J. Aust. Math. Soc. (First published online 2024), page 1 of 34*
doi:10.1017/S1446788724000181
*Provisional—final page numbers to be inserted when paper edition is published

THE PRODUCT OF A GENERALIZED QUATERNION GROUP AND A CYCLIC GROUP

SHAOFEI DU, WENJUAN LUO and HAO YU

(Received 2 December 2023; accepted 11 August 2024)

Communicated by Michael Giudici

Abstract

Let $X = GC$ be a group, where C is a cyclic group and G is either a generalized quaternion group or a dihedral group such that $C \cap G = 1$. In this paper, X is characterized and, moreover, a complete classification for X is given, provided that G is a generalized quaternion group and C is core-free.

2020 *Mathematics subject classification*: primary 20D40; secondary 20B05.

Keywords and phrases: factorizations of groups, generalized quaternion group, dihedral group, regular Cayley map, skew morphism.

1. Introduction

A group G is said to be properly *factorizable* if $G = AB$ for two proper subgroups A and B of G, while the expression $G = AB$ is called a *factorization* of G. Furthermore, if $A \cap B = 1$, then we say that G has an *exact factorization*.

Factorizations of groups naturally arise from the well-known Frattini's argument, including its version in permutation groups. One of the most famous results about factorized groups might be one of the theorems of Itô, saying that any group is metabelian whenever it is the product of two abelian subgroups (see [11]). Later, Wielandt and Kegel showed that the product of two nilpotent subgroups must be soluble (see [13, 19]). Douglas showed that the product of two cyclic groups must be super-solvable (see [3]). The factorizations of almost simple groups with a solvable factor were determined in [15]. There are many other papers related to factorizations, for instance, finite products of soluble groups, factorizations with one nilpotent factor and so on. Here we are not able to list all references and readers may refer to a survey paper [2].

This work is supported in part by the National Natural Science Foundation of China (12071312).

In this paper, we shall focus on the product group $X = GC$ for a finite group G and a cyclic group C such that $G \cap C = 1$. Suppose that C is core-free. Then, X is also called a *skew product group* of G. Recall that the skew morphism of a group G and a skew product group X of G were introduced by Jajcay and Širáň in [12], which is related to studies of regular Cayley maps of G. For the reason of the length of the paper, we are not able to explain them in detail. Recently, there have been many results on skew product groups X of some particular groups G that are cyclic groups, elementary abelian p-groups, finite nonabelian characteristically simple groups, dihedral groups, generalized quaternion groups and so on. In particular, so far, there exists no classification of skew product groups of cyclic groups, and based on big efforts of several authors working on regular Cayley maps, the final classification of skew product groups of dihedral groups was given in [8]. For partial results about generalized quaternion groups, see [9].

Throughout this paper, set $C = \langle c \rangle$ and

$$\begin{aligned} Q &= \langle a, b \mid a^{2n} = 1, b^2 = a^n, a^b = a^{-1} \rangle \cong Q_{4n},\ n \geq 2, \\ D &= \langle a, b \mid a^n = b^2 = 1, a^b = a^{-1} \rangle \cong D_{2n},\ n \geq 2. \end{aligned} \tag{1-1}$$

Let $X(G) = GC$ be a group, where $G \in \{Q, D\}$ and $G \cap C = 1$. In this paper, we give a characterization for $X(Q)$ and a complete classification of $X(Q)$ provided that C is core-free. In the above paper dealing with skew product groups of dihedral groups, the authors adopt some computational techniques on skew morphisms. Alternatively, in this paper, we realize our goals by using classical group theoretical tools and methods (solvable groups, p-groups, permutation groups, group extension theory and so on). In our approach, we pay attention to the global structures of the group $X(G)$. Since $X(Q)$ is closely related to $X(D)$, some properties of $X(D)$ have to be considered too.

Note that $X = X(G) = GC = \langle a, b \rangle \langle c \rangle$ for $G \in \{Q, D\}$. Thus, $\langle a \rangle \langle c \rangle$ is unnecessarily a subgroup of X. Clearly, X contains a subgroup M of the largest order such that $\langle c \rangle \leq M \subseteq \langle a \rangle \langle c \rangle$. This subgroup M plays an important role in this paper. From now on, by S_X, we denote the core $\cap_{x \in X} S^x$ of X in a subgroup S of X.

There are four main theorems in this manuscript. In Theorem 1.1, the global structure of our group $X \in \{X(Q), X(D)\}$ is characterized.

Theorem 1.1. *Let $G \in \{Q, D\}$ and $X = X(G) = GC$, where $G \cap C = 1$. Let M be the subgroup of the largest order in X such that $\langle c \rangle \leq M \subseteq \langle a \rangle \langle c \rangle$. Then the group M is characterized in Table 1.*

Clearly, M is a product of two cyclic subgroups, which has not been determined in general so far, as mentioned before. However, further properties of our group X are given in Theorem 1.2.

Theorem 1.2. *Let $G \in \{Q, D\}$ and $X = X(G)$, and let M be defined as above. Then we have $\langle a^2, c \rangle \leq C_X(\langle c \rangle_X)$ and $|X : C_X(\langle c \rangle_X)| \leq 4$. Moreover, if $\langle c \rangle_X = 1$, then $M_X \cap \langle a^2 \rangle \lhd M_X$. In particular, if $\langle c \rangle_X = 1$ and $M = \langle a \rangle \langle c \rangle$, then $\langle a^2 \rangle \lhd X$.*

https://doi.org/10.1017/S1446788724000181 Published online by Cambridge University Press

TABLE 1. The forms of M, M_X and X/M_X.

Case	M	M_X	X/M_X
1	$\langle a\rangle\langle c\rangle$	$\langle a\rangle\langle c\rangle$	$\mathbb{Z}_2$
2	$\langle a^2\rangle\langle c\rangle$	$\langle a^2\rangle\langle c^2\rangle$	D_8
3	$\langle a^2\rangle\langle c\rangle$	$\langle a^2\rangle\langle c^3\rangle$	A_4
4	$\langle a^4\rangle\langle c\rangle$	$\langle a^4\rangle\langle c^3\rangle$	S_4
5	$\langle a^3\rangle\langle c\rangle$	$\langle a^3\rangle\langle c^4\rangle$	S_4

Using Theorem 1.2, we classify skew product groups of generalized quaternion groups; see the following theorem.

THEOREM 1.3. *Let $G = Q$ and $X = X(G) = G\langle c\rangle$, where $m = \mathrm{o}(c) \geq 2$, $G \cap \langle c\rangle = 1$ and $\langle c\rangle_X = 1$. Set $R := \{a^{2n} = c^m = 1,\ b^2 = a^n,\ a^b = a^{-1}\}$. Then, one of the following holds:*

(1) $X = \langle a, b, c \mid R, (a^2)^c = a^{2r}, c^a = a^{2s}c^t, c^b = a^u c^v\rangle$;
(2) $X = \langle a, b, c \mid R, (a^2)^{c^2} = a^{2r}, (c^2)^a = a^{2s}c^{2t}, (c^2)^b = a^{2u}c^2, a^c = bc^{2w}\rangle$;
(3) $X = \langle a, b, c \mid R, (a^2)^c = a^{2r}, (c^3)^a = a^{2s}c^3, (c^3)^b = a^{2u}c^3, a^c = bc^{im/2}, b^c = a^x b\rangle$;
(4) $X = \langle a, b, c \mid R, (a^4)^c = a^{4r}, (c^3)^{a^2} = a^{4s}c^3, (c^2)^b = a^{4u}c^3, (a^2)^c = bc^{im/2},$
$b^c = a^{2x}b, c^a = a^{2+4z}c^{1+(jm/3)}\rangle$;
(5) $X = \langle a, b, c \mid R, a^{c^4} = a^r, b^{c^4} = a^{1-r}b, (a^3)^{c^{m/4}} = a^{-3}, a^{c^{m/4}} = bc^{3m/4}\rangle$,

where the parameters are given in Lemmas 5.1, 5.2, 5.3, 5.5 and 5.6, respectively.

The relationship between $X(Q)$ and $X(D)$ is characterized in the following theorem.

THEOREM 1.4. *For the group $X(Q)$, we have $\langle a^n\rangle \lhd X(Q)$ for all cases in items (2)–(5) and some cases in item (1). Moreover, corresponding to $D \cong Q/\langle a^n\rangle$, we have $X(D) = X(Q)/\langle a^n, c_1\rangle$, where $\langle a^n\rangle \lhd X(Q)$ and $\langle a^n, c_1\rangle = \langle a^n,\ c\rangle_{X(Q)}$.*

REMARK 1.5. One may determine regular Cayley maps of dihedral groups (which was done in [14] via skew-morphism computations) and of generalized quaternion groups by Theorem 1.3.

After this introductory section, some preliminary results are given in Section 2; and Theorems 1.1, 1.2, 1.3 and 1.4 are proved in Sections 3, 4, 5 and 6, respectively.

2. Preliminaries

In this section, some elementary facts used in this paper are collected.

PROPOSITION 2.1 [17, Theorem 1]. *The finite group $G = AB$ is solvable, where both A and B are subgroups with cyclic subgroups of index no more than 2.*

https://doi.org/10.1017/S1446788724000181 Published online by Cambridge University Press

PROPOSITION 2.2 [10, Theorem 4.5]. *Let H be a subgroup of G. Then $N_G(H)/C_G(H)$ is isomorphic to a subgroup of* $\mathrm{Aut}\,(H)$.

PROPOSITION 2.3 [16, Theorem]. *If G is a transitive permutation group of degree n with a cyclic point-stabilizer, then $|G| \le n(n-1)$.*

PROPOSITION 2.4 [11, Satz 1 and Satz 2]. *Let $G = AB$ be a group, where both A and B are abelian subgroups of G. Then:*

(1) *G is meta-abelian, that is, G' is abelian; and*
(2) *A or B contains a normal subgroup $N \ne 1$ of G if $G \ne 1$.*

PROPOSITION 2.5 [10, Theorem 11.5]. *Let $G = \langle a\rangle\langle b\rangle$ be a group and p be an odd prime. If $|\langle a\rangle| \le |\langle b\rangle|$, then $\langle b\rangle_G \ne 1$. If both $\langle a\rangle$ and $\langle b\rangle$ are p-groups, then G is metacyclic.*

PROPOSITION 2.6 [1, Corollary 1.3.3]. *Let $G = G_1G_2$ be a group. Then for any prime p, there exists $P_i \in Syl_p(G_i)$ such that $P = P_1P_2 \in Syl_p(G)$ for $i = 1$ or 2.*

PROPOSITION 2.7 [7, Satz 1]. *Let $N \le M \le G$ such that $(|N|, |G : M|) = 1$ and N is an abelian normal subgroup of G. If N has a complement in M, then N has a complement in G too.*

The Schur multiplier $M(G)$ of a group G is defined as the second integral homology group $H^2(G; Z)$, where Z is a trivial G-module. It plays an important role in the central expansion of groups. The following result is well known.

PROPOSITION 2.8 [18, (2.21) on page 301]. *The Schur multiplier $M(S_n)$ of S_n is a cyclic group of order 2 if $n \ge 4$ and of order 1 for $n \le 3$.*

Recall that a group H is said to be a *Burnside group* if every permutation group containing a regular subgroup isomorphic to H is either 2-transitive or imprimitive.

PROPOSITION 2.9 [20, Theorems 25.3 and 25.6]. *Every cyclic group of composite order is a Burnside group. Every dihedral group is a Burnside group.*

PROPOSITION 2.10 [5, Lemma 4.1]. *Let $n \ge 2$ be an integer and p a prime. Then,* $\mathrm{AGL}(n, p)$ *contains an element of order p^n if and only if $(n, p) = (2, 2)$ and* $\mathrm{AGL}(2, 2) \cong S_4$.

Recall that our group $X(D) = DC$, where D is a dihedral group of order $2n$ and C is a cyclic group of order m such that $D \cap C = 1$, where $n, m \ge 2$. Then, we have the following results.

PROPOSITION 2.11 [6, Lemma 4.1]. *Suppose that $X(D) = \langle a, b\rangle\langle c\rangle$, $\langle a\rangle\langle c\rangle \le X(D)$ and $\langle c\rangle_{X(D)} = 1$. Then, $\langle a^2\rangle \lhd X(D)$.*

REMARK 2.12. An independent proof of Proposition 2.11 was also given in [4].

https://doi.org/10.1017/S1446788724000181 Published online by Cambridge University Press

LEMMA 2.13. *Suppose that X is a solvable group and has a faithfully 2-transitive permutation representation relative to a subgroup M, whose index is of composite order. Then, $X \leq \mathrm{AGL}(k, p)$, where k is a positive integer and p is a prime. Moreover:*

(i) *if X contains an element of order p^k, then $X = S_4$; and*
(ii) *if the hypotheses hold for $X = X(D)$ and $M = C$, then $X(D) = A_4$.*

PROOF. Set $\Omega = [X : M]$. Let N be a minimal normal subgroup of X. Since X is solvable, $N \cong \mathbb{Z}_p^k$ for some prime p and integer k. Since X is 2-transitive, it is primitive, which implies that N is transitive on Ω and so is regular on Ω. Therefore, $X = N \rtimes X_\alpha \leq \mathrm{AGL}(k, p)$ for some $\alpha \in \Omega$. Since X is 2-transitive and $|\Omega| = p^k$, we know $|X_\alpha| \geq p^k - 1$ for any $\alpha \in \Omega$.

(i) Suppose that X contains an element of order p^k. By Proposition 2.10, we get $(k, p) = (2, 2)$ so that $X = S_4$, reminding us that $|\Omega|$ is not a prime.
(ii) Let $X = X(D)$ and $M = C = \langle c\rangle$ with the order of m. Then, $|X(D)| = 2nm = p^k m$. By Proposition 2.3, we get $p^k m \leq p^k(p^k - 1)$. Therefore, $m = p^k - 1$ as $m = |M| = |X_\alpha| \geq p^k - 1$, which implies that $\langle c\rangle$ is a Singer subgroup of $\mathrm{GL}(k, p)$ and $X(D) = N \rtimes \langle c\rangle$. Then, both D and N are regular subgroups, that is, $|D| = 2n = |\Omega| = p^k$, which implies $p = 2$. Now, we have $|X(D)| = 2^k(2^k - 1)$. Since both N and D are Sylow 2-subgroups of $X(D)$ and $N \lhd X(D)$, we get $D = N$, so that $D \cong \mathbb{Z}_2^2$ and $X(D) = A_4$. □

3. Proof of Theorem 1.1

To prove Theorem 1.1, let $G \in \{D, Q\}$, as defined in (1-1). Let $X = G\langle c\rangle$ be either $X(D)$ or $X(Q)$. Let M be the subgroup of the largest order in X such that $\langle c\rangle \leq M \subsetneqq \langle a\rangle\langle c\rangle$, and set $M_X = \cap_{x\in X} M^x$. By Proposition 2.1, X is solvable. Then, Theorem 1.1 is proved in Lemmas 3.1 and 3.3, which deal with $G = D$ and Q, respectively.

LEMMA 3.1. *Theorem 1.1 holds, provided $G = D$ and $X = X(D)$.*

PROOF. Let $G = D$ and $X = X(D)$. If $m = 1$, then $X = D$ and $M = \langle a\rangle$, as desired. So in what follows, we assume $m \geq 2$. Recall that $m, n \geq 2$, $|X|$ is even and more than 7. The lemma is proved by induction on the order of X. Up to isomorphism, all cases of $|X| \leq 24$ are listed in Table 2, showing the conclusion.

Assume $|X| \gneqq 24$. Then we carry out the proof by the following three steps.

Step 1: Case of $M_X \neq 1$. Suppose that $M_X \neq 1$. Set $M = \langle a^i\rangle\langle c\rangle$ for some i. Since

$$a^i \in \cap_{l_2,l_3} M^{a^{l_2} b^{l_3}} = \cap_{l_1,l_2,l_3} M^{c^{l_1} a^{l_2} b^{l_3}} = M_X,$$

we get that $M_X = M_X \cap (\langle a^i\rangle\langle c\rangle) = \langle a^i\rangle\langle c^r\rangle$ for some r. Set $\overline{X} := X/M_X = \overline{G}\langle\overline{c}\rangle$. Then we claim that $\overline{G} \cap \langle\overline{c}\rangle = 1$. In fact, for any $\overline{g} = \overline{c}' \in \overline{G} \cap \langle\overline{c}\rangle$, for some $g \in G$ and $c' \in \langle\overline{c}\rangle$, we have $gc'^{-1} \in M_X$, that is, $g \in \langle a^i\rangle$ and $c' \in \langle c^r\rangle$, which implies $\overline{g} = \overline{c}' = 1$.

https://doi.org/10.1017/S1446788724000181 Published online by Cambridge University Press

TABLE 2. All cases of $|X| \leq 24$ up to isomorphism.

X	M	X/M_X
$\langle a,b,c \mid a^2 = b^2 = c^m = 1, [a,b] = 1, a^c = b, b^c = a, m \in \{2,4,6\}\rangle$	$\langle a^2\rangle\langle c\rangle$	D_8
$\langle a,b,c \mid a^2 = b^2 = c^m = 1, [a,b] = 1, a^c = b, b^c = ab, m \in \{3,6\}\rangle$	$\langle a^2\rangle\langle c\rangle$	A_4
$\langle a,b,c \mid a^4 = b^2 = c^3 = 1, a^b = a^{-1}, c^a = a^2c^2, b^c = a^2b\rangle$	$\langle a^4\rangle\langle c\rangle$	S_4
$\langle a,b,c \mid a^3 = b^2 = c^4 = 1, a^b = a^{-1}, a^c = bc^{-1}\rangle$	$\langle a^3\rangle\langle c\rangle$	S_4
else	$\langle a\rangle\langle c\rangle$	$\mathbb{Z}_2$

Therefore, $\overline{G} \cap \langle\overline{c}\rangle = 1$. Let $M_0/M_X = \langle\overline{a}^j\rangle\langle\overline{c}\rangle$ be the largest subgroup of $\overline{X}$ containing $\langle\overline{c}\rangle$ and contained in the subset $\langle\overline{a}\rangle\langle\overline{c}\rangle$. Then, $\langle\overline{a}^j\rangle\langle\overline{c}\rangle = \langle\overline{c}\rangle\langle\overline{a}^j\rangle$. Since

$$\langle a^j\rangle\langle c\rangle M_X = \langle a^j\rangle M_X\langle c\rangle = \langle a^j\rangle\langle a^i\rangle\langle c\rangle \quad \text{and} \quad \langle c\rangle\langle a^j\rangle M_X = \langle c\rangle M_X\langle a^j\rangle = \langle c\rangle\langle a^i\rangle\langle a^j\rangle,$$

we get $\langle a^i, a^j\rangle\langle c\rangle \leq X$. By the maximality of M, we have $\langle a^i, a^j\rangle = \langle a^i\rangle$ so that $M_0 = M$.

Using the induction hypothesis on $\overline{X} = \overline{G}\langle\overline{c}\rangle$, noting that $M_0/M_X = M/M_X$ is core-free in $\overline{X}$, we get that $\overline{X}$ is isomorphic to $\mathbb{Z}_2$, D_8, A_4 or S_4, and correspondingly, $o(\overline{a}) = k$, where $k \in \{1,2,3,4\}$, and so $a^k \in M_X$. Since $M = \langle a^i\rangle\langle c\rangle$ and $M_X = \langle a^i\rangle\langle c^r\rangle$, we know that $\langle a^i\rangle = \langle a^k\rangle$, which implies that $i \in \{1,2,3,4\}$. Clearly, if $\overline{X} = \mathbb{Z}_2$, then $M_X = M$; if $\overline{X} = D_8$ and $\mathrm{o}(\overline{c}) = 2$, then $M_X = \langle a^2\rangle\langle c^2\rangle$; if $\overline{X} = A_4$ and $\mathrm{o}(\overline{c}) = 3$, then $M_X = \langle a^2\rangle\langle c^3\rangle$; if $\overline{X} = S_4$ and $\mathrm{o}(\overline{c}) = 4$, then $M_X = \langle a^3\rangle\langle c^4\rangle$; and if $\overline{X} = S_4$ and $\mathrm{o}(\overline{c}) = 3$, then $M_X = \langle a^4\rangle\langle c^3\rangle$.

