Computing maximal subgroups of finite groups

John J. Cannon and Derek F. Holt

Abstract

We describe a practical algorithm for computing representatives of the conjugacy classes of maximal subgroups in a finite group, together with details of its implementation for permutation groups in the MAGMA system. We also describe methods for computing complements of normal subgroups and minimal supplements of normal soluble subgroups of finite groups.

1 Introduction

The principal aim of this paper is to describe an algorithm for computing representatives of the conjugacy classes of maximal subgroups of a finite group G, together with our implementation of this algorithm for finite permutation groups within the MAGMA system for computational algebra [2]. It is not a complete algorithm for solving this problem, because it depends on the availability of certain information about the finite nonabelian simple groups, including a detailed knowledge of their maximal subgroups. It can only be applied to groups G for which this information is already available or readily computable for each nonabelian composition factor of G. The precise extent to which it is currently applicable will be discussed later in Section 5.

We shall call a finite group a *TF-group* if it has no nontrivial soluble normal subgroup. (This is because such groups have trivial Fitting subgroups.) The socle of a TF-group is a direct product of nonabelian simple groups. In particular, a group G is called *almost simple* if its socle is a nonabelian simple group S, and in this case G is isomorphic to a subgroup of the automorphism group $\mathrm{Aut}(S)$ of S. More generally, if S is a simple factor of the socle of a TF-group G, then $\mathbf{N}_G(S)/\mathbf{C}_G(S)$ is an almost simple group associated with G.

The first step in our maximal subgroups algorithm is to find the maximal subgroups of the TF-group G/L, where L is the largest soluble normal subgroup of G, and the bulk of the description will concern this first step. Computing the maximal subgroups of G from those of G/L is done by a relatively straightforward process of lifting through elementary abelian layers of L, and is the same process as that described for all subgroups in our previous paper [6], but is much easier when only maximal subgroups of G are required.

In the mid 1980's two independent descriptions of procedures were given that aimed to reduce the problem of describing the maximal subgroups of arbitrary finite

groups to questions concerning almost simple groups, the first by Aschbacher and Scott in [1] and the second by Kovács in [19]. To handle the TF-case, we needed to translate the descriptions in [1] and [19] into practical algorithms. In fact we have used only the second of these, but this was a more or less arbitrary choice on our part.

Algorithms for computing the maximal subgroups of a finite soluble group defined by a PC-presentation are described in Section 1.6 of [12] and in [8]. An algorithm for computing maximal subgroups of permutation groups that uses basically the same approach as ours is proposed by Eick and Hulpke in [13]. However their algorithm has not yet been fully implemented. They use a rather more refined method, involving the lower central series of the soluble radical L of G, to reduce to the trivial-Fitting case. Then they use the O'Nan-Scott Theorem (see [1] or Chapter 4 of [5]) to handle the trivial-Fitting case, and so the major part of our description, which is based on [19], is disjoint from theirs. Furthermore they have not yet attempted to handle the so-called twisted wreath product case, which we deal with in Subsection 3.6 below.

This paper also contains descriptions of fairly straightforward algorithms for finding representatives of conjugacy classes of complements of normal subgroups and of minimal supplements of soluble normal subgroups in finite groups. (A *supplement* of a normal subgroup N of a group G is a subgroup H of G that satisfies $NH = G$. A supplement is called *minimal* if it does not contain any other supplement of N in G as a proper subgroup.) For the case of complements of insoluble normal subgroups, we sometimes use the maximal subgroups routine as a first step.

We shall assume that the reader has some basic familiarity with algorithms for computing in finite permutation groups, including the theory of bases and strong generating sets. See [4] or [21], for example.

2 Theoretical remarks on maximal subgroups

The description in [19] can be applied, in particular, to the conjugacy classes of maximal subgroups of a finite group having no soluble normal subgroup. In order to turn this description into an algorithm for finding representatives of these conjugacy classes, we need to make parts of it more explicit, and we shall do that in this section.

Section 3 of [19] begins with a hypothesis $(*)$ involving four groups G, M, K, N, which we shall repeat here, and we shall assume throughout this section that it holds. In general, we define x^g to be $g^{-1}xg$, where x is an element or subset of a group G and $g \in G$.

> $(*)$ We have $K \trianglelefteq M \trianglelefteq G$ and $N = \mathbf{N}_G(K)$. It is assumed that the natural homomorphism σ from M onto the direct product $\prod_{t\in T} M/K^t$ is an isomorphism, where T is a right transversal of N in G.

Although it is not assumed in [19] that G is finite, we shall assume that here. We shall also assume that T is a fixed transversal of N in G that contains the identity

element 1 of G. We denote the inverse image of M/K^t under σ by S_t for each $t \in T$. Then M is the direct product of the subgroups S_t, and each S_t is the intersection of all but one of the conjugates in G of K. Hence the S_t are themselves permuted transitively under conjugation by G, and $N = \mathbf{N}_G(S_1)$.

We shall be concerned in this paper with two specific instances of this configuration, and it might be helpful for the reader to focus their attention on these special cases. In both cases, M is the direct product of $d \geq 1$ nonabelian simple groups, all of which are conjugate in G. In the first and basic situation, the groups S_i are just the simple direct factors of M, and K is the direct product of all of these factors except for S_1.

The second situation is a generalization of the first, in which each S_i is a direct product of some number $e > 1$ of the simple factors of M, where e is a proper divisor of d. The simple factors in any particular S_i form a block of imprimitivity of the action of G by conjugation on the set of all simple factors of M. The group K is the direct product of those simple factors which are not subgroups of S_1, and $N = \mathbf{N}_G(S_1)$ is the stabilizer in G of the block of imprimitivity corresponding to S_1.

2.1 High supplements

The following definition is from [19].

Definition 2.1. A supplement H of M in G is called *high* (with respect to K) if either $H \cap M = 1$, or if H and its intersections with M, K and N satisfy the condition $(*)$.

According to Theorem 3.01 of [19], there is a one-one correspondence between the set of conjugacy classes of supplements C/K of M/K in N/K and the set of conjugacy classes of high supplements H of M in G. Furthermore, we can choose the conjugacy class representatives C and H such that $C/K = (H \cap N)K/K$.

Let $L = H \cap M$ where H a high supplement of M in G and a maximal subgroup of G. Then from the above definition, we deduce immediately that $L = \prod_{t \in T} D_t$, where $D_t = H \cap S_t$, and the D_t are all conjugate under the action of H.

Lemma 2.2. *With the above notation, L is conjugate in G to $\prod_{t \in T} D_1^t$.*

Proof. Since the D_t are all conjugate in H and $D_t \leq S_t = S_1^t$, we certainly have $D_t = D_1^{nt}$ for some $n \in N$. Since C/K supplements M/K in N/K, we have $n = cm$ for some $c \in C, m \in M$ and, because $C/K = (H \cap N)K/K$, we can choose $c \in H \cap N = \mathbf{N}_H(D_1)$. Hence $D_t = D_1^{mt} = D_1^{tm'}$ for some $m' \in M$, and since M is the direct product of the groups S_t, we can choose $m' = m_t \in S_t$. But then the element $\prod_{t \in T} m_t$ conjugates $\prod_{t \in T} D_1^t$ to L. □

In Subsections 3.4 and 3.5 below, we shall be constructing maximal subgroups H of G of this kind in situations where D_1 is known and is not normal in S_1. The following proposition justifies the method that we shall use to compute a representative of the conjugacy class of maximal subgroups that contains H.

Proposition 2.3. *Let H be a maximal subgroup of G which is a high supplement of M in G, and let $D_1 = H \cap S_1$ where D_1 is not normal in S_1. Then H is conjugate in G to $\mathbf{N}_G(L_0)$, where $L_0 = \prod_{t \in T} D_1^t$.*

Proof. Since D_1 is not normal in S_1, L is not normal in G, and maximality of H in G implies that $H = \mathbf{N}_G(L)$. The result now follows from the lemma, which says that L and L_0 are conjugate. □

2.2 Diagonal-type subgroups

We first digress to describe a general construction in group theory. This description is taken from Section 2 of [14]. Let N be any subgroup of any group G, and let T be a right transversal of N in G that contains the identity element of G. For $g \in G$, we shall denote the unique element in $Ng \cap T$ by $\overline{g}$. Let $\alpha : G \to P$ be the permutation representation of G acting by right multiplication on the right cosets of N in G. We can regard P as acting on the set T. Let $W = N \wr P$ be the wreath product using this action of P on T. Then the base group Y of W is the set N^T of functions from T to N, where the action $y \to y^p$ of P on Y is given by $y^p(t) = y(tp^{-1})$ for $y \in Y, p \in P$ and $t \in T$. Then there is a monomorphism $\pi : G \to W$ defined by $\pi(g) = \alpha(g)y$ for $g \in G$, where $y \in Y$ is defined by $y(t) = \overline{tg^{-1}}gt^{-1}$ for $t \in T$. In particular, we have:

Remark 2.4. *If $g \in \ker(\alpha)$, then $\pi(g) = y \in Y$, where $y(t) = tgt^{-1}$ for all $t \in T$.*

Definition 2.5. We call $\pi : G \to W = N \wr P$ defined above the *wreathed monomorphism* induced by N and T.

