On the multiple holomorph of a finite almost simple group

Cindy (Sin Yi) Tsang

ABSTRACT. Let G be a group. Let $\mathrm{Perm}(G)$ denote its symmetric group and write $\mathrm{Hol}(G)$ for the normalizer of the subgroup of left translations in $\mathrm{Perm}(G)$. The multiple holomorph $\mathrm{NHol}(G)$ of G is defined to be the normalizer of $\mathrm{Hol}(G)$ in $\mathrm{Perm}(G)$. In this paper, we shall show that the quotient group $\mathrm{NHol}(G)/\mathrm{Hol}(G)$ has order two whenever G is finite and almost simple. As an application of our techniques, we shall also develop a method to count the number of Hopf-Galois structures of isomorphic type on a finite almost simple field extension in terms of fixed point free endomorphisms.

CONTENTS

1. Introduction

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

$$\xi_N : N \longrightarrow G; \quad \xi_N(\eta) = \eta(1_G)$$

is bijective, or equivalently, if the N-action on G is both transitive and free. For example, both $\lambda(G)$ and $\rho(G)$ are regular subgroups of $\mathrm{Perm}(G)$, where

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

denote the left and right regular representations of G, respectively. Plainly, we have $\lambda(G)$ are $\rho(G)$ are equal precisely when G is abelian. Recall further that the *holomorph of G* is defined to be

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

Alternatively, it is not hard to verify that

$$\mathrm{Norm}_{\mathrm{Perm}(G)}(\lambda(G)) = \mathrm{Hol}(G) = \mathrm{Norm}_{\mathrm{Perm}(G)}(\rho(G)).$$

Then, it seems natural to ask whether $\mathrm{Perm}(G)$ has other regular subgroups which also have normalizer equal to $\mathrm{Hol}(G)$. Given any regular subgroup N of $\mathrm{Perm}(G)$, observe that the bijection ξ_N induces an isomorphism

$$\Xi_N : \mathrm{Perm}(N) \longrightarrow \mathrm{Perm}(G); \quad \Xi_N(\pi) = \xi_N \circ \pi \circ \xi_N^{-1} \tag{1.2}$$

under which $\lambda(N)$ is sent to N. Thus, in turn Ξ_N induces an isomorphism

$$\mathrm{Hol}(N) \simeq \mathrm{Norm}_{\mathrm{Perm}(G)}(N),$$

and so we have

$$\mathrm{Norm}_{\mathrm{Perm}(G)}(N) = \mathrm{Hol}(G) \text{ implies } \mathrm{Hol}(N) \simeq \mathrm{Hol}(G).$$

However, in general, the converse is false, and non-isomorphic groups (of the same order) can have isomorphic holomorphs. Let us restrict to the regular subgroups N which are isomorphic to G, and consider

$$\mathcal{H}_0(G) = \left\{ \begin{array}{c} \text{regular subgroups } N \text{ of } \mathrm{Perm}(G) \text{ isomorphic to } G \\ \text{and such that } \mathrm{Norm}_{\mathrm{Perm}(G)}(N) = \mathrm{Hol}(G) \end{array} \right\}.$$

This set was first studied by G. A. Miller [13]. More specifically, he defined the *multiple holomorph of G* to be

$$\mathrm{NHol}(G) = \mathrm{Norm}_{\mathrm{Perm}(G)}(\mathrm{Hol}(G)),$$

which clearly acts on $\mathcal{H}_0(G)$ via conjugation, and he showed that this action is transitive so the quotient group

$$T(G) = \frac{\mathrm{NHol}(G)}{\mathrm{Hol}(G)}$$

acts regularly on $\mathcal{H}_0(G)$; or see Section 2 below for a proof. In [13], he also determined the structure of $T(G)$ for finite abelian groups G. Later in [14], W. H. Mills extended this to all finitely generated abelian groups G, which was also redone in [4] using a different approach. Initially, the study of $T(G)$ did not attract much attention, except in [13] and [14]. But recently in [12], T. Kohl revitalized this line of research by computing $T(G)$ for dihedral and dicyclic groups G. In turn, his work motivated the calculation of $T(G)$ for

some other families of finite groups G; see [5] and [3]. In this paper, we shall continue this research and compute $T(G)$ for finite almost simple groups G.

To explain our motivation, first notice that elements of $\mathcal{H}_0(G)$ are normal subgroups of $\mathrm{Hol}(G)$; this is known and also see Section 2 below for a proof. Instead of $\mathcal{H}_0(G)$, let us consider the possibly larger sets

$$\mathcal{H}_1(G) = \{\text{normal and regular subgroups of } \mathrm{Hol}(G)\},$$

$$\mathcal{H}_2(G) = \{\text{regular subgroups of } \mathrm{Hol}(G) \text{ isomorphic to } G\}.$$

Then, we have the inclusions

$$\mathcal{H}_0(G) \subset \mathcal{H}_1(G) \text{ and } \mathcal{H}_0(G) \subset \mathcal{H}_2(G).$$

If G is finite and non-abelian simple, then we know that

$$\mathcal{H}_2(G) = \{\lambda(G), \rho(G)\}$$

by the proof of [6, Theorem 4], and this in turn implies that

$$\mathcal{H}_0(G) = \{\lambda(G), \rho(G)\} \text{ whence } T(G) \simeq \mathbb{Z}/2\mathbb{Z}. \tag{1.3}$$

Inspired by this observation, it seems natural to ask whether the same or at least a similar phenomenon holds for other finite groups G which are close to being non-abelian simple. Let us consider the following three generalizations of non-abelian simple groups.

Definition 1.1. A group G is said to be
  (1) *quasisimple* if $G = [G, G]$ and $G/Z(G)$ is simple, where $[G, G]$ is the commutator subgroup and $Z(G)$ is the center of G.
  (2) *characteristically simple* if it has no non-trivial proper characteristic subgroup; let us note that for finite G, this is equivalent to $G = T^n$ for some simple group T and natural number n.
  (3) *almost simple* if $\mathrm{Inn}(T) \leq G \leq \mathrm{Aut}(T)$ for some non-abelian simple group T, where $\mathrm{Inn}(T)$ denotes the inner automorphism group of T; let us remark that $\mathrm{Inn}(T)$ is the socle of G in this case, as shown in Lemma 4.2 below, for example.

If G is finite and quasisimple, then we know that

$$\mathcal{H}_2(G) = \{\lambda(G), \rho(G)\}$$

by [16, (1.1) and Theorem 1.3], whence (1.3) holds as above. However, if G is finite and non-abelian characteristically simple or almost simple, then the size of $\mathcal{H}_2(G)$ can be arbitrarily large as the order of G increases, by [17] and [6, Theorem 5]. Nevertheless, if G is finite and non-abelian characteristically simple, then we know that

$$\mathcal{H}_1(G) = \{\lambda(G), \rho(G)\}$$

by a special case of [5, Theorem 7.7], and thus (1.3) holds as well. Our result is that if G is finite and almost simple, then the same phenomenon occurs. More specifically, we shall prove:

Theorem 1.2. *Let G be any finite almost simple group. Then, we have*
$$\mathcal{H}_1(G) = \{\lambda(G), \rho(G)\}.$$
In particular, the statement (1.3) *holds.*

In order to compute $\mathcal{H}_1(G)$, we shall develop a way to describe the regular subgroups of $\mathrm{Hol}(G)$, and not just the ones which are normal; see Section 3. Regular subgroups of $\mathrm{Hol}(G)$ themselves are directly related to Hopf-Galois structures on field extensions. In particular, by [10] and [1], given any finite Galois extension L/K with Galois group G, there exists an explicit bijection between the Hopf-Galois structures on L/K of so-called *type G* and elements of $\mathcal{H}_2(G)$. We shall refer the reader to [7, Chapter 2] for more details. Let us mention in passing that there is also a connection between regular subgroups of $\mathrm{Hol}(G)$ and the non-degenerate set-theoretic solutions of the Yang-Baxter equation; see [11].

