ON THE SOLVABILITY OF REGULAR SUBGROUPS IN THE HOLOMORPH OF A FINITE SOLVABLE GROUP

CINDY (SIN YI) TSANG AND QIN CHAO

ABSTRACT. In this paper, we shall exhibit an infinite family of non-solvable numbers n for which the holomorph of any solvable group of order n has no insolvable regular subgroup.

CONTENTS

1. INTRODUCTION

Let N be a finite group and write $\mathrm{Perm}(N)$ for its symmetric group. First recall that a subgroup $\mathcal{G}$ of $\mathrm{Perm}(N)$ is said to be *regular* if the map

$$\xi_{\mathcal{G}} : \mathcal{G} \longrightarrow N; \quad \xi_{\mathcal{G}}(\sigma) = \sigma(1_N)$$

is bijective, or equivalently, if the $\mathcal{G}$-action on N is both transitive and free. For example, the images of the left and right regular representations

$$\begin{cases} \lambda : N \longrightarrow \mathrm{Perm}(N); & \lambda(\eta) = (x \mapsto \eta x), \\ \rho : N \longrightarrow \mathrm{Perm}(N); & \rho(\eta) = (x \mapsto x\eta^{-1}), \end{cases}$$

respectively, are both regular subgroups of $\mathrm{Perm}(N)$. Plainly, a regular subgroup of $\mathrm{Perm}(N)$ has the same order as N, but is not necessarily isomorphic to N in general. Given a group G of order $|N|$, define

$$\mathcal{E}'(G, N) = \{\text{regular subgroups of } \mathrm{Hol}(N) \text{ isomorphic to } G\},$$

where $\mathrm{Hol}(N)$ denotes the *holomorph of N* and is given by

$$(1.1) \qquad\qquad \mathrm{Hol}(N) = \rho(N) \rtimes \mathrm{Aut}(N).$$

Let us note that this set is an important object in the studies of Hopf-Galois structures and skew braces; see [4, Chapter 2] and [14], respectively, for more details. The latter in turn are related non-degenerate involutive set-theoretic solutions to the Yang-Baxter equation; see [8].

Observe that $\mathcal{E}'(G, N)$ contains $\lambda(N)$ and $\rho(N)$ when $G \simeq N$. However, in general $\mathcal{E}'(G, N)$ might be empty when $G \not\simeq N$. It is then natural to ask:

Question 1.1. For the set $\mathcal{E}'(G, N)$ to be non-empty, what are some restrictions on G and N in terms of their group-theoretic properties?

This question was studied by N. P. Byott in [3], where he showed that:

Proposition 1.2. *Let G and N be two finite groups of the same order such that the set $\mathcal{E}'(G, N)$ is non-empty.*
(a) If N is nilpotent, then G is solvable.
(b) If G is abelian, then N is solvable.

Proof. See [3, Theorems 1 and 2] and the discussion in [3, Section 2]. $\qquad\square$

In fact, the proof of Proposition 1.2 (b) from [3, Section 6] may be used to show the following stronger result. This was first observed by the first author in [17, Theorem 4.2.4] and we shall reproduce the proof in Section 2 below.

Theorem 1.3. *Let G and N be two finite groups of the same order such that the set $\mathcal{E}'(G, N)$ is non-empty.*
(a) If G is cyclic, then N is supersolvable.
(b) If G is abelian, then N is metabelian.
(c) If G is nilpotent, then N is solvable.

In the proof of [3, Corollary 1.1], N. P. Byott gave examples of solvable G and insolvable N with non-empty $\mathcal{E}'(G, N)$. Also, he noted that in contrast, so far there is no known example of

(1.2)   insolvable G and solvable N with non-empty $\mathcal{E}'(G, N)$.

Results in the literature suggest that in fact no such example exists.

Proposition 1.4. *Let G and N be two finite groups of the same order such that the set $\mathcal{E}'(G, N)$ is non-empty.*
(a) If G is non-abelian simple, then $N \simeq G$.
(b) If G is the double cover of A_m with $m \geq 5$, then $N \simeq G$.
(c) If G is S_m with $m \geq 5$, then N contains an isomorphic copy of A_m.
Here A_m and S_m denote, respectively, the alternating and symmetric groups on m letters.

Proof. See [2, Theorem 1.1] as well as the discussion in [2, Section 2] for (a), [15, Theorem 1.6] for (b), and [16, Theorem 1.3] for (c).   □

It leads us to the following conjecture, which we shall study in this paper.

Conjecture 1.5. *For any $n \in \mathbb{N}$, there are no finite groups G and N both of order n for which (1.2) holds.*

In Section 3, using techniques developed by the first author in [15, Section 4.1], we shall prove some necessary criteria for $\mathcal{E}'(G, N)$ to be non-empty. In Sections 4 and 5, by applying our criteria, we shall show that:

Theorem 1.6. *Conjecture 1.5 holds when n is cube-free.*

Theorem 1.7. *Conjecture 1.5 holds when $n = 2^r \cdot n_0$ with*

$$n_0 = 2^2 \cdot 3 \cdot 5,\ 2^4 \cdot 3^2 \cdot 17,\ \text{or}\ 4^{\ell_0}(4^{\ell_0} + 1)(2^{\ell_0} - 1),$$

where ℓ_0 is any odd prime such that $(4^{\ell_0} + 1)(2^{\ell_0} - 1)$ is square-free and r is any non-negative integer.

In Section 6, we shall also present an algorithm which may be used to show that Conjecture 1.5 holds for any given $n \in \mathbb{N}$, provided that all finite groups of order n have been classified. Using our algorithm, we verified that:

Theorem 1.8. *Conjecture 1.5 holds when* $n \leq 2000$.