We now return to our groups G, M, K, N satisfying $(*)$. Throughout this subsection, we shall make the additional assumption that $Z(M/K) = 1$ (and hence that $Z(M) = 1$), and identify M/K with the subgroup $\mathrm{Inn}(M/K)$ of $\mathrm{Aut}(M/K)$. In fact the material to be described in this subsection will only be applied in the situation in which $M/K \cong S_1$ is a nonabelian simple group.

We describe another type of subgroup of G, which we shall call a *diagonal-type* subgroup. These groups are minimal instances of a type of subgroup that is called *full* in [19], and the interested reader should consult [19] for the general definition of full subgroups. Their intersection with M which, as we saw earlier, is a direct product of the factors S_t, is a diagonal subgroup of this direct product.

The information summarized here, which is unavoidably technical, has been extracted from the proof of Theorem 3.03 of [19], which itself depends on Theorem 4.1 of [14].

Let $\psi : N \to \mathrm{Aut}(M/K)$ be the homomorphism induced by conjugation in N/K. As above, let $\alpha : G \to P$ be the permutation representation of G on the right cosets of N in G, let $\pi : G \to N \wr P$ be the wreathed monomorphism induced by N and our fixed transversal T, and let $\rho : G \to \mathrm{Aut}(M/K) \wr P$ be the composite of π and the map $N \wr P \to \mathrm{Aut}(M/K) \wr P$ induced by ψ.

Lemma 2.6. *We have* $\ker(\rho) = \mathbf{C}_G(M)$*, and* ρ *maps* M *isomorphically onto the subgroup* $X := (M/K)^T$ *of the base group* Y *of* $\mathrm{Aut}(M/K) \wr P$*. (Recall that we are identifying* M/K *with* $\mathrm{Inn}(M/K)$*.)*

Proof. Clearly $\ker(\rho) \leq \ker(\alpha)$, and also, since α is equivalent to the conjugation action of G on the direct factors S_t of M, $\mathbf{C}_G(M) \leq \ker(\alpha)$. If $g \in \ker(\alpha)$ then, by Remark 2.4, we have

$$\begin{array}{rcl} g \in \ker(\rho) & \iff & \psi(tgt^{-1}) = 1 \ \forall t \in T \iff tgt^{-1} \in \mathbf{C}_G(S_1) \ \forall t \in T \\ & \iff & g \in \mathbf{C}_G(S_t) \ \forall t \in T \iff g \in \mathbf{C}_G(M), \end{array}$$

and so $\ker(\rho) = \mathbf{C}_G(M)$.

We have seen earlier that M is the direct product of the groups $S_t = S_1^t$ for $t \in T$. By definition of the wreath product, X is the direct product of the groups $(M/K)^t$ for $t \in T$. We shall prove the lemma by showing that ρ maps each S_t isomorphically onto $(M/K)^t$.

Now ψ maps S_1 isomorphically onto $\mathrm{Inn}(M/K)$, which we have already identified with M/K, so we can identify S_1 and M/K, and then $\psi(h) = h$ for $h \in S_1$. If $t \in T \setminus \{1\}$, then $tht^{-1} \in K$, and so $\psi(tht^{-1}) = 1$. Hence, by Remark 2.4, $\rho(h)$ is the element $x \in X$ with $x(1) = h$ and $x(t) = 1$ for $t \in T \setminus \{1\}$. More generally, for $t \in T$,

$$\rho(h^t) = x \in X \text{ with } x(t) = h \text{ and } x(u) = 1 \text{ for } u \in T \setminus \{t\}, \qquad (\dagger)$$

so ρ maps S_t isomorphically onto $(M/K)^t$, as claimed. □

Now ψ induces $\overline{\psi} : N \to \mathrm{Out}(M/K)$, where $\mathrm{Out}(M/K)$ is the outer automorphism group of M/K. Suppose that $\overline{\psi}$ can be extended to a homomorphism $\hat{\psi} : G \to \mathrm{Out}(M/K)$. Then $\hat{\psi}$ can be used to construct a subgroup of G which, according to results proved in [19], is a representative of a conjugacy class of full subgroups of G, as follows.

Let G^* be the pullback of $\hat{\psi}$ and the natural map $\mu : \mathrm{Aut}(M/K) \to \mathrm{Out}(M/K)$; that is,

$$G^* = \{(g, h) \mid g \in G,\ h \in \mathrm{Aut}(M/K),\ \hat{\psi}(g) = \mu(h)\}$$

of $G \times \mathrm{Aut}(M/K)$.

Let N^* be the subgroup of G^* consisting of those $(g, h) \in G^*$ for which $g \in N$. Then

$$N^* = \{\, (g, h) \mid g \in N,\ h \in \mathrm{Aut}(M/K),\ \overline{\psi}(g) = \mu(h) \,\}. \qquad (\dagger\dagger)$$

For each t in the transversal T of N in G, let $\hat{t}$ be some fixed element of $\mathrm{Aut}(M/K)$ for which $\hat{\psi}(t) = \mu(\hat{t})$. Then $T^* = \{(t, \hat{t}) \mid t \in T\}$ is a transversal of N^* in G^* in one-one correspondence with T. If α^* is the permutation representation of G^* on the right cosets of N^* with image acting on the set T^* then, by making this identification between T and T^*, we have $\alpha^*(g, h) = \alpha(g)$, where $\mathrm{im}(\alpha) = \mathrm{im}(\alpha^*) = P$.

Let $\pi^* : G^* \to N^* \wr P$ be the wreathed monomorphism induced by N^* and T^*, as defined in Definition 2.5 above. Let $\tau : G^* \to \mathrm{Aut}(M/K)$ be the natural projection of G^* onto the second component of its elements, and let τ_{N^*} be the restriction of

τ to N^*. Finally, let $\rho^* : G^* \to \mathrm{Aut}(M/K) \wr P$ be the composite of π^* and the map $N^* \wr P \to \mathrm{Aut}(M/K) \wr P$ induced by τ_{N^*}.

Lemma 2.7. *With the above notation, let $(g,h) \in G^*$. Then $\rho^*(g,h) \equiv \rho(g) \pmod X$, where $X = (M/K)^T$ as in Lemma 2.6.*

Proof. By definition of ρ, we have $\rho(g) = \alpha(g)y$, where $y(t) = \psi(\overline{tg^{-1}}gt^{-1})$. By definition of ρ^*, we have $\rho^*(g,h) = \alpha^*(g,h)y' = \alpha(g)y'$, where $y'(t)$ is the second component z_2 of the element

$$(z_1, z_2) := \overline{(t,\hat{t})(g,h)^{-1}}(g,h)(t,\hat{t})^{-1}$$

of N^*. But $z_1 = \overline{tg^{-1}}gt^{-1}$, and by (††) above, we have $\overline{\psi}(z_1) = \mu(z_2)$. In other words, $y(t)$ and $y'(t)$ map onto the same element of $\mathrm{Out}(M/K)$ for all $t \in T$, and since $X = (M/K)^T = \mathrm{Inn}(M/K)^T$, this proves the lemma. □

By Lemma 2.6, we have $X = \rho(M) \leq \mathrm{im}(\rho)$, and so $\mathrm{im}(\rho^*) \leq \mathrm{im}(\rho)$.

Definition 2.8. For a given extension $\hat{\psi} : G \to \mathrm{Out}(M/K)$ of $\overline{\psi} : N \to \mathrm{Out}(M/K)$, the complete inverse image E in G of $\mathrm{im}(\rho^*)$ under ρ is called the *diagonal-type subgroup* corresponding to $\hat{\psi}$.

