MATHEMATICS OF COMPUTATION Volume 00, Number 0, Pages 000–000 S 0025-5718(XX)0000-0

# COMPUTING THE TABLE OF MARKS OF A CYCLIC EXTENSION

#### L. NAUGHTON AND G. PFEIFFER

ABSTRACT. The subgroup pattern of a finite groups G is the table of marks of G together with a list of representatives of the conjugacy classes of subgroups of G. In this article we present an algorithm for the computation of the subgroup pattern of a cyclic extension of G from the subgroup pattern of G. Repeated application of this algorithm yields an algorithm for the computation of the table of marks of a solvable group G, along a composition series of G.

### 1. INTRODUCTION

The actions of a finite group G on finite sets X are closely linked to the subgroup structure of G, since the isomorphism types of transitive actions of G are in bijection to the conjugacy classes of subgroups of G. Thus properties of finite group actions have an impact on the subgroup structure of G, and vice versa. The correspondence between classes of subgroups of G and transitive actions is made explicit in the *table* of marks of G. This matrix was introduced by Burnside [5] as a tool to classify G-sets up to equivalence. In this context, the mark of a subgroup H of G on Xis the number of fixed points of H in the action of G on X, denoted by  $\beta_X(H)$ . If  $H_1, \ldots H_r$  is a list of representatives of the subgroups of G up to conjugacy, the table of marks of G is then the  $(r \times r)$ -matrix

# $\mathcal{M}(G) = (\beta_{G/H_i}(H_j))_{i,j=1,\dots,r}.$

Similar to the character table of G, which classifies matrix representations of G up to isomorphism, the table of marks of G classifies permutation representations of G up to equivalence. Moreover, the table of marks encodes a wealth of information about the subgroup structure of G in a compact way. For instance, up to a known factor, the mark  $\beta_{G/H_i}(H_j)$  is exactly the number of conjugates of the subgroup  $H_i$  which contain  $H_j$  as a subgroup.

Thus, the table of marks provides a close approximation of the subgroup lattice of G and precisely describes the poset of conjugacy classes of subgroups of G. Conversely, the table of marks can be obtained by counting incidences in the subgroup lattice of G. However, both the computation of the subgroup lattice of G as well as incidence counting between conjugacy classes of subgroups are computationally expensive tasks, unless the order of G is small. It is therefore desirable to be able to compute the table of marks in a way that avoids computing the subgroup lattice, or counting incidences, or both.

©XXXX American Mathematical Society

Received by the editor May 2011.

<sup>2010</sup> Mathematics Subject Classification. Primary 20B40; Secondary 19A22, 20D30, 20D08, 20D10.

Pfeiffer [11] describes a procedure for the construction of the table of marks of a finite group G from the tables of marks of its maximal subgroups. This semi-automatic procedure has proven well suited for simple groups up to a certain order, and has been used extensively in building the GAP [7] library of tables of marks Tomlib [12].

In this article we present a new algorithm for the computation of the table of marks of a cyclic extension of G from the table of marks of G. More precisely, we show how to compute the *subgroup pattern* of the extension from the subgroup pattern of G. Here, the subgroup pattern (c.f. [3, 4]) of a finite group G is a list of representatives of its conjugacy classes of subgroups together with its table of marks. As a motivating example we choose the symmetric group  $S_n$  which contains the alternating group  $A_n$  as a normal subgroup of index 2. With this in mind, we will assume from Section 3 on that S is a finite group, that A is a normal subgroup of S of index p for some prime number p, and that the subgroup pattern of A is known.

In Section 2, we introduce notation and review some basic properties of Gsets and G-maps. In Section 3, we describe an algorithm for the computation of the conjugacy classes of subgroups of S from a list of representatives of the conjugacy classes of subgroups of A. Repeated application of this algorithm yields an algorithm for the computation of the conjugacy classes of subgroups of a solvable group. In Section 4, we discuss the building blocks for the computation of the table of marks of S from the table of marks of A, assuming that the conjugacy classes of subgroups of both A and S are known. In the final section, we combine these tools into an algorithm for the computation of the subgroup pattern of S from the subgroup pattern of A. Repeated application of this algorithm yields an algorithm for the computation of the table of marks of a solvable group. The section finishes with a list of concrete results and performance statistics.

### 2. G-Sets and G-Maps

Let G be a finite group. A finite set X together with a map  $X \times G \to X$ , mapping the pair  $(x,g) \in X \times G$  to  $x.g \in X$  is called a G-set if x.1 = x for all  $x \in X$  and (x.g).g' = x.(gg') for all  $x \in X, g, g' \in G$ . A map  $f : X \to Y$  between G-sets X and Y is called a G-map if f(x.g) = f(x).g for all  $x \in X, g \in G$ . We review some notation and basic properties of G-sets and the maps between them.

For a G-set X, we denote by  $\pi_X : G \to \mathbb{N}_0$  the permutation character (see [2]) of the action of G on X, i.e.

$$\pi_X(g) = |\text{Fix}_X(g)| = \#\{x \in X : x \cdot g = g\},\$$

for  $g \in G$ .

The group G partitions any G-set X into orbits. For  $x \in X$ , we denote by  $[x]_G = x.G$  (or simply [x]) the G-orbit (or class) of x, and by

$$X/G = \{ [x]_G : x \in X \}$$

the quotient set (or set of classes). The number of orbits of G on X can be computed from the permutation character as

(2.1) 
$$|X/G| = \frac{1}{|G|} \sum_{g \in G} \pi_X(g)$$

by the Cauchy-Frobenius Lemma (the lemma that is not Burnside's [10]).

If G acts on two sets X and Y then G also acts on their product  $X \times Y$  via (x, y).g = (x.g, y.g) for all  $x \in X, y \in Y, g \in G$ . The following propositions list some general properties of this action on pairs which will be used in the sequel. Their proofs make use of the following easy lemma.

Lemma 2.1. Suppose that X and Y are G-sets. Then,

(i) for all  $x \in X$ ,  $y \in Y$ , we have

$$[x,y]_G \cap (X \times y) = [x]_{G_y} \times y;$$

(ii) for  $y \in Y$ , the map  $[x]_{G_y} \mapsto [x, y]_G$  is a well defined bijection from  $X/G_y$  to  $(X \times [y]_G)/G$ .

*Proof.* (i) The statement is equivalent to

$$\{x' \in X : (x', y) \in (x, y).G\} = x.G_y$$

which is obviously true.

