Cayley graphs of order $16p$ are hamiltonian

Stephen J. Curran

Department of Mathematics, University of Pittsburgh at Johnstown
Johnstown, PA 15904, USA

Dave Witte Morris

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

Joy Morris

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

Abstract

Suppose G is a finite group, such that $|G| = 16p$, 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 $\mathrm{Cay}(G; S)$.

Keywords: Cayley graphs, hamiltonian cycles.

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

1 Introduction

This paper establishes one of the cases of Theorem 1.2(1) of [10]. Namely, several of the main results of that paper combine to show:

$$\text{Every connected Cayley graph on } G \text{ has a hamiltonian cycle}$$
$$\text{if } |G| = kp, \text{ where } p \text{ is prime, } 1 \le k < 32, \text{ and } k \notin \{16, 24, 27, 30\}. \tag{1.1}$$

We handle the first excluded case:

Theorem 1.1. *If $|G| = 16p$, where p is prime, then every connected Cayley graph on G has a hamiltonian cycle.*

E-mail addresses: SJCurran@pitt.edu (Stephen J. Curran), Dave.Morris@uleth.ca (Dave Witte Morris),
Joy.Morris@uleth.ca (Joy Morris)

Remark 1.2. The cases $k = 27$ and $k = 30$ are covered in [5, 6], but it seems that the case $k = 24$ will be more difficult.

Here is an outline of the paper:

2   Preliminaries on hamiltonian cycles in Cayley graphs

For ease of reference, we reproduce several useful results that provide hamiltonian cycles in Cayley graphs.

Notation.

1. G always represents a finite group.
2. For $S \subset G$ and $s_1, s_2, \ldots, s_n \in S \cup S^{-1}$, we use $(s_1, s_2, s_3, \ldots, s_n)$ to denote the walk in $\mathrm{Cay}(G; S)$ that visits (in order) the vertices

$$e, \; s_1, \; s_1 s_2, \; s_1 s_2 s_3, \; \ldots, \; s_1 s_2 \cdots s_n.$$

Also,

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

Notation. For any group G, and any $a, b \in G$, we use:

1. $[a, b]$ to denote the *commutator* $a^{-1}b^{-1}ab$,

2. b^a to denote the *conjugate* $a^{-1}ba$,

3. G' to denote the *commutator subgroup* $[G, G]$ of G, and

4. $\Phi(G)$ to denote the *Frattini subgroup* of G.

See [7, §5.1] for some basic properties of the Frattini subgroup (and its definition).

2.1 Factor Group Lemma

The following elementary results are well known (and easy to prove).

Lemma 2.1 ("Factor Group Lemma" [13, §2.2])**.** Suppose

- N is a cyclic, normal subgroup of G,
- $(s_1, s_2, \ldots, s_m)$ is a hamiltonian cycle in $\mathrm{Cay}(G/N; S)$, and
- the product $s_1 s_2 \cdots s_m$ generates N.

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

Corollary 2.2. *Suppose*

- *N is a cyclic, normal subgroup of G, such that $|N|$ is a prime power,*
- *$\langle s^{-1}t \rangle = N$ for some $s, t \in S \cup S^{-1}$, and*
- *there is a hamiltonian cycle in $\mathrm{Cay}(G/N; S)$ that uses at least one edge labelled s.*

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

Corollary 2.3. *Suppose*

- *N is a cyclic, normal subgroup of G, such that $|N|$ is a prime power,*
- *$s \in S$, with $s^2 \in N \smallsetminus \Phi(N)$, and*
- *there is a hamiltonian cycle in $\mathrm{Cay}(G/N; S)$ that uses at least one edge labelled s.*

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

Lemma 2.4 ([10, Cor. 2.9])**.** *Suppose*

- *S is a generating set of G,*
- *H is a subgroup of G, such that $|H|$ is prime,*
- *the quotient multigraph $H \backslash \mathrm{Cay}(G; S)$ has a hamiltonian cycle C, and*
- *C uses some double-edge of $H \backslash \mathrm{Cay}(G; S)$.*

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

2.2 Generator in a cyclic, normal subgroup

Theorem 2.5 (Alspach [1, Cor. 5.2])**.** *Suppose*

- *s and t are elements of G, and*
- $G = \langle s \rangle \ltimes \langle t \rangle$.

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

The following observation is well known.

Lemma 2.6 ([10, Lem. 2.27])**.** *Let S generate G and let $s \in S$, such that $\langle s \rangle \lhd G$. If*

- $\mathrm{Cay}(G/\langle s \rangle; S)$ *has a hamiltonian cycle, and*
- *either*

  1. $s \in Z(G)$*, or*
  2. $|s|$ *is prime,*

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

Here is another similar result.

Lemma 2.7. *Suppose*

- $s \in S$*, with $\langle s \rangle \lhd G$,*
- $|s|$ *is a divisor of pq, where p and q are distinct primes,*
- $s^p \in Z(G)$,
- $|G/\langle s \rangle|$ *is divisible by q, and*
- $\mathrm{Cay}(G/\langle s \rangle; S)$ *has a hamiltonian cycle.*

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

Proof. We may assume $|s| = pq$ and $s \notin Z(G)$, for otherwise Lemma 2.6 applies. Let

- $(s_1, \ldots, s_m)$ be a hamiltonian cycle in $\mathrm{Cay}(G/\langle s \rangle; S)$,
- $g = s_1 s_2 \cdots s_m$ be its endpoint in G, and
- $k = |s|/|g|$.

Consider the walk

$$\left(s_1, s^{k-1}, s_2, s^{k-1}, \ldots, s_m, s^{k-1} \right).$$

Writing $s = xw$, where x is the q-part of s and w is the p-part of s, and noting that $x \in Z(G)$ (because $x^p = s^p \in Z(G)$), we see that the endpoint is

$$s_1(xw)^{k-1} s_2(xw)^{k-1} \cdots s_m(xw)^{k-1} = g\, x^{(k-1)m} \prod_{g' \in G/\langle s \rangle} w^{g'} = g, \qquad (2.1)$$

since $m = |G/\langle s \rangle|$ is divisible by q, and $\langle w \rangle \cap Z(G) = \{e\}$.

Therefore, the walk

$$\left(s_1, s^{k-1}, s_2, s^{k-1}, \ldots, s_m, s^{k-1} \right)^{|g|}$$

is closed. Also (using (2.1)), it is not difficult to see that the walk traverses all of the elements of G. Therefore, it is a hamiltonian cycle in $\mathrm{Cay}(G; S)$. $\qquad\square$

2.3 Miscellaneous results

Theorem 2.8 (Marušič-Durnberger-Keating-Witte [9])**.** *If* G' *is a cyclic p-group, then every connected Cayley graph on* G *has a hamiltonian cycle.*

The proof in [12] yields the following result.

Theorem 2.9 ([11, Cor. 3.3])**.** *Suppose*

- S *is a generating set of* G,
- N *is a normal p-subgroup of* G, *and*
- $st^{-1} \in N$, *for all* $s, t \in S$.

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

The following observation is also known, but we do not know whether it is in the literature, so we provide a proof. Because it is of independent interest, we prove a more general version than we need.

Lemma 2.10. *Let* S *generate* G, *and let* X *be a subset of* S. *Assume:*

- $\langle X \rangle$ *is abelian* (*and nontrivial*),
- *for each* $g \in G$, *either* g *centralizes every element of* $\langle X \rangle$, *or* g *inverts every element of* $\langle X \rangle$,
- *there is a hamiltonian cycle in* $\mathrm{Cay}(\langle X \rangle; X)$, *and*
- *there is a hamiltonian path in* $\mathrm{Cay}(G/\langle X \rangle; S)$.

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

Proof. Let

- $[x_0, x_1, \ldots, x_m]$ be a hamiltonian cycle in $\mathrm{Cay}(\langle X \rangle; X)$,
- $[g_0, g_1, \ldots, g_n]$ be a path in $\mathrm{Cay}(G; S)$ that is the lift of a hamiltonian path in $\mathrm{Cay}(G/\langle X \rangle; S)$,
- $C = \mathrm{Cay}(\mathbb{Z}_m; \{1\})$ be a cycle of length m,
- L be the path of length n with consecutive vertices $0, 1, \ldots, n$,
- $f \colon V(C) \times V(L) \to G$ be defined by

$$f(i, j) = x_i \, g_j.$$

Note that:

- for $0 \le i < m$ and $0 \le j < n$, we have

$$f(i, j)^{-1} \cdot f(i, j+1) = (x_i \, g_j)^{-1}(x_i \, g_{j+1}) = g_j^{-1} g_{j+1} \in S \cup S^{-1},$$

  because g_j and g_{j+1} are adjacent vertices in $\mathrm{Cay}(G; S)$, and

- for $0 \le i < m$ and $0 \le j \le n$, and letting $x = x_i^{-1} x_{i+1} \in X \cup X^{-1}$, we have

$$f(i, j)^{-1} \cdot f(i+1, j) = (x_i \, g_j)^{-1}(x_{i+1} \, g_j) = g_j^{-1} x g_j = x^{\pm 1} \in X \cup X^{-1}.$$

Thus, f is an isomorphism from the Cartesian product $C \times L$ onto a subgraph of $\mathrm{Cay}(G; S)$. Since the two graphs have the same number of vertices, it is a spanning subgraph. Then, since it is easy to see that $C \times L$ has a hamiltonian cycle [3, Corollary on p. 29], we conclude that $\mathrm{Cay}(G; S)$ has a hamiltonian cycle. $\qquad \square$

Remark 2.11. When we apply Corollary 2.2 or Corollary 2.3 to obtain a hamiltonian cycle in $\mathrm{Cay}(G; S)$, and G has order $16p$, the order of G/N is either $4p$ or $8p$. Thus, (1.1) provides a hamiltonian cycle in $\mathrm{Cay}(G/N; S)$ with at least one edge labelled s. Similarly, (1.1) provides a hamiltonian cycle in $\mathrm{Cay}(G/\langle s \rangle; S)$ for Lemmas 2.6 and 2.7, and it provides a hamiltonian path in $\mathrm{Cay}(G/\langle X \rangle; S)$ for Lemma 2.10.

3 Groups without a normal Sylow p-subgroup

In this section, we prove Theorem 1.1 under the additional assumption that the Sylow p-subgroups of G are not normal.

Proposition 3.1. *If $|G| = 16p$, where p is prime, and the Sylow p-subgroups of G are not normal, then every connected Cayley graph on G has a hamiltonian cycle.*

We begin with the following result, which shows that there are only three possibilities for the order of G.

