International Journal of Algebra and Computation
Vol. 30, No. 2 (2020) 253–265

DOI: 10.1142/S0218196719500735

On the solvability of regular subgroups in the holomorph of a finite solvable group

Cindy (Sin Yi) Tsang* and Chao Qin†
School of Mathematics (Zhuhai), Sun Yat-Sen University
Tangjiawan, Zhuhai, Guangdong 519082, P. R. China
**zengshy26@mail.sysu.edu.cn*
†*qinch23@mail.sysu.edu.cn*

Received 3 July 2019
Accepted 9 September 2019
Published 22 October 2019

Communicated by E. O'Brien

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

Keywords: Regular subgroups; holomorph; classification of finite simple groups.

Mathematics Subject Classification 2020: 20B35, 20F16, 20D05

1. Introduction

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

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

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

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

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

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

where the *holomorph of* N is

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

The enumeration of $\mathcal{E}'(G, N)$ is an important problem in the studies of Hopf-Galois structures and skew braces; see [6, Chap. 2; 19], respectively, for more details. In particular, there is a connection between elements of $\mathcal{E}'(G, N)$ and

(i) Hopf-Galois structures of type N on a Galois extension with Galois group G;
(ii) skew braces with additive group N and multiplicative group G.

We remark that skew braces in turn are related to non-degenerate set-theoretic solutions to the Yang–Baxter equation, see [11].

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

Question 1.1. If $\mathcal{E}'(G, N)$ is non-empty, are there restrictions on G and N in terms of their group-theoretic properties?

This question was studied by Byott [5, Theorems 1 and 2].

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

(a) *If N is nilpotent, then G is solvable.*
(b) *If G is abelian, then N is solvable.*

The proof of Proposition 1.2(b) given in [5, Sec. 6] may be used to show the following stronger result. This was first observed in [22, Theorem 4.2.4], which is unpublished; we reproduce the proof in Sec. 2. Note that Theorem 1.3(c) solves Problem 19.90(d) in the Kourovka notebook [17].

Theorem 1.3. *Let G and N be two finite groups of the same order such that $\mathcal{E}'(G, N)$ 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.*

Byott [5, Corollary 1.1] gave examples of solvable G and insolvable N with non-empty $\mathcal{E}'(G, N)$. He noted that, by contrast, there is no known example of

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

Results in the literature suggest that no such example exists.

Proposition 1.4. *Let G and N be two finite groups of the same order such that $\mathcal{E}'(G, N)$ 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 [4, Theorem 1.1]; [23, Theorem 1.6]; [24, Theorem 1.3]. □

It leads us to the following conjecture first formulated by Byott.

Conjecture 1.5. *For no positive integer n do there exist finite groups G and N both of order n for which* (1.2) *holds.*

In Sec. 3, using techniques developed in [23, Sec. 4.1], we provide some necessary criteria for $\mathcal{E}'(G, N)$ to be non-empty. In Secs. 4 and 5, by applying our criteria, we show the following theorems.

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

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

$$\begin{aligned} |A_5| &= 2^2 \cdot 3 \cdot 5, \\ |\mathrm{PSL}_2(17)| &= 2^4 \cdot 3^2 \cdot 17, \\ |\mathrm{Sz}(2^{2m+1})| &= 4^{2m+1}(4^{2m+1}+1)(2^{2m+1}-1) \text{ for } m \in \mathbb{N}, \end{aligned} \tag{1.3}$$

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

Remark 1.9. Let ℓ_0 be an odd prime and consider 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 show that p is a Wieferich prime, namely $2^{p-1} \equiv 1 \pmod{p^2}$. We thank a referee for pointing this out. If

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

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

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

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

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

In Sec. 6, we present an algorithm which shows that Conjecture 1.5 holds for a given n provided that all groups of order n have been classified. By implementing our algorithm in Magma [2] and using the SmallGroups Library [1], we established the following theorem.

Theorem 1.10. *Conjecture* 1.5 *holds when* $n \leq 2000$.

A number n is *solvable* if every group of order n is solvable, and is *non-solvable* otherwise. Conjecture 1.5 is trivial when n is solvable. Since every multiple of a non-solvable number is non-solvable, the numbers n in Theorem 1.7 are non-solvable by Remark 1.8. See [18, A056866] for the non-solvable numbers at most 2000.

2. Proof of Theorem 1.3

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

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

respectively, denote the projection map and homomorphism afforded by (1.1). Since $\mathcal{G}$ is regular, we may 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.

