HOPF-GALOIS STRUCTURES ON FINITE EXTENSIONS WITH QUASISIMPLE GALOIS GROUP

CINDY (SIN YI) TSANG

ABSTRACT. Let $L/K$ be a finite Galois extension of fields with Galois group $G$. It is known that $L/K$ admits exactly two Hopf-Galois structures when $G$ is non-abelian simple. In this paper, we extend this result to the case when $G$ is quasisimple.

CONTENTS

1. Introduction ................................. 1
2. Crossed homomorphisms ................. 3
3. Consequences of CFSG ................. 5
4. Proof of Theorem 1.4 ................. 6
4.1. Non-perfect groups ................. 7
4.2. Perfect groups .................. 11
Acknowledgments ..................... 17
References ............................... 17

1. Introduction

Let $L/K$ be a finite Galois extension of fields with Galois group $G$. By [10], we know that each Hopf-Galois structure $\mathcal{H}$ on $L/K$ is associated to a group $N_\mathcal{H}$ of the same order as $G$. For each group $N$ of order $|G|$, define

$$e(G, N) = \#\{\text{Hopf-Galois structures } \mathcal{H} \text{ on } L/K \text{ with } N_\mathcal{H} \simeq N\}.$$ 

Let $\text{Perm}(N)$ be the group of all permutations on $N$. Recall that a subgroup of $\text{Perm}(N)$ is regular if its action on $N$ is regular. For example, clearly $\lambda(N)$ and $\rho(N)$ are regular subgroups of $\text{Perm}(N)$, where

$$\begin{cases}
\lambda : N \rightarrow \text{Perm}(N); & \lambda(\eta) = (x \mapsto \eta x) \\
\rho : N \rightarrow \text{Perm}(N); & \rho(\eta) = (x \mapsto x\eta^{-1})
\end{cases}$$
are the left and right regular representations of $N$. By work of [10] and [4], we have the formula
\[
e(G, N) = \frac{|\text{Aut}(G)|}{|\text{Aut}(N)|} \cdot \# \left\{ \text{regular subgroups of Hol}(N) \mid \text{which are isomorphic to } G \right\},
\]
where Hol$(N)$ is the holomorph of $N$ and is defined to be
\[
\text{Hol}(N) = \rho(N) \rtimes \text{Aut}(N).
\]
The calculation of $e(G, N)$ has been an active line of research because Hopf-Galois structures have application in Galois module theory; see [7] for more details. Let us also note in passing that regular subgroups of the holomorph are related to set-theoretic solutions to the Yang-Baxter equation; see [11].

For $N \cong G$, the number $e(G, N)$ must be non-zero because $\lambda(N)$ and $\rho(N)$ are regular subgroups of Hol$(N)$; note that $\lambda(N)$ and $\rho(N)$ are equal exactly when $N$ is abelian. For $N \not\cong G$, the number $e(G, N)$ could very well be zero. In certain extreme cases, it might happen that
\[
e(G, N) = \begin{cases} 
1 & \text{for } N \cong G \text{ when } G \text{ is abelian,} \\
2 & \text{for } N \cong G \text{ when } G \text{ is non-abelian,} \\
0 & \text{for all other } N \not\cong G.
\end{cases}
\]

For $G$ abelian, by [4, Theorem 1] we know exactly when (1.1) occurs:

**Theorem 1.1.** If $G$ is a finite abelian group, then (1.1) holds precisely when the orders of $G$ and $(\mathbb{Z}/|G|\mathbb{Z})^\times$ are coprime.

For $G$ non-abelian, the situation is more complicated. By [5,6], we have:

**Theorem 1.2.** If $G$ is a finite non-abelian simple group, then (1.1) holds.

It is natural to ask whether Theorem 1.2 may be generalized to other non-abelian groups $G$ which are close to being simple. Recall that $G$ is said to be quasisimple if $G = [G, G]$ and $G/Z(G)$ is a simple group, where $[G, G]$ is the commutator subgroup and $Z(G)$ is the center of $G$. In [16, Theorem 1.3], the author has already shown that:

**Theorem 1.3.** If $G$ is a finite quasisimple group, then $e(G, G) = 2$. 
It remains to consider the groups \( N \not\cong G \). In [16, Theorem 1.6], the author has shown that if \( G \) is the double cover of \( A_n \) with \( n \geq 5 \), then \( e(G, N) = 0 \) for all groups \( N \not\cong G \) of order \( n! \). We shall extend this result and prove:

**Theorem 1.4.** If \( G \) is a finite quasisimple group, then \( e(G, N) = 0 \) for all groups \( N \not\cong G \) of order \( |G| \).

In view of Theorems 1.3 and 1.4, one might guess that (1.1) is also true for say, finite almost simple or non-abelian characteristically simple groups \( G \). If \( G = S_n \) with \( n \geq 5 \), however, then by [6, Theorems 5 and 9], we have

\[
e(G, G) \neq 2 \quad \text{and} \quad e(G, N) \neq 0 \quad \text{for some} \quad N \not\cong G.
\]

See [19, 21] for generalizations to other finite almost simple groups \( G \). If \( G \) is a finite non-abelian characteristically simple group which is not simple, then \( e(G, G) \neq 2 \) by [17], but as far as the author knows, there is no investigation yet on whether there exists \( N \not\cong G \) such that \( e(G, N) \neq 0 \).

2. **Crossed homomorphisms**

In this section, let \( G \) and \( \Gamma \) be finite groups, whose orders are not assumed to be equal. Given \( f \in \text{Hom}(G, \text{Aut}(\Gamma)) \), recall that a *crossed homomorphism* (with respect to \( f \)) is a map \( g : G \to \Gamma \) which satisfies

\[
g(\sigma \tau) = g(\sigma) \cdot f(\sigma)(g(\tau)) \quad \text{for all} \quad \sigma, \tau \in G.
\]

Let \( Z^1_f(G, \Gamma) \) be the set of all such maps \( g \). The regular subgroups of \( \text{Hol}(\Gamma) \) isomorphic to \( G \) may be parametrized by the bijective maps in \( Z^1_f(G, \Gamma) \).

