Cayley graphs of order $30p$ are hamiltonian

Ebrahim Ghaderpour, Dave Witte Morris

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

Abstract

Suppose G is a finite group, such that $|G| = 30p$, where p is prime. We show that if S is any generating set of G, then there is a hamiltonian cycle in the corresponding Cayley graph $\mathrm{Cay}(G; S)$.

1. Introduction

There is a folklore conjecture that every connected Cayley graph has a hamiltonian cycle. (See the surveys [3, 12, 14] for some background on this question.) The papers [8] and [10] began a systematic study of this conjecture in the case of Cayley graphs for which the number of vertices has a prime factorization that is small and easy. In particular, combining several of the results in [10] with [4, 5] and this paper shows:

If $|G| = kp$, where p is prime, with $1 \leq k < 32$ and $k \neq 24$, then every connected Cayley graph on G has a hamiltonian cycle.

This paper's contribution to the project is the case $k = 30$:

Theorem 1.1. *If $|G| = 30p$, where p is prime, then every connected Cayley graph on G has a hamiltonian cycle.*

Acknowledgments. This work was partially supported by research grants from the Natural Sciences and Engineering Research Council of Canada.

Email addresses: `Ebrahim.Ghaderpoor@uleth.ca` (Ebrahim Ghaderpour), `Dave.Morris@uleth.ca` (Dave Witte Morris)

URL: `http://people.uleth.ca/~dave.morris/` (Dave Witte Morris)

Preprint submitted to Discrete Mathematics *July 3, 2012*

2. Preliminaries

Before proving Theorem 1.1, we present some useful facts about hamiltonian cycles in Cayley graphs.

Notation. Throughout this paper, G is a finite group.

- For any subset S of G, $\mathrm{Cay}(G;S)$ denotes the *Cayley graph* of G with respect to S. Its vertices are the elements of G, and there is an edge joining g to gs for every $g \in G$ and $s \in S$.
- For $x, y \in G$:
  - $[x, y]$ denotes the *commutator* $x^{-1}y^{-1}xy$, and
  - y^x denotes the *conjugate* $x^{-1}yx$.
- $\langle A \rangle$ denotes the subgroup generated by a subset A of G.
- G' denotes the *commutator subgroup* $[G, G]$ of G.
- $Z(G)$ denotes the *center* of G.
- $G \ltimes H$ denotes a *semidirect product* of the groups G and H.
- D_{2n} denotes the *dihedral group* of order $2n$.
- For $S \subset G$, a sequence $(s_1, s_2, \ldots, s_n)$ of elements of $S \cup S^{-1}$ specifies the walk in the Cayley graph $\mathrm{Cay}(G;S)$ that visits (in order) the vertices

  $$e, s_1, s_1s_2, s_1s_2s_3, \ldots, s_1s_2 \ldots s_n.$$

  If N is a normal subgroup of G, we use $(\overline{s_1}, \overline{s_2}, \ldots, \overline{s_n})$ to denote the image of this walk in the quotient $\mathrm{Cay}(G/N;S)$.
- If the walk $(\overline{s_1}, \overline{s_2}, \ldots, \overline{s_n})$ in $\mathrm{Cay}(G/N;S)$ is closed, then its *voltage* is the product $s_1s_2 \ldots s_n$. This is an element of N.
- For $k \in \mathbb{Z}^+$, we use $(s_1, \ldots, s_m)^k$ to denote the concatenation of k copies of the sequence $(s_1, \ldots, s_m)$. Abusing notation, we often write s^k and s^{-k} for

  $$(s)^k = (s, s, \ldots, s) \quad \text{and} \quad (s^{-1})^k = (s^{-1}, s^{-1}, \ldots, s^{-1}),$$

  respectively. Furthermore, we often write $\big((s_1, \ldots, s_m), (t_1, \ldots, t_n)\big)$ to denote the concatenation $(s_1, \ldots, s_m, t_1, \ldots, t_n)$. For example, we have

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

Theorem 2.1 (Marušič, Durnberger, Keating-Witte [9]). *If G' is a cyclic group of prime-power order, then every connected Cayley graph on G has a hamiltonian cycle.*

Lemma 2.2 ("Factor Group Lemma" [14, §2.2]). *Suppose*

- *S is a generating set of G,*
- *N is a cyclic, normal subgroup of G,*
- *$\overline{C} = (\overline{s_1}, \overline{s_2}, \ldots, \overline{s_n})$ is a hamiltonian cycle in $\mathrm{Cay}(G/N; S)$, and*
- *the voltage of $\overline{C}$ generates N.*

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

The following easy consequence of the Factor Group Lemma (2.2) is well known (and is implicit in [11]).

Corollary 2.3. *Suppose*

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

Then there is a hamiltonian cycle in $\mathrm{Cay}(G; S)$. (note A.1)

Theorem 2.4 (Alspach [1, Cor. 5.2]). *If $G = \langle s \rangle \ltimes \langle t \rangle$, for some elements s and t of G, then $\mathrm{Cay}\big(G; \{s, t\}\big)$ has a hamiltonian cycle.*

Lemma 2.5 ([10, Lem. 2.27]). *Let S generate the finite group G, and let $s \in S$, such that $\langle s \rangle \triangleleft G$. If $\mathrm{Cay}\big(G/\langle s \rangle; S\big)$ has a hamiltonian cycle, and either*

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

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

Lemma 2.6. *Suppose*

- *$G = \langle a \rangle \ltimes \langle S_0 \rangle$, where $\langle S_0 \rangle$ is an abelian subgroup of odd order,*

- $\#(S_0 \cup S_0^{-1}) \geq 3$, *and*
- $\langle S_0 \rangle$ *has a nontrivial subgroup* H*, such that* $H \triangleleft G$ *and* $H \cap Z(G) = \{e\}$.

Then $\mathrm{Cay}\big(G; S_0 \cup \{a\}\big)$ *has a hamiltonian cycle.*

Proof. Since $\langle S_0 \rangle$ is abelian of odd order, and $\#(S_0 \cup S_0^{-1}) \geq 3$, we know that $\mathrm{Cay}\big(\langle S_0 \rangle; S_0\big)$ is hamiltonian connected [2]. Therefore, it has a hamiltonian path $(s_1, s_2, \ldots, s_m)$, such that $s_1 s_2 \cdots s_m \in H$. Then

$$\big(s_1, s_2, \ldots, s_m, a\big)^{|a|}$$

is a hamiltonian cycle in $\mathrm{Cay}\big(G; S_0 \cup \{a\}\big)$. □ (note A.2)

Lemma 2.7 ([4, Cor. 4.4])**.** *If* $a, b \in G$*, such that* $G = \langle a, b \rangle$*, then* $G' = \langle [a, b] \rangle$.

Lemma 2.8 ([13, Prop. 5.5])**.** *If* p*,* q*, and* r *are prime, then every connected Cayley graph on the dihedral group* D_{2pqr} *has a hamiltonian cycle.*

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

Proof. Let S be a minimal generating set of G, let $\varphi \colon G \to D_{2pq}$ be the natural projection, and let T be the group of rotations in D_{2pq}, so $T = \mathbb{Z}_p \times \mathbb{Z}_q$.

For $s \in S$, we may assume:

- If $\varphi(s)$ has order 2, then $s = \varphi(s)$ has order 2. (Otherwise, Corollary 2.3 applies with $t = s^{-1}$.)
- $\varphi(s)$ is nontrivial. (Otherwise, $s \in \mathbb{Z}_r \subset Z(G)$, so Lemma 2.5(1) applies.)

Since $\varphi(S)$ generates D_{2pq}, it must contain at least one reflection (which is an element of order 2). So $S \cap D_{2pq}$ contains a reflection.

Case 1. *Assume* $S \cap D_{2pq}$ *contains only one reflection.* Let $a \in S \cap D_{2pq}$, such that a is a reflection.

Let $S_0 = S \setminus \{a\}$. Since $\langle S_0 \rangle$ is a subgroup of the cyclic, normal subgroup $T \times \mathbb{Z}_r$, we know $\langle S_0 \rangle$ is normal. Therefore $G = \langle a \rangle \ltimes \langle S_0 \rangle$, so:

- If $\#S_0 = 1$, then Theorem 2.4 applies.

- If $\#S_0 \geq 2$, then Lemma 2.6 applies with $H = T$, because $T \times \mathbb{Z}_r$ is abelian of odd order.

Case 2. *Assume $S \cap D_{2pq}$ contains at least two reflections.* Since no minimal generating set of D_{2pq} contains three reflections, the minimality of S implies that $S \cap D_{2pq}$ contains exactly two reflections; say a and b are reflections. (note A.3)

Let $c \in S \setminus D_{2pq}$, so $\mathbb{Z}_r \subset \langle c \rangle$. Since $|c| > 2$, we know $\varphi(c)$ is not a reflection, so $\varphi(c) \in T$. The minimality of S (combined with the fact that $\#S > 2$) implies $\langle \varphi(c) \rangle \neq T$. Since $\varphi(c)$ is nontrivial, this implies we may assume $\langle \varphi(c) \rangle = \mathbb{Z}_p$ (by interchanging p and q if necessary). Hence, we may write (note A.4)

$$c = wz \text{ with } \langle w \rangle = \mathbb{Z}_p \text{ and } \langle z \rangle = \mathbb{Z}_r.$$

We now use the argument of [9, Case 5.3, p. 96], which is based on ideas of D. Marušič [11]. Let

$$\overline{G} = G/\mathbb{Z}_p = \overline{D_{2pq}} \times \mathbb{Z}_r = \overline{D_{2pq}} \times \langle \overline{c} \rangle.$$

Then $\overline{D_{2pq}} \cong D_{2q}$, so $(a,b)^q$ is a hamiltonian cycle in $\mathrm{Cay}\big(\overline{D_{2pq}}; a, b\big)$. With this in mind, it is easy to see that

$$\Big(c^{r-1}, a, \big((b,a)^{q-1}, c^{-1}, (a,b)^{q-1}, c^{-1}\big)^{(r-1)/2}, (b,a)^{q-1}, b\Big).$$

is a hamiltonian cycle in $\mathrm{Cay}(\overline{G}; S)$. This contains the string (note A.5)

$$\big(c, a, (b,a)^{q-1}, c^{-1}, a\big),$$

which can be replaced with the string

$$\big(b, c, (b,a)^{q-1}, b, c^{-1}\big)$$

to obtain another hamiltonian cycle. Since (note A.6)

$$\begin{aligned}
ca(ba)^{q-1}c^{-1}a &= \big(cac^{-1}a\big)(ba)^{-(q-1)} && (ba \in T \text{ is inverted by } a) \\
&= \big((wz)a(wz)^{-1}a\big)(ba)^{-(q-1)} \\
&= \big(w^2\big)(ba)^{-(q-1)} && (a \text{ inverts } w \text{ and centralizes } z) \\
&\neq \big(w^{-2}\big)(ba)^{-(q-1)} \\
&= \big(b(wz)b(wz)^{-1}\big)(ba)^{-(q-1)} && (b \text{ inverts } w \text{ and centralizes } z) \\
&= \big(bcbc^{-1}\big)(ba)^{-(q-1)} \\
&= bc(ba)^{q-1}bc^{-1}, && (ba \in T \text{ is inverted by } b)
\end{aligned}$$

these two hamiltonian cycles have different voltages. Therefore at least one of them must have a nontrivial voltage. This nontrivial voltage must generate $\mathbb{Z}_p$, so the Factor Group Lemma (2.2) provides a hamiltonian cycle in $\mathrm{Cay}(G; S)$. □

Proposition 2.10. *Suppose*

- $|G| = 30p$, *where* p *is prime, and*
- $|G|$ *is not square-free (i.e.,* $p \in \{2, 3, 5\}$*).*

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

Proof. We know $|G|$ is either 60, 90, or 150, and it is known that every connected Cayley graph of any of these three orders has a hamiltonian cycle. This can be verified by exhaustive computer search, or see [10, Props. 7.2 and 9.1] and [6]. □

Lemma 2.11. *Suppose*

- $|G| = 30p$, *where* p *is prime, and*
- $p \geq 7$.

Then

1. G' *is cyclic,*
2. $G' \cap Z(G) = \{e\}$,
3. $G \cong \mathbb{Z}_n \ltimes G'$, *for some* $n \in \mathbb{Z}^+$, *and*
4. *if* b *is a generator of* $\mathbb{Z}_n$, *and we choose* $\tau \in \mathbb{Z}$, *such that* $x^b = x^\tau$ *for all* $x \in G'$, *then* $\gcd(\tau - 1, |a|) = 1$.

Proof. Since $|G|$ is square-free (because $p \geq 7$), we know that every Sylow subgroup of G is cyclic. Therefore the conclusions follow from [7, Thm. 9.4.3, p. 146][1]. □ (note A.7)

[1]The condition $[(r-1), nm] = 1$ in the statement of [7, Cor. 9.4.3, p. 146] suffers from a typographical error — it should say $\gcd((r-1)n, m) = 1$.

3. Proof of the Main Theorem

Proof of Theorem 1.1. Because of Proposition 2.10, we may assume

$$p \geq 7,$$

so the conclusions of Lemma 2.11 hold.

We may also assume $|G'|$ is not prime (otherwise Theorem 2.1 applies). Furthermore, if $|G'| = 15p$, then G is a dihedral group, so Lemma 2.8 applies. (note A.8) In addition, if $|G'| = 15$, then $G \cong D_{30} \times \mathbb{Z}_p$, so Lemma 2.9 applies. Thus, (note A.9) we may assume $|G'| = pq$, where $q \in \{3, 5\}$. So (note A.10)

$$G = \mathbb{Z}_{2r} \ltimes \mathbb{Z}_{pq}, \text{ with } \{q, r\} = \{3, 5\} \text{ (and } G' = \mathbb{Z}_{pq}).$$

Note that $\mathbb{Z}_r$ centralizes $\mathbb{Z}_q$, because there is no nonabelian group of order 15, so $\mathbb{Z}_2$ must act nontrivially on $\mathbb{Z}_q$. Therefore (note A.11)

$$y^x = y^{-1} \text{ whenever } y \in \mathbb{Z}_q \text{ and } \langle x \rangle = \mathbb{Z}_{2r}.$$

We also assume

$$\mathbb{Z}_r \text{ does not centralize } \mathbb{Z}_p,$$

because otherwise $G \cong D_{2pq} \times \mathbb{Z}_r$, so Lemma 2.9 applies. (note A.12)

Given a minimal generating set S of G, we may assume

$$S \cap G' = \emptyset,$$

for otherwise Lemma 2.5(2) applies.

Case 1. *Assume* $\#S = 2$. Write $S = \{a, b\}$.

