HOPF-GALOIS STRUCTURES OF ISOMORPHIC TYPE ON A NON-ABELIAN CHARACTERISTICALLY SIMPLE EXTENSION

CINDY (SIN YI) TSANG

Abstract. Let $L/K$ be a finite Galois extension whose Galois group $G$ is non-abelian and characteristically simple. Using tools from graph theory, we shall give a closed formula for the number of Hopf-Galois structures on $L/K$ with associated group isomorphic to $G$.

Contents

1. Introduction 1
2. Regular subgroups arising from inner automorphisms 4
   2.1. Criteria for fixed point freeness 4
   2.2. Proof of Theorem 1.1: first statement 8
3. Regular subgroups arising from outer automorphisms 9
   3.1. Criteria for regularity 9
   3.2. Proof of Theorem 1.1: second statement 12
References 13

1. Introduction

Let $L/K$ be a finite Galois extension with Galois group $G$. Write $\text{Perm}(G)$ for the symmetric group of $G$. Recall that a subgroup $\mathcal{N}$ of $\text{Perm}(G)$ is said to be regular if the map

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

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

$$\begin{align*}
\lambda : G &\longrightarrow \text{Perm}(G); \quad \lambda(\sigma) = (\tau \mapsto \sigma \tau), \\
\rho : G &\longrightarrow \text{Perm}(G); \quad \rho(\sigma) = (\tau \mapsto \tau \sigma^{-1}),
\end{align*}$$

Date: November 29, 2018.
respectively, are plainly regular subgroups of $\text{Perm}(G)$. By work of C. Greither and B. Pareigis [8], each Hopf-Galois structure $\mathcal{H}$ on $L/K$ is associated to a regular subgroup $\mathcal{N}_{\mathcal{H}}$ of $\text{Perm}(G)$ which is normalized by $\lambda(G)$, and the type of $\mathcal{H}$ is defined to be the isomorphism class of $\mathcal{N}_{\mathcal{H}}$. In particular, for any finite group $N$ of the same order as $G$, there is a one-to-one correspondence between Hopf-Galois structures on $L/K$ of type $N$ and elements in

$$\mathcal{E}(G, N) = \left\{ \text{regular subgroups of } \text{Perm}(G) \text{ which are} \right. \left. \text{isomorphic to } N \text{ and normalized by } \lambda(G) \right\}.$$ 

The enumeration of this set has since become an active line of research. For example, see work of L. N. Childs, N. P. Byott, and T. Kohl. One important result, which was proven by N. P. Byott in [1], is the formula

$$\#\mathcal{E}(G, N) = \frac{|\text{Aut}(G)|}{|\text{Aut}(N)|} \cdot \# \left\{ \text{regular subgroups in } \text{Hol}(N) \right. \left. \text{which are isomorphic to } G \right\},$$

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

$$(1.1) \quad \text{Hol}(N) = \rho(N) \rtimes \text{Aut}(N).$$

In particular, it suffices to study the set

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

which is much easier to understand because of the nice description (1.1). See [5, Chapter 2] for more background on the study of Hopf-Galois structures.

In this paper, we shall be interested in the Hopf-Galois structures on $L/K$ of type $G$, or equivalently, the regular subgroups lying in $\mathcal{E}'(G, G)$. Let

$$\text{proj}_{\text{Aut}} : \text{Hol}(G) \longrightarrow \text{Aut}(G)$$

denote the projection map given by (1.1), and write $\text{Inn}(G)$ for the group of inner automorphisms on $G$. Define

$$\mathcal{E}'_{\text{inn}}(G, G) = \{\mathcal{N} \in \mathcal{E}'(G, G) : \text{proj}_{\text{Aut}}(\mathcal{N}) \subset \text{Inn}(G)\},$$

$$\mathcal{E}'_{\text{out}}(G, G) = \{\mathcal{N} \in \mathcal{E}'(G, G) : \text{proj}_{\text{Aut}}(\mathcal{N}) \not\subset \text{Inn}(G)\},$$

and we shall consider them separately. Let us remark that $\mathcal{E}'_{\text{inn}}(G, G)$ always

contains $\lambda(G)$ and $\rho(G)$, which coincide exactly when $G$ is abelian. Further, recall that a pair $(f, g)$ of endomorphisms on $G$ is said to be fixed point free if $f(\sigma) = g(\sigma)$ holds precisely when $\sigma = 1$. Then, by work of N. P. Byott and L. N. Childs in [3], such a pair gives rise to an element of $E'_{\text{inn}}(G, G)$, and

$$\#E'_{\text{inn}}(G, G) = \frac{1}{|\text{Aut}(G)|} \cdot \# \left\{ \text{fixed point free pairs } (f, g) \right\}$$

when $G$ has trivial center; see [3, Propositions 2 and 6].