Step 2: Show that if $M_X = 1$, then $G \in \{D_{2kp} | k = 2,3,4$ and p is a prime$\}$. Suppose that $M_X = 1$. Since both $\langle a\rangle_X$ and $\langle c\rangle_X$ are contained in M_X, we get $\langle a\rangle_X = \langle c\rangle_X = 1$. Arguing by contradiction, assume that $G_X \neq 1$. If $|G_X| \gneqq 4$, then by $G = \langle a,b\rangle \cong D_{2n}$, we get $\langle a\rangle_X \neq 1$, which is a contradiction. So $|G_X| \leq 4$. Since $G_X \lhd G \cong D_{2n}$, we know that $|G : G_X| \leq 2$, which implies $|G| \leq 8$, that is, $G \cong D_4$ or D_8. A direct check shows that X is D_8, A_4 or S_4, which contradicts $|X| \gneqq 24$. Therefore, $G_X = 1$.

Next, we consider the faithful (right multiplication) action of X on the set of right cosets $\Omega := [X : \langle c\rangle]$. By Proposition 2.9, every dihedral group is a Burnside group, which implies that X is either 2-transitive or imprimitive. If X is primitive, then noting that X has a cyclic point-stabilizer $\langle c\rangle$, by Lemma 2.13(2), we get $G = D_4$ and $X = A_4$, which contradicts $|X| \gneqq 24$. So in what follows, we assume that X is imprimitive. Pick a maximal subgroup H of X that contains $\langle c\rangle$ properly. Then, $H = H \cap X = (H \cap G)\langle c\rangle = \langle a^s, b_1\rangle\langle c\rangle < X$ for some $b_1 \in G \setminus \langle a\rangle$ and some s. Using the same argument as that in Step 1, one has $a^s \in H_X$. Reset $\overline{X} := X/H_X$. Consider the faithful primitive action of $\overline{X}$ on $\Omega_1 := [\overline{X} : \overline{H}]$, with a cyclic regular subgroup of $\langle\overline{a}\rangle$, where $|\Omega_1| = s$. By Proposition 2.9, we know that either s is a prime p such that $\overline{X} \leq \mathrm{AGL}(1,p)$ or s is a composite such that $\overline{X}$ is 2-transitive on Ω_1. In what follows, we consider these two cases when $a^s = 1$ or $a^s \neq 1$, separately.

Case (1): $a^s = 1$. In this case, $H = \langle c\rangle \rtimes \langle b\rangle$ and $X = \langle c,b\rangle.\langle a\rangle$. Then two cases when s is composite or prime are considered, separately.

Suppose that s is a composite such that $\overline{X}$ is 2-transitive on Ω_1. By Lemma 2.13, we get $\overline{X} \le \mathrm{AGL}(l, q)$ for some prime q, which contains a cyclic regular subgroup $\langle\overline{a}\rangle$ of order q^l. By Lemma 2.13(1), $\overline{X} \cong S_4$ and $\mathrm{o}(\overline{a}) = 4$ so that $\mathrm{o}(a) = 4$ (as $H_X \le \langle b, c\rangle$), which in turn implies $G = D_8$. In this case, checking by Magma, we have that either $\mathrm{o}(c) = 2, 3$ and $|X| \le 24$; or $\mathrm{o}(c) = 4$, $|X| = 32$ but $G_X \neq 1$, which is a contradiction.

Suppose that s is a prime p such that $\overline{X} \le \mathrm{AGL}(1, p)$. Then, $\mathrm{o}(a) = p$ such that $G \cong D_{2p}$, where $p \ge 5$, as $|X| \gneqq 24$. Clearly, $\langle\overline{a}\rangle \lhd \overline{X}$. Consider the action of X on the set of blocks of length 2 on $\Omega = [X : \langle c\rangle]$, that is, the orbital of Ω under H, with the kernel $K := H_X$. If $K = 1$, then we get $\overline{X} = X$ and $\langle a\rangle \lhd X$, which is a contradiction. Therefore, $K \neq 1$. Then, $K \nleqq \langle c\rangle$ (as $\langle c\rangle_X = 1$) so that K interchanges two points $\langle c\rangle$ and $\langle c\rangle b$, which implies $|K/K \cap \langle c\rangle| = 2$. Since $K \cap \langle c\rangle$ is cyclic and $K \cap \langle c\rangle$ fixes setwise each block of length 2, we get $|K \cap \langle c\rangle| \le 2$. Therefore, $|K| \le 4$. Since $K \rtimes \langle a\rangle \lhd X$ and $p \ge 5$, we have $K \rtimes \langle a\rangle = K \times \langle a\rangle$ so that $\langle a\rangle \,\mathrm{char}\, (K \times \langle a\rangle) \lhd X$, which contradicts $G_X = 1$.

Case (2): $a^s \neq 1$. First, show $s = p$, a prime. Arguing by a contradiction, assume that s is composite. To do that, recall $\overline{X} = X/H_X = \langle\overline{a}\rangle\overline{H}$ and $\Omega_1 := [\overline{X} : \overline{H}]$. Then, $\overline{X}$ is 2-transitive on Ω_1, with a cyclic regular subgroup of $\langle\overline{a}\rangle$. Since $a^s \in H_X$, we get $H_X \neq 1$ and of course $H_X \nleqq \langle c\rangle$. Suppose that $\langle a^j\rangle\langle c\rangle \le H$. Then $a^j \in M$. Using the same arguments as in the first line of Step 1 again, we get $a^j \in M_X = 1$. Therefore, there exists an l such that $bc^l \in H_X$, which implies $\overline{H} = \langle\overline{c}\rangle$. Then, $\overline{X} = \langle\overline{a}\rangle\langle\overline{c}\rangle$, a product of two cyclic subgroups, cannot be isomorphic to S_4, which contradicts Lemma 2.13(1). Therefore, $s = p$, a prime, and $X/H_X \le \mathrm{AGL}(1, p)$.

Second, consider the quotient group $\overline{H} := H/\langle c\rangle_H = \langle\overline{a}^p, \overline{b}\rangle\langle\overline{c}\rangle$, taking into account $s = p$, a prime. Clearly, we have $\langle\overline{c}\rangle_{\overline{H}} = 1$ and $o(\overline{a}^p) = o(a^p)$. Let $H_0/\langle c\rangle_H = \langle\overline{a}^{pj}\rangle\langle\overline{c}\rangle$ be the subgroup of $\overline{H}$ with the largest order such that $\langle\overline{c}\rangle \le H_0/\langle c\rangle_H \subseteqq \langle\overline{a}^p\rangle\langle\overline{c}\rangle$. Since $|\overline{H}| < |X|$, by the induction hypothesis on $\overline{H}$, we know that $H_0/\langle c\rangle_H = \langle\overline{a}^{pk}\rangle\langle\overline{c}\rangle$ for $k \in \{1, 2, 3, 4\}$, which implies $\langle a^{pk}\rangle\langle c\rangle\langle c\rangle_H = \langle c\rangle\langle a^{pk}\rangle\langle c\rangle_H = \langle c\rangle\langle a^{pk}\rangle$, giving $\langle a^{pk}\rangle\langle c\rangle \le H \le X$. Therefore, we get $a^{pk} \in M_X$. Since $M_X = 1$ and $a^p = a^s \neq 1$, we get that the order of a is kp, where $k \in \{2, 3, 4\}$. Therefore, only the following three groups remain: $G = D_{2kp}$, where $k \in \{2, 3, 4\}$ and p is a prime.

Step 3: Show that G cannot be D_{2kp}, where $k \in \{2, 3, 4\}$and p is a prime, provided $M_X = 1$. Suppose that $G \cong D_{2kp}$, $k \in \{2, 3, 4\}$, recalling that $H = \langle a^p, b\rangle\langle c\rangle$, $M_X = 1$, $\Omega = [X : \langle c\rangle]$ and X has blocks of length $2k$ acting on Ω. Moreover, $\langle a^p\rangle_X = 1$ and there exists no nontrivial element $a^j \in H$ such that $\langle a^j\rangle\langle c\rangle \le H$. Here, we only give the proof for the case $k = 4$, that is, $G \cong D_{8p}$. The proof for other cases is similar but easier.

Let $G = D_{8p}$. If $p = 2$ or 3, then $G \cong D_{16}$ or D_{24}, which can be directly excluded by Magma. So assume $p \ge 5$. Set $a_1 = a^p$ and $a_2 = a^4$ so that $H = \langle a_1, b\rangle\langle c\rangle$, where $\mathrm{o}(a_1) = 4$. Set $C_0 = \langle c\rangle_H$ and $K = H_X$. Then, H contains an element a_1 of order 4 having two orbits of length 4 on each block of length 8, where $a_1 \le K$. Consider the action of $\overline{H} := H/C_0 = \langle\overline{a}_1, \overline{b}\rangle\langle\overline{c}\rangle$ on the block containing the point $\langle c\rangle$, noting that $\langle\overline{c}\rangle$ is core-free. Recall that $\langle a_1\rangle_X = 1$. So $\langle\overline{a}_1, \overline{b}\rangle \cong D_8$ and $\overline{H} \cong S_4$. Moreover, we have $N_{\overline{H}}(\langle\overline{c}\rangle) = \langle\overline{c}\rangle \rtimes \langle\overline{b}\rangle \cong D_6$, by rechoosing b in $\langle a_1, b\rangle$. Therefore, $L := \langle c\rangle\langle b\rangle \le X$.

https://doi.org/10.1017/S1446788724000181 Published online by Cambridge University Press

Now we turn to considering the imprimitive action of X on $\Omega_2 := [X : L]$, which is of degree $4p$. Let $K \cap \langle c\rangle = \langle c_1\rangle$. Then every orbit of $\langle c_1\rangle$ on Ω_2 is of length no more than 4. Observing the cycle decomposition of $c_1L_X \in X/L_X$ on Ω_2, we know that $k_1 := |\langle c_1\rangle L_X/L_X| \mid 12$. Therefore, $c_1^{k_1}$ fixes all points in Ω_2, which implies $c_1^{2k_1}$ fixes all points in Ω. Therefore, $c_1^{2k_1} = 1$ (as $\langle c\rangle_X = 1$), that is, $|K \cap \langle c\rangle| \mid 2k_1$ and, in particular, $|K \cap C_0| \mid 2k_1$. Moreover, since $\langle a_2K\rangle \lhd X/K \cong \mathbb{Z}_p \rtimes \mathbb{Z}_r$ for some $r \mid (p-1)$, we know that $K \rtimes \langle a_2\rangle \lhd X$. Then, $|K \cap C_0| \mid 24$, as $k_1 \mid 12$. Also, $K/(K \cap C_0) \cong KC_0/C_0 \lhd H/C_0 \cong S_4$. Since $\overline{a}_1 \in KC_0/C_0$, where $o(\overline{a}_1) = 4$, and every normal subgroup of S_4 containing an element of order 4 must contain A_4, we know that $K/(K \cap C_0)$ contains a characteristic subgroup $K_1/(K \cap C_0) \cong A_4$.

We claim that $C_{K_1}(K \cap C_0) = K_1$. Arguing by contradiction, assume that $K \cap C_0 \nleq Z(K_1)$. Then, as a quotient of A_4, we have $3 \mid |K_1/C_{K_1}(K \cap C_0)|$. However, since $K_1/C_{K_1}(K \cap C_0) \le \mathrm{Aut}\,(K \cap C_0)$, $K \cap C_0 \le \mathbb{Z}_3 \times \mathbb{Z}_8$ and using the cycle decomposition of the generator of $K \cap C_0$, we get that $K_1/C_{K_1}(K \cap C_0)$ contains no element of order 3, which implies a contradiction. Therefore, $C_{K_1}(K \cap C_0) = K_1$, that is, $(K \cap C_0) \le Z(K_1)$.

Since $K_1/(K \cap C_0) \cong A_4$ and $Z(A_4) = 1$, we get that $K \cap C_0 = Z(K_1)\,\mathrm{char}\,K_1 \lhd X$. Therefore, $K \cap C_0 \le 1$ (as $\langle c\rangle_X = 1$) so that $K \cong A_4$ or S_4, which implies

$$\langle a_2\rangle\,\mathrm{char}\,(K \times \langle a_2\rangle) \lhd X,$$

which contradicts $G_X = 1$ again. □

To handle $X(Q)$, we need the following result.

Lemma 3.2. *Let $X = X(Q) = \langle a, b\rangle\langle c\rangle$. If $\langle c\rangle_X = 1$, then $\langle a\rangle_X \neq 1$.*

Proof. Since $\langle c\rangle_X = 1$, by Proposition 2.3, we have $m < |G|$. So $S := G \cap G^c \neq 1$, otherwise $|X| \ge |G|^2 > |X|$. Take a subgroup T of order a prime p of S. Since $o(a^jb) = 4$ for any integer j, we know $T \le \langle a\rangle$. Since S has a unique subgroup of order p, we get $T^c = T$, giving $T \lhd X$ and so $\langle a\rangle_X \neq 1$, as desired. □

Lemma 3.3. *Theorem 1.1 holds, provided $G = Q$ and $X = X(Q)$.*

Proof. Let X be a minimal counter-example. First, we claim that $\langle c\rangle$ is core-free. Arguing by contradiction, assume that $\langle c\rangle_X \neq 1$. Consider $\overline{X} = X/\langle c\rangle_X$. The subgroup $\overline{M_1}$ of $\overline{X}$ is chosen to have the largest order such that $\langle \overline{c}\rangle \le \overline{M_1} \subsetneqq \langle \overline{a}\rangle\langle \overline{c}\rangle$. Since $|\overline{X}| < |X|$ and $\overline{G}$ is a generalized quaternion group, by the minimality of $\overline{X}$, we get $\overline{M_1} = \langle \overline{a}^i\rangle\langle \overline{c}\rangle$, where $i \in \{1, 2, 3, 4\}$. This gives $M = \langle a^k\rangle\langle c\rangle$, where $k \in \{1, 2, 3, 4\}$, which is a contradiction. Therefore, $\langle c\rangle$ is core-free, that is, $\langle c\rangle_X = 1$.

By Lemma 3.2, $\langle a\rangle_X \neq 1$. If $\langle a\rangle_X = \langle a\rangle$, then $X = (\langle a\rangle \rtimes \langle c\rangle).\langle b\rangle$, which implies $M = \langle a\rangle\langle c\rangle$, and that is a contradiction. So $\langle a\rangle_X < \langle a\rangle$. Set $\overline{X} := X/\langle a\rangle_X = \overline{G}\langle \overline{c}\rangle$ and let the subgroup $\overline{M_2}/\langle a\rangle_X$ of $\overline{X}$ be of the largest order such that $\langle \overline{c}\rangle \le \overline{M_2} \subsetneqq \langle \overline{a}\rangle\langle \overline{c}\rangle$. If $a^n \notin \langle a\rangle_X$, then $\overline{G}$ is a generalized quaternion group; if $a^n \in \langle a\rangle_X$, then $\overline{G}$ is a dihedral group. For the first case, by the minimality of $\overline{X}$, and for the second case, by Lemma 3.1, we get $\overline{M_2} = \langle \overline{a}^i\rangle\langle \overline{c}\rangle$, where $i \in \{1, 2, 3, 4\}$. Then, $\langle a^i\rangle\langle c\rangle\langle a\rangle_X = \langle c\rangle\langle a^i\rangle\langle a\rangle_X$. This gives $(\langle a^i\rangle\langle a\rangle_X)\langle c\rangle \le X$, which implies $M = \langle a^k\rangle\langle c\rangle$, where $k \in \{1, 2, 3, 4\}$, which is a contradiction. □

4. Proof of Theorem 1.2

The proof of Theorem 1.2 consists of the following three lemmas.

LEMMA 4.1. *Suppose that* $G = Q$, $X = X(G)$, $M = \langle a\rangle\langle c\rangle$ *and* $\langle c\rangle_X = 1$. *If* G *is a* 2*-group, then* $\langle a^2\rangle \lhd X$.

PROOF. Suppose that X is a minimal counter-example. Let a_0 be the involution of $\langle a\rangle$. Since $\langle c\rangle_X = 1$, by Lemma 3.2, we get $\langle a\rangle_X \neq 1$, which implies $\langle a_0\rangle \lhd X$, as G is a 2-group. Consider $\overline{X} = X/\langle a_0\rangle = \overline{G}\langle\overline{c}\rangle$. Note that $\overline{G}$ is a dihedral group. Set $\langle\overline{c}\rangle_X = (\langle a_0\rangle \times \langle c_0\rangle)/\langle a_0\rangle$. Then, $\langle c_0^2\rangle \lhd X$, which implies $c_0^2 = 1$. If $c_0 = 1$, by Proposition 2.11, we get $\langle\overline{a}^2\rangle \lhd \overline{X}$. Then, $\langle a^2\rangle \lhd X$ is a contradiction, noting X is a minimal counter-example. Therefore, $o(c_0) = 2$. By using Proposition 2.11 on $X/\langle a_0, c_0\rangle$, we get $(\langle a^2\rangle(\langle a_0\rangle\langle c_0\rangle))/\langle a_0, c_0\rangle \lhd X/\langle a_0, c_0\rangle$, that is, $H := \langle a^2\rangle \rtimes \langle c_0\rangle \lhd X$. Then we continue the proof by the following two steps.

Step 1: Show that X is a 2-group. In fact, noting that $\langle a^4\rangle = \mho_1(H)\,\mathrm{char}\,H \lhd X$, relabel $\overline{X} = X/\langle a^4\rangle$, where we write $\langle\overline{c}\rangle_{\overline{X}} = \langle\overline{c}^i\rangle$. Then, $\langle a^4\rangle \rtimes \langle c^i\rangle \lhd X$. Let Q be the $2'$-Hall subgroup of $\langle c^i\rangle$. Since $\mathrm{Aut}\,(\langle a^4\rangle)$ is a 2-group, we know that $[Q, a^4] = 1$ and so $Q \lhd X$, which contradicts $\langle c\rangle_X = 1$. Therefore, $\langle c^i\rangle$ is also a 2-group. Reset $\overline{X} = X/\langle a^4\rangle\langle c^i\rangle = \overline{G}\langle\overline{c}\rangle$. Now, $|\overline{G}| = 8$ and so $\overline{G} \cong D_8$ (clearly, $\overline{G}$ cannot be Q_8). Since $\langle\overline{c}\rangle_{\overline{X}} = 1$, we have $\mathrm{o}(\overline{c})|4$. Therefore, $\overline{X}$ is a 2-group and so is X.

Step 2: Get a contradiction. Set $K := \langle a_0\rangle \times \langle c_0\rangle \cong \mathbb{Z}_2^2$. Consider the conjugacy of G on K. Since $\langle c_0\rangle \ntrianglelefteq X$, we get $C_X(K) \cap G < G$. Since G may be generated by some elements of the form a^jb, there exists an element $a^ib \in G \setminus C_G(K)$, exchanging c_0 and c_0a_0 (as $(a^ib)^2 = a_0$). To make it easier to write, we write b instead of a^ib. Since $X = GC = (\langle a\rangle\langle c\rangle).\langle b\rangle$, first we write $c^b = a^sc^t$, where $t \neq 0$. Note that

$$c = c^{b^2} = (a^sc^t)^b = a^{-s}(a^sc^t)^t = c^t(a^sc^t)^{t-1},$$

which implies

$$(a^sc^t)^{t-1} = c^{1-t}.$$

Then we have

$$(c^{t-1})^b = (c^b)^{t-1} = (a^sc^t)^{t-1} = c^{1-t}.$$

If $t \neq 1$, then $c_1^b \in \langle c^{t-1}\rangle^b = \langle c^{t-1}\rangle$, which contradicts $c_1^b = a_1c_1$. So $t = 1$, that is, $c^b = a^sc$. Second, we write $c^b = c^{t_1}a^{s_1}$. With the same arguments as the above, we can get $t_1 = 1$ and $c^b = ca^{s_1}$. Therefore, we have $a^sc = c^b = ca^{s_1}$, that is, $(a^s)^c = a^{s_1}$. Clearly, $\langle a^s\rangle = \langle a^{s_1}\rangle$, which implies that c normalizes $\langle a^s, b\rangle$. Note that

$$\langle a^s, b\rangle \leq \cap_{c^i\in\langle c\rangle} G^{c^i} = \cap_{x\in X} G^x = G_X,$$

which implies $b^a = ba^{-2} \in G_X$. Thus, $a^2 \in G_X$, which implies $\langle a^2\rangle \lhd X$. This contradicts the minimality of X. □

LEMMA 4.2. *Suppose that* $G = Q$, $X = X(Q)$, $M = \langle a\rangle\langle c\rangle$ *and* $\langle c\rangle_X = 1$. *Then,* $\langle a^2\rangle \lhd X$.

https://doi.org/10.1017/S1446788724000181 Published online by Cambridge University Press

PROOF. Take a minimal counter-example X and set $\mathrm{o}(c) = m$, $\mathrm{o}(a) = 2n$ and $a_1 := a^n$. By Lemma 4.1, we know that G is not a 2-group. We carry out the proof by the following three steps.