Subcase 1.1. *Assume* $|a|$ *is odd.* This implies a has order r in G/G', so $(a^{-(r-1)}, b^{-1}, a^{r-1}, b)$ is a hamiltonian cycle in $\mathrm{Cay}(G/G'; S)$. Its voltage is

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

Since $\gcd(r-1, |a|) \mid \gcd(r-1, 15p) = 1$, we know $\langle a^{r-1}, b \rangle = \langle a, b \rangle = G$. So (note A.13) $\langle [a^{r-1}, b] \rangle = G'$ (see Lemma 2.7). Therefore the Factor Group Lemma (2.2) applies.

Subcase 1.2. *Assume a and b both have even order.*

Subsubcase 1.2.1. *Assume a has order 2 in G/G'.* Note that $q \nmid |a|$, since $\mathbb{Z}_2$ does not centralize $\mathbb{Z}_q$. Also, if $|a| = 2p$, then Corollary 2.3 applies. (note A.14)

Therefore, we may assume $|a| = 2$.

Now b must generate G/G' (since $\langle a, b \rangle = G$, and b has even order), so b has trivial centralizer in $\mathbb{Z}_{pq}$. Then, since $|a| = 2$ and $\langle a, b \rangle = G$, it follows that a must also have trivial centralizer in $\mathbb{Z}_{pq}$. Therefore (up to isomorphism), we must have either: (note A.15) (note A.16)

1. $a = x^3$ and $b = xyw$, in $G = \mathbb{Z}_6 \ltimes (\mathbb{Z}_5 \times \mathbb{Z}_p) = \langle x \rangle \ltimes \big(\langle y \rangle \times \langle w \rangle \big)$, with $y^x = y^{-1}$ and $w^x = w^d$, where d is a primitive 6^{th} root of 1 in $\mathbb{Z}_p$ (so $d^2 - d + 1 \equiv 0 \pmod p$), or
2. $a = x^5$ and $b = xyw$, in $G = \mathbb{Z}_{10} \ltimes (\mathbb{Z}_3 \times \mathbb{Z}_p) = \langle x \rangle \ltimes \big(\langle y \rangle \times \langle w \rangle \big)$ with $y^x = y^{-1}$ and $w^x = w^d$, where d is a primitive 10^{th} root of 1 in $\mathbb{Z}_p$ (so $d^4 - d^3 + d^2 - d + 1 \equiv 0 \pmod p$).

For (1), we note that the sequence $\big((a, b^{-5})^4, a, b^5\big)$ is a hamiltonian cycle in $\mathrm{Cay}(G/\mathbb{Z}_p; S)$:

$$\begin{array}{ccccccccccc}
\overline{e} & \xrightarrow{a} & \overline{x^3} & \xrightarrow{b^{-1}} & \overline{x^2y} & \xrightarrow{b^{-1}} & \overline{x} & \xrightarrow{b^{-1}} & \overline{y} & \xrightarrow{b^{-1}} & \overline{x^5} \\
& \xrightarrow{b^{-1}} & \overline{x^4y} & \xrightarrow{a} & \overline{xy^4} & \xrightarrow{b^{-1}} & \overline{y^2} & \xrightarrow{b^{-1}} & \overline{x^5y^4} & \xrightarrow{b^{-1}} & \overline{x^4y^2} \\
& \xrightarrow{b^{-1}} & \overline{x^3y^4} & \xrightarrow{b^{-1}} & \overline{x^2y^2} & \xrightarrow{a} & \overline{x^5y^3} & \xrightarrow{b^{-1}} & \overline{x^4y^3} & \xrightarrow{b^{-1}} & \overline{x^3y^3} \\
& \xrightarrow{b^{-1}} & \overline{x^2y^3} & \xrightarrow{b^{-1}} & \overline{xy^3} & \xrightarrow{b^{-1}} & \overline{y^3} & \xrightarrow{a} & \overline{x^3y^2} & \xrightarrow{b^{-1}} & \overline{x^2y^4} \\
& \xrightarrow{b^{-1}} & \overline{xy^2} & \xrightarrow{b^{-1}} & \overline{y^4} & \xrightarrow{b^{-1}} & \overline{x^5y^2} & \xrightarrow{b^{-1}} & \overline{x^4y^4} & \xrightarrow{a} & \overline{xy} \\
& \xrightarrow{b} & \overline{x^2} & \xrightarrow{b} & \overline{x^3y} & \xrightarrow{b} & \overline{x^4} & \xrightarrow{b} & \overline{x^5y} & \xrightarrow{b} & \overline{e}.
\end{array}$$

Calculating modulo the normal subgroup $\langle y \rangle$, its voltage is

$$\begin{aligned}
(ab^{-5})^4(ab^5) &= (ab)^4(ab^{-1}) && (b^6 = e) \\
&\equiv \big(x^3\,(xw)\big)^4 \big(x^3\,(xw)^{-1}\big) \\
&= \big(x^4 w\big)^4 \big((xw^{-1})^{-1}\,x^3\big) && (x^3 \text{ inverts } w) \\
&= \big(x^{16} w^{d^{12}+d^8+d^4+1}\big) \big((wx^{-1})\,x^3\big) \\
&= x^{-2} w^{1+d^2-d+2} x^2 && \begin{pmatrix} x^6 = e \text{ and} \\ d^3 \equiv -1 \pmod p) \end{pmatrix} \\
&= x^{-2} w^{d^2+2} x^2 \\
&= x^{-2} w^{d+1} x^2 && \big(d^2 - d + 1 \equiv 0 \pmod p\big),
\end{aligned}$$

which is nontrivial. Therefore, the voltage generates $\mathbb{Z}_p$, so the Factor Group Lemma (2.2) provides a hamiltonian cycle in $\mathrm{Cay}(G; S)$.

For (2), here is a hamiltonian cycle in $\mathrm{Cay}(G/\mathbb{Z}_p; S)$:

$$
\begin{array}{ccccccccccc}
\overline{e} & \xrightarrow{a} & \overline{x^5} & \xrightarrow{b} & \overline{x^6y} & \xrightarrow{b} & \overline{x^7} & \xrightarrow{b} & \overline{x^8y} & \xrightarrow{b} & \overline{x^9} \\
 & \xrightarrow{a} & \overline{x^4} & \xrightarrow{b} & \overline{x^5y} & \xrightarrow{a} & \overline{y^2} & \xrightarrow{b} & \overline{xy^2} & \xrightarrow{b} & \overline{x^2y^2} \\
 & \xrightarrow{b} & \overline{x^3y^2} & \xrightarrow{b} & \overline{x^4y^2} & \xrightarrow{a} & \overline{x^9y} & \xrightarrow{b^{-1}} & \overline{x^8} & \xrightarrow{b^{-1}} & \overline{x^7y} \\
 & \xrightarrow{b^{-1}} & \overline{x^6} & \xrightarrow{a} & \overline{x} & \xrightarrow{b^{-1}} & \overline{y} & \xrightarrow{a} & \overline{x^5y^2} & \xrightarrow{b} & \overline{x^6y^2} \\
 & \xrightarrow{b} & \overline{x^7y^2} & \xrightarrow{a} & \overline{x^2y} & \xrightarrow{b} & \overline{x^3} & \xrightarrow{b} & \overline{x^4y} & \xrightarrow{a} & \overline{x^9y^2} \\
 & \xrightarrow{b^{-1}} & \overline{x^8y^2} & \xrightarrow{a} & \overline{x^3y} & \xrightarrow{b^{-1}} & \overline{x^2} & \xrightarrow{b^{-1}} & \overline{xy} & \xrightarrow{b^{-1}} & \overline{e}.
\end{array}
$$

Calculating modulo $\langle y \rangle$, its voltage is

$$
\begin{aligned}
&ab^4(aba)b^4(ab^{-3}a)b^{-1}(ab^2)^2(ab^{-1}a)b^{-3} \\
&\qquad \equiv x^5(xw)^4\big(x^5(xw)x^5\big)(xw)^4\big(x^5(xw)^{-3}x^5\big) \\
&\qquad\qquad \cdot (xw)^{-1}\big(x^5(xw)^2\big)^2\big(x^5(xw)^{-1}x^5\big)(xw)^{-3} \\
&\qquad = x^5(xw)^4\big(xw^{-1}\big)(xw)^4\big(xw^{-1}\big)^{-3} \\
&\qquad\qquad \cdot (xw)^{-1}\big((xw^{-1})^2(xw)^2\big)\big(xw^{-1}\big)^{-1}(xw)^{-3} \\
&\qquad = x^5(x^4w^{d^3+d^2+d+1})\big(xw^{-1}\big)(x^4w^{d^3+d^2+d+1})\big(w^{d^2+d+1}x^{-3}\big) \\
&\qquad\qquad \cdot (w^{-1}x^{-1})\big(x^4w^{-d^3-d^2+d+1}\big)\big(wx^{-1}\big)(w^{-(d^2+d+1)}x^{-3}) \\
&\qquad = w^{d(d^3+d^2+d+1)}w^{-1}w^{d^6(d^3+d^2+d+1)}w^{d^6(d^2+d+1)} \\
&\qquad\qquad \cdot w^{-d^9}w^{d^6(-d^3-d^2+d+1)}w^{d^6}w^{-d^7(d^2+d+1)} \\
&\qquad = w^{-2d^9+2d^7+4d^6+d^4+d^3+d^2+d-1}.
\end{aligned}
$$

Modulo p, the exponent of w is:

$$
\begin{aligned}
&-2d^9 + 2d^7 + 4d^6 + d^4 + d^3 + d^2 + d - 1 \\
&\qquad \equiv 2d^4 - 2d^2 - 4d + d^4 + d^3 + d^2 + d - 1 \qquad\qquad (\text{because } d^5 \equiv -1) \\
&\qquad = 3d^4 + d^3 - d^2 - 3d - 1 \\
&\qquad = 3(d^4 - d^3 + d^2 - d + 1) + 4(d^3 - d^2 - 1) \\
&\qquad \equiv 3(0) + 4(d^3 - d^2 - 1) \\
&\qquad = 4(d^3 - d^2 - 1).
\end{aligned}
$$

This is nonzero (mod p), because $d^4 - d^3 + d^2 - d + 1 \equiv 0 \pmod{p}$ and

$$(d^3 - d^2)(d^3 - d^2 - 1) - (d^2 - d - 1)(d^4 - d^3 + d^2 - d + 1) = 1.$$

Therefore the voltage generates $\langle w \rangle = \mathbb{Z}_p$, so the Factor Group Lemma (2.2) applies.

Subsubcase 1.2.2. *Assume a and b both have order $2r$ in G/G'.* Then $|a| = |b| = 2r$ (because $\mathbb{Z}_{2r}$ has trivial centralizer in $\mathbb{Z}_{pq}$). (note A.17)

We have $a \in b^i G'$ for some i with $\gcd(i, 2r) = 1$. We may assume $1 \le i < r$ by replacing a with its inverse if necessary. Here is a hamiltonian cycle in $\mathrm{Cay}(G/G'; S)$: (note A.18)

$$\big((a, b, a^{-1}, b)^{(i-1)/2}, a, b^{2r+1-2i}\big).$$

To calculate its voltage, write $a = b^i y w$, where $\langle y \rangle = \mathbb{Z}_q$ and $\langle w \rangle = \mathbb{Z}_p$. We have $y^b = y^{-1}$ and $w^b = w^d$, where d is a primitive r^{th} or $(2r)^{\text{th}}$ root of unity in $\mathbb{Z}_p$. Then the voltage of the walk is: (note A.19)

$$\begin{aligned}
(aba^{-1}b)^{(i-1)/2}ab^{2r+1-2i} &= \big((b^i yw)b(b^i yw)^{-1}b\big)^{(i-1)/2}(b^i yw)b^{1-2i} \\
&= \big((b^i yw)b(w^{-1}y^{-1}b^{-i})b\big)^{(i-1)/2}(b^i yw)b^{1-2i} \\
&= \big(b^2 y^{-2} w^{(d-1)d^{1-i}}\big)^{(i-1)/2}(b^i yw)b^{1-2i} && \text{(note A.20)} \\
&= \big(b^{i-1} y^{-(i-1)} w^{(d-1)d^{1-i}(d^{i-3}+d^{i-5}+\cdots+d^2+1)}\big)(b^i yw)b^{1-2i} && \text{(note A.21)} \\
&= b^{2i-1} y^{(i-1)+1} w^{(d-1)d(d^{i-3}+d^{i-5}+\cdots+d^2+1)+1} b^{1-2i}. && \text{(note A.22)}
\end{aligned}$$

Now:

- The exponent of y is $(i-1)+1 = i$. If $q \mid i$, then, since $i < r$, we must have $q = 3$, $r = 5$, and $i = 3$. (note A.23)
- The exponent of w is

$$\begin{aligned}
(d-1)d(d^{i-3}+d^{i-5}+\cdots+d^2+1)+1 &= d(d-1)\frac{d^{i-1}-1}{d^2-1}+1 \\
&= d\frac{d^{i-1}-1}{d+1}+1 = \frac{d^i-d}{d+1}+\frac{d+1}{d+1} = \frac{d^i+1}{d+1}.
\end{aligned}$$

  This is not divisible by p, because d is a primitive r^{th} or $(2r)^{\text{th}}$ root of 1 in $\mathbb{Z}_p$, and $\gcd(i, 2r) = 1$.

Thus, the voltage generates G' (so the Factor Group Lemma (2.2) applies) unless $q = 3$, $r = 5$, and $i = 3$.

In this case, since $i = 3$, we have $a = b^3yw$. Also, we may assume $b = x$. Then a hamiltonian cycle in $\mathrm{Cay}(G/\mathbb{Z}_p; S)$ is:

$$\begin{array}{ccccccccccc}
\overline{e} & \xrightarrow{a^{-1}} & \overline{x^7y} & \xrightarrow{a^{-1}} & \overline{x^4} & \xrightarrow{a^{-1}} & \overline{xy} & \xrightarrow{a^{-1}} & \overline{x^8} & \xrightarrow{a^{-1}} & \overline{x^5y} \\
& \xrightarrow{a^{-1}} & \overline{x^2} & \xrightarrow{a^{-1}} & \overline{x^9y} & \xrightarrow{a^{-1}} & \overline{x^6} & \xrightarrow{a^{-1}} & \overline{x^3y} & \xrightarrow{b} & \overline{x^4y^2} \\
& \xrightarrow{a} & \overline{x^7y^2} & \xrightarrow{a} & \overline{y^2} & \xrightarrow{a} & \overline{x^3y^2} & \xrightarrow{a} & \overline{x^6y^2} & \xrightarrow{a} & \overline{x^9y^2} \\
& \xrightarrow{a} & \overline{x^2y^2} & \xrightarrow{a} & \overline{x^5y^2} & \xrightarrow{a} & \overline{x^8y^2} & \xrightarrow{a} & \overline{xy^2} & \xrightarrow{b} & \overline{x^2y} \\
& \xrightarrow{a} & \overline{x^5} & \xrightarrow{a} & \overline{x^8y} & \xrightarrow{a} & \overline{x} & \xrightarrow{a} & \overline{x^4y} & \xrightarrow{a} & \overline{x^7} \\
& \xrightarrow{a} & \overline{y} & \xrightarrow{a} & \overline{x^3} & \xrightarrow{a} & \overline{x^6y} & \xrightarrow{a} & \overline{x^9} & \xrightarrow{b} & \overline{e}.
\end{array}$$

Calculating modulo $\langle y \rangle$, and noting that $|a| = 2r = 10$, its voltage is

$$\begin{aligned} a^{-9}b(a^9b)^2 = ab(a^{-1}b)^2 &\equiv \big((x^3w)x\big)\big(w^{-1}x^{-2}\big)^2 \\ &= \big(x^4w^d\big)\big(w^{-1-d^2}x^{-4}\big) = x^4w^{-(d^2-d+1)}x^{-4}. \end{aligned}$$

Since d is a primitive 5^{th} or 10^{th} root of 1 in $\mathbb{Z}_p$, we know that it is not a primitive 6^{th} root of 1, so $d^2 - d + 1 \not\equiv 0 \pmod{p}$. Therefore the voltage is nontrivial, and hence generates $\mathbb{Z}_p$, so the Factor Group Lemma (2.2) applies.