**Proposition 2.1.** The regular subgroups of \( \text{Hol}(\Gamma) \) isomorphic to \( G \) are precisely the sets \( \{ \rho(g(\sigma)) \cdot f(\sigma) : \sigma \in G \} \), as \( f \) ranges over \( \text{Hom}(G, \text{Aut}(\Gamma)) \) and \( g \) over the bijective maps in \( Z^1_f(G, \Gamma) \).

**Proof.** The proof is straightforward; see [16, Proposition 2.1]. \(\square\)

Hence, when \( \Gamma \) has order \( |G| \), that \( e(G, \Gamma) \) is non-zero is equivalent to the existence of a bijective map \( g \in Z^1_f(G, \Gamma) \) for some \( f \in \text{Hom}(G, \text{Aut}(\Gamma)) \). Let us give two approaches to study these crossed homomorphisms. The first is to define another \( h \in \text{Hom}(G, \text{Aut}(\Gamma)) \). The idea originates from [6] and was
formalized by the author in [19, Proposition 3.4] or [21, Proposition 2.3]. The second is to use characteristic subgroups of \( \Gamma \), that is, subgroups \( \Lambda \) such that \( \varphi(\Lambda) = \Lambda \) for all \( \varphi \in \text{Aut}(\Gamma) \). The idea comes from [5] and was restated in terms of crossed homomorphisms by the author in [16, Lemma 4.1].

**Proposition 2.2.** Let \( f \in \text{Hom}(G, \text{Aut}(\Gamma)) \) and \( g \in Z^1_f(G, \Gamma) \). Define

\[
h : G \rightarrow \text{Aut}(\Gamma); \quad h(\sigma) = \text{conj}(g(\sigma)) \cdot f(\sigma),
\]

where \( \text{conj}(\cdot) = \lambda(\cdot)\rho(\cdot) \). Then:

(a) We have \( h \in \text{Hom}(G, \text{Aut}(\Gamma)) \).

(b) For any \( \sigma \in G \), we have \( f(\sigma) = h(\sigma) \) if and only if \( \sigma \in g^{-1}(Z(\Gamma)) \).

(c) The map \( \sigma \mapsto g(\sigma) \) defines a homomorphism \( \ker(f) \rightarrow \Gamma \).

(d) The map \( \sigma \mapsto g(\sigma)^{-1} \) defines a homomorphism \( \ker(h) \rightarrow \Gamma \).

*Proof.* Part (a) appeared in [19, Proposition 3.4], while parts (b) – (d) were stated in [21, Proposition 2.3]. The proofs are straightforward. \( \square \)

**Proposition 2.3.** Let \( f \in \text{Hom}(G, \text{Aut}(\Gamma)) \) and \( g \in Z^1_f(G, \Gamma) \). Let \( \Lambda \) be any characteristic subgroup of \( \Gamma \). Consider the homomorphism

\[
\overline{f} : G \xrightarrow{f} \text{Aut}(\Gamma) \xrightarrow{\varphi \mapsto (\gamma\Lambda \mapsto \varphi(\gamma)\Lambda)} \text{Aut}(\Gamma/\Lambda)
\]

induced by \( f \) and the map

\[
\overline{g} : G \xrightarrow{g} \Gamma \xrightarrow{\text{quotient map}} \Gamma/\Lambda
\]

induced by \( g \). Then:

(a) We have \( \overline{g} \in Z^1_f(G, \Gamma/\Lambda) \).

(b) The preimage \( g^{-1}(\Lambda) \) is a subgroup of \( G \).

(c) In the case that \( g \) is bijective, there is a regular subgroup of \( \text{Hol}(\Lambda) \) which is isomorphic to \( g^{-1}(\Lambda) \).

*Proof.* Parts (a) and (b) are clear; see [16, Proposition 4.1] for a proof of the latter. For part (c), see [20, Proposition 3.3]. \( \square \)

Following [5], we shall take \( \Lambda \) to be a maximal characteristically subgroup of \( \Gamma \). Then, the quotient \( \Gamma/\Lambda \) is a non-trivial characteristically simple group,
and since $\Gamma$ is finite, we know that

\[(2.1) \quad \Gamma/\Lambda \cong T^m, \text{ where } T \text{ is a simple group and } m \in \mathbb{N},\]

in which case the structure of $\text{Aut}(\Gamma/\Lambda)$ is well-known. This approach turns out to be very useful and was crucial in all of $[16,18,20,21]$.

### 3. Consequences of CFSG

In this section, let $A$ be a finite non-abelian simple group. We shall require some consequences of the classification of finite simple groups (CFSG).

One difficulty in dealing with finite quasisimple groups, as opposed to non-abelian simple groups, is that they need not be centerless. But their center is a quotient of the Schur multiplier of the associated finite non-abelian simple group; see [1, Section 33] for more on Schur multipliers.

Let $m(A)$ denote the order of the Schur multiplier of $A$. We shall say that $\text{PSL}_n(q)$ and $\text{PSU}_n(q)$, respectively, are non-exceptional if

\[(3.1) \quad m(\text{PSL}_n(q)) = \gcd(n, q - 1) \quad \text{and} \quad m(\text{PSU}_n(q)) = \gcd(n, q + 1).\]

As a consequence of CFSG, we know that $m(A)$ is small, in fact at most 12, except when $A \cong \text{PSL}_n(q), \text{PSU}_n(q)$. More specifically:

**Lemma 3.1.** Let $\mathcal{M} = \{1, 2, 3, 4, 6, 12\}$.

(a) If $A \not\cong \text{PSL}_n(q), \text{PSU}_n(q)$, then $m(A) \in \mathcal{M}$.

(b) If $A = \text{PSL}_n(q), \text{PSU}_n(q)$, then $m(A) \in \mathcal{M}$ or $A$ is non-exceptional, except that $m(\text{PSL}_3(4)) = 48$ and $m(\text{PSU}_4(3)) = 36$.