In the proof of [4, Theorem 4], S. Carnahan and L. N. Childs showed that

$$\#E'_{\text{inn}}(G, G) = 2 \quad \text{and} \quad \#E'_{\text{out}}(G, G) = 0$$

when $G$ is non-abelian simple. Our main theorem is the following significant generalization of their result to the case when $G$ is non-abelian characteristically simple, that is, when $G$ is a direct product of copies of some non-abelian simple group.

**Theorem 1.1.** Suppose that $G$ is a direct product of $n \in \mathbb{N}$ copies of a finite non-abelian simple group $T$. Then, we have

$$\#E'_{\text{inn}}(G, G) = 2^n \cdot (n|\text{Aut}(T)| + 1)^{n-1} \quad \text{and} \quad \#E'_{\text{out}}(G, G) = 0.$$
where $\theta \in \text{Map}(\mathbb{N}_n, \mathbb{N}_{0,n})$, and for each $i \in \mathbb{N}_n$, we have

$$\varphi_i \in \text{Hom}(T^{\theta(i)}, T^{(i)}) \text{ such that } \begin{cases} \varphi_i \text{ is trivial} & \text{if } \theta(i) = 0, \\ \varphi_i \text{ is bijective} & \text{if } \theta(i) \neq 0. \end{cases}$$

Also, write $\text{Aut}^0(G)$ for the subgroup consisting of those which are automorphisms, or equivalently $\text{Aut}^0(G) = \text{Aut}(T) \wr S_n$. Here, the wreath product $\wr$ is the obvious one, with $S_n$ acting on $\mathbb{N}_n$, and $S_n$ is the symmetric group on $n$ letters. The consideration of $\text{End}^0(G)$ is motivated by the fact that

$$\text{End}(G) = \text{End}^0(G) \text{ and in particular } \text{Aut}(G) = \text{Aut}^0(G)$$

when $T$ is non-abelian simple; see the proof of [2, Lemma 3.2], for example. Using (1.4), as well as drawing tools from graph theory and group theory, respectively, we shall then prove the first and second equalities of Theorem 1.1.

2. Regular subgroups arising from inner automorphisms

2.1. Criteria for fixed point freeness. Throughout this subsection, consider a pair $(f, g)$ with $f, g \in \text{End}^0(G)$. Then, we have

$$f(x^{(1)}, \ldots, x^{(n)}) = (\varphi_{f,1}(x^{\theta_f(1)}), \ldots, \varphi_{f,n}(x^{\theta_f(n)})),$$

$$g(x^{(1)}, \ldots, x^{(n)}) = (\varphi_{g,1}(x^{\theta_g(1)}), \ldots, \varphi_{g,n}(x^{\theta_g(n)})),$$

where $\theta_f, \theta_g \in \text{Map}(\mathbb{N}_n, \mathbb{N}_{0,n})$, and $\varphi_{f,i}, \varphi_{g,i}$ are as in (1.3) for $i \in \mathbb{N}_n$. Put

$$\theta_f = (\theta_f(1), \ldots, \theta_f(n)) \text{ and } \theta_g = (\theta_g(1), \ldots, \theta_g(n)).$$

Using these $n$-tuples, we may associate $(f, g)$ to a graph as follows.

**Definition 2.1.** For any two $n$-tuples $\mu = (u_1, \ldots, u_n)$ and $\nu = (v_1, \ldots, v_n)$ with entries in $\mathbb{N}_{0,n}$, define $\Gamma_{\{\mu, \nu\}}$ to be the undirected multigraph with vertex set $\mathbb{N}_{0,n}$, and for each $i \in \mathbb{N}_n$, we draw one edge joining $u_i$ and $v_i$.

**Definition 2.2.** Define $\Gamma_{\{f,g\}}$ to be the undirected multigraph associated to the $n$-tuples $\theta_f$ and $\theta_g$. Define $\Gamma_{\{f,g\}}$ to be the directed multigraph with vertex set $\mathbb{N}_{0,n}$, and for each $i \in \mathbb{N}_n$, we draw one arrow $a_i$ from $\theta_f(i)$ to $\theta_g(i)$ if $\varphi_{g,i}$ is bijective, as well as one arrow $b_i$ from $\theta_g(i)$ to $\theta_f(i)$ if $\varphi_{f,i}$ is bijective.
Note that by the condition in (1.3), the multigraph $\Gamma_{(f,g)}$ may be obtained from $\Gamma_{\{f,g\}}$ via the following operations:

- Remove every loop at the vertex 0.
- Replace every edge $0 \rightarrow i$ by the arrow $0 \rightarrow i$ when $i \neq 0$.
- Replace every edge $i \rightarrow j$ by the pair of arrows $i \leftarrow j$ when $i, j \neq 0$.