Case 2. *Assume $\#S = 3$, and S remains minimal in $G/\mathbb{Z}_p = \overline{G}$.* Since $G = \mathbb{Z}_{2r} \ltimes \mathbb{Z}_{pq}$ and $\mathbb{Z}_r$ centralizes $\mathbb{Z}_q$, we know $\overline{G} \cong (\mathbb{Z}_2 \ltimes \mathbb{Z}_q) \times \mathbb{Z}_r$. Also, since $\mathbb{Z}_2$ inverts $\mathbb{Z}_q$, we have $\mathbb{Z}_2 \ltimes \mathbb{Z}_q \cong D_{2q}$. Therefore, $\overline{G} \cong D_{2q} \times \mathbb{Z}_r$, so we may write $S = \{a, b, c\}$ with $\langle \overline{a}, \overline{b} \rangle = D_{2q}$ and $\langle \overline{c} \rangle = \mathbb{Z}_r$. Since $S \cap G' = \emptyset$, we know that $\overline{a}$ and $\overline{b}$ are reflections, so they have order 2 in $G/\mathbb{Z}_p$. Therefore, we may assume $|a| = |b| = 2$, for otherwise Corollary 2.3 applies. Also, since $\mathbb{Z}_r$ does not centralize $\mathbb{Z}_p$, we know that $|c| = r$. Replacing c by a conjugate, we may assume $\langle c \rangle = \mathbb{Z}_r$. (note A.24) (note A.25)

We may assume $\mathbb{Z}_r \not\subset Z(G)$ (otherwise Lemma 2.9 applies), so we may assume $[a, c] \neq e$ (by interchanging a and b if necessary). Let (note A.26)

$$W = \big((b, a)^{q-1}, c, (c^{r-2}, a, c^{-(r-2)}, b)^{q-1}\big).$$

Then

$$\big(W, c^{r-2}, a, c^{-(r-1)}, a\big) \quad \text{and} \quad \big(W, c^{r-3}, a, c^{-(r-1)}, a, c\big)$$

are hamiltonian cycles in $\mathrm{Cay}(G/G'; S)$. Let v be the voltage of the first of (note A.27) these, and let $\gamma = [a,c]\,[a,c]^{ac}$. Then the voltage of the second is

$$\begin{aligned} v \cdot (c^{r-2} a c^{-(r-1)} a)^{-1} (c^{r-3} a c^{-(r-1)} a c) &= v \cdot \big(a c^{r-1} a c^{-(r-2)}\big)(c^{r-3} a c^{-(r-1)} a c) \\ &= v \cdot \big(a c^{-1} a c^{-1} a c a c\big) \\ &= v \cdot \big(a c^{-1} [a,c] a c\big) \\ &= v \cdot \big(a c^{-1} a c [a,c]^{ac}\big) \\ &= v \cdot \big([a,c]\,[a,c]^{ac}\big) \\ &= v\gamma. \end{aligned}$$

Since $[a,c]$ generates $\mathbb{Z}_p$, and ac does not invert $\mathbb{Z}_p$ (this is because a inverts $\mathbb{Z}_p$, and c does not centralize $\mathbb{Z}_p$), we know $\gamma \neq e$. Therefore v and $v\gamma$ cannot both be trivial, so at least one of them generates $\mathbb{Z}_p$. Then the Factor Group Lemma (2.2) provides a hamiltonian cycle in $\mathrm{Cay}(G; S)$.

Case 3. *Assume $\#S = 3$, and S does not remain minimal in $G/\mathbb{Z}_p$.* Choose a 2-element subset $\{a, b\}$ of S that generates $G/\mathbb{Z}_p$. As in Case 2, we have $G/\mathbb{Z}_p \cong D_{2q} \times \mathbb{Z}_r$. From the minimality of S, we see that $\langle a, b \rangle = D_{2q} \times \mathbb{Z}_r$ (up to a conjugate). The projection of $\{a, b\}$ to D_{2q} must be of the form (note A.28) $\{f, y\}$ or $\{f, fy\}$, where f is a reflection and y is a rotation. Thus, using z to denote a generator of $\mathbb{Z}_r$ (and noting that $y \notin S$, because $S \cap G' = \emptyset$), we see that $\{a, b\}$ must be of the form (note A.29)

1. $\{f, yz\}$, or
2. $\{f, fyz\}$, or
3. $\{fz, yz^{\ell}\}$, with $\ell \not\equiv 0 \pmod{r}$, or
4. $\{fz, fyz^{\ell}\}$, with $\ell \not\equiv 0 \pmod{r}$.

Let c be the final element of S. We may write

$$c = f^i y^j z^k w \quad \text{with} \;\; 0 \le i < 2, \;\; 0 \le j < q, \;\; \text{and} \;\; 0 \le k < r.$$

Note that, since $S \cap G' = \emptyset$, we know that i and k cannot both be 0. Let d be a primitive r^{th} root of unity in $\mathbb{Z}_p$, such that

$$w^z = w^d \text{ for } w \in \mathbb{Z}_p.$$

Subcase 3.1. *Assume $a = f$ and $b = yz$.* From the minimality of S, we know $\langle b, c \rangle \neq G$, so $i = 0$, so we must have $k \neq 0$. (note A.30)

Subsubcase 3.1.1. *Assume $k = 1$.* Then $b \equiv c \pmod{G'}$, so we have the hamiltonian cycles $(a, b^{-(r-1)}, a, b^{r-2}, c)$ and $(a, b^{-(r-1)}, a, b^{r-3}, c^2)$ in $\mathrm{Cay}(G/G'; S)$. The voltage of the first is

$$\begin{aligned} ab^{-(r-1)}ab^{r-2}c &= \big(ab^{-(r-1)}ab^{r-1}\big)\big(b^{-1}c\big) \\ &= \big((f)(yz)^{-(r-1)}(f)(yz)^{r-1}\big)\big((yz)^{-1}(y^j zw)\big) \\ &= \big(y^{2(r-1)}\big)\big(y^{j-1}w\big) && \text{(note A.31)} \\ &= \begin{cases} y^{j+3}w & \text{if } r = 3 \text{ and } q = 5, \\ y^{j+7}w & \text{if } r = 5 \text{ and } q = 3 \end{cases} \\ &= y^{j-2}w, && \text{(note A.32)} \end{aligned}$$

which generates $\mathbb{Z}_q \times \mathbb{Z}_p = G'$ if $j \neq 2$.

So we may assume $j = 2$ (for otherwise the Factor Group Lemma (2.2) applies). In this case, the voltage of the second hamiltonian cycle is

$$\begin{aligned} ab^{-(r-1)}ab^{r-3}c^2 &= \big(ab^{-(r-1)}ab^{r-1}\big)\big(b^{-2}c^2\big) \\ &= \big((f)(yz)^{-(r-1)}(f)(yz)^{r-1}\big)\big((yz)^{-2}(y^2 zw)^2\big) \\ &= \big(y^{2(r-1)}\big)\big(y^2 w^{d+1}\big) && \text{(note A.33)} \\ &= \begin{cases} y^6 w^{d+1} & \text{if } r = 3 \text{ and } q = 5, \\ y^{10} w^{d+1} & \text{if } r = 5 \text{ and } q = 3 \end{cases} \\ &= yw^{d+1}, && \text{(note A.34)} \end{aligned}$$

which generates $\mathbb{Z}_q \times \mathbb{Z}_p = G'$. So the Factor Group Lemma (2.2) provides a hamiltonian cycle in $\mathrm{Cay}(G; S)$. (note A.35)

Subsubcase 3.1.2. *Assume $k > 1$.* We may replace c with its inverse, so we may assume $k \leq (r-1)/2$. Therefore $r \neq 3$, so we must have $r = 5$ and $k = 2$. So $a = f$, $b = yz$, and $c = y^j z^2 w$.

Subsubsubcase 3.1.2.1. *Assume $j = 0$.* Here is a hamiltonian cycle in $\mathrm{Cay}(G/\mathbb{Z}_p; S)$:

$$
\begin{array}{ccccccccccc}
\overline{e} & \xrightarrow{a} & \overline{f} & \xrightarrow{b} & \overline{fyz} & \xrightarrow{a} & \overline{y^2z} & \xrightarrow{b} & \overline{z^2} & \xrightarrow{a} & \overline{fz^2} \\
 & \xrightarrow{b} & \overline{fyz^3} & \xrightarrow{a} & \overline{y^2z^3} & \xrightarrow{b} & \overline{z^4} & \xrightarrow{a} & \overline{fz^4} & \xrightarrow{b^{-1}} & \overline{fy^2z^3} \\
 & \xrightarrow{a} & \overline{yz^3} & \xrightarrow{b} & \overline{y^2z^4} & \xrightarrow{c^{-1}} & \overline{y^2z^2} & \xrightarrow{a} & \overline{fyz^2} & \xrightarrow{c} & \overline{fyz^4} \\
 & \xrightarrow{b^{-1}} & \overline{fz^3} & \xrightarrow{a} & \overline{z^3} & \xrightarrow{b} & \overline{yz^4} & \xrightarrow{a} & \overline{fy^2z^4} & \xrightarrow{c^{-1}} & \overline{fy^2z^2} \\
 & \xrightarrow{a} & \overline{yz^2} & \xrightarrow{c^{-1}} & \overline{y} & \xrightarrow{a} & \overline{fy^2} & \xrightarrow{b} & \overline{fz} & \xrightarrow{a} & \overline{z} \\
 & \xrightarrow{b^{-1}} & \overline{y^2} & \xrightarrow{a} & \overline{fy} & \xrightarrow{b} & \overline{fy^2z} & \xrightarrow{a} & \overline{yz} & \xrightarrow{b^{-1}} & \overline{e}.
\end{array}
$$

Letting $\epsilon \in \{\pm 1\}$, such that $w^f = w^\epsilon$, and calculating modulo $\langle y \rangle$, its voltage is

$$
\begin{aligned}
&(ab)^4(ab^{-1}ab)(c^{-1}ac)(b^{-1}ab)(ac^{-1})^2(abab^{-1})^2 \\
&\quad \equiv (fz)^4(fz^{-1}fz)(w^{-1}z^{-2}fz^2w)(z^{-1}fz)(fw^{-1}z^{-2})^2(fzfz^{-1})^2 \\
&\quad = (z^4)(e)(w^{\epsilon-1}f)(f)(w^{-(\epsilon+d^2)}z^{-4})(e) \qquad \text{(note A.36)} \\
&\quad = z^4 w^{-(d^2+1)} z^{-4}.
\end{aligned}
$$

Since d is a primitive 5^{th} root of unity in $\mathbb{Z}_p$, we know that $d^2+1 \not\equiv 0 \pmod{p}$, so the voltage is nontrivial, and hence generates $\mathbb{Z}_p$, so the Factor Group Lemma (2.2) applies.

Subsubsubcase 3.1.2.2. *Assume $j \neq 0$.* Since $\langle a, c \rangle \neq G$, this implies f centralizes $\mathbb{Z}_p$, so $G = D_6 \times (\mathbb{Z}_5 \ltimes \mathbb{Z}_p)$. (note A.37)

If $j = 1$ (so $c = yz^2w$), here is a hamiltonian cycle in $\mathrm{Cay}(G/\mathbb{Z}_p; S)$:

$$
\begin{array}{ccccccccccc}
\overline{e} & \xrightarrow{a} & \overline{f} & \xrightarrow{b} & \overline{fyz} & \xrightarrow{a} & \overline{y^2z} & \xrightarrow{b} & \overline{z^2} & \xrightarrow{a} & \overline{fz^2} \\
 & \xrightarrow{b} & \overline{fyz^3} & \xrightarrow{a} & \overline{y^2z^3} & \xrightarrow{b} & \overline{z^4} & \xrightarrow{b} & \overline{y} & \xrightarrow{a} & \overline{fy^2} \\
 & \xrightarrow{b} & \overline{fz} & \xrightarrow{a} & \overline{z} & \xrightarrow{b^{-1}} & \overline{y^2} & \xrightarrow{a} & \overline{fy} & \xrightarrow{b} & \overline{fy^2z} \\
 & \xrightarrow{a} & \overline{yz} & \xrightarrow{b} & \overline{y^2z^2} & \xrightarrow{a} & \overline{fyz^2} & \xrightarrow{c} & \overline{fy^2z^4} & \xrightarrow{a} & \overline{yz^4} \\
 & \xrightarrow{b^{-1}} & \overline{z^3} & \xrightarrow{a} & \overline{fz^3} & \xrightarrow{b} & \overline{fyz^4} & \xrightarrow{a} & \overline{y^2z^4} & \xrightarrow{b^{-1}} & \overline{yz^3} \\
 & \xrightarrow{a} & \overline{fy^2z^3} & \xrightarrow{b} & \overline{fz^4} & \xrightarrow{c^{-1}} & \overline{fy^2z^2} & \xrightarrow{a} & \overline{yz^2} & \xrightarrow{c^{-1}} & \overline{e}.
\end{array}
$$

Calculating modulo the normal subgroup $D_6 = \langle f, y \rangle$, its voltage is

$$\begin{aligned}
&(ab)^4(ba)^2(b^{-1}a)(ba)^2(c)(ab^{-1}ab)^2(c^{-1}ac^{-1}) \\
&\qquad \equiv (ez)^4(ze)^2(z^{-1}e)(ze)^2(z^2w)(ez^{-1}ez)^2(w^{-1}z^{-2}ew^{-1}z^{-2}) \\
&\qquad = z^7w^{-1}z^{-2} \\
&\qquad = z^2w^{-1}z^{-2},
\end{aligned}$$

because $|z| = r = 5$. Since this voltage generates $\mathbb{Z}_p$, the Factor Group Lemma (2.2) provides a hamiltonian cycle in $\mathrm{Cay}(G; S)$.

