', so it generates G'. Hence, the Factor Group Lemma 2.4 applies.

Subcase 3.2. *Assume $\overline{a}$, $\overline{b}$, and $\overline{c}$ are not all distinct.* We may assume $\overline{a} = \overline{c}$ (which means $\ell = 1$). We may also assume $p \geq 5$, for otherwise Subcase 3.1 applies. Therefore

$$p - k \geq p - (p-1)/2 = (p+1)/2 \geq (5+1)/2 = 3,$$

so we have the following two hamiltonian cycles in $\mathrm{Cay}(\overline{G}; \overline{A})$:

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

Their voltages are

$$\begin{aligned} \mathbb{V}(C_1) &= ba^{-(k-1)}bca^{p-k-2} \\ &= a^k\gamma \cdot a^{-(k-1)} \cdot a^k\gamma \cdot a\gamma' \cdot a^{p-k-2} \\ &= a^k\, \gamma_q\gamma_r\, a\, \gamma_q\gamma_r\, a\, \gamma_r'\gamma_s'\, a^{-k-2} \end{aligned}$$

and

$$\begin{aligned}\mathbb{V}(C_2) &= ba^{-(k-1)}baca^{p-k-3}\\ &= a^k\gamma \cdot a^{-(k-1)} \cdot a^k\gamma \cdot a \cdot a\gamma' \cdot a^{p-k-3}\\ &= a^k\,\gamma_q\gamma_r\,a\,\gamma_q\gamma_r\,a^2\,\gamma'_r\gamma'_s\,a^{-k-3}.\end{aligned}$$

Since a does not invert γ_q (because a has odd order), we see that the two occurrences of γ_q in these voltages cannot cancel each other. Hence, both voltages project nontrivially to $\mathcal{C}_q$. Also, there is nothing in either voltage that could cancel the single occurrence of γ'_s, so both voltages also project nontrivially to $\mathcal{C}_s$.

Therefore, in order to apply the Factor Group Lemma 2.4, it suffices to show that at least one of these voltages projects nontrivially to $\mathcal{C}_r$. If not, then both projections are trivial, so

$$\begin{aligned}a^k\gamma_r a\gamma_r a \cdot \gamma'_r a \cdot a^{-k-3} &= a^k\gamma_r a\gamma_r a\gamma'_r a^{-k-2}\\ &= \mathbb{V}(C_1)_r\\ &= e\\ &= \mathbb{V}(C_2)_r\\ &= a^k\gamma_r a\gamma_r a^2\gamma'_r a^{-k-3}\\ &= a^k\gamma_r a\gamma_r a \cdot a\gamma'_r \cdot a^{-k-3},\end{aligned}$$

which implies $\gamma'_r a = a\gamma'_r$. This contradicts the fact that a does not centralize any nontrivial element of G' (see Lemma 2.6(3)(a)).

Subcase 3.3. *Assume* $\ell \neq (p-3)/2$. We may assume that the preceding case does not apply. In particular, then $\bar{b} \neq \bar{c}$, so $k \neq \ell$, so we have $\ell \leq (p-5)/2$, which implies $k+\ell \leq p-3$. Therefore, we have the following two hamiltonian cycles in $\mathrm{Cay}(\overline{G};\overline{A})$:

$$C_1 = (\bar{b}, \bar{a}^{-(k-1)}, \bar{b}, \bar{c}, \bar{a}^{-(\ell-1)}, \bar{c}, \bar{a}^{p-k-\ell-2}) \tag{A}$$

and

$$C_2 = (\bar{b}, \bar{a}^{-(k-1)}, \bar{b}, \bar{a}, \bar{c}, \bar{a}^{-(\ell-1)}, \bar{c}, \bar{a}^{p-k-\ell-3}).$$