We shall illustrate Definition 2.2 via the following example.

**Example 2.3.** Take $n = 4$. Suppose that

\[
\begin{align*}
    f(x^{(1)}, x^{(2)}, x^{(3)}, x^{(4)}) &= (\varphi_{f,1}(x^{(0)}), \varphi_{f,2}(x^{(1)}), \varphi_{f,3}(x^{(2)}), \varphi_{f,4}(x^{(3)})), \\
    g(x^{(1)}, x^{(2)}, x^{(3)}, x^{(4)}) &= (\varphi_{g,1}(x^{(0)}), \varphi_{g,2}(x^{(0)}), \varphi_{g,3}(x^{(1)}), \varphi_{g,4}(x^{(3)})),
\end{align*}
\]

where the $\varphi_{f,i}, \varphi_{g,i}$ are as in (1.3). Then, according to Definition 2.2, we have

\[
\begin{array}{c}
    0 \quad 1 \quad 2 \\
    3 \quad 4
\end{array}
\quad \text{and} \quad
\begin{array}{c}
    0 \rightarrow 1 \leftrightarrow 2 \\
    3 \leftrightarrow 4
\end{array}
\]

for the graphs $\Gamma_{\{f,g\}}$ and $\Gamma_{(f,g)}$, respectively.

Let us briefly explain the ideas behind Definition 2.2. For each $i \in \mathbb{N}_n$, the corresponding edge joining $\theta_f(i)$ and $\theta_g(i)$ may be viewed as representing the equation $\varphi_{f,i}(x^{\theta_f(i)}) = \varphi_{g,i}(x^{\theta_g(i)})$, while the arrows $a_i$ and $b_i$ may be regarded as the homomorphisms

\[
\begin{align*}
    \gamma_{a_i} &= \varphi_{g,i}^{-1} \circ \varphi_{f,i} \quad \text{if } \varphi_{g,i} \text{ is bijective}, \\
    \gamma_{b_i} &= \varphi_{f,i}^{-1} \circ \varphi_{g,i} \quad \text{if } \varphi_{f,i} \text{ is bijective},
\end{align*}
\]

respectively. Given a directed path $p$ in $\Gamma_{(f,g)}$, we may write it as a concatenation of arrows, say

\[
p = c_{i_m} \cdots c_{i_1}, \quad \text{where } c_{i_k} \in \{a_{i_k}, b_{i_k}\} \text{ for each } 1 \leq k \leq m,
\]

and the concatenation is from right to left. Define

\[
\gamma_p = \gamma_{c_{i_m}} \circ \cdots \circ \gamma_{c_{i_1}}
\]

in this case. Then, we clearly have the following lemma:
Lemma 2.4. Let $\sigma = (\sigma^{(1)}, \ldots, \sigma^{(n)}) \in G$. Then, we have $f(\sigma) = g(\sigma)$ if and only if $\sigma^{(h(p))} = \gamma_p(\sigma^{(t(p))})$ holds for all directed paths $p$ in $\Gamma_{(f,g)}$, where $h(p)$ and $t(p)$ denote its head and tail, respectively.

Let us note that Definition 2.2 and the forward implication of Lemma 2.4 are still valid even if $\varphi_{f,i}, \varphi_{g,i}$ are only non-trivial but not necessarily bijective for $\theta_f(i), \theta_g(i) \neq 0$. However, the analysis for determining when $(f, g)$ is fixed point free is much more complicated. For the purpose of this paper, we have thus restricted to the situation when the condition in (1.3) holds.

We shall now give criteria for $(f, g)$ to be fixed point free in terms of properties of $\Gamma_{(f,g)}$. Let us point out that the condition in (1.3) is crucial for some of the arguments to hold. In particular, it ensures that if we have a path in $\Gamma_{(f,g)}$ joining $i$ and $j$, then we also have a directed path in $\Gamma_{(f,g)}$ from $i$ to $j$, unless $j = 0$.

Recall that a tree is a connected graph which has no cycle. Equivalently, a tree is a graph in which any two vertices can be connected by a unique simple path. For a graph $\Gamma$ with $m$ vertices, it is known that $\Gamma$ is a tree if and only if $\Gamma$ is connected and has exactly $m - 1$ edges, for any $m \in \mathbb{N}$.