Therefore, other than $\mathcal{H}_0(G)$ and $\mathcal{H}_1(G)$, it is also of interest to determine $\mathcal{H}_2(G)$. If G is finite and non-abelian characteristically simple, then this was already solved in [17]. However, if G is finite and almost simple, then as far as the author is aware, the only known result is [6, Theorem 5 and Corollary 6], which states that for all $n \geq 5$, we have

$$\#\mathcal{H}_2(S_n) = 2 \cdot (1 + \#\{\sigma \in A_n : \sigma \text{ has order two}\})$$
$$= 2 \cdot \sum_{\substack{0 \leq k \leq n/2 \\ k \text{ is even}}} \frac{n!}{(n-2k)! \cdot 2^k \cdot k!}.$$

Here S_n and A_n, respectively, denote the symmetric and alternating groups on n letters. Using the techniques to be developed in Section 3, which were largely motivated by [6], we shall also generalize the above result as follows. Recall that an endomorphism f on G is said to be *fixed point free* if

$$f(\sigma) = \sigma \text{ holds precisely when } \sigma = 1_G.$$

Let $\mathrm{End}_{\mathrm{fpf}}(G)$ denote the set of all such endomorphisms. Also, write $\mathrm{Inn}(G)$ for the inner automorphism group G. Then, we shall prove:

Theorem 1.3. *Let G be any finite almost simple group such that $\mathrm{Inn}(G)$ is the only subgroup isomorphic to G in $\mathrm{Aut}(G)$. Then, we have*

$$\#\mathcal{H}_2(G) = 2 \cdot \#\mathrm{End}_{\mathrm{fpf}}(G).$$

Moreover, in the case that $\mathrm{Soc}(G)$ has prime index p in G, we have

$$\#\mathrm{End}_{\mathrm{fpf}}(G) = 1 + \#\{\sigma \in \mathrm{Soc}(G) : \sigma \text{ has order } p\}$$
$$+ (p-2)/(p-1) \cdot \#\{\sigma \in G \setminus \mathrm{Soc}(G) : \sigma \text{ has order } p\},$$

where $\mathrm{Soc}(G)$ denotes the socle of G.

It is well-known, or by Lemma 4.3 below, that for $G = \mathrm{Aut}(T)$ with T a non-abelian simple group, we have $\mathrm{Aut}(G) \simeq G$, and so the first hypothesis of Theorem 1.3 is obviously satisfied. Now, consider the 26 sporadic simple

groups T. Their outer automorphism group $\mathrm{Out}(T)$ and element structures are available on the world-web-wide ATLAS [18]. In particular, exactly 12 of them have non-trivial $\mathrm{Out}(T)$, in which case the order is two. By plugging in $p = 2$ in Theorem 1.3, we then obtain the values of $\#\mathcal{H}_2(G)$, as given in the table below. The notation for the sporadic groups is the same as in [18].

T	no. of elements of order two in T	$\#\mathcal{H}_2(G)$ for $G = \mathrm{Aut}(T)$
M_{12}	891	$1,784$
M_{22}	$1,155$	$2,312$
HS	$21,175$	$42,352$
J_2	$2,835$	$5,672$
McL	$22,275$	$44,552$
Suz	$2,915,055$	$5,830,112$
He	$212,415$	$424,832$
HN	$75,603,375$	$151,206,752$
Fi_{22}	$37,706,175$	$75,412,352$
$\mathrm{Fi'}_{24}$	$7,824,165,773,823$	$15,648,331,547,648$
O'N	$2,857,239$	$5,714,480$
J_3	$26,163$	$52,328$

Since $\#\mathcal{H}_2(T) = 2$ for all finite non-abelian simple groups T, the number $\#\mathcal{H}_2(G)$ is now known for all almost simple groups G of sporadic type.

Finally, let us remark that if $G/\mathrm{Soc}(G)$ is not cyclic (of prime order), then the enumeration of $\mathrm{End}_{\mathrm{fpf}}(G)$ becomes much more complicated. Currently, the author does not have a systematic way of treating the general case.

2. Preliminaries on the multiple holomorph

In this section, we shall give a proof of the fact that the action of $\mathrm{NHol}(G)$ on the set $\mathcal{H}_0(G)$ via conjugation is transitive, and the fact that elements of $\mathcal{H}_0(G)$ are normal subgroups of $\mathrm{Hol}(G)$. Both of them are already known in the literature and are consequences of the next simple observation.

Lemma 2.1. *Isomorphic regular subgroups of* $\mathrm{Perm}(G)$ *are conjugates.*

Proof. Let N_1 and N_2 be any two isomorphic regular subgroups of $\mathrm{Perm}(G)$. Let $\varphi : N_1 \longrightarrow N_2$ be an isomorphism and note that the isomorphism

$$\Xi_\varphi : \mathrm{Perm}(N_1) \longrightarrow \mathrm{Perm}(N_2); \quad \Xi_\varphi(\pi) = \varphi \circ \pi \circ \varphi^{-1}$$

sends $\lambda(N_1)$ to $\lambda(N_2)$. For $i = 1, 2$, recall that the isomorphism Ξ_{N_i} defined as in (1.2) sends $\lambda(N_i)$ to N_i. It follows that $\Xi_{N_2} \circ \Xi_\varphi \circ \Xi_{N_1}^{-1}$ maps N_1 to N_2. We then deduce that N_1 and N_2 are conjugates via $\xi_{N_2} \circ \varphi \circ \xi_{N_1}^{-1}$. $\qquad\square$

Lemma 2.1 implies that the regular subgroups of $\mathrm{Perm}(G)$ isomorphic to G are precisely the conjugates of $\lambda(G)$. For any $\pi \in \mathrm{Perm}(G)$, we have

$$\mathrm{Norm}_{\mathrm{Perm}(G)}(\pi\lambda(G)\pi^{-1}) = \pi\mathrm{Hol}(G)\pi^{-1},$$

which is equal to $\mathrm{Hol}(G)$ if and only if $\pi \in \mathrm{NHol}(G)$. It follows that

$$\mathcal{H}_0(G) = \{\pi\lambda(G)\pi^{-1} : \pi \in \mathrm{NHol}(G)\} \tag{2.1}$$

and thus clearly $\mathrm{NHol}(G)$ acts transitively on $\mathcal{H}_0(G)$ via conjugation. Since the stabilizer of any element of $\mathcal{H}_0(G)$ under this action is equal to $\mathrm{Hol}(G)$, the quotient $T(G)$ acts regularly on $\mathcal{H}_0(G)$. For any $\pi \in \mathrm{Perm}(G)$, we have

$$\pi\lambda(G)\pi^{-1} \lhd \mathrm{Hol}(G) \iff \begin{cases} \pi\lambda(G)\pi^{-1} \leq \mathrm{Hol}(G), \\ \mathrm{Hol}(G) \leq \mathrm{Norm}_{\mathrm{Perm}(G)}(\pi\lambda(G)\pi^{-1}). \end{cases}$$

Since $\lambda(G) \leq \mathrm{Hol}(G)$, both of the conditions on the right are clearly satisfied for $\pi \in \mathrm{NHol}(G)$, and so elements of $\mathcal{H}_0(G)$ are normal subgroups of $\mathrm{Hol}(G)$. In the case that G is finite, the second condition on the right is satisfied only for $\pi \in \mathrm{NHol}(G)$, whence we have the alternative description

$$\mathcal{H}_0(G) = \{N \lhd \mathrm{Hol}(G) : N \simeq G \text{ and } N \text{ is regular}\}$$

for $\mathcal{H}_0(G)$ in addition to (2.1), and in particular $\mathcal{H}_0(G) = \mathcal{H}_1(G) \cap \mathcal{H}_2(G)$.