Their voltages are

$$\begin{aligned}\mathbb{V}(C_1) &= ba^{-(k-1)}bca^{-(\ell-1)}ca^{p-k-\ell-2}\\ &= a^k\gamma \cdot a^{-(k-1)} \cdot a^k\gamma \cdot a^\ell\gamma' \cdot a^{-(\ell-1)} \cdot a^\ell\gamma' \cdot a^{p-k-\ell-2}\\ &= a^k \cdot \gamma_q\gamma_r a\gamma_q\gamma_r \cdot a^\ell \cdot \gamma'_r\gamma'_s a\gamma'_r\gamma'_s \cdot a^{p-k-\ell-2}\end{aligned} \tag{B}$$

and

$$\begin{aligned}\mathbb{V}(C_2) &= ba^{-(k-1)}baca^{-(\ell-1)}ca^{p-k-\ell-3}\\ &= a^k\gamma \cdot a^{-(k-1)} \cdot a^k\gamma \cdot a \cdot a^\ell\gamma' \cdot a^{-(\ell-1)} \cdot a^\ell\gamma' \cdot a^{p-k-\ell-3}\\ &= a^k \cdot \gamma_q\gamma_r a\gamma_q\gamma_r \cdot a^{\ell+1} \cdot \gamma'_r\gamma'_s a\gamma'_r\gamma'_s \cdot a^{p-k-\ell-3}.\end{aligned}$$

In each product, the two occurrences of γ_q cannot cancel each other, and the two occurrences of γ_s' cannot cancel each other (because a does not invert any nontrivial element of G'), so both voltages project nontrivially to $\mathcal{C}_q$ and $\mathcal{C}_s$.

Therefore, in order to apply the Factor Group Lemma 2.4, it suffices to show that at least one of these voltages projects nontrivially to $\mathcal{C}_r$. If not, then both projections are trivial, so, much as in Subcase 3.2, we have

$$\begin{aligned}
a^k\gamma_r a\gamma_r a^\ell \cdot \gamma_r' a\gamma_r' a \cdot a^{p-k-\ell-3} &= a^k \cdot \gamma_r a\gamma_r \cdot a^\ell \cdot \gamma_r' a\gamma_r' \cdot a^{p-k-\ell-2} \\
&= \mathbb{V}(C_1)_r \\
&= e \\
&= \mathbb{V}(C_2)_r \\
&= a^k \cdot \gamma_r a\gamma_r \cdot a^{\ell+1} \cdot \gamma_r' a\gamma_r' \cdot a^{p-k-\ell-3} \\
&= a^k\gamma_r a\gamma_r a^\ell \cdot a\gamma_r' a\gamma_r' \cdot a^{p-k-\ell-3},
\end{aligned}$$

so $\gamma_r' a\gamma_r' a = a\gamma_r' a\gamma_r'$.

Now, note that $\langle\gamma_r'\rangle \triangleleft G$ (since every subgroup of the cyclic normal subgroup G' is normal), so there is some $\widehat{\gamma} \in \langle\gamma_r'\rangle$, such that $a\gamma_r' = \widehat{\gamma}a$. With this notation, the conclusion of the preceding paragraph tells us that $\gamma_r'\widehat{\gamma}a^2 = \widehat{\gamma}a^2\gamma_r'$. Since γ_r' and $\widehat{\gamma}$ are in the abelian group $\langle\gamma_r'\rangle$, we know that they commute with each other, so this implies $\gamma_r' a^2 = a^2\gamma_r'$.

However, since $\overline{a}$ generates $\overline{G}$, and $|\overline{G}| = p$ is odd, we know that $\overline{a}^2$ also generates $\overline{G}$. Hence, we see from Lemma 2.6(3)(a) that a^2 does not centralize any nontrivial element of G'. This contradicts the conclusion of the preceding paragraph.