Proposition 2.5. If $\Gamma_{(f,g)}$ is a tree, then $(f, g)$ is fixed point free.

Proof. Suppose that $\Gamma_{(f,g)}$ is a tree. By the connectedness of $\Gamma_{(f,g)}$ and (1.3), for each $i \in \mathbb{N}_n$, we have a directed path $p_i$ in $\Gamma_{(f,g)}$ from 0 to $i$. Hence, whenever $f(\sigma) = g(\sigma)$, where $\sigma = (\sigma^{(1)}, \ldots, \sigma^{(n)}) \in G$, we have $\sigma^{(i)} = \gamma_{p_i}(\sigma^{(0)}) = 1$ for all $i \in \mathbb{N}_n$ by Lemma 2.4. This shows that $(f, g)$ is fixed point free. \[ \square \]

However, the converse of Proposition 2.5 is false in general. As the next example shows, the issue lies in the existence of fixed point free automorphisms $\varphi$ on $T$, that is $\varphi(\sigma) = \sigma$ holds precisely when $\sigma = 1$.

Example 2.6. Take $n = 2$. Suppose that

$$f(x^{(1)}, x^{(2)}) = (\varphi_{f,1}(x^{(1)}), \varphi_{f,2}(x^{(2)})),$$

$$g(x^{(1)}, x^{(2)}) = (\varphi_{g,1}(x^{(1)}), \varphi_{g,2}(x^{(2)})).$$
where the $\varphi_{f,i}, \varphi_{g,i}$ are as in (1.3). It is clear that $(f, g)$ is fixed point free as long as both $\varphi_{f,1}^{-1} \circ \varphi_{g,1}$ and $\varphi_{f,2}^{-1} \circ \varphi_{g,2}$ are fixed point free automorphisms.

Nevertheless, we have the following partial converses of Proposition 2.5.

**Proposition 2.7.** If $(f, g)$ is fixed point free, then the connected component of $\Gamma_{\{f,g\}}$ containing 0 is a tree, and the other connected components of $\Gamma_{\{f,g\}}$ have the same number of edges and vertices.

**Proof.** Suppose that $(f, g)$ is fixed point free. Let $\Gamma_0, \Gamma_1, \ldots, \Gamma_r$, with $r \geq 0$, denote the connected components of $\Gamma_{\{f,g\}}$, such that 0 lies in $\Gamma_0$. For each $0 \leq k \leq r$, write $v_k$ and $e_k$, respectively, for the number of vertices and edges in $\Gamma_k$, as well as note that $e_k \geq v_k - 1$ because $\Gamma_k$ is connected. Also, we have

$$n + 1 = v_0 + v_1 + \cdots + v_r$$

and

$$n = e_0 + e_1 + \cdots + e_r$$

by definition. Below, we shall show that $e_k \geq v_k$ for all $1 \leq k \leq r$. Together with the above equalities, this implies that $e_0 \leq v_0 - 1$. We then deduce that in fact $e_0 = v_0 - 1$, namely $\Gamma_0$ is a tree, and that $e_k = v_k$ for $1 \leq k \leq r$.

Suppose for contradiction that $e_{k_0} = v_{k_0} - 1$, namely $\Gamma_{k_0}$ is a tree, for some $1 \leq k_0 \leq r$. Let $i_0$ be any vertex in $\Gamma_{k_0}$ and fix some non-trivial element $\sigma^{(i_0)}$ in $T^{(i_0)}$. For any vertex $i \neq i_0$ in $\Gamma_{k_0}$, by connectedness and (1.3), there is a directed path $p_i$ in $\Gamma_{\{f,g\}}$ from $i_0$ to $i$. Plainly $\gamma_{p_i}$ is independent of the choice of $p_i$ because $\Gamma_{\{f,g\}}$ contains no cycle. For $i \neq i_0$, define

$$\sigma^{(i)} = \begin{cases} \\
\gamma_{p_i}(\sigma^{(i_0)}) & \text{if } i \text{ is in } \Gamma_{k_0}, \\
1 & \text{if } i \text{ is not in } \Gamma_{k_0},
\end{cases}$$

and put $\sigma = (\sigma^{(1)}, \ldots, \sigma^{(n)})$ But then $f(\sigma) = g(\sigma)$ by Lemma 2.4 and $\sigma \neq 1$. This contradicts that $(f, g)$ is fixed point free. \qed

**Proposition 2.8.** Suppose that $T$ does not admit any fixed point free automorphism. If $(f, g)$ is fixed point free, then $\Gamma_{\{f,g\}}$ is a tree.