Strictly speaking, this subgroup E is not well-defined, because it depends on the choice of the elements $\hat{t}$, but it follows easily from Proposition 2.9 below, that a different choice of $\hat{t}$ leads to a conjugate subgroup E, and we are only interested in representatives of the conjugacy classes of subgroups of G.

The following proposition shows that E intersects M in a diagonal subgroup of M, which explains the name. It will be used to justify our algorithm for computing subgroups of this type described in Subsection 3.5 below

Proposition 2.9. *Let E be a diagonal-type subgroup of G. Then $EM = G$ and $E = \mathbf{N}_G(L)$, where $L = E \cap M$.*

Furthermore, $L \cong S_1$, and each element of L has the form $\prod_{t\in T}(h^{\hat{t}^{-1}})^t$ for an element $h \in S_1$, where S_1 has been identified with M/K.

Proof. Let $g \in G$, and choose some $h \in \mathrm{Aut}(M/K)$ with $(g,h) \in G^*$. By Lemma 2.7, $\rho^*(g,h) = \rho(g)x$ for some $x \in X$ and so, by Lemma 2.6, $\rho^*(g,h) = \rho(gm)$ for some $m \in M$, so $gm \in E$ and hence $EM = G$.

If $g \in M$, then $\overline{\psi}(g) = 1$, and so $(g,h) \in G^*$ if and only if $h \in \mathrm{Inn}(M/K) = M/K$. We then have $\rho^*(g,h) = x \in X$, where $x(t) = \hat{t}h\hat{t}^{-1} = h^{\hat{t}^{-1}}$. From the equation (†) above, we see that $x = \rho(m)$, where $m = \prod_{t\in T}(h^{\hat{t}^{-1}})^t$, and M/K has been identified with S_1. By Lemma 2.6, m is the unique element of M with $\rho(m) = x$, and so L is a diagonal subgroup of M and is isomorphic to S_1.

It is straightforward to show that a diagonal subgroup of a direct product of isomorphic groups with trivial centre is self-normalizing. Hence $L = \mathbf{N}_M(L)$, and it follows from $G = EM$ that $E = \mathbf{N}_G(L)$. □

2.3 Some results from the Kovács paper

For the convenience of the reader, we shall now state two results from [19] which we shall make frequent use of in the algorithm to be described in the next section. These are Theorem 4.3 and Lemma 5.1 of [19]. We have made some minor alterations in the notation in order to agree with ours. Note also that, although we are assuming throughout this section that G is a finite group, in [19] Theorem 2.10 assumes only that $|G : N|$ is finite, whereas Theorem 2.11 does not assume finiteness of G.

Theorem 2.10. *Assume the hypothesis* $(*)$*, and that* M/K *is a nonabelian simple group. Then the cardinality of the set of conjugacy classes of maximal subgroups of* G *not containing* M *is equal to* $a + b + c$*, where:*

(i) *a is the sum, over all subgroups D/M of G/M minimal with respect to properly containing N/M, of the cardinalities of the sets $\mathcal{X}_D$ of homomorphisms $D/M \to \mathrm{Out}(M/K)$ whose restrictions to N/M are equal to the map induced by conjugation in the extension $1 \to M/K \to N/K \to N/M \to 1$.*

(ii) *b is the cardinality of the set of conjugacy classes in N/K of maximal subgroups of N/K which neither avoid nor contain M/K.*

(iii) *c is the cardinality of the set of conjugacy classes of those maximal subgroups of N/K which complement M/K and have the property that the homomorphisms of N/M into $\mathrm{Aut}(M/K)$ determined by them are not restrictions of homomorphisms into $\mathrm{Aut}(M/K)$ from any subgroup of G/M properly containing N/M.*

Notice that the statement of this theorem refers only to cardinalities of the classes of maximal subgroups. The construction of the subgroups themselves is described in detail in Section 3 of [19], and it is the details of this construction that we have attempted to summarize in Subsections 2.1 and 2.2.

Let us call the maximal subgroups counted in a, b and c the a-type subgroups, the b-type subgroups and the c-type subgroups, respectively.

The b-type subgroups are the maximal subgroups of G which are high supplements of M in G with respect to K, as defined in Subsection 2.1, and which intersect M nontrivially. Our algorithm to construct them will be described in Subsection 3.4 below. Although we are not making any direct use of the O'Nan-Scott Theorem, the reader might be interested to know that the corresponding primitive permutation groups are of *product type*.

The c-type subgroups are also high supplements of M in G, but they intersect M trivially. Our algorithm to construct them will be described in Subsection 3.6 below. The corresponding primitive permutation groups are of *twisted wreath product type*. The smallest example of a group having a maximal subgroup of this type is $A_5 \wr A_6$.

The a-type subgroups are more complicated in general. They are the maximal full subgroups, as defined in [19], but our algorithm to construct them, which will be described in Subsection 3.5 below, uses a combination of the techniques discussed

above in Subsections 2.1 and 2.2. For each minimal overgroup D/M of N/M in G/M, we first construct the maximal subgroups of D of diagonal type, and then construct corresponding maximal subgroups of G from these as supplements of M which are high with respect to the (unique) normal complement of $D \cap M$ in M.

We shall also use the following result from [19] to help us handle the case when G has two isomorphic nonabelian minimal normal subgroups.

Theorem 2.11. *Let M_1 and M_2 be nontrivial normal subgroups of a group G, and let μ_i be the natural homomorphisms $G/M_i \to G/M_1M_2$. Suppose that $M_1 \cap M_2 = 1$. Then G has corefree maximal subgroups if and only if the following conditions hold.*

(i) *M_1 and M_2 are nonabelian.*

(ii) *Each nontrivial normal subgroup of G/M_i contains M_1M_2/M_i.*

(iii) *There exists an isomorphism $\phi : G/M_2 \to G/M_1$ such that $\mu_1\phi = \mu_2$.*

Moreover, if conditions (i) and (ii) hold, then the set of all corefree maximal subgroups of G is equivalent to the set of all such isomorphisms ϕ in such a way that the subgroups corresponding to ϕ, ϕ' are conjugate if and only if $\phi = \phi'\rho$, where ρ is an inner automorphism of G/M_2 induced by an element of M_1M_2/M_2.

3 The algorithm for finding maximal subgroups

3.1 Reduction to the TF case

Let L be the largest soluble normal subgroup of G, and let N_i $(0 \le i \le r)$ be normal subgroups of G such that

$$1 = N_0 \lhd N_1 \lhd \cdots \lhd N_r = L \lhd G$$

and each N_i/N_{i-1} is an elementary abelian chief factor of G. As in [7], we use the algorithm described in [22] for computing L, and the N_i are then found by calculating the derived series of L and refining it into elementary abelian layers. Unlike in [7], where it was necessary for the N_i to be characteristic subgroups of G, we refine the series until the factors N_i/N_{i-1} are all irreducible as G/N_i-modules.

As in [6], we first find representatives of the conjugacy classes of maximal subgroups of $G/N_r = G/L$, and then lift through the elementary abelian layers, finding the maximal subgroups of G/N_{i-1} from those of G/N_i for $i = r, r-1, \ldots, 1$. However, the situation is much simpler than in [6], where we were looking for all subgroups of G. Since we have chosen the series such that each factor N_i/N_{i-1} is irreducible as a G/N_i-module, a subgroup H/N_{i-1} of G/N_{i-1} is maximal if and only if either $N_i \le H$ and H/N_i is maximal in G/N_i, or H/N_{i-1} is a complement of N_i/N_{i-1} in G/N_{i-1}. So the only computation that needs to be done during the lifting process is to find representatives of the conjugacy classes of complements of the elementary abelian

section N_i/N_{i-1} in G/N_{i-1}. This is handled by a cohomological calculation that is described in detail in Section 5 of [6]. The same method has also been described for finite soluble groups in [10], and it was probably first proposed by Zassenhaus in [23]. In the maximal subgroups algorithm presented in [13], an improved version of this method that uses the lower central series of L is described.

It remains to describe the computation in the TF-group G/L. So, for the remainder of this section, we shall assume that G is a TF-group; that is, that $L = 1$. In an implementation for permutation groups, this presents no difficulty, because a faithful permutation representation of G/L of degree at most that of G, together with the corresponding epimorphism $G \to G/L$ can be constructed; see, for example, [11] or [16].

3.2 The homomorphisms into wreath products

The material in this section is very similar to that in Section 3 of our paper [7] that describes a method for the computation of automorphism groups of finite groups, so we shall just give a brief outline here.