Step 1: Show that the possible groups for G are Q_{4p^k}, where p is an odd prime. By Lemma 3.2, let p be the maximal prime divisor of $|\langle a\rangle_X|$ and set $a_0 = a^{2n/p}$. Clearly, $a_0 \in \langle a^2\rangle$ if p is odd. Consider $\overline{X} = X/\langle a_0\rangle = \overline{G}\langle\overline{c}\rangle$ and set $\langle\overline{c}\rangle_{\overline{X}} = \langle\overline{c_0}\rangle$. Then depending on whether p is 2, $\overline{G}$ is either a dihedral group or a generalized quaternion group. We claim that $1 \neq \langle\overline{c}\rangle_{\overline{X}} = \langle\overline{c_0}\rangle \lneqq \langle\overline{c}\rangle$. Arguing by contradiction, assume that $\langle\overline{c}\rangle_{\overline{X}}$ is either 1 or $\langle\overline{c}\rangle$. Suppose that $\langle\overline{c}\rangle_{\overline{X}} = 1$. Then by the minimality of X or Proposition 2.11, we get $\langle\overline{a}^2\rangle \lhd \overline{X}$, which implies $\langle a^2\rangle\langle a_0\rangle \lhd X$. Since $\langle a^2\rangle\langle a_0\rangle$ is either $\langle a^2\rangle$ or $\langle a\rangle$, we get $\langle a^2\rangle \lhd X$, which is a contradiction. Suppose that $\langle\overline{c}\rangle \lhd \overline{X}$. Then, $\overline{X}/C_{\overline{X}}(\langle\overline{c}\rangle) \leq \mathrm{Aut}\,(\langle\overline{c}\rangle)$ which is abelian and so $\overline{X}' \leq C_{\overline{X}}(\langle\overline{c}\rangle)$. Then, $\overline{a}^2 \in \overline{G}' \leq \overline{X}' \leq C_{\overline{X}}(\langle\overline{c}\rangle)$, that is, $[a^2, c] \in \langle a_0\rangle$, which implies $\langle a^2, a_0\rangle \lhd X$, and again we get $\langle a^2\rangle \lhd X$, which is a contradiction. Therefore, we have $1 \neq \langle\overline{c}\rangle_{\overline{X}} = \langle\overline{c_0}\rangle \lneqq \langle\overline{c}\rangle$.

Consider $X_1 = G\langle c_0\rangle < X$. By the minimality of X, we get $\langle a^2\rangle \lhd X_1$, which implies that $\langle c_0\rangle$ normalizes $\langle a^2\rangle$. Reset

$$K = \langle a_0\rangle \rtimes \langle c_0\rangle,\ \overline{X} = X/K = \overline{G}\langle\overline{c}\rangle \quad \text{and} \quad H = \langle a^2\rangle \rtimes \langle c_0\rangle.$$

If $\mathrm{o}(a_0) < \mathrm{o}(c_0)$, then $1 \neq \langle c_0^j\rangle = Z(K) \lhd X$ is, for some j, a contradiction. Therefore, $1 < \mathrm{o}(c_0) \leq \mathrm{o}(a_0)$. Note that K is either a Frobenius group or $\mathbb{Z}_p^2$. Thus, we have the following two cases.

Case (1): $K = \langle a_0\rangle \rtimes \langle c_0\rangle \cong \mathbb{Z}_p \rtimes \mathbb{Z}_r$, a Frobenius group, where $r \geq 2$ and $r \mid (p-1)$. In this case, p is odd, which implies $a_0 \in \langle a^2\rangle$. Set $\overline{X} = X/K$. By the minimality of X, we have $H/K = \langle\overline{a}^2\rangle \lhd \overline{X}$, that is, $H := \langle a^2\rangle \rtimes \langle c_0\rangle \lhd X$. Since $K \lhd X$, we know that $\langle a^2\rangle/\langle a_0\rangle$ and $\langle c_0\rangle\langle a_0\rangle/\langle a_0\rangle$ are normal in $H/\langle a_0\rangle$. Then, $[a^2, c_0] \leq \langle a_0\rangle$. So

$$H = \langle a^2, c_0 \mid a^n = c_0^r = 1,\ (a^2)^{c_0} = a^2 a_0^j\rangle.$$

Let $P \in \mathrm{Syl}_p(H)$. Actually, $P \leq \langle a^2\rangle$. Then, $P \,\mathrm{char}\, H \lhd X$ so that $P \leq \langle a\rangle_X$. Clearly, $Z(H) = \langle a^{2p}\rangle$. Then, $\langle a^{2p}\rangle \leq \langle a\rangle_X$. Noting that $\langle a^{2p}, P\rangle = \langle a^{2p}, a^{n/p^k}\rangle = \langle a^2\rangle$, where $p^k \| n$, we get $a^2 \in \langle a\rangle_X$, which is a contradiction.

Case (2): $K = \langle a_0\rangle \times \langle c_0\rangle \cong \mathbb{Z}_p^2$. In this case, we claim that $a_0 \in \langle a^2\rangle$. Arguing by contradiction, assume that $a_0 \notin \langle a^2\rangle$. Then, $p = 2$ and n is odd. In $\overline{X}$, we know that $\overline{H} \lhd \overline{X}$, which implies $\langle a_0\rangle H \lhd X$. Noting $\langle a^2\rangle$ is a $2'$-Hall subgroup of $\langle a_0\rangle H$, we have $\langle a^2\rangle \,\mathrm{char}\, \langle a_0\rangle H \lhd X$, which implies $a^2 \in \langle a\rangle_X$, and that is a contradiction. Therefore, $a_0 \in \langle a^2\rangle$, which implies that p is an odd prime. With the same reason as that in Case (1), we have $H \lhd X$. Let H_1 be the $p'-$Hall subgroup of H. We get that H_1 is also the p'-Hall subgroup of $\langle a^2\rangle$ as $\mathrm{o}(c_0) = p$. Then, $H_1 \,\mathrm{char}\, H \lhd X$, which implies $H_1 \leq \langle a\rangle_X$. We claim that $H_1 = 1$. Arguing by contradiction, assume that $H_1 \neq 1$. Then there exists an element a_1 of prime order q in H_1, where $q < p$, as p is maximal. Consider $\overline{X} := X/\langle a_1\rangle = \overline{G}\langle c\rangle$. Similarly, we have $1 \neq \langle\overline{c}\rangle_{\overline{X}} := \langle\overline{c_1}\rangle \lneqq \overline{C}$ and

$H_0 := \langle a^2\rangle \rtimes \langle c_1\rangle \lhd X$. Let $P \in \mathrm{Syl}_p(H_0)$. Then, $P \,\mathrm{char}\, H$ and so $P \lhd X$, which implies $P \leq \langle a\rangle_X$. Noting $\langle H_1, P\rangle = \langle a^2\rangle$, we therefore get $a^2 \in \langle a\rangle_X$, which is a contradiction. So $H_1 = 1$, which means that G is Q_{4p^k} where p is an odd prime as G is not a 2-group.

Step 2: Show that the possible values of m are pq^e for a prime q (may be equal to p) and an integer e. Arguing by contradiction, assume that $m = pq^e m_1$, where $m_1 \neq 1$ and $q \nmid m_1$. Reset $a_1 = a^n$, the involution of $\langle a\rangle$. Suppose that $a_1 \in \langle a\rangle_X$. Let $\langle a_1\rangle \rtimes \langle c_1\rangle$ be the core of $\langle a_1, c\rangle$ in X, noting $\langle a_1\rangle \lhd X$. Since $\langle c_1^2\rangle \lhd X$ and $\langle c\rangle_X = 1$, we get $c_1^2 = 1$. Consider $\overline{X} = X/\langle a_1\rangle\langle c_1\rangle$. Since $\overline{G} \cong D_{2p^k}$ is a dihedral group, by Proposition 2.11, we get $\langle \overline{a}^2\rangle = \langle \overline{a}\rangle \lhd \overline{X}$, which implies $\langle a\rangle \rtimes \langle c_1\rangle \lhd X$. Then, $\langle a^2\rangle \lhd X$ is a contradiction. So in what follows (including Step 3), we assume that $a_1 \notin \langle a\rangle_X$, which implies that $\langle a\rangle_X$ is a p-group.

Recall $H = \langle a^2\rangle \rtimes \langle c_0\rangle$. Since $H \lhd X$ and $b^2 = a_1$, we get $\overline{X} = X/H = \langle \overline{b}\rangle\langle \overline{c}\rangle$ and $\langle \overline{b}\rangle \cong \mathbb{Z}_4$. By considering the permutation representation of $\overline{X}$ on the cosets $[\overline{X} : \langle \overline{c}\rangle]$ of size 4, we know that $\langle \overline{c}^2\rangle \lhd \overline{X}$. So $\langle b, c^2, H\rangle \leq X$, that is, $X_1 := \langle b, c^2, H\rangle = \langle a, b\rangle\langle c^2\rangle = G\langle c^2\rangle \leq X$.

First, suppose that m $(=o(c))$ is even. Then, $[X : X_1] = 2$. Let $\langle c_2\rangle$ be the Sylow 2-subgroup of $\langle c\rangle$. By induction on X_1, $\langle a^2\rangle \lhd X_1$ and, in particular, $\langle c^2\rangle$ normalizes $\langle a^2\rangle$. By Proposition 2.6, we know that $\langle a^i b\rangle\langle c_2\rangle$ is a Sylow 2-subgroup of X for some i. Then we get $X_2 := H(\langle a^i b\rangle\langle c_2\rangle) = \langle a, b\rangle\langle c_0, c_2\rangle < X$. By the minimality of X again, $\langle a^2\rangle \lhd X_2$, which implies $\langle c_2\rangle$ normalizes $\langle a^2\rangle$. Since both $\langle c_2\rangle$ and $\langle c^2\rangle$ normalize $\langle a^2\rangle$ and $\langle c_2, c^2\rangle = \langle c\rangle$, we get $\langle a^2\rangle \lhd X$, which is a contradiction.

Second, suppose that m is odd. Then both q and m_1 are odd, so that $X = X_1 = ((\langle a^2\rangle \rtimes \langle c_0\rangle).\langle c\rangle) \rtimes \langle b\rangle$. By induction on $X_3 := \langle H, c^{m/m_1}\rangle = \langle a, b\rangle\langle c_0, c^{m/m_1}\rangle < X$ and $X_4 := \langle H, c^{m/pq^e}\rangle = \langle a, b\rangle\langle c^{m/pq^e}\rangle < X$, we respectively get both $\langle c^{m/m_1}\rangle$ and $\langle c^{m/pq^e}\rangle$ normalize $\langle a^2\rangle$. Noting $\langle c^{m/m_1}, c^{m/pq^e}\rangle = \langle c\rangle$, we get $\langle a^2\rangle \lhd X$, which is a contradiction again.

Step 3: Exclude the case $m = pq^e$ for a prime q and an integer e. Recall that $a_1 = a^n$ is the unique involution in G; $\langle a_0\rangle$ is a normal subgroup of order p in X; $K = \langle a_0\rangle \times \langle c_0\rangle = (\langle a_0\rangle\langle c\rangle)_X \cong \mathbb{Z}_p^2$; $H = \langle a^2\rangle \rtimes \langle c_0\rangle \lhd X$ (by the induction hypothesis) and $X = ((H.\langle c\rangle).\langle a_1\rangle).\langle b\rangle$. Suppose that $e = 0$. Then, consider $S := G \cap G^c$. Since $a_1 \notin \langle a\rangle_X \leq S$, we get that S is also a p-group, $S \leq \langle a\rangle_X$ and $|S| \leq p^{k-1}$. However, noting $16p^{k+1} \leq |G||G^c|/|S| < |X| = 4p^{k+1}$, we get a contradiction. Suppose that $q = 2$ and $e = 1, 2$. Then using the same argument as above, we get a contradiction again. So in what follows, we assume that either q is odd and $e \geq 1$; or $q = 2$ and $e \geq 3$.

Since H is a p-group and $\langle a^{2p}\rangle = \mho_1(H) \,\mathrm{char}\, H \lhd X$, we get $\langle a^{2p}\rangle \lhd X$. Set $X_5 := (H.\langle c^q\rangle) \rtimes \langle b\rangle = \langle a, b\rangle\langle c^q\rangle < X$. By the induction hypothesis on X_5, we get $\langle a^2\rangle \lhd X_5$, that is, $X_5 = ((\langle a^2\rangle \rtimes \langle c^q\rangle) \rtimes \langle b\rangle$. Clearly, $\langle a^2\rangle = G' \leq X_5' \leq \langle a^2, c^q\rangle$. So set $X_5' = \langle a^2, c_3\rangle$ for some $c_3 \in \langle c^q\rangle$. By Proposition 2.2, both $X/C_X(\langle a^{2p}\rangle)$ and $X_5/C_{X_5}(\langle a^2\rangle)$ are abelian, which implies that $X' \leq C_X(\langle a^{2p}\rangle)$ and $X_5' \leq C_{X_5}(\langle a^2\rangle)$. Then, X_5' is abelian as $\langle a^2\rangle \leq X_5' = \langle a^2, c_3\rangle$. The p'-Hall subgroup of X_5' is normal, which contradicts $\langle c^q\rangle_{X_5} = 1$, meaning that X_5' is an abelian p-group. Set $L := H \rtimes \langle a_1\rangle = \langle a\rangle\langle c_0\rangle < X_5$.

We claim that $L \ntrianglelefteq X$. Arguing by contradiction, assume that $L \lhd X$. If H is abelian, then we get that either $\langle a^2\rangle = Z(L)\,\mathrm{char}\,L \lhd X$, which is a contradiction; or L is abelian, forcing $\langle a_1\rangle\,\mathrm{char}\,L \lhd X$, which is a contradiction again. Therefore, H is nonabelian. Note that $X_5' = \langle a^2, c_3\rangle$ for $c_3 \in \langle c^q\rangle$. If $c_3 \neq 1$, then $c_0 \in \langle c_3\rangle \leq X_5'$ as $\mathrm{o}(c_0) = p$, which implies that $H = \langle a^2, c_0\rangle$ is abelian, which is a contradiction. Therefore, $X_5' = \langle a^2\rangle$, which implies $L = \langle a\rangle \rtimes \langle c_0\rangle$. Note that $\langle a_1\rangle\,\mathrm{char}\,L \lhd X$. Thus, we get $\langle a_1\rangle \lhd X$, which contradicts $a_1 \notin \langle a\rangle_X$. Therefore, $L \ntrianglelefteq X$, which implies that $\langle\overline{c}\rangle$ does not normalize $\langle\overline{a_1}\rangle$ in $\overline{X} = X/H$.

In $\overline{X} = X/H = (\langle\overline{c}\rangle \rtimes \langle\overline{a_1}\rangle).\langle\overline{b}\rangle$, we get that either $\overline{c}^{\overline{a_1}} = \overline{c}^{-1}$ if q is odd; or $\overline{c}^{\overline{a_1}}$ is either $\overline{c}^{-1}$ or $\overline{c}^{\pm 1+2^{e-1}}$ if $q = 2$. Then we divide the proof into the following two cases.

Case (1): q is an odd prime. In this case, q is odd. Since $\overline{c}^{\overline{a_1}} = \overline{c}^{-1}$ in $\overline{X} = X/H$, we get $\langle a^2, c^{qp}\rangle \leq X_5' \leq \langle a^2\rangle\langle c^q\rangle$. Note that X_5' is the abelian p-group. Thus, either $q \neq p$ and $e = 1$; or $q = p$. Suppose that $q \neq p$ and $e = 1$, that is, $\mathrm{o}(c) = pq$. Consider $M = \langle a\rangle\langle c\rangle \lhd X$. Then, by Proportion 2.4, M' is abelian. Note that $\langle c\rangle_X = 1$ and G_X is the p-group. Thus, M' is an abelian p-group with the same argument as the case of X_5'. Noting that $\langle a_1\rangle\langle c^p\rangle$ is the p'-Hall subgroup of M, we get $[a_1, c^p] \in \langle a_1\rangle\langle c^p\rangle \cap M' = 1$, which implies $\overline{c}^{\overline{a_1}} = \overline{c}$ in $\overline{X} = X/H$, which is a contradiction. So in what follows, we assume that $q = p$, that is, $\mathrm{o}(c) = p^{e+1}$. Note that $\overline{c}^{\overline{a_1}} = \overline{c}^{-1}$ in $\overline{X} = X/H$ and $\langle a^2\rangle \leq X_5'$. Thus, X_5' is either $\langle a^2\rangle\langle c^p\rangle$ or $\langle a^2\rangle$, noting $X_5' = \langle a^2\rangle$ only happens when $e = 1$.

Suppose that $X_5' = \langle a^2\rangle\langle c^p\rangle$. Since $H = \langle a^2\rangle \rtimes \langle c_0\rangle \leq X_5' \leq C_{X_5}(\langle a^2\rangle)$, we get that $H = \langle a^2\rangle \times \langle c_0\rangle$ is abelian. Note that both $\langle a^2\rangle$ and $\langle c\rangle$ are p-groups and $X = (H.\langle c\rangle) \rtimes \langle b\rangle$. Set $(a^2)^c = a^{2s}c_0^t$ and $c^b = a^{2u}c^v$, where $s \equiv 1(\mathrm{mod}\ p)$ and $p \nmid v$. Then for an integer w, we get $(a^2)^{c^w} = a^{2x_1}c_0^{wt}$ and $c_0^b = a^{x_2}c_0^v$ for some integers x_1 and x_2. Since $((a^2)^c)^b = (a^{2s}c_0^t)^b$, there exist some integers x and y such that

$$((a^2)^c)^b = (a^{-2})^{c^v} = a^x c_0^{-vt} \quad \text{and} \quad ((a^2)^s c_0^t)^b = a^y c_0^{vt},$$

which gives $t \equiv 0\,(\mathrm{mod}\ p)$. Then, $\langle a^2\rangle \lhd X$, which is a contradiction.

Suppose that $X_5' = \langle a^2\rangle$. Then, $\mathrm{o}(c) = p^2$, $c_0 = c^p$ and $X_5 = \langle a, b\rangle\langle c_0\rangle$. Since $X_5' \leq G \leq X_5$, we get that $\langle a_1\rangle\,\mathrm{char}\,G \lhd X$, which implies that $\langle a_1\rangle \leq Z(X_5)$ as a_1 is an involution. Thus, $[c_0, a_1] = 1$. Set $c^{a_1} = a^x c^{-1+yp}$ as $\overline{c}^{\overline{a_1}} = \overline{c}^{-1}$ in $\overline{X} = X/H$. Then,

$$c = c^{a_1^2} = (a^x c^{-1} c_0^y)^{a_1} = a^x (a^x c^{-1} c_0^y)^{-1} c_0^y = a^x c_0^{-y} c a^{-x} c_0^y = a^x c^{1-yp} a^{-x} c^{yp},$$

which implies $(a^x)^{c^{1-yp}} = a^x$. Then, $[a^x, c] = 1$. Note that $c_0 = c^p$ and $c_0 = c_0^{a_1} = (c^{a_1})^p = a^x c^{-p}$ for some x. Thus, we get $c_0^2 = 1$, which contradicts $\mathrm{o}(c_0) = p$.