(ii) Consider the map  $\gamma: X \to (X \times Y)/G$  defined by  $\gamma(x) = [x, y]_G$  for  $x \in X$ . Then  $\gamma(X) = (X \times [y]_G)/G$ , and by (i),  $\gamma^{-1}([x, y]_G) = [x]_{G_y}$ .

**Proposition 2.2.** Suppose that X and Y are transitive G-sets and that  $Z \subseteq X \times Y$  is a G-invariant subset of pairs. Let  $(x, y) \in Z$ . Then the stabilizers  $G_y, G_x$  act on

$$Zy = \{x' \in X : (x', y) \in Z\}, \quad xZ = \{y' \in Y : (x, y') \in Z\}$$

respectively, and the map  $\xi: Zy/G_y \to xZ/G_x$ , given by

$$\xi([x.a]_{G_y}) = [y.a^{-1}]_{G_x}$$

for  $a \in G$ , is a well defined bijection of orbits.

*Proof.* By Lemma 2.1, the maps  $\alpha: Zy/G_y \to Z/G$  and  $\beta: xZ/G_x \to Z/G$ , defined by

$$\alpha([x']_{G_y}) = [x', y]_G, \quad \beta([y']_{G_x}) = [x, y']_G$$

for  $x' \in Zy, y' \in xZ$ , are well defined bijections, and  $\xi = \beta^{-1} \circ \alpha$ .

**Proposition 2.3.** Suppose that X and Y are G-sets and that  $f : X \to Y$  is a G-map. Then the map

$$\zeta: \coprod_{[y]\in Y/G} f^{-1}(y)/G_y \to X/G$$

defined by  $\zeta([x]_{G_{f(x)}}) = [x]_G$  for  $x \in f^{-1}(y)$ , where y ranges over a set of representatives of the G-orbits on Y, is a well defined bijection.

Proof. The set  $Z = \{(x, y) \in X \times Y : y = f(x)\}$  is a *G*-invariant subset of  $X \times Y$  with  $xZ = \{f(x)\}$  for all  $x \in X$ , and  $Zy = f^{-1}(y)$  for all  $y \in Y$ , in the notation of Proposition 2.2. By Lemma 2.1, for each orbit  $[y] \in Y/G$ , there is a bijection  $[x]_G \mapsto [x, y]_G$  between  $f^{-1}(y)/G_y$  and  $(X \times [y])/G$ , which in turn is a bijection to  $f^{-1}([y])/G$  via  $[x, f(x)]_G \mapsto [x]_G$ . The claim then follows from the fact that

$$X = \prod_{y \in Y} f^{-1}(y) = \prod_{[y] \in Y/G} f^{-1}([y]_G),$$

whence  $X/G = \coprod_{[y] \in Y/G} f^{-1}([y])/G$ .

2.1. **Marks.** We call the collection of all marks which G leaves on X, that is the function  $\beta_X : \operatorname{Sub}(G) \to \mathbb{Z}$ , which assigns to each subgroup H of G its mark

$$\beta_X(H) = |\operatorname{Fix}_X(H)| = \#\{x \in X : x \cdot h = x \text{ for all } h \in H\},\$$

the *impression* of G on X. Clearly,  $\beta_X$  is constant on conjugacy classes, so we can regard  $\beta_X$  as a function from the set  $\operatorname{Sub}(G)/G$  of conjugacy classes of subgroups of G to  $\mathbb{Z}$ , or simply as the list of integers

$$\beta_X = (\beta_X(H_1), \dots, \beta_X(H_r))$$

where  $H_1, \ldots, H_r$  is a fixed list of representatives of the conjugacy classes of subgroups of G. The table of marks of G is then the  $r \times r$ -matrix which has as its rows the impressions of the transitive G-sets  $G/H_i$ ,  $i = 1, \ldots, r$ . Marks can also be viewed as incidences between conjugacy classes of subgroups due to the following formula (e.g., see [11, Prop 1.2]):

(2.2) 
$$\beta_{G/K}(H) = |N_G(K) : K| \cdot \#\{K^g : H \le K^g, g \in G\}$$

**Theorem 2.4** (Burnside [5]). Let G be a finite group, and X and Y be finite G sets. Then the G-sets X and Y are isomorphic if and only if  $\beta_X = \beta_Y$ .

2.2. The Burnside Ring. For any G-set X, let [X] denote its isomorphism class. The Burnside ring of G, denoted  $\Omega(G)$  is the free abelian group

$$\Omega(G) = \{\sum_{i=1}^{r} a_i [G/H_i] : a_i \in \mathbb{Z}\}$$

generated by the isomorphism classes of transitive G-sets  $[G/H_i]$ , i = 1, ..., r. The sum [X] + [Y] of the isomorphism classes of G-sets X and Y is the isomorphism class  $[X \sqcup Y]$  of the disjoint union of X and Y, and the product  $[X] \cdot [Y]$  is the isomorphism class  $[X \times Y]$  of the Cartesian product of X and Y. This turns  $\Omega(G)$ into a commutative ring with identity [G/G] (see [1]).

2.3. **Dress Congruences.** Note that, if X and Y are G-sets, and H is a subgroup of G, then  $\beta_{X \sqcup Y}(H) = \beta_X(H) + \beta_Y(H)$  and  $\beta_{X \times Y}(H) = \beta_X(H) \times \beta_Y(H)$ . Theorem 2.4 has the following consequence. Each subgroup H of G defines a ring homomorphism  $\Omega(G) \to \mathbb{Z}$  by  $[X] \mapsto \beta_X(H)$ . Since  $\beta_X(H) = \beta_X(K)$  if H and K are conjugate in G, it follows that the product mapping

$$\beta: \quad \Omega(G) \quad \to \mathbb{Z}^r$$
$$[X] \quad \mapsto \beta_X = (\beta_X(H_1), \dots, \beta_X(H_r))$$

is injective. In this context  $\mathbb{Z}^r$  is often called the *ghost ring* of G.