**Proof.** Suppose that $(f, g)$ is fixed point free. Suppose also for contradiction that $\Gamma_{\{f,g\}}$ is not a tree, namely it is not connected, and let $\Gamma_*$ be a connected component not containing 0. By Proposition 2.7, we have exactly one simple
cycle in $\Gamma_*$. Then, by (1.3), we have a corresponding directed simple cycle $q$ in $\Gamma_{(f,g)}$, based at the vertex $i_0$ say. Note that $\gamma_q$ is an automorphism on $T^{(i_0)}$, which cannot be fixed point free by hypothesis, and hence $\gamma_q(\sigma^{(i_0)}) = \sigma^{(i_0)}$ for some non-trivial element $\sigma^{(i_0)}$ in $T^{(i_0)}$.

As in the proof of Proposition 2.7, for any vertex $i \neq i_0$ in $\Gamma_*$, by connectedness and (1.3), there exists a directed path $p_i$ in $\Gamma_{(f,g)}$ from $i_0$ to $i$. Notice that $\gamma_{p_i}$ might depend on the choice of $p_i$, but $\gamma_{p_i}(\sigma^{(i_0)})$ does not, because $\Gamma_*$ has a unique simple cycle and $\gamma_q(\sigma^{(i_0)}) = \sigma^{(i_0)}$. For $i \neq i_0$, define

$$
\sigma^{(i)} = \begin{cases} 
\gamma_{p_i}(\sigma^{(i_0)}) & \text{if } i \text{ is in } \Gamma_*, \\
1 & \text{if } i \text{ is not in } \Gamma_*,
\end{cases}
$$

and put $\sigma = (\sigma^{(1)}, \ldots, \sigma^{(n)})$. But then $f(\sigma) = g(\sigma)$ by Lemma 2.4 and $\sigma \neq 1$. This contradicts that $(f, g)$ is fixed point free. \hfill \Box

**Remark 2.9.** By the classification theorem of finite simple groups, any finite insolvable group has no fixed point free automorphism; see [7, Theorem 1.48].

### 2.2. Proof of Theorem 1.1: first statement.

Put

$$
\mathcal{F}(G, G) = \{(f, g) \in \text{End}^0(G) \times \text{End}^0(G) : \Gamma_{\{f, g\}} \text{ is a tree}\}.
$$

First, we shall prove the following general statement:

**Proposition 2.10.** We have

$$
\#\mathcal{F}(G, G) = 2^n \cdot n! \cdot |\text{Aut}(T)|^n \cdot (n|\text{Aut}(T)| + 1)^{n-1}.
$$

**Proof.** Observe that for any tree $\Gamma$ with vertex set $\mathbb{N}_{0,n}$, which by definition has exactly $n$ edges, we have the equality

$$
\#\{(\mu, \nu) \in (\mathbb{N}_{0,n})^n \times (\mathbb{N}_{0,n})^n : \Gamma_{\{\mu, \nu\}} = \Gamma\} = 2^n \cdot n!.
$$

This is because we have $2^n \cdot n!$ ways to pick an orientation for each edge and then label the $n$ arrows as $e_i$ for $i \in \mathbb{N}_n$. Once such a choice is made, define the $i$th entries of $\mu$ and $\nu$, respectively, to be the tail and the head of $e_i$. We then have $\Gamma_{\{\mu, \nu\}} = \Gamma$, and the fact that $\Gamma$ has no cycle implies that different choices give rise to different pairs $(\mu, \nu)$. 

Now, for any $\mu, \nu \in (\mathbb{N}_0, n)^n$, say $\mu = (u_1, \ldots, u_n)$ and $\nu = (v_1, \ldots, v_n)$, put
\[ d(\mu, \nu) = \#\{ i \in \mathbb{N}_0, n : u_i = 0 \} + \#\{ i \in \mathbb{N}_0, n : v_i = 0 \}, \]
which is also equal to the degree of the vertex 0 in $\Gamma_{\{\mu, \nu\}}$. Then, we have
\[ \# \{ (f, g) \in \text{End}^0(G) \times \text{End}^0(G) : (\Theta_f, \Theta_g) = (\mu, \nu) \} = |\text{Aut}(T)|^{2n - d(u, v)} \]
by (1.3), and note that for $\Gamma_{\{\mu, \nu\}}$ to be a tree, necessarily $1 \leq d(\mu, \nu) \leq n$.