3. Descriptions of regular subgroups in the holomorph

In this section, Let Γ be a group of the same cardinality as G. Then, the regular subgroups of $\mathrm{Hol}(G)$ isomorphic to Γ are precisely the images of the homomorphisms in the set

$$\mathrm{Reg}(\Gamma, \mathrm{Hol}(G)) = \{\text{injective } \beta \in \mathrm{Hom}(\Gamma, \mathrm{Hol}(G)) : \beta(\Gamma) \text{ is regular}\}.$$

Note that for G and Γ finite, the map β is automatically injective when $\beta(\Gamma)$ is regular. Below, we shall give two different ways of describing this set, and it shall be helpful to recall the definition of $\mathrm{Hol}(G)$ given in (1.1).

The first description uses bijective crossed homomorphisms.

Definition 3.1. Given $\mathfrak{f} \in \mathrm{Hom}(\Gamma, \mathrm{Aut}(G))$, a map $\mathfrak{g} \in \mathrm{Map}(\Gamma, G)$ is said to be a *crossed homomorphism with respect to* $\mathfrak{f}$ if

$$\mathfrak{g}(\gamma\delta) = \mathfrak{g}(\gamma) \cdot \mathfrak{f}(\gamma)(\mathfrak{g}(\delta)) \text{ for all } \gamma, \delta \in \Gamma.$$

Write $Z^1_{\mathfrak{f}}(\Gamma, G)$ for the set of all such maps. Also, let $Z^1_{\mathfrak{f}}(\Gamma, G)^*$ and $Z^1_{\mathfrak{f}}(\Gamma, G)^\circ$, respectively, denote the subsets consisting of those maps which are bijective and injective. Note that these two subsets coincide when G and Γ are finite.

Proposition 3.2. *For $\mathfrak{f} \in \mathrm{Map}(\Gamma, \mathrm{Aut}(G))$ and $\mathfrak{g} \in \mathrm{Map}(\Gamma, G)$, define*

$$\beta_{(\mathfrak{f},\mathfrak{g})} : \Gamma \longrightarrow \mathrm{Hol}(G); \quad \beta_{(\mathfrak{f},\mathfrak{g})}(\gamma) = \rho(\mathfrak{g}(\gamma)) \cdot \mathfrak{f}(\gamma).$$

Then, we have

$$\mathrm{Map}(\Gamma, \mathrm{Hol}(G)) = \{\beta_{(\mathfrak{f},\mathfrak{g})} : \mathfrak{f} \in \mathrm{Map}(\Gamma, \mathrm{Aut}(G)), \, \mathfrak{g} \in \mathrm{Map}(\Gamma, G)\},$$

$$\mathrm{Hom}(\Gamma, \mathrm{Hol}(G)) = \{\beta_{(\mathfrak{f},\mathfrak{g})} : \mathfrak{f} \in \mathrm{Hom}(\Gamma, \mathrm{Aut}(G)), \, \mathfrak{g} \in Z^1_{\mathfrak{f}}(\Gamma, G)\},$$

$$\mathrm{Reg}(\Gamma, \mathrm{Hol}(G)) = \{\text{injective } \beta_{(\mathfrak{f},\mathfrak{g})} : \mathfrak{f} \in \mathrm{Hom}(\Gamma, \mathrm{Aut}(G)), \, \mathfrak{g} \in Z^1_{\mathfrak{f}}(\Gamma, G)^*\}.$$

Proof. This follows easily from (1.1); or see [16, Proposition 2.1] for a proof and note that the argument there does not require G and Γ to be finite. $\quad\square$

The second description uses fixed point free pairs of homomorphisms. The use of such pairs already appeared in [2, 6, 8] and our Proposition 3.4 below is largely motivated by the arguments on [6, pp. 83–84].

Definition 3.3. For any groups Γ_1 and Γ_2, a pair (f, h) of homomorphisms from Γ_1 to Γ_2 is said to be *fixed point free* if the equality $f(\gamma) = h(\gamma)$ holds precisely when $\gamma = 1_{\Gamma_1}$.

Let $\mathrm{Out}(G)$ denote the outer automorphism group of G and write

$$\pi_G : \mathrm{Aut}(G) \longrightarrow \mathrm{Out}(G); \quad \pi_G(\varphi) = \varphi \cdot \mathrm{Inn}(G)$$

for the natural quotient map. Given $\mathfrak{f} \in \mathrm{Hom}(\Gamma, \mathrm{Aut}(G))$, define

$$\mathrm{Hom}_{\mathfrak{f}}(\Gamma, \mathrm{Aut}(G)) = \{\mathfrak{h} \in \mathrm{Hom}(\Gamma, \mathrm{Aut}(G)) : \pi_G \circ \mathfrak{f} = \pi_G \circ \mathfrak{h}\}, \tag{3.1}$$
$$\mathrm{Hom}_{\mathfrak{f}}(\Gamma, \mathrm{Aut}(G))^\circ = \{\mathfrak{h} \in \mathrm{Hom}_{\mathfrak{f}}(\Gamma, \mathrm{Aut}(G)) : (\mathfrak{f}, \mathfrak{h}) \text{ is fixed point free}\}.$$

In view of Proposition 3.2, it is enough to consider $Z_{\mathfrak{f}}^1(\Gamma, G)^*$, which in turn is equal to $Z_{\mathfrak{f}}^1(\Gamma, G)^\circ$ when G and Γ are finite. In the case that G has trivial center, the next proposition, which may be viewed as a generalization of [16, Propositions 2.4 and 2.5], gives an alternative description of this latter set.

Proposition 3.4. *Let $\mathfrak{f} \in \mathrm{Hom}(\Gamma, \mathrm{Aut}(G))$. For $\mathfrak{g} \in Z_{\mathfrak{f}}^1(\Gamma, G)$, define*

$$\mathfrak{h}_{(\mathfrak{f},\mathfrak{g})} : \Gamma \longrightarrow \mathrm{Aut}(G); \quad \mathfrak{h}_{(\mathfrak{f},\mathfrak{g})}(\gamma) = \mathrm{conj}(\mathfrak{g}(\gamma)) \cdot \mathfrak{f}(\gamma),$$

where $\mathrm{conj}(\cdot) = \lambda(\cdot)\rho(\cdot)$. Then, the map $\mathfrak{h}_{(\mathfrak{f},\mathfrak{g})}$ is always a homomorphism. Moreover, in the case that G has trivial center, the maps

$$Z_{\mathfrak{f}}^1(\Gamma, G) \longrightarrow \mathrm{Hom}_{\mathfrak{f}}(\Gamma, \mathrm{Aut}(G)); \quad \mathfrak{g} \mapsto \mathfrak{h}_{(\mathfrak{f},\mathfrak{g})} \tag{3.2}$$
$$Z_{\mathfrak{f}}^1(\Gamma, G)^\circ \longrightarrow \mathrm{Hom}_{\mathfrak{f}}(\Gamma, \mathrm{Aut}(G))^\circ; \quad \mathfrak{g} \mapsto \mathfrak{h}_{(\mathfrak{f},\mathfrak{g})} \tag{3.3}$$

are well-defined bijections.