Lemma 2.1. *Let* Γ *be a finite group which is a product of two subgroups* Δ_1, Δ_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 [9, 15, 16], respectively. □

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

Proof. For cyclic and abelian groups, this is clear. For nilpotent and supersolvable groups, a proof may be found in [12, Theorems 10.3.1 and 10.5.1]. For metabelian and solvable groups, see [14, Lemma 3.10 and the discussion after Lemma 3.11]. □

3. Criteria for Non-Emptiness

In 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. As noticed in [23, Proposition 2.1], by (1.1) this is equivalent to the existence of

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

satisfying the relation

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

We use (3.1) to give two necessary relations between G and N, each not hard to prove. Yet, the criterion in Proposition 3.3 seems to be fairly powerful, and allows us to prove Theorems 1.6 and 1.7. Recall the following standard result, see [14, Lemma 3.10], for example.

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

Let $\mathrm{Inn}(N)$ and $\mathrm{Out}(N)$ denote the inner and outer automorphism groups of N, respectively. Let $\pi : \mathrm{Aut}(N) \to \mathrm{Out}(N)$ denote the natural quotient map with kernel $\mathrm{Inn}(N)$.

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

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

and $\mathfrak{g}$ restricts to a homomorphism $\ker(\mathfrak{f}) \to N$ 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

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

$(\pi \circ \mathfrak{f})(G)$ is insolvable, again by Lemma 3.1. □

Recall that a subgroup M of N is *characteristic* if $\varphi(M) = M$ for all $\varphi \in \mathrm{Aut}(N)$. Clearly M is normal in N, and we write

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

for the natural homomorphism. The use of characteristic subgroups of N is motivated by the arguments in [4]; also see [23, Sec. 4.1]. Our main tool is the following proposition; also see Proposition 6.1.

Proposition 3.3. *Let M be a characteristic subgroup of N. Now $H := \mathfrak{g}^{-1}(M)$ 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. That H is a subgroup of G follows from (3.1); see [23, Lemma 4.1] for a proof. Also, we have a homomorphism

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

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

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

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

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

Hence, analogously, we deduce from (1.1) that $\mathcal{E}'(H, M)$ is non-empty. This proves the first statement.

Next, as noted in [23, Lemma 4.1], the relation (3.1) implies that

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

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

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

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 follows. □

Although Proposition 3.3 is valid for every characteristic subgroup M of N, we focus on 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

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

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

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

The following is well known.

Lemma 3.4. $\mathrm{GL}_m(p)$ *is solvable precisely when* $m = 1$ *or* $m = 2$ *with* $p \leq 3$.

4. Proof of Theorem 1.6

Suppose for contradiction that the claim is false. 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 a maximal characteristic subgroup of N. Clearly M is solvable because N is solvable. As in (3.2), we then know that

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

But $|M| = n/p^m$, where $m = 1, 2$ because n is cube-free. Thus, by Lemma 4.1(b) below, the kernel of every homomorphism $G \to \mathrm{Aut}(N/M)$ is insolvable. From Proposition 3.3, we then see that $\mathcal{E}'(H, M)$ is non-empty for some insolvable subgroup H of G having 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 a 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 so both 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 $\mathrm{SL}_2(p)$. The subgroups of $\mathrm{SL}_2(p)$ have been completely classified; see [21, Theorem 6.17]. None is non-abelian simple, and we obtain a contradiction. We thank a referee for bringing Dickson's result on the subgroups of $\mathrm{PSL}_2(p)$ to our attention. This proves part (a). Since every insolvable group of cube-free order has a non-abelian simple subgroup by [8], part (b) follows from part (a) and Lemma 3.1. □

5. Almost Square-Free Orders

In this section, we prove Theorem 1.7. First, we 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*

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

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

(1) *all subgroups of index a power of* 2 *in an insolvable group of order* n_0 *are 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 if* 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* $r \in \mathbb{N}_{\geq 0}$.

Now, Conjecture 1.5 *holds when* $n = 2^r \cdot n_0$ *for every* $r \in \mathbb{N}$.

Proof. Suppose for contradiction that the four stated conditions are satisfied but the conclusion is false. Let r be the smallest number such that Conjecture 1.5 does not hold when $n = 2^r \cdot n_0$. Let G and N be two groups of order n satisfying (1.2). Let M be a maximal characteristic subgroup of N. Clearly M is solvable because N is solvable. As in (3.2),

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

Note that $|M| = n/p^m$. By Proposition 3.3, we know that $\mathcal{E}'(H, M)$ is non-empty for some subgroup H of G of the same order as M.