Lemma 3.2. *If $|G| = 16p$, where p is prime, and the Sylow p-subgroups of G are not normal, then $p \in \{3, 5, 7\}$, so $|G| \in \{48, 80, 112\}$.*

Proof. By Sylow's Theorem [8, Thm. 15.7, p. 230], we know that the number of Sylow p-subgroups is a divisor of 16, and is congruent to 1, modulo p. Since the only prime divisors of $2 - 1 = 1$, $4 - 1 = 3$, $8 - 1 = 7$, and $16 - 1 = 15 = 3 \times 5$ are 3, 5, and 7, this implies there is only one Sylow p-subgroup (which is normal) unless $p \in \{3, 5, 7\}$. $\qquad \square$

We now list the nine nonabelian groups of order 16, The list will be used repeatedly in the remainder of the paper, because each of these nine groups arises as the Sylow 2-subgroup of a group of order $16p$.

Proposition 3.3 ([2, §118, p. 146])**.** *There are nine nonabelian groups of order* 16:

1. *three groups with $Q/Q' \cong \mathbb{Z}_2 \times \mathbb{Z}_2$:*

   (a) D_{16} *("dihedral"),*
   (b) Q_{16} *("generalized quaternion"), and*
   (c) $\mathbb{Z}_2 \ltimes \mathbb{Z}_8 = \langle x \rangle \ltimes \langle y \rangle$ *with $x^{-1}yx = y^3$ ("semidihedral" or "quasidihedral").*

2. *three groups with $Q/Q' \cong \mathbb{Z}_4 \times \mathbb{Z}_2$:*

   (a) $\mathbb{Z}_2 \ltimes \mathbb{Z}_8 = \langle x \rangle \ltimes \langle y \rangle$ *with $x^{-1}yx = y^5$,*
   (b) $\mathbb{Z}_4 \ltimes \mathbb{Z}_4 = \langle x \rangle \ltimes \langle y \rangle$ *with $x^{-1}yx = y^{-1}$, and*
   (c) $\mathbb{Z}_4 \ltimes (\mathbb{Z}_2 \times \mathbb{Z}_2) = \langle x \rangle \ltimes \langle y, z \rangle$ *with $x^{-1}yx = yz$ and $x^{-1}zx = z$.*

3. *three groups with $Q/Q' \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$:*

   (a) $D_8 \times \mathbb{Z}_2 = \langle f, t \mid f^2 = t^4 = (ft)^2 = e \rangle \times \langle z \rangle$,

(b) $Q_8 \times \mathbb{Z}_2$, and

(c) $\mathbb{Z}_2 \ltimes (\mathbb{Z}_2 \times \mathbb{Z}_4) = \langle x \rangle \ltimes \langle y, z \rangle$ *with* $x^{-1}yx = yz^2$ *and* $x^{-1}zx = z$.

The three possible orders of G are discussed individually in Propositions 3.4, 3.5 and 3.8 below.

3.1 Groups of order 48

Proposition 3.4 ([4])**.** *If* $|G| = 48$, *and the Sylow* 3-*subgroups of* G *are not normal, then every connected Cayley graph on* G *has a hamiltonian cycle.*

Comments on the proof. A computer search can find hamiltonian cycles in all of these Cayley graphs fairly quickly. Alternatively, a proof can be written by hand, but, unfortunately, our presentation of this [4] is an unilluminating, 15-page case-by-case analysis, so we omit the details. □

It would be interesting to have a conceptual proof of Proposition 3.4, or, failing that, a human-readable proof of only 2 or 3 pages.

3.2 Groups of order 80

Proposition 3.5. *If* $|G| = 80$, *and the Sylow* 5-*subgroups of* G *are not normal, then every connected Cayley graph on* G *has a hamiltonian cycle.*

Proof. From Sylow's Theorem (and the observation that 16 is the only nontrivial divisor of 16 that is congruent to 1 modulo 5), we know there are 16 Sylow 5-subgroups. These contain $16 \times 4 = 64 = |G| - 16$ nonidentity elements of G, so the Sylow 2-subgroup must be normal. Therefore $G = \mathbb{Z}_5 \ltimes Q$, where Q is the Sylow 2-subgroup. Since $\mathbb{Z}_5 \not\triangleleft G$, we know the action on Q is nontrivial.

We claim G is isomorphic to a semidirect product $\mathbb{Z}_5 \ltimes (\mathbb{Z}_2)^4$. If not, then Q is not elementary abelian, so $Q/\Phi(Q)$ has order 2, 4, or 8. Since groups of order 2, 4, or 8 have no automorphisms of order 5, this implies that $\mathbb{Z}_5$ acts trivially on $Q/\Phi(Q)$. Therefore $\mathbb{Z}_5$ acts trivially on Q [7, Thm. 5.3.5]. This is a contradiction.

Now let S be a minimal generating set for G. Then S must contain an element x that generates $G/(\mathbb{Z}_2)^4$. Then $|x| = 5$, so, by passing to a conjugate, we may assume $\langle x \rangle = P$. Also, since $|x| = 5$, we know that x acts on $(\mathbb{Z}_2)^4$ via a linear transformation whose minimal polynomial is $\lambda^4 + \lambda^3 + \lambda^2 + \lambda + 1$. Therefore, with respect to any basis of the form $\{v, v^x, v^{x^2}, v^{x^3}\}$,

$$x \text{ acts via multiplication on the right by the matrix } A = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 \end{bmatrix}.$$

(This is "Rational Canonical Form.")

Let s be another element of S. Then $\langle x, s \rangle$ has nontrivial intersection with $(\mathbb{Z}_2)^4$. Since $\mathrm{GL}_k(2)$ does not have any elements of order 5 when $k < 4$, we know that x acts irreducibly, so this implies that $\langle x, s \rangle$ contains all of $(\mathbb{Z}_2)^4$. Therefore $S = \{x, s\}$ (if S is minimal). Obviously, s is of the form $s = x^i v$, for some $v \in (\mathbb{Z}_2)^4$ and (by passing to the inverse if necessary) we may assume $0 \le i \le 2$. If $i = 1$, then $x^{-1}s \in (\mathbb{Z}_2)^4$, so Theorem 2.9 applies. Thus, we may assume $i \in \{0, 2\}$. So

$$S = \{x, v\} \text{ or } S = \{x, x^2 v\},$$

and (by choosing an appropriate basis) $v = (1, 0, 0, 0) \in (\mathbb{Z}_2)^4$.

Case 1. *Assume* $S = \{x, v\}$. We claim that a hamiltonian cycle in $\mathrm{Cay}(G; S)$ is given by:

$$x^4, v, x^{-2}, v, x, v, (x^2, v)^3, (x, v)^2, x^{-2}, v, x, v, x^{-1}, v, (x^2, v)^2, x^{-2}, v, x, v, x^2, v,$$
$$x^{-2}, v, (x^{-1}, v)^2, x, v, x^2, v, x^{-2}, v, x^{-1}, v, x, v, (x^2, v)^2, (x^{-1}, v)^3, x^2, v, x, v.$$

To verify this, we list the vertices of the cycle, using a, b, c, and d to denote the generators of $(\mathbb{Z}_2)^4$, where $a = v$, $b = v^x$, $c = b^x = v^{x^2}$, and $d = c^x = v^{x^3}$. Then $d^x = v^{x^4} = abcd$. The hamiltonian cycle visits the vertices of $\mathrm{Cay}(G; S)$ in the order:

$e, x, x^2, x^3, x^4, bx^4, bx^3, bx^2, bdx^2, bdx^3, bcdx^3, bcdx^4, bcd, abcd, abcdx, abcdx^2, abcx^2,$
$abcx^3, abcx^4, acx^4, ac, c, cx, abdx, abd, abdx^4, adx^4, ad, d, dx^4, bdx^4, bd, bdx, acx, acx^2,$
$acx^3, ax^3, ax^2, ax, bcdx, bcdx^2, bcx^2, bcx^3, bcx^4, cx^4, cx^3, cx^2, cdx^2, cdx, abx, ab, b, bx,$
$acdx, acdx^2, acdx^3, adx^3, adx^2, adx, bcx, bc, abc, abcx, dx, dx^2, dx^3, cdx^3, cdx^4, cd,$
$acd, acdx^4, abcdx^4, abcdx^3, abdx^3, abdx^2, abx^2, abx^3, abx^4, ax^4, a, e.$

Case 2. *Assume* $S = \{x, x^2 v\}$. A hamiltonian cycle in the quotient multigraph $P \backslash \mathrm{Cay}(G; S)$ is given by:

$$x^2 v, x^{-1}, (x^2 v)^{-1}, x^{-4}, x^2 v, x, (x^2 v)^{-1}, x^{-1}, (x^2 v)^{-1}, x^2, (x^2 v)^2.$$

Again we use the notation $a = v$, $b = v^x$, $c = v^{x^2}$, and $d = v^{x^3}$ to list the vertices in this hamiltonian cycle:

$P, Pa, Pabcd, Pcd, Pbc, Pab, Pbcd, Pabc, Pb, Pc, Pad, Pabd, Pacd, Pac, Pbd, Pd, P.$

The edge from Pac to Pbd is a double edge, coming from both x and $x^2 v$, so Lemma 2.4 provides a hamiltonian cycle in $\mathrm{Cay}(G; S)$.   □

3.3   Groups of order 112

Before finding a hamiltonian cycle in $\mathrm{Cay}(G; S)$, we prove two results that determine the structure of G.

Lemma 3.6. *If G is any group of order* 112*, then G has a normal Sylow subgroup.*

Proof by contradiction. Assume G has no normal Sylow subgroups, and let P be a Sylow 7-subgroup of G. Let N be a minimal normal subgroup of G. Since G is solvable (for example, this follows from Burnside's $p^a q^b$ Theorem [7, Thm. 4.3.3]), N is an elementary abelian normal subgroup of G. Since P is not normal, we must have $|N| = 2^k$ for some k.

Case 1. *Assume* $k \neq 3$. We know $k \neq 4$, since the Sylow 2-subgroups are not normal, so $k \in \{1, 2\}$. Furthermore, we know that the Sylow 2-subgroups of G/N are not normal. Observe that $|G/N|$ is either 28 or 56.

     We claim that $PN \lhd G$. If not, then the Sylow 7-subgroup of G/N is not normal, so $|G/N| = 56$ and G/N has eight Sylow 7-subgroups. Thus, there are $|G/N| - |QN/N| = 56 - 8 = 48$ elements of order 7 in G/N. So G/N has only one Sylow 2-subgroup, which must be normal. This contradicts the assumption that G has no normal Sylow subgroups.

Since $|PN| = 7|N| \in \{14, 28\}$, we know P is normal (hence characteristic) in PN, so $P \triangleleft G$. This contradicts the assumption that G has no normal Sylow subgroups.

Case 2. *Assume* $k = 3$. Then $|G/(PN)| = 2$, so $PN \triangleleft G$. Since P does not centralize N (otherwise P would be normal in G), it must act on N via a linear transformation of order 7.

Since there is no normal 7-complement, we know there is an element of G that normalizes P, but does not centralize it [7, Thm. 7.4.3]. So some element of G inverts P, which means that every element of P is conjugate to its inverse.