*Proof.* See [15, Theorem 5.1.4].

**Lemma 3.2.** The outer automorphism group $\text{Out}(A)$ of $A$ is solvable.

*Proof.* This is known as Schreier conjecture; see [9, Theorem 1.46].

**Lemma 3.3.** Every $\varphi \in \text{Aut}(A)$ has a fixed point other than $1_A$.

*Proof.* See [9, Theorem 1.48].

**Lemma 3.4.** There do not exist subgroups $B_1$ and $B_2$ of $A$ such that both of them have non-trivial center and $A = B_1B_2$. 

*Proof.*
Lemma 3.5. Suppose that $A$ has a subgroup of index $p^a$, where $p$ is a prime and $a \in \mathbb{N}$. Then, one of the following holds:

(a) $A \simeq A_{p^a}$ with $p^a \geq 5$;
(b) $A \simeq \text{PSL}_n(q)$ with $p^a = (q^n - 1)/(q - 1)$;
(c) $A \simeq \text{PSL}_2(11)$ with $p^a = 11$;
(d) $A \simeq M_{11}$ with $p^a = 11$, or $A \simeq M_{23}$ with $p^a = 23$;
(e) $A \simeq \text{PSU}_4(2)$ with $p^a = 27$.

Proof. See [12, Theorem 1]. □

4. PROOF OF THEOREM 1.4

In this section, let $G$ be a finite quasisimple group, and let $N$ be any group of order $|G|$. Suppose that $e(G, N) \neq 0$, namely there is a regular subgroup $\mathcal{G}$ of $\text{Hol}(N)$ isomorphic to $G$. In the next two subsections, we shall prove:

**Proposition 4.1.** The group $N$ must be perfect, namely $N = [N, N]$.

**Proposition 4.2.** The regular subgroup $\mathcal{G}$ is either $\rho(N)$ or $\lambda(N)$.

Theorem 1.4 would follow, because then $N \simeq \mathcal{G} \simeq G$.

Let us first set up the notation. By Proposition 2.1, we know that

$$\mathcal{G} = \{\rho(g(\sigma)) \cdot f(\sigma) : \sigma \in G\},$$

where

$$\begin{cases}
    f \in \text{Hom}(G, \text{Aut}(N)), \\
    g \in \text{Z}_f^1(G, N) \text{ is bijective}.
\end{cases}$$

Alternatively, we may rewrite it as

$$\mathcal{G} = \{\lambda(g(\sigma))^{-1} \cdot h(\sigma) : \sigma \in G\},$$

where $h \in \text{Hom}(G, \text{Aut}(N))$ is defined as in Proposition 2.2. Let $M$ be any maximal characteristic subgroup of $N$. Then, as in Proposition 2.3, we have homomorphisms

$$\overline{f}, \overline{h} : G \to \text{Aut}(N) \xrightarrow{\varphi \mapsto (\eta \mapsto \varphi(\eta) M)} \text{Aut}(N/M)$$

induced by $f$ and $h$, respectively, and a surjective crossed homomorphism

$$\overline{g} : G \to N \xrightarrow{\text{quotient map}} N/M$$
with respect to \( \tilde{f} \) induced by \( \tilde{g} \). We shall also need the facts that

\[
(4.1) \quad Z(G) \text{ is a quotient of the Schur multiplier of } G/Z(G),
\]

\[
(4.2) \quad \text{all proper normal subgroups of } G \text{ are contained in } Z(G).
\]

See [1, (33.8)] for the former, and the latter is an easy exercise.

4.1. Non-perfect groups. Suppose for contradiction that \( N \) is not perfect, in which case we may take \( M \) to contain \([N, N]\). By (2.1), we then have

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

Let us first make a simple observation.

**Lemma 4.3.** The homomorphism \( \tilde{f} \) is non-trivial and \( m \geq 2 \).

**Proof.** Suppose for contradiction that \( \tilde{f} \) is trivial. Then, the map

\[
G \xrightarrow{\tilde{g}} N/M \xrightarrow{\cong} (\mathbb{Z}/p\mathbb{Z})^m
\]

is a homomorphism by Proposition 2.2(c), and so must be trivial because \( G \) is perfect. This contradicts that \( \tilde{g} \) is surjective, so indeed \( \tilde{f} \) is non-trivial. It follows that \( m \geq 2 \), for otherwise

\[
G \xrightarrow{\tilde{f}} \text{Aut}(N/M) \xrightarrow{\cong} (\mathbb{Z}/p\mathbb{Z})^\times
\]

would be trivial again because \( G \) is perfect, which we know is impossible. \( \square \)

Define \( H = g^{-1}(M) \), which is a subgroup of \( G \) by Proposition 2.3(b), and whose order is \(|M|\) because \( g \) is bijective. Thus, we have \([G : H] = p^m\). Put

\[
p^z = [HZ(G) : H] = [Z(G) : H \cap Z(G)], \text{ where } 0 \leq z \leq m.
\]

Note that \( p \) divides \(|Z(G)|\) unless \( z = 0 \). Also \( m - z \geq 1 \), for otherwise

\[
G = HZ(G) \text{ and in particular } G = [G, G] = [H, H],
\]

which is impossible because \( H \) is a proper subgroup. Since

\[
\left[ \frac{G}{Z(G)} : \frac{HZ(G)}{Z(G)} \right] = \frac{[G : H]}{[HZ(G) : H]} = p^{m-z},
\]

by Lemma 3.5 one of the following holds:
(a) $G/Z(G) \simeq A_{p^{m-z}}$ with $p^{m-z} \geq 5$;
(b) $G/Z(G) \simeq \text{PSL}_n(q)$ with $p^{m-z} = (q^n - 1)/(q - 1)$;
(c) $G/Z(G) \simeq \text{PSL}_2(11)$ with $p^{m-z} = 11$;
(d) $G/Z(G) \simeq M_{11}$ with $p^{m-z} = 11$, or $G/Z(G) \simeq M_{23}$ with $p^{m-z} = 23$;
(e) $G/Z(G) \simeq \text{PSU}_4(2)$ with $p^{m-z} = 27$.