In a TF-group G, the socle M of G is the direct product of its minimal normal subgroups $M_1, M_2, \ldots, M_r$, where each M_i is a direct product of the isomorphic nonabelian simple groups $S_{i1}, S_{i2}, \ldots, S_{id_i}$. The socle factors S_{ij} are permuted under the action of conjugation in G, and the orbits under this action are precisely the sets of factors of M_i for $1 \leq i \leq r$. (The notation M for socle was chosen to be consistent with the notation used in [19].) The first step is to compute M and its factors S_{ij}, and to identify the isomorphism types of the S_{ij} as abstract simple groups.

We need to assume at this stage that, for each isomorphism type of nonabelian finite simple group, we can construct fixed permutation groups S and A, where $S \leq A$, S is simple of the given isomorphism type, and $A \cong \mathrm{Aut}(S)$, where the action of A as the automorphism group of S is given by conjugation in A. We also need to be able to set up an explicit isomorphism between an arbitrary permutation group isomorphic to a subgroup B of A containing S and B itself.

This is a special case of the problem of black box recognition of finite almost simple groups, which is currently a very active area of research in computational group theory. See, for example, [18]. In principal, we can expect that effective methods for solving this problem will eventually become available for all finite nonabelian simple groups.

We shall discuss how we are handling this problem in our implementation of the maximal subgroups algorithm in Section 5. We are of course not currently able to do it for all finite simple groups, and so our implementation will fail if M has nonabelian composition factors which we are unable to handle.

For $1 \leq i \leq r$, let S_i and A_i be the fixed permutation groups with $S_i \cong S_{ij}$ $(1 \leq j \leq d_i)$ and $A_i \cong \mathrm{Aut}(S_i)$. Put $N_i = \mathbf{N}_G(S_{i1})$ for $1 \leq i \leq r$. As described in detail in Section 3 of [7], we construct the conjugation-action homomorphisms $\psi_i : N_i \to A_i$ that restrict to isomorphisms $S_{i1} \to S_i$ and have kernels $\mathbf{C}_G(S_{i1})$.

We then go on to construct homomorphisms $\rho_i : G \to W_i$ for $1 \leq i \leq r$, where W_i is the wreath product $A_i \wr \mathrm{Sym}(d_i)$, which is isomorphic to $\mathrm{Aut}(M_i)$. Let P_i be the image of the permutation representation of G on the right cosets of N_i, let T_i be a fixed right transversal of N_i in G_i, and let $\pi_i : G \to N_i \wr P_i$ be the wreathed monomorphism induced by N_i and T_i, as defined in Definition 2.5. Then ρ_i is defined to be the composite of π_i and the map $N_i \wr P_i \to A_i \wr \mathrm{Sym}(d_i)$ induced by $\psi_i : N_i \to A_i$ and the embedding $P_i \to \mathrm{Sym}(d_i)$.

So ρ_i is virtually the same as the map ρ defined in Subsection 2.2, but with the M_i in place of M. The only difference is that we have enlarged the codomain of the map from $A_i \wr P_i$ to $A_i \wr \mathrm{Sym}(d_i)$. By Lemma 2.6, the kernel of ρ_i is $\mathbf{C}_G(M_i)$. Hence the intersection of all of these kernels is $\mathbf{C}_G(M) = 1$. Again by Lemma 2.6, ρ_i maps M_i isomorphically onto the subgroup $S_i^{T_i}$ of the base group of the wreath product $W_i = A_i \wr \mathrm{Sym}(d_i)$, and $S_i^{T_i} = \mathrm{Soc}(W_i)$, so $\rho_i(M_i) = \mathrm{Soc}(W_i)$. It is convenient to carry out some parts of our computations of the maximal subgroups of G within the images of the ρ_i in W_i and then to pull the results back to G.

Note that $W_i/\mathrm{Soc}(W_i) \cong (A_i/S_i) \wr \mathrm{Sym}(d_i)$, which has a faithful permutation representation of degree $|A_i/S_i|d_i$. The fact that $|A_i/S_i|$ is small in comparison with S_i means that a reasonably small degree permutation representation of $W_i/\mathrm{Soc}(W_i)$ can be computed. The point of this is that, for TF-groups G, we can compute effectively in $G/\mathrm{Soc}(G)$. See Section 2.3 of [9] for the details of this construction. It is also possible to find a workable permutation representation of $G/\langle M_i \mid i \in I\rangle$ for any subset I of $\{1, \ldots, r\}$. Such a quotient can be constructed as a subdirect product of G/M and the groups $\{\mathrm{im}(\rho_i) \mid i \notin I\}$.

3.3 The different types of maximal subgroups

The maximal subgroups of G that contain the socle M correspond to the maximal subgroups of G/M, so we find these by solving the problem recursively in G/M.

Let H be a maximal subgroup of G not containing M, and let Z be the core of H in G. Then G/Z is isomorphic to a primitive permutation group, and its socle is nonabelian, because it contains MZ/Z. It is well-known (see Theorem 4.4 of [5], where this result is described as 'folklore') and not hard to prove that G/Z has either one or two minimal normal subgroups and, in the latter case, they are isomorphic.

If G/Z has a unique minimal normal subgroup, then Z must contain all of the M_i except one. By Theorem 2.10, the maximal subgroups in this category fall into three different types, which we called the a-type, the b-type and the c-type, and we shall deal with these in detail in the following three subsections.

If G/Z has two minimal normal subgroups, then Z either contains all M_i except one, or it contains all M_i except two. The first possibility can occur, for example, in $A_5 \times (A_5 \wr A_5)$, where Z is the base group of the wreath product, and maximal subgroups arise from diagonal subgroups of the quotient $G/Z \cong A_5 \times A_5$. To handle this case, for each k, we work recursively in G/M_k', where M_k' is the direct product of all of the M_i except M_k, and look for maximal subgroups of this 'two minimal normal

subgroup' type whose core does not contain the image of M_k in G/M_k'. Otherwise, Z contains all M_i except for two of them, M_k and M_l, say, where M_k and M_l must be isomorphic. Then Z contains $\ker(\rho_k) \cap \ker(\rho_l) = \mathbf{C}_G(\langle M_k, M_l \rangle)$, and so we can carry out our computations within the image of (ρ_k, ρ_l) in $W_k \times W_l$. This situation is dealt with in Theorem 2.11, and we describe the associated algorithm in the final subsection of this section.

3.4 Unique minimal normal subgroup, first type

In this and the following two subsections, the cores of the maximal subgroups that we are looking for contain all of the M_i except one, which we may as well take to be M_1. Since we shall only be concerned with M_1 in these subsections, we shall drop the first subscript 1, and denote M_1 by M, S_1 by S, A_1 by A, S_{1i} by S_i, d_1 by d, ρ_1 by ρ, and $\psi_1 : N \to A$ by ψ, where $N = \mathbf{N}_G(S_1)$. Let T be a fixed right transversal of N in G containing the identity. Then each socle factor S_i occurs as S_1^t for a unique $t \in T$, and we shall also denote S_1^t by S_t. The notation has been chosen to correspond with that used in the hypothesis $(*)$ defined in Section 2. The subgroup K used in $(*)$ is the direct product of all of the S_i except for S_1.

The maximal subgroups of the first type are those of b-type, as defined after the statement of Theorem 2.10. They are the maximal subgroups H of G which are high supplements of M in G with respect to K, as discussed in Subsection 2.1 above, and which satisfy $H \cap M \neq 1$.

By Theorem 2.10, the conjugacy classes of subgroups of this type correspond to the conjugacy classes of maximal subgroups C of N that neither avoid nor contain S_1. Since the normal subgroups S_1 and $\mathbf{C}_G(S_1)$ of N have trivial intersection, such subgroups C must contain $\mathbf{C}_G(S_1)$, and then $C/\mathbf{C}_G(S_1)$ is a maximal subgroup of $N/\mathbf{C}_G(S_1) \cong \mathrm{im}(\psi)$ which does not contain the image of S_1.

As explained in Subsection 3.2, we have already computed the map $\psi : N \to A$ with kernel $\mathbf{C}_G(S_1)$, and $\mathrm{im}(\psi)$ is a subgroup of A containing S. At this stage, we have to assume that we have available or are able to compute easily a list of the conjugacy classes of maximal subgroups of B not containing S, for all groups B with $S \leq B \leq A$. We shall discuss how this is currently achieved in our implementation in Section 5 below. Of course, in practice, we are not able to do this for all simple groups S, and so our algorithm will fail in some cases.