A natural number n is called *solvable* if every group of order n is solvable, and is called *non-solvable* otherwise. Conjecture 1.5 is of course trivial when n is a solvable number. The numbers in Theorem 1.7 are non-solvable because

$$|A_5| = 2^2 \cdot 3 \cdot 5 \text{ and } |\mathrm{PSL}_2(17)| = 2^4 \cdot 3^2 \cdot 17,$$

as well as

$$(1.3) \qquad |\mathrm{Sz}(2^{2m+1})| = 4^{2m+1}(4^{2m+1} + 1)(2^{2m+1} - 1) \text{ for all } m \in \mathbb{N},$$

where $\mathrm{Sz}(-)$ denotes the Suzuki groups. Let us also remark that

$$60, 120, 168, 180, 240, 300, 336, 360, 420, 480, 504, 540, 600, 660, 672, 720, 780,$$
$$840, 900, 960, 1008, 1020, 1080, 1092, 1140, 1176, 1200, 1260, 1320, 1344, 1380,$$
$$1440, 1500, 1512, 1560, 1620, 1680, 1740, 1800, 1848, 1860, 1920, 1980$$

is a complete list of the non-solvable numbers $n \leq 2000$; see [13, A056866].

2. Proof of Theorem 1.3

Let N be a finite group and let $\mathcal{G}$ be any regular subgroup of $\mathrm{Hol}(N)$. Let

$$\mathrm{proj}_\rho : \mathrm{Hol}(N) \longrightarrow \rho(N) \text{ and } \mathrm{proj}_{\mathrm{Aut}} : \mathrm{Hol}(N) \longrightarrow \mathrm{Aut}(N),$$

respectively, denote the projection map and homomorphism afforded by (1.1). Since $\mathcal{G}$ is regular, we easily verify that $(\mathrm{proj}_\rho)|_\mathcal{G}$ is bijective and that

$$\rho(N) \rtimes \mathrm{proj}_{\mathrm{Aut}}(\mathcal{G}) = \mathcal{G} \cdot \mathrm{proj}_{\mathrm{Aut}}(\mathcal{G}).$$

Theorem 1.3 then follows directly from Lemmas 2.1 and 2.2 below.

Lemma 2.1. *Let* Γ *be a finite group which is a product of two subgroups* Δ_1 *and* Δ_2, *namely, elements of* Γ *are of the shape* $\delta_1\delta_2$ *with* $\delta_1 \in \Delta_1, \delta_2 \in \Delta_2$.
(a) If Δ_1 *and* Δ_2 *are cyclic, then* Γ *is supersolvable.*
(b) If Δ_1 *and* Δ_2 *are abelian, then* Γ *is metabelian.*
(c) If Δ_1 *and* Δ_2 *are nilpotent, then* Γ *is solvable.*

Proof. This is known, by [5], [10], and [11], respectively. □

Lemma 2.2. *The properties "cyclic", "abelian", "nilpotent", "supersolvable", "metabelian", "solvable" are all quotient-closed and subgroup-closed.*

Proof. This is well-known and is easily verified. $\square$

3. Criteria for non-emptiness

Throughout this section, assume that G and N are two finite groups of the same order such that the set $\mathcal{E}'(G, N)$ is non-empty. Then, as noticed in [15, Proposition 2.1], for example, by (1.1) this implies that there exist

$$\mathfrak{f} \in \mathrm{Hom}(G, \mathrm{Aut}(N)) \text{ and a bijective } \mathfrak{g} \in \mathrm{Map}(G, N)$$

satisfying the relation

(3.1) $$\mathfrak{g}(\sigma\tau) = \mathfrak{g}(\sigma) \cdot \mathfrak{f}(\sigma)(\mathfrak{g}(\tau)) \text{ for all } \sigma, \tau \in G.$$

Below, we shall use (3.1) to prove two necessary criteria relating G and N, both of which are very simple. Yet, the criterion in Proposition 3.3 seems to be fairly powerful, and it alone allows us to prove Theorems 1.6 and 1.7. Let us also recall the following useful fact.

Lemma 3.1. *Let Γ be a group containing a normal subgroup Δ. Then, the group Γ is solvable if and only if both Δ and Γ/Δ are solvable.*

Proof. This is well-known and is easily verified. $\square$

To state the first criteria, let $\mathrm{Inn}(N)$ and $\mathrm{Out}(N)$, respectively, denote the inner and outer automorphism groups of N. Write $\pi : \mathrm{Aut}(N) \longrightarrow \mathrm{Out}(N)$ for the natural quotient map with kernel equal to $\mathrm{Inn}(N)$. Then, we have:

Proposition 3.2. *If G is insolvable and N is solvable, then $(\pi \circ \mathfrak{f})(G)$ is an insolvable subgroup of $\mathrm{Out}(N)$.*

Proof. Observe that $\mathfrak{f}$ induces an embedding

$$\ker(\pi \circ \mathfrak{f})/\ker(\mathfrak{f}) \longrightarrow \mathrm{Inn}(N)$$

and that $\mathfrak{g}$ restricts to a homomorphism $\ker(\mathfrak{f}) \longrightarrow N$ by (3.1). Hence, if N is solvable, then both $\ker(\mathfrak{f})$ and $\mathrm{Inn}(N)$ are solvable by Lemma 2.2, and so

$\ker(\pi \circ \mathfrak{f})$ is solvable by Lemma 3.1. If G is insolvable in addition, then since

$$G/\ker(\pi \circ \mathfrak{f}) \simeq (\pi \circ \mathfrak{f})(G),$$

we see that $(\pi \circ \mathfrak{f})(G)$ is insolvable, again by Lemma 3.1. $\square$

To state the second criteria, recall that a subgroup M of N is called *characteristic* if $\varphi(M) = M$ for all $\varphi \in \mathrm{Aut}(N)$. In this case, plainly M is normal in N, and we shall write

$$\theta_M : \mathrm{Aut}(N) \longrightarrow \mathrm{Aut}(N/M); \quad \theta_M(\varphi) = (\eta M \mapsto \varphi(\eta)M)$$

for the natural homomorphism. The use of characteristic subgroups of N is motivated by the arguments in [2]; also see [15, Section 4.1]. Our main tool is the following proposition; also see Proposition 6.1 in Section 6.