The matrix M(G) of the linear map  $\beta$  with respect to the basis  $\{G/H_i\}_{i=1,...,r}$  of  $\Omega(G)$  and to the canonical basis  $\{u_i\}_{i=1,...,r}$  of  $\mathbb{Z}^r$  is the table of marks of G. Thus, if

$$[X] = \sum_{i=1}^{r} a_i [G/H_i] \in \Omega(G),$$

then  $\beta_X$  can be expressed in terms of the table of marks M(G) as

$$\beta_X = (a_1, \ldots, a_r) \mathbf{M}(G)$$

**Theorem 2.5.** (Dress, see [1, 6]) Let G be a finite group. For  $H, U \leq G$ , set

$$n(U,H) = \#\{Ua \in N_G(U)/U : \langle U,a \rangle \sim_G H\}.$$

Then the element  $y = (y_1, \ldots, y_r)$  of  $\mathbb{Z}^r$  is in the image of  $\beta$  if and only if

$$\sum_{i=1}^{r} n(U, H_i) y_i \equiv 0 \mod |N_G(U)/U|.$$

for all  $U \leq G$ .

Theorem 2.5 yields a set of congruences which, in particular, must be satisfied by the rows of the table of marks of G.

## 3. The Subgroups of S

From now on, let S be a finite group, and let A be a normal subgroup of S of index p for some prime p. In this section we describe an algorithm for the computation of the conjugacy classes of subgroups of S from the conjugacy classes of subgroups of A. For the purpose of exposition we distinguish between two types of subgroups of S: the subgroups of A will be called *blue subgroups*, and the subgroups of S which are not contained in A will be called *red subgroups*. The set of subgroups of S then is a disjoint union

$$\mathrm{Sub}(S) = \mathcal{B} \sqcup \mathcal{R},$$

where

$$\mathcal{B} = \operatorname{Sub}(A), \quad \mathcal{R} = \operatorname{Sub}(S) \setminus \operatorname{Sub}(A).$$

Since no red subgroup is conjugate to a blue subgroup, both  $\mathcal{B}$  and  $\mathcal{R}$  are S-sets. The aim of this section is to obtain an effective description of the conjugacy classes

$$\operatorname{Sub}(S)/S = \mathcal{B}/S \sqcup \mathcal{R}/S$$

of subgroups of S from the conjugacy classes  $\operatorname{Sub}(A)/A = \mathcal{B}/A$  of subgroups of A. As a simple example, the separation of  $\operatorname{Sub}(S_4)/S_4$  into blue and red classes of subgroups is illustrated in Figure 1, where, blue subgroups are connected by blue edges, red subgroups are connected by black edges, and dashed red egges are used to connect blue subgroups to red subgroups.



FIGURE 1. Poset of Conjugacy Classes of Subgroups of  $S_4$ 

3.1. Classes of Blue Subgroups. Blue conjugacy classes of subgroups of S are unions of A-conjugacy classes of subgroups of A. The following proposition shows that a blue conjugacy class in S is a union of exactly one or p A-conjugacy classes.

**Proposition 3.1.** Let  $H \leq A$  and let  $t \in S \setminus A$ . Then

$$[H]_S = [H]_A \cup [H^t]_A \cup \dots \cup [H^{t^{p^{-1}}}]_A$$
  
where either  $[H]_S = [H]_A$  and  $|N_S(H) : N_A(H)| = p$ , or  $N_S(H) = N_A(H)$  and

 $|[H]_S| = p |[H]_A|.$ 

*Proof.* First, note that each S-conjugate of H lies in one of  $[H]_A, [H^t]_A, \ldots, [H^{t^{p^{-1}}}]_A$ , since  $S = A \cup tA \cup \cdots \cup t^{p^{-1}}A$ . Moreover, each of the A-conjugacy classes of the S-conjugates of H have the same size, since conjugation by t induces a bijection between  $[H]_A$  and  $[H^t]_A$ . By the Orbit-Stabilizer Theorem,

$$[H]_{S}| \cdot |N_{S}(H)| = |S| = p |A| = p |[H]_{A}| \cdot |N_{A}(H)|$$

From  $[H]_A \subseteq [H]_S$  and  $N_A(H) \leq N_S(H)$ , it follows that either  $[H]_A = [H]_S$  and  $|N_S(H)| = p |N_A(H)|$  or that  $N_S(H) = N_A(H)$  and  $|[H]_S| = p |[H]_A|$ .  $\Box$ 

According to the dichotomy in this proposition, we denote

 $\mathcal{B}_1 = \{ H \in \mathcal{B} : [H]_S = [H]_A \}, \ \mathcal{B}_2 = \{ H \in \mathcal{B} : N_S(H) = N_A(H) \}$ 

Then  $\mathcal{B} = \mathcal{B}_1 \sqcup \mathcal{B}_2$  implies  $\mathcal{B}/A = \mathcal{B}_1/A \sqcup \mathcal{B}_2/A$  and the S-conjugacy class of blue subgroups can be described as follows.

**Corollary 3.2.**  $\mathcal{B}/S = \mathcal{B}_1/A \sqcup \mathcal{B}_2/S$ . In particular, S has  $b = b_1 + \frac{1}{p}b_2$  conjugacy classes of blue subgroups, where  $b_i = |\mathcal{B}_i/A|, i = 1, 2$ .

Corollary 3.2 yields the following algorithm to compute the set  $\mathcal{B}/S$  of blue subgroups of S from the set  $\mathcal{B}/A$ .

## Algorithm 1 BlueSubgroups()

Input Representatives of  $\mathcal{B}/A$ Output Representatives of  $\mathcal{B}/S$ Initialize  $B_1 \leftarrow \{\}, B_2 \leftarrow \{\}$ for  $H \in \mathcal{B}/A$  do if  $N_S(H) \nleq A$  then Add H to  $B_1$ . else Add H to  $B_2$ . end if end for return  $B_1 \cup$  (a set of representatives of S-conjugate subgroups in  $B_2$ ).

**Example 3.3.** The special linear group  $L_2(32)$  is a normal subgroup of index 5 in  $L_2(32)$ :5. Figure 2 illustrates how the blue classes of subgroups of  $L_2(32)$  fuse to form blue classes of subgroups of  $L_2(32)$ :5.



FIGURE 2. Class Fusions in  $L_2(32)$ :5

3.2. Classes of Red Subgroups. Red conjugacy classes of subgroups of S correspond to certain conjugacy classes of subgroups of order p in normalizer quotients.