Proof. First, let $\mathfrak{g} \in Z_{\mathfrak{f}}^1(\Gamma, G)$. For any $\gamma, \delta \in \Gamma$, we have

$$\begin{aligned}
\mathfrak{h}_{(\mathfrak{f},\mathfrak{g})}(\gamma\delta) &= \mathrm{conj}(\mathfrak{g}(\gamma\delta)) \cdot \mathfrak{f}(\gamma\delta) \\
&= \mathrm{conj}(\mathfrak{g}(\gamma))\mathfrak{f}(\gamma) \cdot \mathfrak{f}(\gamma)^{-1}\mathrm{conj}(\mathfrak{f}(\gamma)(\mathfrak{g}(\delta)))\mathfrak{f}(\gamma) \cdot \mathfrak{f}(\delta) \\
&= \mathrm{conj}(\mathfrak{g}(\gamma))\mathfrak{f}(\gamma) \cdot \mathrm{conj}(\mathfrak{g}(\delta))\mathfrak{f}(\delta) \\
&= \mathfrak{h}_{(\mathfrak{f},\mathfrak{g})}(\gamma)\mathfrak{h}_{(\mathfrak{f},\mathfrak{g})}(\delta).
\end{aligned}$$

This means that $\mathfrak{h}_{(\mathfrak{f},\mathfrak{g})}$ is a homomorphism and that (3.2) is well-defined.

Now, suppose that G has trivial center, in which case $\mathrm{conj} : G \longrightarrow \mathrm{Inn}(G)$ is an isomorphism. Given $\mathfrak{h} \in \mathrm{Hom}_{\mathfrak{f}}(\Gamma, \mathrm{Aut}(G))$, define

$$\mathfrak{g} : \Gamma \longrightarrow G; \quad \mathfrak{g}(\gamma) = \mathrm{conj}^{-1}(\mathfrak{h}(\gamma)\mathfrak{f}(\gamma)^{-1}),$$

where $\mathfrak{h}(\gamma)\mathfrak{f}(\gamma)^{-1} \in \mathrm{Inn}(G)$ since $\pi_G \circ \mathfrak{h} = \pi_G \circ \mathfrak{f}$. For any $\gamma, \delta \in \Gamma$, we have

$$
\begin{aligned}
\mathrm{conj}(\mathfrak{g}(\gamma\delta)) &= \mathfrak{h}(\gamma\delta)\mathfrak{f}(\gamma\delta)^{-1} \\
&= \mathfrak{h}(\gamma)\mathfrak{f}(\gamma)^{-1} \cdot \mathfrak{f}(\gamma)\mathfrak{h}(\delta)\mathfrak{f}(\delta)^{-1}\mathfrak{f}(\gamma)^{-1} \\
&= \mathrm{conj}(\mathfrak{g}(\gamma)) \cdot \mathrm{conj}(\mathfrak{f}(\gamma)(\mathfrak{g}(\delta))) \\
&= \mathrm{conj}(\mathfrak{g}(\gamma) \cdot \mathfrak{f}(\gamma)(\mathfrak{g}(\delta))),
\end{aligned}
$$

and hence $\mathfrak{g}$ is a crossed homomorphism with respect to $\mathfrak{f}$. Clearly $\mathfrak{h} = \mathfrak{h}_{(\mathfrak{f},\mathfrak{g})}$ and so this shows that (3.2) is surjective. Let $\mathfrak{g}_1, \mathfrak{g}_2, \mathfrak{g} \in Z_{\mathfrak{f}}^1(\Gamma, G)$. For any $\gamma \in \Gamma$, since conj is an isomorphism, we have

$$\mathfrak{g}_1(\gamma) = \mathfrak{g}_2(\gamma) \iff \mathrm{conj}(\mathfrak{g}_1(\gamma)) = \mathrm{conj}(\mathfrak{g}_2(\gamma)) \iff \mathfrak{h}_{(\mathfrak{f},\mathfrak{g}_1)}(\gamma) = \mathfrak{h}_{(\mathfrak{f},\mathfrak{g}_2)}(\gamma)$$

and so (3.2) is also injective. For any $\gamma_1, \gamma_2 \in \Gamma$, similarly

$$\mathfrak{g}(\gamma_1) = \mathfrak{g}(\gamma_2) \iff \mathrm{conj}(\mathfrak{g}(\gamma_1)) = \mathrm{conj}(\mathfrak{g}(\gamma_2)) \iff \mathfrak{h}_{(\mathfrak{f},\mathfrak{g})}(\gamma_1^{-1}\gamma_2) = \mathfrak{f}(\gamma_1^{-1}\gamma_2)$$

and this implies that (3.3) is a well-defined bijection as well. $\qquad\square$

In the case that G is finite, observe that

$$\#\mathcal{H}_2(G) = \frac{1}{|\mathrm{Aut}(G)|} \cdot \#\mathrm{Reg}(G, \mathrm{Hol}(G)).$$

From Proposition 3.2, we then deduce that

$$\#\mathcal{H}_2(G) = \frac{1}{|\mathrm{Aut}(G)|} \cdot \#\{(\mathfrak{f}, \mathfrak{g}) : \mathfrak{f} \in \mathrm{Hom}(G, \mathrm{Aut}(G)),\ \mathfrak{g} \in Z_{\mathfrak{f}}^1(G, G)^*\}.$$

By Proposition 3.4, when G has trivial center, we further have

$$\#\mathcal{H}_2(G) = \frac{1}{|\mathrm{Aut}(G)|} \cdot \#\left\{ (\mathfrak{f}, \mathfrak{h}) : \begin{array}{l} \mathfrak{f} \in \mathrm{Hom}(G, \mathrm{Aut}(G)) \\ \mathfrak{h} \in \mathrm{Hom}_{\mathfrak{f}}(G, \mathrm{Aut}(G))^\circ \end{array} \right\}. \qquad (3.4)$$

This formula shall be useful for the proof of Theorem 1.3.

Finally, we shall give a necessary condition for a subgroup of $\mathrm{Hol}(G)$ to be normal in terms of the notation of Propositions 3.2 and 3.4.