For each such maximal subgroup E of $\mathrm{im}(\psi)$, we compute the inverse image under ψ of $D := E \cap S$. This inverse image is $D_1 \times \mathbf{C}_G(S_1)$, where D_1 is the subgroup of S_1 corresponding to $D < S$, and D_1 can be computed from $D_1 \times \mathbf{C}_G(S_1)$ by projecting onto the first direct factor of M.

Let L be the direct product of the subgroups $D_t = D_1^t$ of S_t for $t \in T$. Then, by Proposition 2.3, $H := \mathbf{N}_G(L)$ is a representative of the conjugacy class of maximal subgroups of G corresponding to the class of C in N. We have $H \cap M = L$ and $HM = G$, so H has index $|S_1 : D_1|^d$ in G.

3.5 Unique minimal normal subgroup, second type

These are the maximal subgroups of a-type, as defined after Theorem 2.10. In general, they are constructed by using a combination of the constructions of diagonal-type maximal subgroups and of high supplements, discussed in Subsections 2.1 and 2.2, respectively. They do not occur when $N = G$, so we shall assume that $N < G$; that is, that $d > 1$.

From the definition of the number a in Theorem 2.10, it is clear that, in order to find representatives of the conjugacy classes of maximal subgroups of G in this class, we first have to find the minimal overgroups D of N in G; in other words, subgroups D of G for which $N < D \leq G$ and N is maximal in D. This is a straightforward permutation group calculation, because the D arise as the stabilizers of the minimal blocks of imprimitivity containing S_1 in the conjugation action of G on the socle factors S_i. Of course, if this action is primitive, then G itself is the only possible group D.

For each such D, we proceed as follows. The basic idea is first to construct the maximal subgroups of D of diagonal-type (see Definition 2.8). Then, if $D < G$, we use the high supplements construction on these maximal subgroups of D, with D in place of the N in Subsection 2.1, to find the corresponding maximal subgroups of G.

The map $\psi : N \to A$ induced by the conjugation action of N on S_1 induces a homomorphism $\overline{\psi} : N \to A/S = \mathrm{Out}(S)$. Theorem 3.03 of [19] says that each extension of $\overline{\psi}$ to $\hat{\psi} : D \to \mathrm{Out}(S)$ corresponds to one class of maximal subgroups of G of this type. (Of course, there may be no such extensions.) Calculating extensions of homomorphisms is not a particularly straightforward or thoroughly researched computational problem, but in this situation the groups involved are sufficiently small that it can be done by brute force. Since D is a minimal overgroup of N, it has only one extra generator not in N, and so we simply try all possible elements of $\mathrm{Out}(S)$ as images of this generator and check whether this defines a homomorphism extending $\overline{\psi}$.

So suppose that we have such an extension $\hat{\psi}$. Then a representative of the corresponding conjugacy class of maximal subgroups of D and then of G can be found as follows. Let $T_D = T \cap D$, and for each $t \in T_D$, choose an element $\hat{t}$ of A that maps onto $\hat{\psi}(t)$. Then, as we saw in Proposition 2.9, (but with D in place of G and T_D in place of T), we can define a diagonal subgroup E of the subgroup of M generated by the socle factors $\{S_t \mid t \in T_D\}$ by

$$E = \{ \prod_{t \in T_D} (h^{\hat{t}^{-1}})^t \mid h \in S_1 \}.$$

The normalizer $\mathbf{N}_D(E)$ is then the subgroup of D of diagonal-type corresponding to $\hat{\psi}$, and the fact that N is maximal in D implies that $\mathbf{N}_D(E)$ is maximal in D with $\mathbf{N}_D(E) \cap \prod_{t \in T_D} S_t = E$.

Now let U be a right transversal of D in G (we can choose U to be a subset of T) and, for $u \in U$, let $L = \langle E^u \mid u \in U \rangle$ (which is the direct product of the E^u). Then,

from Proposition 2.3 (but with K now replaced by the direct product of those S_t with $t \notin T_D$, and D in place of N) the required maximal subgroup H of G can be computed as the normalizer in G of L. Note that $|E| = |S|$, $|L| = |S|^{|G:D|}$ and, since $L = H \cap M$ and $HM = G$, we have $|G : H| = |S|^{d-c}$, where $c = |G : D|$.

As an example, we see that $A_5 \wr C_2$ has two classes of maximal subgroups of this type. We have $N = S_1$ in this case and $D = G$ is the only possibility. The map $\overline{\psi}$ is trivial, and has two extensions to maps $G \to \mathrm{Out}(S)$, one trivial and the other surjective. However, if we choose $G = S_5 \wr C_2$, then $\overline{\psi}$ is nontrivial and the normal closure of $\ker(\overline{\psi})$ in G contains elements in $N \setminus \ker(\overline{\psi})$, so $\overline{\psi}$ has no extension to G, and there are no maximal subgroups of this type. For an example with $D \neq G$, consider $A_5 \wr C_4$. Then there is a single possible subgroup D, which has index 2 in G. There are two possible extensions of $\overline{\psi}$ to $D \to \mathrm{Out}(S)$ giving rise to two possible classes of subgroups E, which are diagonal subgroups of $A_5 \times A_5$ of order 60. The corresponding subgroups L of A_5^4 have order 60^2, and their normalizers, which are maximal in G, have order 4.60^2.

3.6 Unique minimal normal subgroup, third type

These are the maximal subgroups of c-type, as defined after Theorem 2.10. They are the maximal subgroups H which are high supplements of M, as discussed in Subsection 2.1 above, and which satisfy $H \cap M = 1$. Since the calculations in this case involve the structure of wreath products, it is convenient to carry them out in $\mathrm{im}(\rho)$. However, we shall continue to use the same notation, G, M, S_i, N, etc. for the isomorphic images of these subgroups under ρ. In addition, let K be the image under ρ of $\langle S_i \mid 2 \leq i \leq d \rangle$.

Maximal subgroups of this type are certain complements of M in G. If such complements exist, then G is isomorphic to a twisted wreath product of S by G/M and, by Theorem 4 of [15] for example, there is a one-one correspondence between the conjugacy classes of complements of $S_1 \cong M/K$ in N/K and of M in G. Furthermore, the proof of that theorem describes the correspondence explicitly, so we can construct one from the other.

As we shall see shortly, a subgroup H in a conjugacy class of subgroups of G that corresponds to the conjugacy class containing a complement C/K of M/K in N/K can be maximal in G only if C/K is maximal in N/K. We therefore find our candidate complements C/K by applying the maximal subgroups algorithm recursively to find representatives of the conjugacy classes of maximal subgroups of N/K, and checking to see which of these (if any) is a complement of M/K in N/K. For this recursive application, we require a faithful permutation representation of N/K; this can be found by using the methods described in the final paragraph of Subsection 3.2, but with N in place of G.

Let C/K be a complement of M/K in N/K and H a corresponding complement of M in G. For the sake of completeness, we shall now describe explicitly how to construct H from C; for proofs, see [15]. It is clearly sufficient if, for each element

$g \in G$, we can find the unique element $h \in H$ with $Mh = g$, so we shall explain how to do this. As in Subsection 2.2, for any $g \in G$, we denote the unique element of $Ng \cap T$ by $\overline{g}$, where T is our fixed transversal of N in G. For $g \in G$ and $t \in T$, let x_t be the (unique) element of S_1 for which $tg\overline{tg}^{-1}x_t \in C$. Then $h = g\prod_{t\in T}(x_t)^t$.

Note that $C/K \cong N/M$, and there is a homomorphism $\tau : N/M \to \mathrm{Aut}(M/K) \cong A$ induced by conjugation by elements of C/K. By Theorem 2.10, H is a maximal subgroup of G if and only if the following two conditions hold

(i) C/K is maximal in N/K;

(ii) The homomorphism τ defined above does not extend to a homomorphism $\hat{\tau} : D/M \to \mathrm{Aut}(M/K)$ for any minimal overgroup D of N in G.

Condition (i) is satisfied already, because we have only chosen those C/K which are maximal in N/K. Checking Condition (ii) is similar to a condition that needed to be checked for maximal subgroups of the second type in Subsection 3.5 above. The computation is apparently more difficult in this case, because the codomain of the homomorphisms involved is A rather than the much smaller group A/S, but since we have $d \geq 6$, the groups S will not be very large in examples within the practical range of the algorithm.