**Proposition 3.4.** For  $H \in \mathcal{B}$ , let  $T_H \subseteq S$  be such that  $\{H\langle t \rangle : t \in T_H\}$  is a transversal of the conjugacy classes of subgroups of order p of  $N_S(H)/H$  which lie outside  $N_A(H)/H$ . Then the set

$$\coprod_{[H]_A \in \mathcal{B}/A} \{ \langle H, t \rangle : t \in T_H \},\$$

where H ranges over a transversal of  $\mathcal{B}/A$ , is a transversal of  $\mathcal{R}/S$ .

Proof. Consider the map  $\gamma : \mathcal{R} \to \mathcal{B}$ , defined by  $\gamma(K) = A \cap K$  for  $K \in \mathcal{R}$ . From  $\gamma(K^s) = K^s \cap A = K^s \cap A^s = (K \cap A)^s = \gamma(K)^s$ 

for any  $s \in S$ , it follows that  $\gamma$  is an S-map. For  $H \in \mathcal{B}$ , the map  $K \mapsto K/H$  is a bijection between

$$\mathcal{R}_H = \{ K \in \mathcal{R} : \gamma(K) = H \} = \gamma^{-1}(H)$$

and the set of subgroups of order p in the quotient  $N_S(H)/H$  which are not contained in  $N_A(H)/H$ . Moreover, these two sets are equivalent as  $N_S(H)/H$ -sets. By Proposition 2.3,

$$\mathcal{R}/S = \coprod_{[H]_S \in \mathcal{B}/S} \mathcal{R}_H/N_S(H),$$

where H ranges over a transversal of the conjugacy classes of blue subgroups of S. The statement remains true, if H ranges over a transversal of  $\mathcal{B}_1/S = \mathcal{B}_1/A$ , or over a transversal of  $\mathcal{B}/A$ , since  $\mathcal{R}_H = \emptyset$  for all  $H \in \mathcal{B}_2$ .

Note that  $T_H \subseteq S$  can easily be determined from a list of representatives of the conjugacy classes of  $N_S(H)/H$ . In fact, modulo H, the set  $T_H$  is in bijection to the set of rational classes of elements of order p in  $N_S(H)/H \setminus N_A(H)/H$ . Moreover, each  $t \in T_H$  can be chosen to be an element of order a power of p.

**Corollary 3.5.** With the above notation, S has

$$r = \sum_{[H]_A \in \mathcal{B}/A} |\mathcal{R}_H/N_S(H)| = \sum_{[H]_A \in \mathcal{B}/A} |T_H|$$

conjugacy classes of red subgroups.

Proposition 3.4 yields the following algorithm to compute the set  $\mathcal{R}/S$  of red subgroups of S.

## Algorithm 2 RedSubgroups()

```
Input Representatives of \mathcal{B}/A

Output Representatives of \mathcal{R}/S

output \leftarrow {}.

for H \in \mathcal{B}/A do

if N_S(H) \nleq A then

Use RationalClasses (N_S(H)/H) to compute T_H

for t \in T_H do

Append {\langle H, t \rangle : t \in T_H} to output.

end for

end if

end for

return \mathcal{R}/S.
```

It follows with Corollaries 3.2 and 3.5 that  $|\operatorname{Sub}(S)/S| = b+r$ . The b+r conjugacy classes of subgroups of S can now be enumerated by the following combination of Algorithms 1 and 2.

Algorithm 3 SubgroupsByCyclicExtension()	
<b>Input</b> Representatives of $\mathcal{B}/A$ .	
<b>Output</b> Representatives of $\operatorname{Sub}(S)/S$ .	
$ ext{return BlueSubgroups}(\mathcal{B}/A) \cup  ext{RedSubgroups}(\mathcal{B}/A).$	

Recall from the introduction that the subgroup pattern of S consists of the list of representatives of the conjugacy classes of subgroups of S and the table of marks of S. Accordingly, the task of computing the subgroup pattern of S from that of A requires the computation of the conjugacy classes of subgroups of S from those of A, and the computation of the table of marks of S from that of A. Algorithm 3 accomplishes the first part of this task.

3.3. Computing the Subgroups of a Solvable Group. Algorithm 3 has enabled us to produce a new algorithm to compute the conjugacy classes of subgroups of a solvable group G in an iterative fashion starting with the conjugacy classes of subgroups of the trivial group. Recall that a solvable group G has a composition series of the form

$$1 = G_0 \trianglelefteq G_1 \ldots \trianglelefteq G_n = G$$

in which each factor  $G_{i+1}/G_i$  is cyclic of prime order. In such cases we can apply the methods described in Propositions 3.1 and 3.4 to compute the conjugacy classes of subgroups of G in a step by step fashion.

The performance of our implementation of this algorithm in GAP compares quite favourably to the existing GAP functions for computing conjugacy classes of subgroups, notably SubgroupsSolvableGroup (see [8]), and the standard GAP function ConjugacyClassesSubgroups for computing conjugacy classes of subgroups.

**Example 3.6.** Consider the General linear group  $GL_2(3)$  of all invertible  $2 \times 2$  matrices over the field with 3 elements.  $GL_2(3)$  is a solvable group and has the following composition series

 $1 \lhd 2 \lhd 4 \lhd Q_8 \lhd \operatorname{SL}_2(3) \lhd \operatorname{GL}_2(3)$ 

Figure 3 shows the growth and fusion of conjugacy classes of subgroups as we incrementally extend from one group in the composition series to the next.

L. NAUGHTON AND G. PFEIFFER



FIGURE 3. Class Fusions in  $GL_2(3)$ 

### 4. The Table of Marks of S

In this section we develop tools for the computation of the table of marks of S from the table of marks of A. For the purpose of describing the table of marks of S in terms of the table of marks of A, we use the partition of the subgroups of S into blue and red subgroups to subdivide the table of marks of S into four quarters, labeled by pairs of colors. We illustrate the situation with the example of the alternating group  $A_5$  as a subgroup of index p = 2 of the symmetric group  $S_5$ . The table of marks of  $A_5$  is shown Figure 4.

$A_{5}/1$	60								
$A_5/C_2$	30	2							
$A_5/C_3$	20		2						
$A_{5}/2^{2}$	15	3		3					
$A_5/C_5$	12				2				
$A_{5}/S_{3}$	10	2	1			1			
$A_{5}/D_{10}$	6	2			1		1		
$A_5/A_4$	5	1	2	1				1	
$A_{5}/A_{5}$	1	1	1	1	1	1	1	1	1
	1	$C_2$	$C_3$	$2^{2}$	$C_5$	$S_3$	$D_{10}$	$A_4$	$A_5$

FIGURE 4. Table of Marks of  $A_5$ 

The subdivided table of marks of  $S_5$  is shown in Figure 5.