Since Theorem 1.4 holds when $G$ is a finite non-abelian simple group by [5], and when $G$ is the double cover of $A_n$ with $n \geq 5$ by [16, Theorem 1.6], we may henceforth assume that:

**Assumption.** The center $Z(G)$ of $G$ is non-trivial.

Recall from (4.1) that $|Z(G)|$ divides $m(G/Z(G))$. Hence, this assumption in particular restricts that $m(G/Z(G)) \neq 1$.

**Assumption.** The group $G$ is not the double cover of an alternating group.

**Lemma 4.4.** We must be in case (b).

**Proof.** Case (d) does not occur by our first assumption because

$$m(M_{11}) = 1 = m(M_{23}).$$

To deal with cases (a), (c), and (e), note that

$$m(A_n) = \begin{cases} 2 & \text{if } n = 5 \text{ or } n \geq 8 \\ 6 & \text{if } n = 6, 7 \end{cases} \quad \text{and } m(\text{PSL}_2(11)) = 2 = m(\text{PSU}_4(2)).$$

For case (a), we must have $p^{m-z} = 7$ by our second assumption. For case (c), we have $p^{m-z} = 11$. In both cases, note that $p$ does not divide $m(G/Z(G))$, so $z = 0$ and $m = 1$. But this contradicts Lemma 4.3. For case (e), we have $p^{m-z} = 27$. Since $p$ does not divide $m(G/Z(G))$, we have $z = 0$ and $m = 3$. Also, by our first assumption, necessarily

$$|Z(G)| = 2, \text{ and so } |G| = 2|\text{PSU}_4(2)| = 51840.$$  

But $|\text{GL}_m(p)| = |\text{GL}_3(3)| = 11232$, so the homomorphism

$$G \rightarrow \text{Aut}(N/M) \rightarrow \text{GL}_3(3)$$
is trivial by (4.2) and by comparing orders. But this contradicts Lemma 4.3. Thus, indeed we must be in case (b).

In view of Lemma 4.4, we now know that

$$G/Z(G) \simeq \operatorname{PSL}_n(q) \text{ with } p^{m-z} = (q^n - 1)/(q - 1).$$

By [15, Theorem 5.1.4], we also know that \( m(\operatorname{PSL}_n(q)) = \gcd(n, q - 1) \), unless \((n, q)\) equals one of the five pairs stated in the next lemma. Let us first rule out these cases.

**Lemma 4.5.** We have \((n, q) \neq (2, 4), (2, 9), (3, 2), (3, 4), (4, 2)\).

**Proof.** Suppose for contradiction that \((n, q)\) is one of the stated pairs. Then this pair must be \((2, 4)\) or \((3, 2)\) because \((q^n - 1)/(q - 1)\) is a prime power. Note that

$$p^{m-z} = \frac{q^n - 1}{q - 1} = \begin{cases} 5 & \text{if } (n, q) = (2, 4), \\ 7 & \text{if } (n, q) = (3, 2). \end{cases}$$

But \( m(\operatorname{PSL}_2(4)) = 2 = m(\operatorname{PSL}_3(2)) \). In either case, since \( p \) does not divide 2, we see that \( z = 0 \), and so \( m = 1 \). But this contradicts Lemma 4.3. \( \square \)

**Lemma 4.6.** We have \( G \simeq \operatorname{SL}_n(q) \) and \( |Z(G)| = n = p. \)

**Proof.** By Lemma 4.5 and our first assumption, respectively, we have

$$m(G/Z(G)) = \gcd(n, q - 1) \text{ and } m(G/Z(G)) \neq 1.$$

As noted in [12, (3.3)], that \( p^{m-z} = (q^n - 1)/(q - 1) \) implies that \( n \) is a prime. It then follows that

$$\gcd(n, q - 1) = n, \text{ and so } q \equiv 1 \pmod{n}.$$ 

Moreover, we must have \( |Z(G)| = n \) and also \( G \simeq \operatorname{SL}_n(q) \), the universal cover of \( \operatorname{PSL}_n(q) \). Note that

$$p^{m-z} \equiv q^{n-1} + \cdots + q + 1 \equiv 1 + \cdots + 1 + 1 \equiv n \equiv 0 \pmod{n}$$

so in fact \( n = p. \) This completes the proof. \( \square \)

We shall now use the next proposition to get a contradiction and thus prove Proposition 4.1; cf. [5, Theorem 4.3] and the argument in [5, Section 4].
Proposition 4.7. Suppose that $\text{SL}_n(q)$ has a non-trivial irreducible representation of degree $d$ over a field of characteristic coprime to $q$, where

$$(n, q) \neq (3, 2), (3, 4), (4, 2), (4, 3).$$

Then, we have

$$d \geq \begin{cases} 
(q - 1)/\gcd(2, q - 1) & \text{if } n = 2, \\
(q^n - 1)/(q - 1) - 2 & \text{if } n \geq 3.
\end{cases}$$

Proof. See [13, Lemma 9.1.1 and Theorem 9.1.5].

Proof of Proposition 4.1. By Lemmas 4.3 and 4.6, we have $m \geq 2$ and there is a non-trivial homomorphism

$$\text{SL}_n(q) \rightarrow G \rightarrow \text{Aut}(N/M) \rightarrow \text{GL}_m(p).$$

Since $p^{m-z} = (q^n - 1)/(q - 1)$, we have $\gcd(p, q) = 1$ and also $(n, q) \neq (4, 3)$. By Lemma 4.5, we may then apply Proposition 4.7 as follows. Recall that $|Z(G)| = n = p$ by Lemma 4.6, which in turn implies $z = 0, 1$.