However, if we let

- g be a generator of P,
- A be the linear transformation induced by g on the vector space $(\mathbb{Z}_2)^3$, and
- $f(\lambda)$ be the minimal polynomial of A,

then $f(\lambda)$ is an irreducible polynomial of degree 3. Since 3 is odd, the roots of $f(\lambda)$ cannot come in pairs, so there is some root α of $f(\lambda)$ (in an extension field), such that α^{-1} is not a root of $f(\lambda)$. Therefore g and g^{-1} do not have the same minimal polynomial, so g is not conjugate to g^{-1} in $\mathrm{GL}_3(2)$. This contradicts the conclusion of the preceding paragraph. $\square$

Corollary 3.7. *If* $|G| = 112$*, and* G *has no normal Sylow* 7*-subgroup, then*

$$G \cong \big(\mathbb{Z}_7 \ltimes (\mathbb{Z}_2)^3\big) \times \mathbb{Z}_2,$$

where a generator of $\mathbb{Z}_7$ *acts via multiplication on the right by the matrix*

$$A = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix}.$$

Proof. Let P be a Sylow 7-subgroup of G. From Lemma 3.6, we know that G has a normal Sylow 2-subgroup Q, so $G = P \ltimes Q$. Since $P \ntriangleleft G$, we know that P acts nontrivially on Q, so it also acts nontrivially on $Q/\Phi(Q)$ [7, Thm. 5.3.5].

Case 1. *Assume* $\Phi(Q)$ *is trivial.* Then $Q \cong (\mathbb{Z}_2)^4$, and a generator x of P acts by a linear transformation. Since

$$|\mathrm{GL}_4(2)| = (2^4 - 1)(2^4 - 2)(2^4 - 2^2)(2^4 - 2^3)$$

is not divisible by 7^2, we know that all subgroups of order 7 in $\mathrm{GL}_4(2)$ are conjugate, so the semidirect product $\mathbb{Z}_7 \ltimes (\mathbb{Z}_2)^4$ is unique. Therefore G must be as described.

Case 2. *Assume* $\Phi(Q)$ *is nontrivial.* Since $7 \nmid (2^i - 1)$ for $1 \in \{1, 2\}$, we must have $|Q/\Phi(Q)| = 2^3$. (So $\Phi(Q) = Q'$ has order 2.) Therefore, a generator x of P acts transitively on the nonidentity elements of $Q/\Phi(Q)$.

If Q is nonabelian, then Q is one of the groups listed in Proposition 3.3(3), since $Q/Q' \cong (\mathbb{Z}_2)^3$. In each of these groups, $\Phi(Q)$ is a proper subgroup of $Z(Q)$. Thus $Z(Q)/\Phi(Q)$ is a proper subspace of $Q/\Phi(Q)$; a contradiction.

Therefore Q is abelian. Then we see that every element of Q has order 2, for otherwise the elements of order 2 in Q provide an invariant, proper subspace of $Q/\Phi(Q)$. This contradicts the fact that $\Phi(Q)$ is nontrivial. $\square$

Proposition 3.8. *If $|G| = 112$, and the Sylow 7-subgroups are not normal, then every connected Cayley graph on G has a hamiltonian cycle.*

Proof. Corollary 3.7 provides an explicit description of G. Let

- x be a generator of $P = \mathbb{Z}_7$,
- $v = (1, 0, 0) \in (\mathbb{Z}_2)^3$, and
- z be a generator of $Z(G) \cong \mathbb{Z}_2$.

Case 1. *Assume $\#S = 2$.* Let s be an element of S that is not in Q. Replacing s by a conjugate, we may assume s is either x or xz.

Since $|x| = 7$, we know that the minimal polynomial of x is a divisor of

$$\lambda^6 + \lambda^5 + \lambda^4 + \lambda^3 + \lambda^2 + \lambda + 1 = (\lambda^3 + \lambda + 1)(\lambda^3 + \lambda^2 + 1) \quad \text{(over } \mathbb{Z}_2\text{)}.$$

So the minimal polynomial of x is either $\lambda^3 + \lambda + 1$ or $\lambda^3 + \lambda^2 + 1$. Since (as explained in the proof of Lemma 3.6), the minimal polynomials of x and x^{-1} are not the same, we may assume (by replacing x with x^{-1} if necessary) that the minimal polynomial of x is $\lambda^3 + \lambda + 1$. Then (for any basis of the form $\{v, v^x, v^{x^2}\}$), x acts on $(\mathbb{Z}_2)^3$ via multiplication on the right by the matrix A in the statement of Corollary 3.7. (This is "Rational Canonical Form.")

Let t be the other element of S. We have $t = x^i v z^j$ for some i and j, where $v = (1, 0, 0) \in (\mathbb{Z}_2)^3$. We may assume $i \in \{0, 1, 2, 4\}$ (by replacing t with its inverse if necessary). Consider the basis $\{a, b, c\}$ of $(\mathbb{Z}_2)^3$ where

$$a = v, \, b = v^x, \text{ and } c = b^x = v^{x^2}.$$

Then G is given by

$$G = \left\langle a, b, c, x, z \; \middle| \; \begin{array}{l} a^2 = b^2 = c^2 = x^7 = z^2 = e, \; a^b = a^c = a^z = a, \\ b^c = b^z = b, c^z = c, \; a^x = b, \; b^x = c, \; c^x = ab, \; x^z = x \end{array} \right\rangle$$

Let $\psi \colon G \to G$ be the homomorphism defined by

$$\psi(a) = bc, \, \psi(b) = ac, \, \psi(c) = b, \, \psi(x) = abcxz, \text{ and } \psi(z) = z.$$

One can show that the relations of the group are preserved by ψ and that ψ is onto. Thus ψ is an automorphism of G that sends the pair $(x^4 v, x)$ to $(x, x^2 v)$; so we may assume $i \neq 4$. Also, if $i = 1$, then Theorem 2.9 applies. Thus, the generating sets to consider are:

- $S = \{x, vz\}$,
- $S = \{x, x^2 vz\}$,
- $S = \{xz, v\}$,
- $S = \{xz, vz\}$,
- $S = \{xz, x^2 v\}$,
- $S = \{xz, x^2 vz\}$.

In all cases, x acts on $(\mathbb{Z}_2)^3$ via multiplication on the right by the matrix A, with respect to the basis $\{a, b, c\}$.

Subcase 1.1. *Assume* $S = \{x, vz\}$. A hamiltonian cycle in $\mathrm{Cay}(G/\langle z \rangle; S)$ is given by:

$$\big(x^{-1}, vz, x, vz, x^4, vz, x, vz, x^2, vz, x^{-2}, vz, x^{-3}, vz, (x^{-4}, vz)^2,$$
$$x^{-3}, vz, x, vz, x^2, vz, x^3, vz, x^{-2}, vz, (x, vz)^2, x^{-3}, vz, x^{-1}\big).$$

To verify this, we list the vertices (according to a coset representative of $\langle z \rangle$) in the order they are visited:

$$e, x^6, bx^6, b, ab, abx, abx^2, abx^3, abx^4, x^4, x^5, cx^5, cx^6, c, ac, acx^6,$$
$$acx^5, ax^5, ax^4, ax^3, ax^2, bcx^2, bcx, bc, bcx^6, bcx^5, bx^5, bx^4, bx^3, bx^2, bx, abcx,$$
$$abc, abcx^6, abcx^5, abx^5, abx^6, ax^6, a, ax, cx, cx^2, cx^3, cx^4, abcx^4, abcx^3, abcx^2, x^2,$$
$$x^3, bcx^3, bcx^4, acx^4, acx^3, acx^2, acx, x, e.$$

Since z is in the center of G, and the generator vz is used an odd number of times in the hamiltonian cycle (specifically, 17 times), the endpoint in G is z, so the Factor Group Lemma (2.1) provides a hamiltonian cycle in $\mathrm{Cay}(G; S)$.

Subcase 1.2. *Assume* $S = \{x, x^2 vz\}$. A hamiltonian cycle in $P\backslash\mathrm{Cay}(G; S)$ is:

$$\big(x^2 vz, x^{-1}, x^2 vz, x, (x^2 vz, x^{-1})^2, (x^2 vz)^{-2}, x, x^2 vz, x, (x^2 vz)^3\big).$$

It passes through the vertices of the quotient multigraph in the order:

$$P, Paz, Pacz, Pab, Pbc, Pcz, Pbz, Pb, Pa, Pz, Pabc, Pac, Pabz, Pbcz, Pc, Pabcz, P.$$

The edge between Pbz and Pb is a double edge, coming from both $x^2 vz$ and $(x^2 vz)^{-1}$, so Lemma 2.4 provides a hamiltonian cycle in $\mathrm{Cay}(G; S)$.

Subcase 1.3. *Assume* $S = \{xz, v\}$. A hamiltonian cycle in $P\backslash\mathrm{Cay}(G; S)$ is:

$$\big(xz, v, (xz)^4, v, xz, v, (xz)^{-1}, v, xz, v, (xz)^2, v\big).$$

It passes through the vertices of the quotient multigraph in the order:

$$P, Pz, Paz, Pb, Pcz, Pab, Pbcz, Pabcz, Pac, Pc, Pbz, Pabz, Pbc, Pabc, Pacz, Pa, P.$$

The edge between P and Pz is a double edge, coming from both xz and $(xz)^{-1}$, so Lemma 2.4 provides a hamiltonian cycle in $\mathrm{Cay}(G; S)$.

Subcase 1.4. *Assume* $S = \{xz, vz\}$. A hamiltonian cycle in $P\backslash\mathrm{Cay}(G; S)$ is:

$$\big(xz, vz, (xz)^2, vz, (xz)^{-1}, vz, (xz)^{-2}, vz, ((xz)^{-1}, vz)^3\big).$$

It passes through the vertices of the quotient multigraph in the order:

$$P, Pz, Pa, Pbz, Pc, Pacz, Pabc, Pbcz, Pab, Pcz, Pac, Pabcz, Pbc, Pabz, Pb, Paz, P.$$

The edge between P and Pz is a double edge, coming from both xz and $(xz)^{-1}$.

Subcase 1.5. *Assume* $S = \{xz, x^2 v\}$. A hamiltonian cycle in $P\backslash\mathrm{Cay}(G; S)$ is:

$$\big(xz, x^2 v, (xz)^2, (x^2 v, xz)^2, (xz)^2, x^2 v, xz, x^2 v, (xz)^{-2}, (x^2 v)^{-1}\big).$$

It passes through the vertices of the quotient multigraph in the order:

$$P, Pz, Paz, Pb, Pcz, Pabcz, Pac, Pab, Pbcz, Pabc, Pacz, Pabz, Pbc, Pc, Pbz, Pa, P.$$

The edge between P and Pz is a double edge, coming from both xz and $(xz)^{-1}$, so Lemma 2.4 provides a hamiltonian cycle in $\mathrm{Cay}(G; S)$.