Subcase 3.4. *Assume* $p = 7$. We may assume Subcase 3.2 does not apply, so $1 < \ell < k \leq (p-1)/2$. Since $(p-1)/2 = (7-1)/2 = 3$, we conclude that $\ell = 2$ and $k = 3$. Thus, we have

$$p = 7, \ \overline{c} = \overline{a}^2, \text{ and } \overline{b} = \overline{a}^3.$$

Now, the Cayley graph $\operatorname{Cay}(\overline{G}; \overline{a}, \overline{b}, \overline{c})$ is the complete graph K_7, so it has *many* hamiltonian cycles. In particular, we have the hamiltonian cycle

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

Since G' is a cyclic, normal subgroup of G (and $|a| = p = 7$), there is some $\alpha \in \mathbb{Z}^+$, such that $\alpha^7 \equiv 1 \pmod{qrs}$ and

$$a\,g = g^\alpha\,a \ \text{ for all } g \in G'.$$

Also, we may write $\gamma_r' = \gamma_r^x$ for some $x \in \mathbb{Z}^+$. With this notation, the voltage of C is

$$\begin{aligned}
\mathbb{V}(C) &= ca^2ca^{-1}ba^{-1} \\
&= a^2\gamma' \cdot a^2 \cdot a^2\gamma' \cdot a^{-1} \cdot a^3\gamma \cdot a^{-1} \\
&= a^2\gamma' a^4\gamma' a^2\gamma a^{-1} \\
&= (\gamma')^{\alpha^2+\alpha^6}\gamma^\alpha \\
&= (\gamma_r'\gamma_s')^{\alpha^2+\alpha^6}(\gamma_q\,\gamma_r)^\alpha \\
&= (\gamma_r^x\gamma_s')^{\alpha^2+\alpha^6}(\gamma_q\,\gamma_r)^\alpha \\
&= \gamma_q^\alpha\,\gamma_r^{(\alpha^2+\alpha^6)x+\alpha}\,(\gamma_s')^{\alpha^2+\alpha^6}.
\end{aligned}$$

Since $\alpha^7 \equiv 1 \pmod{qrs}$, we know that $\alpha^7 \equiv 1 \pmod q$ and $\alpha^7 \equiv 1 \pmod s$, so it is easy to see that $\alpha \not\equiv 0 \pmod q$ and $\alpha^2 + \alpha^6 \not\equiv 0 \pmod s$. Hence, it is clear that $\mathbb{V}(C)$ projects nontrivially to $\mathcal{C}_q$ and $\mathcal{C}_s$. Therefore, if Theorem 2.4 does not apply, then this voltage projects trivially to $\mathcal{C}_r$, which means

$$(\alpha^2 + \alpha^6)x + \alpha \equiv 0 \pmod r. \tag{C}$$

We also have the hamiltonian cycle

$$C' = (\bar{b}, \overline{a}^{-2}, \bar{b}, \bar{c}, \overline{a}^{-1}, \bar{c}).$$

It is easy to see that the voltage of this hamiltonian cycle projects nontrivially to $\mathcal{C}_q$ and $\mathcal{C}_s$. (As in Subcase 3.3, this is because the only occurrences of γ_q come from the two occurrences of $\bar{b}$, and the only occurrences of γ_s come from the two occurrences of $\bar{c}$. None of these can cancel each other, because no element of G inverts γ_q or γ_s.) Therefore, if $\mathbb{V}(C')$ does not generate G', then this voltage must project trivially to $\mathcal{C}_r$.

Note that the hamiltonian cycle C' can be obtained from the hamiltonian cycle C_1 of Equation (A), with $p = 7$, $k = 3$, and $\ell = 2$, by deleting the final term $\overline{a}^{p-k-\ell-2} = \overline{a}^{7-3-2-2} = \overline{a}^0$ of C_1. Therefore, the formula (B) for the voltage of C_1 also yields the voltage of C' (if we delete the irrelevant final term $a^{p-k-\ell-2} = a^0 = e$), so we have

$$\begin{aligned} e &= \mathbb{V}(C_1)_r \\ &= a^k \cdot \gamma_r a \gamma_r \cdot a^\ell \cdot \gamma_r' a \gamma_r' \\ &= a^3 \cdot \gamma_r a \gamma_r \cdot a^2 \cdot \gamma_r^x a \gamma_r^x \\ &= \gamma_r^{\alpha^3 + \alpha^4 + \alpha^6 x + \alpha^7 x}, \end{aligned}$$