For $n = 2$, note that $p^{m-z} = q + 1$, and we obtain

$$m \geq \frac{q - 1}{\gcd(2, q - 1)} = \frac{p^{m-z} - 2}{\gcd(2, p^{m-z} - 2)} \geq \frac{2^{m-1} - 2}{2}.$$ 

For $n \geq 3$, similarly we have

$$m \geq \frac{q^n - 1}{q - 1} - 2 = p^{m-z} - 2 \geq 3^{m-1} - 2.$$ 

From the above inequalities, we deduce that

$$(m, p) = \begin{cases} 
(2, 2), (3, 2), (4, 2) & \text{if } n = 2, \\
(2, 3) & \text{if } n \geq 3.
\end{cases}$$

Since $n^{m-z} = p^{m-z} = (q^n - 1)/(q - 1)$ and $z = 0, 1$, it follows that

$$(n, q) = (2, 3), (2, 7), \text{ and in fact necessarily } (n, q) = (2, 7)$$

because $\text{PSL}_2(3)$ is not simple. We are left with the possibility $G \simeq \text{SL}_2(7)$.

Using the Holomorph and RegularSubgroups commands in Magma [2], we checked that $\text{Hol}(N)$ has no regular subgroup isomorphic to $G \simeq \text{SL}_2(7)$.
for all non-perfect groups $N$ of order 336. We remark that in fact it suffices to check the insolvable groups $N$ of order 336 by [20, Theorem 1.10]. Thus, we obtain a contradiction, so indeed $N$ must be perfect. □

4.2. Perfect groups. By Proposition 4.1, we know that $N$ must be perfect, in which case all quotients of $N$ are also perfect. By (2.1), we then have

$$N/M \simeq T^m,$$

where $T$ is non-abelian simple and $m \in \mathbb{N},$

and by [5, Lemma 3.2] for example, we know that

$$\text{Aut}(T^m) = \text{Aut}(T)^m \rtimes S_m.$$

We shall also use Burnside’s theorem, which states that the order of a finite insolvable group is divisible by at least three distinct primes.

The cases $G/Z(G) \simeq \text{PSL}_n(q), \text{PSU}_n(q)$ require special arguments because then $m(G/Z(G))$ and so $|Z(G)|$ could be arbitrarily large. Let us recall that

$$(4.3) \quad |\text{PSL}_n(q)| = \frac{1}{\gcd(n, q-1)} \left( q \left( \frac{n}{2} \prod_{i=2}^{n} (q^i - 1) \right) \right),$$

$$|\text{PSU}_n(q)| = \frac{1}{\gcd(n, q+1)} \left( q \left( \frac{n}{2} \prod_{i=2}^{n} (q^i - (-1)^i) \right) \right).$$

We shall prove that either $f$ or $h$ is trivial in a sequence of steps.

**Lemma 4.8.** The image $\overline{f}(G)$ lies in $\text{Inn}(N/M)$.

**Proof.** Below, we shall show that the homomorphism

$$\overline{f}_{S_m} : G \xrightarrow{\overline{f}} \text{Aut}(N/M) \xrightarrow{\text{identification}} \text{Aut}(T)^m \rtimes S_m \xrightarrow{\text{projection}} S_m$$

is trivial. Then, the image $\overline{f}(G)$ lies in $\text{Aut}(T)^m$, and the homomorphism

$$G \xrightarrow{\overline{f}} \text{Aut}(T)^m \xrightarrow{\text{projection}} \text{Out}(T)^m$$

is also trivial, because $G$ is perfect while $\text{Out}(T)$ is solvable by Lemma 3.2. It follows that $\overline{f}(G)$ lies in $\text{Inn}(T)^m$, which is identified with $\text{Inn}(N/M)$.

To prove that $\overline{f}_{S_m}$ is trivial, let $\ell$ be any prime factor of $|T|$. For any finite group $\Gamma$, let $v_\ell(\Gamma)$ be the non-negative integer such that $\ell^{v_\ell(\Gamma)}$ exactly divides
We have $v_\ell(G) \geq m$ because $|G| = |N| = |T|^m|M|$. It is well-known that
\[ v_\ell(S_m) = \left\lfloor \frac{m}{\ell} \right\rfloor + \left\lfloor \frac{m}{\ell^2} \right\rfloor + \left\lfloor \frac{m}{\ell^3} \right\rfloor + \cdots \] and so $v_\ell(S_m) < \frac{m}{\ell - 1}$.

Since $G/\ker(\widehat{f}_{S_m})$ embeds into $S_m$, we then deduce that
\[ v_\ell(G) - v_\ell(\ker(\widehat{f}_{S_m})) \leq v_\ell(S_m) < \frac{m}{\ell - 1}. \tag{4.4} \]

Suppose now for contradiction that $\widehat{f}_{S_m}$ is non-trivial, in which case $\ker(\widehat{f}_{S_m})$ lies in $Z(G)$ by (4.2). From $m \leq v_\ell(G)$ and (4.4), we see that
\[ m - v_\ell(Z(G)) \leq v_\ell(G) - v_\ell(Z(G)) \leq v_\ell(G) - v_\ell(\ker(\widehat{f}_{S_m})) < \frac{m}{\ell - 1}, \]
and so $v_\ell(Z(G)) \geq 1$. This implies that every prime factor of $|T|$ also divides $|Z(G)|$. From Burnside’s theorem and (4.1), it then follows that $m(G/Z(G))$ has at least three distinct prime divisors. From Lemma 3.1, we deduce that
\[ G/Z(G) \simeq \text{PSL}_n(q), \text{PSU}_n(q) \text{ with } \text{PSL}_n(q), \text{PSU}_n(q) \text{ non-exceptional.} \]

Put $v_\ell(G) = x$ and $v_\ell(Z(G)) = y$, where $x, y \geq 1$. Then, we have
\[ x - y < \frac{m}{\ell - 1} \leq \frac{x}{\ell - 1} \text{ and in particular } y > \frac{\ell - 2}{\ell - 1} \cdot x. \]