For each $1 \leq d \leq n$, let $T_n(d)$ denote the number of trees with vertex set $\mathbb{N}_0, n$ in which the vertex 0 has degree $d$, where two such trees are regarded as distinct if and only if there is a pair of vertices which are joined by an edge in one tree but not in the other. Then, the above discussion implies that
\[ \# \mathcal{F}(G, G) = \sum_{d=1}^{n} (T_n(d) \cdot 2^n \cdot n! \cdot |\text{Aut}(T)|^{2n-d}). \]
For each $1 \leq d \leq n$, it was shown in [6] that
\[ T_n(d) = \binom{n-1}{d-1} n^{n-d}. \]
A simple calculation using the binomial theorem then yields the claim. \(\square\)

Now, suppose that $T$ is non-abelian simple. Then, for any $f, g \in \text{End}^0(G)$, the pair $(f, g)$ is fixed point free precisely when $\Gamma_{\{f, g\}}$ is a tree, by Propositions 2.5 and 2.8 as well as Remark 2.9. From (1.2) and (1.4), we see that
\[ \# \mathcal{E}'_{\text{inn}}(G, G) = \frac{1}{|\text{Aut}^0(G)|} \cdot \# \mathcal{F}(G, G) = \frac{1}{|\text{Aut}(T)|^{n} \cdot n!} \cdot \# \mathcal{F}(G, G) \]
The first claim in Theorem 1.1 is then immediate from Proposition 2.10.

3. Regular subgroups arising from outer automorphisms

3.1. Criteria for regularity. Throughout this subsection, consider a subgroup $\mathcal{N}$ of $\text{Hol}(G)$ isomorphic to $G$, with $\text{proj}_{\text{Aut}}(\mathcal{N}) \subset \text{Aut}^0(G)$. As noted in [9, Proposition 2.1], which follows from (1.1), we have
\[ \mathcal{N} = \{ \rho(g(\sigma)) \cdot \hat{f}(\sigma) : \sigma \in G \}, \]
where
\[ \begin{cases} \hat{f} \in \text{Hom}(G, \text{Aut}^0(G)) \\ g \in \text{Map}(G, G) \end{cases} \]
are such that
\[ g(\sigma \tau) = g(\sigma) \cdot f(\sigma)(g(\tau)) \] for all \( \sigma, \tau \in G \).

Moreover, as one easily sees, we have

\[ \mathcal{N} \text{ is regular if and only if } g \text{ is bijective.} \]  

(3.2)

Recall that by definition, we have

\[ \text{Aut}^0(G) = \text{Aut}(T) \wr S_n = \text{Aut}(T)^n \rtimes S_n, \]

and define \( f_{S_n} \) to be the homomorphism \( f \) composed with the natural projection map \( \text{Aut}^0(G) \longrightarrow S_n \). Let us first make the following observation, which is motivated by an argument in [4, p. 84].

**Proposition 3.1.** Suppose that the outer automorphism group \( \text{Out}(T) \) of \( T \) is solvable and that \( \ker(f_{S_n}) \) is perfect. Then, we have \( f(\ker(f_{S_n})) \subset \text{Inn}(G) \).

**Proof.** Observe that the homomorphism

\[ \ker(f_{S_n}) \xrightarrow{f} \text{Aut}(T)^n \xrightarrow{\text{quotient}} \text{Out}(T)^n, \]

is trivial because \( \ker(f_{S_n}) \) is perfect but \( \text{Out}(T) \) is solvable. Thus, indeed the image of \( \ker(f_{S_n}) \) under \( f \) lies in \( \text{Inn}(T)^n \), which is equal to \( \text{Inn}(G) \). \( \square \)

**Remark 3.2.** By Schreier’s conjecture, which is a consequence of the classification theorem of finite simple groups, the outer automorphism group of any finite non-abelian simple group is solvable; see [7, Theorem 1.46].

Below, we shall study the case when \( \ker(f_{S_n}) \nsubseteq G \), and investigate when it is possible for \( \mathcal{N} \) to be regular, or equivalently, for \( g \) to be bijective.

Given any \( \sigma \in G \), the assumption that \( f(G) \) lies in \( \text{Aut}^0(G) \) implies

\[ f(\sigma)(x^{(1)}, \ldots, x^{(n)}) = (\varphi_{\sigma,1}(x^{(\theta_{\sigma}(1))}), \ldots, \varphi_{\sigma,n}(x^{(\theta_{\sigma}(n))})), \]

where \( \theta_{\sigma} = f_{S_n}(\sigma) \), and \( \varphi_{\sigma,i} \in \text{Aut}(T) \) sends \( T^{(\theta_{\sigma}(i))} \) to \( T^{(i)} \). Also, write

\[ g(\sigma) = (a_{\sigma}^{(1)}, \ldots, a_{\sigma}^{(n)}). \]