If $j = 2$ (so $c = y^2z^2w$), here is a hamiltonian cycle in $\mathrm{Cay}(G/\mathbb{Z}_p; S)$:

$$\begin{array}{ccccccccccc}
\overline{e} & \xrightarrow{b^{-1}} & \overline{y^2z^4} & \xrightarrow{a} & \overline{fyz^4} & \xrightarrow{b} & \overline{fy^2} & \xrightarrow{b} & \overline{fz} & \xrightarrow{a} & \overline{z} \\
& \xrightarrow{b} & \overline{yz^2} & \xrightarrow{a} & \overline{fy^2z^2} & \xrightarrow{b} & \overline{fz^3} & \xrightarrow{a} & \overline{z^3} & \xrightarrow{c} & \overline{y^2} \\
& \xrightarrow{b^{-1}} & \overline{yz^4} & \xrightarrow{a} & \overline{fy^2z^4} & \xrightarrow{b} & \overline{f} & \xrightarrow{b} & \overline{fyz} & \xrightarrow{a} & \overline{y^2z} \\
& \xrightarrow{b} & \overline{z^2} & \xrightarrow{a} & \overline{fz^2} & \xrightarrow{b} & \overline{fyz^3} & \xrightarrow{a} & \overline{y^2z^3} & \xrightarrow{c} & \overline{y} \\
& \xrightarrow{b^{-1}} & \overline{z^4} & \xrightarrow{a} & \overline{fz^4} & \xrightarrow{b} & \overline{fy} & \xrightarrow{b} & \overline{fy^2z} & \xrightarrow{a} & \overline{yz} \\
& \xrightarrow{b} & \overline{y^2z^2} & \xrightarrow{a} & \overline{fyz^2} & \xrightarrow{b} & \overline{fy^2z^3} & \xrightarrow{a} & \overline{yz^3} & \xrightarrow{c} & \overline{e}.
\end{array}$$

Calculating modulo the normal subgroup $D_6 = \langle f, y \rangle$, its voltage is

$$\big(b^{-1}ab^2(ab)^2(ac)\big)^3 \equiv \big(z^{-1}ez^2(ez)^2(ez^2w)\big)^3 = \big(z^5w\big)^3 = w^3,$$

because $|z| = r = 5$. Since this voltage generates $\mathbb{Z}_p$, the Factor Group Lemma (2.2) provides a hamiltonian cycle in $\mathrm{Cay}(G; S)$.

Subcase 3.2. *Assume $a = f$ and $b = fyz$.* Since $\langle b, c \rangle \neq G$, we must have $c \in \langle fy, z \rangle w$, so (note A.38)

$$c = (fy)^i z^k w \quad \text{with} \quad 0 \le i < 2 \quad \text{and} \quad 0 \le k < r.$$

Subsubcase 3.2.1. *Assume $k = 0$.* Then $c = fyw$, so we have $c \equiv a \pmod{G'}$. Therefore $(b^{-(r-1)}, a, b^{r-1}, c)$ is a hamiltonian cycle in $\mathrm{Cay}(G/G'; S)$. Since

$$b^{r-1} = (fyz)^{r-1} = (fy)^{r-1}(z^{r-1}) = (e)(z^{-1}) = z^{-1}, \qquad \text{(note A.39)}$$

its voltage is

$$b^{-(r-1)}ab^{r-1}c = (b^{-(r-1)}ab^{r-1}a)(ac) = [b^{r-1}, a](ac) = [z^{-1}, f](yw) = yw,$$

which generates $\mathbb{Z}_q \times \mathbb{Z}_p = G'$, so the Factor Group Lemma (2.2) provides a hamiltonian cycle in $\mathrm{Cay}(G; S)$.

Subsubcase 3.2.2. *Assume $i = 0$.* Then $c = z^k w$, and we know $k \neq 0$, because $S \cap G' = \emptyset$.

If $k = 1$, then $\big((a, c)^{r-1}, a, b\big)$ is a hamiltonian cycle in $\mathrm{Cay}(G/G'; S)$. (note A.40) Letting $\epsilon \in \{\pm 1\}$, such that $w^f = w^\epsilon$, its voltage is

$$\begin{aligned}
(ac)^{r-1}\, a\, b &= (ac)^r\, (c^{-1}\, b) && \text{(note A.41)}\\
&= (fzw)^r \big((zw)^{-1}(fyz)\big)\\
&= \big(f^r z^r w^{(\epsilon d)^{r-1} + (\epsilon d)^{r-2} + \cdots + 1}\big)\big(w^{-1} z^{-1} fyz\big) && \text{(note A.42)}\\
&= f\, w^{(\epsilon d)^{r-1} + (\epsilon d)^{r-2} + \cdots + \epsilon d}\, fy && \text{(note A.43)}\\
&= w^{\epsilon((\epsilon d)^{r-1} + (\epsilon d)^{r-2} + \cdots + \epsilon d)} y\\
&= w^{d((\epsilon d)^{r-2} + (\epsilon d)^{r-3} + \cdots + 1)} y.
\end{aligned}$$

Since ϵd is a primitive r^{th} or $(2r)^{\text{th}}$ root of unity in $\mathbb{Z}_p$, it is clear that the exponent of w is nonzero (mod p). Therefore the voltage generates $\mathbb{Z}_p \times$ (note A.44) $\mathbb{Z}_q = G'$, so the Factor Group Lemma (2.2) provides a hamiltonian cycle in $\mathrm{Cay}(G; S)$.

We may now assume $k \geq 2$. However, we may also assume $k \leq (r-1)/2$ (by replacing c with its inverse if necessary). So $r = 5$ and $k = 2$. In this case, here is a hamiltonian cycle in $\mathrm{Cay}(G/\mathbb{Z}_p; S)$:

$$\begin{array}{ccccccccccc}
\overline{e} & \xrightarrow{a} & \overline{f} & \xrightarrow{b} & \overline{fyz} & \xrightarrow{a} & \overline{y^2z} & \xrightarrow{b^{-1}} & \overline{y} & \xrightarrow{a} & \overline{fy^2}\\
 & \xrightarrow{b} & \overline{fz} & \xrightarrow{a} & \overline{z} & \xrightarrow{b^{-1}} & \overline{y^2} & \xrightarrow{a} & \overline{fy} & \xrightarrow{b} & \overline{fy^2z}\\
 & \xrightarrow{a} & \overline{yz} & \xrightarrow{b} & \overline{y^2z^2} & \xrightarrow{a} & \overline{fyz^2} & \xrightarrow{b} & \overline{fy^2z^3} & \xrightarrow{a} & \overline{yz^3}\\
 & \xrightarrow{b} & \overline{y^2z^4} & \xrightarrow{a} & \overline{fyz^4} & \xrightarrow{b^{-1}} & \overline{fz^3} & \xrightarrow{a} & \overline{z^3} & \xrightarrow{b} & \overline{yz^4}\\
 & \xrightarrow{c^{-1}} & \overline{yz^2} & \xrightarrow{a} & \overline{fy^2z^2} & \xrightarrow{c} & \overline{fy^2z^4} & \xrightarrow{b^{-1}} & \overline{fyz^3} & \xrightarrow{a} & \overline{y^2z^3}\\
 & \xrightarrow{b} & \overline{z^4} & \xrightarrow{a} & \overline{fz^4} & \xrightarrow{c^{-1}} & \overline{fz^2} & \xrightarrow{a} & \overline{z^2} & \xrightarrow{c^{-1}} & \overline{e}.
\end{array}$$

Its voltage is

$$(abab^{-1})^2(ab)^4(ab^{-1}ab)(c^{-1}ac)(b^{-1}ab)(ac^{-1})^2.$$

Since the voltage is in $\mathbb{Z}_p$, it is a power of w, and it is clear that the only terms that contribute a power of w to the product are contained in the last three parenthesized expressions (because c does not appear anywhere else). Choosing $\epsilon \in \{\pm 1\}$, such that $w^f = w^\epsilon$, we calculate the product of these three expressions modulo $\langle y \rangle$:

$$\begin{aligned}(c^{-1}ac)(b^{-1}ab)(ac^{-1})^2 &\equiv \big((z^2w)^{-1}f(z^2w)\big)\big((fz)^{-1}f(fz)\big)\big(f(z^2w)^{-1}\big)^2 \\ &= \big(w^{\epsilon-1}f\big)\big(f\big)\big(w^{-(\epsilon+d^2)}z^{-4}\big) \\ &= w^{-(d^2+1)}z^{-4}\end{aligned}$$ (note A.45)

Since the power of w is nonzero, the voltage generates $\mathbb{Z}_p$, so the Factor Group Lemma (2.2) provides a hamiltonian cycle in $\mathrm{Cay}(G; S)$.

Subsubcase 3.2.3. *Assume i and k are both nonzero.* Since $\langle a, c\rangle \neq G$, this implies that f centralizes w. Therefore $G = D_{2q} \times (\mathbb{Z}_r \ltimes \mathbb{Z}_p)$. Also, (note A.46) since $0 \leq i < 2$, we know $i = 1$, so $c = fyz^k w$. We may assume $k \neq 1$ (for otherwise $b \equiv c \pmod{\mathbb{Z}_p}$, so Corollary 2.3 applies). Since we may also assume that $k \leq (r-1)/2$ (by replacing c with its inverse if necessary), then we have $r = 5$ and $k = 2$.

Here is a hamiltonian cycle in $\mathrm{Cay}(G/\mathbb{Z}_p; S)$:

$$\begin{array}{ccccccccccccc}
\overline{e} & \xrightarrow{a} & \overline{f} & \xrightarrow{b} & \overline{yz} & \xrightarrow{a} & \overline{fy^2z} & \xrightarrow{b} & \overline{y^2z^2} & \xrightarrow{a} & \overline{fyz^2} \\
 & \xrightarrow{c} & \overline{z^4} & \xrightarrow{a} & \overline{fz^4} & \xrightarrow{b^{-1}} & \overline{yz^3} & \xrightarrow{a} & \overline{fy^2z^3} & \xrightarrow{c} & \overline{y^2} \\
 & \xrightarrow{a} & \overline{fy} & \xrightarrow{b} & \overline{z} & \xrightarrow{a} & \overline{fz} & \xrightarrow{b} & \overline{yz^2} & \xrightarrow{a} & \overline{fy^2z^2} \\
 & \xrightarrow{c} & \overline{y^2z^4} & \xrightarrow{a} & \overline{fyz^4} & \xrightarrow{b^{-1}} & \overline{z^3} & \xrightarrow{a} & \overline{fz^3} & \xrightarrow{c} & \overline{y} \\
 & \xrightarrow{a} & \overline{fy^2} & \xrightarrow{b} & \overline{y^2z} & \xrightarrow{a} & \overline{fyz} & \xrightarrow{b} & \overline{z^2} & \xrightarrow{a} & \overline{fz^2} \\
 & \xrightarrow{c} & \overline{yz^4} & \xrightarrow{a} & \overline{fy^2z^4} & \xrightarrow{b^{-1}} & \overline{y^2z^3} & \xrightarrow{a} & \overline{fyz^3} & \xrightarrow{c} & \overline{e}.
\end{array}$$

Calculating modulo the normal subgroup $D_6 = \langle f, y\rangle$, its voltage is

$$\begin{aligned}\big((ab)^2acab^{-1}ac\big)^3 &\equiv \big((ez)^2e(z^2w)ez^{-1}e(z^2w)\big)^3 \\ &= \big(z^4wzw\big)^3 \\ &= w^{3(d+1)},\end{aligned}$$ (note A.47)

which generates $\langle w\rangle = \mathbb{Z}_p$, so the Factor Group Lemma (2.2) applies. (note A.48)

Subcase 3.3. *Assume $a = fz$ and $b = yz^\ell$, with $\ell \neq 0$.* Since $\langle a, c\rangle \neq G$ and $\langle b, c\rangle \neq G$, we must have $c \in \langle f, z\rangle w$ and $c \in \langle y, z\rangle w$. So $c \in \langle z\rangle w$; write (note A.49)

$c = z^k w$ (with $k \neq 0$, because $S \cap G' = \emptyset$).

Subsubcase 3.3.1. *Assume $\ell = k$.* Then $b \equiv c \equiv z^\ell \pmod{G'}$, so

$$\left(a^{-1}, b^{-(r-1)}, a, b^{r-2}, c\right)$$

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

$$\begin{aligned} a^{-1}b^{-(r-1)}ab^{r-2}c &= (fz)^{-1}(yz^\ell)^{-(r-1)}(fz)(yz^\ell)^{r-2}(z^\ell w) \\ &= (f^{-1}y^{-(r-1)}f)y^{r-2}w && \begin{pmatrix} z \text{ commutes} \\ \text{with } f \text{ and } y \end{pmatrix} \\ &= (y^{r-1})y^{r-2}w && (f \text{ inverts } y) \\ &= y^{2r-3}w. \end{aligned}$$

Since $2(3) - 3 \not\equiv 0 \pmod 5$ and $2(5) - 3 \not\equiv 0 \pmod 3$, we have $2r - 3 \not\equiv 0 \pmod q$, so y^{2r-3} is nontrivial, and hence generates $\mathbb{Z}_q$. Therefore, this voltage generates $\mathbb{Z}_q \times \mathbb{Z}_p = G'$. So the Factor Group Lemma (2.2) provides a hamiltonian cycle in $\mathrm{Cay}(G; S)$.

Subsubcase 3.3.2. *Assume $\ell \neq k$.* We may assume $\ell, k \leq (r-1)/2$ (perhaps after replacing b and/or c by their inverses). Then we must have $r = 5$ and $\{\ell, k\} = \{1, 2\}$. (note A.50)

For $(\ell, k) = (1, 2)$, here is a hamiltonian cycle in $\mathrm{Cay}(G/\mathbb{Z}_p; S)$:

$$\begin{array}{ccccccccccc}
\overline{e} & \xrightarrow{a} & \overline{fz} & \xrightarrow{b} & \overline{fyz^2} & \xrightarrow{a^{-1}} & \overline{y^2z} & \xrightarrow{a^{-1}} & \overline{fy} & \xrightarrow{b^{-1}} & \overline{fz^4} \\
 & \xrightarrow{a^{-1}} & \overline{z^3} & \xrightarrow{a^{-1}} & \overline{fz^2} & \xrightarrow{a^{-1}} & \overline{z} & \xrightarrow{a^{-1}} & \overline{f} & \xrightarrow{b^{-1}} & \overline{fy^2z^4} \\
 & \xrightarrow{a} & \overline{y} & \xrightarrow{a} & \overline{fy^2z} & \xrightarrow{a} & \overline{yz^2} & \xrightarrow{a} & \overline{fy^2z^3} & \xrightarrow{a} & \overline{yz^4} \\
 & \xrightarrow{a} & \overline{fy^2} & \xrightarrow{a} & \overline{yz} & \xrightarrow{a} & \overline{fy^2z^2} & \xrightarrow{a} & \overline{yz^3} & \xrightarrow{b} & \overline{y^2z^4} \\
 & \xrightarrow{a^{-1}} & \overline{fyz^3} & \xrightarrow{a^{-1}} & \overline{y^2z^2} & \xrightarrow{a^{-1}} & \overline{fyz} & \xrightarrow{a^{-1}} & \overline{y^2} & \xrightarrow{a^{-1}} & \overline{fyz^4} \\
 & \xrightarrow{a^{-1}} & \overline{y^2z^3} & \xrightarrow{b} & \overline{z^4} & \xrightarrow{a^{-1}} & \overline{fz^3} & \xrightarrow{a^{-1}} & \overline{z^2} & \xrightarrow{c^{-1}} & \overline{e}.
\end{array}$$

Its voltage is

$$aba^{-2}b^{-1}a^{-4}b^{-1}a^{9}ba^{-6}ba^{-2}c^{-1}.$$

Since there is precisely one occurrence of c in this product, and therefore only one occurrence of w, it is impossible for this appearance of w to cancel. So the voltage is nontrivial, and therefore generates $\mathbb{Z}_p$, so the Factor Group Lemma (2.2) provides a hamiltonian cycle in $\mathrm{Cay}(G; S)$.