Proposition 3.5. *Let $\mathfrak{f} \in \mathrm{Hom}(\Gamma, \mathrm{Aut}(G))$ and $\mathfrak{g} \in Z_{\mathfrak{f}}^1(\Gamma, G)$ be such that the subgroup $\beta_{(\mathfrak{f},\mathfrak{g})}(\Gamma)$ is normal in $\mathrm{Hol}(G)$. Then, both of the subgroups $\mathfrak{f}(\Gamma)$ and $\mathfrak{h}_{(\mathfrak{f},\mathfrak{g})}(\Gamma)$ are also normal in $\mathrm{Aut}(G)$.*

Proof. Consider $\gamma \in \Gamma$ and $\varphi \in \mathrm{Aut}(G)$. Since $\beta_{(\mathfrak{f},\mathfrak{g})}(\Gamma)$ is normal in $\mathrm{Hol}(G)$, there exists $\gamma_\varphi \in \Gamma$ such that

$$\varphi\beta_{(\mathfrak{f},\mathfrak{g})}(\gamma)\varphi^{-1} = \beta_{(\mathfrak{f},\mathfrak{g})}(\gamma_\varphi).$$

Rewriting this equation yields

$$\rho(\varphi(\mathfrak{g}(\gamma))) \cdot \varphi\mathfrak{f}(\gamma)\varphi^{-1} = \rho(\mathfrak{g}(\gamma_\varphi)) \cdot \mathfrak{f}(\gamma_\varphi).$$

Since (1.1) is a semi-direct product, this in turn gives

$$\varphi(\mathfrak{g}(\gamma)) = \mathfrak{g}(\gamma_\varphi) \text{ and } \varphi\mathfrak{f}(\gamma)\varphi^{-1} = \mathfrak{f}(\gamma_\varphi).$$

The latter shows that $\mathfrak{f}(\Gamma)$ is normal in $\mathrm{Aut}(G)$. The above also implies that

$$\varphi\mathfrak{h}_{(\mathfrak{f},\mathfrak{g})}(\gamma)\varphi^{-1} = \mathrm{conj}(\varphi(\mathfrak{g}(\gamma))) \cdot \varphi\mathfrak{f}(\gamma)\varphi^{-1} = \mathrm{conj}(\mathfrak{g}(\gamma_\varphi)) \cdot \mathfrak{f}(\gamma_\varphi) = \mathfrak{h}_{(\mathfrak{f},\mathfrak{g})}(\gamma_\varphi),$$

and hence $\mathfrak{h}_{(\mathfrak{f},\mathfrak{g})}(\Gamma)$ is normal in $\mathrm{Aut}(G)$ as well. $\qquad\square$

4. Basic properties of almost simple groups

In this section, let S be an almost simple group and let T be a non-abelian simple group such that $\mathrm{Inn}(T) \leq S \leq \mathrm{Aut}(T)$. Notice that $\mathrm{Inn}(T)$ is normal in $\mathrm{Aut}(T)$ and thus is normal in S as well. Recall the known fact, which is easily verified, that for any $\varphi \in \mathrm{Aut}(T)$, we have

$$\varphi \circ \psi = \psi \circ \varphi \text{ for all } \psi \in \mathrm{Inn}(T) \text{ implies } \varphi = \mathrm{Id}_T. \qquad (4.1)$$

This implies the next three basic properties of S which we shall need. They are known but we shall give a proof for the convenience of the reader.

Lemma 4.1. *The center of S is trivial.*

Proof. This follows directly from (4.1). $\qquad\square$

Lemma 4.2. *Every non-trivial normal subgroup of S contains $\mathrm{Inn}(T)$.*

Proof. Let R be a normal subgroup of S such that $R \not\supseteq \mathrm{Inn}(T)$, or equivalently $R \cap \mathrm{Inn}(T) \neq \mathrm{Inn}(T)$. Then, since $R \cap \mathrm{Inn}(T)$ is normal in $\mathrm{Inn}(T)$, and $\mathrm{Inn}(T) \simeq T$ is simple, this means that $R \cap \mathrm{Inn}(T) = 1$. For any $\varphi \in R$, because both R and $\mathrm{Inn}(T)$ are normal in S, we have

$$\psi \circ \varphi \circ \psi^{-1} \circ \varphi^{-1} \in R \cap \mathrm{Inn}(T) \text{ for all } \psi \in \mathrm{Inn}(T).$$

We then deduce from (4.1) that $\varphi = \mathrm{Id}_T$ and so R is trivial. $\qquad\square$

Lemma 4.3. *There is an injective homomorphism*

$$\iota : \mathrm{Aut}(S) \longrightarrow \mathrm{Aut}(T)$$

such that the composition

$$S \xrightarrow{\hspace{2cm}} \mathrm{Inn}(S) \xrightarrow{\text{\textit{inclusion}}} \mathrm{Aut}(S) \xrightarrow{\hspace{0.8cm}\iota\hspace{0.8cm}} \mathrm{Aut}(T)$$

is the inclusion map, where the first arrow is the map $\varphi \mapsto (x \mapsto \varphi x \varphi^{-1})$.

Proof. Put $T^{\#} = \mathrm{Inn}(T)$, which is the socle of S by Lemma 4.2, and thus is a characteristic subgroup of S. We then have a well-defined homomorphism

$$\mathrm{Aut}(S) \longrightarrow \mathrm{Aut}(T^{\#}); \quad \theta \mapsto \theta|_{T^{\#}}. \qquad (4.2)$$

Suppose that θ is in its kernel. For any $\varphi \in S$, we have

$$\theta(\varphi) \circ \psi \circ \theta(\varphi)^{-1} = \theta(\varphi \circ \psi \circ \varphi^{-1}) = \varphi \circ \psi \circ \varphi^{-1} \text{ for all } \psi \in T^{\#}.$$

From (4.1), we deduce that $\theta(\varphi) = \varphi$, whence $\theta = \mathrm{Id}_S$. This shows that the homomorphism (4.2) is injective. Let us identify T and $T^{\#}$ via $\sigma \mapsto \mathrm{conj}(\sigma)$, where $\mathrm{conj}(\cdot) = \lambda(\cdot)\rho(\cdot)$. We then obtain an injective homomorphism

$$\iota : \mathrm{Aut}(S) \longrightarrow \mathrm{Aut}(T)$$

from (4.2). Since for any $\varphi \in S$ and $\sigma \in T$, we have the relation

$$\varphi \circ \mathrm{conj}(\sigma) \circ \varphi^{-1} = \mathrm{conj}(\varphi(\sigma)) \text{ in } \mathrm{Aut}(T),$$

the stated composition is indeed the inclusion map. □

5. Proof of the theorems

In this section, we shall prove Theorems 1.2 and 1.3.

5.1. Some consequences of the CFSG. Our proof relies on the following consequences of the classification theorem of finite simple groups.

Lemma 5.1. *Let T be a finite non-abelian simple group.*
  (a) *There is no fixed point free automorphism on T.*
  (b) *The outer automorphism group $\mathrm{Out}(T)$ of T is solvable.*
  (c) *The inequality $|T|/|\mathrm{Out}(T)| \geq 30$ holds.*

Proof. They are all consequences of the classification theorem of finite simple groups; see [9, Theorems 1.46 and 1.48] for parts (a),(b) and [15, Lemma 2.2] for part (c). □

Lemma 5.1 (c) in particular implies the following corollaries.