$S_{5}/1$	120																		
$S_{5}/C_{2}$	60	4																	
$S_{5}/C_{3}$	40		4																
$S_{5}/2^{2}$	30	6		6															
$S_{5}/C_{5}$	24				4														
$S_{5}/S_{3}$	20	4	2			2													
$S_{5}/D_{10}$	12	4			2		2												
$S_5/A_4$	10	2	4	2				2											
$S_{5}/A_{5}$	2	2	2	2	2	2	2	2	2										
$S_{5}/C_{2}$	60									6									
$S_{5}/C_{4}$	30	2								.	2								
$S_{5}/2^{2}$	30	2								6		2							
$S_{5}/S_{3}$	20		2							6			2						
$S_{5}/C_{6}$	20		2							2				2					
$S_{5}/D_{8}$	15	3		3						3	1	1			1				
$S_5/D_{12}$	10	2	1			1				4		2	1	1		1			
$S_5/5:4$	6	2			1		1			.	2						1		
$S_{5}/S_{4}$	5	1	2	1				1		3	1	1	2		1			1	
$S_{5}/S_{5}$	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
	1	$C_2$	$C_3$	$2^2$	$C_5$	$S_3$	$D_{10}$	$A_4$	$A_5$	$C_2$	$C_4$	$2^2$	$S_3$	$C_6$	$D_8$	$D_{12}$	5:4	$S_4$	$S_5$

FIGURE 5. Table of Marks of  $S_5$ 

Since no red subgroup can be contained in any blue subgroup, the top right quarter, which represents the fixed points of red subgroups on blue subgroups, is zero. In this example, the top left quarter, which represents the fixed points of blue subgroups on blue subgroups, is exactly p times the table of marks of  $A_5$ . The bottom left quarter, which represents the fixed points of blue subgroups on red subgroups, looks like a modified copy of the table of marks of  $A_5$ , in the sense that some rows are repeated, and the row in the table of marks of  $A_5$  corresponding to  $A_5/C_5$  does not appear at all. The bottom right quarter, which represents the fixed points of red subgroups on red subgroups, does not bear any immediate resemblance to the table of marks of  $A_5$ . In the following sections we will examine each of these nonzero quarters separately.

4.1. The Top Left Quarter. Recall that the marks in this quarter represent fixed points of blue groups on blue groups.

**Proposition 4.1.** Suppose that  $H, U \leq A$ . let  $t \in S \setminus A$  and denote  $H_j = H^{t^j}$ , for  $j = 0, 1, \ldots, p-1$ . Then

$$\beta_{S/H}(U) = \sum_{j=0}^{p-1} \beta_{A/H_j}(U).$$

In particular if  $[H]_S = [H]_A$  then  $\beta_{S/H}(U) = p\beta_{A/H}(U)$ .

*Proof.* The coset space S/H is a disjoint union of U-sets,  $\{Hat^j : a \in A\} = \{Ht^ja : a \in A\}$  equivalent to  $A/H_j = \{H^{t^j}a : a \in A\}$ , for j = 0, 1, ..., p - 1.

If  $\mathcal{B}_2 = \emptyset$  then Proposition 4.1 implies that the top left quarter of the table of marks of S will be exactly p times the table of marks of A as observed in the example of  $A_5$  and  $S_5$ . In general this quarter has one row for each class [H]in  $\mathcal{B}/S = \mathcal{B}_1/S \sqcup \mathcal{B}_2/S$ , where, if  $[H] \in \mathcal{B}_1/S$  the row is a p-multiple of the corresponding row in the table of marks of A, and if  $[H] \in \mathcal{B}_2/S$  the row is then the sum of the rows corresponding to the p A-conjugacy classes of subgroups which fuse to form a single S-conjugacy class of subgroups.

4.2. The Bottom Left Quarter. Recall that the marks in this quarter represent the fixed points of blue subgroups on red subgroups.

**Proposition 4.2.** Suppose that  $K \leq S$  is a red subgroup with  $\gamma(K) = H \leq A$ . then the coset spaces S/K and A/H are equivalent as A-sets. In particular,

$$\beta_{S/K}(U) = \beta_{A/H}(U)$$

for all subgroups  $U \leq A$ .

*Proof.* The map  $f : A/H \to S/K$ , defined by  $f(Ha) \mapsto Ka$  for  $a \in A$ , is an A-equivariant bijection and thus the coset spaces are equivalent as U-sets as well.  $\Box$ 

It follows that for any  $K \in \mathcal{R}$  with  $\gamma(K) = H$  we insert a copy of the row corresponding to H in the table of marks of A into the bottom left quarter of the table of marks of S. This accounts for the duplicate rows observed in the example of  $A_5$  and  $S_5$ .

4.3. The Bottom Right Quarter. Recall that the marks in the bottom right quarter represent the fixed points of red subgroups on red subgroups. The marks in this section usually cannot be computed from the table of marks of A using a simple formula. There are, however, obvious lower and upper bounds on these numbers, and various conditions which reduce the number of values that a particular mark can take. If a mark is not uniquely determined by these conditions, one can still compute it explicitly by counting incidences between the relevant conjugacy classes of subgroups. In this section we describe these bounds and conditions on the marks in question and describe how they can be completely determined.

4.3.1. *Bounds.* The marks in the bottom left quarter yield a first upper bound for the marks in the bottom right quarter.

**Lemma 4.3.** Let  $H \leq K \leq S$ . Then

$$\beta_{S/U}(K) \le \beta_{S/U}(H)$$

for all subgroups  $U \leq S$ .

*Proof.* Since  $H \leq K$ , clearly K cannot fix more cosets than H.

In particular if K is a red subgroup with  $\gamma(K) = H \leq A$  then  $\beta_{S/U}(K) \leq \beta_{S/U}(H)$ . Thus the marks in the bottom left quarter, provide an upper bound for the marks in the bottom right quarter. Combining Lemma 4.3 with the following Proposition we obtain a finite range of values for each of the marks in the bottom right quarter.

**Lemma 4.4.** Suppose  $U, V \leq S$  with  $U \leq V$  of index q a prime, and let X be an S-set. Then

$$\beta_X(U) \equiv \beta_X(V) \mod q.$$

*Proof.* Clearly,  $\operatorname{Fix}_X(U)$  can be regarded as a V/U-set. Since the quotient V/U is cyclic of prime order, It follows that V/U can only make orbits of length 1 or q on X.