so

$$\alpha^3 + \alpha^4 + \alpha^6 x + \alpha^7 x \equiv 0 \pmod r.$$

Multiplying by α^4, and recalling that $\alpha^7 \equiv 1 \pmod r$, we conclude that

$$(1 + \alpha) + \alpha^3(1 + \alpha)x \equiv 0 \pmod r.$$

Dividing this equation by $1 + \alpha$ yields $1 + \alpha^3 x = 0$ (in $\mathbb{Z}_r$), so $x = -1/\alpha^3$. Plugging this into Equation (C) yields $-(\alpha^2 + \alpha^6)/\alpha^3 + \alpha = 0$ in $\mathbb{Z}_r$, so (multiplying by $-\alpha$) we have $1 + \alpha^4 - \alpha^2 \equiv 0 \pmod r$. Recall that we also know $\alpha^7 - 1 \equiv 0 \pmod r$. Since the polynomial $1 + x^4 - x^2$ is relatively prime to $x^7 - 1$, this is impossible. More concretely, we have

$$\begin{aligned} 0 &= (\alpha^6 - \alpha^5 + \alpha^4 - \alpha^3 - 1) \cdot 0 \; - \; (\alpha^3 - \alpha^2) \cdot 0 \\ &\equiv (\alpha^6 - \alpha^5 + \alpha^4 - \alpha^3 - 1)(1 + \alpha^4 - \alpha^2) - (\alpha^3 - \alpha^2)(\alpha^7 - 1) \qquad \pmod r \\ &= -1, \end{aligned}$$

which is an obvious contradiction.

Subcase 3.5. *Assume that the preceding cases do not apply.* Since Subcase 3.3 does not apply, we must have $\ell = (p-3)/2$. Since $\ell < k \leq (p-1)/2$, this implies

$$k = \frac{p-1}{2} = 1 + \frac{p-3}{2} = 1 + \ell.$$

Therefore

$$\overline{a}\,\overline{c} = \overline{a}\,\overline{a}^{\ell} = \overline{a}^{1+\ell} = \overline{a}^{k} = \overline{b}.$$

Putting c into the role of a will usually give us new values for k and ℓ. Indeed, if Subcase 3.3 does not apply after this change (that is, after replacing the triple (a,b,c) with the appropriate triple $(c, a^{\epsilon_1}, b^{\epsilon_2})$ or $(c, b^{\epsilon_1}, a^{\epsilon_2})$, with $\epsilon_1, \epsilon_2 \in \{\pm 1\}$), then either

$$\overline{a}^{\pm 1} = \overline{c}^{(p-3)/2} \text{ and } \overline{b}^{\pm 1} = \overline{c}^{(p-1)/2} = \overline{a}^{\pm 1}\,\overline{c}$$

or

$$\overline{b}^{\pm 1} = \overline{c}^{(p-3)/2} \text{ and } \overline{a}^{\pm 1} = \overline{c}^{(p-1)/2} = \overline{b}^{\pm 1}\,\overline{c}.$$

However, we have

$$\overline{a}^{-1}\,\overline{c} = \overline{a}^{\ell-1} = \overline{a}^{(p-5)/2} \notin \{\overline{a}^{\pm(p-1)/2}\} = \{\overline{b}^{\pm 1}\}$$

and

$$\overline{b}\,\overline{c} = \overline{a}^{k+1} = \overline{a}^{(p+1)/2} \notin \{\overline{a}^{\pm 1}\}.$$