Proposition 3.3. *Let M be any characteristic subgroup of N and define*

$$H = \mathfrak{g}^{-1}(M).$$

Then, this set H is a subgroup of G, and $\mathcal{E}'(H, M)$ is non-empty. Moreover, if N/M is solvable and $\ker(\theta_M \circ \mathfrak{f})$ is insolvable, then H is insolvable.

Proof. The set H is a subgroup of G by (3.1); see [15, Lemma 4.1]. Also, we have a homomorphism

$$\mathrm{res}(\mathfrak{f}) : H \longrightarrow \mathrm{Aut}(M); \quad \mathrm{res}(\mathfrak{f})(\sigma) = \mathfrak{f}(\sigma)|_M$$

induced by $\mathfrak{f}$ since M is characteristic, as well as a bijective map

$$\mathrm{res}(\mathfrak{g}) : H \longrightarrow M; \quad \mathrm{res}(\mathfrak{g})(\sigma) = \mathfrak{g}(\sigma)$$

induced by $\mathfrak{g}$ since $\mathfrak{g}$ is bijective. Clearly, it follows directly from (3.1) that

$$\mathrm{res}(\mathfrak{g})(\sigma\tau) = \mathrm{res}(\mathfrak{g})(\sigma) \cdot (\mathrm{res}(\mathfrak{f})(\sigma))(\mathrm{res}(\mathfrak{g})(\tau)) \text{ for all } \sigma, \tau \in H.$$

Then, by [15, Proposition 2.1], which is a consequence of (1.1), this implies that $\mathcal{E}'(H, M)$ is non-empty. This proves the first statement.

Next, as noted in [15, Lemma 4.1], the relation (3.1) implies that

$$\ker(\theta_M \circ \mathfrak{f}) \longrightarrow N/M; \quad \sigma \mapsto \mathfrak{g}(\sigma)M$$

induced by $\mathfrak{g}$ is a homomorphism, and so we have an embedding

$$\frac{\ker(\theta_M \circ \mathfrak{f})}{\ker(\theta_M \circ \mathfrak{f}) \cap H} \longrightarrow N/M.$$

Thus, if N/M is solvable and $\ker(\theta_M \circ \mathfrak{f})$ is insolvable, then $\ker(\theta_M \circ \mathfrak{f}) \cap H$ must be insolvable by Lemma 3.1, which in turn implies that H is insolvable by Lemma 2.2. The second statement then follows. □

Although Proposition 3.3 is valid for any characteristic subgroup M of N, motivated by [2], we shall consider the case when M is a proper and maximal characteristic subgroup of N. In this case, the quotient N/M is a non-trivial characteristically simple group, and so we know that

$$N/M \simeq T^m, \text{ where } T \text{ is a simple group and } m \in \mathbb{N}.$$

Hence, if N is solvable, then there exists a prime p such that

$$(3.2) \qquad N/M \simeq (\mathbb{Z}/p\mathbb{Z})^m \text{ and in particular } \mathrm{Aut}(N/M) \simeq \mathrm{GL}_m(p).$$

Let us observe that:

Lemma 3.4. *Given a prime p and $m \in \mathbb{N}$, the group $\mathrm{GL}_m(p)$ is solvable if and only if $m = 1$ or $m = 2$ with $p \leq 3$.*

Proof. We know that $\mathrm{PSL}_m(p)$ is non-abelian simple if $m \geq 3$ or $m = 2$ with $p \geq 5$. Since $\mathrm{PSL}_m(p)$ is a quotient of $\mathrm{SL}_m(p)$, the forward implication then follows from Lemma 2.2. The backward implication is clear. □

4. PROOF OF THEOREM 1.6

Suppose for contradiction that the claim is false and let n be the smallest cube-free number for which Conjecture 1.5 fails. Let G and N be two groups of order n satisfying (1.2). Let M be any proper and maximal characteristic subgroup of N. Clearly M is solvable because N is solvable. As in (3.2), we then know that

$$N/M \simeq (\mathbb{Z}/p\mathbb{Z})^m, \text{ where } p \text{ is a prime and } m \in \mathbb{N}.$$

Notice that $|M| = n/p^m$ and that $m = 1, 2$ because n is cube-free. Hence, by Lemma 4.1 (b) below, the kernel of any homomorphism $G \longrightarrow \mathrm{Aut}(N/M)$ is

insolvable. From Proposition 3.3, it follows that $\mathcal{E}'(H, M)$ is non-empty for some insolvable subgroup H of G of the same order as M. This contradicts the minimality of n and so Theorem 1.6 must be true.

Lemma 4.1. *Let p be any prime and let $m = 1, 2$.*

(a) The group $\mathrm{GL}_m(p)$ has no non-abelian simple subgroup.

(b) The kernel of a homomorphism from a finite insolvable group of cube-free order to $\mathrm{GL}_m(p)$ is insolvable.