Also, from (3.1) and (4.1), we see that
\[ |Z(G)| \text{ divides } \begin{cases} \gcd(n, q - 1) & \text{if } G/Z(G) \simeq \text{PSL}_n(q), \\ \gcd(n, q + 1) & \text{if } G/Z(G) \simeq \text{PSU}_n(q). \end{cases} \tag{4.5} \]

Since $\ell^y$ divides $|Z(G)|$, from (4.5) we have $\ell^y \leq n$, that is $y \leq \log(n)/\log(\ell)$. Observe that the order formulae in (4.3) imply that
\[ (q - 1)^{n-2} \text{ divides } |\text{PSL}_n(q)|, \]
\[ (q + 1)^{\lfloor n/2 \rfloor - 1} \text{ divides } |\text{PSU}_n(q)|. \]

Since $\ell^y$ divides $|Z(G)|$, again from (4.5) we see that $\ell$ divides $q - 1$ and $q + 1$, respectively, and in particular
\[ v_\ell(G) - v_\ell(Z(G)) \geq \begin{cases} n - 2 & \text{if } G/Z(G) \simeq \text{PSL}_n(q), \\ \lfloor n/2 \rfloor - 1 & \text{if } G/Z(G) \simeq \text{PSU}_n(q). \end{cases} \]
In either case, this in turns yields
\[ x - 1 \geq x - y \geq \frac{n}{2} - \frac{1}{2} - 1 \] and so \( x \geq \frac{n - 1}{2} \).

Again, by Burnside’s theorem, we may take \( \ell \geq 5 \). We obtain
\[
\frac{4}{3} \cdot \frac{\log(n)}{\log(5)} \geq \frac{\ell - 1}{\ell - 2} \cdot \frac{\log(n)}{\log(\ell)} \geq \frac{\ell - 1}{\ell - 2} \cdot y > x \geq \frac{n - 1}{2}.
\]

But then \( n = 2 \), which contradicts that \( 5 \leq \ell \leq n \). Hence, indeed \( \tilde{f}_{S_m} \) must be trivial, and this completes the proof. \( \square \)

**Lemma 4.9.** We have \( N/M \simeq T \).

**Proof.** We have \( \text{Inn}(N/M) \simeq N/M \simeq T^m \). Depending on whether \( \tilde{f} \) is trivial or not, by Proposition 2.2(c) and Lemma 4.8, respectively, we see that there is a non-trivial homomorphism \( \varphi : G \to T^m \). Let \( 1 \leq i \leq m \) be such that
\[
\varphi^{(i)} : G \xrightarrow{\varphi} T^m \xrightarrow{\text{projection}} T^{(i)} \quad \text{(the } i\text{th copy of } T)\]
is non-trivial. Since \( \ker(\varphi^{(i)}) \) lies in \( Z(G) \) by (4.2), we have
\[
\frac{|T|^m |M|}{|Z(G)|} [Z(G) : \ker(\varphi^{(i)})] = \frac{|G|}{|\ker(\varphi^{(i)})|} = |\varphi^{(i)}(G)| = \frac{|T|}{[T^{(i)} : \varphi^{(i)}(G)]},
\]
and in particular
\[
(4.6) \quad |Z(G)| = |T|^{m-1} |M| [Z(G) : \ker(\varphi^{(i)})] [T^{(i)} : \varphi^{(i)}(G)].
\]
Suppose for contradiction that \( m \geq 2 \), in which case \( |T| \) divides \( |Z(G)| \) and hence \( m(G/Z(G)) \) by (4.1). Since all groups of order at most 48 are solvable, from Lemma 3.1 and (3.1), we see that
\[
G/Z(G) \simeq \text{PSL}_n(\ell^a), \text{PSU}_n(\ell^a), \text{ where } \ell \text{ is a prime, and } \ell \nmid |Z(G)|.
\]
But \( \ell \) divides \( |G| = |T|^m |M| \) by (4.3) and thus \( |T||M| \). This shows that (4.6) cannot hold, so indeed \( m = 1 \), and we have \( N/M \simeq T \). \( \square \)

For any \( \sigma \in G \), recall that \( \overline{h}(\sigma) = \text{conj}(\overline{g}(\sigma)) \cdot \tilde{f}(\sigma) \) by definition, and so
\[
(4.7) \quad \tilde{f}(\sigma) = \overline{h}(\sigma) \iff \overline{g}(\sigma) = 1_{N/M} \iff \sigma \in g^{-1}(M)
\]
because \( N/M \) has trivial center.

\[ x - 1 \geq x - y \geq \frac{n}{2} - \frac{1}{2} - 1 \] and so \( x \geq \frac{n - 1}{2} \).
Lemma 4.10. We have $G/Z(G) \simeq T$ and $|M| = |Z(G)|$.

Proof. By Lemma 4.8, the image $\tilde{f}(G)$ lies in $\text{Inn}(N/M)$, and so plainly $\tilde{h}(G)$ lies in $\text{Inn}(N/M)$ as well. Since $\text{Inn}(N/M) \simeq N/M$, we then have

$$|G/\ker(\tilde{f})|, |G/\ker(\tilde{h})| \leq |N/M|,$$

and so $|M| \leq |\ker(\tilde{f})|, |\ker(\tilde{h})|$. Trivially $\tilde{f}(\sigma) = \tilde{h}(\sigma)$ for all $\sigma \in \ker(\tilde{f}) \cap \ker(\tilde{h})$, so by (4.7) we have

$$|\ker(\tilde{f}) \cap \ker(\tilde{h})| \leq |g^{-1}(M)|, \text{ and } |g^{-1}(M)| = |M|$$

because $g$ is bijective. Since $\overline{\mathbf{f}}$ is surjective, we also have the factorization

$$\text{Inn}(N/M) = \tilde{f}(G)\tilde{h}(G),$$

whence $\tilde{f}(G)$ or $\tilde{h}(G)$ has trivial center by Lemmas 3.4 and 4.9. This implies that $\ker(\tilde{f}) \subset \ker(\tilde{h})$ or $\ker(\tilde{h}) \subset \ker(\tilde{f})$ has to hold, for otherwise $\ker(\tilde{f}), \ker(\tilde{h}) \leq Z(G)$ by (4.2), and both $\tilde{f}(G)$ and $\tilde{h}(G)$ would have non-trivial center. By symmetry, we may assume that the former inclusion holds. Then, from the above inequalities, we deduce that

$$|M| = |\ker(\tilde{f})|, \text{ and so } G/\ker(\tilde{f}) \simeq \text{Inn}(N/M) \simeq T$$

by comparing orders. But $\ker(\tilde{f})$ lies in $Z(G)$ again by (4.2), and $T$ has trivial center, so in fact $\ker(\tilde{f}) = Z(G)$. Both claims now follow. □