Now given a column in the bottom right quarter corresponding to  $K \in \mathcal{R}$  with  $\gamma(K) = H$  the marks in the columns corresponding to H and K are congruent modulo q. The practical significance of Lemmas 4.3 and 4.4 is the following; Lemma 4.3 provides an upper bound for each mark in the bottom right quarter. We then utilize Lemma 4.4 to produce, for each undecided mark in the bottom right quarter, a finite range of possible values which the mark might take. It is worth noting that if the upper bound obtained from Lemma 4.3 is an integer < q then we immediately obtain the correct mark in the bottom right quarter.

The task now is to attempt to reduce the size of the finite range of values at each undecided position in the bottom right quarter.

4.3.2. Transitivity. Our first tool to reduce the number of possibilities at each position in the bottom right quarter is based on the notion of transitivity. This process provides upper and lower bounds for undecided marks in the bottom right quarter of the table of marks of S. The procedure, which is described below, is based on the transitivity of subgroup inclusion,

$$U \leq V$$
 and  $V \leq K \Rightarrow U \leq K$ .

In terms of conjugacy classes of subgroups this means the following. If V is contained in p conjugates of K then so is U. And if V contains m conjugates of U then so does K.

At this point in the computation an undecided entry,  $\beta_{S/K}(U)$ , is represented by a finite range of possible values, one of which is the correct mark. The strategy is to use transitivity to reduce the number of values in this range. For clarity we distinguish between the following two situations in Corollary 4.5 and Corollary 4.6.

# Corollary 4.5. Let $U \leq V \leq K$ . Then

- (i) any lower bound for  $\beta_{S/K}(V)$  is also a lower bound for  $\beta_{S/K}(U)$ .
- (ii)  $\beta_{S/K}(U) \ge \beta_{S/V}(U)/|\dot{K}:V|$ .

*Proof.* (i) Follows from Lemma 4.3. (ii) Follows from the fact that K contains at least as many conjugates of U as V does, together with Formula 2.2.

**Corollary 4.6.** Let  $V \leq U \leq K$ . Then any upper bound for  $\beta_{S/K}(V)$  is also an upper bound for  $\beta_{S/K}(U)$ .

*Proof.* Follows from the fact that U is contained in at least as many conjugates of K as V is, or simply from Lemma 4.3.

4.3.3. Dress Congruences. In this section we will describe a refinement of the Dress congruences which enables us to decide the correct entry in many of the positions in the bottom right quarter. Let  $U \leq A$ . As before denote  $W = N_S(U)/U$ , and regard W as the union of  $B = N_A(U)/U$  (its "blue" elements) and  $R = W \setminus B$  (its "red" elements). Note that  $|B| = \frac{1}{p}|W|$  and that  $|R| = (p-1)|B| = \frac{p-1}{p}|W|$ . If X is an S-set, then  $Y = \operatorname{Fix}_X(U)$  is a W-set and by restriction a B-set.

Consider the S-set X = S/K for a red subgroup K with  $\gamma(K) = H \leq A$ . By Proposition 4.2, X is equivalent to A/H as an A-set. It follows that  $\operatorname{Fix}_{S/K}(H)$  is equivalent to  $Y = \operatorname{Fix}_{A/H}(H)$  as *B*-sets. We set

$$o_W = \frac{1}{|W|} \sum_{w \in W} \pi_Y(w)$$

to be the number of orbits of W on Y, and set

$$o_B = \frac{1}{|B|} \sum_{w \in B} \pi_Y(w)$$

to be the number of orbits of B on Y. We also set

$$o_R = \frac{1}{|B|} \sum_{w \in R} \pi_Y(w).$$

**Proposition 4.7.** With the above notation

(i)  $o_R \equiv -o_B \pmod{p}$ , (ii)  $o_R \leq (p-1)o_B$ .

*Proof.* By construction,

$$po_W = o_B + o_R$$

and  $o_B \in \mathbb{Z}$  implies  $o_R \in \mathbb{Z}$  and

$$o_B + o_R \equiv 0 \pmod{p}$$

Moreover,  $B \leq W$  implies  $o_W \leq o_B$ , and thus

$$o_R = po_W - o_B \le po_B - o_B = (p - 1)o_B$$

as claimed.

Let  $\{H_i\}, i = 1, ..., b$  and  $\{K_j\}, j = 1, ..., r$  be a list of representatives of  $\mathcal{B}/S$  and  $\mathcal{R}/S$  respectively, and let X be an S-set. It follows from Theorem 2.5 that,

(4.1) 
$$\sum_{i=1}^{b} n(U, H_i) \beta_X(H_i) + \sum_{j=1}^{r} n(U, K_j) \beta_X(K_j) = c \cdot |W|,$$

for  $U \leq S$  where c is the number of orbits of W on  $Y = \operatorname{Fix}_X(U)$ , i.e.  $c = o_W$ . Moreover,

(4.2) 
$$\sum_{i=1}^{o} n(U, H_i) \beta_X(H_i) = |B| \cdot o_B$$

and

(4.3) 
$$\sum_{j=1}^{r} n(U, K_j) \beta_X(K_j) = |B| \cdot o_R.$$

Since the numbers  $o_B$  are determined by the marks in the bottom left quarter of the table of marks of S, we get the following conditions on the marks in the bottom right quarter.

**Corollary 4.8.** Let  $K \in \mathcal{R}$  and let  $U, o_B$  be as above. Then the marks  $\beta_{S/K}(K_j)$  must satisfy,

$$\frac{1}{|B|} \sum_{j=1}^{r} n(U, K_j) \beta_{S/K}(K_j) \equiv -o_B \pmod{p}$$

and

Ī

$$\frac{1}{|B|} \sum_{j=1}^{r} n(U, K_j) \beta_{S/K}(K_j) \le (p-1) \cdot o_B.$$

**Example 4.9.** Table 6 shows the complete Dress congruence matrix for  $S_5$ . The integer entries in the table represent the numbers

$$n(U,H) = \#\{Ua \in N_{S_5}(U)/U : \langle U,a \rangle \sim_{S_5} H\}$$

where U and H run over a transversal of the conjugacy classes of subgroups of S. The final column lists |W| for  $W = N_{S_5}(U)/U$ .