Proof. For $m = 1$ or $p = 2$, the group $\mathrm{GL}_m(p)$ is solvable by Lemma 3.4, and the claims hold by Lemmas 2.2 and 3.1. For $m = 2$ and p odd, first suppose for contradiction that $\mathrm{GL}_2(p)$ has a subgroup A which is non-abelian simple. Observe that the homomorphism

$$A \xrightarrow{\text{inclusion}} \mathrm{GL}_2(p) \xrightarrow{\text{determinant}} (\mathbb{Z}/p\mathbb{Z})^\times$$

must be trivial and so A is in fact a subgroup of $\mathrm{SL}_2(p)$. Also, note that A has an element of order two by the Feit-Thompson theorem. Since p is odd, the matrix $\left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix} \right)$, which belongs to the center, is the only element in $\mathrm{SL}_2(p)$ of order two. It then follows that A has non-trivial center, which is impossible, and this proves part (a). Since any finite insolvable group of cube-free order has a non-abelian simple subgroup by [6], we see that part (b) follows from part (a) as well as Lemma 3.1. □

5. Almost square-free orders

In this section, we shall prove Theorem 1.7. First, let us prove the following more general and stronger statement.

Theorem 5.1. *Suppose that $n_0 = 2^{r_0} \cdot 3^{\epsilon_0} \cdot p_1 \cdots p_{k_0}$, where*

$$r_0, k_0 \in \mathbb{N}, \ \epsilon_0 \in \{0, 1, 2\}, \ \text{and} \ p_1, \ldots, p_{k_0} \geq 5 \ \text{are distinct primes,}$$

and that Conjecture 1.5 holds when $n = n_0$. If all of the conditions

(1) the subgroups of index a power of two of an insolvable group of order n_0 are all insolvable;

(2) there is no non-abelian simple group of order $2^r \cdot n_0$ for $r \in \mathbb{N}$;

(3) *the numbers $(2^r \cdot n_0)/p$, where p ranges over the odd primes dividing n_0,*
   are all solvable for $r \in \mathbb{N} \cup \{0\}$;

are satisfied, then Conjecture 1.5 also holds when $n = 2^r \cdot n_0$ for any $r \in \mathbb{N}$.

Proof. Suppose for contradiction that conditions (1),(2),(3) are satisfied but the conclusion is false. Let $r \in \mathbb{N}$ be the smallest number such that Conjecture 1.5 fails to hold when $n = 2^r \cdot n_0$ as well as let G and N be two groups of order n satisfying (1.2). Let M be any proper and maximal characteristic subgroup of N. Clearly M is solvable because N is solvable. As in (3.2), we then know that

$$N/M \simeq (\mathbb{Z}/p\mathbb{Z})^m, \text{ where } p \text{ is a prime and } m \in \mathbb{N}.$$

Notice that $|M| = n/p^m$. Also, we know from Proposition 3.3 that $\mathcal{E}'(H, M)$ is non-empty for some subgroup H of G of the same order as M. For p odd, the group $\mathrm{GL}_m(p)$ is solvable by Lemma 3.4 and the assumption on n_0. The kernel of any homomorphism $G \longrightarrow \mathrm{Aut}(N/M)$ must then be insolvable by Lemma 3.1. Thus, we may take H to be insolvable by Proposition 3.3, which contradicts condition (3). For $p = 2$, we have $|H| = 2^{r-m} \cdot n_0$, and hence H is insolvable by Lemma 5.2 below. Since Conjecture 1.5 holds when $n = n_0$, we must have $r - m \geq 1$, but this contradicts the minimality of r. We now deduce that the theorem is true. $\qquad \square$

Lemma 5.2. *For any $n_0 \in \mathbb{N}$, under conditions (1),(2),(3) in Theorem 5.1, the subgroups of index a power of two of an insolvable group of order $2^r \cdot n_0$ are all insolvable for any $r \in \mathbb{N} \cup \{0\}$.*

Proof. We shall use induction on r and notice that the case $r = 0$ is simply condition (1). Next, suppose that $r \geq 1$ and let G be an insolvable group of order $2^r \cdot n_0$. By condition (2), we know that G is non-simple. Let A be any non-trivial and proper normal subgroup of G. Note that either A or G/A is insolvable by Lemma 3.1. By condition (3), this implies that

$$2^a \cdot n_0 = \begin{cases} |A| & \text{if } A \text{ is insolvable,} \\ |G/A| & \text{if } G/A \text{ is insolvable,} \end{cases}$$

where $0 \leq a \leq r - 1$. Now, let H be any subgroup of G of index a power of two. Observe that $AH/A \simeq H/A \cap H$, as well as that

$$[A : A \cap H] = [G : H]/[G : AH],$$

$$[G/A : AH/A] = [G : H]/[A : A \cap H],$$

both of which are powers of two. Hence, by the induction hypothesis, we see that either $A \cap H$ or $H/A \cap H$ is insolvable. It then follows from Lemma 2.2 that H is insolvable, as desired. $\qquad\square$

We shall apply Theorem 5.1 to prove Theorem 1.7. To that end, we shall first show that the numbers n_0 in the statement of Theorem 1.7 satisfy conditions (1),(2),(3) in Theorem 5.1.

Lemma 5.3. *The following statements are true.*

(a) A non-solvable number is a multiple of the order of a non-abelian simple group.

(b) A non-solvable number is divisible by at least three distinct primes.

(c) A finite non-abelian simple group whose order is not divisible by three is a Suzuki group.