In the above notation, we then have the following.
Lemma 3.3. Let $\sigma, \tau \in G$ be such that $\sigma \tau = \tau \sigma$ and $\tau \in \ker(f_{S_n})$. Then, for all $i \in \mathbb{N}_n$, we have the relation
\[
\varphi_{\sigma,i}(a_{\sigma}^{(\theta_{\sigma}(i))}) = (a_{\sigma}^{(i)})^{-1} \cdot a_{\sigma}^{(i)} \cdot \varphi_{\tau,i}(a_{\sigma}^{(i)}).
\]

Proof. The hypothesis $\tau \in \ker(f_{S_n})$ implies that
\[
g(\sigma \tau) = g(\sigma) \cdot f(\sigma)(g(\tau)) = (a_{\sigma}^{(1)} \varphi_{\sigma,1}(a_{\sigma}^{(\theta_{\sigma}(1))}), \ldots, a_{\sigma}^{(n)} \varphi_{\sigma,n}(a_{\sigma}^{(\theta_{\sigma}(n))})),
\]
\[
g(\tau \sigma) = g(\tau) \cdot f(\tau)(g(\sigma)) = (a_{\tau}^{(1)} \varphi_{\tau,1}(a_{\sigma}^{(1)}), \ldots, a_{\tau}^{(n)} \varphi_{\tau,n}(a_{\sigma}^{(n)})).
\]
Since $\sigma \tau = \tau \sigma$, the claim is now clear. \hfill \square

In what follows, fix a prime $p$ dividing $|T|$. For each $i \in \mathbb{N}_n$, further choose a subgroup $P^{(i)}$ of $T^{(i)}$ of order $p$, and put
\[
(3.3) \quad H = P^{(1)} \times \cdots \times P^{(n)},
\]
which is an elementary abelian $p$-group of rank $n$. Write $m \geq 0$ for the rank of $f_{S_n}(H)$, and let us consider the $f_{S_n}(H)$-action on $\mathbb{N}_n$; the restriction to the subgroup $H$ is only for convenience. We may decompose
\[
\mathbb{N}_n = X_0 \sqcup X_1 \sqcup \cdots \sqcup X_r, \text{ with } r \geq 0,
\]
where $X_0$ is the set of fixed points and $X_1, \ldots, X_r$ are the non-trivial orbits of $\mathbb{N}_n$ under the $f_{S_n}(H)$-action. For each $1 \leq k \leq r$, let us fix a representative $i_k \in X_k$, and for each $i \in X_k$, choose an element $\sigma_i \in H$ such that $\theta_{\sigma_i}(i_k) = i$.

Lemma 3.4. Suppose that for all $i \in \mathbb{N}_n$, the element $\sigma_i \in H$ commutes with every element of $\ker(f_{S_n})$. Then, the image of $\ker(f_{S_n})$ under $g$ lies in the set
\[
\prod_{i \in X_0} T^{(i)} \times \prod_{k=1}^{r} \prod_{i \in X_k} \varphi_{\sigma_i,i_k}^{-1} \left( (a_{\sigma_i}^{(i_k)})^{-1} \cdot a \cdot \varphi(a_{\sigma_i}^{(i_k)}) \right) : a \in T^{(i_k)}, \varphi \in \text{Aut}(T^{(i_k)}).
\]
Moreover, in the case that $f(\ker(f_{S_n})) \subset \text{Inn}(G)$, for each $1 \leq k \leq r$, we may replace $\text{Aut}(T^{(i_k)})$ by $\text{Inn}(T^{(i_k)})$ in the above, and in particular, we have
\[
(3.4) \quad \#g(\ker(f_{S_n})) \leq |T|^{\#X_0} \cdot (|T| |\text{Inn}(T)|)^r \leq |T|^{\#X_0 + 2r}.
\]

Proof. This follows immediately from Lemma 3.3. \hfill \square
Lemma 3.5. For each $1 \leq k \leq r$, we have $\#X_k = p^{m_k}$ for some $m_k \in \mathbb{N}$. In addition, we have the relations

$$n - \#X_0 = \sum_{k=1}^{r} p^{m_k} \text{ and } m \leq \sum_{k=1}^{r} m_k.$$ 

Proof. The first claim is clear because $X_1, \ldots, X_r$ are non-trivial orbits under the action of a $p$-group. The equality is also obvious from the definition.