Case (2): $q = 2$. In this case, we know that $\mathrm{o}(c) \geq 8p$, $X_5 = (\langle a^2\rangle\langle c^2\rangle) \rtimes \langle b\rangle \lhd X$ and $\overline{c}^{\overline{a_1}}$ is either $\overline{c}^{-1}$ or $\overline{c}^{\pm 1+2^{e-1}}$ in X/H.

We show $\overline{c}^{\overline{a_1}} = \overline{c}^{1+2^{e-1}}$ in X/H. Since $\langle a^2\rangle \leq X_5'\,\mathrm{char}\,X_5 \lhd X$ and X_5' is the abelian p-group, we get $X_5' = H$, which implies that H is abelian. By Proposition 2.6, we get that both $\langle a^{i_1}b\rangle\langle c^p\rangle$ and $\langle a^{i_2}b\rangle\langle c^{2p}\rangle$ are Sylow 2-subgroups of X and X_5 for some i_1 and i_2, respectively. Then, $[c^{2p}, a^{i_2}b] \in X_5' \cap \langle c^{2p}\rangle\langle a^{i_2}b\rangle = 1$, which implies that $\langle c^{2p}\rangle\langle a^{i_2}b\rangle$ is abelian. So, $[c^{2p}, a_1] = 1$. Since $\overline{c}^{\overline{a_1}}$ is either $\overline{c}^{-1}$ or $\overline{c}^{\pm 1+2^{e-1}}$ in X/H, we get

https://doi.org/10.1017/S1446788724000181 Published online by Cambridge University Press

$\overline{c}^{\overline{a_1}} = \overline{c}^{1+2^{e-1}}$ in X/H. Since $\langle a^{i_1}b\rangle\langle c^p\rangle = (\langle c^p\rangle \rtimes \langle a_1\rangle).\langle a^{i_1}b\rangle$, we know $(c^p)^{a_1} = c^{p+2^{e-1}p}$, which implies $c^{2^{e-1}p} \in M'$.

Noting that $\langle c^p\rangle \rtimes \langle a_1\rangle = \langle a_1, c^p | a_1^2 = c^{2^e p} = 1, (c^p)^{a_1} = c^{(1+2^{e-1})p}\rangle$, there are only three involutions in $\langle c^p\rangle \rtimes \langle a_1\rangle$: $a_1, c^{2^{e-1}p}$ and $a_1c^{2^{e-1}p}$. By Proposition 2.5, we know that $\langle c^{2p}\rangle \lhd \langle a^{i_1}b\rangle\langle c^q\rangle$. Recall that $M = \langle a\rangle\langle c\rangle$. By Proposition 2.4, M' is abelian. Let M_2 be the Sylow 2-subgroup of M'. Note that $M_2 \operatorname{char} M' \operatorname{char} M \lhd X$, $c^{2^{e-1}p} \in M'$, $\langle c\rangle_X = 1$ and a_1 is an involution. Thus, we get $M_2 \cong \mathbb{Z}_2^2$, that is, $M_2 = \langle c^{2^{e-1}p}\rangle \times \langle a_1\rangle$. Consider $HM_2 \le X$. Since $M_2 \lhd X$, $H \lhd X$, $H \cap M_2 = 1$ and p is odd prime, we get $HM_2 = H \times M_2 \lhd X$, which implies that a normalizes $\langle c^{2^{e-1}p}\rangle$. Recall that $\langle c^{2p}\rangle\langle a^{i_2}b\rangle$ is abelian. Then, we get $[c^{2p}, a^{i_2}b] = 1$. Since $\langle c^{2^{e-1}p}\rangle \le \langle c^{2p}\rangle$, we get that b also normalizes $\langle c^{2^{e-1}p}\rangle$. Since $X = \langle a, b, c\rangle$, we get $\langle c^{2^{e-1}p}\rangle \lhd X$, which is a contradiction. □

LEMMA 4.3. *Theorem 1.2 holds.*

PROOF. (1) Suppose that $\langle c\rangle_X = 1$. For the five cases of Theorem 1.1, we know that M_X is M, $\langle a^2\rangle\langle c^2\rangle$, $\langle a^2\rangle\langle c^3\rangle$, $\langle a^3\rangle\langle c^4\rangle$ or $\langle a^4\rangle\langle c^3\rangle$. Set $M_X = \langle a^i\rangle\langle c^j\rangle$, which is one of the above five cases, and $X_1 = GM_X = \langle a, b\rangle\langle c^j\rangle$, where $G \in \{Q, D\}$. Then, $\langle c^j\rangle_{X_1} = 1$. By Proposition 2.11 and Lemma 4.2, we get $\langle a^2\rangle \lhd X_1$, that is, c^j normalizes $\langle a^2\rangle$, and so $M_X \cap \langle a^2\rangle \lhd M_X$.

(2) Suppose $\langle c_1\rangle := \langle c\rangle_X \neq 1$. Then, by Proposition 2.2, we get $\langle c\rangle \le C_X(\langle c_1\rangle) \lhd X$ and $\overline{X} = X/C_X(\langle c_1\rangle) = \langle \overline{a}, \overline{b}\rangle$ is abelian. This implies $\langle \overline{a}, \overline{b}\rangle \lesssim \mathbb{Z}_2 \times \mathbb{Z}_2$ or $\mathbb{Z}_4$. Therefore, $\langle a^2, c\rangle \le C_X(\langle c_1\rangle)$. Therefore, $|X : C_X(\langle c_1\rangle)| \le 4$. □

To classify skew product groups of generalized quaternion groups, the following lemma is useful.

LEMMA 4.4. *Let $G \in \{Q, D\}$ and $X = X(G)$. If $\langle c\rangle_X = 1$ and $\langle a\rangle \lhd X$, then $G \lhd X$.*

PROOF. $X = (\langle a\rangle \rtimes \langle c\rangle).\langle b\rangle$, and so we may write $a^c = a^i$ and $c^b = a^kc^j$. If $j = 1$, then $G \lhd X$. So assume $j \neq 1$. Since $b^2 = a^n$ ($o(a^n) = 1$ or 2 if $G = D$ or $G = Q$, respectively) and $\langle a^n\rangle \lhd X$, we get $a^n \in Z(X)$, which implies $c = c^{b^2}$. Then,

$$c = (c^b)^b = (a^kc^j)^b = a^{-k}(a^kc^j)^j = c^j(a^kc^j)^{j-1},$$

that is, $c^{1-j} = (a^kc^j)^{j-1} = (c^{j-1})^b$, so that b normalizes $\langle c^{1-j}\rangle$. Since $\overline{X} = X/C_X(\langle a\rangle) \le \operatorname{Aut}(\langle a\rangle)$, which is abelian, we get $\overline{c} = \overline{c}^{\overline{b}} = \overline{c}^j$, that is, $c^{1-j} \le C_X(\langle a\rangle)$ so that $[c^{1-j}, a] = 1$. Thus, we get $\langle c^{1-j}\rangle \lhd X$. It follows from $\langle c\rangle_X = 1$ that $j = 1$, which is a contradiction. □

5. Proof of Theorem 1.3

To prove Theorem 1.3, set $R := \{a^{2n} = c^m = 1, b^2 = a^n, a^b = a^{-1}\}$. Recall that M is the subgroup of the largest order in $X(Q)$ such that $\langle c\rangle \le M \subsetneqq \langle a\rangle\langle c\rangle$. By Theorems 1.1 and 1.2, we get that $X(Q)$, where $\langle c\rangle_{X(Q)} = 1$ has the forms listed in Table 3. Then, we deal with these five cases in the following five subsections, separately.

TABLE 3. The forms of $\langle c\rangle_{X(Q)} = 1$.

Case	M	$M_{X(Q)}$	$X(Q)/M_{X(Q)}$
1	$\langle a\rangle\langle c\rangle$	$(\langle a^2\rangle \rtimes \langle c\rangle).\langle a\rangle$	$\mathbb{Z}_2$
2	$\langle a^2\rangle\langle c\rangle$	$\langle a^2\rangle \rtimes \langle c^2\rangle$	D_8
3	$\langle a^2\rangle\langle c\rangle$	$\langle a^2\rangle \rtimes \langle c^3\rangle$	A_4
4	$\langle a^4\rangle\langle c\rangle$	$\langle a^4\rangle \rtimes \langle c^3\rangle$	S_4
5	$\langle a^3\rangle\langle c\rangle$	$(\langle a^6\rangle \rtimes \langle c^4\rangle).\langle a^3\rangle$	S_4

Let $A = G.\langle t\rangle$, where $G \lhd A$, be a group and $t^l = g \in G$. Then, t induces an automorphism τ of G by conjugacy. Recall that by the cyclic extension theory of groups, this extension is valid if and only if

$$\tau^l = \mathrm{Inn}(g) \quad \text{and} \quad \tau(g) = g.$$

5.1. $M = \langle a\rangle\langle c\rangle$.

LEMMA 5.1. *Suppose that $X = X(Q)$, $M = \langle a\rangle\langle c\rangle$ and $\langle c\rangle_X = 1$. Then,*

$$X = \langle a, b, c \mid R, (a^2)^c = a^{2r}, c^a = a^{2s}c^t, c^b = a^u c^v\rangle, \tag{5-1}$$

where

$$r^m \equiv r^{t-1} \equiv r^{v-1} \equiv 1 \pmod{n}, t^2 \equiv 1 \pmod{m},$$

$$2s\sum_{l=1}^{t} r^l + 2sr \equiv 2sr + 2s\sum_{l=1}^{v} r^l - u\sum_{l=1}^{t} r^l + ur \equiv 2(1-r) \pmod{2n},$$

$$2s\sum_{l=1}^{w} r^l \equiv u\sum_{l=1}^{w}\Big(1 - s\Big(\sum_{l=1}^{t} r^l + r\Big)\Big)^l \equiv 0 \pmod{2n}$$

only when $w \equiv 0 \pmod{m}$, and moreover, if $2 \mid n$, then $u(\sum_{l=0}^{v-1} r^l - 1) \equiv 0 \pmod{2n}$ and $v^2 \equiv 1 \pmod{m}$; if $2 \nmid n$, then $u\sum_{l=1}^{v} r^l - ur \equiv 2sr + (n-1)(1-r) \pmod{2n}$ and $v^2 \equiv t \pmod{m}$; and if $t \neq 1$, then u is even.

PROOF. Noting $\langle a^2\rangle \lhd X$ and $M = \langle a\rangle\langle c\rangle \leq X$, the group X may be obtained by three cyclic extensions of groups in order:

$$\langle a^2\rangle \rtimes \langle c\rangle, \quad (\langle a^2\rangle \rtimes \langle c\rangle).\langle a\rangle \quad \text{and} \quad ((\langle a^2\rangle \rtimes \langle c\rangle).\langle a\rangle).\langle b\rangle.$$

So X has presentation as in (5-1). Then, we should determine the parameters r, s, t, u and v by analysing three extensions.

(1) $\langle a^2\rangle \rtimes \langle c\rangle$, where $(a^2)^c = a^{2r}$. Set $\pi_1 \in \mathrm{Aut}\,(\langle a^2\rangle)$ such that $\pi_1(a^2) = a^{2r}$. Since $\pi_1(\langle a^2\rangle) = \langle a^{2r}\rangle$, we get $(r, n) = 1$. As mentioned before, this extension is valid if and only if $\mathrm{o}(\pi_1(a^2)) = \mathrm{o}(a^2)$ and $\pi_1^m = 1$, that is,

$$r^m - 1 \equiv 0 \pmod{n}. \tag{5-2}$$

(2) $(\langle a^2\rangle \rtimes \langle c\rangle).\langle a\rangle$, where $c^a = a^{2s}c^t$. Set $\pi_2 \in \mathrm{Aut}\,(\langle a^2\rangle \rtimes \langle c\rangle)$: $a^2 \to a^2$ and $c \to a^{2s}c^t$. Since $\pi_2(\langle a^2, c\rangle) = \langle a^2, a^{2s}c^t\rangle$, we get $(t, m) = 1$. This extension is valid if and only if the following three equalities hold:

(i) π_2 preserves $(a^2)^c = a^{2r}$:

$$r^{t-1} - 1 \equiv 0\,(\mathrm{mod}\ n); \tag{5-3}$$

(ii) $\mathrm{o}(\pi_2(c)) = m$: for any integer i,

$$(a^{2s}c^t)^i = c^{it}(a^{2s})^{c^{it}} \cdots (a^{2s})^{c^t} = c^{it}a^{2s\sum_{l=1}^{i} r^{tl}} = c^{ti}a^{2s\sum_{l=1}^{i} r^l}.$$

Note that $c^{it} \neq 1$ for any $0 < i < m$. Thus, we only show $(a^{2s}c^t)^m = 1$, that is,

$$s\sum_{l=1}^{m} r^l \equiv 0\,(\mathrm{mod}\ n); \tag{5-4}$$

(iii) $\pi_2^2 = \mathrm{Inn}(a^2)$:

$$ca^{2-2r} = \mathrm{Inn}(a^2)(c) = \pi_2^2(c) = (a^{2s}c^t)^a = a^{2s}(a^{2s}c^t)^t = c^{t^2}a^{2sr+2s\sum_{l=1}^{t} r^l},$$

that is,

$$t^2 - 1 \equiv 0\,(\mathrm{mod}\ m) \quad \text{and} \quad s\sum_{l=1}^{t} r^l + rs + r - 1 \equiv 0\,(\mathrm{mod}\ n). \tag{5-5}$$

(3) $((\langle a^2\rangle \rtimes \langle c\rangle).\langle a\rangle).\langle b\rangle$, where $c^b = a^uc^v$. Set $\pi_3 \in \mathrm{Aut}\,((\langle a^2\rangle \rtimes \langle c\rangle).\langle a\rangle) : a \to a^{-1}$ and $c \to a^uc^v$, where $(v, m) = 1$. We divide the proof into two cases according to the parity of u, separately.

Case 1: u is even.

(i) π_3 preserves $(a^2)^c = a^{2r}$:

$$r^{v-1} - 1 \equiv 0\,(\mathrm{mod}\ n). \tag{5-6}$$

(ii) $\mathrm{o}(\pi_3(c)) = m$:

$$1 = (a^uc^v)^m = c^{vm}a^{u\sum_{l=1}^{m} r^l},$$

that is,

$$u\sum_{l=1}^{m} r^l \equiv 0\,(\mathrm{mod}\ 2n). \tag{5-7}$$

(iii) π_3 preserves $c^a = a^{2s}c^t$: we get $(c^a)^b = (a^{2s}c^t)^b$, which implies $a^uc^v = ((a^{2s}c^t)^b)^a$.

$$a^uc^v = (a^{-2s}(a^uc^v)^t)^a = a^{-2s}(a^u(a^{2s}c^t)^v)^t = a^{-2s}c^{t^2v}a^{(ru+2s\sum_{l=1}^{v} r^l)\sum_{l=0}^{t-1} r^l},$$

that is,

$$r(u+2s) \equiv \Big(ru + 2s\sum_{l=1}^{v} r^l\Big)\sum_{l=0}^{t-1} r^l \pmod{2n}. \tag{5-8}$$

By (5-5), (5-8) is equivalent to

$$u\sum_{l=1}^{t} r^l - ur - 2s\sum_{l=1}^{v} r^l - 2sr + 2(1-r) \equiv 0 \pmod{2n}. \tag{5-9}$$

(iv) $\pi_3^2 = \mathrm{Inn}(a^n)$: Suppose that n is even. Then, $a^n \in \langle a^2\rangle$, which implies $(a^n)^c = a^n$. Then, $\pi_3^2 = \mathrm{Inn}(a^n) = 1$.

$$c = \mathrm{Inn}(a^n)(c) = \pi_3^2(c) = c^{b^2} = a^{-u}(a^u c^v)^v = c^{v^2} a^{u\sum_{l=1}^{v} r^l - ur},$$

that is,

$$u\sum_{l=1}^{v} r^l - ur \equiv 0 \pmod{2n} \quad \text{and} \quad v^2 - 1 \equiv 0 \pmod{m}. \tag{5-10}$$

Suppose that n is odd. Then, $c^{a^n} = c^t a^{(n-1)(1-r)+2sr}$, so

$$c^t a^{(n-1)(1-r)+2sr} = \mathrm{Inn}(a^n)(c) = \pi_3^2(c) = c^{b^2} = a^{-u}(a^u c^v)^v = c^{v^2} a^{u\sum_{l=1}^{v} r^l - ur},$$

that is,

$$u\sum_{l=1}^{v} r^l - ur \equiv (n-1)(1-r) + 2sr \pmod{2n} \quad \textit{and} \quad v^2 - t \equiv 0 \pmod{m}. \tag{5-11}$$

Case 2: u is odd. If $t = 1$, then c normalizes $\langle a\rangle$, which implies $\langle a\rangle \lhd X$. By Lemma 4.4, we get $G \lhd X$. Then, $v = 1$. With the same argument as Case 1,

$$u\sum_{l=1}^{m} (1-2sr)^l \equiv 0 \pmod{2n}. \tag{5-12}$$

So assuming $t \neq 1$, we shall get a contradiction.

Let $S = \langle a^2, c\rangle$. Since u is odd again, we know that $\langle a^2\rangle \leq S_X < S$. Since $|X : S| = 4$, we have $\overline{X} = X/S_X = \langle \overline{c}, \overline{a}\rangle.\langle \overline{b}\rangle \lesssim S_4$. The only possibility is $\mathrm{o}(\overline{c}) = 2$ and $\overline{X} \cong D_8$ so that m is even and v is odd. Then, t is odd, as $t^2 \equiv 1 \pmod{m}$. Moreover, we have $\langle a^2, c^2\rangle = S_X \lhd X$.

Consider $\overline{X} = X/\langle a^2\rangle = \langle \overline{a}, \overline{c}\rangle.\langle \overline{b}\rangle$, where $\overline{a}^{\overline{b}} = \overline{a}$, $\overline{b}^2 = \overline{a}^n$, $\overline{c}^{\overline{a}} = \overline{c}^t$ and $\overline{c}^{\overline{b}} = \overline{ac}^v$. Let π_3 be defined as above. Since the induced action of π_3 preserves $\overline{c}^{\overline{a}} = \overline{c}^t$, we have $(\overline{ac}^v)^{\overline{a}} = (\overline{ac}^v)^t$, that is $\overline{ac}^{tv} = \overline{ac}^v((\overline{ac}^v)^2)^{(t-1)/2} = \overline{ac}^v(\overline{c}^{tv+v})^{(t-1)/2} = \overline{ac}^{v+(v(t+1)(t-1))/2}$, which implies $tv \equiv v + v(t+1)(t-1)/2 \pmod{m}$. Noting that $t^2 \equiv 1 (\mathrm{mod}\ m)$, $t \neq 1$

and $(v, m) = 1$,

$$t \equiv 1 + \frac{m}{2} \pmod{m}. \tag{5-13}$$

Let $X_1 = GS_X = \langle a, b\rangle\langle c^2\rangle$. By (5-13), we have $(c^2)^a = (a^{2s}c^t)^2 = a^{2s(1+r^{-1})}c^2$, which implies that c^2 normalizes $\langle a\rangle$. By Lemma 4.4, we get $G \lhd X_1$.

If n is odd, then $X_1 = \langle a, b\rangle \rtimes \langle c^2\rangle \lhd X$, which implies $\langle a^n\rangle \lhd X_1$. Note that a^n is an involution and $\langle c^2\rangle_{X_1} = 1$, then a^n is the unique involution in $Z(X_1)$. Then $\langle a^n\rangle \operatorname{char} X_1 \lhd X$, which implies $a^n \in G_X$, that is, $\langle a\rangle \lhd X$. By Lemma 4.4 again, we get $G \lhd X$, which implies $t = v = 1$, which is a contradiction. So in what follows, we assume that n is even.