U	1	$C_2$	$C_3$	$2^2$	$C_5$	$S_3$	$D_{10}$	$A_4$	$A_5$	$C_2$	$C_4$	$2^2$	$S_3$	$C_6$	$D_8$	$D_{12}$	5:4	$S_4$	$S_5$	W
1	1	15	20		24					10	30			20						120
$C_2$		1		1							1	1								4
$C_3$			1			1							1	1						4
$2^2$				1				2							3					6
$C_5$					1		1										2			4
$S_3$						1										1				2
$D_{10}$							1										1			2
$A_4$								1										1		2
$A_5$									1										1	2
$C_2$										1		3		2						6
$C_4$											1				1					2
$2^2$												1			1					2
$S_3$													1			1				2
$C_6$														1		1				2
$D_8$															1					1
$D_{12}$																1				1
5:4																	1			1
$S_4$																		1		1
$S_5$																			1	1

FIGURE 6. Dress Congruence Matrix for  $S_5$ 

For example, the congruence corresponding to U = 1 is

 $y_1 + 15y_2 + 20y_3 + 24y_5 + 10y_{10} + 30y_{11} + 20y_{14} \equiv 0 \pmod{120}.$ 

Each row of the table of marks of  $S_5$  must satisfy all the congruences.

To illustrate how Corollary 4.8 yields conditions on the marks in the bottom right quarter, consider the impression

 $\beta_{S_5/D_{12}} = \big(10, 2, 1, 0, 0, 1, 0, 0, 0, y_{10}, y_{11}, y_{12}, y_{13}, y_{14}, y_{15}, y_{16}, y_{17}, y_{18}, y_{19}\big)$ 

of  $S_5$  on  $S_5/D_{12}$ . The marks  $\{y_1, \ldots, y_9\}$  of the blue subgroups are known from Section 4.2. The marks of the red subgroups are represented by  $y_i$  for  $i \in \{10, \ldots, 19\}$ . The congruence from  $U = C_2$  in the top half of Figure 6 reads

$$y_2 + y_4 + y_{11} + y_{12} \equiv 0 \pmod{4}.$$

Clearly  $o_B = \frac{1}{2}(y_2 + y_4) = 1$ . Moreover,  $o_R = \frac{1}{2}(y_{11} + y_{12})$ . It follows from Corollary 4.8 that

(i)  $o_R \equiv 1 \pmod{2}$ (ii)  $o_R \leq 1$ .

Hence  $o_R = 1$  and so  $y_{11} + y_{12} = 2$ . Lemmas 4.3 and 4.4 yield  $y_{11}, y_{12} \in \{0, 2\}$ . We conclude that either  $y_{11} = 0, y_{12} = 2$  or  $y_{11} = 2, y_{12} = 0$ . In this fashion the congruences yield conditions on the marks in the bottom right quarter of the table of marks.

4.3.4. Explicit Testing of Incidences. If all other approaches fail, one can explicitly count the number of conjugates of K which lie above a subgroup V and compute the mark  $\beta_{S/K}(V)$  using Proposition 2.2.

In order to avoid listing entire conjugacy classes of subgroups, we introduce the following subsets of a conjugacy class of subgroups. For a subgroup  $K \leq S$  and an element  $t \in S$  denote

$$X(K,t) = \{K' \in [K]_S : t \in K'\}.$$

**Lemma 4.10.** Let  $V \leq S$  and  $t \in S$ . Then

$$\{K' \in [K]_S : V \le K'\} = \{K' \in X(K,t) : V \le K'\}$$

*Proof.* By definition X(K,t) is precisely the subset of  $[K]_S$  consisting of those conjugates K' of K which contain the element  $t \in V$ . Thus  $K' \geq V$  implies  $K' \in X(K,t)$ .

In particular if V is a red subgroup and  $t \in V \setminus A$  then

$$\beta_{S/K}(V) = |N_S(K) : K| \cdot \#\{K' \in X(K, t) : V \le K'\}.$$

Such a set X(K,t) can be computed efficiently, using Proposition 2.2, as follows.

**Proposition 4.11.** Let  $K \leq S$  and  $t \in S$ . Then

- (i) the centralizer  $C = C_S(t)$  acts on X(K, t) by conjugation;
- (ii) the normalizer  $N = N_S(K)$  acts on  $T = K \cap [t]_S$  by conjugation;
- (iii) the map  $\xi: X/C \to T/N$  given by

$$\xi([K^s]_C) = [t^{s^{-1}}]_N$$

is a well defined bijection.

*Proof.* (i) and (ii) are obvious. (iii) If  $Z = \{(K', t') \in [K]_S \times [t]_S : t' \in K'\}$  then Z is S-invariant, X(k,t) = Zt and the claim follows with Proposition 2.2.

This result allows us to compute the set

$$X(K,t) = \prod_{[a]_N \in K/N, a^s = t} [K^s]_C$$

systematically as a disjoint union of *C*-orbits of conjugates of *K*, by first computing the conjugacy classes of elements of *K*, partitioning them into *N*-orbits, and selecting those consisting of conjugates of *t*. For each such *N*-orbit  $[a]_N$  one finds a conjugating element  $s \in S$  with  $a^s = t$  and then computes the *C*-orbit of the conjugate  $K^s$ .

### 5. Computation

Propositions 4.1 and 4.2 enable us to determine the marks in the top left and bottom left quarters respectively. The bounds described in Section 4.3.1 yield a partially complete bottom right quarter, where, if a mark is undecided, it is represented by a finite range of values. We work our way down through the table of marks completing each row before we move on to the next one. We apply the congruences and the transitivity tests until the row is completed or no new mark is obtained. If there are still undecided marks we use the explicit incidence test from Section 4.3.4 with a single t to compute as many marks as possible. Then we apply the congruences and transitivity tests again. If there are still undecided marks we run the incidence test again with a different t and repeat the process until the row is complete. The entire process is summarized in Algorithm 5.

# Algorithm 5 TableOfMarksByCyclicExtension() **Input** Subgroup pattern (Sub(A)/A, M(A)) of A. **Output** Subgroup pattern of S. Compute $\operatorname{Sub}(S)/S$ as $\operatorname{SubgroupsByCyclicExtension}(\operatorname{Sub}(A)/A)$ . Use Proposition 4.1 to compute top left quarter of M(S). Use Proposition 4.2 to compute bottom left quarter of M(S). for each row in bottom right of M(S) do Implement bounds from Subsection 4.3.1. while row is incomplete do Apply congruences (4.3.3) and transitivity (4.3.2) until no more new marks are found. if row still contains undecided marks then Compute some marks explicitly (4.3.4). end if end while end for return $(\operatorname{Sub}(S)/S, \operatorname{M}(S))$ .