The smallest example for which maximal subgroups of this type occur is $A_5 \wr A_6$, which is quite a large group, but has a permutation representation of degree 30.

3.7 Two minimal normal subgroups

These are the maximal subgroups described in Theorem 2.11. As explained in Subsection 3.3, we may assume, in this case, that the cores K in G of the maximal subgroups H of this type contain all of the minimal normal subgroups M_i of G except for two isomorphic M_i. This means that we need to examine all unordered pairs $\{M_k, M_l\}$ of the M_i, but we only need to proceed further for those pairs for which $M_k \cong M_l$. So we shall assume in this description that we are considering M_1 and M_2, and that $M_1 = S_{11} \times \ldots \times S_{1d}$ and $M_2 = S_{21} \times \ldots \times S_{2d}$, where, for $i = 1$ or 2, each S_{ij} is isomorphic to the same simple group S.

Since $M_i \leq K$ for all $i > 2$, we shall assume for the remainder of this section that $d = 2$, and so $M = M_1 \times M_2$. Let $N_i = \mathbf{N}_G(S_{i1})$ for $i = 1, 2$. Recall that we have computed homomorphisms $\psi_i : N_i \to A = \mathrm{Aut}(S)$ that induce isomorphisms onto S when restricted to S_{i1}. We carry out our computations within the image of the map $(\rho_1, \rho_2) : G \to W_1 \times W_2$ induced by the homomorphisms $\rho_i : G \to W_i = A \wr \mathrm{Sym}(d)$ $(i = 1, 2)$ that were defined in Subsection 3.2. This enables us effectively to assume that $d = 2$ within the implementation as well as in the theoretical description.

Condition (i) of Theorem 2.11 clearly holds and, since M_1 and M_2 are the unique minimal normal subgroups of G, condition (ii) is equivalent to $\mathbf{C}_G(M_1) = M_2$ and $\mathbf{C}_G(M_2) = M_1$. But $\mathbf{C}_G(M_1) = \ker(\rho_1)$ and $\mathbf{C}_G(M_2) = \ker(\rho_2)$, so condition (ii) is equivalent to $|\mathrm{im}(\rho_1)| = |\mathrm{im}(\rho_2)|$ and $|G| = |\mathrm{im}(\rho_1)|\,|M_1|$. These two conditions can

be checked immediately. If they do not hold, then there are no maximal subgroups of G of this type, and we can abort the calculations. So, we shall assume from now on that they do hold.

Condition (iii) of Theorem 2.11 is equivalent the statement that there exists an isomorphism $\phi : G/M_2 \to G/M_1$ that maps M/M_2 to M/M_1 and induces the identity on G/M. Assume that ϕ is an isomorphism with this property. Now we have natural isomorphisms $G/M_2 \cong \mathrm{im}(\rho_1)$ and $G/M_1 \cong \mathrm{im}(\rho_2)$, and we shall use $\hat{\phi}$ to denote the isomorphism $\mathrm{im}(\rho_1) \to \mathrm{im}(\rho_2)$ induced by ϕ. The condition that $\phi_{G/M}$ is the identity says that $\hat{\phi}(\rho_1(g)\rho_1(M_1)) = \rho_2(g)\rho_2(M_2)$ for all $g \in G$. So we need to check whether or not the map $\mathrm{im}(\rho_1)/\rho_1(M_1) \to \mathrm{im}(\rho_2)/\rho_2(M_2)$ that takes $\rho_1(g)\rho_1(M_1)$ to $\rho_2(g)\rho_2(M_2)$ for all $g \in G$ lifts to an isomorphism $\hat{\phi} : \mathrm{im}(\rho_1) \to \mathrm{im}(\rho_2)$.

We now recall that $\mathrm{im}(\rho_1) \subseteq W_1$ and $\mathrm{im}(\rho_2) \subseteq W_2$, where $W_1 = W_2 = W = A \wr \mathrm{Sym}(d)$. Furthermore, $\mathrm{im}(\rho_1)$ and $\mathrm{im}(\rho_2)$ both contain $X := \mathrm{Soc}(W)$, and by Lemma 2.6 $\rho_1(M_1) = \rho_2(M_2) = X$, where $W \cong \mathrm{Aut}(X)$. Hence any isomorphism $\mathrm{im}(\rho_1) \to \mathrm{im}(\rho_2)$ induces an automorphism of X, and is itself induced by an inner automorphism of W. So, to test whether the map $\hat{\phi}$ exists, we test for the existence of $x \in W$ that satisfies $\rho_1(g)^x\rho_1(M_1) = \rho_2(g)\rho_2(M_2)$ for all $g \in G$. This is a straightforward conjugacy test in W/X.

If there is no such x, then there are no maximal subgroups of this type, so we abort the computation. If there does exist such an $x \in W$, then $x' \in W$ will have the same property if and only if $x' = rx$ with $rX \in \mathbf{C}_{W/X}(\mathrm{im}(\rho_1)X)$. But from Theorem 2.11, we know that the subgroups corresponding to x and $x' = rx$ are conjugate if and only if $r \in X$, because such an r corresponds to an inner automorphism of G/M_2 induced by an element of M_1M_2/M_2. So, if R is a right transversal of X in the complete inverse image in W of $\mathbf{C}_{W/X}(\mathrm{im}(\rho_1)X)$, then there is a one-one correspondence between the elements rx and the conjugacy classes of maximal subgroups of G of this type.

To find a representative H of the class of maximal subgroups corresponding to the element x, we proceed as follows. Let the subgroup F of $X \times X$ be defined by $F = \{(g, g^x) \mid g \in X\}$, and let $\hat{H}$ be the normalizer in $\mathrm{im}(\rho_1, \rho_2)$ of F. Then H is the complete inverse image in G of $\hat{H}$ under (ρ_1, ρ_2)

As an example, let G be the wreath product $Y \wr C_3$, where Y is $A_5 \times A_5$ and C_3 is cyclic of order 3. Then $W = S_5 \wr S_3$, so $W/X \cong C_2 \wr C_3$ with $\mathrm{im}(\rho_1)X$ cyclic of order 3. So the centralizer of $\mathrm{im}(\rho_1)X$ in $W/X \cong C_2 \wr C_3$ has order 6, and there are 6 conjugacy classes of maximal subgroups of G of this type isomorphic to $A_5 \wr C_3$.

4 Finding complements and supplements

Let N, M be normal subgroups of a finite group G with $N < M$. In this section, we briefly describe algorithms for computing representatives of the conjugacy classes of complements of M/N in G/N and, in the case when M/N is soluble, representatives of the conjugacy classes of minimal supplements of M/N in G/N. These functions

have been implemented in MAGMA in the case of permutation groups G, but the methods are generic, and so it should not be difficult to implement them for other types of representations of finite groups, such as matrix groups. Of course, from a theoretical viewpoint, we are simply describing computation in the quotient group G/N, but we have introduced N as an extra parameter in order to avoid the problem of computing explicitly in quotients of permutation groups. Almost all of the computations take place within G rather than in G/N, and functions return the complete inverse images in G of the complements or supplements of M/N.

We start by finding a series of normal subgroups of G

$$N = N_0 \lhd N_1 \lhd \cdots \lhd N_r = M \lhd G$$

in which each factor N_{i+1}/N_i is a characteristically simple group. This means that it is either elementary abelian or a direct product of isomorphic nonabelian simple groups. It is not necessary for these factors to be as small as possible; in fact computations tend to be faster with fewer and larger factors. If N happens to be soluble, then the soluble radical L/N of M/N is just the quotient of the soluble radical L of M, which we can compute using the algorithm described in [22]. We can then use the derived series of L to refine L/N into elementary abelian layers, and refine the TF-group M/L by working in a permutation representation of the quotient M/L of degree at most that of G. We ensure that our subgroups N_i are normal in G by choosing them all to be characteristic in M.

If N is not soluble, then we work upwards from N to M, finding elementary abelian normal subgroups first, by calculating the cores in G of the subgroups PN for $P \in \mathrm{Syl}_p(M)$ and refining. After finding the largest normal soluble subgroup L/N of M/N, if $L \neq M$, then we need to compute the nonabelian socle of M/L, and for this we are currently reduced to working in the regular permutation representation of M/L.

So we can find a series of normal subgroups as described above. Our next aim is to reduce the problem to the case when $r = 1$, so let us assume for the moment that we can solve it when $r = 1$. In the general case, we proceed to find representatives of conjugacy classes of complements or minimal supplements of M/N_i in G/N_i for $i = r-1, r-2, \ldots, 1, 0$ successively.