By $G \lhd X_1$, we get $b^{c^2} \in G$. Since $b^{c^2} = c^{v(t+1)-2}a^x b$ for some x, we get $v(t+1) - 2 \equiv 0 \pmod{m}$. By combining this with (5-13),

$$v \equiv 1 \pm \frac{m}{4} \left(\operatorname{mod} \frac{m}{2}\right), \quad 4|m. \tag{5-14}$$

Since $\overline{c} = \overline{c}^{\overline{b}^{-2}} = \overline{a}(\overline{ac}^v)^v = \overline{c}^v(\overline{ac}^v\overline{ac}^v)^{(v-1)/2} = \overline{c}^{v+(tv+v)(v-1)/2}$,

$$(v-1)\left(\frac{v(t+1)}{2} + 1\right) \equiv 0 \pmod{m}. \tag{5-15}$$

Then (5-14) and (5-15) may give $m/2 \equiv 0 \pmod{m}$, which is a contradiction.

(4) Ensure $\langle c\rangle_X = 1$: If $t = 1$, then $v = 1$ and $1 - 2sr \equiv r \pmod{n}$ by (5-5). For any integer w,

$$(c^w)^a = (a^{2s}c)^w = c^w a^{2s\sum_{l=1}^{w} r^l} \quad \text{and} \quad (c^w)^b = (a^u c)^w = c^w a^{u\sum_{l=1}^{w}(1-2sr)^l}.$$

Since $\langle c\rangle_X = 1$, we know that $2s\sum_{l=1}^{w} r^l \equiv 0 \equiv u\sum_{l=1}^{w}(1-2sr)^l \pmod{2n}$ only when $w \equiv 0 \pmod{m}$.

If $t \neq 1$, then u is even, for any integer w,

$$(c^w)^a = (a^{2s}c^t)^w = c^{tw} a^{2s\sum_{l=1}^{w} r^l} \quad \text{and} \quad (c^w)^b = (a^u c^v)^w = c^{vw} a^{u\sum_{l=1}^{w} r^l}.$$

Since $\langle c\rangle_X = 1$, we know that $2s\sum_{l=1}^{w} r^l \equiv 0 \equiv u\sum_{l=1}^{w} r^l \pmod{2n}$ if and only if $w \equiv 0 \pmod{m}$.

Summarizing (5-2)–(5-12), we get the parameters (m, n, r, s, t, u, v) as shown in the lemma. Moreover, since all the above conditions are sufficient and necessary, our group $X = X(Q)$ really does exist for any given parameters satisfying the equations. □

5.2. $M = \langle a^2\rangle\langle c\rangle$ and $X/M_X \cong D_8$.

Lemma 5.2. *Suppose that $X = X(Q)$, $M = \langle a^2\rangle\langle c\rangle$, $X/M_X \cong D_8$ and $\langle c\rangle_X = 1$. Then,*

$$X = \langle a, b, c \mid R, (a^2)^{c^2} = a^{2r}, (c^2)^a = a^{2s}c^{2t}, (c^2)^b = a^{2u}c^2, a^c = bc^{2w}\rangle,$$

https://doi.org/10.1017/S1446788724000181 Published online by Cambridge University Press

where either $w = 0$ *and* $r = s = t = u = 1$*; or*

$$\begin{aligned} w \neq 0,\ s = u^2 \sum_{l=0}^{w-1} r^l + (un/2),\ t = 2wu + 1, \\ r^{2w} - 1 \equiv \Big(u \sum_{l=1}^{w} r^l + n/2\Big)^2 - r \equiv 0 \,(\mathrm{mod}\ n), \\ s \sum_{l=1}^{t} r^l + sr \equiv 2sr - u \sum_{l=1}^{t} r^l + ur \equiv 1 - r \,(\mathrm{mod}\ n), \\ 2w(1 + uw) \equiv nw \equiv 2w(r - 1) \equiv 0 \,(\mathrm{mod}\ m/2) \end{aligned}$$

and $2^{1+(-1)^u/2} \sum_{l=1}^{i} r^l \equiv 0 \,(\mathrm{mod}\ n)$ *only when* $i \equiv 0 \,(\mathrm{mod}\ m/2)$.

PROOF. Under the hypothesis, $M_X = \langle a^2 \rangle \rtimes \langle c^2 \rangle$. Set $2n = \mathrm{o}(a)$ and $m = \mathrm{o}(c)$. If n is odd, then $\langle \overline{a}, \overline{b} \rangle \cong \mathbb{Z}_4$, which is a contradiction. So both n and m are even. Since $X/M_X = \langle \overline{a}, \overline{b} \rangle \langle \overline{c} \rangle \cong D_8$, we can choose $\overline{b}$ in X/M_X such that $\overline{a}^{\overline{c}} = \overline{b}$ and $\overline{b}^{\overline{c}} = \overline{a}$. Set $c_1 := c^2$ and $X_1 = GM_X = \langle a, b \rangle \langle c_1 \rangle$. Noting that $\langle a \rangle \langle c_1 \rangle \leq X_1$ and $\langle c_1 \rangle_{X_1} = 1$, by Lemma 5.1, we get $X_1 = \langle a, b, c_1 | R, (a^2)^{c_1} = a^{2r}, c_1^a = a^{2s} c_1^t, c_1^b = a^{2u} c_1^v \rangle$, where

$$\begin{aligned} & r^{m/2} - 1 \equiv r^{t-1} - 1 \equiv r^{v-1} - 1 \equiv u\Big(\sum_{l=0}^{v-1} r^l - 1\Big) \equiv 0 \,(\mathrm{mod}\ n), \\ & s \sum_{l=1}^{t} r^l + sr \equiv sr + s \sum_{l=1}^{v} r^l - u \sum_{l=1}^{t} r^l + ur \equiv 1 - r \,(\mathrm{mod}\ n), \\ & t^2 \equiv v^2 \equiv 1 \Big(\mathrm{mod}\ \frac{m}{2}\Big), \\ & s \sum_{l=1}^{i} r^l \equiv u \sum_{l=1}^{i} r^l \equiv 0 \,(\mathrm{mod}\ n) \text{ if and only if } i \equiv 0 \Big(\mathrm{mod}\ \frac{m}{2}\Big). \end{aligned} \tag{5-16}$$

Moreover, since n is even and $\langle c_1 \rangle_{X_1} = 1$, we get that $b^2 = a^n$ is the unique involution of $Z(X_1)$. Then, $a^n \in Z(X)$, that is, $[b^2, c] = [a^n, c] = 1$. Now $X = X_1.\langle c \rangle$. Set $a^c = bc_1^w$. Then, X may be defined by R and

$$(a^2)^{c_1} = a^{2r},\ c_1^a = a^{2s} c^{2t},\ c_1^b = a^{2u} c^{2v},\ a^c = bc_1^w. \tag{5-17}$$

Then, $a^{c_1} = a^{1-2sr} c_1^{1-t}$ and $b = a^c c_1^{-w}$.

If $w \equiv 0 \,(\mathrm{mod}\ m/2)$, then $\mathrm{o}(a) = \mathrm{o}(a^c) = \mathrm{o}(b) = 4$, which implies

$$X = \langle a, b, c \mid a^4 = c^4 = 1, b^2 = a^2, a^b = a^{-1}, a^c = b, b^c = a^{-1} \rangle,$$

that is, the former part of Lemma 5.2. So in what follows, we assume that $w \not\equiv 0 \,(\mathrm{mod}\ m/2)$.

https://doi.org/10.1017/S1446788724000181 Published online by Cambridge University Press

Recalling $c_1 = c^2$,

$$b^c = (a^c c_1^{-w})^c = a^{c_1} c_1^{-w} = a^{1-2sr} c_1^{1-t-w}.$$

Since $b^2 = a^n \in Z(X)$, we also get $b^c = (b^{-1}a^n)^c = (b^c)^{-1}a^n = c_1^{w+t-1}a^{2sr-1+n}$. Set $\pi \in \mathrm{Aut}\,(X_1) : a \to bc_1^w, b \to a^{1-2sr}c_1^{1-t-w}$ and $c_1 \to c_1$. We need to carry out the following seven steps.

(i) $\mathrm{o}(\pi(b)) = 4$: Since $b^2 \in Z(X)$, we only need to show $(b^c)^2 = a^n$:

$$\begin{aligned} a^n &= (b^c)^2 = (c_1^{w+t-1}a^{2sr-1+n})^2 = c_1^{w+t-1}a^{2sr-1}c_1^{w+t-1}a^{2sr-1} \\ &= c_1^{w+t-1}(c_1^{w+t-1})^a a^{-1}(a^{2sr})^{c_1^{w+t-1}} a^{2sr-1} = c_1^{w+t-1}(a^{2s}c_1^t)^{w+t-1}a^{2sr^{w+1}+2sr-2} \\ &= c_1^{(t+1)(w+t-1)}a^{2sr^{w+1}+2s\sum_{l=1}^{t+w-1} r^l+2sr-2} \\ &= c_1^{w(t+1)}a^{2sr^{w+1}+2s\sum_{l=1}^{w+t-1} r^l+2sr-2}, \end{aligned}$$

that is,

$$w(t+1) \equiv 0\left(\mathrm{mod}\ \frac{m}{2}\right) \quad \text{and} \quad sr^{w+1} + s\sum_{l=1}^{w+t-1} r^l + sr - 1 \equiv \frac{n}{2}\,(\mathrm{mod}\ n), \tag{5-18}$$

which implies $r^{2w} \equiv r^{w(t+1)} \equiv 1\,(\mathrm{mod}\ n)$. Hence, $[c_1^{w(v+1)}, a^2] = [c_1^w, a^2] = 1$.

(ii) $\mathrm{o}(\pi(a)) = 2n$:

$$\begin{aligned} 1 &= (bc_1^w)^{2n} = (a^n(c_1^w)^b c_1^w)^n = (bc_1^w bc_1^w)^n = ((a^{2u}c_1^v)^w c_1^w a^n)^n \\ &= (c_1^{w(v+1)}a^{2ur^w\sum_{l=1}^{w} r^l+n})^n \\ &= c_1^{nw(v+1)}a^{2nur^w\sum_{l=1}^{w} r^l+n^2} = c_1^{nw(v+1)}, \end{aligned}$$

that is,

$$nw(v+1) \equiv 0\left(\mathrm{mod}\ \frac{m}{2}\right). \tag{5-19}$$

(iii) π preserves $(a^2)^{c_1} = a^{2r}$:

$$((a^2)^{c_1})^c = ((a^2)^c)^{c_1} = (bc_1^w bc_1^w)^{c_1} = (c_1^{w(v+1)}a^{2ur^w\sum_{l=1}^{w} r^l+n})^{c_1} = c^{2w(v+1)}a^{2ur^{w+1}\sum_{l=1}^{w} r^l+n}$$

and

$$(a^{2r})^c = ((a^2)^c)^r = (c_1^{w(v+1)}a^{2ur^w\sum_{l=1}^{w} r^l+n})^r = c^{2wr(v+1)}a^{2ur^{w+1}\sum_{l=1}^{w} r^l+n},$$

that is,

$$w(v+1)(r-1) \equiv 0\left(\mathrm{mod}\ \frac{m}{2}\right). \tag{5-20}$$

(iv) π preserves $c_1^a = a^{2s}c_1^t$:

$$(c_1^a)^c = c^{-1}a^{-1}cc_1c^{-1}ac = c_1{}^{(a^c)} = c_1^{bc_1^w} = (c_1^v a^{2ur})^{c_1^w} = c_1^v a^{2ur^{w+1}}$$

https://doi.org/10.1017/S1446788724000181 Published online by Cambridge University Press

and

$$(a^{2s}c_1^t)^c = (c_1^{w(v+1)}a^{2ur^w\sum_{l=1}^{w} r^l+n})^s c_1^t = c_1^{ws(v+1)+t}a^{2sur^{w+1}\sum_{l=1}^{w} r^l+ns},$$

that is,

$$v \equiv ws(v+1)+t\left(\operatorname{mod}\frac{m}{2}\right) \quad \text{and} \quad u \equiv su\sum_{l=1}^{w} r^l + \frac{ns}{2}\ (\operatorname{mod} n). \tag{5-21}$$

(v) π preserves $c_1^b = a^{2u}c_1^v$:

$$(c_1^b)^c = c_1{}^{(b^c)} = c_1^{c_1^{w+t-1}a^{2sr-1+n}} = c_1^t a^{2sr^{2-w}}$$

and

$$(a^{2u}c_1^v)^c = (c_1^{w(v+1)}a^{2ur^w\sum_{l=1}^{w} r^l+n})^u c_1^v = c_1^{wu(v+1)+v}a^{2u^2r^{w+1}\sum_{l=1}^{w} r^l+un},$$

that is,

$$t \equiv wu(v+1)+v\left(\operatorname{mod}\frac{m}{2}\right) \quad \text{and} \quad s \equiv u^2\sum_{l=0}^{w-1} r^l + \frac{un}{2}\ (\operatorname{mod} n). \tag{5-22}$$

(vi) $\pi^2 = \operatorname{Inn}(c_1)$: Recall $\operatorname{Inn}(c_1)(a) = a^{1-2sr}c_1^{1-t}$, $\operatorname{Inn}(c_1)(a^2) = a^{2r}$ and $\operatorname{Inn}(c_1)(b) = c_1^{v-1}a^{2ur}b$.

$$a^{1-2sr}c^{2-2t} = \operatorname{Inn}(c_1)(a) = \pi^2(a) = a^{1-2sr}c^{2-2t-2w+2w},$$

as desired;

$$\begin{aligned} a^{2r} &= \operatorname{Inn}(c_1)(a^2) = \pi^2(a^2) = ((a^2)^c)^c \\ &= (c_1^{w(v+1)}a^{2ur^w\sum_{l=1}^{w} r^l+n})^c = c_1^{w(v+1)}(c_1^{w(v+1)}a^{2ur^w\sum_{l=1}^{w} r^l+n})^{ur^w\sum_{l=1}^{w} r^l+\frac{n}{2}} \\ &= c_1^{w(v+1)(1+uw+n/2)}a^{2(u\sum_{l=1}^{w} r^l+n/2)^2}, \end{aligned}$$

that is,

$$w(v+1)\left(1+uw+\frac{n}{2}\right) \equiv 0\left(\operatorname{mod}\frac{m}{2}\right) \quad \text{and} \quad r \equiv \left(u\sum_{l=1}^{w} r^l + n/2\right)^2 (\operatorname{mod} n); \tag{5-23}$$

and noting (5-20) and (5-21), we get $w(v+1)(r-1) \equiv ws(v+1)+t-v \equiv 0\,(\operatorname{mod} m/2)$ and $u \equiv su\sum_{l=1}^{w} r^l + (ns/2)\,(\operatorname{mod} n)$. Then,

$$\begin{aligned} c^{2(v-1)}a^{2ur}b = \operatorname{Inn}(c_1)(b) &= \pi^2(b) = (c_1^{w+t-1}a^{2sr-1+n})^c \\ &= c_1^{w+t-1}(c_1^{w(v+1)}a^{2ur^w\sum_{l=1}^{w} r^l+n})^{sr}(bc_1^w)^{-1}a^n \\ &= c_1^{t-1+wsr(v+1)}a^{2usr\sum_{l=1}^{w} r^l+srn}b, \end{aligned}$$

as desired.

(vii) Ensure $\langle c\rangle_X = 1$: Since $\langle c\rangle_X \leq M$, we get $\langle c\rangle_X \leq M_X = \langle a^2\rangle\langle c^2\rangle$. Then, $\langle c\rangle_X = \cap_{x\in X}\langle c\rangle^x = \cap_{x\in G}\langle c\rangle^x = \cap_{x\in G}\langle c^2\rangle^x = \langle c^2\rangle_{X_1} = 1$. Recall $s\sum_{l=1}^{i} r^l \equiv u\sum_{l=1}^{i} r^l \equiv 0 \pmod{n}$ if and only if $i \equiv 0 \pmod{(m/2)}$.

Now we are ready to determine the parameters by summarizing (5-16)–(5-23). If $v = 1$, then inserting $v = 1$ in (5-16)–(5-23), we get that $s = u^2\sum_{l=0}^{w-1} r^l + (n/2)$ and $t = 2wu + 1$ by (5-22); $nw \equiv 0 \pmod{m/2}$ by (5-18), (5-19) and (5-23); and $2w(r-1) \equiv 2w(1+uw) \equiv 0 \pmod{m/2}$ by (5-20) and (5-23). All these are summarized in the lemma. So in what follows, we show $v = 1$, that is, $v \equiv 1 \pmod{m/2}$.

Suppose that u is odd. Then by (5-23), we get $(u, n) = (\sum_{l=1}^{w} r^l, n/2) = 1$ as $(r, n) = 1$. Moreover, if $n/2$ is odd, then $\sum_{l=1}^{w} r^l$ is even as r is odd. Then by (5-22), we get $s \equiv u^2\sum_{l=0}^{w-1} r^l + (n/2) \pmod{n}$, which implies $(s, n) = 1$. Then, we have $\sum_{l=1}^{i} r^l \equiv 0 \pmod{n}$ if and only if $i \equiv 0 \pmod{m/2}$ by item (vii) and $\sum_{l=0}^{v-1} r^l \equiv 1 \pmod{n}$ from (5-16). Then, $v \equiv 1 \pmod{m/2}$.

Suppose that u is even. Then, by (5-23), we get $(u, n/2) = (\sum_{l=1}^{w} r^l, n/2) = 1$. Then by (5-22), we get $s \equiv u^2\sum_{l=0}^{w-1} r^l \pmod{n}$, which implies s is even. Then, by (5-21), we get $u \equiv su\sum_{l=1}^{w} r^l \pmod{n}$. Then, we have $\sum_{l=1}^{i} r^l \equiv 0 \pmod{n/2}$ if and only if $i \equiv 0 \pmod{m/2}$ by item (vii) and $\sum_{l=0}^{v-1} r^l \equiv 1 \pmod{n/2}$ from (5-16). Then, $v \equiv 1 \pmod{m/2}$. □

5.3. $M = \langle a^2\rangle\langle c\rangle$ and $X/M_X \cong A_4$.

