The Burnside Ring and Applications: Outline for Math8245, Spring 2016

1. The Möbius Function. Hall's application to finding numbers of generators.
References:
Nathan Fox, Some applications of the Möbius function, Honors thesis, University of Minnesota 2012.
P. Hall, The Eulerian Functions of a Group, Quart. J. Math. (Oxford) 7 (1936), 134-151.

2. The Burnside Ring. The marks homomorphism and semisimplicity. The idempotent formula of Gluck and Yoshida.
References: D.J. Benson, Representations and cohomology I, Cambridge University Press, section 5.4.
S. Bouc, Burnside rings, Handbook of algebra vol 2, 739 - 804, Elsevier 2000.
D. Gluck, Idempotent formula for the Burnside ring with applications to the p-subgroups complex, Illinois J. Math 25 (1981), 63-67.

3. Conlon's induction theorem and formulas for cohomology.
References: Benson and Bouc as above.
P.J. Webb, Subgroup complexes, pp. 349-365 in: ed. P. Fong, The Arcata Conference on Representations of Finite Groups, AMS Proceedings of Symposia in Pure Mathematics 47 (1987).
P.J. Webb, A local method in group cohomology, Commentarii Math. Helv. 62 (1987), 135-167.

4. The posets of non-identity p-subgroups, elementary abelian p-subgroups, and p-radical subgroups. Homotopy equivalence, contractibility of fixed points and of the orbit space, cohomology formulas.
References as above, and
P.J. Webb and J. Thévenaz, Homotopy equivalence of posets with a group action, J. Combinat. Theory Ser. A. 56 (1991), 173-181.

Some Applications of the Möbius Function

Nathan Fox

April 26, 2012

Abstract

The Möbius function is an important concept in combinatorics. First developed for number theory, it has since been extended to arbitrary posets, where it allows inversion of certain functions. One type of poset of particular interest is the subgroup lattice of a finite group. In this paper, we examine some fundamental results about the Möbius function, including the powerful inversion formula, and then we discuss the implications of applying the Möbius function to subgroup lattices.

1 The Möbius Function

We have the following definition [4]:

Definition 1.1. Given a partially ordered set P, and given $a, b \in P$, the *Möbius function* associated to P is a map $\mu : P \times P \to \mathbb{Z}$ such that

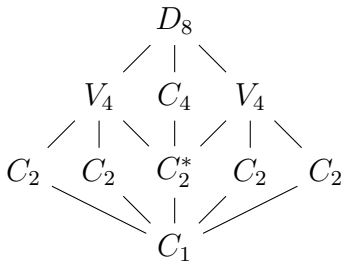
$$\mu(a,b) = \begin{cases} 1 & a = b \\ -\sum_{a<c\leq b} \mu(c,b) & a < b \\ 0 & \text{otherwise} \end{cases}.$$

If P has a largest element $\mathbf{1}$, the argument b is often omitted, and $\mu(a)$ is assumed to mean $\mu(a, \mathbf{1})$.

A special case of a Möbius function is the classical Möbius function from number theory. In that case, the poset is the positive integers, where $a < b$

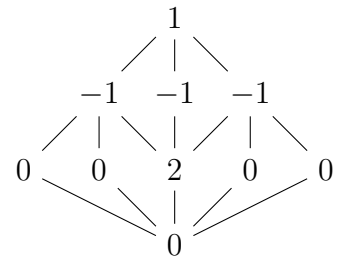
if $a \mid b$ and $a \neq b$. For the most part, we will consider Möbius functions over subgroup lattices of finite groups (ordered by containment).

As an example, here is the subgroup lattice of D_8, the dihedral group of order 8:



The four C_2 subgroups not marked with an asterisk are those generated by the group elements including a reflection. They are all conjugate to one another, as are the Klein four groups labeled V_4 which contain them. The asterisked C_2 is not conjugate to the others. It is generated by the 180° rotation of the square on which D_8 acts.