Subcase 1.6. *Assume* $S = \{xz, x^2vz\}$. A hamiltonian cycle in $P\backslash\mathrm{Cay}(G; S)$ is:

$$\big((xz, x^2vz)^5, (xz)^5, (x^2vz)^{-1}\big).$$

It passes through the vertices of the quotient multigraph in the order:

$$P, Pz, Pa, Pbz, Pb, Pcz, Pabc, Pacz, Pab, Pbcz, Pc, Pabz, Pbc, Pabcz, Pac, Paz, P.$$

The edge between P and Pz is a double edge, coming from both xz and $(xz)^{-1}$, so Lemma 2.4 provides a hamiltonian cycle in $\mathrm{Cay}(G; S)$.

Case 2. *Assume* $\#S > 2$. Every minimal generating set of $G/Z(G) \cong \mathbb{Z}_7 \ltimes (\mathbb{Z}_2)^3$ has only 2 elements, so there exist $s, t \in S$, such that $\langle s, t \rangle = \langle x, v \rangle$. We may assume $s = x$. And we have $t = x^i v$.

Since $\langle s, t \rangle$ has index 2 in G, we must have $\#S = 3$; let u be the third element of S, so $u = x^j wz$ with $w \in (\mathbb{Z}_2)^3$.

- Since $\langle x, x^j wz \rangle = \langle s, u \rangle \neq G$, we must have $w = e$. So $u = x^j z$.
- Then we must have $j = 0$, for otherwise $\langle u \rangle = \langle x, z \rangle \ni x = s$, which contradicts the fact that S is a minimal generating set.

But then $u = z \in Z(G)$, so Lemma 2.6(1) and Remark 2.11 apply. □

4   Preliminaries on groups of order $16p$

Because of Proposition 3.1, we henceforth

<div align="center">assume that the Sylow p-subgroups of G are normal.</div>

Notation.   Throughout the remainder of this paper:

- G is a group of order $16p$, where p is an odd prime,
- $P \cong \mathbb{Z}_p$ is a Sylow p-subgroup of G (and $P \triangleleft G$),
- Q is a Sylow 2-subgroup of G, so $|Q| = 16$, and
- S is a minimal generating set of G.

We wish to show $\mathrm{Cay}(G; S)$ has a hamiltonian cycle.

We know $P \cong \mathbb{Z}_p$, and the possibilities for Q are given in Proposition 3.3.

Lemma 4.1. *We may assume:*

1. *$G = Q \ltimes P$,*
2. *Q is nonabelian, and acts nontrivially on P,*

   3. $G' = Q' \times P$ *is cyclic.*

Proof. (1) Since $P \lhd G$, $G = QP$, and $Q \cap P = \{e\}$, we have $G \cong Q \ltimes P$.

   (2, 3) Since the automorphism group of $P \cong \mathbb{Z}_p$ is abelian, we know Q' centralizes P. So (1) implies that $Q' \leq G' \leq Q' \times P$. Since all of the groups in Proposition 3.3 have a cyclic commutator subgroup, we know Q' is cyclic. Also, by Theorem 2.8, we may assume G' is not a cyclic subgroup of prime-power order. Thus, we may assume $G' \neq Q'$ and $G' \neq P$. So $G' = Q' \times P$ (and $Q' \neq \{e\}$, so Q is nonabelian). Since Q' and P are both cyclic, this implies G' is cyclic. Furthermore, since $P \subset G'$, we know that $G \ncong Q \times P$, so the action of Q on P is nontrivial. $\qquad \square$

   The following corollary shows there are three possibilities for G/G'; each of these possibilities will be considered individually, in Sections 5, 6 and 7, respectively.

Corollary 4.2. *We may assume G/G' is isomorphic to either $\mathbb{Z}_2 \times \mathbb{Z}_2$, $\mathbb{Z}_4 \times \mathbb{Z}_2$, or $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.*

Proof. Since $G = QP$ and $G' = Q'P$ (see Lemma 4.1), we have $G/G' \cong Q/Q'$. Then the desired conclusion follows from inspection of Proposition 3.3. $\qquad \square$

Corollary 4.3. *We may assume*

   1. $Q' \lhd G$,

   2. $Q' \leq \Phi(G)$, *and*

   3. S *is a minimal generating set of* G/Q'.

Proof. (1) From Lemma 4.1(3), we know that Q' is normalized by P (indeed, it is centralized by P). Then, since it is also normalized by Q, it is normalized by $PQ = G$.

   (2) Let M be a maximal subgroup of G.

- If M contains P, then M/P is a maximal subgroup of G/P, so M/P contains $\Phi(G/P) = \Phi(Q)P/P \geq Q'P/P$, so $M \geq Q'$.

- If M does not contain P, then M is a 2-group, so the maximality implies it is a Sylow 2-subgroup of G. Every Sylow 2-subgroup (such as M) contains every normal 2-subgroup (such as Q'), so $M \geq Q'$.

Thus, every maximal subgroup of G contains Q', so $Q' \leq \Phi(G)$.

   (3) Since S is a minimal generating set of G, this follows from (2). $\qquad \square$

Corollary 4.4. *If $G = \langle a, b \rangle$ is 2-generated, then $G' = \langle [a, b] \rangle$.*

Proof. By Lemma 4.1(3), G' is cyclic. Since every subgroup of a cyclic, normal subgroup is normal, we know $\langle [a, b] \rangle \lhd G$. Since $\langle a, b \rangle = G$, and a commutes with b in $G/\langle [a, b] \rangle$, we know $G/\langle [a, b] \rangle$ is abelian, so $G' \subset \langle [a, b] \rangle$. The opposite inclusion is obvious. $\qquad \square$

5 The case where $G/G' \cong \mathbb{Z}_2 \times \mathbb{Z}_2$

Proposition 5.1. *Assume $|G| = 16p$. If $G/G' \cong \mathbb{Z}_2 \times \mathbb{Z}_2$, then $\mathrm{Cay}(G;S)$ has a hamiltonian cycle.*

Proof. We proceed via case-by-case analysis.

Case 1. *Assume $\#S = 2$.* Write $S = \{a, b\}$. Then (a^{-1}, b^{-1}, a, b) is a hamiltonian cycle in $\mathrm{Cay}(G/G'; S)$ whose endpoint in G is $a^{-1}b^{-1}ab = [a, b]$. This generates G' (see Corollary 4.4), so the Factor Group Lemma (2.1) applies.

Case 2. *Assume $\#S \geq 3$.* Since $|G/Q'| = 4p$ is a product of only 3 primes, Corollary 4.3(3) implies $\#S \leq 3$. Therefore $\#S = 3$; write

$$S = \{a, b, c\}.$$

Subcase 2.1. *Assume $|c|$ is divisible by p.* Since $|G/Q'|$ is a product of only 3 primes, and P is the unique subgroup of order p in G, the minimality of S (and Corollary 4.3(3)) implies

- the image of $\langle c \rangle$ in G/Q' has order p, and
- the image of $\langle a, b \rangle$ in G/Q' has order 4.

Thus, b has order 2 in G/Q', so b either centralizes P or inverts it: let $\epsilon \in \{\pm 1\}$ such that $w^b = w^\epsilon$ for all $w \in P$. Since Q' is a cyclic group of order 4, its only automorphisms are the identity automorphism and the one that inverts every element in Q'. Let $\epsilon' \in \{\pm 1\}$, such that $u^b = u^{\epsilon'}$ for all $u \in Q'$. Write $c = uw$ for some $u \in Q'$ and $w \in P$. Then

$$c^b = u^{\epsilon'} w^\epsilon = c^\epsilon u^{\epsilon' - \epsilon} \in c^\epsilon \Phi(Q') \ \text{ since } \ \epsilon' - \epsilon \in \{0, \pm 2\}.$$

Now

$$(a^{-1}, c^{-(p-1)}, b^{-1}, c^{\varepsilon(p-1)}, a, c^{-(p-1)}, b, c^{\varepsilon(p-1)})$$

is a hamiltonian cycle in $\mathrm{Cay}\big(G/Q'; S\big)$ whose endpoint in $G/\Phi(Q')$ is

$$a^{-1}c^{-(p-1)}b^{-1}c^{\varepsilon(p-1)}ac^{-(p-1)}bc^{\varepsilon(p-1)} = a^{-1}b^{-1}ab = [a, b],$$

which generates Q' (see Corollary 4.4). So the Factor Group Lemma (2.1) provides a hamiltonian cycle in $\mathrm{Cay}(G;S)$.

Subcase 2.2. *Assume no element of S has order divisible by p.* This implies that every element of S is a 2-element. Also, since Q/Q' is a Sylow 2-subgroup of G/Q', and $Q/Q' \cong G/G' \cong \mathbb{Z}_2 \times \mathbb{Z}_2$, we know that G/Q' has no elements of order 4. Therefore

$$\text{every element of } S \text{ has order 2 in } G/Q'.$$

So we may assume every element of S has order 2 in $G/\Phi(Q')$, for otherwise Corollary 2.3 and Remark 2.11 apply with $N = Q'$. Then we may assume

$$\text{every element of } S \text{ has order 2,}$$

for otherwise Corollary 2.3 and Remark 2.11 apply with $N = \Phi(Q')$.

Since $G/P \cong Q$ is a 2-generated 2-group, we know that all of its minimal generating sets have the same cardinality, so some 2-element subset of S generates G/P. Since two elements of order 2 always generate a dihedral group, we conclude that

$$Q \cong D_{16} = \langle f, t \,|\, f^2 = t^8 = (ft)^2 = e \rangle.$$

Subsubcase 2.2.1. *Assume no element of S centralizes P.* Let $\overline{S}$ be the image of S in

$$G/Q' \cong (\mathbb{Z}_2 \times \mathbb{Z}_2) \ltimes \mathbb{Z}_p \cong D_{4p}.$$

From Corollary 4.3(3), we see that $\overline{S}$ is a minimal generating set of D_{4p}. Also, by the assumption of this subsubcase, we know that every element of $\overline{S}$ is a reflection; let $f \in \overline{S}$. There are only two proper subgroups of D_{4p} that properly contain $\langle f \rangle$ (because $\mathbb{Z}_2$ and $\mathbb{Z}_p$ are the only nontrivial proper subgroups of the group $\mathbb{Z}_{2p}$ of rotations), so we may assume $\overline{S} = \{f, fx, fy\}$, where x and y are rotations of orders 2 and p in D_{4p}, respectively. Then $\langle fx, fy \rangle = D_{4p}$, which contradicts the minimality of $\overline{S}$.