Lemma 4.11. Either $\tilde{f}$ or $\tilde{h}$ is trivial, and $Z(G) = g^{-1}(M)$.

Proof. Suppose for contradiction that both $\tilde{f}$ and $\tilde{h}$ are non-trivial. By (4.2), this means that both $\ker(\tilde{f})$ and $\ker(\tilde{h})$ lie in $Z(G)$. Since $G/\ker(\tilde{f}), G/\ker(\tilde{h})$ embed into $\text{Inn}(N/M)$, by comparing orders and by Lemma 4.10, we have

$$\ker(\tilde{f}) = Z(G) = \ker(\tilde{h}) \text{ and } \tilde{f}(G) = \text{Inn}(N/M) = \tilde{h}(G).$$

From (4.7), we then deduce that $Z(G) \subset g^{-1}(M)$, which must be an equality by Lemma 4.10 and the bijectivity of $g$. The above also implies that $\tilde{f}$ and $\tilde{h}$, respectively, induce isomorphisms

$$\varphi_f, \varphi_h : G/Z(G) \longrightarrow \text{Inn}(N/M), \text{ and } \varphi_h^{-1} \circ \varphi_f \in \text{Aut}(G/Z(G)).$$

But for any $\sigma \in G$, again by (4.7), we have

$$(\varphi_h^{-1} \circ \varphi_f)(\sigma Z(G)) = \sigma Z(G) \iff \sigma \in g^{-1}(M) \iff \sigma Z(G) = 1_{G/Z(G)}.$$
This contradicts Lemma 3.3. Thus, at least one of $\overline{f}$ or $\overline{h}$ is trivial.

Now, by Proposition 2.2(c),(d), the surjective map
\[
\varphi : G \longrightarrow N/M; \quad \varphi(\sigma) = \begin{cases} 
\overline{g}(\sigma) & \text{if } \overline{f} \text{ is trivial} \\
\overline{g}(\sigma)^{-1} & \text{if } \overline{h} \text{ is trivial}
\end{cases}
\]
is a homomorphism, and $\ker(\varphi)$ lies in $Z(G)$ by (4.2). By comparing orders, we see from Lemma 4.10 that in fact $\ker(\varphi) = Z(G)$. But in both cases, we have $\ker(\varphi) = g^{-1}(M)$ by definition, so the claim follows. □

**Lemma 4.12.** We have $M \subset Z(N)$.

*Proof.* Since $M$ is normal in $N$, we have a homomorphism
\[
\Phi : N \longrightarrow \text{Aut}(M) \longrightarrow \text{Out}(M)
\]
whose kernel clearly contains $M$. Either $\Phi$ is trivial or $\ker(\Phi) = M$ because $N/M$ is simple by Lemma 4.9.

Suppose first that $\Phi$ is trivial. This implies that
\[
N = MC, \text{ where } C \text{ is the centralizer of } M \text{ in } N.
\]
Given $i \in \mathbb{N}_{\geq 0}$ and a group $\Gamma$, let $\Gamma^{(i)}$ denote its $i$th derived subgroup. Since elements in $M$ and $C$ commute, we easily see that
\[
N^{(i)} = M^{(i)}C^{(i)} \text{ for all } i \in \mathbb{N}_{\geq 0}.
\]
By Lemma 4.11 and Proposition 2.3(c), there is a regular subgroup of $\text{Hol}(M)$ which is isomorphic to $Z(G)$. Since $Z(G)$ is abelian, it then follows from [20, Theorem 1.3(b)] that $M$ is metabelian, namely $M^{(2)} = 1$. Since $N$ is perfect, we deduce that
\[
N = N^{(1)} = N^{(2)} = M^{(2)}C^{(2)} = C^{(2)} \text{ and so } N = C.
\]
This means that all elements in $N$ centralize $M$, that is $M \subset Z(N)$.

Suppose now that $\ker(\Phi) = M$, in which case $N/M$ embeds into $\text{Out}(M)$. From Lemmas 4.9 and 4.10, we then see that
\[
G/Z(G) \text{ embeds into } \text{Out}(M), \text{ and recall } |M| = |Z(G)|.
\]
Notice that then $\text{Out}(M)$ and in particular $\text{Aut}(M)$ must be insolvable. Let $\mathcal{M} = \{1, 2, 3, 4, 6, 12\}$ be as in Lemma 3.1. We consider three cases.

1. $m(G/Z(G))$ lies in $\mathcal{M}$: By (4.1) we know that $|M| = |Z(G)|$ divides one of the numbers in $\mathcal{M}$. But we checked in MAGMA [2] that no such group $M$ has insolvable $\text{Aut}(M)$.