Since we can solve the problem when $r = 1$, we can do this for $i = r - 1$. So suppose inductively that, for some $i \leq r-1$, we have already found the required representatives of complements or minimal supplements of M/N_i in G/N_i and we want to find those of M/N_{i-1} in G/N_{i-1}. For each representative complement or minimal supplement C/N_i of M/N_i in G/N_i, we apply the $r = 1$ case of the problem to find representatives of the conjugacy classes of complements or minimal supplements of $(M \cap C)/N_{i-1}$ in C/N_{i-1}.

We claim that the union of the sets of these representatives over all such C provides a complete set of representatives of the conjugacy classes of complements or minimal supplements of M/N_i in G/N_i, as required. This claim is justified theoretically by the following straightforward result.

Proposition 4.1. *Let N and M be normal subgroups of a group G with $N < M$.*

(i) If C is a complement of M in G then CN/N is a complement of M/N in G/N.

(ii) If S is a minimal supplement of M in G then SN/N is a minimal supplement of M/N in G/N.

Proof. We omit the proof of (i), which is easy. Suppose that S is a minimal supplement of M in G. Then certainly SN/N is a supplement of M/N in G/N. If it is not minimal, then there exists a smaller supplement T/N with $TM = G$ and $T < SN$. Then, since $N \leq T$, we have $T = (S \cap T)N$, which implies that $G = TM = (S \cap T)M$. Hence $S \cap T$ is a supplement of M in G strictly contained in S, contradicting the minimality of S. □

So we have now successfully reduced to the case $r = 1$, and we can assume that M/N is either elementary abelian or a direct product of isomorphic nonabelian simple groups.

The method for finding complements when M/N is elementary abelian is moderately well-known, and was briefly discussed above in Subsection 3.1. To apply this method, we require a finitely presented group F isomorphic to G/M, together with an explicit isomorphism $\rho : F \to G/M$. We can find F by first finding a presentation of G itself on a suitable generating set (which can either be the given generators if G is small, or a set of strong generators when G is large; see Sections 5 and 7 of [20], for example), and then adding words that represent generators of M as extra relators.

For the supplements computation, we are not yet attempting to handle the case when M/N is insoluble, so we can assume that M/N is an elementary abelian p-group for some prime p, and then we can regard M/N as a module for G over the field $\mathrm{GF}(p)$. If S/N is a supplement of M/N in G/N and $L = S \cap M$, then $SM = G$ implies that L/N is a G-submodule of M/N.

We start with the supplement G/N and test it for minimality as a supplement of M/N in G/N. If it is minimal then we are done and, if not, then we find representatives of the conjugacy classes of maximal sub-supplements of G/N. Then we test each of these sub-supplements for minimality as a supplement, and carry on in this way, until we have found representatives of all classes of minimal supplements.

To test a particular supplement S/N for minimality, we let $L := S \cap M$ and, for each maximal G-submodule K/N of L/N, we test whether or not L/K has complements in S/K. Such complements correspond to the maximal sub-supplements of S, if any. We omit the details, which are routine.

Finally, we describe the computation of complements in the case when M/N is is insoluble. If G/M happens to be a p-group for some prime p, then the required complements CN/N will be p-groups, and will therefore be conjugate to subgroups of PN/N for $P \in \mathrm{Syl}_p(G)$. So we first find $P \in \mathrm{Syl}_p(G)$, and then find representatives

of the conjugacy classes of complements of the soluble section $(PN \cap M)/N$ in PN/N, and finally test these representative complements for conjugacy in G.

In the general case, where G/M is not a p-group, we start by using our algorithm for maximal subgroups described earlier in the paper to find representatives of the conjugacy classes of maximal subgroups of G that contain N. For each such maximal subgroup H such that $HM = G$, we apply the complements algorithm recursively to find representatives of the conjugacy classes of complements of $(HN \cap M)/N$ in HN/N. Finally, we test the representative complements coming from all of the maximals H for conjugacy in G.

This recursive process could potentially be rather slow. In moderately sized examples, we typically reduce to the soluble section case after the first maximal subgroups computation. However, when M/N contains larger composition factors such as A_n for $n > 7$, which cause the algorithms to recurse several times, the performance deteriorates, and further work is required to handle such examples in a satisfactory manner.

5 Implementation Issues and Performance

As we remarked at the beginning of Subsection 3.2, the part of the algorithm in which the simple composition factors of the socle of a TF-group are identified, and the associated homomorphisms into wreath products constructed, are the same as in our algorithm for constructing automorphism groups of finite groups described in [7], and, in our implementation, that part of the code is common to both algorithms.

In Subsection 3.2 we left open the problem of how we go about defining our standard copies S and their automorphism groups A of the isomorphism types of finite nonabelian simple groups, and how we set up the isomorphisms between the almost simple groups which arise in the course of the algorithm and their standard copies. In addition, in Subsection 3.4, we left open the question of how we find the maximal subgroups of the groups B with $S \leq B \leq A$.

Our current policy is to store all of this information in a database for the smaller order nonabelian simple groups. The isomorphisms are set up using random searches which are designed such that the expected time taken is as small as possible. See Section 3.2 of [7] for more details about this. We have stored the necessary data for all nonabelian simple groups S of order up to order 16482816, together with a few other interesting examples with low degree permutation representations, such as the Mathieu group M_{24} and $L_6(2)$.

For each such S, and for all B with $S \leq B \leq A$, we have stored representatives E of the conjugacy classes of maximal subgroups of B that do not contain S. More precisely, we have stored the intersections $E \cap S$ rather than E since it is the intersections with S that are needed in the algorithm. We may yet append a few more individual groups to this database, but our future plans are now geared towards leaving the database relatively stable, and handling larger examples generically, in families.

Group	Order	Degree	#MaxSubs	Time
$\mathrm{PGL}(3,4)$	60480	21	5	0.2
$\mathrm{PGL}(3,4)$	60480	2240	5	1.0
$\mathrm{PGL}(3,4)$	60480	12096	5	5.7
Sz_8	29120	65	4	0.1
$\mathrm{Aut}(\mathrm{PGL}(3,4))$	241920	42	8	0.5
$P\Gamma L(2,125)$	5859000	126	6	0.5
A_{32}	$1.3\ 10^{35}$	32	22	5.3
S_{50}	$3.0\ 10^{64}$	50	30	49.8
$A_6 \wr S_3$	$1.3\ 10^{16}$	18	20	2.5
$L_2(7) \wr (C_3 \times C_4)$	$4.5\ 10^{16}$	56	17	2.5
$A_5 \wr A_6$	$1.7\ 10^{13}$	30	11	2.1
$A_9 \wr A_{10}$	$7.0\ 10^{58}$	90	18	62.8
$L_3(4)^2$	$4.1\ 10^{8}$	42	30	0.7
$L_3(4)^2 \wr C_3$	$2.0\ 10^{26}$	126	61	24.2
$L_3(4)^2 \wr C_5$	$5.5\ 10^{43}$	210	81	122.3
$L_3(4)^2 \wr S_5$	$1.3\ 10^{45}$	210	36	100.0

Table 1: Times for maximal subgroups of TF groups

Currently, we are able to handle simple groups in the families $L_2(p)$, $L_2(p^2)$, $L_2(p^3)$, $L_3(p)$, and $U_3(p)$ for all primes p, and the symmetric and alternating groups up to degree 1000. We are actively engaged in writing code which enables us to handle further families of low-dimensional groups of Lie type. Further details of the methods involved for these generic classes will be published in a future paper, but we should mention that we are using the algorithm described in [3] for the black box recognition of the alternating and symmetric groups.

Although one might hope that practical black box recognition algorithms will become available for all isomorphism types of almost simple groups in the foreseeable future, there is no realistic prospect of being able to describe all of the maximal subgroups even of every isomorphism type of finite simple group in a uniform manner. One might usefully aim to make the algorithm work effectively for all finite groups that can currently be stored explicitly on a computer, and for which we can carry out basic computations such as computing the order. We are admittedly still some way yet from achieving that aim!

As we have seen, the maximal subgroups of TF-groups G are nearly all computed as normalizers of suitable subgroups of the socle of G. Computing normalizers in large permutation groups can be very slow, and we found that to be the case when there were large numbers of simple factors in the socle. But it is not difficult (we leave the details to the reader) to reduce these normalizer calculations to a number of subgroup conjugacy tests within the simple factors themselves, and this worked much faster than just naively attempting to compute the normalizer.