LEMMA 5.3. *Suppose that $X = X(Q)$, $M = \langle a^2\rangle\langle c\rangle$, $X/M_X \cong A_4$ and $\langle c\rangle_X = 1$. Then,*

$$X = \langle a, b, c \mid R, (a^2)^c = a^{2r}, (c^3)^a = a^{2s}c^3, (c^3)^b = a^{2u}c^3, a^c = bc^{im/2}, b^c = a^x b\rangle,$$

where $n \equiv 2 \pmod 4$ and either:

(1) *$i = s = u = 0$, $r = x = 1$; or*

(2) *$i = 1$, $6|m$, $r^{m/2} \equiv -1 \pmod{n}$ with $o(r) = m$, $s \equiv (r^{-3}-1)/2 + n/2 \pmod{n}$, $u \equiv (r^3-1)/2r^2 + n/2 \pmod{n}$, $x \equiv -r + r^2 + n/2 \pmod{n}$.*

PROOF. Under the hypothesis, $M_X = \langle a^2\rangle \rtimes \langle c^3\rangle$. Set $o(a) = 2n$ and $o(c) = m$. If n is odd, then we get $\langle \overline{a}, \overline{b}\rangle \cong \mathbb{Z}_4$, which is a contradiction. So n is even and $3|m$. Since $X/M_X = \langle \overline{a}, \overline{b}\rangle\langle \overline{c}\rangle \cong A_4$, we can choose $\overline{b}$ such that $\overline{a}^{\overline{c}} = \overline{b}$ and $\overline{b}^{\overline{c}} = \overline{a}\overline{b}$ in X/M_X. Set $c_1 := c^3$ and $X_1 = GM_X = \langle a, b\rangle\langle c_1\rangle$. By Lemma 5.1, we get

$$X_1 = \langle a, b, c_1 \mid R, (a^2)^{c_1} = a^{2r}, (c_1)^a = a^{2s}c_1^t, (c_1)^b = a^{2u}c_1^v\rangle,$$

where

$$r^{m/3} - 1 \equiv r^{t-1} - 1 \equiv r^{v-1} - 1 \equiv u\Big(\sum_{l=0}^{v-1} r^l - 1\Big) \equiv 0 \pmod{n},$$

$$s\sum_{l=1}^{t} r^l + sr \equiv sr + s\sum_{l=1}^{v} r^l - u\sum_{l=1}^{t} r^l + ur \equiv 1 - r \pmod{n},$$

https://doi.org/10.1017/S1446788724000181 Published online by Cambridge University Press

$$t^2-1\equiv v^2-1\equiv 0\left(\mathrm{mod}\ \frac{m}{3}\right),$$
$$s\sum_{l=1}^{i}r^l\equiv u\sum_{l=1}^{i}r^l\equiv 0\ (\mathrm{mod}\ n)\text{ if and only if }i\equiv 0\left(\mathrm{mod}\ \frac{m}{3}\right).\tag{5-24}$$

Moreover, since n is even and $\langle c_1\rangle_{X_1}=1$, we get that $b^2=a^n$ is the unique involution of $Z(X_1)$. Then, $a^n\in Z(X)$. Now $X=X_1.\langle c\rangle$. Set $a^c=bc_1^w$. Then, X may be defined by R and

$$(a^2)^{c_1}=a^{2r},(c_1)^a=a^{2s}c_1^t,(c_1)^b=a^{2u}c_1^v,\ a^c=bc_1^w,b^c=a^{1+2x}bc_1^y.\tag{5-25}$$

If $w\equiv 0\ (\mathrm{mod}\ m/3)$, then $\mathrm{o}(a)=\mathrm{o}(a^c)=\mathrm{o}(b)=4$, which implies

$$X=\langle a,b,c\mid a^4=c^3=1,b^2=a^2,a^b=a^{-1},a^c=b,b^c=ab\rangle,$$

that is, the former part of Lemma 5.3. So in what follows, we assume $w\not\equiv 0\ (\mathrm{mod}\ m/3)$.

What we should do is to determine the parameters r,s,t,u,v,w,x and y by analysing the last extension $X_1.\langle c\rangle$, where $a^c=bc_1^w$ and $b^c=a^{1+2x}bc_1^y$. Set $\pi\in\mathrm{Aut}\,(X_1):a\to bc_1^w,\ b\to a^{1+2x}bc_1^y,\quad c_1\to c_1$. We need to carry out the following eight steps.

(i) $\mathrm{o}(\pi(b))=4$: Since $b^2\in Z(X)$, we only need to show $(b^c)^2=a^n$:

$$\begin{aligned}a^n&=(b^c)^2=(a^{1+2x}bc_1^y)^2=a^{2x+n}(c_1^y)^{ab}a^{-2x}c_1^y\\&=a^{2x+n}(c_1^{vt}a^{2u\sum_{l=1}^{t}r^l-2sr})^ya^{-2x}c_1^y=a^{2x+n}c_1^{vty}a^{2u\sum_{l=1}^{ty}r^l-2s\sum_{l=1}^{y}r^l-2x}c_1^y\\&=c_1^{vty+y}a^{r^y(2u\sum_{l=1}^{ty}r^l+2x(r^y-1)-2s\sum_{l=1}^{y}r^l)+n},\end{aligned}$$

that is,

$$y(tv+1)\equiv 0\left(\mathrm{mod}\ \frac{m}{3}\right)\quad\text{and}\quad u\sum_{l=1}^{ty}r^l+xr^y-x-s\sum_{l=1}^{y}r^l\equiv 0\ (\mathrm{mod}\ n),\tag{5-26}$$

which implies $r^{2y}\equiv r^{y(tv+1)}\equiv 1\ (\mathrm{mod}\ n)$.

(ii) $\mathrm{o}(\pi(ab))=4$: Since $(ab)^2=a^n\in Z(X)$, we only show $((ab)^c)^2=a^n$:

$$\begin{aligned}a^n&=(bc_1^wa^{1+2x}bc_1^y)^2=(a^{n-1}(c_1^w)^{ab}a^{-2x}c_1^y)^2=(a^{n-1}c_1^{wvt+y}a^{r^y(2u\sum_{l=1}^{tw}r^l-2s\sum_{l=1}^{w}r^l-2x)})^2\\&=(c_1^{wvt+y})^aa^{-2+r^y(2u\sum_{l=1}^{tw}r^l-2s\sum_{l=1}^{w}r^l-2x)}c_1^{wvt+y}a^{r^y(2u\sum_{l=1}^{tw}r^l-2s\sum_{l=1}^{w}r^l-2x)}\\&=c_1^{vw+yt+tvw+y}a^{2((r^{w+y}+1)(ur^y\sum_{l=1}^{w}r^l-r^yx+s\sum_{l=1}^{y}r^l)+s\sum_{l=1}^{vw+yt}r^l-1)},\end{aligned}$$

that is,

$$\begin{aligned}&vw+yt+tvw+y\equiv 0\left(\mathrm{mod}\ \frac{m}{3}\right),\\&(r^{w+y}+1)\left(ur^y\sum_{l=1}^{w}r^l-r^yx+s\sum_{l=1}^{y}r^l\right)+s\sum_{l=1}^{vw+yt}r^l-1\equiv\frac{n}{2}\ (\mathrm{mod}\ n),\end{aligned}\tag{5-27}$$

which implies $r^{2w}\equiv r^{vw+yt+tvw+y}\equiv 1\ (\mathrm{mod}\ n)$. Hence, $[c_1^{w(v+1)},a^2]=[c_1^{2w},a^2]=1$.

https://doi.org/10.1017/S1446788724000181 Published online by Cambridge University Press

(iii) $\mathrm{o}(\pi(a)) = 2n$:

$$\begin{aligned} 1 &= ((a^2)^c)^n = (bc_1^w bc_1^w)^n = (c_1^{w(v+1)} a^{2ur^w \sum_{l=1}^w r^l + n})^n \\ &= c_1^{nw(v+1)} a^{2nur^w \sum_{l=1}^w r^l + n^2} = c_1^{nw(v+1)}, \end{aligned}$$

that is,

$$nw(v+1) \equiv 0 \left(\mathrm{mod}\ \frac{m}{3}\right). \tag{5-28}$$

(iv) π preserves $(a^2)^{c_1} = a^{2r}$:

$$((a^2)^{c_1})^c = ((a^2)^c)^{c_1} = (c_1^{w(v+1)} a^{2ur^w \sum_{l=1}^w r^l + n})^{c_1} = c_1^{w(v+1)} a^{2ur^{w+1} \sum_{l=1}^w r^l + n}$$

and

$$(a^{2r})^c = ((a^2)^c)^r = (c_1^{w(v+1)} a^{2ur^w \sum_{l=1}^w r^l + n})^r = c_1^{wr(v+1)} a^{2ur^{w+1} \sum_{l=1}^w r^l + n},$$

that is,

$$w(v+1)(r-1) \equiv 0 \left(\mathrm{mod}\ \frac{m}{3}\right). \tag{5-29}$$

(v) π preserves $c_1^a = a^{2s} c_1^t$:

$$(c_1^a)^c = {c_1}^{(a^c)} = c_1^{bc_1^w} = (a^{2u} c_1^v)^{c_1^w} = c_1^v a^{2ur^{w+1}}$$

and

$$(a^{2s} c_1^t)^c = (c_1^{w(v+1)} a^{2ur^w \sum_{l=1}^w r^l + n})^s c_1^t = c_1^{ws(v+1)+t} a^{2sur^{w+1} \sum_{l=1}^w r^l + sn},$$

that is,

$$v \equiv ws(v+1) + t \left(\mathrm{mod}\ \frac{m}{3}\right) \quad \text{and} \quad u \equiv su \sum_{l=1}^{w} r^l + \frac{sn}{2} \ (\mathrm{mod}\ n). \tag{5-30}$$

(vi) π preserves $c_1^b = a^{2u} c_1^v$: Since $b^c = (a^n b^{-1})^c = c_1^{-y} a^{1+2x} b$,

$$(c_1^b)^c = {c_1}^{(b^c)} = c_1^{c_1^{-y} a^{1+2x} b} = c_1^{a^{1+2x} b} = c_1^{tv} a^{2(u \sum_{l=1}^t r^l - sr + x(r-1))}$$

and

$$(a^{2u} c_1^v)^c = (c_1^{w(v+1)} a^{2ur^w \sum_{l=1}^w r^l + n})^u c_1^v = c_1^{wu(v+1)+v} a^{2u^2 r^{w+1} \sum_{l=1}^w r^l + un},$$

that is,

$$\begin{gathered} tv \equiv wu(v+1) + v \left(\mathrm{mod}\ \frac{m}{3}\right), \\ u \sum_{l=1}^{t} r^l - sr + x(r-1) \equiv u^2 r^{w+1} \sum_{l=1}^{w} r^l + \frac{un}{2} \ (\mathrm{mod}\ n). \end{gathered} \tag{5-31}$$

https://doi.org/10.1017/S1446788724000181 Published online by Cambridge University Press

(vii) $\pi^3 = \mathrm{Inn}(c_1)$: Recall $\mathrm{Inn}(c_1)(a) = a^{1-2sr}c_1^{1-t} = a^{-1}c_1^{1-t}a^{2-2sr}$, $\mathrm{Inn}(c_1)(a^2) = a^{2r}$ and $\mathrm{Inn}(c_1)(b) = c^{3(v-1)}a^{2ur}b$.

$$\begin{aligned}a^{-1}c_1^{1-t}a^{2-2sr} &= \mathrm{Inn}(c_1)(a) = \pi^3(a) = (a^{1+2x}bc_1^{w+y})^c = ((a^2)^c)^x(ab)^c c_1^{w+y}\\ &= (c_1^{w(v+1)}a^{2ur^w\sum_{l=1}^{w} r^l+n})^x a^{n-1}c_1^{wvt+y}a^{r^y(2u\sum_{l=1}^{tw} r^l-2s\sum_{l=1}^{w} r^l-2x)}c_1^{w+y}\\ &= a^{-1}c_1^{vtw(1+x(v+1))+w+2y}a^{n+2ur^w\sum_{l=1}^{tw(1+x(v+1))} r^l-r^w(2s\sum_{l=1}^{w(1+x(v+1))} r^l+2ux\sum_{l=w+1}^{2w} r^l+xn+2x)},\end{aligned}$$

that is,

$$\begin{aligned}&1-t \equiv t(wv+wxv+wx)+w+2y\Big(\mathrm{mod}\ \frac{m}{3}\Big),\\ &r^w\Big(u\sum_{l=1}^{tw(1+x(v+1))} r^l - s\sum_{l=1}^{w(1+x(v+1))} r^l - ux\sum_{l=w+1}^{2w} r^l - \frac{(x+1)n}{2} - x\Big)\\ &\qquad \equiv 1-sr\,(\mathrm{mod}\ n);\end{aligned} \tag{5-32}$$

$$\begin{aligned}a^{2r} &= \mathrm{Inn}(c_1)(a^2) = \pi^3(a^2) = (c_1^{w(v+1)}a^{2ur^w\sum_{l=1}^{w} r^l+n})^{c^2}\\ &= c_1^{w(v+1)}((c_1^{w(v+1)}a^{2ur^w\sum_{l=1}^{w} r^l+n})^{ur^w\sum_{l=1}^{w} r^l})^c a^n\\ &= c_1^{w(v+1)+uw^2(v+1)}((c_1^{w(v+1)}a^{2ur^w\sum_{l=1}^{w} r^l+n})^{(u\sum_{l=1}^{w} r^l)^2}a^{uwn+n}\\ &= c_1^{w(v+1)+uw^2(v+1)(1+uw)}a^{2r^w(u\sum_{l=1}^{w} r^l)^3+n},\end{aligned}$$

that is,

$$\begin{aligned}&w(v+1)+uw^2(v+1)(uw+1) \equiv 0\Big(\mathrm{mod}\ \frac{m}{3}\Big),\\ &r \equiv r^w\Big(u\sum_{l=1}^{w} r^l\Big)^3 + \frac{n}{2}\,(\mathrm{mod}\ n),\end{aligned} \tag{5-33}$$

which implies $(u, n/2) = (\sum_{l=1}^{w} r^l, n/2) = 1$ as $(r, n) = 1$. Moreover, if u is even, then $n/2$ is odd. Noting (5-30), that is, $u \equiv su\sum_{l=1}^{w} r^l + sn/2\,(\mathrm{mod}\ n)$, and $a^{c_1} = b^{c^2}c_1^w$, we get that $(s, n/2) = 1$ and

$$\begin{aligned}c_1^{v-1}a^{2ur}b = \mathrm{Inn}(c_1)(b) = \pi^3(b) &= a^n((b^{-1})^{c^2})^c = a^n((a^{c_1}c_1^{-w})^{-1})^c\\ &= c_1^w(c_1^{t-1}a^{2sr-1})^c a^n = c_1^{w+t-1}(c_1^{w(v+1)}a^{2ur^w\sum_{l=1}^{w} r^l+n})^{sr}(bc_1^w)^{-1}a^n\\ &= c_1^{t-1+ws(v+1)}a^{2usr\sum_{l=1}^{w} r^l+sn}b,\end{aligned}$$

that is,

$$v \equiv t + ws(v+1)\Big(\mathrm{mod}\ \frac{m}{3}\Big). \tag{5-34}$$

(viii) Ensure $\langle c\rangle_X = 1$: Since $\langle c\rangle_X \le M$, we get $\langle c\rangle_X \le M_X = \langle a^2\rangle\langle c^3\rangle$. Noting that $\langle c\rangle_X = \cap_{x\in X}\langle c\rangle^x = \cap_{x\in G}\langle c\rangle^x = \cap_{x\in G}\langle c^3\rangle^x = \langle c^3\rangle_{X_1} = 1$, $s\sum_{l=1}^{i} r^l \equiv u\sum_{l=1}^{i} r^l \equiv 0\,(\mathrm{mod}\ n)$ if and only if $i \equiv 0\,(\mathrm{mod}\ m/3)$, $(s, n/2) = (u, n/2) = 1$, and

https://doi.org/10.1017/S1446788724000181 Published online by Cambridge University Press

both u and s are even only if $n/2$ is odd, we have $2^{(1+(-1)^u)/2}\sum_{l=1}^{i} r^l \equiv 0 \pmod{n}$ if and only if $i \equiv 0 \pmod{m/3}$.

Now we are ready to determine the parameters by summarizing (5-24)–(5-34) by the following three steps.

Step 1: Show $t = v = 1$, $w = m/6$, $r^w \equiv -1 \pmod{n}$ *and* $s \equiv (1-r)/2r \pmod{n/2}$. Since $(r, n) = (u, n/2) = 1$ (after (5-33)), we get from (5-24) that $2^{(1+(-1)^u)/2}\sum_{l=1}^{v-1} r^l \equiv 0 \pmod{n}$. By item (viii), $2^{(1+(-1)^u)/2}\sum_{l=1}^{i} r^l \equiv 0 \pmod{n}$ if and only if $i \equiv 0 \pmod{m/3}$, which means $v \equiv 1 \pmod{m/3}$.

Inserting $v = 1$ in (5-24)–(5-34), we get that $2w(wu+1) \equiv 0 \pmod{m/3}$ and $t \equiv 1 + 2wu \equiv 1 - 2ws \pmod{m/3}$ by (5-27), (5-30) and (5-31). Then, $2w \equiv 0 \pmod{m/3}$ by (5-33), which implies $w = m/6$ as $w \not\equiv 0 \pmod{m/3}$. Inserting $w = m/6$ in (5-24)–(5-34) again, we get $t \equiv 1 \pmod{m/3}$ by (5-31), $s \equiv (1-r)/2r \pmod{n/2}$ by (5-24), and $r^w \equiv -1 \pmod{n}$ by (5-24) and (5-33).

Step 2: Show $y = 0$. Since $2y \equiv 0 \pmod{m/3}$ by (5-26), we know that y is either 0 or $m/6$. Arguing by contradiction, assume that $y = m/6 = w$. Then by (5-27), we get that $n/2$ is odd, and with 5-26) and (5-27), we get $2x \equiv (u-s)\sum_{l=1}^{w} r^l \equiv (n/2) - 1 \pmod{n}$. By (5-30) and $(u, n/2) = 1$, we get $s\sum_{l=1}^{w} r^l \equiv 1 + (sn)/2 \pmod{n}$, then $u\sum_{l=1}^{w} r^l \equiv 0 \pmod{n/2}$, which contradicts $(u, n/2) = (\sum_{l=1}^{w} r^l, n/2) = 1$. So $y = 0$.

Step 3: Determine u *and* x. By (5-27), we get $s\sum_{l=1}^{w} r^l \equiv 1 + n/2 \pmod{n}$. Then, $(s+u)n/2 \equiv 0 \pmod{n}$ in (5-30), which implies $u \equiv s \pmod{2}$. By (5-31), we get $x(r-1) \equiv (s-u)r - u^2 r\sum_{l=1}^{w} r^l + (un/2) \pmod{n}$. If $n/2$ is even, then $u\sum_{l=1}^{w} r^l$ is even. However, in (5-33), we get $r \equiv -(u\sum_{l=1}^{w} r^l)^3 + n/2 \pmod{n}$ which implies that $u\sum_{l=1}^{w} r^l$ is odd as $2 \nmid r$ and $2|n/2$, which is a contradiction. So $n/2$ is odd. Then we get $u\sum_{l=1}^{w} r^l$ is even in (5-33) and u is even in (5-31). Then, $\sum_{l=1}^{i} r^l \equiv 0 \pmod{n/2}$ if and only if $i \equiv 0 \pmod{m/3}$. Recall $s \equiv (r^{-1} - 1)/2 \pmod{n/2}$ in (5-24) and $s\sum_{l=1}^{w} r^l \equiv 1 + n/2 \pmod{n}$ in (5-27). Since $(\sum_{l=1}^{w} r^l, n/2) = 1$ and $x(r-1) \equiv (s-u)r - u^2 r\sum_{l=1}^{w} r^l \pmod{n}$, we get $2x \equiv u\sum_{l=1}^{w} r^l + (u\sum_{l=1}^{w} r^l)^2 - 1 + n/2 \pmod{n}$. Additionally, by (5-33), we get $-r \equiv (u\sum_{l=1}^{w} r^l)^3 + n/2 \pmod{n}$. Take $l = -u\sum_{l=1}^{w} r^l + n/2$, then $r \equiv l^3 \pmod{n}$, $u \equiv (l^3 - 1)/2l^2 + n/2 \pmod{n}$ and $1 + 2x \equiv -l + l^2 + n/2 \pmod{n}$. Let us rewrite l as r and $1 + 2x$ as x for the sake of formatting. Then, $s \equiv ((r^{-3} - 1)/2) + n/2 \pmod{n}$, $u \equiv ((r^3 - 1)/2r^2) + n/2 \pmod{n}$ and $x \equiv -r + r^2 + n/2 \pmod{n}$. □

In fact, if we add the conditions $t = 1$ and $w \neq 0$ and delete $\langle c\rangle_X = 1$ in the above calculation, then we can get the following.

Lemma 5.4. *With the above notation, suppose that* $t = 1$ *and* $w \neq 0$*. Then,*

$$X = \langle a, b, c \mid R, (a^2)^c = a^{2r}, (c^3)^a = a^{2s}c^3, (c^3)^b = a^{2u}c^3, a^c = bc^{m/2}, b^c = a^x b\rangle,$$

where $n \equiv 2 \pmod{4}$, $m \equiv 0 \pmod{6}$, $r^{m/2} \equiv -1 \pmod{n}$, $s \equiv ((r^{-3} - 1)/2) + n/2 \pmod{n}$, $u \equiv ((r^3 - 1)/2r^2) + n/2 \pmod{n}$ *and* $x \equiv -r + r^2 + n/2 \pmod{n}$.

https://doi.org/10.1017/S1446788724000181 Published online by Cambridge University Press

5.4. $M = \langle a^4\rangle\langle c\rangle$ and $X/M_X \cong S_4$.