For $(\ell, k) = (2, 1)$, here is a hamiltonian cycle in $\mathrm{Cay}(G/\mathbb{Z}_p; S)$:

$$\begin{array}{cccccccccccc}
\overline{e} & \xrightarrow{a^{-1}} & \overline{fz^4} & \xrightarrow{a^{-1}} & \overline{z^3} & \xrightarrow{a^{-1}} & \overline{fz^2} & \xrightarrow{a^{-1}} & \overline{z} & \xrightarrow{a^{-1}} & \overline{f} \\
 & \xrightarrow{a^{-1}} & \overline{z^4} & \xrightarrow{b} & \overline{yz} & \xrightarrow{a^{-1}} & \overline{fy^2} & \xrightarrow{a^{-1}} & \overline{yz^4} & \xrightarrow{c} & \overline{y} \\
 & \xrightarrow{a^{-1}} & \overline{fy^2z^4} & \xrightarrow{a^{-1}} & \overline{yz^3} & \xrightarrow{a^{-1}} & \overline{fy^2z^2} & \xrightarrow{c} & \overline{fy^2z^3} & \xrightarrow{a^{-1}} & \overline{yz^2} \\
 & \xrightarrow{a^{-1}} & \overline{fy^2z} & \xrightarrow{b} & \overline{fz^3} & \xrightarrow{a^{-1}} & \overline{z^2} & \xrightarrow{a^{-1}} & \overline{fz} & \xrightarrow{b} & \overline{fyz^3} \\
 & \xrightarrow{a^{-1}} & \overline{y^2z^2} & \xrightarrow{a^{-1}} & \overline{fyz} & \xrightarrow{c} & \overline{fyz^2} & \xrightarrow{a^{-1}} & \overline{y^2z} & \xrightarrow{a^{-1}} & \overline{fy} \\
 & \xrightarrow{a^{-1}} & \overline{y^2z^4} & \xrightarrow{c} & \overline{y^2} & \xrightarrow{a^{-1}} & \overline{fyz^4} & \xrightarrow{a^{-1}} & \overline{y^2z^3} & \xrightarrow{b} & \overline{e}.
\end{array}$$

Choosing $\epsilon \in \{\pm 1\}$, such that $w^f = w^\epsilon$, we calculate the voltage, modulo $\langle y \rangle$:

$$\begin{aligned}
&a^{-4}\Big(\big(a^{-2}ba^{-2}\big)ca^{-3}c\big(a^{-2}b\big)\Big)^2 \\
&\quad \equiv (fz)^{-4}\Big(\big((fz)^{-2}z^2(fz)^{-2}\big)(zw)(fz)^{-3}(zw)\big((fz)^{-2}z^2\big)\Big)^2 \\
&\quad = z^{-4}\big((z^{-2})(zw)(fz^{-3})(zw)(e)\big)^2 && \text{(note A.51)} \\
&\quad = z^{-4}\big(z^{-1}wfz^{-2}w\big)^2 \\
&\quad = z^{-4}\big(w^{d^6+\epsilon d^4+\epsilon d^3+d}z^{-6}\big) && \text{(note A.52)} \\
&\quad = z^{-4}\big(w^{d(\epsilon d^3+\epsilon d^2+2)}z^4\big). && \text{(note A.53)}
\end{aligned}$$

Since d is a primitive r^{th} root of unity in $\mathbb{Z}_p$, and $r = 5$, we know $d^4 + d^3 + d^2 + d + 1 \equiv 0 \pmod 5$. Combining this with the fact that

$$-(d^3 + d^2 - 1)(d^3 + d^2 + 2) + (d^2 + d - 1)(d^4 + d^3 + d^2 + d + 1) = 1,$$

and

$$(d^3+d^2+3)(-d^3+-d^2+2)+(d^2+d-1)(d^4+d^3+d^2+d+1) = 5 \not\equiv 0 \pmod p,$$

we see that $\epsilon d^3 + \epsilon d^2 + 2$ is nonzero in $\mathbb{Z}_p$. Therefore the voltage is nontrivial, so it generates $\mathbb{Z}_p$. Hence, the Factor Group Lemma (2.2) provides a hamiltonian cycle in $\mathrm{Cay}(G; S)$.

Subcase 3.4. *Assume $a = fz$ and $b = fyz^\ell$, with $\ell \neq 0$.* Since $\langle a, c\rangle \neq G$ and $\langle b, c\rangle \neq G$, we must have $c \in \langle f, z\rangle w$ and $c \in \langle fy, z\rangle w$. So $c \in \langle z\rangle w$; (note A.54) write $c = z^k w$ (with $k \neq 0$ because $S \cap G' = \emptyset$).

We may assume $k, \ell \leq (r-1)/2$, by replacing either or both of b and c with their inverses if necessary. We may also assume $\ell \neq 1$, for otherwise $a \equiv b \pmod{\langle y \rangle}$, so Corollary 2.3 applies. Therefore, we must have $r = 5$ (note A.55) and $\ell = 2$. We also have $k \in \{1, 2\}$.

For $k = 1$, here is a hamiltonian cycle in $\mathrm{Cay}(G/\mathbb{Z}_p; S)$:

$$
\begin{array}{ccccccccccc}
\overline{e} & \xrightarrow{a} & \overline{fz} & \xrightarrow{b^{-1}} & \overline{yz^4} & \xrightarrow{a^{-1}} & \overline{fy^2z^3} & \xrightarrow{a^{-1}} & \overline{yz^2} & \xrightarrow{b} & \overline{fz^4} \\
& \xrightarrow{a^{-1}} & \overline{z^3} & \xrightarrow{a^{-1}} & \overline{fz^2} & \xrightarrow{a^{-1}} & \overline{z} & \xrightarrow{a^{-1}} & \overline{f} & \xrightarrow{b^{-1}} & \overline{yz^3} \\
& \xrightarrow{a} & \overline{fy^2z^4} & \xrightarrow{a} & \overline{y} & \xrightarrow{a} & \overline{fy^2z} & \xrightarrow{c^{-1}} & \overline{fy^2} & \xrightarrow{a} & \overline{yz} \\
& \xrightarrow{a} & \overline{fy^2z^2} & \xrightarrow{b} & \overline{y^2z^4} & \xrightarrow{a^{-1}} & \overline{fyz^3} & \xrightarrow{a^{-1}} & \overline{y^2z^2} & \xrightarrow{a^{-1}} & \overline{fyz} \\
& \xrightarrow{a^{-1}} & \overline{y^2} & \xrightarrow{a^{-1}} & \overline{fyz^4} & \xrightarrow{a^{-1}} & \overline{y^2z^3} & \xrightarrow{a^{-1}} & \overline{fyz^2} & \xrightarrow{a^{-1}} & \overline{y^2z} \\
& \xrightarrow{a^{-1}} & \overline{fy} & \xrightarrow{b} & \overline{z^2} & \xrightarrow{a} & \overline{fz^3} & \xrightarrow{a} & \overline{z^4} & \xrightarrow{c} & \overline{e}.
\end{array}
$$

Its voltage is

$$ab^{-1}a^{-2}ba^{-4}b^{-1}a^3c^{-1}a^2ba^{-9}ba^2c$$

Calculating modulo y, the product between the occurrence of c^{-1} and the occurrence of c is

$$a^2ba^{-9}ba^2 \equiv (fz)^2(fz^2)(fz)^{-9}(fz^2)(fz)^2 = z^{-1}, \qquad \text{(note A.51)}$$

which does not centralize w. So the occurrence of w^{-1} in c^{-1} does not cancel the occurrence of w in c. Therefore the voltage is nontrivial, so it generates $\mathbb{Z}_p$, so the Factor Group Lemma (2.2) applies.

For $k = 2$, here is a hamiltonian cycle in $\mathrm{Cay}(G/\mathbb{Z}_p; S)$:

$$
\begin{array}{ccccccccccc}
\overline{e} & \xrightarrow{a} & \overline{fz} & \xrightarrow{b} & \overline{yz^3} & \xrightarrow{b} & \overline{f} & \xrightarrow{a} & \overline{z} & \xrightarrow{a} & \overline{fz^2} \\
& \xrightarrow{a} & \overline{z^3} & \xrightarrow{a} & \overline{fz^4} & \xrightarrow{b^{-1}} & \overline{yz^2} & \xrightarrow{a} & \overline{fy^2z^3} & \xrightarrow{a} & \overline{yz^4} \\
& \xrightarrow{a} & \overline{fy^2} & \xrightarrow{a} & \overline{yz} & \xrightarrow{a} & \overline{fy^2z^2} & \xrightarrow{c} & \overline{fy^2z^4} & \xrightarrow{a} & \overline{y} \\
& \xrightarrow{a} & \overline{fy^2z} & \xrightarrow{b} & \overline{y^2z^3} & \xrightarrow{a} & \overline{fyz^4} & \xrightarrow{a} & \overline{y^2} & \xrightarrow{a} & \overline{fyz} \\
& \xrightarrow{a} & \overline{y^2z^2} & \xrightarrow{a} & \overline{fyz^3} & \xrightarrow{a} & \overline{y^2z^4} & \xrightarrow{a} & \overline{fy} & \xrightarrow{a} & \overline{y^2z} \\
& \xrightarrow{a} & \overline{fyz^2} & \xrightarrow{b} & \overline{z^4} & \xrightarrow{a^{-1}} & \overline{fz^3} & \xrightarrow{a^{-1}} & \overline{z^2} & \xrightarrow{c^{-1}} & \overline{e}.
\end{array}
$$

Its voltage is

$$ab^2a^4b^{-1}a^5ca^2ba^9ba^{-2}c^{-1}.$$

Calculating modulo y, the product between the occurrence of c and the occurrence of c^{-1} is

$$a^2ba^9ba^{-2} \equiv (fz)^2(fz^2)(fz)^9(fz^2)(fz)^{-2} = fz^{13} = fz^3,$$ (note A.56)

which does not centralize w. So the occurrence of w^{-1} in c^{-1} does not cancel the occurrence of w in c. Therefore the voltage is nontrivial, so it generates $\mathbb{Z}_p$, so the Factor Group Lemma (2.2) applies. (note A.57)

Case 4. *Assume* $\#S \geq 4$. Write $S = \{s_1, s_2, \ldots, s_\ell\}$, and let $G_i = \langle s_1, \ldots, s_i \rangle$ for $i = 1, 2, \ldots, \ell$. Since S is minimal, we know

$$\{e\} \subsetneq G_1 \subsetneq G_2 \subsetneq \cdots \subsetneq G_\ell \subseteq G.$$

Therefore, the number of prime factors of $|G_i|$ is at least i. Since $|G| = 30p$ is the product of only 4 primes, and $\ell = \#S \geq 4$, we conclude that $|G_i|$ has exactly i prime factors, for all i. (In particular, we must have $\#S = 4$.) By permuting the elements of $\{s_1, s_2, \ldots, s_\ell\}$, this implies that if S_0 is any subset of S, then $|\langle S_0 \rangle|$ is the product of exactly $\#S_0$ primes. In particular, by letting $\#S_0 = 1$, we see that every element of S must have prime order.

Now, choose $\{a, b\} \subset S$ to be a 2-element generating set of $G/G' \cong \mathbb{Z}_2 \times \mathbb{Z}_r$. From the preceding paragraph, we see that we may assume $|a| = 2$ and $|b| = r$ (by interchanging a and b if necessary). Since $|\langle a, b \rangle|$ is the product of only two primes, we must have $|\langle a, b \rangle| = 2r$, so $\langle a, b \rangle \cong G/G'$. Therefore

$$G = \big(\langle a \rangle \times \langle b \rangle\big) \ltimes G'.$$

Since $\langle S \rangle = G$, we may choose $s_1 \in S$, such that $s_1 \notin \langle a, b \rangle \, \mathbb{Z}_p$. Then $\langle a, b, s_1 \rangle = \langle a, b \rangle \, \mathbb{Z}_q$. Since a centralizes both a and b, but does not centralize $\mathbb{Z}_q$, which is contained in $\langle a, b, s_1 \rangle$, we know that $[a, s_1]$ is nontrivial. Therefore $\langle a, s_1 \rangle$ contains $\langle a, b, s_1 \rangle' = \mathbb{Z}_q$. Then, since $|\langle a, s_1 \rangle|$ is only divisible by two primes, we must have $|\langle a, s_1 \rangle| = 2q$. Also, since $S \cap G' = \emptyset$, we must have $|s_1| \neq q$; therefore $|s_1| = 2$. Hence $2r \mid |\langle b, s_1 \rangle|$, so we must have $|\langle b, s_1 \rangle| = 2r$. Therefore (note A.58)

$$[b, s_1] \in \langle b, s_1 \rangle \cap \langle a, b, s_1 \rangle' = \langle b, s_1 \rangle \cap \mathbb{Z}_q = \{e\},$$

so b centralizes s_1. It also centralizes a, so b centralizes $\langle a, s_1 \rangle = \mathbb{Z}_2 \ltimes \mathbb{Z}_q$.

Similarly, if we choose $s_2 \in S$ with $s_2 \notin \langle a, b \rangle \mathbb{Z}_q$, then a centralizes $\langle b, s_2 \rangle = \mathbb{Z}_r \ltimes \mathbb{Z}_p$.

