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

CINDY (SIN YI) TSANG AND CHAO QIN

ABSTRACT. We exhibit infinitely many natural numbers n for which there exists at least one insolvable group of order n, and yet the holomorph of any solvable group of order n has no insolvable regular subgroup. We also solve Problem 19.90 (d) in the Kourovka notebook.

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

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

This set $\mathcal{E}'(G, N)$ is an important object in the studies of Hopf-Galois structures and skew braces; see [5, Chapter 2] and [19], respectively. In particular, there is a connection between elements of $\mathcal{E}'(G, N)$ and

1. Hopf-Galois structures of type N on a Galois extension with group G;
2. skew braces with additive group N and multiplicative group G.

Let us remark that skew braces in turn are closely related to non-degenerate set-theoretic solutions to the Yang-Baxter equation; see [10].

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 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 [4], 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 [4, Theorems 1 and 2]. □

In fact, the proof of Proposition 1.2 (b) from [4, Section 6] may be used to show the following stronger result. This was observed by the first author in [24, Theorem 4.2.4], which is unpublished, and we shall reproduce the proof in Section 2 below. Let us remark that Theorem 1.3 (c) solves Problem 19.90 (d) in the Kourovka notebook [16].

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 [4, 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 by 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 [3, Theorem 1.1], [22, Theorem 1.6], and [23, Theorem 1.3].   □

It leads us to the following conjecture. It was N. P. Byott who told the first author about this problem in person and Conjecture 1.5 should be attributed to him.

Conjecture 1.5. *For any $n \in \mathbb{N}$, there do not exist 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 [22, 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*

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

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.

Remark 1.8. The numbers n_0 in Theorem 1.7 are significant because

$$|A_5| = 2^2 \cdot 3 \cdot 5,$$

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

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

where $\mathrm{Sz}(-)$ denotes the Suzuki groups [20], and there is a unique insolvable group of order n_0 which is non-abelian simple; see Lemmas 5.5 and 5.7. Also, the key is that they satisfy the special conditions in Theorem 5.1 below.

Remark 1.9. Let ℓ_0 be an odd prime and let us discuss how often

$$(4^{\ell_0} + 1)(2^{\ell_0} - 1)$$

is square-free. Note that $4^5 + 1$ is divisible by 25, so let us assume that $\ell_0 \neq 5$.

Suppose that p is a prime and p^2 divides $(4^{\ell_0} + 1)(2^{\ell_0} - 1)$. Clearly $p \geq 5$ and p cannot divide both $4^{\ell_0} + 1$ and $2^{\ell_0} - 1$. We shall show that p must be a Wieferich prime, namely $2^{p-1} \equiv 1 \pmod{p^2}$. We thank one of the referees for pointing out this relation with Wieferich primes. If

$$2^{\ell_0} \equiv 1 \pmod{p^2},$$

then $\ell_0 \mid p - 1$ and p is clearly a Wieferich prime. If

$$4^{\ell_0} \equiv -1 \pmod{p^2}, \text{ and in particular } 2^{4\ell_0} \equiv 16^{\ell_0} \equiv 1 \pmod{p^2},$$

then -1 is a square mod p and $4 \mid p - 1$. Since $4^{10} \equiv 1 \pmod{25}$ and $\ell_0 \neq 5$, it also implies that $p \neq 5$. Thus, we have $p \geq 7$ and so $16 \not\equiv 1 \pmod{p}$. Then, it follows that $\ell_0 \mid p - 1$, whence $4\ell_0 \mid p - 1$ and we see that p is a Wieferich prime.

Except 1093 and 3511, there is no Wieferich prime less than 4×10^{12} by [6]. This suggests that $(4^{\ell_0} + 1)(2^{\ell_0} - 1)$ is square-free for most $\ell_0 \geq 7$, if not all.

In Section 6, we shall also present an algorithm which may be used to show that Conjecture 1.5 holds for any given $n \in \mathbb{N}$, given that all finite groups of order n have been classified. By implementing our algorithm in MAGMA [17] and using the SMALLGROUPS Library [1], we verified that:

Theorem 1.10. *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. Since any multiple of a non-solvable number is again non-solvable, the numbers n in Theorem 1.7 are non-solvable by Remark 1.8. See [18, A056866] for a complete list of non-solvable numbers at most 2000.