LEMMA 5.5. *Suppose that* $X = X(Q)$, $M = \langle a^4\rangle\langle c\rangle$, $X/M_X \cong S_4$ *and* $\langle c\rangle_X = 1$. *Then,* $X = \langle a, b, c \mid R, (a^4)^c = a^{4r}, (c^3)^{a^2} = a^{4s}c^3, (c^3)^b = a^{4u}c^3, (a^2)^c = bc^{im/2}, b^c = a^{2x}b, c^a = a^{2(1+2z)}c^{1+(jm/3)}\rangle$, *where either:*

(1) $i = 0$, $r = j = 1, x = 3, s = u = z = 0$; *or*
(2) $i = 1$, $n \equiv 4 \pmod{8}$, $6|m$, $r^{m/2} \equiv -1 \pmod{n/2}$, $\mathrm{o}(r) = m$, $s \equiv (r^{-3} - 1)/2 + n/4 \pmod{n/2}$, $u \equiv (r^3 - 1)/2r^2 + n/4 \pmod{n/2}$, $x \equiv -r + r^2 + n/4 \pmod{n/2}$, $1 + 2z \equiv (1 - r)/2r \pmod{n/2}$, $j \in \{1, 2\}$.

PROOF. Under the hypothesis, $M_X = \langle a^4\rangle \rtimes \langle c^3\rangle$. Set $2n = \mathrm{o}(a)$ and $m = \mathrm{o}(c)$. Then, n is even and $3|m$. If $n/2$ is odd, then $\langle \overline{a}, \overline{b}\rangle \cong Q_8$, a contradiction. So $n/2$ is even. Since $X/M_X = \langle \overline{a}, \overline{b}\rangle\langle \overline{c}\rangle \cong S_4$, we can choose $\overline{b}$ such that the form of X/M_X is the following: $(\overline{a}^2)^{\overline{c}} = \overline{b}$, $\overline{b}^{\overline{c}} = \overline{a}^2\overline{b}$ and $(\overline{c})^{\overline{a}} = \overline{a}^2\overline{c}^2$. Take $a_1 = a^2$ and $c_1 = c^3$. Then, we set $a_1^c = bc_1^w$, $b^c = a_1^x bc_1^y$ and $c^a = a_1^{1+2z}c^{2+3d}$, where x is odd.

Suppose $w \equiv 0 \pmod{m/3}$. Note that $\mathrm{o}(a_1) = \mathrm{o}(a_1^c) = \mathrm{o}(b) = 4$, which implies $G \cong Q_{16}$. Thus, X can only have the following form:

$$X = \langle a, b, c \mid a^8 = c^3 = 1, b^2 = a^4, a^b = a^{-1}, b^c = a_1^3 b, c^a = a_1 c^2\rangle.$$

So in what follows, we assume that $w \not\equiv 0 \pmod{m/3}$.

Then consider $X_1 = GM_X = \langle a, b\rangle\langle c_1\rangle$. Noting $\langle a\rangle\langle c_1\rangle \le X_1$ and $\langle c_1\rangle_{X_1} = 1$, by Theorem 1.2, we know $\langle a_1\rangle \lhd X_1$, which implies that c_1 normalizes $\langle a_1\rangle$. Take $X_2 = \langle a_1, b\rangle\langle c\rangle$. Then we get $X_2 = (\langle a_1, b\rangle\langle c_1\rangle).\langle c\rangle$. Note that c_1 normalizes $\langle a_1\rangle$ in X_2. Thus, by Lemma 5.4, we get

$$X_2 = \langle a_1, b, c \mid R, (a_1^2)^c = a_1^{2r}, c_1^{a_1} = a_1^{2s}c_1, c_1^b = a_1^{2u}c_1, a_1^c = bc^{m/2}, b^c = a^x b\rangle,$$

where

$$n \equiv 4 \pmod{8}, m \equiv 0 \pmod{6}, r^{m/2} \equiv -1 \left(\mathrm{mod}\ \frac{n}{2}\right),$$
$$s \equiv \frac{r^{-3} - 1}{2} + \frac{n}{4} \left(\mathrm{mod}\ \frac{n}{2}\right), u \equiv \frac{r^3 - 1}{2r^2} + \frac{n}{4} \left(\mathrm{mod}\ \frac{n}{2}\right), x \equiv -r + r^2 + \frac{n}{4} \left(\mathrm{mod}\ \frac{n}{2}\right).$$

Note $X = X_2.\langle a\rangle$. Thus, X may be defined by R and

$$(a_1^2)^c = a_1^{2r}, c_1^{a_1} = a_1^{2s}c_1, c_1^b = a_1^{2u}c_1, a_1^c = bc^{m/2}, b^c = a_1^x b, c^a = a_1^{1+2z}c^{2+3d}.$$

What we should do is to determine the parameters r, z and d by analysing the last one extension $X_2.\langle a\rangle$, where $c^a = a_1^{1+2z}c^{2+3d}$. Set $\pi \in \mathrm{Aut}\,(X_1) : a_1 \to a_1, b \to a_1^{-1}b$ and $c \to a_1^{1+2z}c^{2+3d}$, where d is odd. We need to carry out the following eight steps.

(i) π preserves $(a_1^2)^c = a_1^{2r}$:

$$a_1^{2r} = ((a_1^2)^c)^a = ((a_1^2)^a)^{(c^a)} = (a_1^2)^{(c^a)} = (a_1^2)^{a_1^{1+2z}c^{2+3d}} = a_1^{2r^{2+3d}},$$

https://doi.org/10.1017/S1446788724000181 Published online by Cambridge University Press

that is,

$$r^{1+3d}-1\equiv 0\left(\mathrm{mod}\ \frac{n}{2}\right).$$

Since $r^{m/2}\equiv -1\,(\mathrm{mod}\ n/2)$, we get $r^{(1+3d)/2}-1\equiv -1\,(\mathrm{mod}\ n/2)$ and so $\sum_{l=1}^{1+3d} r^{3l}\equiv 0\,(\mathrm{mod}\ n/2)$.

(ii) π preserves $c_1^{a_1}=a_1^{2s}c_1$, that is, $a_1^{c_1}=a_1^{1-2sr^3}$: Since

$$\begin{aligned}c_1^a=(c^a)^3&=a_1^{1+2z}c^{2+3d}a_1^{1+2z}c^{2+3d}a_1^{1+2z}c^{2+3d}\\&=a_1^{1+2z}c_1^{1+d}(c^{-1}a_1^{1+2z}c)c_1^{1+d}(c^{-2}a_1^{1+2z}c^2)c_1^d\\&=a_1^{1+2z}c_1^{1+d}a^{2zr}bc_1^{1+d+m/6}a_1^xbc_1^{m/6}a_1^{2zr^2}c_1^d\\&=a_1^{1+2z}c_1^{1+d}a^{2zr+n2}(a_1^{2u}c_1)^{1+d+m/6}a_1^{-x}c_1^{d+m/6}a_1^{2zr}\\&=c_1^{2+3d}a^{2z(r+r^2+r^3)+2-2sr^3+r^2-x(1-2sr^3)^{d+m/6}+nm/12},\end{aligned}$$

we get

$$(a_1^{c_1})^a=a_1^{c_1^a}=a_1^{(1-2sr^3)^{2+3d}}=a_1^{1-2sr^3},$$

that is,

$$(1-2sr^3)^{1+3d}-1\equiv 0\,(\mathrm{mod}\ n).$$

Set $f=2z(r+r^2+r^3)+2-2sr^3+r^2-x(1-2sr^3)^{d+(m/6)}+nm/12$. Then, f is even and $c_1^a=c_1^{2+3d}a_1^f$. Recalling $s\equiv(r^{-3}-1)/2+n/4\,(\mathrm{mod}\ n/2)$ and $x\equiv -r+r^2+n/4\,(\mathrm{mod}\ n/2)$, we get $2f\equiv 2(1+2z)(r+r^2+r^3)+n/2\,(\mathrm{mod}\ n)$.

(iii) π preserves $c_1^b=a_1^{2u}c_1$, that is, $b^{c_1}=a_1^{2ur^3}b$:

$$(b^{c_1})^a=(b^a)^{(c_1^a)}=(a_1^{-1}b)^{(c_1^a)}=a_1^{2ur^3-r^3+n/2-2f}b=a_1^{2ur^3-r^3-2(1+2z)(r+r^2+r^3)}b$$

and

$$(a_1^{2ur^3}b)^a=a_1^{2ur^3-1}b,$$

that is,

$$2(1+2z)(r+r^2+r^3)\equiv 1-r^3\,(\mathrm{mod}\ n).$$

(iv) π preserves $a_1^c=bc^{m/2}$:

$$(a_1^c)^a=(a_1^a)^{(c^a)}=a_1^{(c^a)}=a^{a_1^{1+2z}c^{2+3d}}=a_1^{x(1-2sr^3)^d+2u\sum_{l=1}^{d}r^{3l}}bc^{m/2}$$

and

$$(bc^{m/2})^a=a_1^{-1}b(c_1^a)^{m/6}=a_1^{(2z(r+r^2+r^3)-2sr^3+r^2-x(1-2sr^3)^{d+m/6}+2)\sum_{l=0}^{m/6-1}r^{3l}-1}bc^{m/2},$$

https://doi.org/10.1017/S1446788724000181 Published online by Cambridge University Press

that is,

$$\Delta \cdot \sum_{l=0}^{m/6-1} r^{3l} \equiv x(1-2sr^3)^d + 2u\sum_{l=1}^{d} r^{3l} + 1 \pmod{n},$$

where $\Delta = r^2 - 2sr^3 - x(1-2sr^3)^{d+m/6} + 2z(r+r^2+r^3) + 2$.

(v) π preserves $b^c = a_1^x b$:

$$\begin{aligned}(b^c)^a &= (ba_1)^{(c^a)} = (a_1^{-2(1+2z)}ba_1)^{c^{2+3d}}\\ &= a_1^{-2(1+2z)r}(ba_1)^{c^{2+3d}} = a_1^{-2(1+2z)r}(a_1^{(x-1+n/2)r}b)^{c_1^d}\\ &= a_1^{x-1-2(1+2z)r+n/2+2u\sum_{l=1}^{d} r^{3l}}b\end{aligned}$$

and

$$(a_1^x b)^a = a_1^{x-1}b,$$

that is,

$$-2(1+2z)r + \frac{n}{2} + 2u\sum_{l=1}^{d} r^{3l} \equiv 0 \pmod{n}. \tag{5-35}$$

(vi) $o(\pi(c)) = m$: By $r^{m/2} \equiv -1 \pmod{n/2}$ again,

$$\sum_{l=0}^{m/3-1} r^{3l} = (1+r^{m/2})\sum_{l=0}^{m/6-1} r^{3l} \equiv 0 \left(\mathrm{mod}\ \frac{n}{2}\right),$$

which implies $f\sum_{l=0}^{m/(3-1)} r^{3l} \equiv 0 \pmod{n}$ as f is even. Then,

$$(c^a)^m = (c_1^a)^{m/3} = (c_1^{2+3d}a_1^f)^{m/3} = c_1^{(2+3d)m/3}a_1^{f\sum_{l=0}^{m/3-1} r^{3l}} = a_1^{f\sum_{l=0}^{m/3-1} r^{3l}} = 1,$$

as desired.

(vii) $\pi^2 = \mathrm{Inn}(a_1)$: Recall $\mathrm{Inn}(a_1)(c) = c^{1+(m/2)}a_1^{n/(2-1)}b$.

$$\begin{aligned}&c^{1+m/2}a_1^{-1+n/2}b\\ &\quad= \mathrm{Inn}(a_1)(c) = \pi^2(c) = (a^{1+2z}c^{2+3d})^a = a^{1+2z}(c^a)^2(c_1^{2+3d}a_1^f)^d\\ &\quad= a^{2+4z}c^{2+3d}a^{1+2z}c^{2+3d(3+3d)}a^{f\sum_{l=0}^{d-1} r^{3l}}\\ &\quad= c^{(3d+2)^2+m/2}a_1^{-3r-1-2z-4zr+(n(2+\sum_{l=0}^{d-1} r^{3l}+(1-2sr^3)^d))/4+(2sr^3-(2zr+1)(1+r+r^2))\sum_{l=0}^{d-1} r^{3l}}b,\end{aligned}$$

that is,

$$\begin{aligned}&(1+d)(1+3d) \equiv 0 \pmod{m/3},\\ &-3r-2z-4zr+\alpha\cdot\sum_{l=0}^{d-1} r^{3l} \equiv 2 + \frac{n(\sum_{l=0}^{d-1} r^{3l} + (1-2sr^3)^d)}{4} \pmod{n},\end{aligned}$$

where $\alpha = 2sr^3 - (2zr+1)(1+r+r^2)$.

https://doi.org/10.1017/S1446788724000181 Published online by Cambridge University Press

(viii) Ensure $\langle c\rangle_X = 1$: Since $\langle c\rangle_X \le M$, we get $\langle c\rangle_X \le M_X = \langle a_1^2\rangle\langle c_1\rangle$, which implies $\langle c\rangle_X = \cap_{x\in X}\langle c\rangle^x = \cap_{x\in G}\langle c\rangle^x = \cap_{x\in G}\langle c_1\rangle^x = \langle c_1\rangle_{X_1}$. Then, it is sufficient to ensure $\langle c^3\rangle_{X_1} = 1$.

Recall

$$X_1 = \langle a, b, c_1 | R, (a_1)^{c_1} = a_1^{r^3}, c_1^b = a_1^{2u}c_1, (c_1)^a = c_1^{2+3d}a_1^i\rangle,$$

where $r^{m/2} \equiv -1 \,(\text{mod}\, n/2)$, $2u \equiv (r^3-1)/r^2 \,(\text{mod}\, n/2)$ and $i \equiv (3(1-r^3)/2) + n/4 \,(\text{mod}\ n/2)$. By (5-35), we get that u is even. Noting $\langle c_1\rangle_{X_1} = 1$ and $(u, n/4) = 1$, by Lemma 5.1,

$$\sum_{l=1}^{j} r^{3l} \equiv 0 \Big(\text{mod}\ \frac{n}{4}\Big) \text{ if and only if } j \equiv 0 \Big(\text{mod}\ \frac{m}{3}\Big).$$

Note that $\sum_{i=1}^{1+3d} r^{3i} \equiv 0 \,(\text{mod}\ n/2)$. Thus, $1+3d \equiv 0 \,(\text{mod}\ m/3)$. Since $1+3d \ne 0$, we get $1+3d$ is either $m/3$ or $2m/3$. By (5-35), we get $1+2z \equiv (1-r)/2r \,(\text{mod}\, n/2)$. □

5.5. $M = \langle a^3\rangle\langle c\rangle$ and $X/M_X \cong S_4$.

LEMMA 5.6. *Suppose that $X = X(Q)$, $M = \langle a^3\rangle\langle c\rangle$, $X/M_X \cong S_4$ and $\langle c\rangle_X = 1$. Then,*

$$X = \langle a, b, c \mid R, a^{c^4} = a^r, b^{c^4} = a^{1-r}b, (a^3)^{c^{m/4}} = a^{-3}, a^{c^{m/4}} = bc^{3m/4}\rangle, \tag{5-36}$$

where $m \equiv 4 \,(\text{mod}\ 8)$ and r is of order $m/4$ in $\mathbb{Z}_{2n}^*$.

In this subsection, $M_X = \langle a^3\rangle\langle c^4\rangle$. Set $a^3 = a_1$ and $c^4 = c_1$ so that $M_X = \langle a_1\rangle\langle c_1\rangle$. Set $\text{o}(a) = 2n$ and $\text{o}(c) = m$, where $3|n$ and $4|m$. Then, we show $\langle a_1\rangle \lhd X$ in Lemma 5.7 and get the classification of X in Lemma 5.8.

LEMMA 5.7. $\langle a_1\rangle \lhd X$.

PROOF. Let $X_1 = M_XG$. Since $\langle a\rangle\langle c_1\rangle \le X_1$ and $\langle c_1\rangle_{X_1} = 1$, the subgroup X_1 has been given in Lemma 5.1:

$$X_1 = \langle a, b, c_1 \mid R,\ (a^2)^{c_1} = a^{2r},\ (c_1)^a = a_1^{2s}c_1^t,\ (c_1)^b = a_1^u c_1^v\rangle, \tag{5-37}$$

$$r^{\frac{m}{4}} \equiv r^{t-1} \equiv r^{v-1} \equiv 1 \ (\text{mod}\ n),\ t^2 \equiv 1 \ (\text{mod}\ m/4),$$

$$6s\sum_{l=1}^{t} r^l + 6sr \equiv 6sr + 6s\sum_{l=1}^{v} r^l - 3u\sum_{l=1}^{t} r^l + 3ur \equiv 2(1-r) \ (\text{mod}\ 2n),$$

$$6s\sum_{l=1}^{w} r^l \equiv 3u\sum_{l=1}^{w}\Big(1 - 3s\Big(\sum_{l=1}^{t} r^l + r\Big)\Big)^l \equiv 0 \ (\text{mod}\ 2n)$$

only when $w \equiv 0$ $(\text{mod}\ m/4)$, and moreover, if $2 \mid n$, then $3u(\sum_{l=0}^{v-1} r^l - 1) \equiv 0$ $(\text{mod}\ 2n)$ and $v^2 \equiv 1$ $(\text{mod}\ m/4)$; if $2 \nmid n$, then $3u\sum_{l=1}^{v} r^l - 3ur \equiv 6sr + (n-1)(1-r)$ $(\text{mod}\ 2n)$ and $v^2 \equiv t$ $(\text{mod}\ m/4)$; and if $t \ne 1$, then u is even.

https://doi.org/10.1017/S1446788724000181 Published online by Cambridge University Press

Now $X = \langle X_1, c\rangle$. Since $X/M_X = \langle \overline{a}, \overline{b}\rangle\langle \overline{c}\rangle \cong S_4$, the only possibility under our conditions is

$$\overline{a}^3 = \overline{c}^4 = \overline{b}^2 = 1, \overline{a}^{\overline{b}} = \overline{a}^{-1}, \overline{a}^{\overline{c}} = \overline{a}^i\overline{b}\overline{c}^3, \tag{5-38}$$

where $i \in \mathbb{Z}_3$. Observing (5-37) and (5-38), we may relabel $a^{i+3x}b$ by b for some $x \in \mathbb{Z}$. Then, in the perimage X, (5-38) corresponds to

$$a^3 = a_1, b^2 = a^n, c^4 = c_1, a^c = bc^{3+4w}. \tag{5-39}$$

Set

$$(a_1)^c = a_1^z c_1^d, \tag{5-40}$$

necessarily, z is odd, as $o(a_1)$ is even. Then, X is uniquely determined by (5-37), (5-39) and (5-40). To show $\langle a_1\rangle \lhd X$, for the contrary, we assume $d \neq 0$. Then we need to deal with two cases according to the parameter t of X_1, separately.

Case 1: $t = 1$. In this case, we get $v = 1$ and $1 - 6sr - r \equiv 0 \pmod{n}$ by X_1. Set $r_1 = 1 - 6sr$. Then, $r_1 \equiv 1 \pmod{6}$, $a^{c_1} = a^{r_1}$ and $b^{c_1} = a_1^{ur_1}b$. By (5-37), (5-39) and (5-40), we get $b^c = a^{2+3x}bc^{4y}$ for some x and y.