Corollary 5.2. *Let T be a finite non-abelian simple group. Then, any finite group S of order less than $30|\mathrm{Aut}(T)|$ cannot have subgroups T_1 and T_2, both of which are isomorphic to T, such that $T_1 \cap T_2 = 1$.*

Proof. Suppose that S is a finite group having subgroups T_1 and T_2, both of which are isomorphic to T, such that $T_1 \cap T_2 = 1$. Then, we have

$$|T_1 T_2| = |T_1||T_2| = |\mathrm{Inn}(T)||T| = |\mathrm{Aut}(T)||T|/|\mathrm{Out}(T)|.$$

Since $T_1 T_2$ is a subset of S, from Lemma 5.1 (c), it follows that S must have order at least $30|\mathrm{Aut}(T)|$. □

Corollary 5.3. *Let T be a finite non-abelian simple group. Then, the inner automorphism group $\mathrm{Inn}(T)$ is the only subgroup isomorphic to T in $\mathrm{Aut}(T)$.*

Proof. Let R be a subgroup of $\mathrm{Aut}(T)$ isomorphic to T. Since $\mathrm{Inn}(T) \cap R$ is normal in R, and it cannot be trivial by Corollary 5.2, it has to be equal to the entire R. It follows that $R \subset \mathrm{Inn}(T)$, and we have equality because these are finite groups of the same order. □

5.2. Proof of Theorem 1.2. Let G be any finite almost simple group, say

$$\mathrm{Inn}(T) \leq G \leq \mathrm{Aut}(T),$$

where T is a finite non-abelian simple group. From Lemma 4.3, we see that the group $\mathrm{Aut}(G)$ is also almost simple, as well as that

$$\mathrm{Inn}(T^{\#}) \leq \mathrm{Aut}(G) \leq \mathrm{Aut}(T^{\#}),$$

where $T^{\#}$ is a group isomorphic to T. Now, consider a regular subgroup N of $\mathrm{Hol}(G)$. By Proposition 3.2, we may write it as

$$N = \{\rho(\mathfrak{g}(\gamma)) \cdot \mathfrak{f}(\gamma) : \gamma \in \Gamma\}, \quad \text{where} \quad \begin{cases} \mathfrak{f} \in \mathrm{Hom}(\Gamma, \mathrm{Aut}(G)) \\ \mathfrak{g} \in Z_{\mathfrak{f}}^1(\Gamma, G)^* \end{cases}$$

and Γ is a group isomorphic to N. By Proposition 3.4, we may define

$$\mathfrak{h} \in \mathrm{Hom}(\Gamma, \mathrm{Aut}(G)); \quad \mathfrak{h}(\gamma) = \mathrm{conj}(\mathfrak{g}(\gamma)) \cdot \mathfrak{f}(\gamma),$$

and $(\mathfrak{f}, \mathfrak{h})$ is fixed point free since G has trivial center by Lemma 4.1.

Observe that plainly

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

which must be equalities because N is regular. In what follows, assume that both $\mathfrak{f}(\Gamma)$ and $\mathfrak{h}(\Gamma)$ are non-trivial. Also, suppose for contradiction that N is normal in $\mathrm{Hol}(G)$. Then, by Proposition 3.5, both $\mathfrak{f}(\Gamma)$ and $\mathfrak{h}(\Gamma)$ are normal subgroups of $\mathrm{Aut}(G)$, so they contain $\mathrm{Inn}(T^{\#})$ by Lemma 4.2. We have

$$\mathrm{Inn}(T^{\#}) \leq \mathfrak{f}(\Gamma), \mathfrak{h}(\Gamma) \leq \mathrm{Aut}(G) \leq \mathrm{Aut}(T^{\#}), \tag{5.1}$$

which means that $\mathfrak{f}(\Gamma)$ and $\mathfrak{h}(\Gamma)$ are almost simple as well.

(a) **Suppose that both** $\ker(\mathfrak{f})$ **and** $\ker(\mathfrak{h})$ **are non-trivial.**
Note that $\ker(\mathfrak{f}) \cap \ker(\mathfrak{h}) = 1$ because $(\mathfrak{f}, \mathfrak{h})$ is fixed point free. This means that $\mathfrak{f}$ restricts to an injective homomorphism

$$\mathrm{res}(\mathfrak{f}) : \ker(\mathfrak{h}) \longrightarrow \mathrm{Aut}(G), \text{ and } \mathfrak{f}(\ker(\mathfrak{h})) \text{ is non-trivial.}$$

Since $\mathfrak{f}(\ker(\mathfrak{h}))$ is normal in $\mathfrak{f}(\Gamma)$, by Lemma 4.2 and (5.1), we have

$$\mathrm{Inn}(T^{\#}) \leq \mathfrak{f}(\ker(\mathfrak{h})),$$

whence there is a subgroup $\Delta_{\mathfrak{h}}$ of $\ker(\mathfrak{h})$ isomorphic to T. Similarly, there is a subgroup $\Delta_{\mathfrak{f}}$ of $\ker(\mathfrak{f})$ isomorphic to T. But

$$\Delta_{\mathfrak{f}} \cap \Delta_{\mathfrak{h}} \subset \ker(\mathfrak{f}) \cap \ker(\mathfrak{h}) \text{ and so } \Delta_{\mathfrak{f}} \cap \Delta_{\mathfrak{h}} = 1.$$

This contradicts Corollary 5.2 because $|\Gamma| = |G|$ and G is contained in $\mathrm{Aut}(T)$ by assumption.

(b) **Suppose that** $\ker(\mathfrak{f})$ **is trivial but** $\ker(\mathfrak{h})$ **is non-trivial.**
Note that $\mathfrak{f}$ is injective, so $\mathfrak{f}$ induces an isomorphism

$$\frac{\Gamma}{\ker(\mathfrak{h})} \simeq \frac{\mathfrak{f}(\Gamma)}{\mathfrak{f}(\ker(\mathfrak{h}))}, \text{ and } \mathfrak{f}(\ker(\mathfrak{h})) \text{ is non-trivial.} \tag{5.2}$$

On the one hand, the quotient on the left in (5.2) is isomorphic to $\mathfrak{h}(\Gamma)$ and so is insolvable by (5.1). On the other hand, since $\mathfrak{f}(\ker(\mathfrak{h}))$ is normal in $\mathfrak{f}(\Gamma)$, by Lemma 4.2 and (5.1), we have

$$\mathrm{Inn}(T^{\#}) \leq \mathfrak{f}(\ker(\mathfrak{h})).$$

There are natural homomorphisms

$$\frac{\mathfrak{f}(\Gamma)}{\mathrm{Inn}(T^\#)} \xrightarrow{\ \text{surjective}\ } \frac{\mathfrak{f}(\Gamma)}{\mathfrak{f}(\ker(\mathfrak{h}))} \ \text{ and } \ \frac{\mathfrak{f}(\Gamma)}{\mathrm{Inn}(T^\#)} \xrightarrow{\ \text{injective}\ } \mathrm{Out}(T^\#).$$

Since $\mathrm{Out}(T^\#)$ is solvable by Lemma 5.1 (b), this implies that the quotient on the right in (5.2) is solvable, which is a contradiction.

(c) **Suppose that** $\ker(\mathfrak{h})$ **is trivial but** $\ker(\mathfrak{f})$ **is non-trivial.**
By symmetry, we obtain a contradiction as in case (b).

(d) **Suppose that both** $\ker(\mathfrak{f})$ **are** $\ker(\mathfrak{h})$ **are trivial.**
Note that $\mathrm{Inn}(T^\#)$ is the only subgroup isomorphic to T in $\mathrm{Aut}(G)$ by Corollary 5.3. Similarly, since $\Gamma \simeq \mathfrak{f}(\Gamma)$, from (5.1) we see that Γ contains a unique subgroup Δ isomorphic to T. Since both $\mathfrak{f}$ and $\mathfrak{h}$ are injective, they restrict to isomorphisms

$$\mathrm{res}(\mathfrak{f}), \mathrm{res}(\mathfrak{h}) : \Delta \longrightarrow \mathrm{Inn}(T^\#), \ \text{ and } \ \mathrm{res}(\mathfrak{f})^{-1} \circ \mathrm{res}(\mathfrak{h}) \in \mathrm{Aut}(\Delta)$$

is fixed point free because $(\mathfrak{f}, \mathfrak{h})$ is fixed point free. This contradicts Lemma 5.1 (a).