Therefore $G = \langle a, s_1 \rangle \times \langle b, s_2 \rangle$, so

$$\mathrm{Cay}(G; S) \cong \mathrm{Cay}\big(\langle a, s_1 \rangle; \{a, s_1\}\big) \times \mathrm{Cay}\big(\langle b, s_2 \rangle; \{b, s_2\}\big).$$

This is a Cartesian product of hamiltonian graphs and therefore is hamiltonian. □

References

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

[2] C. C. Chen and N. Quimpo: On strongly hamiltonian abelian group graphs, in K. L. McAvaney, ed.: *Combinatorial Mathematics VIII (Proceedings, Geelong, Australia 1980),* Springer-Verlag, Berlin, 1981, pp. 23–24.

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

[4] S. J. Curran, D. W. Morris, and J. Morris: Cayley graphs of order $16p$ are hamiltonian, *Ars Math. Contemp.* (to appear). http://amc.imfm.si/index.php/amc/article/view/207

[5] E. Ghaderpour and D. W. Morris: Cayley graphs of order $27p$ are hamiltonian, *Internat. J. Comb.* 2011, Article ID 206930, 16 pages. http://www.hindawi.com/journals/ijct/2011/206930/

[6] E. Ghaderpour and D. W. Morris: Cayley graphs of order 150 are hamiltonian (unpublished). http://arxiv.org/src/1102.5156/anc/150.pdf

[7] M. Hall: *The Theory of Groups,* Macmillan, New York, 1959.

[8] D. Jungreis and E. Friedman: Cayley graphs on groups of low order are hamiltonian (unpublished).

[9] K. Keating and D. Witte: On Hamilton cycles in Cayley graphs with cyclic commutator subgroup, *Ann. Discrete Math.* 27 (1985) 89–102.

[10] 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), no. 1, 27–71.
http://amc.imfm.si/index.php/amc/article/view/177

[11] D. Marušič: Hamiltonian circuits in Cayley graphs, *Discrete Math.* 46 (1983), no. 1, 49–54.

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

[13] D. Witte: On hamiltonian circuits in Cayley diagrams, *Discrete Math.* 38 (1982) 99–108.

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

Appendix A. Notes to aid the referee

A.1. By assumption, there is a hamiltonian cycle $C = (s_i)_{i=1}^{n}$ in $\mathrm{Cay}(G/N;S)$, such that $s_i = s$, for some i. Replacing s_i with t does not change the hamiltonian cycle in $\mathrm{Cay}(G/N;S)$, because $t \equiv s = s_i \pmod{N}$, but the voltage of the new cycle is

$$s_1 s_2 \cdots s_{i-1} t s_{i+1} s_{i+2} \cdots s_n.$$

Since $t \neq s_i$, this is not equal to the voltage of the original cycle. So at least one of the two cycles has a voltage that is $\neq e$. Since $|N|$ is prime, it is generated by any of its nontrivial elements, so the Factor Group Lemma (2.2) applies.

A.2. The walk traverses all of the vertices in $\langle S_0 \rangle$, then the vertices in the coset $a\langle S_0 \rangle$, then the vertices in $a^2\langle S_0 \rangle$, etc., so it visits all of the vertices in G. Also, note that, for any $h \in H$, we have

$$\left(\prod_{x \in \langle a \rangle} h^x \right)^a = \prod_{x \in \langle a \rangle} h^{xa} = \prod_{x \in \langle a \rangle} h^x,$$

so $\prod_{x \in \langle a \rangle} h^x \in C_H(a)$. Therefore, letting $h = s_1 s_2 \cdots s_m \in H$, we have

$$\begin{aligned}
(ha)^{|a|} &= a^{|a|}(a^{-|a|} h a^{|a|}) \cdots (a^{-3} h a^3)(a^{-2} h a^2)(a^{-1} h a) \\
&= \prod_{x \in \langle a \rangle} h^x && (\text{because } a^{|a|} = e) \\
&\in C_H(a) \\
&= H \cap Z(G) && \begin{pmatrix} H \subset \langle S_0 \rangle \text{ and } \langle S_0 \rangle \text{ abelian} \Rightarrow \\ C_H(a) \subset C_H\big(\langle S_0, a \rangle\big) = C_H(G) \end{pmatrix} \\
&= \{e\},
\end{aligned}$$

so the walk is closed. Since the length of the walk is $|G|$, these facts imply that it is a hamiltonian cycle in $\mathrm{Cay}(G;S)$.

A.3. Suppose S_0 is a minimal generating set of D_{2pq}, and S_0 contains 3 reflections a, at^i, and at^j, where t is a rotation that generates T. Since $|D_{2pq}|$ is the product of 3 primes, and the minimality of S_0 implies

$$\langle a \rangle \subsetneq \langle a, at^i \rangle \subsetneq \langle a, at^i, at^j \rangle,$$

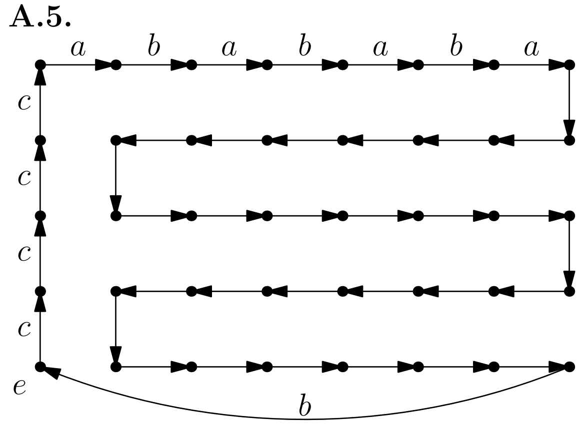
we must have $\langle a, at^i, at^j \rangle = D_{2pq}$. From the minimality of S_0, we know $\langle at^i, at^j \rangle$ is a proper subgroup D_{2pq}, so we may assume $q \mid (i - j)$ (after interchanging p and q if necessary). Since $\langle a, at^i \rangle$ and $\langle a, at^j \rangle$ must also be proper subgroups (and are not equal to each other), we may assume $p \mid i$ and $q \mid j$ (after interchanging i and j if necessary). Then

$$q \mid (i - j) + j = i.$$

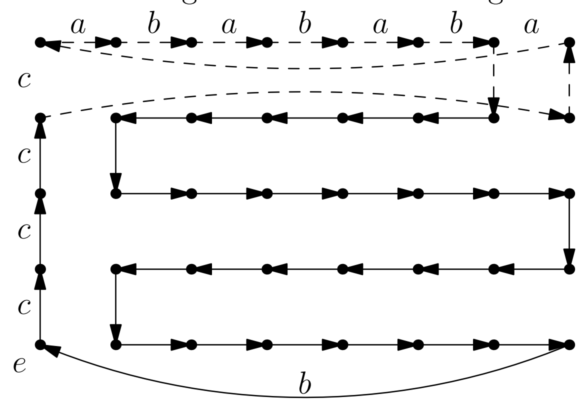
So $pq \mid i$, which means $at^i = a$. This contradicts the fact that a and at^i are two different reflections.

A.4. If $\langle \varphi(c) \rangle = T$, then $\langle c \rangle = T \times \mathbb{Z}_r$ has index 2 in G. So $\langle a, c \rangle = G$, which contradicts the fact that S is a minimal generating set.

A.5.



A.6. The edges from the new string are dashed.



A.7. From the cited theorem of [7] (but replacing the symbol r with τ), we know that G is "metacyclic", and there exist $a, b \in G$, such that

- $G = \langle b \rangle \ltimes \langle a \rangle$, and
- $\gcd\big((\tau - 1)|b|, |a|\big) = 1$, where $\tau \in \mathbb{Z}$ is chosen so that $a^b = a^\tau$.

(1) Since G is metacyclic, we know G' is cyclic. In fact, the proof points out that $G' = \langle a \rangle$. (This follows easily from the fact that $\gcd\big(\tau - 1, |a|\big) = 1$.)

(2) Suppose $a^k \in Z(G)$. This means

$$e = [a^k, b] = a^{-k}(a^k)^b = a^{-k}a^{k\tau} = a^{(\tau-1)k},$$

so $|a| \mid (\tau - 1)k$. Since $\gcd\big(\tau - 1, |a|\big) = 1$, this implies $|a| \mid k$, so $a^k = e$.

(3) Let $\mathbb{Z}_n = \langle b \rangle$. Then $G = \langle b \rangle \ltimes \langle a \rangle = \mathbb{Z}_n \ltimes G'$.

(4) This is one of the conclusions of the cited theorem of [7] (except that we have replaced r with τ).

A.8. From Lemma 2.11, we may write $G = \langle b \rangle \ltimes \langle a \rangle$ with $|b| = 2$ and $\langle a \rangle = G' \cong \mathbb{Z}_{15p}$. Choose $\tau \in \mathbb{Z}$, such that $a^b = a^\tau$. Since $|b| = 2$, we must have $\tau^2 \equiv 1 \pmod{15p}$, so $\tau \equiv \pm 1$ modulo each prime divisor of $15p$. Also, we know

$$\gcd(\tau - 1, 15p) = \gcd\big(\tau - 1, |a|\big) = 1,$$

which means $\tau \not\equiv 1$ modulo any prime divisor of $15p$. We conclude that $\tau \equiv -1 \pmod{15p}$, so $G \cong D_{30p}$.

A.9. From Lemma 2.11, we may write $G = \langle b \rangle \ltimes \langle a \rangle$ with $\langle b \rangle \cong \mathbb{Z}_{2p} \cong \mathbb{Z}_2 \times \mathbb{Z}_p$ and $\langle a \rangle = G' \cong \mathbb{Z}_{15}$. Since

$$\gcd\bigl(|\mathbb{Z}_p|, |\operatorname{Aut}(\mathbb{Z}_{15})|\bigr) = \gcd\bigl(p, \phi(15)\bigr) = \gcd(p, 8) = 1,$$

we know that $\mathbb{Z}_p$ centralizes $\mathbb{Z}_{15}$. So $G = (\mathbb{Z}_2 \ltimes \mathbb{Z}_{15}) \times \mathbb{Z}_p$. Since $G' = \mathbb{Z}_{15}$, the argument of A.8 implies that $\mathbb{Z}_2 \ltimes \mathbb{Z}_{15} \cong D_{30}$.

A.10. From Lemma 2.11, we may write $G = \langle b \rangle \ltimes \langle a \rangle$, with $G' = \langle a \rangle$. Choose $\tau \in \mathbb{Z}$, such that $a^b = a^\tau$.

We claim $|a|$ is odd. Suppose not. From Lemma 2.11(4), we know that $\gcd(\tau - 1, |a|) = 1$, so τ is even. But this contradicts the fact that τ must be relatively prime to $|a|$.

So $|G'|$ is an odd divisor of $30p$. In other words, $|G'|$ is a divisor of $15p$. However, we are assuming that $|G'|$ is not prime, and that it is not 15. Therefore, $|G'|$ is either $3p$ or $5p$.

A.11. From Lemma 2.11, we know $G' \cap Z(G) = \{e\}$, so some element of $\mathbb{Z}_{2r}$ must act nontrivially on $\mathbb{Z}_q$.

A.12. We already know that $\mathbb{Z}_r$ centralizes $\mathbb{Z}_q$. Obviously, it also centralizes $\mathbb{Z}_{2r}$. If it also centralizes $\mathbb{Z}_p$, then it centralizes all of G, so it is in $Z(G)$. This implies that $G = (\mathbb{Z}_2 \ltimes \mathbb{Z}_{pq}) \times \mathbb{Z}_r$. Since $G' = \mathbb{Z}_{pq}$, the argument of A.8 implies that $\mathbb{Z}_2 \ltimes \mathbb{Z}_{pq} \cong D_{2pq}$.

A.13. Since $r \in \{3, 5\}$, we have $r - 1 \in \{2, 4\}$. Since $15p$ is odd, this implies $\gcd(r - 1, 15p) = 1$.

A.14. If $q \mid |a|$, then $\langle a \rangle$ contains a subgroup of order q, which is obviously centralized by a. However, $\mathbb{Z}_q$ is the unique subgroup of order q in G (since a normal Sylow $q$subgroup is unique). So a centralizes $\mathbb{Z}_q$. Since the image of a in G/G' has order 2, this implies that $\mathbb{Z}_2$ centralizes $\mathbb{Z}_q$.

A.15. Since b has even order, there is some $k \in \mathbb{Z}$, such that $|b^k| = 2$. Then $\langle a \rangle$ and $\langle b^k \rangle$ are Sylow 2-subgroups of G, so they must be conjugate. Since b generates G/G' and centralizes b^k, this implies there is some $x \in G'$, such that $a^x = b^k$. Writing $G' = C_{G'}(a) \times H$, for some subgroup H, we may write $x = ch$ with $c \in C_{G'}(a)$ and $h \in H$. Then

$$a^h = a^{ch} = a^x = b^k \in \langle b \rangle,$$

so $a \in \langle b, h \rangle = \langle b \rangle \ltimes H$. Since $\langle a, b \rangle = G$, we conclude that $\langle b \rangle \ltimes H = G$, so $H = G'$. Therefore $C_{G'}(a)$ is trivial.

A.16. We have either $r = 3$ or $r = 5$. We now show that, for a given choice of r, we need only consider the single situation described in the text.

Since all elements of order 2 are conjugate, we may assume a is the unique element of order 2 in $\mathbb{Z}_{2r}$; in other words, $a = x^r$. Since b generates G/G', there is no harm in assuming that the projection of b to $\mathbb{Z}_{2r}$ is the generator x, so $b = xg'$ for some $g' \in G'$. Since $\langle a, b \rangle = G$, we must have $\langle g' \rangle = G'$, so there is no harm in assuming that $g' = yw$.

We said earlier that $y^x = y^{-1}$.

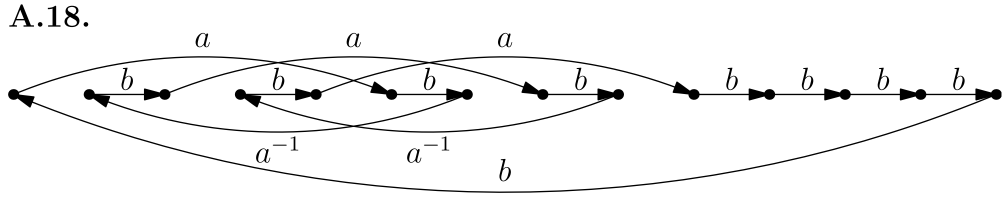
Choose $d \in \mathbb{Z}$, such that $w^x = w^d$. Since a does not centralize $\mathbb{Z}_p$, we know that x^r does not centralize $\mathbb{Z}_p$, so $d^r \not\equiv 1 \pmod{p}$. Also, we said earlier that $\mathbb{Z}_r$ does not centralize $\mathbb{Z}_p$, so x^2 does not centralize $\mathbb{Z}_p$, so $d^2 \not\equiv 1 \pmod{p}$. On the other hand, $x^{2r} = e$ does centralize $\mathbb{Z}_p$, so $d^{2r} \equiv 1 \pmod{p}$. Therefore d is a primitive $(2r)^{\text{th}}$ root of 1 in $\mathbb{Z}_p$. This implies that $d^r \equiv -1 \pmod{p}$. Since $d \not\equiv -1 \pmod{p}$, we may divide by $d+1$, so, since r is odd, we have

$$\sum_{i=0}^{r-1} (-1)^i d^i = \frac{d^r + 1}{d+1} \equiv \frac{0}{d+1} \equiv 0 \pmod{p}.$$

A.17. We have $a^{2r} \in G'$ (since $|G/G'| = 2r$), and a obviously centralizes a^{2r}. Since $\langle a \rangle$ has trivial centralizer in G', this implies $a^{2r} = e$, so $|a| = 2r$.