Proof. Part (a) is clear. Part (b) is Burnside's theorem while part (c) follows from the classification of finite simple groups. $\qquad\square$

Lemma 5.4. *Let $n_0 = 2^{r_0} \cdot 3^{\epsilon_0} \cdot p$, where $r_0 \in \mathbb{N}$, $\epsilon_0 \in \{1, 2\}$, and $p \geq 5$ is a prime. If there exists a non-abelian simple group Γ of order n_0, then*

$$(5.1) \qquad n_0 \in \{2^2 \cdot 3 \cdot 5,\ 2^3 \cdot 3 \cdot 7,\ 2^3 \cdot 3^2 \cdot 7,\ 2^4 \cdot 3^2 \cdot 17,\ 2^3 \cdot 3^2 \cdot 5\}$$

with

$$\Gamma \simeq \begin{cases} A_5 & \text{for } n_0 = 2^2 \cdot 3 \cdot 5, \\ \mathrm{PSL}_2(7) & \text{for } n_0 = 2^3 \cdot 3 \cdot 7, \\ \mathrm{PSL}_2(8) & \text{for } n_0 = 2^3 \cdot 3^2 \cdot 7, \\ \mathrm{PSL}_2(17) & \text{for } n_0 = 2^4 \cdot 3^2 \cdot 17, \\ A_6 & \text{for } n_0 = 2^3 \cdot 3^2 \cdot 5. \end{cases}$$

In particular, condition (2) in Theorem 5.1 is satisfied for n_0 in (5.1).

Proof. Notice that the Sylow p-subgroups of any group of order n_0 are cyclic. If $p > 3^{\epsilon_0}$, then the claim follows from [9, Theorem 1]. If not, then $p = 5, 7$, and the claim follows from [1] and [18], respectively. $\qquad\square$

Lemma 5.5. *Let $n_0 = 2^2 \cdot 3 \cdot 5$ or $2^4 \cdot 3^2 \cdot 17$. Then, up to isomorphism A_5 or $\mathrm{PSL}_2(17)$, respectively, is the only insolvable group of order n_0. Moreover, conditions (1),(3) in Theorem 5.1 are satisfied.*

Proof. From Lemmas 5.3 (a),(b) and 5.4, it is easy to deduce the first claim and that condition (3) holds. Condition (1) may then be verified directly. $\quad\square$

Note that $n_0 = 2^3 \cdot 3 \cdot 7$ fails condition (1) while $n_0 = 2^3 \cdot 3^2 \cdot 7$ and $2^3 \cdot 3^2 \cdot 5$ fail condition (3) in Theorem 5.1.

Lemma 5.6. *Let $n_0 = 2^{r_0}(4^{2m_0+1}+1)(2^{2m_0+1}-1)$, where $r_0, m_0 \in \mathbb{N}$. If there exists a non-abelian simple group Γ of order n_0, then*

$$r_0 = 2(2m_0 + 1) \ \text{ with } \ \Gamma \simeq \mathrm{Sz}(2^{2m_0+1}).$$

In particular, condition (2) in Theorem 5.1 is satisfied for $r_0 = 2(2m_0 + 1)$.

Proof. This is clear from Lemma 5.3 (c) and (1.3). $\qquad\qquad\square$

Lemma 5.7. *Let $n_0 = 4^{\ell_0}(4^{\ell_0}+1)(2^{\ell_0}-1)$, where ℓ_0 is an odd prime. Then, up to isomorphism $\mathrm{Sz}(2^{\ell_0})$ is the only insolvable group of order n_0. Moreover, conditions (1),(3) in Theorem 5.1 are satisfied.*

Proof. Suppose for contradiction that there is an insolvable group of order n_0 which is not isomorphic to $\mathrm{Sz}(2^{\ell_0})$, and thus cannot be non-abelian simple by Lemma 5.6. Then, from Lemma 5.3 (a),(c) and (1.3), we deduce that

$$4^{\ell_0}(4^{\ell_0} + 1)(2^{\ell_0} - 1) = n_0 = d \cdot 4^k(4^k + 1)(2^k - 1),$$

where $d, k \in \mathbb{N}$ with $d \geq 2$ and $k \geq 3$ odd. Plainly $\ell_0 > k$, and because ℓ_0 is prime, we deduce that

$$\gcd(2^k - 1, 2^{\ell_0} - 1) = 2^{\gcd(k,\ell_0)} - 1 = 1.$$

This means that $2^k - 1$ divides $4^{\ell_0} + 1$. Note that then $k \leq 2\ell_0$. But

$$(2^k - 1) + (2^{2\ell_0 - tk} + 1) = 2^k(2^{2\ell_0 - (t+1)k} + 1) \text{ for all } t \in \mathbb{N} \cup \{0\}.$$

By induction, this implies that $2^k - 1$ divides $2^s + 1$ for some $0 \leq s \leq k - 1$, which is impossible because $k \geq 3$. This proves the first claim.

Now, the subgroups of $\mathrm{Sz}(2^{\ell_0})$ are known; see [19, Theorem 4.2], for example. None of them has index a non-trivial power of two and so condition (1) is satisfied. To prove condition (3), suppose for contradiction that $(2^r \cdot n_0)/p$ is insolvable for some odd prime p divisor of n_0 and $r \in \mathbb{N} \cup \{0\}$. Again, by Lemma 5.3 (a),(c) and (1.3), we have

$$2^r \cdot 4^{\ell_0}(4^{\ell_0} + 1)(2^{\ell_0} - 1) = d \cdot p \cdot 4^k(4^k + 1)(2^k - 1),$$

where $d, k \in \mathbb{N}$ with $k \geq 3$ odd. A comparison of the odd parts of the above expressions tells us that $\ell_0 > k$. Using the same argument as above, we then obtain a contradiction, and this completes the proof. $\qquad\square$

5.1. **Proof of Theorem 1.7.** Let n_0 be as in the statement of the theorem. By Lemmas 5.4, 5.5, 5.6, and 5.7, conditions (1),(2),(3) in Theorem 5.1 are satisfied. Also, up to isomorphism there is only one insolvable group of order n_0 and it is non-abelian simple. It then follows from Proposition 1.4 (a) that Conjecture 1.5 holds when $n = n_0$. We now deduce directly from Theorem 5.1 that Conjecture 1.5 also holds when $n = 2^r \cdot n_0$ for any $n \in \mathbb{N}$.