Subsubcase 2.2.2. *Assume S contains an element that centralizes P.* Each element of S must map to a reflection in $G/P \cong Q \cong D_{16}$ (since the elements of S all have order 2 in both G/P and $G/(Q'P)$). Then, by the assumption of this subsubcase, we know that some reflection centralizes P. Because Q acts nontrivially on P, we have

$$G = \langle f, t, w \mid f^2 = t^8 = w^p = e,\ ftf = t^{-1},\ fwf = w,\ t^{-1}wt = w^{-1} \rangle.$$

From the assumption of this subsubcase, we may assume $f \in S$. By the minimality of S, we must have $\langle f, s \rangle = Q$, for some $s \in S$ (after replacing Q by a conjugate). Since all elements of $S \cap Q$ are reflections, we may assume $s = ft$. To generate G (and map to a reflection in G/P), the final element of S must be of the form $ft^i w^j$, with $p \nmid j$. By replacing w with w^j, we may assume $j = 1$. So the final element of S is $ft^i w$. Since all elements of S have order 2 in G, it must be the case that t^i inverts w, so i is odd. So

$$S \text{ is of the form } \{f, ft, ft^i w\}, \text{ with } i \text{ odd}.$$

By Corollary 4.3(1), we know $Q' \lhd G$. Observe that the image of f is central in G/Q', and $ft^i w \equiv ftw \pmod{Q'}$ (because $Q' = \langle t^2 \rangle$ and i is odd), so

$$\mathrm{Cay}(G/Q'; S) \cong \mathrm{Cay}\big(\langle ft, ft^i w \rangle / Q'; \{ft, ft^i w\}\big) \times \mathrm{Cay}\big(\langle f \rangle; \{f\}\big) \cong C_{2p} \times K_2$$

is a prism, which has the natural hamiltonian cycle $\big((ft, ft^i w)^p \#, f\big)^2$. The endpoint in G is

$$\begin{aligned}
\Big(\big((ft)(ft^i w)\big)^p (ft^i w)^{-1} f\Big)^2 &= \Big((t^{i-1}w)^p w^{-1} t^{-i}\Big)^2 \\
&= \big(t^{(i-1)p-i} w^{-1}\big)^2 \\
&= t^{2(i-1)p - 2i}.
\end{aligned}$$

Since i is odd, the exponent of t is congruent to 2 modulo 4, so the endpoint generates $\langle t^2 \rangle = Q'$. Thus, the Factor Group Lemma (2.1) provides a hamiltonian cycle in $\mathrm{Cay}(G; S)$. $\qquad\square$

6   The case where $G/G' \cong \mathbb{Z}_4 \times \mathbb{Z}_2$

Proposition 6.1. *Assume $|G| = 16p$. If $G/G' \cong \mathbb{Z}_4 \times \mathbb{Z}_2$, then $\mathrm{Cay}(G; S)$ has a hamiltonian cycle.*

Proof. We proceed via case-by-case analysis.

Case 1. *Assume $\#S = 2$.* Let

- $S = \{a, b\}$, with a of order 4 in G/G', and
- $k \in \mathbb{Z}$ with $g^a = g^k$ for $g \in G'$.

Then (a^{-3}, b^{-1}, a^3, b) is a hamiltonian cycle in G/G', and its endpoint in G is

$$[a^3, b] = [a, b]^{a^2}[a, b]^a[a, b] = [a, b]^{k^2}[a, b]^k[a, b] = [a, b]^{k^2+k+1}.$$

By Corollary 4.4, this generates G' unless $\gcd(k^2 + k + 1, |G'|) > 1$. Since $|G'| = 2p$, and $k^2 + k + 1$ is always odd, this generates G' unless $k^2 + k + 1 \equiv 0 \pmod{p}$, which implies $k^3 \equiv 1 \pmod{p}$. This means that a^3 centralizes P. But $a^4 \in G' \leq C_G(P)$, so this implies that a centralizes P: therefore $k \equiv 1 \pmod{p}$. Since $k^2 + k + 1 \equiv 0 \pmod{p}$, we conclude that

$$p = 3 \text{ and } a \text{ centralizes } P.$$

From Lemma 4.1(2) (and the fact that a centralizes P), we know that

$$b \text{ does not centralize } P.$$

Since $G' = Q'P$ is cyclic of order 6, we know G' has only two automorphisms; namely, the identity automorphism and the automorphism that inverts G'. Thus $x^b = x^{-1}$ for all $x \in G'$. If b has order 4 in G/G', then the hamiltonian cycle (b^{-3}, a^{-1}, b^3, a) in $\mathrm{Cay}(G/G'; S)$ has endpoint

$$[b^3, a] = [b, a]^{b^2}[b, a]^b[b, a] = [b, a][b, a]^{-1}[b, a] = [b, a]$$

in G, which generates G'. Thus $\mathrm{Cay}(G; S)$ has a hamiltonian cycle by the Factor Group Lemma (2.1). So we may assume that b has order 2 in G/G'. Write $b = qw$ for some $q \in Q$ and $w \in P$, where $q^{-1}wq = w^{-1}$. Then $b^2 = q^2 w^q w = q^2$. Hence, the order of b is not divisible by p, so b is a 2-element. Thus, we may assume (after replacing Q by a conjugate) that $b \in Q$. Thus, the order of b in G/Q' is 2. So we may assume $|b| = 2$, for otherwise Corollary 2.3 and Remark 2.11 apply.

Since $b \in Q$, and $\langle a, b \rangle = G$, we know $a \notin Q$. Since a centralizes P, this implies that $|a|$ is divisible by p (i.e., 3). But $|a|$ is also a multiple of 4 (its order in G/G'). So $|a|$ is divisible by 12. Since $|G| = 16p = 48$ (and G is not cyclic), this implies $|a|$ is either 12 or 24. If $|a| = 24$, then $G = \langle b \rangle \ltimes \langle a \rangle$, so Theorem 2.5 applies. So we may assume $|a| = 12$.

Now, of the three groups listed in Proposition 3.3(2),

- group (2a) has no generating set without an element of order 8, and
- group (2b) has no 2-element generating set with an element of order 2.

So Q must be group (2c), and we may assume $a = xw$ (by relabeling the elements of Q).

Since $\langle a, b \rangle = G$, we know $\langle x, b \rangle = Q$, so (since $|b| = 2$), we may assume $b = y$ (by further relabeling the elements of Q). Note that, since $z \in Z(G)$, we know z centralizes both a and b.

Let $N = \langle a^2 \rangle = \langle x^2, w \rangle$, and consider the hamiltonian cycle $\left((b, a)^4 \#, a^{-1} \right)$ in $\mathrm{Cay}(G/N; S)$, which passes through the vertices in the following order:

$$N, Ny, Nxyz, Nxz, Nz, Nyz, Nxy, Nx, N.$$

Its endpoint in G is

$$(ba)^4 a^{-2} = (yxw)^4 a^{-2} = e \cdot a^{-2} = a^{-2},$$

which generates $\langle a^2 \rangle = N$. So the Factor Group Lemma (2.1) provides a hamiltonian cycle in $\mathrm{Cay}(G; S)$.

Case 2. *Assume* $\#S > 2$. Since $G/G' \cong \mathbb{Z}_4 \times \mathbb{Z}_2$, there exists a 2-element subset $\{a, b\}$ of S that generates G/P. Since $\{a, b\} \subsetneq S$, and S is minimal, we have $P \not\subset \langle a, b \rangle$. Therefore, by passing to a conjugate, we may assume $\langle a, b \rangle = Q$.

Let c be a third element of S (so $c \notin Q$). Then $\langle a, b, c \rangle$ properly contains Q. But Q is a maximal subgroup of G (since $|G/Q| = p$ is prime), so this implies $\langle a, b, c \rangle = G$. So the minimality of S implies $S = \{a, b, c\}$.

Claim 6.2. *We may assume, for each* $s \in S$, *that either* $s^2 \in P$, *or* $sP \in \Phi(Q)P$, *or* s *acts on* P *via an automorphism of order* 4.

Suppose there exists $s \in S$ that has none of the three properties. Since $\#S > 2$ and $sP \notin \Phi(Q)P$, we know $p \nmid |s|$, so (up to conjugacy) $s \in Q$. Then, since $Q/Z(Q) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$, we have $s^2 \in Z(Q)$, so $\langle s^2 \rangle \lhd Q$. Also, since s does not act on P by an automorphism of order 4, we know s^2 centralizes P. Therefore $s^2 \in Z(G)$, so $\langle s^2 \rangle \lhd G$, Hence, Corollary 2.3 and Remark 2.11 apply.

Subcase 2.1. *Assume* $Q \cong \mathbb{Z}_4 \ltimes \mathbb{Z}_4 = \langle x \rangle \ltimes \langle y \rangle$. Since some element of S must generate $G/(\langle y \rangle P)$, we may assume $x \in S$ (after replacing Q by a conjugate). That is, we may assume $a = x$.

Observe that $x^2 \notin P$ and $xP \notin \Phi(Q)P$. Thus, the Claim tells us that x acts on P via an automorphism of order 4. Hence, $Q/C_Q(P) \cong \mathbb{Z}_4$. Therefore, $C_Q(P)$ is a cyclic normal subgroup of Q with a cyclic quotient, so we may assume $C_Q(P) = \langle y \rangle$.

Since Q has no 2-element generating set that contains an element of order 2, we know $|b| > 2$. Therefore, from the Claim, we know that b generates $Q/C_Q(P) = Q/\langle y \rangle$. So $b \equiv a^{\pm 1} \pmod{\langle y \rangle}$; assume (by replacing b with its inverse if necessary) that $ba \in \langle y \rangle$. Then, since $\langle a, b \rangle = Q$, we must have $\langle ba \rangle = \langle y \rangle \lhd G$. Then, since $|y| = 4$, Corollary 2.2 and Remark 2.11 apply.

Subcase 2.2. *Assume* $c \notin \Phi(Q)P$. Since Q does not centralize P, we may assume b does not centralize P. Write $c = wu$ for some $w \in P$ and $u \in Q$. Since $c \notin Q$, we have $w \neq e$. Since b does not centralize P, we have $(w^{-1})^b \neq w^{-1}$. Thus

$$[b, c] = (u^{-1})^b (w^{-1})^b wu = (u^{-1})^b u ((w^{-1})^b w)^u,$$

where $(u^{-1})^b u \in Q$, $((w^{-1})^b w)^u \in P$, and $((w^{-1})^b w)^u \neq e$. Hence, $[b, c] \notin Q'$ and $[b, c] \in G' = Q' \times P$. Thus the order of $[b, c]$ is a divisor of $|G'| = 2p$, but not a divisor

of $|Q'| = 2$. Hence, p divides the order of $[b, c]$ and we must have $P \subset \langle [b, c] \rangle$. If $c \in \{a, ab\}\Phi(Q)P$, then $\langle b, c \rangle = G$ which contradicts the minimality of S. Thus $c \in b\,\Phi(Q)P$. (But we may assume $c \notin b^{\pm 1}P$, for otherwise Corollary 2.2 and Remark 2.11 apply.) Since $c \notin a\Phi(Q)P$, the argument of the preceding paragraph (by interchanging a and b) implies that a must centralize P. That is, $a \in C_Q(P)$. Therefore, the Claim implies $|a| = 2$. In summary, we know:

- $|a| = 2$, and a centralizes P,

- b does not centralize P, and

- $c \in b\,\Phi(Q)\,P$, but $c \notin b^{\pm 1}P$.