Similarly, $|b| = 2r$.

A.18.



A.19. Since $|b| = 2r$, we know $d^{2r} \equiv 1 \pmod p$. Also, since $\langle b^2 \rangle = \mathbb{Z}_r$ does not centralize y, we have $d^2 \not\equiv 1 \pmod p$. Therefore d is either a primitive r^{th} or $(2r)^{\text{th}}$ root of unity modulo p.

A.20. To calculate the exponents of b and y, we can work modulo the normal subgroup $\langle w \rangle$. Since $\gcd(i, 2r) = 1$, we know $1 - i$ is odd, so b^{1-i} inverts y (but b inverts y). Therefore

$$\begin{aligned}(b^i y) b (y^{-1} b^{-i}) b &= b^i y^2 b^{2-i} && (b \text{ inverts } y) \\ &= b^2 y^{-2} && \begin{pmatrix} \gcd(i, 2r) = 1, \text{ so } 2 - i \text{ is odd,} \\ \text{so } b^{2-i} \text{ inverts } y \end{pmatrix}.\end{aligned}$$

Now, to calculate the exponent of y, we can work modulo the normal subgroup $\langle y \rangle$. Since $w^b = w^d$, we have

$$(b^i w) b (w^{-1} b^{-i}) b = b^{i+1} w^{d-1} b^{1-i} = b^2 w^{(d-1)d^{1-i}}.$$

A.21. To calculate the exponents of b and y, we work modulo $\langle w \rangle$. Since b inverts y, we know b^2 centralizes y, so

$$(b^2 y^{-2})^{(i-1)/2} = (b^2)^{(i-1)/2} (y^{-2})^{(i-1)/2} = b^{i-1} y^{-(i-1)}.$$

Now, to calculate the exponent of w, we can work modulo the normal subgroup $\langle y \rangle$. For convenience, let $\underline{b} = b^2$, $\underline{w} = w^{(d-1)d^{1-i}}$, and $i' = (i-1)/2$. Then

$$\begin{aligned}
(b^2 w^{(d-1)d^{1-i}})^{(i-1)/2} &= (\underline{b}\underline{w})^{i'} \\
&= \underline{b}^{i'} (\underline{b}^{-(i'-1)} \underline{w} \underline{b}^{i'-1})(\underline{b}^{-(i'-2)} \underline{w} \underline{b}^{i'-2}) \cdots (\underline{b}^{-1} \underline{w} \underline{b}^{1})(\underline{b}^{-0} \underline{w} \underline{b}^{0}) \\
&= b^{i-1} (b^{-(i-3)} \underline{w} b^{i-3})(b^{-(i-5)} \underline{w} b^{i-5}) \cdots (b^{-2} \underline{w} b^{2})(b^{-0} \underline{w} b^{0}) \\
&= b^{i-1} (\underline{w}^{d^{i-3}})(\underline{w}^{d^{i-5}}) \cdots (\underline{w}^{d^2})(\underline{w}^{d^0}) \\
&= b^{i-1} \underline{w}^{d^{i-3} + d^{i-5} + \cdots + d^2 + 1} \\
&= b^{i-1} w^{(d-1)d^{1-i}(d^{i-3} + d^{i-5} + \cdots + d^2 + 1)}.
\end{aligned}$$

A.22. For convenience, let $\underline{w} = w^{(d-1)(d^{i-3} + d^{i-5} + \cdots + d^2 + 1)}$. Then

$$\begin{aligned}
&\big(b^{i-1} y^{-(i-1)} w^{(d-1)d^{1-i}(d^{i-3} + d^{i-5} + \cdots + d^2 + 1)}\big)(b^i y w) \\
&\quad = \big(b^{i-1} y^{-(i-1)} \underline{w}^{d^{1-i}}\big)(b^i y w) \\
&\quad = \big(b^{2i-1} y^{i-1} (\underline{w}^{d^{1-i}})^{d^i}\big)(y w) && (b^i \text{ inverts } y, \text{ since } i \text{ is odd}) \\
&\quad = b^{2i-1} y^{(i-1)+1} \underline{w}^d (w) && \begin{pmatrix} y \text{ commutes with } w, \\ \text{since both are in } \mathbb{Z}_{pq} \end{pmatrix}.
\end{aligned}$$

Also, we have

$$\underline{w}^d (w) = (w^{(d-1)(d^{i-3} + d^{i-5} + \cdots + d^2 + 1)})^d (w) = w^{(d-1)d(d^{i-3} + d^{i-5} + \cdots + d^2 + 1) + 1}.$$

A.23. Recall that $\{q, r\} = \{3, 5\}$. Since $q \mid i$ and $i < r$, we must have $q < r$, so $q = 3$ and $r = 5$. Then, since $q \mid i$ and $i < r$, we have $3 \mid i$ and $i < 5$, so it is obvious that $i = 3$.

A.24. Let c be an element of S with nontrivial projection to $\mathbb{Z}_r$, so $\mathbb{Z}_r \subset \langle c \rangle$. Since S is minimal and $\#\big(S \smallsetminus \{c\}\big) > 1$, we know that $|\overline{G}/\langle \overline{c} \rangle|$ cannot be prime. Therefore $\langle \overline{c} \rangle = \mathbb{Z}_r$.

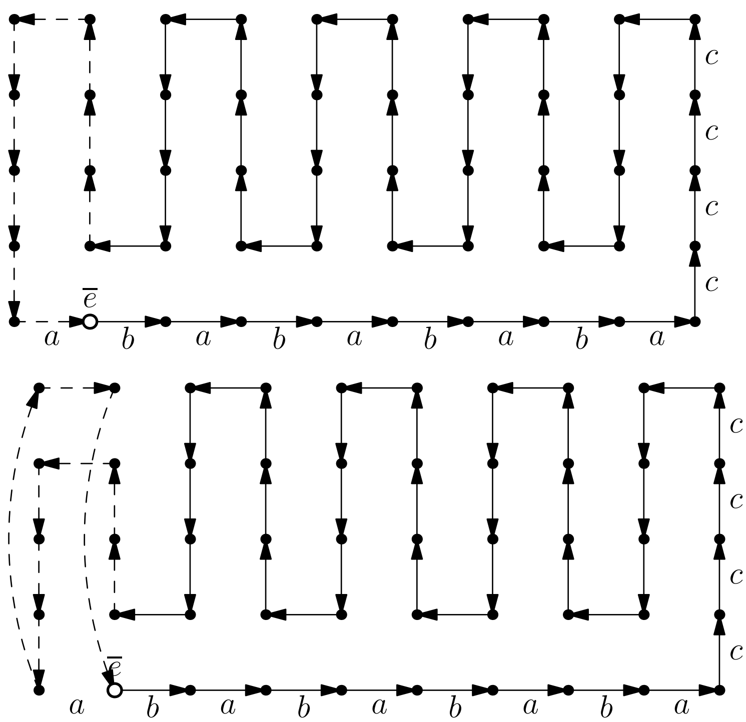
The other elements of S must have trivial projection to $\mathbb{Z}_r$. (Otherwise, the previous paragraph implies they belong to $\mathbb{Z}_r = \langle \overline{c} \rangle$, contradicting the minimality of $\overline{S}$. So $\overline{a}, \overline{b} \in D_{2q}$.

A.25. We have $c^r \in \mathbb{Z}_p$ (since $\overline{c}^r = \overline{e}$), and c obviously centralizes c^r. Since $\langle \overline{c} \rangle = \mathbb{Z}_r$ acts nontrivially on $\mathbb{Z}_p$, and hence has trivial centralizer in $\mathbb{Z}_p$, this implies $c^r = e$, so $|c| = r$.

This implies that $\langle c \rangle$ is a Sylow r-subgroup of G, so it is conjugate to any other Sylow r-subgroup, including $\mathbb{Z}_r$.

A.26. If $\mathbb{Z}_r \subset Z(G)$, then $G = \langle a, b \rangle \times \mathbb{Z}_r$. Also, since $|a| = |b| = 2$, we know that $\langle a, b \rangle$ is a dihedral group. Therefore Lemma 2.9 applies.

A.27. Edges not in W are dashed.



A.28. Let $H = \langle a, b \rangle$. Since $\langle \overline{a}, \overline{b} \rangle = \overline{G}$, we know $2qr \mid |H|$. On the other hand, the minimality of S implies $H \neq G$, so H is a proper divisor of $|G| = 2pqr$. Therefore $|H| = 2qr$. Since G is solvable, any two Hall subgroups of the same order are conjugate [7, Thm. 9.3.1(2), p. 141], so H is conjugate to $D_{2q} \times \mathbb{Z}_r$.

A.29. Let $\varphi \colon \langle a, b \rangle \to D_{2q}$ be the projection with kernel $\mathbb{Z}_r$.

Case 1. *Assume the projection of a to $\mathbb{Z}_r$ is trivial.* This means $a = f$. Then b must project nontrivially to $\mathbb{Z}_r$ (since $\langle a, b \rangle = D_{2q} \times \mathbb{Z}_r$). Therefore, we may assume the projection of b to $\mathbb{Z}_r$ is z (since every nontrivial element of $\mathbb{Z}_r$ is a generator). Therefore b is either yz or fyz, depending on whether $\varphi(b)$ is y or fy, respectively.

Case 2. *Assume the projection of a to $\mathbb{Z}_r$ is nontrivial.* We may assume $a = fz$ (since every nontrivial element of $\mathbb{Z}_r$ is a generator).

We have $b = \varphi(b)\, z^{\ell}$ for some $\ell \in \mathbb{Z}$, and we wish to show that we may assume $\ell \not\equiv 0 \pmod{r}$. That is, we wish to show that we may assume $b \neq \varphi(b)$.

- Since $y \notin S$, we know that $b \neq \varphi(b)$ if $\varphi(b) = y$.
- If $b = \varphi(b) = fy$, then interchanging a and b would put us in Case 1.

A.30. Suppose $i \neq 0$, which means $i = 1$. Since y and z commute, we have $\langle yz \rangle = \langle y \rangle \times \langle z \rangle$. Therefore

$$\langle b, c \rangle = \langle y, z, fy^j z^k w \rangle = \langle y, z, fw \rangle.$$

This contains

$$(fw)^{-1}(fw)^z = (fw)^{-1}(fw^d) = w^{d-1}.$$

Since $d \neq 1$, we have $\langle w^{d-1} \rangle = \mathbb{Z}_p$, so $\langle b, c \rangle$ contains w. Since it also contains y, z, and fw, we conclude that $\langle b, c \rangle = G$.

A.31. We have

$$\begin{aligned}\big((f)(yz)^{-(r-1)}(f)\big)(yz)^{r-1} &= f^2(y^{-1}z)^{-(r-1)}(yz)^{r-1} && (f \text{ inverts } y \text{ and centralizes } z)\\ &= y^{2(r-1)} && (|f| = 2 \text{ and } y \text{ commutes with } z).\end{aligned}$$

Also, $(yz)^{-1}(y^j zw) = y^{j-1}w$, since y commutes with z.

A.32. Since $|y| = q$, it suffices to check (for each of the two possible values of q) that the given exponent of y is congruent to $j-2$, modulo q:

- If $q = 5$, then $j + 3 \equiv j - 2 \pmod{q}$.
- If $q = 3$, then $j + 7 \equiv j - 2 \pmod{q}$.

A.33. We have

$$\begin{aligned}\big((f)(yz)^{-(r-1)}(f)\big)(yz)^{r-1} &= f^2(y^{-1}z)^{-(r-1)}(yz)^{r-1} && (f \text{ inverts } y \text{ and centralizes } z)\\ &= y^{2(r-1)} && (|f| = 2 \text{ and } y \text{ commutes with } z).\end{aligned}$$

Also,

$$\begin{aligned}(y^2zw)^2 &= (y^2zw)(y^2zw)\\ &= (y^4zw)(zw) && (y \text{ commutes with both } z \text{ and } w)\\ &= y^4z^2w^{d+1} && (w^z = w^d),\end{aligned}$$

so

$$(yz)^{-2}(y^2zw)^2 = (yz)^{-2}(y^4z^2w^{d+1}) = y^2w^{d+1},$$

since y commutes with z.

A.34. Since $|y| = q$, it suffices to check (for each of the two possible values of q) that the given exponent of y is congruent to 1, modulo q:

- If $q = 5$, then $6 \equiv 1 \pmod{q}$.
- If $q = 3$, then $10 \equiv 1 \pmod{q}$.

A.35. Since d is a primitive r^{th} root of unity in $\mathbb{Z}_p$, we know $d \not\equiv -1 \pmod{p}$. Therefore w^{d+1} is nontrivial, and hence generates $\mathbb{Z}_p$.

A.36. Since y commutes with z, we have

$$\begin{aligned}
(fz)^4 &= f^4 z^4 = z^4, \\
fz^{-1}fz &= f^2 = e, \\
w^{-1}z^{-2}fz^2w &= w^{-1}fw = w^{-1+\epsilon}f, \\
z^{-1}fz &= f, \\
(fzfz^{-1})^2 &= (f^2)^2 = e^2 = e.
\end{aligned}$$

Also,

$$\begin{aligned}
(fw^{-1}z^{-2})^2 &= (fw^{-1}z^{-2})(fw^{-1}z^{-2}) \\
&= fw^{-1}fw^{-d^2}z^{-4} && (z \text{ commutes with } f, \text{ but } w^z = w^d) \\
&= f^2w^{-\epsilon-d^2}z^{-4} && (w^f = w^\epsilon) \\
&= w^{-(\epsilon+d^2)}z^{-4} && (|f| = 2).
\end{aligned}$$

A.37. Since y centralizes both z and w (and $j \neq 0$), we have

$$\langle c \rangle = \langle y^j z^2 w \rangle = \langle y \rangle \times \langle z^2 w \rangle.$$

Therefore $\langle a, c \rangle = \langle f, y, z^2 w \rangle$.

Since f centralizes z, this contains

$$(z^2w)^{-1}(z^2w)^f = (z^2w)^{-1}(z^2w^f) = [w, f].$$

If f does not centralize $\mathbb{Z}_p$, then $[w, f]$ is nontrivial, so it generates $\mathbb{Z}_p = \langle w \rangle$. This implies that $\langle a, c \rangle$ contains w. Since it also contains a, c, and z^2w, this would imply that $\langle a, c \rangle = G$, which is a contradiction. Therefore f centralizes $\mathbb{Z}_p$.