6. Algorithm to test the conjecture

In this section, we shall describe an algorithm which may be used to prove Conjecture 1.5 for a given n, as long as all finite groups of order n are known. Then, we shall apply our algorithm to prove Theorem 1.8.

Recall that given any finite group Γ, the *Fitting subgroup* of Γ, denoted by $\mathrm{Fit}(\Gamma)$, is the unique largest normal nilpotent subgroup of Γ. Plainly $\mathrm{Fit}(\Gamma)$ is a characteristic subgroup of Γ.

Proposition 6.1. *Let G and N be two finite groups of the same order such that the set $\mathcal{E}'(G, N)$ is non-empty. Put*

$$\mathcal{M}(N) = \{|M| : M \text{ is a characteristic subgroup of } N\},$$
$$\mathcal{H}(G) = \{|H| : H \text{ is a subgroup of } G\}.$$

Then, we have $\mathcal{M}(N) \subset \mathcal{H}(G)$. *Also, there is a solvable subgroup of* G *whose order is the same as* $\mathrm{Fit}(N)$.

Proof. This follows directly from Propositions 1.2 (a) and 3.3. □

While Proposition 6.1 gives us a way to test whether a pair (G, N) satisfies condition (1.2), applying it directly to prove Conjecture 1.5 has two issues:

- In general, there are many groups of a given order n, and it is inefficient to test whether (1.2) holds for each pair (G, N) of groups of order n.
- It is time-consuming to compute characteristic subgroups.

To overcome these difficulties, our idea is to let G vary, and check that

$$(6.1) \qquad \mathcal{E}'(G, N) \neq \emptyset \text{ for some insolvable group } G \text{ of order } |N|$$

cannot hold for each fixed N separately. Also, we shall apply the test involving the Fitting subgroup first because it is the least time-consuming.

Given any $n \in \mathbb{N}$, let us define $\mathcal{N}_0(n)$ to be the set of all solvable groups of order n. Our idea is to remove the groups $N \in \mathcal{N}_0(n)$ for which (6.1) cannot be satisfied, until the set gets empty, which would mean that Conjecture 1.5 holds for n.

Algorithm 6.2. Let $n \in \mathbb{N}$ be any non-solvable number.

a. Compute the set $\mathcal{L}_1(n)$ of the orders of the solvable subgroups of G with G ranges over all insolvable groups of order n. Then, define $\mathcal{N}_1(n)$ to be the set of $N \in \mathcal{N}_0(n)$ such that $|\mathrm{Fit}(N)| \in \mathcal{L}_1(n)$.
   – Condition (6.1) cannot hold for $N \in \mathcal{N}_0(n) \setminus \mathcal{N}_1(n)$ by Proposition 6.1.
b. Define $\mathcal{N}_2(n)$ to be the set of $N \in \mathcal{N}_1(n)$ such that $\mathrm{Aut}(N)$ is insolvable.
   – Condition (6.1) plainly cannot hold for $N \in \mathcal{N}_0(n) \setminus \mathcal{N}_2(n)$ by (1.1).

Thus, if $\mathcal{N}_2(n) = \emptyset$, then Conjecture 1.5 holds for n.

In the case that $\mathcal{N}_2(n)$ is non-empty, there are three further tests which we can try, as stated below. Note that two of them involve only N but not G.

Algorithm 6.3. Let $n \in \mathbb{N}$ be any non-solvable number.

1. Define $N_{31}(n)$ to be the set of $N \in \mathcal{N}_2(n)$ such that $n/2 \notin \mathcal{M}(N)$.
   Note that a subgroup of index two (if exists) of an insolvable group must

be insolvable by Lemma 3.1. By induction, we then deduce that:
   – Condition 6.1 cannot hold for $N \in \mathcal{N}_0(n) \setminus \mathcal{N}_{31}(n)$ by Proposition 3.3,
   provided that Conjecture 1.5 holds for $n/2$.
2. Compute the set $\mathcal{L}_2(n)$ of the orders of all subgroups of G with G ranges
   over all insolvable groups of order n. Then, define $\mathcal{N}_{32}(n)$ to be the set of
   $N \in \mathcal{N}_2(n)$ such that $\mathcal{M}(N) \subset \mathcal{L}_2(n)$.
   – Condition 6.1 cannot hold for $N \in \mathcal{N}_0(n) \setminus \mathcal{N}_{32}(n)$ by Proposition 6.1.
3. Define $\mathcal{N}_{33}(n)$ to be the set of $N \in \mathcal{N}_2(n)$ such that the greatest common
   divisor of n and $|\mathrm{Out}(N)|$ is a non-solvable number.
   – Condition 6.1 cannot hold for $N \in \mathcal{N}_0(n) \setminus \mathcal{N}_{33}(n)$ by Proposition 3.2.