Subsubcase 2.2.1. *Assume* $Q \cong \mathbb{Z}_2 \ltimes \mathbb{Z}_8 = \langle x \rangle \ltimes \langle y \rangle$. Since $|a| = 2$, we may assume $a = x$. Then we must have $|b| = 8$, so we may assume $b = y$. Then $\Phi(Q) = \langle b^2 \rangle$, so $c \in \{b^3, b^5\}P$. By replacing c with its inverse, we may assume $c \in b^5 P$. Then

$$S = \{a, b, c\} \text{ with } a = x, \; b = y, \text{ and } c = y^5 w, \text{ where } w \text{ generates } P.$$

Also, from the above properties of a and b, we know x centralizes P, but y acts on P via an automorphism of order 4.

Consider the hamiltonian cycle

$$(b^2, c^{-1}, b^2, c, b^{-1}, a, b^{-7}, a)$$

in $\mathrm{Cay}(G/P; S)$, which passes through the vertices of the graph in the order:

$$P, Py, Py^2, Py^5, Py^6, Py^7, Py^4, Py^3, Pxy^7, Pxy^6, Pxy^5, Pxy^4,$$
$$Pxy^3, Pxy^2, Pxy, Px, P.$$

Note that, since the action of y on P has order 4, we know that y^2 inverts w, so the endpoint in G is

$$b^2 c^{-1} b^2 c b^{-1} a b^{-7} a = y^2 (w^{-1} y^{-5}) y^2 (y^5 w) y^{-1} x y^{-7} x = y^2 w^{-1} y^2 w y^{-1} x y x = w^2,$$

which generates $P = \langle w \rangle$. By the Factor Group Lemma (2.1), we have a hamiltonian cycle in $\mathrm{Cay}(G; S)$.

Subsubcase 2.2.2. *Assume* $Q \cong \mathbb{Z}_4 \ltimes (\mathbb{Z}_2 \times \mathbb{Z}_2) = \langle x \rangle \ltimes \langle y, z \rangle$. Since $|a| = 2$, we may assume $a = y$. Then we may assume $b = x$. Since $\Phi(Q) = \langle b^2, z \rangle$, we must have $c \in \{bz, b^{-1}z\}P$. By replacing c with its inverse, we may assume $c \in bzP$. Then

$$S = \{x, y, xzw\}, \text{ where } w \text{ generates } P.$$

And y centralizes P, but x acts on P via an automorphism of order 4.

Let $k \in \mathbb{Z}_p$, such that $x^{-1}wx = w^k$. Since the action of x on P has order 4, we have $2 \le k \le p - 2$. Consider the hamiltonian cycle

$$(xzw, x^3, y, x^2, xzw, x^3, xzw, y, x^{-3})$$

in $\mathrm{Cay}(G/P; S)$ that passes through the vertices of this graph in the order:

$$P, Pxz, Px^2z, Px^3z, Pz, Pyz, Pxy, Px^2yz, Px^3yz, Py, Pxyz, Px^2y,$$
$$Px^3y, Px^3, Px^2, Px, P.$$

The endpoint of this cycle in G is

$$(xzw)(x^3yx^3zw)(x^4zw)(yx^{-3}) = (xzw)(x^2yw)(zw)(xyz)$$
$$= x^4y^2z^4w^{-k}w^kw^k = w^k.$$

Since k is coprime to p (recall $2 \le k \le p - 2$), this generates $P = \langle w \rangle$. By the Factor Group Lemma (2.1), we have a hamiltonian cycle in $\mathrm{Cay}(G; S)$.

Subcase 2.3. *Assume $c \in \Phi(Q)\, P$. We may assume $c \notin G'$, for otherwise Lemma 2.7 applies.*

Subsubcase 2.3.1. *Assume $Q \cong \mathbb{Z}_2 \ltimes \mathbb{Z}_8 = \langle x \rangle \ltimes \langle y \rangle$.* Up to automorphism, any 2-element generating set of Q is of the form $\{xy^i, y\}$. Since xy^4 has order 2, it may be replaced with x (if $i \in \{3, 4, 5\}$). This implies that we may assume $-2 \le i \le 2$. Then, since we may replace y with y^{-1}, we may assume $0 \le i \le 2$. However, xy^2 has order 4, but its square is in Q', so it cannot act on P by an automorphism of order 4; therefore, the Claim implies it is not in S. So $i \in \{0, 1\}$.

Since $\Phi(Q) = \langle y^2 \rangle$ and $Q' = \langle y^4 \rangle$, we must have $c \in \{y^2, y^6\}P$; replacing c with c^{-1}, we may assume $c \in y^2 P$. Thus, either

$$S = \{x, y, y^2w\} \quad \text{or} \quad S = \{xy, y, y^2w\}, \quad \text{where } \langle w \rangle = P.$$

Also:

- x either centralizes P or inverts it, and
- y acts on P by an automorphism of order 4.

Let $\epsilon \in \{\pm 1\}$ such that $x^{-1}wx = w^\epsilon$, and let $k \in \mathbb{Z}_p$ such that $y^{-1}wy = w^k$. Since the action of y on P has order 4, we have $2 \le k \le p - 2$. Let $N = \langle y^4, P \rangle = \langle y^4w \rangle \cong \mathbb{Z}_{2p}$.

For the first generating set,

$$(y^2w, y^{-1}, y^2w, x, y^{-3}, x)$$

is a hamiltonian cycle in $\mathrm{Cay}(G/N; S)$ that passes through the vertices of this graph in the order:
$$N, Ny^2, Ny, Ny^3, Nxy^3, Nxy^2, Nxy, Nx, N.$$

The endpoint of this cycle in G is

$$y^2wywxy^{-3}x = y^2wywy = y^2wy^2w^k = y^4w^{k-1}.$$

Since $k - 1$ is coprime to p (recall $2 \le k \le p - 2$), and y^4 has order 2, this generates $N = \langle y^4w \rangle$. So the Factor Group Lemma (2.1) provides a hamiltonian cycle in $\mathrm{Cay}(G; S)$.

For the second generating set,

$$\left(xy, y^{-1}, y^2w, y, (xy)^{-1}, y^{-1}, y^2w, y\right)$$

is a hamiltonian cycle in $\mathrm{Cay}(G/N; S)$ that passes through the vertices of this graph in the order:

$$N, Nxy, Nx, Nxy^2, Nxy^3, Ny^2, Ny, Ny^3, N.$$

The endpoint of this cycle in G is

$$xy^2 wx^{-1} ywy = xy^2 x^{-1} w^\epsilon y^2 w^k = y^4 w^{k-\epsilon}$$

(with $\epsilon \in \{\pm 1\}$ depending on whether x centralizes or inverts P.) Since $k - 1$ and $k + 1$ are coprime to p (recall $2 \leq k \leq p - 2$) and y^4 has order 2, this generates $N = \langle y^4 w \rangle$. So the Factor Group Lemma (2.1) provides a hamiltonian cycle in $\mathrm{Cay}(G; S)$.

Subsubcase 2.3.2. *Assume* $Q \cong \mathbb{Z}_4 \ltimes (\mathbb{Z}_2 \times \mathbb{Z}_2)$. Up to automorphism, any 2-element generating set of Q is of the form $\{x, x^i y\}$. Of course, by replacing x with x^{-1}, we may assume $0 \leq i \leq 2$. Also, since $x^2 y$ has order 2, it may be replaced with y; so we may assume $i \in \{0, 1\}$.

Since $\Phi(Q) = \langle x^2, z \rangle$ and $Q' = \langle z \rangle$, we must have $c \in \{x^2, x^2 z\} P$. Thus, letting w be a generator of P, either:

$$S = \{x, y, x^2 w\} \ \text{ or } \ S = \{x, xy, x^2 w\}, \ \text{ or } \ S = \{x, y, x^2 zw\}, \ \text{ or } \ S = \{x, xy, x^2 zw\}.$$

Also:

- x acts on P by an automorphism of order 4 (so x^2 inverts P),
- y either centralizes P or inverts it, and
- z centralizes P.

Let $k \in \mathbb{Z}_p$, such that $x^{-1} wx = w^k$. Since the action of x on P has order 4, we have $2 \leq k \leq p - 2$. Let $N = \langle z, P \rangle$. Since z centralizes P, the order of z is 2, and the order of w is p, we have $N = \langle zw \rangle \cong \mathbb{Z}_{2p}$.

For the first generating set,

$$\left(x^2 w, x^{-1}, x^2 w, y, x^{-3}, y \right)$$

is a hamiltonian cycle in $\mathrm{Cay}(G/N; S)$ that passes through the vertices of this graph in the order:

$$N, Nx^2, Nx, Nx^3, Nx^3 y, Nx^2 y, Nxy, Ny, N.$$

Similarly, replacing each instance of $x^2 w$ with $x^2 zw$ yields a hamiltonian cycle in the graph $\mathrm{Cay}(G/N; S)$ for the third generating set that passes through the vertices of this graph in the same order as the hamiltonian cycle for the first generating set. Since z is in the center of G and z appears exactly twice in the list of edges, the endpoints of these cycles in G are the same and they are given by

$$x^2 wxwyxy = x^2 wxwxz = x^2 wx^2 w^k z = x^4 w^{k-1} z = w^{k-1} z.$$

Since $k - 1$ is coprime to p, and z has order 2, this generates $N = \langle wz \rangle$. So the Factor Group Lemma (2.1) provides a hamiltonian cycle in $\mathrm{Cay}(G; S)$.

For the second generating set,

$$\left(x^2 w, x, x^2 w, xy, x^3, (xy)^{-1} \right)$$

is a hamiltonian cycle in $\mathrm{Cay}(G/N; S)$ that passes through the vertices of this graph in the order:

$$N, Nx^2, Nx^3, Nx, Nx^2y, Nx^3y, Ny, Nxy, N.$$

Similarly, replacing each instance of x^2w with x^2zw yields a hamiltonian cycle in the graph $\mathrm{Cay}(G/N; S)$ for the fourth generating set that passes through the vertices in the same order as the hamiltonian cycle for the second generating set. Since z is in the center of G and z appears exactly twice in the list of edges, the endpoints of each cycle are the same and is given by

$$x^2wx^3wxyx^3y^{-1}x^{-1} = x^2wx^3wxyx^2yz = x^2wx^3wx^3z = x^2wx^2w^{-k}z = w^{-(k+1)}z.$$

Since z has order 2 and $-(k+1)$ is coprime to p (recall $2 \leq k \leq p-2$), this generates $N = \langle wz \rangle$. So the Factor Group Lemma (2.1) provides a hamiltonian cycle in $\mathrm{Cay}(G; S)$. □

7   The case where $G/G' \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$

Proposition 7.1. *Assume* $|G| = 16p$. *If* $G/G' \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, *then* $\mathrm{Cay}(G; S)$ *has a hamiltonian cycle.*

Proof. We proceed via case-by-case analysis.