To prove the inequality, recall that $m$ is the rank of the elementary abelian group $\mathfrak{f}_{S_n}(H)$. Given any subset $X$ of $\mathbb{N}_n$, write $S_X$ for its symmetric group regarded as a subgroup of $S_n$. For each $1 \leq k \leq r$, define $\Delta_k$ to be the image, which is an elementary abelian group, of the homomorphism

$$\mathfrak{f}_{S_n}(H) \xrightarrow{\text{inclusion}} S_n \xrightarrow{\theta \mapsto \theta|X_k} S_{X_k} \xrightarrow{\text{inclusion}} S_n.$$ 

Plainly, the $\Delta_k$-action on $X_k$ is transitive. For any $\theta \in \mathfrak{f}_{S_n}(H)$, since $\mathfrak{f}_{S_n}(H)$ is abelian, if $\theta$ fixes an element of the orbit $X_k$, then $\theta$ fixes all elements of $X_k$. This means the $\Delta_k$-action on $X_k$ is also free. Thus, we have $|\Delta_k| = \#X_k$, and so $\Delta_k$ has rank equal to $m_k$. Observe that $\mathfrak{f}_{S_n}(H)$ is generated by $\Delta_1, \ldots, \Delta_r$. We then see that the stated inequality holds. \qed

Proposition 3.6. Suppose that $\mathfrak{f}_{S_n}(H) \neq 1$ and that $|\mathfrak{f}_{S_n}(G)| = |T|^m$. If $g$ is bijective and (3.4) holds, then necessarily $p \leq 3$.

Proof. The hypothesis implies that $r \geq 1$ and that $|\ker(\mathfrak{f}_{S_n})| = |T|^{n-m}$. Suppose now that $g$ is bijective and that (3.4) holds. Then, we have

$$|T|^n - |T|^m \leq |T|^{|X_0| + 2r} \text{ and so } n - \#X_0 \leq 2r + m.$$ 

Using Lemma 3.5, we further deduce that

$$\sum_{k=1}^{r} p^{m_k} \leq 2r + \sum_{k=1}^{r} m_k \text{ and so } \sum_{k=1}^{r} (p^{m_k} - 2) \leq \sum_{k=1}^{r} m_k.$$ 

For $p \geq 5$, we have $p^x - 2 > x$ for all $x \geq 1$. Hence, we must have $p \leq 3$ for the above inequality to hold. \qed

3.2. Proof of Theorem 1.1: second statement. Suppose that $T$ is non-abelian simple. Consider a subgroup $\mathcal{N}$ of $\text{Hol}(G)$ which is isomorphic to $G$. 
By (1.4), it must have the shape (3.1), and we may use the same notation as in the previous subsection. It is well-known and is not hard to show that the normal subgroups of $G$ are exactly all the products among $T^{(1)}, \ldots, T^{(n)}$. In particular, there exists $0 \leq m \leq n$ and $i_1, \ldots, i_{n-m} \in \mathbb{N}_n$ such that

$$\ker(f_{S_n}) = T^{(i_1)} \times \cdots \times T^{(i_{n-m})}. \quad (3.5)$$

Observe that the $m$ here coincides with the $m$ defined after (3.3). Also, the above implies that $|f_{S_n}(G)| = |T|^m$, a hypothesis in Proposition 3.6. Further, it implies that for all $i \in \mathbb{N}_n$, we may choose $\sigma_i \in H$ to commute with every element of $\ker(f_{S_n})$, a hypothesis of Lemma 3.4.

Now, suppose that $f(G) \not\subset \text{Inn}(G)$. By Proposition 3.1 and Remark 3.2, we have $f(\ker(f_{S_n})) \subset \text{Inn}(G)$, whence the inequality (3.4) holds. Also, we have $f_{S_n}(G) \neq 1$, which implies that $f_{S_n}(H) \neq 1$ by (3.5), and thus Proposition 3.6 applies. It follows that if $\mathcal{N}$ were regular, which means that $g$ is bijective by (3.2), then $|T|$ would be divisible only by the primes $p \leq 3$. This is impossible since $T$ is non-abelian simple. The second claim in Theorem 1.1 then follows.

References

[1] 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.

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

[3] N. P. Byott and L. N. Childs, *Fixed-point free pairs of homomorphisms and nonabelian Hopf-Galois structures*, New York J. Math. 18 (2012), 707–731.

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

[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] L. E. Clarke, *On Cayley’s formula for counting trees*, J. London Math. Soc. 33 (1958), 471–474.

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

[8] C. Greither and B. Pareigis, *Hopf-Galois theory for separable field extensions*, J. Algebra 106 (1987), no. 1, 261–290.

[9] C. Tsang, *Non-existence of Hopf-Galois structures and bijective crossed homomorphism*, to appear in J. Pure Appl. Algebra.

School of Mathematics, Sun Yat-Sen University, Zhuhai

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

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