We have thus shown that for N to be normal in $\mathrm{Hol}(G)$, either $\mathfrak{f}(\Gamma)$ or $\mathfrak{h}(\Gamma)$ must be trivial, and consequently N is equal to $\lambda(G)$ or $\rho(G)$. Hence, indeed $\lambda(G)$ are $\rho(G)$ are the only elements of $\mathcal{H}_1(G)$, as desired.

5.3. Proof of Theorem 1.3: The first claim. Let G be any finite almost simple group. Since G has trivial center by Lemma 4.1, we have

$$\#\mathcal{H}_2(G) = \frac{1}{|\mathrm{Aut}(G)|} \cdot \# \left\{ (\mathfrak{f}, \mathfrak{h}) : \begin{array}{l} \mathfrak{f} \in \mathrm{Hom}(G, \mathrm{Aut}(G)) \\ \mathfrak{h} \in \mathrm{Hom}_\mathfrak{f}(G, \mathrm{Aut}(G))^\circ \end{array} \right\} \tag{5.3}$$

as in (3.4). Consider a pair $(\mathfrak{f}, \mathfrak{h})$ as above. We must have $\ker(\mathfrak{f}) \cap \ker(\mathfrak{h}) = 1$ because $(\mathfrak{f}, \mathfrak{h})$ is fixed point free. From Lemma 4.2, we then deduce that at least one of $\mathfrak{f}$ and $\mathfrak{h}$ is injective.

Suppose now that $\mathrm{Inn}(G)$ is the only subgroup isomorphic to G in $\mathrm{Aut}(G)$. If $\mathfrak{h}$ is injective, then $\mathfrak{h}(G)$ must be equal to $\mathrm{Inn}(G)$, and by definition (3.1), we deduce that $\mathfrak{f}(G)$ has to lie in $\mathrm{Inn}(G)$. Since $\mathrm{Inn}(G) \simeq G$, we may then identify any pair $(\mathfrak{f}, \mathfrak{h})$ in (5.3) with $\mathfrak{h}$ injective as a pair (f, h), where

$$f \in \mathrm{End}(G) \text{ and } h \in \mathrm{Aut}(G) \text{ are such that } (f, h) \text{ is fixed point free.}$$

It follows that

$$\#\{(\mathfrak{f}, \mathfrak{h}) : \mathfrak{f} \in \mathrm{Hom}(G, \mathrm{Aut}(G)), \ \mathfrak{h} \in \mathrm{Hom}_\mathfrak{f}(G, \mathrm{Aut}(G))^\circ, \ \mathfrak{h} \text{ is injective}\}$$

$$= \#\{(f, h) : f \in \mathrm{End}(G), \ h \in \mathrm{Aut}(G), \ (f, h) \text{ is fixed point free}\}$$

$$= \#\{(f, h) : f \in \mathrm{End}(G), \ h \in \mathrm{Aut}(G), \ h^{-1} \circ f \in \mathrm{End}_{\mathrm{fpf}}(G)\}$$

$$= |\mathrm{Aut}(G)| \cdot \#\mathrm{End}_{\mathrm{fpf}}(G).$$

By the symmetry between $\mathfrak{f}$ and $\mathfrak{h}$, we similarly have

$$\#\{(\mathfrak{f}, \mathfrak{h}) : \mathfrak{f} \in \mathrm{Hom}(G, \mathrm{Aut}(G)), \ \mathfrak{h} \in \mathrm{Hom}_\mathfrak{f}(G, \mathrm{Aut}(G))^\circ, \ \mathfrak{f} \text{ is injective}\}$$

$$= |\mathrm{Aut}(G)| \cdot \#\mathrm{End}_{\mathrm{fpf}}(G).$$

We now conclude that

$$\#\mathcal{H}_2(G) = \frac{1}{|\mathrm{Aut}(G)|} \cdot 2 \cdot |\mathrm{Aut}(G)| \cdot \#\mathrm{End}_{\mathrm{fpf}}(G) = 2 \cdot \#\mathrm{End}_{\mathrm{fpf}}(G)$$

and this proves the first claim in Theorem 1.3.

5.4. Proof of Theorem 1.3: The second claim. Observe that

$$\mathrm{End}_{\mathrm{fpf}}(G) = \bigsqcup_{H \triangleleft G} \{f \in \mathrm{End}_{\mathrm{fpf}}(G) : \ker(f) = H\}$$

and let us begin by proving the following general statement.

Lemma 5.4. *Let G be a group and let p be a prime. Then, for any normal subgroup H of G of index p and any element σ of G of order p, we have*

$$\#\{f \in \mathrm{End}_{\mathrm{fpf}}(G) : \ker(f) = H \text{ and } f(G) = \langle \sigma \rangle\} = \begin{cases} p - 1 & \text{if } \sigma \in H, \\ p - 2 & \text{if } \sigma \notin H. \end{cases}$$

Proof. Fix an element $\tau \in G$ such that τH generates G/H. Then, we have exactly $p - 1$ endomorphisms $f_1, \ldots, f_{p-1}$ on G with kernel equal to H and image equal to $\langle \sigma \rangle$. Explicitly, for each $1 \leq k \leq p - 1$, we may define f_k by

$$\begin{aligned} f_k(H) &= \{1\}, \\ f_k(\tau H) &= \{\sigma^k\}, \\ &\;\;\vdots \\ f_k(\tau^{p-1}H) &= \{\sigma^{k(p-1)}\}. \end{aligned}$$

Observe that f_k is not fixed point free if and only if

$$\sigma^{ki} \in \tau^i H \text{ for some } i = 1, \ldots, p - 1.$$

Since σ and τH have order p, this in turn is equivalent to $\sigma^k \in \tau H$, and

$$\begin{cases} \sigma^k \notin \tau H \text{ for all } k = 1, \ldots, p - 1 & \text{if } \sigma \in H, \\ \sigma^k \in \tau H \text{ for exactly one } k = 1, \ldots, p - 1 & \text{if } \sigma \notin H. \end{cases}$$

We then see that the claim holds. $\qquad\square$

Now, let G be any finite almost simple group such that $\mathrm{Soc}(G)$ has prime index p in G, in which case by Lemma 4.2, there are exactly three normal subgroups in G, namely 1, $\mathrm{Soc}(G)$, and G. Hence, we have

$$\#\mathrm{End}_{\mathrm{fpf}}(G) = \sum_{H \in \{1, \mathrm{Soc}(G), G\}} \#\{f \in \mathrm{End}_{\mathrm{fpf}}(G) : \ker(f) = H\}.$$