Therefore, $\overline{c}^{(p-3)/2}$ must be either $\overline{a}$ or $\overline{b}^{-1}$. Noting that (since $\overline{a}\,\overline{c} = \overline{b}$) we have $\overline{b} = \overline{a}\,\overline{c}$ and $\overline{a}^{-1} = \overline{b}^{-1}\,\overline{c}$, this implies that the only possibilities are that either

$$\overline{a} = \overline{c}^{(p-3)/2} \text{ and } \overline{b} = \overline{a}\,\overline{c} = \overline{c}^{(p-1)/2} \tag{D}$$

or

$$\overline{b}^{-1} = \overline{c}^{(p-3)/2} \text{ and } \overline{a}^{-1} = \overline{b}^{-1}\,\overline{c} = \overline{c}^{(p-1)/2}. \tag{E}$$

If (D) holds, then

$$\overline{a} = \overline{c}^{(p-3)/2} = \left(\overline{a}^{\ell}\right)^{(p-3)/2} = \left(\overline{a}^{(p-3)/2}\right)^{(p-3)/2} = \overline{a}^{(p-3)^2/4},$$

so $(p-3)^2/4 \equiv 1 \pmod p$, so $9 \equiv 4 \pmod p$, which implies $p = 5$. However, since Subcase 3.2 does not apply, we know that $\overline{c} \neq \overline{a}$, so $\ell > 1$. This means $(p-3)/2 \geq 2$, so $p \geq 7$. This contradicts our recent previous conclusion that $p = 5$.

So (E) must hold. Then $\overline{b}^{-1} = \overline{c}^{(p-3)/2}$. Since $\overline{b} = \overline{a}^{k} = \overline{a}^{(p-1)/2}$ and $\overline{c} = \overline{a}^{\ell} = \overline{a}^{(p-3)/2}$, this means

$$-(p-1)/2 \equiv (p-3)^2/4 \pmod p.$$

so $2 \equiv 9 \pmod p$, which implies $p = 7$. So Subcase 3.4 applies.

References

[1] C. C. Chen and N. F. Quimpo, On strongly Hamiltonian abelian group graphs, in: *Combinatorial Mathematics, VIII (Geelong, 1980)*, Springer, Berlin-New York, volume 884 of *Lecture Notes in Math.*, pp. 23–34, 1981, doi:10.1007/bfb0091805.

[2] E. Durnberger, Every connected Cayley graph of a group with prime order commutator group has a Hamilton cycle, in: *Cycles in Graphs (Burnaby, B.C., 1982)*, North-Holland, Amsterdam, volume 115 of *North-Holland Math. Stud.*, pp. 75–80, 1985, doi:10.1016/s0304-0208(08)72997-9.

[3] E. Ghaderpour and D. W. Morris, Cayley graphs on nilpotent groups with cyclic commutator subgroup are Hamiltonian, *Ars Math. Contemp.* **7** (2014), 55–72, doi:10.26493/1855-3974.280.8d3.

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

[5] M. Hall, Jr., *The Theory of Groups*, The Macmillan Company, New York, N.Y., 1959, https://store.doverpublications.com/0486816907.html.

[6] K. Kutnar, D. Marušič, D. W. Morris, J. Morris and P. Šparl, Hamiltonian cycles in Cayley graphs whose order has few prime factors, *Ars Math. Contemp.* **5** (2012), 27–71, doi:10.26493/1855-3974.177.341.

[7] F. Maghsoudi, Cayley graphs of order $6pq$ and $7pq$ are Hamiltonian, *Art Discrete Appl. Math.* **5** (2022), Paper No. 1.10, 55, doi:10.26493/2590-9770.1389.fa2.

[8] D. W. Morris, Cayley graphs on groups with commutator subgroup of order $2p$ are hamiltonian, *Art Discrete Appl. Math.* **1** (2018), Paper No. 1.04, 31, doi:10.26493/2590-9770.1240.60e.

[9] D. W. Morris and W. K. Cayley graphs of order kp are hamiltonian for $k < 48$, *Art Discrete Appl. Math.* **3** (2020), Paper No. 2.02, doi:10.26493/2590-9770.1250.763.

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

[11] D. Witte Morris, Odd-order Cayley graphs with commutator subgroup of order pq are hamiltonian, *Ars Math. Contemp.* **8** (2015), 1–28, doi:10.26493/1855-3974.330.0e6.