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 [7], [14], and [15], respectively.   □

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

Proof. For "cyclic" and "abelian", this is obvious. For "nilpotent" and "supersolvable", a proof may be found in [11, Theorems 10.3.1 and 10.5.1]. As for "metabelian" and "solvable", see [13, 3.10 and the discussion after 3.11].   □

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 [22, Proposition 2.1], for example, by (1.1) this is equivalent to the existence of

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

satisfying the relation

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

Below, we shall use (3.1) to give two necessary relations between G and N, both of which are not very hard to prove. 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. Also, let us 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 a standard result; see [13, 3.10], for example.   □

To state the first criterion, let $\mathrm{Inn}(N)$ and $\mathrm{Out}(N)$, denote the inner and outer automorphism groups of N, respectively. Let $\pi : \mathrm{Aut}(N) \longrightarrow \mathrm{Out}(N)$ denote 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. $\qquad \square$

To state the second criterion, let us 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 [3]; also see [22, Section 4.1]. Our main tool is the following proposition; also see Proposition 6.1.

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 [22, 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, and also 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 [22, 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 [22, 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 [3], we shall consider the case when M is a (proper) 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

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

where p is a prime. The following is well-known.

Lemma 3.4. *For any 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 $p \leq 3$.*

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 lies in the center, is the only element in $\mathrm{SL}_2(p)$ of order two. It follows that A has non-trivial center, which is a contradiction. Alternatively, the subgroups of $\mathrm{SL}_2(p)$ have been classified; see [21, Theorem 6.17]. None of the groups listed there are non-abelian simple, and we obtain a contradiction. We thank one of the referees for bringing Dickson's result on the subgroups of $\mathrm{PSL}_2(p)$ to our attention, which led us to this simpler proof which does not use the Feit-Thompson theorem. This proves part (a). Since any insolvable group of cube-free order has a non-abelian simple subgroup by [8], we see that part (b) follows from part (a) and Lemma 3.1. $\square$

5. Almost square-free orders

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

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

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

and that Conjecture 1.5 holds when $n = n_0$. Assume that the following hold.

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 number $n_0/2$ is solvable in the case that n_0 is even;*

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

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

Proof. Suppose for contradiction that the four conditions are satisfied but the conclusion is false. Let $r \in \mathbb{N}$ be the smallest number such that Conjecture 1.5 does not hold when $n = 2^r \cdot n_0$. Also, 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 have

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

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, we have $m \leq 2$ if $p = 3$ and $m = 1$ if $p \geq 5$ by the hypothesis on n_0, so $\mathrm{GL}_m(p)$ is solvable by Lemma 3.4. Then, the kernel of any homomorphism $G \longrightarrow \mathrm{Aut}(N/M)$ must be insolvable by Lemma 3.1, and we may take H to be insolvable by Proposition 3.3, which contradicts condition 4. In the case that $\epsilon_0 = 2$, it is possible that $m = 2$ when $p = 3$, but note that $2^r \cdot n_0/9$ is also solvable by condition 4 since a factor of a solvable number is solvable.

For $p = 2$, we have $|H| = 2^{r-m} \cdot n_0$, and thus H is insolvable by Lemma 5.2 below. Observe that $r - m \geq 0$ by condition 3. Since Conjecture 1.5 holds when $n = n_0$ by assumption, we in fact have $r - m \geq 1$, which contradicts the minimality of r. $\qquad\square$

Lemma 5.2. *Let $n_0 \in \mathbb{N}$ be any integer such that the conditions 1, 2, 3, 4 in Theorem 5.1 are satisfied. Then, for any $r \in \mathbb{N}_{\geq 0}$, we have:*

(i) *the subgroups of index a power of two of any insolvable group of order $2^r \cdot n_0$ are insolvable;*

(ii) any insolvable group of order $2^r \cdot n_0$ has a non-abelian composition factor of order n_0.

Proof. Notice that since a non-solvable number is a multiple of the order of a non-abelian simple group, conditions 3 and 4 imply that an insolvable group of order n_0 must be non-abelian simple.

We shall use induction on r. For $r = 0$, claim (i) is simply condition 1, and claim (ii) holds by the above observation. Suppose now 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 has a non-trivial and proper normal subgroup A. Either A or G/A is insolvable by Lemma 3.1. Since a factor of a solvable number is solvable, we have

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

where $0 \leq a \leq r - 1$, conditions 3 and 4. By the induction hypothesis, either A or G/A has a non-abelian composition factor of order n_0. It follows that G has a non-abelian composition factor of order n_0 also, which proves (ii). Next, let H be a subgroup of G of index a power of two. Observe that $AH/A \simeq H/A \cap H$, and also 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, which proves (i). □

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, 4 in Theorem 5.1.