Thus, if $\mathcal{N}_{32}(n) \cap \mathcal{N}_{33}(n) = \emptyset$, or if $\mathcal{N}_{31}(n) \cap \mathcal{N}_{32}(n) \cap \mathcal{N}_{33}(n) = \emptyset$ and Conjecture 1.5 holds for $n/2$, then Conjecture 1.5 holds for n.

In the appendix, we have included both the MAGMA [12] and GAP [7] codes implementing Algorithm 6.2 and the first two parts of Algorithm 6.3. In the table below, we give their runtimes when we apply them to the non-solvable numbers n for which a library of all groups of order n is available.

In the appendix, we have also included a code which uses the RegularSubgroups command in MAGMA to test Conjecture 1.5 directly. To illustrate the efficiency of our algorithms, let us note that this code takes 231 min 11 sec to run just for the non-solvable numbers up to 1000 (excluding $480, 672, 960$).

The calculations were done on an Intel Xeon CPU E5-1620 vs3 @ 3.5GHz machine with 16GB of RAM under Ubuntu 16.04LTS.

n	MAGMA	GAP
the single non-solvable number 1920	19 min 46 sec	not enough memory
all non-solvable numbers ≤ 2000 except 1920	1 min 50 sec	17 min 48 sec
all cube-free numbers ≤ 50000	library unavailable	287 min 12 sec

TABLE 1. Runtimes for Algorithm 6.2 and the first two parts of Algorithm 6.3

6.1. **Proof of Theorem 1.8.** We ran Algorithm 6.2 to get that among the non-solvable numbers $n \leq 2000$, the set $\mathcal{N}_2(n)$ is empty except for

$$480, 600, 960, 1008, 1200, 1320, 1344, 1440, 1512, 1680, 1800, 1920.$$

We then ran Algorithm 6.3 to get that among the numbers in the above list, the intersection $\mathcal{N}_{31}(n) \cap \mathcal{N}_{32}(n)$ is empty except for 1008 and 1512. In fact, for these two values of n, we have

$$\mathcal{N}_2(1008) = \mathcal{N}_{31}(n) \cap \mathcal{N}_{32}(1008) = \{\text{SmallGroup}(1008, 910)\},$$

$$\mathcal{N}_2(1512) = \mathcal{N}_{31}(n) \cap \mathcal{N}_{32}(1512) = \{\text{SmallGroup}(1512, 841)\}.$$

By using the OuterOrder command in MAGMA, we computed that $\mathcal{N}_{33}(1008)$ and $\mathcal{N}_{33}(1512)$ are both empty. Thus, we conclude that Conjecture 1.5 holds when $n \leq 2000$. Let us remark that the cases $n = 60, 120, 240, 480, 960, 1920$ also follow from Theorem 1.6.

7. ACKNOWLEDGMENTS

REFERENCES

[1] R. Brauer, *On simple groups of order* $5 \cdot 3^a \cdot 2^b$, Bull. Amer. Math. Soc. 74 (1968), 900–903.

[2] N. P. Byott, *Hopf-Galois structures on field extensions with simple Galois groups*, Bull. London Math. Soc. 36 (2004), no. 1, 23–29.

[3] N. P. Byott, *Solubility criteria for Hopf-Galois structures*, New York J. Math. 21 (2015), 883–903.

[4] L. N. Childs, *Taming wild extensions: Hopf algebras and local Galois module theory*. Mathematical Surveys and Monographs, 80. American Mathematical Society, Providence, RI, 2000.

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

[6] H. Dietrich and B. Eick, *On the groups of cube-free order*, J. Algebra 292 (2005), no. 1, 122–137. Addendum, *ibid*, 367 (2012), 247–248.

[7] The GAP Group, GAP – Groups, Algorithms, and Programming, Version 4.10.0; 2018.

[8] L. Guarnieri and L. Vendramin, *Skew braces and the Yang-Baxter equation*, Math. Comp. 86 (2017), no. 307, 2519–2534.

[9] M. Herzog, *On finite simple groups of order divisible by three primes only*, J. Algebra 10 (1968), 383–388.

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

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

[12] W. Bosma, J. Cannon, and C. Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput., 24 (1997), 23–265.

[13] OEIS Foundation Inc., The On-Line Encyclopedia of Integer Sequences, `http://oeis.org`.

[14] A. Smoktunowicz and L. Vendramin, *On skew braces* (with an appendix by N. Byott and L. Vendramin), J. Comb. Algebra 2 (2018), no. 1, 47–86.

[15] C. Tsang, *Non-existence of Hopf-Galois structures and bijective crossed homomorphisms*, J. Pure Appl. Algebra 223 (2019), no. 7, 2804–2821.

[16] C. Tsang, *Hopf-Galois structures on a Galois S_n-extension*, preprint. arXiv:1812.06419.

[17] C. Tsang, *Galois module structures and Hopf-Galois structures on extensions of number fields*, Postdoctoral report, Tsinghua University, 2018.

[18] D. Wales, *Simple groups of order $7 \cdot 3^a \cdot 2^b$*, J. Algebra 16 (1970), 575–596.

[19] R. A. Wilson, *The finite simple groups.* Graduate Texts in Mathematics, 251. Springer-Verlag London, Ltd., London, 2009.