Since c preserves $a_1^{c_1} = a_1^{r_1}$,

$$((a_1)^{c_1})^c = (a_1^c)^{c_1} = (a_1^z c_1^d)^{c_1} = c_1^d a_1^{zr_1^{1+d}}$$

and

$$(a_1^{r_1})^c = (a_1^z c_1^d)^{r_1} = c_1^{dr_1} a_1^{z\sum_{l=1}^{r_1} r_1^{dl}},$$

which gives $d \equiv dr_1 \pmod{m/4}$. Since c preserves $b^{c_1} = a_1^{ur_1}b$, there exists some x such that $(b^{c_1})^c = a^{(2+3x+3u)r_1}bc^{4y}$ and $(a_1^{ur_1}b)^c = c_1^{dur_1}a_1^{z\sum_{l=1}^{ur_1} r_1^{dl}}a^{2+3x}bc^{4y}$, which gives $du \equiv 0 \pmod{m/4}$. Since $a_1^{c_1} = a_1^{c^4} = a_1^{x_1}c_1^{d(z^3+z^2+z+1)}$ for some x_1,

$$d(z^3 + z^2 + z + 1) \equiv 0 \left(\bmod\ \frac{m}{4}\right). \tag{5-41}$$

By (5-39), we get $ac = cbc^{3+4w}$. Then, $a_1^{ac} = a_1^z c_1^d$ and $a_1^{cbc^{3+4w}} = a_1^{x_1}c_1^{d-dz(z^2+z+1)}$, which gives

$$dz(z^2 + z + 1) \equiv 0 \left(\bmod\ \frac{m}{4}\right).$$

With (5-41), we know $d \equiv 0 \pmod{m/4}$, which contradicts $d = 0$.

Case 2: $t \neq 1$. In this case, we have $t \neq 1$. If $\langle a_1^2\rangle \lhd X$, then by considering $\overline{X} = X/\langle a_1^2\rangle$ and $\langle \overline{c_1}\rangle \lhd \overline{X}$, one may get $t = 1$, which is a contradiction, as $\langle \overline{c}\rangle \leq C_{\overline{X}}(\langle \overline{c_1}\rangle) = \overline{X}$. In what follows, we show $\langle a_1^2\rangle \lhd X$.

By (5-37), u is even and $r \equiv 1 \pmod{3}$. By using (5-37), (5-39) and (5-40), we get $b^c = a^{2+6x}bc_1^y$ for some x and y, omitting the details.

https://doi.org/10.1017/S1446788724000181 Published online by Cambridge University Press

Since c preserves $(a_1^2)^{c_1} = a_1^{2r}$, there exists some x_1 such that $((a_1^2)^{c_1})^c = a_1^{x_1} c_1^{d(t+1)}$ and $(a_1^{2r})^c = a_1^{x_1} c_1^{d(t+1)r}$, which gives $d(t+1)(r-1) \equiv 0 \pmod{m/4}$. Since c preserves $(c_1)^b = a_1^u c_1^v$, there exists some x_1 such that $(c_1^b)^c = a_1^{x_1} c_1^v$ and $(a_1^u c_1^v)^c = a_1^{x_1} c_1^{(du(t+1)/2)+v}$, which gives $du(t+1)/2 \equiv 0 \pmod{m/4}$. Since c preserves $c_1^a = a_1^{2s} c_1^t$, we get $c_1^{bc^{2+4w}} = a_1^{2s} c_1^t$. Then, there exists some x_1 such that $c_1^{bc^{2+4w}} = (a_1^u c_1^v)^{c^{2+4w}} = ((a_1^z c_1^d)^z c_1^d)^{ur^w} c_1^v = a_1^{x_1} c_1^v$, which gives $v \equiv t \pmod{m/4}$. By (5-39) again, we get $ac^2 = cbc^{4(w+1)}$. Then there exists some x_1 such that $(a_1^2)^{ac^2} = a_1^{x_1} c_1^{d(t+1)(z+1)}$ and $(a_1^2)^{cbc_1^{w+1}} = a_1^{x_1} c_1^{d(t+1)}$, which gives

$$dz(t+1) \equiv 0 \left(\operatorname{mod} \frac{m}{4}\right). \tag{5-42}$$

Since $\mathrm{o}(a_1^c) = 2n/3$, we get $dn(t+1)/3 \equiv 0 \pmod{m/4}$. With $(n/3, z) = 1$ and (5-42), we get $d(t+1) \equiv 0 \pmod{m/4}$. Then, $(a_1^2)^c = (a_1^z c_1^d)^2 = a_1^{x_1} c_1^{d(t+1)} = a_1^{x_1}$ for some x_1, which implies $\langle a_1^2 \rangle \lhd X$, as desired. □

LEMMA 5.8. *The group X is given by (5-36).*

PROOF. By the lemma, $\langle a_1 \rangle \lhd X$, that is, $(a_1)^c = a_1^z$ by (5-40). Since $\langle a^2 \rangle \lhd X_1$, we get $\langle a \rangle \lhd X_1$ and so $G \lhd X_1$, that is, $t = v = 1$ in (5-37). Then, by (5-37), (5-39) and (5-40), we can set $X = \langle a, b, c \mid R, a^{c_1} = a^{r_1}, b^{c_1} = a_1^{ur_1} b, (a_1)^c = a_1^z, a^c = bc^{3+4w} \rangle$, where $r_1 = 1 - 6sr$, $r_1^{m/4} - 1 \equiv 2(r_1 - r) \equiv 0 \pmod{2n}$ and $2s \sum_{l=1}^{j} r^l \equiv 0 \equiv u \sum_{l=1}^{j} r_1^l \pmod{2n/3}$ if and only if $j \equiv 0 \pmod{m/4}$. Note that $2s \sum_{l=1}^{j} r^l \equiv 0 \pmod{2n/3}$ if and only if $r_1^j - 1 \equiv 0 \pmod{2n}$.

In what follows, we divide the proof into two steps.

Step 1: Show $m \equiv 4 \pmod 8$. Set $\langle c \rangle = \langle c_2 \rangle \times \langle c_3 \rangle$, where $\langle c_2 \rangle$ is a 2-group and $\langle c_3 \rangle$ is the $2'$–Hall subgroup of $\langle c \rangle$. Then, $\langle c_1 \rangle = \langle c_2^4 \rangle \times \langle c_3 \rangle$. To show $m \equiv 4 \pmod 8$, we only need to show $c_2^4 = 1$.

Consider $\overline{X} = X/\langle a_1 \rangle = \langle \overline{a}, \overline{b} \rangle \langle \overline{c} \rangle$. Then, $C_{\overline{X}}(\langle \overline{c}_1 \rangle) = \overline{X}$, which implies $\langle \overline{c_1} \rangle \le Z(\overline{X})$ and $\overline{X}/\langle \overline{c_1} \rangle \cong S_4$. Note that $\langle \overline{c}_3 \rangle \le \langle \overline{c}_3 \rangle (\langle \overline{c}_2^4 \rangle \langle \overline{a} \rangle) \le \overline{X}$, where $(|\overline{X} : \langle \overline{c}_3 \rangle (\langle \overline{c}_2^4 \rangle \langle \overline{a} \rangle)|, |\langle \overline{c}_3 \rangle|) = 1$. Thus, by Proposition 2.7, we get that $\langle \overline{c}_3 \rangle$ has a complement in $\overline{X}$, which implies $X = (\langle a, b \rangle \langle c_2 \rangle) \rtimes \langle c_3 \rangle$.

Consider $X_2 = \langle a, b \rangle \langle c_2 \rangle$, where $\langle c_2 \rangle_{X_2} = 1$ and $\langle a_1 \rangle \lhd X_2$, and $\overline{X_2} = X_2/\langle a_1 \rangle = \langle \overline{a}, \overline{b} \rangle \langle \overline{c_2} \rangle$. Note that $\langle \overline{c_2}^4 \rangle \lhd \overline{X_2}$. Then, $C_{\overline{X}_2}(\langle \overline{c_2}^4 \rangle) = \overline{X}_2$, which implies that $\overline{X}_2$ is the central expansion of S_4. By Lemma 2.8, we get the Schur multiplier of S_4 is $\mathbb{Z}_2$, and then $\mathrm{o}(c_2)$ is either 4 or 8. Arguing by contradiction, assume that $\mathrm{o}(c_2) = 8$. Then, c_2^4 normalizes G, and we set $a^{c_2^4} = a^i$, where $i \equiv 1 \pmod 3$. Note that $\langle a \rangle \le C_{X_2}(\langle a_1 \rangle) \lhd X_2$. Then, $\langle a, bc_2, c_2^2 \rangle \le C_{X_2}(\langle a_1 \rangle)$, which implies $\langle a_1 \rangle \times \langle c_2^4 \rangle \lhd X_2$. Since $i \equiv 1 \pmod{2n/3}$ and $i^2 \equiv 1 \pmod{2n}$, we get $i = 1$, which implies $[a, c_2^4] = 1$. Then we have $\langle a, c_2^2 \rangle \le C_{X_2}(\langle a_1 \rangle \times \langle c_2^4 \rangle) \lhd X_2$, which implies $bc_2 \in C_{X_2}(\langle a_1 \rangle \times \langle c_2^4 \rangle)$. So $(c_2^4)^b = c_2^4$.

https://doi.org/10.1017/S1446788724000181 Published online by Cambridge University Press

Then, $c_2^4 \lhd X_2$ is a contradiction. So $\mathrm{o}(c_2) = 4$, which implies $\langle c_1\rangle = \langle c_3\rangle$. Then, $X = (\langle a, b\rangle\langle c_2\rangle) \rtimes \langle c_1\rangle$.

Step 2: Determine the parameters r_1, u, w and z. In $X_2 = \langle a, b\rangle\langle c_2\rangle$, we know $a^{c_2} = bc_2^3$ by (5-39). Consider $\langle a\rangle \le C_{X_2}(\langle a_1\rangle) \lhd X_2$. Then, $C_{X_2}(\langle a_1\rangle)$ is either $\langle a, bc_2, c_2^2\rangle$ or X_2.

Suppose that $C_{X_2}(\langle a_1\rangle) = X$. Then we know $a_1 = b^2$ as $[a_1, b] = 1$, that is, $n = 3$ and $a_1 = a_1^{-1}$. Then, $m = 4$ and $z, r = 1$, as desired.

Suppose that $C_{X_2}(\langle a_1\rangle) = \langle a, bc_2, c_2^2\rangle$. Then, $a_1 = a_1^{bc_2} = (a_1^{-1})^{c_2}$, which implies $z = -1$. In $X_1 = \langle a, b\rangle \rtimes \langle c_1\rangle$, we know $X_1 = \langle a, b, c_1 \mid R, a^{c_1} = a^{r_1}, b^{c_1} = a_1^{ur_1}b\rangle$. Since c_2 preserves $a^{c_1} = a^{r_1}$, we get

$$(bc_2^3)^{c_1} = a_1^{ur_1}bc_2^3 \quad \text{and} \quad (a^{r_1})^{c_2} = (a_1^{(r_1-1)/3})^{c_2}a^{c_2} = a_1^{(1-r_1)/3}bc_2^3,$$

which gives

$$ur_1 \equiv \frac{1 - r_1}{3}\Big(\mathrm{mod}\ \frac{2n}{3}\Big).$$

Recall that $r_1^j - 1 \equiv 0 \equiv 3u\sum_{l=1}^{j} r_1^l \pmod{2n}$ if and only if $j \equiv 0 \pmod{m/4}$. Then, we get that $r_1^j - 1 \equiv 0 \pmod{2n}$ if and only if $j \equiv 0 \pmod{m/4}$, which implies $\mathrm{o}(r_1) = m/4$. For the purpose of formatting uniformity, replacing r_1 by r, then we get (5-36), as desired. □

6. Proof of Theorem 1.4

As mentioned before, the group $X(D)$ where $\langle c\rangle_{X(D)} = 1$ has been classified in [8, Theorem 1.2] by using computational methods in skew morphisms. Actually, with almost the same methods as those that we used in $X(Q)$, we may get a classification of $X(D)$, which has a different representation from [8, Theorem 1.2]. Here is our classification. One may see [4] for its computation in detail.

LEMMA 6.1. *Let $G = D$ and $X = X(D) = G\langle c\rangle$, where $m = \mathrm{o}(c) \ge 2$, $G \cap \langle c\rangle = 1$ and $\langle c\rangle_X = 1$. Set $R := \{a^n = b^2 = c^m = 1, a^b = a^{-1}\}$. Then one of the following holds.*

(1) $X = \langle a, b, c \mid R, (a^2)^c = a^{2r}, c^a = a^{2s}c^t, c^b = a^u c^v\rangle$, *where*

$$2(r^{t-1} - 1) \equiv 2(r^{v-1} - 1) \equiv u\Big(\sum_{l=0}^{v-1} r^l - 1\Big) \equiv 0 \ (\mathrm{mod}\ n),$$

$$t^2 \equiv v^2 \equiv 1 \ (\mathrm{mod}\ m),$$

$$2s\sum_{l=1}^{t} r^l + 2sr \equiv 2sr + 2s\sum_{l=1}^{v} r^l - u\sum_{l=1}^{t} r^l + ur \equiv 2(1 - r) \ (\mathrm{mod}\ n),$$

$$2s\sum_{l=1}^{w} r^l \equiv u\sum_{l=1}^{w}\Big(1 - s\Big(\sum_{l=1}^{t} r^l + r\Big)\Big)^l \equiv 0 \ (\mathrm{mod}\ n)$$

if and only if $w \equiv 0$ (mod m), and if $t \ne 1$, then $u \equiv 0$ (mod 2).

(2) $X = \langle a, b, c \mid R, (a^2)^{c^2} = a^{2r}, (c^2)^b = a^{2s}c^2, (c^2)^a = a^{2u}c^{2v}, a^c = bc^{2w}\rangle$, *where either* $w = s = u = 0$ *and* $r = t = 1$; *or* $w \neq 0$, $s = u^2 \sum_{l=0}^{w-1} r^l$, $t = 1 + 2wu$, $nw \equiv 2w(r-1) \equiv 2w(1 + uw) \equiv 0 \pmod{m/2}$, $r^{2w} - 1 \equiv (u \sum_{l=1}^{w} r^l)^2 - r \equiv (r^w + 1)(1 + s \sum_{l=0}^{w-1} r^l) \equiv 0 \pmod{n/2}$ *and* $\sum_{l=1}^{i} r^l \equiv 0 \pmod{n/2}$ *if and only if* $i \equiv 0 \pmod{m/2}$.

(3) $X = \langle a, b, c \mid R, a^{c^3} = a^r, (c^3)^b = a^{2u}c^3, a^c = bc^{im/2}, b^c = a^x b\rangle$, *where* $n \equiv 2 \pmod 4$ *and either* $i = u = 0$ *and* $r = x = 1$; *or* $i = 1$, $6 \mid m$, $l^{m/2} \equiv -1 \pmod{n/2}$ *with* $\mathrm{o}(l) = m$, $r = l^3$, $u = (l^3 - 1)/2l^2$ *and* $x \equiv -l + l^2 + n/2 \pmod n$.

(4) $X = \langle a, b, c \mid R, (a^2)^{c^3} = a^{2r}, (c^3)^b = a^{(2(l^3-1))/l^2}c^3, (a^2)^c = bc^{im/2}, b^c = a^{2(-l+l^2+n/4)} b, c^a = a^{2+4z}c^{2+3d}\rangle$, *where either* $i = z = d = 0$ *and* $l = 1$; *or* $i = 1$, $n \equiv 4 \pmod 8$, $m \equiv 0 \pmod 6$, $l^{m/2} \equiv -1 \pmod{n/4}$ *with* $\mathrm{o}(l) = m$, $r = l^3$, $z = (1 - 3l)/4l$, $1 + 3d \equiv 0 \pmod{m/3}$ *and* $\sum_{i=1}^{j} r^i \equiv 0 \pmod{n/2}$ *if and only if* $j \equiv 0 \pmod{m/3}$.

(5) $X = \langle a, b, c \mid R, a^{c^4} = a^r, b^{c^4} = a^{1-r}b, (a^3)^{c^{m/4}} = a^{-3}, a^{c^{m/4}} = bc^{3m/4}\rangle$, *where* $m \equiv 4 \pmod 8$ *and* r *is of order* $m/4$ *in* $\mathbb{Z}_n^*$.

Moreover, in the families of groups (1)–(5), for any given parameters satisfying the relevant equations, there exists $X = X(D)$.

PROOF. Comparing Theorem 1.3 and Lemma 6.1, we get that $\langle a^n\rangle \lhd X(Q)$ for all cases in groups (2), (3) and some cases in group (1) under the hypothesis $\langle c\rangle_X = 1$. Moreover, corresponding to $D \cong Q/\langle a^n\rangle$, we have $X(D) = X(Q)/\langle a^n, c_1\rangle$, where $\langle a^n\rangle \lhd X(Q)$ and $\langle a^n, c_1\rangle = \langle a^n, c\rangle_{X(Q)}$. Thus, Theorem 1.4 is proved. □

Acknowledgements

The authors would like to thank the reviewers for their valuable comments and suggestions.

References

[1] B. Amberg, S. Franciosi and F. de Giovanni, *Products of Groups* (Oxford University Press, New York, 1992).

[2] B. Amberg and L. Kazarin, 'Factorizations of groups and related topics', *Sci. China Ser. A* **52**(2) (2009), 217–230.

[3] J. Douglas, 'On the supersolvability of bicyclic groups', *Proc. Natl. Acad. Sci. USA* **47** (1961), 1493–1495.

[4] S. F. Du, W. J. Luo and H. Yu, 'The product of a generalized quaternion group and a cyclic group', Preprint, 2023, arXiv:2305.08617.

[5] S. F. Du, A. Malnič and D. Marušič, 'Classification of 2-arc-transitive dihedrants', *J. Combin. Theory Ser. B* **98**(6) (2008), 1349–1372.

[6] S. F. Du and J. Y. Zhang, 'On the skew-morphisms of dihedral groups', *J. Group Theory* **19** (2016), 993–1016.

[7] W. Gaschütz, 'Zur Erweiterunstheorie endlicher Gruppen', *J. Math.* **190** (1952), 93–107.

[8] K. Hu, I. Kovács and Y. S. Kwon, 'Classification of skew morphisms of dihedral groups', *J. Group Theory* **26**(3) (2023), 547–569.

[9] K. Hu and D. Y. Ruan, 'Smooth skew morphisms of dicyclic groups', *J. Algebraic Combin.* **56** (2022), 1119–1134.

https://doi.org/10.1017/S1446788724000181 Published online by Cambridge University Press

[10] B. Huppert, *Endliche Gruppen. I* (Springer, Berlin, 1967).

[11] N. Itô, 'Über das Produkt von zwei abelschen Gruppen', *Math. Z.* **62** (1955), 400–401.

[12] R. Jajcay and J. Širáň, 'Skew-morphisms of regular Cayley maps', *Discrete Math.* **224**(2002), 167–179.

[13] O. H. Kegel, 'Produkte nilpotenter Gruppen', *Arch. Math.* **12** (1961), 90–93.

[14] I. Kovács and Y. S. Kwon, 'Regular Cayley maps for dihedral groups', *J. Combin. Theory Ser. B* **148** (2021), 84–124.

[15] C. H. Li and B. Z. Xia, 'Factorizations of almost simple groups with a solvable factor, and Cayley graphs of solvable groups', *Mem. Amer. Math. Soc.* **279**(1375) (2022), v+99 pages.

[16] A. Lucchini, 'On the order of transitive permutation groups with cyclic point-stabilizer', *Atti. Accad. Naz. Lincei CI. Sci. Fis. Mat. Natur. Rend. Lincei (9) Mat. Appl*. **9** (1998), 241–243.

[17] V. S. Monakhov, 'The product of two groups, one of which contains a cyclic subgroup of index ≤ 2', *Mat. Zametki* **16** (1974), 285–295.

[18] M. Suzuki, *Group Theory. I* (Springer, Berlin, 1982).

[19] H. Wielandt, 'Über Produkte von nilpotenter Gruppen', *Illinois J. Math.* **2** (1958), 611–618.

[20] H. Wielandt, *Finite Permutation Groups* (Academic Press, New York, 1964).

SHAOFEI DU, Capital Normal University,
School of Mathematical Sciences, Beijing 100048, PR China
e-mail: dushf@mail.cnu.edu.cn

WENJUAN LUO, Capital Normal University,
School of Mathematical Sciences, Beijing 100048, PR China
e-mail: wenjuan2202@163.com

HAO YU, Capital Normal University,
School of Mathematical Sciences, Beijing 100048, PR China
e-mail: 3485676673@qq.com

https://doi.org/10.1017/S1446788724000181 Published online by Cambridge University Press