Case 1. *Assume* $\#S = 3$. Write $S = \{a, b, c\}$. Since $G/G' \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, it is easy to see that the sequence

$$(a, b, a, c, a, b, a, c)$$

is a hamiltonian cycle in $\mathrm{Cay}(G/G'; S)$. Also, since every nontrivial element of G/G' has order 2, we know $s^{-1} \equiv s \pmod{G'}$, for every $s \in S$, so, for any choice of $i_1, \ldots, i_8 \in \{\pm 1\}$,

$$(a^{i_1}, b^{i_2}, a^{i_3}, c^{i_4}, a^{i_5}, b^{i_6}, a^{i_7}, c^{i_8}) \text{ is a hamiltonian cycle in } \mathrm{Cay}(G/G'; S). \qquad (7.1)$$

Now:

- If $|a| = 2p$, then a has order 2 in G/P, but not in G, so Corollary 2.3 and Remark 2.11 apply.
- If $|a| = 4p$, then a^2 generates G'. Since $\langle a \rangle / G'$ is normal in $G/G' \cong (\mathbb{Z}_2)^3$, we have $\langle a \rangle \lhd G$. Choose $\beta, \gamma \in \{\pm 1\}$ such that

$$x^b = x^\beta \text{ and } x^c = x^\gamma, \text{ for all } x \in \langle a \rangle.$$

Then, letting $i_k = 1$ for $k \notin \{1, 3, 5\}$, the endpoint of the path (7.1) in G is

$$a^{i_1}ba^{i_3}ca^{i_5}bac = a^{i_1}a^{\beta i_3}a^{\beta \gamma i_5}g \in G' = \langle a^2 \rangle, \text{ where } g = bcbac.$$

Since each of i_1, i_3, i_5 can be ± 1 independently, the endpoints that can be obtained in this way are:

$$a^{-3}g, \ a^{-1}g, \ ag, \ a^3g.$$

Since $\langle a^2 \rangle \cong \mathbb{Z}_{2p}$, and at least one of any 4 consecutive integers is relatively prime to $2p$, it must be the case that at least one of these endpoints generates $\langle a^2 \rangle = G'$. So the Factor Group Lemma (2.1) applies.

Thus, we may assume no element of S has order divisible by p. Therefore, $s^2 \in Q'$ for every $s \in S$. So we may assume

$$\text{every element of } S \text{ has order 2}$$

for otherwise Corollary 2.3 and Remark 2.11 apply.

Let

$$g' = abacabac = [a,b]\,bc\,[a,b]\,bc$$

be the endpoint of the path (7.1) in G.

Observation 7.2. For future reference, we note the following:

1. Since Q_8 is not generated by elements of order 2, we know Q is not the group described in (3b) of Proposition 3.3.

2. Suppose Q is the group described in (3c) of Proposition 3.3. Let $\overline{S}$ be the image of S in Q. It is not difficult to see that xyz is the only element of order 2 that is of the form $x^i y^j z$. Thus, we must have $xyz^{\pm1} \in S$, and the other two elements of S must be in $\langle x, y \rangle$. Since all elements of S have order 2 (and $|xy| = 4$), we conclude that S is of the form
   $$\overline{S} = \{\, xz^{2i}, yz^{2j}, xyz^{\pm1} \,\}.$$
   Up to automorphism (replacing x with xz^{2i}, replacing y with yz^{2j}, and, if necessary, replacing z with z^{-1}), we have
   $$\overline{S} = \{\, x, y, xyz \,\} \qquad \text{(if } Q = \mathbb{Z}_2 \ltimes (\mathbb{Z}_2 \times \mathbb{Z}_4)\text{).} \tag{7.2}$$

Subcase 1.1. *Assume $[b,c]$ generates G'.* Since both b and c have order 2, they generate a dihedral group. Since $G' = \langle (bc)^2 \rangle$ has order $2p$, we know $\langle bc \rangle$ has order $4p$ and $\langle b, c \rangle \cong D_{8p}$. Thus both b and c invert $\langle bc \rangle$ and G'.

Therefore bc centralizes G', so $g' = [a,b]^2[b,c]$. So the Factor Group Lemma (2.1) applies unless $P \subset \langle [a,b] \rangle$ (which implies that a inverts P), and

$$[b,c] \equiv [a,b]^{-2} \pmod{Q'}. \tag{7.3}$$

Replacing Q by a conjugate, we may assume $b \in Q$. Write $a = \overline{a}w$ and $c = \overline{c}w'$ with $\overline{a}, \overline{c} \in Q$ and $w, w' \in P$. Since both a and c invert P, we know both $\overline{a}$ and $\overline{c}$ invert P.

We have

$$[b,c] = (bc)^2 = (b\overline{c}w')^2 = (b\overline{c})^2 (w')^2$$

and

$$[a,b] = (ab)^2 = (\overline{a}wb)^2 = (\overline{a}b)^2 w^{-2} \text{ (since } \overline{a} \text{ and } b \text{ invert } P\text{),}$$

so (7.3) tells us that

$$w' = w^2. \tag{7.4}$$

Subsubcase 1.1.1. *Assume $[a,b]$ generates G'.* We may interchange a and c, so the preceding calculations tell us that $w = (w')^2 = (w^2)^2 = w^4$. Therefore, we must have $p = 3$.

Subsubsubcase 1.1.1.1. *Assume Q is as described in Proposition 3.3(3c).* From (7.2) and (7.4), we see that

$$S = \{xw, y, xyzw^{-1}\}, \quad \text{where } P = \langle w \rangle.$$

Let $N = \langle xy \rangle = \{e, xy, z^2, xyz^2\}$ be the cyclic group of order 4 generated by xy. Observe that $N \triangleleft G$ and that the graph $\mathrm{Cay}(G/N; S)$ is isomorphic to $\mathrm{Cay}(D_{12}; \{R, F\})$, where $\{R, F\}$ is the natural generating set for D_{12}, under the vertex identification ϕ : $G/N \to D_{12}$ given by

$$\phi(N(xwy)^k) = R^{2k},$$
$$\phi(N(xwy)^k(xw)) = R^{2k+1},$$
$$\phi(N(xwy)^k(xyzw^{-1})) = R^{2k}F, \text{ and}$$
$$\phi(N(xwy)^k(xw)(xyzw^{-1})) = R^{2k+1}F,$$

for any integer k. The natural hamiltonian cycle $(R^5, F)^2$ in $\mathrm{Cay}(D_{12}; \{R, F\})$ corresponds to the hamiltonian cycle

$$((xw, y)^3 \#, xyzw^{-1}, (y, xw)^3 \#, xyzw^{-1})$$

in $\mathrm{Cay}(G/N; S)$. The endpoint in G is

$$(xwy)^3(y^{-1})(xyzw^{-1})(yxw)^3(xw)^{-1}(xyzw^{-1}) =$$
$$= (xyz^2)(y)(xyzw^{-1})(xy)(w^{-1}x)(xyzw^{-1})$$
$$= (xyz^2)(xz^{-1}w^{-1})(xy)(yzw)$$
$$= (yz^{-1}w^{-1})(xzw) = xyz^2 = (xy)^{-1},$$

which generates $\langle xy \rangle = N$. Thus, the Factor Group Lemma (2.1) provides a hamiltonian cycle in $\mathrm{Cay}(G; S)$.

Subsubsubcase 1.1.1.2. *Assume* $Q = D_8 \times \mathbb{Z}_2 = \langle f, t \rangle \times \mathbb{Z}_2$. Since $[\overline{a}, b]$ is nontrivial, we may assume $\overline{a} = f$ and $b = ft$. Because $\langle b, c \rangle$ is a dihedral group and S is minimal, we must have $\overline{c} = ft^i z$, for some integer i. Since $[b, \overline{c}] = (b\overline{c})^2 = (ftft^i z)^2 = t^{2i-2}$ is nontrivial, i must be even. We may replace z with $t^2 z$ since the order of $t^2 z$ is 2 and $t^2 z \in Z(Q)$. Thus we may assume $\overline{c} = fz$. Then, from (7.4), we see that

$$S = \{fw, ft, fzw^{-1}\},$$

where f inverts w, whereas t and z centralize w (and w is a generator of P).

Let $N = \langle tz \rangle = \{e, tz, t^2, t^3 z\}$ be the cyclic group of order 4 generated by tz. Observe that $N \triangleleft G$ and that $\mathrm{Cay}(G/N; S)$ is graph isomorphic to $\mathrm{Cay}(D_{12}; \{R, F\})$, where $\{R, F\}$ is the natural generating set for D_{12}, under the vertex identification $\phi: G/N \to D_{12}$ given by

$$\phi(N((ft)(fzw^{-1}))^k) = R^{2k},$$
$$\phi(N((ft)(fzw^{-1}))^k(ft)) = R^{2k+1},$$
$$\phi(N((ft)(fzw^{-1}))^k(fw)) = R^{2k}F, \text{ and}$$
$$\phi(N((ft)(fzw^{-1}))^k(ft)(fw)) = R^{2k+1}F,$$

for any integer k. The natural hamiltonian cycle $(R^5, F)^2$ in $\mathrm{Cay}(D_{12}; \{R, F\})$ corresponds to the hamiltonian cycle

$$((ft, fzw^{-1})^3 \#, fw, (fzw^{-1}, ft)^3 \#, fw)$$

in $\text{Cay}(G/N; S)$. The endpoint in G is

$$
\begin{aligned}
(ftfzw^{-1})^3(fzw^{-1})^{-1}(fw)(fzw^{-1}ft)^3(ft)^{-1}(fw) &= \\
&= (tz)(wz^{-1}f^{-1})(fw)(t^3z)(t^{-1}f^{-1})(fw) \\
&= (tz)(wz^{-1}w)(t^3z)(t^{-1}w) \\
&= (tw^2)(t^2zw) = t^3z = (tz)^{-1},
\end{aligned}
$$

which generates $\langle tz \rangle = N$. Thus, the Factor Group Lemma (2.1) provides a hamiltonian cycle in $\text{Cay}(G; S)$.