For p odd, observe $m \leq 2$ if $p = 3$, and $m = 1$ otherwise by the hypothesis on n_0, so $\mathrm{GL}_m(p)$ is solvable by Lemma 3.4. By Lemma 3.1, the kernel of every homomorphism $G \to \mathrm{Aut}(N/M)$ must be insolvable. Hence, by Proposition 3.3, we may take H to be insolvable, but this contradicts condition 4. In the case that

$\epsilon_0 = 2$, it is possible for $m = 2$ 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 $p = 2$, observe $|H| = 2^{r-m} \cdot n_0$ and so H is insolvable by Lemma 5.2. Note that $r - m \geq 0$ by condition 3. Since Conjecture 1.5 holds when $n = n_0$, we deduce that $r - m \geq 1$, but this contradicts the minimality of r. □

Lemma 5.2. *Let n_0 be a positive integer such that conditions 1–4 in Theorem 5.1 are satisfied. For every $r \in \mathbb{N}_{\geq 0}$, all subgroups of index a power of 2 of an insolvable group of order $2^r \cdot n_0$ are insolvable, and an insolvable group of order $2^r \cdot n_0$ has a non-abelian composition factor of order n_0.*

Proof. 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 use induction on r. For $r = 0$, the first claim is simply condition 1, and the second holds by the above observation. Now, suppose that $r \geq 1$, and let G be an insolvable group of order $2^r \cdot n_0$. By condition 2, G has a non-trivial and proper normal subgroup A. Note that either A or G/A is insolvable by Lemma 3.1. Since a factor of a solvable number is solvable,

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

where $0 \leq a \leq r - 1$, by 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, proving the second claim. Next, let H be a subgroup of G of index a power of 2. 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 are powers of 2. Hence, by the induction hypothesis, either $A \cap H$ or $H/A \cap H$ is insolvable. Lemma 2.2 implies that H is insolvable. □

We apply Theorem 5.1 to prove Theorem 1.7. To do so, we first show that the numbers n_0 in the statement of Theorem 1.7 satisfy conditions 1–4 in Theorem 5.1.

Lemma 5.3. *The following are true*:

(a) *A non-solvable number is divisible by at least* 3 *distinct primes.*
(b) *A finite non-abelian simple group whose order is not divisible by* 3 *must be 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*

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

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 every group of order n_0 is cyclic. If $p > 3^{\epsilon_0}$, then the claim follows from [13, Theorem 1]. If not, then $\epsilon_0 = 2$ with $p = 5, 7$ and the claim follows from [3, 25], respectively. □

Lemma 5.5. *Let* $n_0 = 2^2 \cdot 3 \cdot 5$ *or* $2^4 \cdot 3^2 \cdot 17$. *Up to isomorphism, there is exactly one insolvable group of order* n_0, *namely* A_5 *or* $\mathrm{PSL}_2(17)$. *Furthermore, 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 then holds trivially because both A_5 and $\mathrm{PSL}_2(17)$ have no proper subgroup of index a power of 2. □

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 5.3(b) and (1.3) imply the following lemma.

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*

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

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

Lemma 5.7. *Let* $n_0 = 4^{\ell_0}(4^{\ell_0} + 1)(2^{\ell_0} - 1)$ *where* ℓ_0 *is an odd prime. Up to isomorphism, there is exactly one insolvable group of order* n_0, *namely* $\mathrm{Sz}(2^{\ell_0})$. *Furthermore, conditions* $1, 3, 4$ *in Theorem* 5.1 *are satisfied.*

Proof. Suppose for contradiction that there exists an insolvable group of order n_0 which is not isomorphic to $\mathrm{Sz}(2^{\ell_0})$. It cannot be non-abelian simple by Lemma 5.6. Since a non-solvable number is a 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 $d \geq 2$. Clearly $\ell_0 \neq k$, and because ℓ_0 is prime,

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

Hence 2^k-1 divides $4^{\ell_0}+1$, so $k \leq 2\ell_0$. But

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

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.

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 2, so condition 1 is trivially 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),

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

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

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

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

5.1. *Proof of Theorem* 1.7

Let n_0 be as in the statement of the theorem. By Lemmas 5.4–5.7, we know that conditions 1–4 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 every $r \in \mathbb{N}$.

6. Algorithm to Test the Conjecture

In this section, we describe an algorithm which may be used to prove Conjecture 1.5 for a given n, provided that all groups of order n are known. We apply our algorithm to prove Theorem 1.10.

Let $\mathrm{Fit}(\Gamma)$ denote the Fitting subgroup of a finite group Γ; recall $\mathrm{Fit}(\Gamma)$ is the unique largest normal nilpotent subgroup of Γ and so it is characteristic. Propositions 1.2(a) and 3.3 imply the following proposition.

Proposition 6.1. *Let G and N be two finite groups of the same order such that $\mathcal{E}'(G,N)$ 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 $\mathcal{M}(N) \subset \mathcal{H}(G)$. *Moreover,* G *has a solvable subgroup whose order is that of* $\mathrm{Fit}(N)$.

While Proposition 6.1 gives us a way to check whether a pair (G, N) satisfies condition (1.2), applying it directly to verify Conjecture 1.5 faces two challenges.

- 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

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

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

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

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

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

- 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 a subgroup of index 2 (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 $\gcd(n, |\mathrm{Out}(N)|)$ is solvable, then (6.1) does not hold by Proposition 3.2.