Group	Order	Degree	#MaxSubs	Time
$C_2 \wr L_3(4)$	$4.2\ 10^{10}$	42	14	0.8
$S_3 \wr L_3(4)$	$4.4\ 10^{20}$	63	15	5.4
$S_4 \wr L_3(4)$	$1.9\ 10^{33}$	84	16	41.1
$S_3 \wr \mathrm{Sz}_8$	$1.1\ 10^{55}$	195	7	760.0
$S_3 \wr A_{32}$	$1.0\ 10^{60}$	96	24	60.2
$S_3 \wr (A_6 \wr S_3)$	$2.8\ 10^{22}$	54	12	4.0
$S_3 \wr (A_5 \wr A_6)$	$3.7\ 10^{36}$	90	14	35.4
$C_6 \times (A_5 \wr A_6)$	$1.0\ 10^{14}$	36	13	3.4
$C_6 \times L_3(4)^2$	$2.4\ 10^{9}$	48	32	1.0
$C_6 \times (L_3(4)^2 \wr C_3)$	$1.2\ 10^{27}$	128	65	24.0

Table 2: Times for maximal subgroups of non-TF groups

Degree	Number of Groups	Total Time	Average Time
6	16	0.3	0.02
7	7	0.2	0.02
8	50	1.4	0.03
9	34	1.2	0.04
10	45	2.6	0.06
11	8	0.5	0.06
12	301	13.9	0.05
13	9	0.9	0.10
14	63	5.1	0.08
15	104	7.7	0.07
16	1954	142.9	0.07
17	10	2.5	0.25
18	983	99.4	0.10
19	8	3.6	0.46
20	1117	158.0	0.14
21	164	29.2	0.18
22	59	17.7	0.30

Table 3: Aggregate Times for maximal subgroups of low degree groups

Group	$\lvert G\rvert$	Degree	$\lvert M\rvert$	#Comps	#Supps	Time
$\mathrm{AGL}(8,2)$	$1.4\ 10^{21}$	256	256	1	1	8.7
$2^8.\mathrm{Sp}(8,2)$	$1.2\ 10^{13}$	256	256	2	2	1.8
$L_5(5)_1$	$7.3\ 10^{13}$	781	625	1	1	3.8
$L_5(5)_1$	$7.3\ 10^{13}$	781	1350	0	1	4.4
$L_5(5)_1$	$7.3\ 10^{13}$	781	2700	0	1	5.3
$L_5(5)_1$	$7.3\ 10^{13}$	781	$1.8\ 10^{13}$	8		48.2
$L_5(5)_1$	$7.3\ 10^{13}$	781	$3.6\ 10^{13}$	0		4.1
$A_5 \wr A_6$	$1.7\ 10^{13}$	30	$4.7\ 10^{10}$	3		11.3
$A_8 \times A_7$	$5.1\ 10^{7}$	15	20160	3		14.3
$A_{10} \times A_{10}$	$3.3\ 10^{12}$	20	$1.8\ 10^{6}$	3		93.4

Table 4: Times for complements and supplements of M in G

In the tables, we list some process times, in seconds, for maximal subgroups computations and, in the final table, for some complements and supplements computations. These were all run on a Sun Ultra 80 Workstation.

The examples in the first table are TF-groups, whereas those in the second table are non TF-groups in which the radical quotient is one of the groups in the first table, so the additional time required for lifting through the layers can be estimated. The first three examples in the first table are the same group with different degree permutation representations.

A full catalogue of all transitive permutation groups of degree up to 30 has been computed by Hulpke [17], and these provide convenient test examples. In the third table we list aggregate times for all transitive permutations groups of degree between 6 and 22. The vast majority of these groups are soluble, and for these we compared the results with those of the corresponding algorithm for soluble groups in MAGMA, and found that they agreed in all cases.

In the final table, for the computation of complements and minimal supplements of a normal subgroup M of G in G, the time given is the total time for finding complements and supplements; these component times were roughly the same. The times do not include the time taken for computing a presentation of G, because this was occasionally large enough to distort the overall time. The group $G = L_5(5)_1$ is the point stabilizer of the natural representation of $L_5(5)$ of degree 781, and it has the structure $5^4.4.L_4(5).4$. The supplements column is empty in those cases where M is not soluble.

References

[1] M. Aschbacher and L. Scott. Maximal subgroups of finite groups. *J. Algebra*, 92:44–80, 1985.

[2] W. Bosma, J. Cannon, and C. Playoust. The MAGMA algebra system I: The user language. *J. Symb. Comput.*, 24:235–265, 1997.

[3] S. Bratus and I. Pak. Fast constructive recognition of a black box group isomorphic to S_n or A_n using Goldbach's conjecture. *J. Symb. Comput.*, 29:33–57, 2000.

[4] G. Butler. *Fundamental Algorithms for Permutation Groups*, volume 559 of *Lecture Notes in Comput. Sci.* Springer-Verlag, Berlin, Heidelberg, New York, 1991.

[5] Peter J. Cameron. *Permutation Groups*, volume 45 of *London Math. Soc. Stud. Texts*. Cambridge University Press, Cambridge, 1999.

[6] J.J. Cannon, B. Cox, and D.F. Holt. Computing the subgroups of a permutation group. *J. Symb. Comput.*, 31:149–161, 2001.

[7] J.J. Cannon and D.F. Holt. Automorphism group computation and isomorphism testing in finite groups. *J. Symb. Comput.*, 35:241–267, 2003.

[8] J.J. Cannon and C.R. Leedham-Green. Presentations of finite soluble groups. In preparation, 2003.

[9] J.J. Cannon and B. Souvignier. On the computation of normal subgroups in permutation groups. To appear, 2003.

[10] F. Celler, J. Neubüser, and C.R.B. Wright. Some remarks on the computation of complements and normalizers in soluble groups. *Acta Applicandae Mathematicae*, 21:57–76, 1990.

[11] D. Easdown and C. E. Praeger. On minimal faithful permutation representations of finite groups. *Bull. Aust. Math. Soc.*, 38:207–220, 1988.

[12] B. Eick. Special presentations for finite soluble groups and computing (pre-)Frattini subgroups. In W.M. Kantor and L. Finkelstein, editors, *Groups and Computation II*, volume 28 of *Amer. Math. Soc. DIMACS Series*, pages 101–112. (DIMACS, 1995), 1997.

[13] B. Eick and A. Hulpke. Computing the maximal subgroups of a permutation group I. In W.M. Kantor and Á. Seress, editors, *Groups and Computation III*, pages 155–168. Ohio, 1999, Walter de Gruyter, 2001.

[14] F. Gross and L.G. Kovács. On normal subgroups which are direct products. *J. Algebra*, 90:133–168, 1984.

[15] D.F. Holt. Embeddings of group extensions into wreath products. *Quart. J. Math. (Oxford)*, 29:463–468, 1978.

[16] D.F. Holt. Representing quotients of permutation groups. *Quart. J. Math. (Oxford)*, 48:347–350, 1978.

[17] A. Hulpke. *Konstruktion transitiver Permutationsgruppen*. PhD thesis, RWTH Aachen, 1996.

[18] W.M. Kantor and Á. Seress. Black box classical groups. *Memoirs Amer. Math. Soc.*, 149:708, 2001.

[19] L.G. Kovács. Maximal subgroups in composite finite groups. *J. Algebra*, 99:114–131, 1986.

[20] J. Neubüser. An elementary introduction to coset table methods in computational group theory. In *Groups – St Andrews* 1981, volume 71 of *London Math. Soc. Lecture Note Ser.*, pages 1–45, Cambridge, 1982. Cambridge University Press.

[21] Á. Seress. An introduction to computational group theory. *Notices Amer. Math. Soc.*, 44:671–679, 1997.

[22] W.R. Unger. Computing the solvable radical of a permutation group. In preparation, 2003.

[23] H. Zassenhaus. Über einen Algorithmus zur Bestimmung der Raumgruppen. *Comment. Math. Helvet.*, 21:117–141, 1948.

Addresses:

School of Mathematics and Statistics
University of Sydney
NSW 2006
Australia
e-mail: john@maths.usyd.edu.au

Mathematics Institute
University of Warwick
Coventry CV4 7AL
Great Britain
e-mail: dfh@maths.warwick.ac.uk