This algorithm completes the task of computing the subgroup pattern of S from that of A. Some of the results obtained by a GAP implementation of this algorithm are listed in Section 5.2.

5.1. Computing the Table of Marks of a Solvable Group. In Section 3.3 we described a new algorithm to compute the conjugacy classes of subgroups of a solvable group G. In the same spirit we have developed an algorithm to compute the table of marks of a solvable group G based on the procedures described in the preceding sections. The strategy is the same as in Section 3.3. We take as input a solvable group G, and work our way up through the composition series of G starting with the table of marks of the trivial group, computing the table of marks of each group in the series in turn until we obtain the table of marks of G itself.

Algorithm 6 TableOfMarksSolvableGroup()

Input A solvable group G. Output Subgroup pattern  $(\operatorname{Sub}(G)/G, \operatorname{M}(G))$  of G. Compute a composition series  $1 = G_0 \leq G_1 \leq \ldots \leq G_n = G$ Set  $P_0 \leftarrow (\operatorname{Sub}(1)/1, \operatorname{M}(1))$ . for  $i \in \{1, \ldots, n\}$  do  $P_i \leftarrow \operatorname{TableOfMarksByCyclicExtension}(P_{i-1})$ . end for return  $P_n$ .

**Example 5.1.** Recall the example of  $GL_2(3)$  from Section 3.3, and its associated composition series

$$1 \triangleleft 2 \triangleleft 4 \triangleleft Q_8 \triangleleft \operatorname{SL}_2(3) \triangleleft \operatorname{GL}_2(3)$$

In this example we apply Algorithm 6 starting with the table of marks of the trivial group to obtain the table of marks of  $GL_2(3)$ .



FIGURE 7. Table of Marks of  $GL_2(3)$ 

5.2. Results and Statistics. The methods described in this article have been used to extend the GAP table of marks library Tomlib. Tables 1 and 2 list some of the groups to which these methods have been applied together with running times for the computations. Table 1 contains two extra columns labeled #X(K,t) and  $\max[X(K,t)]$  where #X(K,t) records the number of times a mark is computed

explicitly based on Section 4.3.4, and  $\max|X(K,t)|$  records the length of the largest orbit which is computed for such a calculation. The computations were carried out on an Apple MacBook Pro with an Intel Core 2 Duo CPU T7500 @ 2.20GHz with 2 gigabytes of RAM.

A	S	$ \operatorname{Sub}(A)/A $	$ \operatorname{Sub}(S)/S $	#X(K,t)	$\max  X(K,t) $	Time
$A_5$	$S_5$	9	19	0	0	1s
$A_6$	$S_6$	22	56	2	4	2s
$A_7$	$S_7$	40	96	3	20	3s
$A_8$	$S_8$	137	296	26	60	20s
$A_9$	$S_9$	223	554	82	140	50s
$A_{10}$	$S_{10}$	430	1593	381	384	6m
$A_{11}$	$S_{11}$	788	3094	912	960	20m
$A_{12}$	$S_{12}$	2537	10723	6161	3240	7h
$A_{13}$	$S_{13}$	4558	20832	12316	15120	43h

TABLE 1. Results for Symmetric Groups

A	S	$ \operatorname{Sub}(A)/A $	$ \mathrm{Sub}(S)/S $	Time
He	He.2	1698	1930	$231 \mathrm{m}$
HS	HS.2	589	2057	35m
Sz(8)	Sz(8).3	22	39	3s
$^{2}F_{4}(2)'$	$^{2}F_{4}(2)$	434	849	48m
$L_2(32)$	$L_2(32).5$	24	30	4s

## TABLE 2. More Results

A GAP implementation of the algorithms is available on request from the authors.

Acknowledgment: Much of the work in this article is based on the first authors PhD thesis (see [9]). This research was supported by Science Foundation Ireland (07/RFP/MATF466).

### References

- Serge Bouc, Burnside rings, Handbook of algebra, Vol. 2, North-Holland, Amsterdam, 2000, pp. 739–804. MR 1759611 (2001m:19001)
- Thomas Breuer and Götz Pfeiffer, Finding possible permutation characters, J. Symbolic Comput. 26 (1998), no. 3, 343–354. MR 1633876 (99e:20005)
- Francis Buekenhout, Diagrams for geometries and groups, J. Combin. Theory Ser. A 27 (1979), no. 2, 121–151. MR 542524 (83f:51003)
- Francis Buekenhout and Sarah Rees, The subgroup structure of the Mathieu group M<sub>12</sub>, Math. Comp. 50 (1988), no. 182, 595–605. MR 929556 (88m:20024)
- W. Burnside, Theory of groups of finite order, Dover Publications Inc., New York, 1955, 2d ed. MR 0069818 (16,1086c)
- Andreas Dress, A characterisation of solvable groups, Math. Z. 110 (1969), 213–217. MR 0248239 (40 #1491)
- 7. The GAP Group, GAP Groups, Algorithms, and Programming, Version 4.4.12, 2008, http://www.gap-system.org.

- Alexander Hulpke, Computing subgroups invariant under a set of automorphisms, J. Symbolic Comput. 27 (1999), no. 4, 415–427. MR 1681348 (2000a:20001)
- 9. Liam Naughton, Computing the table of marks of a finite group, Ph.D. thesis.
- Peter M. Neumann, A lemma that is not Burnside's, Math. Sci. 4 (1979), no. 2, 133–141. MR 562002 (81g:01012)
- Götz Pfeiffer, The subgroups of M<sub>24</sub>, or how to compute the table of marks of a finite group, Experiment. Math. 6 (1997), no. 3, 247–270. MR 1481593 (98h:20032)
- 12. Tomlib, Version 1.2.1, (2011), http://schmidt.nuigalway.ie/tomlib.

SCHOOL OF MATHEMATICS, STATISTICS AND APPLIED MATHEMATICS, NUI, GALWAY *E-mail address*: liam.naughton@nuigalway.ie, goetz.pfeiffer@nuigalway.ie