2. $G/Z(G) \cong \text{PSL}_3(4), \text{PSU}_4(3)$: Recall Lemma 3.1. Again by (4.1) we know that $|M| = |Z(G)|$ divides 48 or 36. Since $\text{Aut}(M)$ must be insolvable, we checked in MAGMA that $M$ has SMALLGROUP ID equal to one of

\[(4.8) \quad (8, 5), (16, 14), (24, 15), (48, 50), (48, 51), (48, 52),\]

and in particular $m(G/Z(G))$ is divisible by 8. Hence, we have

$$G/Z(G) \cong \text{PSL}_3(4), \text{ and note that } |\text{PSL}_3(4)| = 20160.$$  

Again, using the \texttt{OuterOrder} command, we computed in MAGMA that

$$|\text{Out}(M)| = 168, 20160, 336, 120, 1344, 40320,$$

respectively, when $M$ has SMALLGROUP ID in (4.8). Moreover, the group $M$ is abelian and there is no subgroup isomorphic to $\text{PSL}_3(4)$ in $\text{Aut}(M)$, when $M$ has SMALLGROUP ID equal to (16, 14), (48, 52). We then deduce that $G/Z(G)$ cannot embed into $\text{Out}(M)$.

3. $G/Z(G) \cong \text{PSL}_n(q), \text{PSU}_n(q)$ with $\text{PSL}_n(q), \text{PSU}_n(q)$ non-exceptional: We may assume that $M \neq 1$. Then, by [14, Corollary 3.3], we have

$$|\varphi| \leq |M| - 1 \text{ for all } \varphi \in \text{Aut}(M).$$

Since $|M| = |Z(G)|$, from (3.1) and (4.1), we deduce that

$$|\varphi \text{Inn}(M)| \leq |\varphi| \leq \min\{n - 1, q\} \text{ for all } \varphi \in \text{Aut}(M).$$

Since $\text{Aut}(M)$ is insolvable, we must have $n \geq 4$, and so $n = 2 + 1 + n_0$ for some integer $n_0 \geq 1$. But then $G/Z(G)$ would contain an element of order $q^2 - 1 > q$ by [3, Corollary 3(3)] and so cannot embed into $\text{Out}(M)$.

In all cases, we obtained a contradiction. Hence, the case $\ker(\Phi) = M$ in fact does not occur, so indeed $M \subset Z(N)$. \qed
We are now ready to prove Proposition 4.2.

Proof of Proposition 4.2. By Lemma 4.11, either $f$ or $h$ is trivial. Since $N$ is perfect, and $M \subset Z(N)$ by Lemma 4.12, the homomorphism

$$\text{Aut}(N) \longrightarrow \text{Aut}(N/M); \quad \varphi \mapsto (\eta M \mapsto \varphi(\eta)M)$$

is injective; see the proof of [16, Proposition 3.5(c)], for example. Therefore, either $f$ or $h$ is trivial. But clearly

$$G = \begin{cases} 
\rho(N) & \text{if } f \text{ is trivial,} \\
\lambda(N) & \text{if } h \text{ is trivial.}
\end{cases}$$

This completes the proof. $\square$

Acknowledgments

Research supported by the Young Scientists Fund of the National Natural Science Foundation of China (Award No.: 11901587).

The author thanks the referee for helpful comments.

References

[1] M. Aschbacher, *Finite group theory*. Second edition. Cambridge Studies in Advanced Mathematics, 10. Cambridge University Press, Cambridge, 2000.

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

[3] A. A. Buturlakin, *Spectra of finite linear and unitary groups* (Russian), Algebra Logika 47 (2008), no. 2, 157–173, 264; translation in Algebra Logic 47 (2008), no. 2, 91–99.

[4] N. P. Byott, *Uniqueness of Hopf-Galois structure of separable field extensions*, Comm. Algebra 24 (1996), no. 10, 3217–3228. Corrigendum, *ibid.* no. 11, 3705.

[5] N. P. Byott, *Hopf-Galois structures on field extensions with simple Galois groups*, Bull. London Math. Soc. 36 (1997), no. 1, 23–29.

[6] S. Carnahan and L. N. Childs, *Counting Hopf-Galois structures on non-abelian Galois field extensions*, J. Algebra 218 (1999), no. 1, 81–92.

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

[8] E. Fisman and Z. Arad, *A proof of Szep’s conjecture on nonsimplicity of certain finite groups*, J. Algebra 108 (1987), no. 2, 340–354.

[9] D. Gorenstein, *Finite simple groups. An introduction to their classification*. University Series in Mathematics. Plenum Publishing Corp., New York, 1982.

[10] C. Greither and B. Pareigis, *Hopf-Galois theory for separable field extensions*, J. Algebra 106 (1987), no. 1, 261–290.
[11] L. Guarnieri and L. Vendramin, *Skew braces and the Yang-Baxter equation*, Math. Comp. 86 (2017), no. 307, 2519–2534.

[12] R. M. Guralnick, *Subgroups of prime power index in a simple group*, J. Algebra 81 (1983), no. 2, 304–311.

[13] R. Guralnick, T. Penttila, C. E. Praeger, and J. Saxl, *Linear groups with orders having certain large prime divisors*, Proc. London Math. Soc. (3) 78 (1999), no. 1, 167–214.

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

[15] P. Kleidman and M. Liebeck, *The subgroup structure of the finite classical groups*. London Mathematical Society Lecture Note Series, 129. Cambridge University Press, Cambridge, 1990.

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

[17] C. Tsang, *Hopf-Galois structures of isomorphic-type on a non-abelian characteristically simple extension*, Proc. Amer. Math. Soc. 147 (2019), no. 12, 5093–5103.

[18] C. Tsang, *Hopf-Galois structures on a Galois $S_n$-extension*, J. Algebra 531 (2019), 349–361.

[19] C. Tsang, *On the multiple holomorph of a finite almost simple group*, New York J. Math. 25 (2019), 949–963.

[20] C. Tsang and C. Qin, *On the solvability of regular subgroups in the holomorph of a finite solvable group*, Internat. J. Algebra Comput. 30 (2020), no. 2, 253–265.

[21] C. Tsang, *Hopf-Galois structures on finite extensions with almost simple Galois group*, J. Number Theory 214 (2020), 286–311.

School of Mathematics (Zhuhai), Sun Yat-Sen University, Zhuhai, Guangdong, China

E-mail address: zengshy26@mail.sysu.edu.cn

URL: http://sites.google.com/site/cindysinyitsang/