Observe that

$$\begin{aligned} \#\{f \in \mathrm{End}_{\mathrm{fpf}}(G) : \ker(f) = 1\} &= 0, \\ \#\{f \in \mathrm{End}_{\mathrm{fpf}}(G) : \ker(f) = G\} &= 1, \end{aligned}$$

where the former follows from Lemma 5.1 (a) and the latter is trivial. For the case $H = \mathrm{Soc}(G)$, let us first rewrite

$$\#\{f \in \mathrm{End}_{\mathrm{fpf}}(G) : \ker(f) = \mathrm{Soc}(G)\}$$

$$= \sum_{P \leq G, |P|=p} \#\{f \in \mathrm{End}_{\mathrm{fpf}}(G) : \ker(f) = \mathrm{Soc}(G) \text{ and } f(G) = P\}$$

$$= \frac{1}{p-1} \sum_{\sigma \in G, |\sigma|=p} \#\{f \in \mathrm{End}_{\mathrm{fpf}}(G) : \ker(f) = \mathrm{Soc}(G) \text{ and } f(G) = \langle\sigma\rangle\}.$$

Applying Lemma 5.4 then yields

$$\#\{f \in \mathrm{End}_{\mathrm{fpf}}(G) : \ker(f) = \mathrm{Soc}(G)\}$$

$$= \frac{1}{p-1}\left(\sum_{\sigma \in \mathrm{Soc}(G), |\sigma|=p} (p-1) + \sum_{\sigma \notin \mathrm{Soc}(G), |\sigma|=p} (p-2) \right)$$

$$= \#\{\sigma \in \mathrm{Soc}(G) : \sigma \text{ has order } p\}$$

$$\quad + (p-2)/(p-1) \cdot \#\{\sigma \in G \setminus \mathrm{Soc}(G) : \sigma \text{ has order } p\}.$$

This completes the proof of the second claim in Theorem 1.3.

6. Acknowledgments

The author would like to thank the referee for helpful comments.

References

[1] BYOTT, NIGEL P. Uniqueness of Hopf Galois structure of separable field extensions. *Comm. Algebra* **24** (1996), no. 10, 3217–3228. MR1402555 (97j:16051a), Zbl 0878.12001, doi: 10.1080/00927879608825743; Corrigendum, *Comm. Algebra* **24** (1996), no. 11, 3705. MR1405283 (97j:16051b), doi: 10.1080/00927879608825779. 952

[2] BYOTT, NIGEL P.; CHILDS, LINDSAY N. Fixed-point free pairs of homomorphisms and nonabelian Hopf–Galois structures. *New York J. Math.* **18** (2012), 707–731. MR2991421, Zbl 1282.12002. 955

[3] CARANTI, ANDREA. Multiple holomorphs of finite p-groups of class two. *J. Algebra* **516** (2018), 352–372. MR3863482, Zbl 06958057, arXiv:1801.10410, doi: 10.1016/j.jalgebra.2018.09.031. 951

[4] CARANTI, ANDREA; DALLA VOLTA, FRANCESCA The multiple holomorph of a finitely generated abelian group. *J. Algebra* **481** (2017), 327–347. MR3639478, Zbl 06714605, arXiv:1611.05662, doi: 10.1016/j.jalgebra.2017.03.006. 950

[5] CARANTI, ANDREA; DALLA VOLTA, FRANCESCA. Groups that have the same holomorph as a finite perfect group. *J. Algebra* **507** (2018), 81–102. MR3807043, Zbl 06880672, arXiv:1612.03573, doi: 10.1016/j.jalgebra.2018.04.006. 951

[6] CARNAHAN, SCOTT; CHILDS, LINDSAY N. Counting Hopf Galois structures on nonabelian Galois field extensions. *J. Algebra* **218** (1999), no. 1, 81–92. MR1704676 (2000e:12010), Zbl 0988.12003, doi: 10.1006/jabr.1999.7861. 951, 952, 955

[7] CHILDS, LINDSAY N. Taming wild extensions: Hopf algebras and local Galois module theory. Mathematical Surveys and Monographs, 80. *American Mathematical Society, Providence, RI,* 2000. viii+215 pp. ISBN: 978-0-8218-2131-2. MR1767499 (2001e:11116), Zbl 0944.11038, doi: /10.1090/surv/080. 952

[8] CHILDS, LINDSAY N. Fixed-point free endomorphisms and Hopf Galois structures. *Proc. Amer. Math. Soc.* **141** (2013), no. 4, 1255–1265. MR3008873, Zbl 1269.12003, doi: 10.1090/S0002-9939-2012-11418-2. 955

[9] GORENSTEIN, DANIEL. Finite simple groups. An introduction to their classification. University Series in Mathematics. *Plenum Publishing Corp., New York,* 1982. x+333 pp. ISBN: 0-306-40779-5. MR0698782 (84j:20002), Zbl 0483.20008, doi: 10.1007/978-1-4684-8497-7. 958

[10] GREITHER, CORNELIUS; PAREIGIS, BODO. Hopf Galois theory for separable field extensions. *J. Algebra* **106** (1987), no. 1, 239–258. MR0878476 (88i:12006), Zbl 0615.12026, doi: 10.1016/0021-8693(87)90029-9. 952

[11] GUARNIERI, L.; VENDRAMIN, LEANDRO. Skew braces and the Yang-Baxter equation. *Math. Comp.* **86** (2017), no. 307, 2519–2534. MR3647970, Zbl 1371.16037, arXiv:1511.03171, doi: 10.1090/mcom/3161. 952

[12] KOHL, TIMOTHY. Multiple holomorphs of dihedral and quaternionic groups. *Comm. Algebra* **43** (2015), no. 10, 4290–4304. MR3366576, Zbl 1342.20001, doi: 10.1080/00927872.2014.943842. 950

[13] MILLER, GEORGE A. On the multiple holomorphs of a group. *Math. Ann.* **66** (1908), no. 1, 133–142. MR1511494, Zbl 39.0200.02, doi: 10.1007/BF01450918. 950

[14] MILLS, WILLIAM H. Multiple holomorphs of finitely generated abelian groups. *Trans. Amer. Math. Soc.* **71** (1951), 379–392. MR0045117 (13,530a), Zbl 0043.25703, doi: 10.2307/1990698. 950

[15] QUICK, MARTYN. Probabilistic generation of wreath products of non-abelian finite simple groups. *Comm. Algebra* **32** (2004), no. 12, 4753–4768. MR2111594 (2005h:20164), Zbl 1077.20079, doi: 10.1081/AGB-200036751. 958

[16] TSANG, CINDY (SIN YI). Non-existence of Hopf-Galois structures and bijective crossed homomorphisms. *J. Pure Appl. Algebra* **223** (2019), no. 7, 2804–2821. MR3912948, Zbl 07032786, arXiv:1805.10830, doi: 10.1016/j.jpaa.2018.09.016. 951, 954, 955

[17] TSANG, CINDY (SIN YI). Hopf-Galois structures of isomorphic type on a non-abelian characteristically simple extension. *Proc. Amer. Math. Soc.* To appear. arXiv:1811.11399, doi: 10.1090/proc/14627. 951, 952

[18] WILSON, ROBERT; WALSH, PETER; TRIPP, JONATHAN; SULEIMAN, IBRAHIM; PARKER, RICHARD; NORTON, SIMON; NICKERSON, SIMON; LINTON, STEVE; BRAY, JOHN; ABBOTT, RACHEL A world-wide-web ATLAS of group representations - Version 3. http://brauer.maths.qmul.ac.uk/Atlas/v3/. 953

(Cindy (Sin Yi) Tsang) SCHOOL OF MATHEMATICS (ZHUHAI), SUN YAT-SEN UNIVERSITY, ZHUHAI, GUANGDONG PROVINCE, CHINA
zengshy26@mail.sysu.edu.cn
http://sites.google.com/site/cindysinyitsang/