Lemma 5.3. *The following statements are true.*

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

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

Proof. Part (a) is Burnside's theorem. Part (b) follows from the classification of finite simple groups. □

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*

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

and

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

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

Proof. Since p exactly divides n_0, a Sylow p-subgroup of any group of order n_0 is cyclic. If $p > 3^{\epsilon_0}$, then the claim follows from [12, Theorem 1]. If not, then $\epsilon_0 = 2$ with $p = 5, 7$, and the claim follows from [2] and [25], respectively. □

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 $1, 3, 4$ in Theorem 5.1 are satisfied.*

Proof. Since a non-solvable number is a multiple of the order of a non-abelian simple group, from Lemmas 5.3 (a) and 5.4, it is easy to deduce the first claim and that conditions 3 and 4 hold. Condition 1 holds trivially because A_5 and $\mathrm{PSL}_2(17)$ have no proper subgroup of index a power of two. □

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 4 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 (b) and (1.3). □

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, 4 *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. Since a non-solvable number is the multiple of the order of a non-abelian simple group, from Lemma 5.3 (b) 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 $k \geq 3$ odd and $d \geq 2$. Plainly $\ell_0 \neq k$, and because ℓ_0 is prime, we deduce that

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

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

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

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 maximal subgroups of $\mathrm{Sz}(2^{\ell_0})$ are known; see [26, Theorem 4.1], for example. None has index a non-trivial power of two and so condition 1 is satisfied. To prove conditions 3 and 4, note that if $n_0/2$ were non-solvable, then it would be a multiple of the order of a non-abelian simple group, so by Lemma 5.3 (b) and (1.3), we have

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

where $d, k \in \mathbb{N}$ with $k \geq 3$ odd. Similarly, if $(2^r \cdot n_0)/p$ were non-solvable for some odd prime p divisor of n_0 and $r \in \mathbb{N}_{\geq 0}$, then we have

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

where $d, k \in \mathbb{N}$ with $k \geq 3$ odd. In both cases, using the same argument as above, we obtain a contradiction. This completes the proof. □

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, 4 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 $r \in \mathbb{N}$.

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 1.10.

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. Define*

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

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

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

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:

- Often 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) $\qquad \mathcal{E}'(G, N) \neq \emptyset$ for some insolvable group G 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.

For $n \in \mathbb{N}$, define the following sets:

$$\mathcal{L}_1(n) = \bigcup_{\substack{|G|=n \\ G \text{ is insolvable}}} \{|H| : H \text{ is a solvable subgroup of } G\},$$

$$\mathcal{L}_2(n) = \bigcup_{\substack{|G|=n \\ G \text{ is insolvable}}} \{|H| : H \text{ is a subgroup of } G\}.$$

Write $\mathcal{N}_0(n)$ for the set of all solvable groups of order n. For all $N \in \mathcal{N}_0(n)$:

- If $|\mathrm{Fit}(N)| \notin \mathcal{L}_1(n)$, then (6.1) does not hold by Proposition 6.1.
- If $\mathrm{Aut}(N)$ is solvable, then $\mathrm{Hol}(N)$ is solvable by Lemma 3.1 and so it has no insolvable subgroup by Lemma 2.2, whence (6.1) does not hold.
- If $n/2 \in \mathcal{M}(N)$ and Conjecture 1.5 holds for $n/2$, then (6.1) does not hold by Proposition 3.3, because any subgroup of index two (when it exists) of an insolvable group must be insolvable by Lemma 3.1.
- If $\mathcal{M}(N) \not\subset \mathcal{L}_2(n)$, then (6.1) does not hold by Proposition 6.1.
- If the greatest common divisor of n and $|\mathrm{Out}(N)|$ is solvable, then (6.1) does not hold by Proposition 3.2.

Our algorithm uses thee above criteria, and removes the groups $N \in \mathcal{N}_0(n)$ for which (6.1) fails to hold; if the set becomes empty, then Conjecture 1.5 holds for n. More specifically, define the following sets:

$$\mathcal{N}_1(n) = \{N \in \mathcal{N}_0(n) : |\mathrm{Fit}(N)| \in \mathcal{L}_1(n)\},$$

$$\mathcal{N}_2(n) = \{N \in \mathcal{N}_1(n) : \mathrm{Aut}(N) \text{ is insolvable}\},$$

$$\mathcal{N}_{31}(n) = \{N \in \mathcal{N}_2(n) : n/2 \notin \mathcal{M}(N)\},$$

$$\mathcal{N}_{32}(n) = \{N \in \mathcal{N}_2(n) : \mathcal{M}(N) \subset \mathcal{L}_2(n)\},$$

$$\mathcal{N}_{33}(n) = \{N \in \mathcal{N}_2(n) : \gcd(n, |\mathrm{Out}(N)|) \text{ is non-solvable}\}.$$

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

We have implemented the computations of the above sets, except $\mathcal{N}_{33}(n)$, in MAGMA [17] and GAP [9]. The code may be found in the appendix.