Subsubcase 1.1.2. *Assume* $[a, b]$ *does not generate* G'. Because we could interchange b and c, we may assume $[a, c]$ also does not generate G'. Since

$$
[a, c] = (ac)^2 = (\bar{a}w\,\bar{c}w^2)^2 = (\bar{a}\,\bar{c}w)^2 = (\bar{a}\,\bar{c})^2w^2,
$$

and w^2 generates P, this implies that $\bar{a}$ commutes with $\bar{c}$. By the same argument, $\bar{a}$ commutes with b. So $\bar{a}$ is in the center of Q. Therefore $Q = \langle b, \bar{c} \rangle \times \langle \bar{a} \rangle$. Looking at the list of groups in Proposition 3.3(3) (and recalling that $\bar{a}$, b, and $\bar{c}$ all have order 2), we conclude that $Q = D_8 \times \mathbb{Z}_2$. Furthermore, we have $\bar{a} = z$, and $\langle b, \bar{c} \rangle = D_8$, so we may assume

$$
S = \{zw, f, ftw^2\}
$$

where f and z invert w, and t centralizes w (and w is the generator of P).

Let $N = Q' = \langle t^2 \rangle = \{e, t^2\}$. Observe that the graph $\text{Cay}(G/N; S)$ is isomorphic to $\text{Cay}(\mathbb{Z}_2 \ltimes \mathbb{Z}_{4p}; \{X, Y\})$, where $\{X, Y\}$ is the natural generating set for $\mathbb{Z}_2 \ltimes \mathbb{Z}_{4p}$ given by

$$
\mathbb{Z}_2 \ltimes \mathbb{Z}_{4p} = \langle X, Y \mid X^2 = Y^{4p} = 1, X^{-1}YX = Y^{2p-1} \rangle.
$$

This graph isomorphism is given by the vertex identification $\phi \colon G/N \to \mathbb{Z}_2 \ltimes \mathbb{Z}_{4p}$ where

$$
\begin{aligned}
\phi(N(fftw^2)^k) &= Y^{2k}, \\
\phi(N(fftw^2)^k f) &= Y^{2k+1}, \\
\phi(N(fftw^2)^k(zw)) &= Y^{2k}X, \text{ and} \\
\phi(N(fftw^2)^k(f)(zw)) &= Y^{2k+1}X,
\end{aligned}
$$

for any integer k. The hamiltonian cycle $(Y^{2p-1}, X)^4$ in $\text{Cay}(\mathbb{Z}_2 \ltimes \mathbb{Z}_{4p}; \{X, Y\})$ corresponds to the hamiltonian cycle

$$
\left((f, ftw^2)^p\#, zw, (ftw^2, f)^p\#, zw\right)^2
$$

in $\text{Cay}(G/N; S)$. The endpoint in G is

$$
\begin{aligned}
\left((fftw^2)^p(ftw^2)^{-1}(zw)(ftw^2f)^p(f)^{-1}(zw)\right)^2 &= \\
&= \left((t^p)(w^{-2}t^{-1}f^{-1})(zw)(t^{-p})(f^{-1})(zw)\right)^2 \\
&= \left((ft^{-p+1}w^2)(zw)(ft^p)(zw)\right)^2 \\
&= (t^{2p-1})^2 = t^2,
\end{aligned}
$$

which generates $\langle t^2 \rangle = N$. Thus, the Factor Group Lemma (2.1) provides a hamiltonian cycle in $\mathrm{Cay}(G; S)$.

Subcase 1.2. *Assume there do not exist $s, t \in S$, such that $\langle [s, t] \rangle = G'$. Then, since*

$$\langle [a, b], [a, c], [b, c] \rangle = G' = Q' \times P,$$

we may assume $\langle [a, b] \rangle = P$ and $\langle [b, c] \rangle = Q'$.

Note that if bc centralizes G', then $g' = [a, b]^2 [b, c]$, so g' generates G'. Therefore, the Factor Group Lemma (2.1) applies in this case. Thus, we may assume bc does not centralize G', so

$$bc \text{ inverts } G'.$$

Subsubcase 1.2.1. *Assume $Q = D_8 \times \mathbb{Z}_2$. Since $\langle b, c \rangle$ is dihedral and $Q' = \langle [b, c] \rangle = \langle (bc)^2 \rangle$ has order 2, it must be the case that ab has order 4 and $\langle b, c \rangle \cong D_8$. So we may assume $b = f$ and $c = ft$.*

Write $a = \overline{a} w$ with $\overline{a} \in Q$ and $w \in P$. Since a and b have order 2, we know they generate a dihedral group, so $\overline{a}$ and b both invert P, but c centralizes P (since bc inverts G').

Since $[a, b] \in P$ projects trivially into Q, we know $\overline{a}$ commutes with $b = f$, so $\overline{a} \in \langle f, t^2 \rangle z$. However, since $t^2 z$ is in the center of Q, there is no harm in replacing z with $t^2 z$, so we may assume $\overline{a} \in \langle f \rangle z$. Thus, there are only two generating sets to consider:

$$S = \{zw, f, ft\} \text{ or } S = \{fzw, f, ft\}.$$

In each case, assume the first two generators invert P, and the third generator centralizes P. (Thus, in both cases, f and t invert P. However, z inverts P in the first case, but z centralizes P in the second case.)

The cycle $\left((ft, f)^4 \#, a \right)^2$ in each of these generating sets (so in the first, $a = zw$, and in the second, $a = fzw$) is a hamiltonian cycle in $\mathrm{Cay}(G/P; S)$, and its endpoint in G is $\left((ftf)^4 f^{-1} a \right)^2 = (fa)^2$. In the first case, the endpoint $(fa)^2$ is $(fzw)^2 = f^2 z^2 w^2 = w^2$, while in the second case, it is $(ffzw)^2 = (zw)^2 = w^2$. Since w^2 certainly generates P, the Factor Group Lemma (2.1) provides a hamiltonian cycle in $\mathrm{Cay}(G; S)$.

Subsubcase 1.2.2. *Assume $Q \neq D_8 \times \mathbb{Z}_2$. We will show that this case cannot occur.* From (7.2), it is easy to see that no two elements of $\overline{S}$ commute. So the image of $[a, b]$ in Q is nontrivial, which contradicts the fact that $\langle [a, b] \rangle = P$.

Case 2. *Assume $\#S > 3$.* Since $G/P \cong Q$ is a 3-generated 2-group, there is a 3-element subset $\{a, b, c\}$ of S that generates G/P. The minimality of S implies $\langle a, b, c \rangle \neq G$, so $|\langle a, b, c \rangle| = 16$. Thus, we may assume $\langle a, b, c \rangle = Q$.

Since a, b, and c all have order 2 in Q/Q', they also have order 2 in G/Q'. So we may assume

$$a, b, \text{ and } c \text{ all have order 2}$$

for otherwise Corollary 2.3 and Remark 2.11 apply.

Let s be the fourth element of S. We may assume $s \notin G'$, for otherwise Lemma 2.10 and Remark 2.11 apply with $X = \{s\}$.

Let $s = wq$ where w generates P and $q \in Q$. If c centralizes P, we have

$$[c, s] = c^{-1} (wq)^{-1} c wq = (q^{-1})^c (w^{-1})^c wq = (q^{-1})^c w^{-1} wq = (q^{-1})^c q = [c, q] \in Q'.$$

Since

$$G' = Q' \times P = \langle [a,b], [a,c], [b,c], [a,s], [b,s], [c,s] \rangle$$

and $Q' = \langle [a,b], [a,c], [b,c] \rangle$, we may assume $P \subset \langle [c,s] \rangle$. Thus $[c,s] \notin Q'$ and c inverts P. Therefore, $P \subset \langle [c,s] \rangle \subset \langle c,s \rangle$.

We claim that $s \in cG'$. If not, then the image of $\langle c,s \rangle$ in G/G' has order 4, so we may assume $\{a,c,s\}$ generates $G/G' \cong Q/Q' = Q/\Phi(Q)$. But this implies that $\{a,c,s\}$ generates $G/P \cong Q$. Since we also know that $P \subset \langle c,s \rangle \subset \langle a,c,s \rangle$, we conclude that $\langle a,c,s \rangle = G$. This contradicts the minimality of S.

We may assume $s \notin cP$, for otherwise Corollary 2.2 and Remark 2.11 apply. Let u be a generator of $Q' \cong \mathbb{Z}_2$. Then $s \in cG' = cQ'P = \{c,cu\}P$. Since $s \notin cP$ and $s \notin Q$, we have $s = cuw$ for some generator w of $P \cong \mathbb{Z}_p$. Let $\gamma = uw$. Then $s = c\gamma$ and

$$\langle \gamma \rangle = \langle uw \rangle = \langle u \rangle \langle w \rangle = Q'P = G'.$$

Since $[c,s]$ generates P, we see that c inverts P.

We claim that both a and b centralize P. If not, we may assume a inverts P. Then $P \subset \langle [a,s] \rangle \subset \langle a,s \rangle$. Since $\{a,b,s\}$ and $\{a,b,c\}$ have the same image in $G/G' \cong Q/Q' = Q/\Phi(Q)$, we know $\{a,b,s\}$ generates G/G'. This implies that $\{a,b,s\}$ generates $G/P \cong Q$. Hence, $\{a,b,s\}$ generates G, contradicting the minimality of S.

Now, since $G/G' \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ (and $s \equiv c \pmod{G'}$), it is easy to see that all three of the following sequences are hamiltonian cycles in $\mathrm{Cay}(G/G'; S)$:

$$(a,c,b,c,a,c,b,c), \ (a,c,b,c,a,c,b,s), \ (a,c,b,s,a,c,b,s).$$

Let $g = acbcacbc$ be the endpoint (in G) of the first cycle. Then the endpoints of the other two cycles are:

$$gc^{-1}s = g\gamma \ \text{ and } \ acbsacbs = acb(c\gamma)acb(c\gamma) = g\gamma^2.$$

Now $g \in Q' = \langle \gamma^p \rangle$, and $|\gamma| = 2p$. Now, it is easy to see that if m is a multiple of p, then either $m+1$ or $m+2$ is relatively prime to $2p$. Therefore, either $g\gamma$ or $g\gamma^2$ generates $\langle \gamma \rangle = G'$, so the Factor Group Lemma (2.1) applies. $\qquad \square$

References

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

[2] W. Burnside, *Theory of Groups of Finite Order, 2nd ed.* Dover, New York, 1955.

[3] 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. 23–34.

[4] S. J. Curran, D. W. Morris and J. Morris Cayley graphs of order 48 are hamiltonian (unpublished). http://arxiv.org/src/1104.0081/anc/48.pdf

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

[6] E. Ghaderpour and D. W. Morris, Cayley graphs of order $30p$ are hamiltonian (preprint). http://arxiv.org/abs/1102.5156

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

[8] T. W. Judson, *Abstract Algebra*, Virginia Commonwealth University, 2009. http://abstract.pugetsound.edu/download.html

[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), 27–71.

[11] D. W. Morris, 2-generated Cayley digraphs on nilpotent groups have hamiltonian paths, *Contrib. Discrete Math.* (to appear). http://arxiv.org/abs/1103.5293

[12] D. Witte: Cayley digraphs of prime-power order are hamiltonian. *J. Comb. Theory B* **40** (1986), 107–112.

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