School of Mathematics, Sun Yat-Sen University, Zhuhai, China
E-mail address: `zengshy26@mail.sysu.edu.cn`
URL: `http://sites.google.com/site/cindysinyitsang/`

Department of Mathematics, University of Waikato, New Zealand
E-mail address: `cq22@students.waikato.ac.nz`

MAGMA code for Algorithm 6.2 and the first two parts of Algorithm 6.3:

```
TestOrders:=[*any list of non-solvable numbers n which we wish to test*];
for n in TestOrders do
//Compute LL1 and LL2.
GG:=SmallGroups(n,func<x|not IsSolvable(x)>);
L1:=[];
L2:=[];
for G in GG do
Sub:=Subgroups(G);
  for H in Sub do
  order:=H'order;
    if IsSolvable(H'subgroup) then
    Append(~L1,order);
    end if;
    Append(~L2,order);
  end for;
end for;
LL1:=Set(L1);
LL2:=Set(L2);
//Compute NN1, NN2, NN31, NN32.
```

```
NN0:=[i:i in [1..#SmallGroups(n:Warning:=false)]|IsSolvable(SmallGroup(n,i))];
NN1:=[];
NN2:=[];
NN31:=[];
NN32:=[];
for i in NN0 do
N:=SmallGroup(n,i);
Fit:=FittingSubgroup(N);
//Determine whether N is in NN1.
  if Order(Fit) in LL1 then
  Append(~NN1,i);
  end if;
if i in NN1 then
Aut:=AutomorphismGroup(N);
//Determine whether N is in NN2.
  if not IsSolvable(Aut) then
  Append(~NN2,i);
  end if;
if i in NN2 then
Out:=[a:a in Generators(Aut)|not IsInner(a)];
NorSub:=NormalSubgroups(N);
```

```
CharSub:=[x:x in NorSub|forall{a:a in Out|a(x'subgroup) eq x'subgroup}];
MM:={M'order:M in CharSub};
//Determine whether N is in NN31.
  if n/2 notin MM then
  Append(~NN31,i);
  end if;
//Determine whether N is in NN32.
  if MM subset LL2 then
  Append(~NN32,i);
  end if;
end if;
end if;
end for;
//If NN2 is empty, then Conjecture 1.5 holds for n.
//If NN31 ∩ NN32 is empty, then Conjecture 1.5 holds for n as long as it holds for n/2.
//If NN31 ∩ NN32 is non-empty, then further test is required.
if IsEmpty(NN2) then
printf "Conjecture 1.5 holds for %o\n",n;
else
  if IsEmpty(NN32) then
  printf "Conjecture 1.5 holds for %o\n",n;
```

```
  else
    Inter:=Set(NN31) meet Set(NN32);
    if IsEmpty(Inter) then
    printf "Conjecture 1.5 holds for %o if it holds for %o\n",n,n/2;
    else
    print n,Inter;
    end if;
  end if;
end if;
end for;
```

GAP code for Algorithm 6.2 and the first two parts of Algorithm 6.3:

```
TestOrders:=[*any list of non-solvable numbers n which we wish to test*];;
for n in TestOrders do
GG:=Filtered(AllSmallGroups(n),G->not IsSolvable(G));
#Compute LL1 and LL2.
L1:=[];
L2:=[];
for G in GG do
Sub:=List(ConjugacyClassesSubgroups(G),Representative);
  for H in Sub do
```

```
    order:=Order(H);
      if IsSolvable(H) then
      Add(L1,order);
      fi;
      Add(L2,order);
    od;
od;
LL1:=Set(L1);
LL2:=Set(L2);
#Compute NN1, NN2, NN31, NN32.
NN0:=Filtered([1..Size(AllSmallGroups(n))],i->IsSolvable(SmallGroup(n,i)));
NN1:=[];
NN2:=[];
NN31:=[];
NN32:=[];
for i in NN0 do
N:=SmallGroup(n,i);
Fit:=FittingSubgroup(N);
#Determine whether N is in NN1.
  if Order(Fit) in LL1 then
  Add(NN1,i);
```

```
  fi;
if i in NN1 then
Aut:=AutomorphismGroup(N);
#Determine whether N is in NN2.
  if not IsSolvable(Aut) then
  Add(NN2,i);
  fi;
if i in NN2 then
CharSub:=CharacteristicSubgroups(N);
MM:=Set(CharSub,Order);
#Determine whether N is in NN31.
  if not n/2 in MM then
  Add(NN31,i);
  fi;
#Determine whether N is in NN32.
  if IsSubset(LL2,MM) then
  Add(NN32,i);
  fi;
fi;
fi;
od;
```

```
#If NN2 is empty, then Conjecture 1.5 holds for n.
#If NN31 ∩ NN32 is empty, then Conjecture 1.5 holds for n as long as it holds for n/2.
#If NN31 ∩ NN32 is non-empty, then further test is required.
if IsEmpty(NN2) then
Print("Conjecture 1.5 holds for ",n,"\n");
else
  if IsEmpty(NN32) then
  Print ("Conjecture 1.5 holds for ",n,"\n");
  else
    Inter:= Intersection(NN31,NN32);
    if IsEmpty(Inter) then
    Print("Conjecture 1.5 holds for ",n," if it holds for ",n/2,"\n");
    else
    Print(n,Inter,"\n");
    fi;
  fi;
fi;
od;
```

MAGMA code to test Conjecture 1.5 directly:

```
TestOrders:=[*any list of non-solvable numbers n which we wish to test*];
for n in TestOrders do
```

```
NN0:=[i:i in [1..#SmallGroups(n:Warning:=false)]|IsSolvable(SmallGroup(n,i))];
NNOO:=[];
for i in NN0 do
N:=SmallGroup(n,i);
Hol:=Holomorph(N);
RegSub:=RegularSubgroups(Hol);
InsolRegSub:=[R:R in RegSub| not IsSolvable(R'subgroup)];
   if not IsEmpty(InsolRegSub) then
   Append(~NN0,i);
   end if;
end for;
//NNOO is empty if and only if Conjecture 1.5 holds for n.
print n,NNOO;
end for;
```