6.1. **Proof of Theorem 1.10.** The groups of order $n \leq 2000$ are available in the SMALLGROUPS Library [1]. Using this library, we ran our algorithm in MAGMA to the non-solvable numbers $n \leq 2000$.

First, we computed that $\mathcal{N}_2(n)$ is empty except for

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

Among these numbers, we further computed that $\mathcal{N}_{31}(n) \cap \mathcal{N}_{32}(n)$ is empty except for $n = 1008, 1512$. In fact, we have

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

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

Then, using the MAGMA command `OuterOrder`, we checked that $\mathcal{N}_{33}(1008)$ and $\mathcal{N}_{33}(1512)$ are empty. Thus, we now conclude that Conjecture 1.5 indeed holds when $n \leq 2000$.

The calculations of $\mathcal{N}_2(n), \mathcal{N}_{31}(n) \cap \mathcal{N}_{32}(n)$ took a total of 22 min for all non-solvable numbers $n \leq 2000$. By contrast, it took a total of 231 min to confirm Conjecture 1.5 directly by using the MAGMA command `RegularSubgroups` for all non-solvable numbers $n \leq 1000$ with $n \neq 480, 672, 960$. The calculations were done on an Intel Xeon CPU E5-1620 vs3 @ 3.5GHz machine with 16GB of RAM under Ubuntu 16.04LTS.

The cases $n = 60, 120, 240, 480, 960, 1920$ also follow from Theorem 1.7.

7. ACKNOWLEDGMENTS

The first author would like to thank Prof. Leandro Vendramin for pointing out that Theorem 1.3 (c) solves Problem 19.90 (d) in [16].

Finally, we would like to thank the editor Prof. Eamonn O'Brien and the two referees for some very helpful suggestions. We would particularly like to thank one of the referees for pointing out a small gap in Theorem 5.1 in the original manuscript.

References

[1] H. U. Besche, B. Eick, and E. A. O'Brien, *A millennium project: constructing small groups*, Internat. J. Algebra Comput. 12 (2002), no. 5, 623–644.

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

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

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

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

[6] R. Crandall, K. Dilcher, and C. Pomerance, *A search for Wieferich and Wilson primes*, Math. Comp. 66 (1997), no. 217, 433–449.

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

[8] 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.

[9] The GAP Group, GAP – *Groups, Algorithms, and Programming, Version 4.10.2*; 2019, (https://www.gap-system.org).

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

[11] M. Hall, Jr., *The theory of groups.* The Macmillan Co., New York, N.Y. 1959.

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

[13] I. M. Isaacs, *Finite group theory.* Graduate Studies in Mathematics, 92. American Mathematical Society, Providence, RI, 2008.

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

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

[16] E. Khukhro and V. Mazurov, *Kourovka Notebook (Unsolved Problems in Group Theory). No. 19*, 2019.

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

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

[19] 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.

[20] M. Suzuki, *A new type of simple groups of finite order*, Proc. Nat. Acad. Sci. U.S.A. 46 (1960), 868–870.

[21] M. Suzuki, *Group theory. I.* Translated from the Japanese by the author. Grundlehren der Mathematischen Wissenschaften, 247. Springer-Verlag, Berlin-New York, 1982.

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

[23] C. Tsang, *Hopf-Galois structures on a Galois S_n-extension*, J. Algebra 531 (2019), no. 1, 349–361.

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

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

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

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

School of Mathematics (Zhuhai), Sun Yat-Sen University, P. R. China
E-mail address: qinch23@mail.sysu.edu.cn

Magma code to compute $\mathcal{N}_1(n), \mathcal{N}_2(n), \mathcal{N}_{31}(n), \mathcal{N}_{32}(n)$:

```
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 to compute $\mathcal{N}_1(n), \mathcal{N}_2(n), \mathcal{N}_{31}(n), \mathcal{N}_{32}(n)$:

```
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;
```