Our algorithm uses the 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:

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

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

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

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

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

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

We implemented the computations of the above sets, excluding $\mathcal{N}_{33}(n)$, in Magma [2] and GAP [10]. The code may be found in the appendix of the arXiv version of this paper: arXiv:1901.10636.

6.1. *Proof of Theorem* 1.10

The groups of order at most 2000 are available in the SmallGroups Library [1]. Using this library, we applied 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 computed that $\mathcal{N}_{31}(n) \cap \mathcal{N}_{32}(n)$ is empty except for $n = 1008, 1512$. In fact,

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

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

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

The calculations of $\mathcal{N}_2(n)$ and $\mathcal{N}_{31}(n) \cap \mathcal{N}_{32}(n)$ took 22 min for all non-solvable numbers $n \leq 2000$. By contrast, it took 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 @ 3.5 GHz machine with 16 GB of RAM under Ubuntu 16.04LTS.

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

Acknowledgments

Part of this research was done while the authors visited each other at the University of Waikato and at the Yau Mathematical Sciences Center at Tsinghua University in 2018. The visits were supported by the China Postdoctoral Science Foundation Special Financial Grant (Grant No. 2017T100060). We thank both institutions; the first author especially thanks Prof. Daniel Delbourgo for his hospitality.

The first author thanks Prof. Leandro Vendramin for pointing out that Theorem 1.3(c) solves Problem 19.90(d) in [17].

Finally, we thank the editor Prof. Eamonn O'Brien and the two referees for some very helpful suggestions. We particularly 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, *Int. J. Algebra Comput.* **12**(5) (2002) 623–644.
[2] W. Bosma, J. Cannon and C. Playoust, The Magma algebra system. I. The user language, *J. Symbolic Comput.* **24** (1997) 23–265.
[3] R. Brauer, On simple groups of order $5 \cdot 3^a \cdot 2^b$, *Bull. Amer. Math. Soc.* **74** (1968) 900–903.
[4] N. P. Byott, Hopf-Galois structures on field extensions with simple Galois groups, *Bull. London Math. Soc.* **36**(1) (2004) 23–29.
[5] N. P. Byott, Solubility criteria for Hopf-Galois structures, *New York J. Math.* **21** (2015) 883–903.
[6] L. N. Childs, *Taming Wild Extensions*: *Hopf Algebras and Local Galois Module Theory*, Mathematical Surveys and Monographs, Vol. 80 (American Mathematical Society, Providence, RI, 2000).
[7] R. Crandall, K. Dilcher and C. Pomerance, A search for Wieferich and Wilson primes, *Math. Comput.* **66**(217) (1997) 433–449.
[8] H. Dietrich and B. Eick, On the groups of cube-free order, *J. Algebra* **292**(1) (2005) 122–137; Addendum, **367** (2012) 247–248.
[9] J. Douglas, On the supersolvability of bicyclic groups, *Proc. Natl. Acad. Sci. USA* **47** (1961) 1493–1495.
[10] The GAP Group, GAP — Groups, Algorithms, and Programming, Version 4.10.2 (2019), https://www.gap-system.org.
[11] L. Guarnieri and L. Vendramin, Skew braces and the Yang–Baxter equation, *Math. Comput.* **86**(307) (2017) 2519–2534.
[12] M. Hall, Jr., *The Theory of Groups* (The Macmillan Co., New York, 1959).
[13] M. Herzog, On finite simple groups of order divisible by three primes only, *J. Algebra* **10** (1968) 383–388.
[14] I. M. Isaacs, *Finite Group Theory*, Graduate Studies in Mathematics, Vol. 92 (American Mathematical Society, Providence, RI, 2008).
[15] N. Ito, Über das Produkt von zwei abelschen Gruppen, *Math. Z.* **62** (1955) 400–401.
[16] O. H. Kegel, Produkte nilpotenter Gruppen, *Arch. Math.* (*Basel*) **12** (1961) 90–93.
[17] E. Khukhro and V. Mazurov, *Unsolved Problems in Group Theory*, Kourovka Notebook, No. 19 (2019), https://kourovka-notebook.org/.
[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**(1) (2018) 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*, Grundlehren der Mathematischen Wissenschaften, Vol. 247 (Springer-Verlag, Berlin-New York, 1982).
[22] C. Tsang, Galois module structures and Hopf-Galois structures on extensions of number fields, *Postdoctoral Report*, Tsinghua University (2018).
[23] C. Tsang, Non-existence of Hopf-Galois structures and bijective crossed homomorphisms, *J. Pure Appl. Algebra* **223**(7) (2019) 2804–2821.
[24] C. Tsang, Hopf-Galois structures on a Galois S_n-extension, *J. Algebra* **531**(1) (2019) 349–361.
[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, Vol. 251 (Springer-Verlag, London, 2009).