So f and y each centralize both z and w. Therefore

$$G = \langle f, y \rangle \times \langle z, w \rangle = D_{2q} \times (\mathbb{Z}_r \ltimes \mathbb{Z}_p) = D_6 \times (\mathbb{Z}_5 \ltimes \mathbb{Z}_p).$$

A.38. Since z commutes with f and y, we have $\langle fyz\rangle = \langle fy\rangle \times \langle z\rangle$. Also, since $c = f^i y^j z^k w$, we have $c \in \langle fy, z\rangle y^\ell w$ for some $\ell \in \mathbb{Z}$. Therefore

$$\langle b, c\rangle = \langle fy, z, c\rangle = \langle fy, z, y^\ell w\rangle.$$

This contains

$$\begin{aligned} (y^\ell w)^{-1}(y^\ell w)^z &= (y^\ell w)^{-1}(y^\ell w^z) && (z \text{ centralizes } y) \\ &= w^{-1}w^z \\ &= [w, z]. \end{aligned}$$

Since $\mathbb{Z}_r$ does not centralize $\mathbb{Z}_p$, this commutator is nontrivial, so it generates $\mathbb{Z}_p = \langle w\rangle$. Therefore $\langle b, c\rangle$ contains w. It also contains fy, z, and $y^\ell w$. If $\ell \neq 0$, this implies $\langle b, c\rangle = G$, which contradicts the minimality of S.

Therefore, we must have $\ell = 0$, so $c \in \langle fy, z\rangle y^\ell w = \langle fy, z\rangle w$.

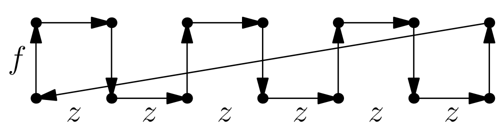
A.39.

- z commutes with both f and y, so $(fyz)^{r-1} = (fy)^{r-1} z^{r-1}$
- fy is a reflection, so it has order 2, so $(fy)^{r-1} = e$, since $r - 1$ is even.
- $z^r = e$, since $z \in \mathbb{Z}_r$, so $z^{r-1} = z^{-1}$.

A.40. Modulo $G' = \langle y, w\rangle$, we have $a \equiv f$, $b \equiv fz$, and $c \equiv z$. Since f commutes with z, we have

$$(ac)^{r-1}ab) \equiv (fz)^{r-1} f\, fz = f^{r+1} z^r = e,$$

since $|f| = 2$, $r+1$ is even, and $|z| = r$. Therefore, the walk in $\mathrm{Cay}(G/G'; S)$ is closed.



A.41.
$(ac)^{r-1}\,a\,b = (ac)^{r-1}\big((ac)(ac)^{-1}\big)\,a\,b = \big((ac)^{r-1}(ac)\big)(c^{-1}a^{-1})\,a\,b = (ac)^r\,(c^{-1}\,b)$

A.42.

$$\begin{aligned}(fzw)^r &= \big((fz)w\big)\big((fz)w\big)\cdots\big((fz)w\big)\big((fz)w\big)\\ &= (fz)^r\big((fz)^{-(r-1)}w(fz)^{r-1}\big)\big((fz)^{-(r-2)}w(fz)^{r-2}\big)\cdots\big((fz)^{-1}w(fz)^{1}\big)\big((fz)^{-0}w(fz)^{0}\big)\\ &= f^r z^r w^{(\epsilon d)^{r-1}+(\epsilon d)^{r-2}+\cdots+1}.\end{aligned}$$

A.43.

- $f^r = f$ because $|f| = 2$ and r is odd.
- $|z| = r$ and z commutes with both f and y.

A.44. Let $\omega \in \mathbb{Z}$. If

$$\omega^{r-2} + \omega^{r-3} + \cdots \omega + 1 \equiv 0 \pmod p,$$

then

$$\omega^{r-1} - 1 = (\omega - 1)(\omega^{r-2} + \omega^{r-3} + \cdots \omega + 1) \equiv (\omega - 1)(0) = 0 \pmod p,$$

so ω is an $(r-1)^{\text{st}}$ root of unity in $\mathbb{Z}_p$. Therefore, it cannot be a primitive r^{th} or $(2r)^{\text{th}}$ root of unity.

A.45. We have

$$\begin{aligned}
(z^2w)^{-1}f(z^2w) &= (w^{-1}z^{-2})f(z^2w) \\
&= w^{-1}fw && (z \text{ commutes with } f) \\
&= w^{-1}(fwf)f && (f^2 = e) \\
&= w^{\epsilon-1}f, \\
(fz)^{-1}f(fz) &= (z^{-1}f^{-1})f(fz) \\
&= f && (f \text{ and } z \text{ commute}).
\end{aligned}$$

and

$$\begin{aligned}
\big(f(z^2w)^{-1}\big)^2 &= (fw^{-1}z^{-2})(fw^{-1}z^{-2}) \\
&= (fw^{-1}f)(z^{-2}w^{-1}z^2)z^{-4} && (f \text{ and } z \text{ commute}) \\
&= (w^{-\epsilon})(w^{-d^2})z^{-4} \\
&= w^{-(\epsilon+d^2)}z^{-4}.
\end{aligned}$$

A.46. Since $0 \leq i < 2$ and we are assuming that $i \neq 0$, we have $c = fyz^kw$, so

$$\langle a, c\rangle = \langle f, fyz^kw\rangle = \langle f, yz^kw\rangle.$$

Since y commutes with both z and w, we have

$$\langle yz^kw\rangle = \langle y\rangle \times \langle z^kw\rangle,$$

so $\langle a, c\rangle$ contains both y and z^kw. Therefore, since f centralizes z, it also contains

$$(z^kw)^{-1}(z^kw)^f = (w^{-1}z^{-k})(z^kw^f) = w^{-1}w^f = [w, f].$$

If f does not centralize w, then this commutator is nontrivial, so it generates $\mathbb{Z}_p = \langle w\rangle$. This implies that $\langle a, c\rangle$ contains w. Since it also contains f, y, and z^kw (with $k \neq 0$), we conclude that $\langle a, c\rangle = G$. This is a contradiction. So f must centralize w.

Hence, f and y each centralize both z and w, so

$$G = \langle f, y\rangle \times \langle z, w\rangle = D_{2q} \times (\mathbb{Z}_r \ltimes \mathbb{Z}_p).$$

A.47.

$$\begin{aligned}\left(z^4wzw\right)^3 &= \left((z^{-1}wz)w\right)^3 && (|z| = r = 5)\\ &= \left(w^d w\right)^3\\ &= w^{3(d+1)}.\end{aligned}$$

A.48. d is a primitive r^{th} root of unity in $\mathbb{Z}_p$, so $d+1 \not\equiv 0 \pmod p$. Since $p \geq 7$, this implies $3(d+1) \not\equiv 0 \pmod p$. Therefore $w^{3(d+1)}$ is nontrivial, and hence generates $\mathbb{Z}_p$.

A.49. We have $c = f^i y^j z^k w$.

We claim that $j = 0$ (which means $c \in \langle f, z\rangle w$). Since z commutes with f, we have

$$\langle a\rangle = \langle fz\rangle = \langle f\rangle \times \langle z\rangle.$$

Therefore

$$\langle a, c\rangle = \langle f, z, f^i y^j z^k w\rangle = \langle f, z, y^j w\rangle,$$

which contains

$$(y^j w)^{-1}(y^j w)^z = (w^{-1}y^{-j})(y^j w^z) = w^{-1}w^z = [w, z].$$

Since $\mathbb{Z}_r$ does not centralize $\mathbb{Z}_p$, this commutator is nontrivial, so it generates $\mathbb{Z}_p = \langle w\rangle$. Therefore $\langle a, c\rangle$ contains w. So it contains $(y^j w)w^{-1} = y^j$.

If $j \neq 0$, this implies that $\langle a, c\rangle$ contains y. Since it also contains f, z, and w, we would have $\langle a, c\rangle = G$, which is a contradiction. Therefore $j = 0$, as claimed.

We claim that $i = 0$ (which means $c \in \langle y, z\rangle w$). Since z commutes with y (and $\ell \neq 0$), we have

$$\langle b\rangle = \langle yz^\ell\rangle = \langle y\rangle \times \langle z^\ell\rangle = \langle y\rangle \times \langle z\rangle.$$

Therefore

$$\langle b, c\rangle = \langle y, z, f^i y^j z^k w\rangle = \langle y, z, f^i w\rangle,$$

which contains

$$(f^i w)^{-1}(f^i w)^z = (w^{-1}f^{-i})(f^i w^z) = w^{-1}w^z = [w, z].$$

Since $\mathbb{Z}_r$ does not centralize $\mathbb{Z}_p$, this commutator is nontrivial, so it generates $\mathbb{Z}_p = \langle w \rangle$. Therefore $\langle b, c \rangle$ contains w. So it contains $(f^i w)w^{-1} = f^i$.

If $i \neq 0$, this implies that $\langle b, c \rangle$ contains f. Since it also contains y, z, and w, we would have $\langle b, c \rangle = G$, which is a contradiction. Therefore $i = 0$, as claimed.

Since $i = 0$ and $j = 0$, we have $c = z^k w$.

A.50. If $r = 3$, then $(r-1)/2 = 1$, so $\ell = k = 1$, contradicting the fact that $\ell \neq k$.

Thus, we must have $r = 5$, so $(r-1)/2 = 2$. Since $\ell \neq k$, we must have $\{\ell, k\} = \{1, 2\}$.

A.51. Recall that f commutes with z, and $f^2 = e$

A.52.

$$\begin{aligned}
\big(z^{-1}wfz^{-2}w\big)^2 &= \big((z^{-1}wz)f(z^{-3}wz^3)z^{-3}\big)^2 && (f \text{ commutes with } z)\\
&= \big((w^d)f(w^{d^3})z^{-3}\big)^2\\
&= \big(fw^{d^3+\epsilon d}z^{-3}\big)^2\\
&= \big(fw^{d^3+\epsilon d}z^{-3}\big)\big(fw^{d^3+\epsilon d}z^{-3}\big)\\
&= (fw^{d^3+\epsilon d}f)(z^{-3}w^{d^3+\epsilon d}z^3)z^{-6} && (f \text{ commutes with } z)\\
&= (w^{\epsilon(d^3+\epsilon d)})(w^{d^3(d^3+\epsilon d)})z^{-6}\\
&= (w^{d^6+\epsilon d^4+\epsilon d^3+d})z^{-6} && (\epsilon^2 = 1).
\end{aligned}$$

A.53. Since d is an r^{th} root of unity in $\mathbb{Z}_p$, and $r = 5$, we have $d^6 \equiv d \pmod{p}$, so, modulo p, we have

$$d^6 + \epsilon d^4 + \epsilon d^3 + d \equiv d + \epsilon d^4 + \epsilon d^3 + d = \epsilon d^4 + \epsilon d^3 + 2d = d(\epsilon d^3 + \epsilon d^2 + 2).$$

Also, since $|z| = r = 5$, we have $z^{-6} = z^4$.

A.54. If we write $c = f^i y^j z^k w$, then, exactly as in note A.49, we must have $j = 0$ (which means $c \in \langle f, z \rangle w$).

We may also write write $c = (fy)^i y^{j'} z^k w$. We claim that $j' = 0$ (which means $c \in \langle fy, z \rangle w$). Since z commutes with both f and y (and $\ell \neq 0$), we have

$$\langle b \rangle = \langle fyz^\ell \rangle = \langle fy \rangle \times \langle z^\ell \rangle = \langle fy \rangle \times \langle z \rangle.$$

Therefore

$$\langle b, c \rangle = \langle fy, z, (fy)^i y^{j'} z^k w \rangle = \langle fy, z, y^{j'} w \rangle,$$

which contains

$$(y^{j'} w)^{-1} (y^{j'} w)^z = (w^{-1} y^{-j'})(y^{j'} w^z) = w^{-1} w^z = [w, z].$$

Since $\mathbb{Z}_r$ does not centralize $\mathbb{Z}_p$, this commutator is nontrivial, so it generates $\mathbb{Z}_p = \langle w \rangle$. Therefore $\langle b, c \rangle$ contains w. So it contains $(y^{j'} w) w^{-1} = y^{j'}$.

If $j' \neq 0$, this implies that $\langle b, c \rangle$ contains y. Since it also contains fy, z, and w, we would have $\langle b, c \rangle = G$, which is a contradiction. Therefore $j' = 0$, as claimed.

Therefore

$$c \in \langle f, z \rangle w \cap \langle fy, z \rangle w = \big(\langle f, z \rangle \cap \langle fy, z \rangle \big) w = \langle z \rangle w.$$

A.55. If $r = 3$, we have $1 < \ell \leq (r-1)/2 = 1$, which is impossible. Therefore $r = 5$. So we have $1 < \ell \leq (r-1)/2 = 2$, which implies $\ell = 2$. Also, since $1 \leq k \leq (r-1)/2 = 2$, we have $k \in \{1, 2\}$.

A.56. Recall that f commutes with z, and $f^2 = e$. Also, we have $z^5 = z^r = e$, so $z^{13} = z^3$.

A.57. We have

$$(fz^3)^{-1}w(fz^3) = z^{-3}(f^{-1}wf)z^3 = z^{-3}w^{\epsilon}z^3 = w^{\epsilon d^3}.$$

Since d is a primitive r^{th} root of unity in $\mathbb{Z}_p$, we know $d^3 \not\equiv \pm 1 \pmod{p}$. Therefore $\epsilon d^3 \not\equiv 1 \pmod{p}$, so $(fz^3)^{-1}w(fz^3) \neq w$.

A.58. Since $|\langle a, b, s_1 \rangle|$ is the product of only three primes (and is divisible by $|\langle a, b \rangle| = 2r$), it must be either $2qr$ or $2pr$.

However, if $|\langle a, b, s_1 \rangle| = 2pr$, then $\langle a, b, s_1 \rangle$ contains $\mathbb{Z}_p$ (since $\mathbb{Z}_p$ is a normal Sylow p-subgroup of G, and hence is the unique subgroup of order p in G). So

$$\langle a, b, s_1 \rangle \supset \langle a, b \rangle \, \mathbb{Z}_p.$$

Since they have the same order, these two subgroups must be equal, so

$$s_1 \in \langle a, b, s_1 \rangle = \langle a, b \rangle \, \mathbb{Z}_p.$$

This contradicts the choice of s_1.

Therefore $|\langle a, b, s_1 \rangle| = 2qr$. Since $\mathbb{Z}_q$ is a normal Sylow q-subgroup of G, we know that it is the unique subgroup of order q in G. So $\mathbb{Z}_q \subset \langle a, b, s_1 \rangle$. Hence (by comparing orders) we must have $\langle a, b, s_1 \rangle = \langle a, b \rangle \, \mathbb{Z}_q$.