We will now compute the Möbius function of each of these subgroups. We will consider each conjugate collection of subgroups once, as all will have the same value of the Möbius function. First, by definition, $\mu(D_8) = 1$. Then, $\mu(V_4)$ and $\mu(C_4)$ must both equal -1. From here, we see that $\mu(C_2) = -(-1+1) = 0$ and $\mu(C_2^*) = -(-1-1-1+1) = 2$. Finally, $\mu(C_1) = -(2-1-1-1+1) = 0$. Here is the same diagram as before, with each subgroup replaced by the value of its Möbius function:



Additionally, we note that there is an alternative, equivalent definition for the Möbius function:

Proposition 1.2. *Given a poset P and $a, b \in P$, we have*

$$\mu(a,b) = \begin{cases} 1 & a = b \\ -\sum_{a \le c < b} \mu(a,c) & a < b \\ 0 & \text{otherwise} \end{cases}.$$

Proof. This equivalence is proved inductively by length of the longest chain between a and b. (We will include the endpoints in computing the length of a chain.) First, if the longest such chain has length 2, the original formula equals $\mu(b,b) = 1$, and this new formula equals $\mu(a,a) = 1$. Now, assume that these formulas are equivalent if the length of the longest chain between the two elements is less than m. Assume that the length of the longest chain between a and b is m. The old formula gives (with the inductive hypothesis assumed)

$$\begin{aligned} \mu(a,b) &= -\sum_{a < c \le b} \mu(c,b) \\ &= -\mu(b,b) - \sum_{a < c \le b} \left(-\sum_{c \le d < b} \mu(c,d) \right) \\ &= -1 + \sum_{a < c \le d < b} \mu(c,d) \end{aligned}$$

and the new formula gives

$$\begin{aligned} \mu(a,b) &= -\sum_{a \le c < b} \mu(a,c) \\ &= -\mu(a,a) - \sum_{a \le c < b} \left(-\sum_{c < d \le b} \mu(c,d) \right) \\ &= -1 + \sum_{a < c \le d < b} \mu(c,d). \end{aligned}$$

These formulas are clearly the same. □

2 The Möbius Inversion Formula

The Möbius function has a well-known application to inverting certain functions over posets. Here is the Möbius inversion formula [4]:

Proposition 2.1. *Let P be a poset, let G be an additive abelian group, and let $f : P \to G$ be a function. Let $a \in P$ be fixed. We define another function, $F : P \to G$ as follows: For $b \in P$,*

$$F(b) = \sum_{a \leq x \leq b} f(x).$$

Then, for $b \geq a$, we have

$$f(b) = \sum_{a \leq x \leq b} \mu(x, b) F(x).$$

Proof. We will prove this formula inductively. First, we have that

$$f(a) = F(a).$$

Hence, a satisfies the formula

$$f(a) = \sum_{a \leq x \leq a} \mu(x, a) F(a) = F(a).$$

Now, let $b \in P$ such that $a \leq b$, and assume we have shown for $a \leq c < b$ that

$$f(c) = \sum_{a \leq x \leq c} \mu(x, c) F(x).$$

The quantity $f(b)$ is given by

$$\begin{aligned}
f(b) &= F(b) - \sum_{a \leq x < b} f(x) \\
&= F(b) - \sum_{a \leq x < b} \sum_{y \leq x} \mu(y, x) F(y) \\
&= F(b) - \sum_{a \leq y < x} \sum_{y \leq x < b} \mu(y, x) F(y) \\
&= F(b) - \sum_{a \leq y < b} F(y) \sum_{y \leq x < b} \mu(y, x) \\
&= \mu(b, b) F(b) - \sum_{a \leq y < b} F(y) (-\mu(y, b)) \\
&= \sum_{a \leq y \leq b} \mu(y, b) F(b).
\end{aligned}$$

as required. □

3 Number of Generating n-Tuples of a Group

In 1936, Philip Hall published a paper that first showed the importance of the inversion formula over a lattice of subgroups. His application of the inversion formula allows for computation of the the number of ordered n-tuples which generate a finite group G in terms of the Möbius function over the subgroup lattice of G. He denotes the number of such n-tuples by $\phi_n(G)$. Here is Hall's inversion formula [2]:

Theorem 3.1. *Let G be a finite group. Then, for each positive integer n,*

$$\phi_n(G) = \sum_{H \leq G} \mu(H) |H|^n.$$

Proof. Let H be any subgroup of G. Let $F(H)$ be the total number of n-tuples of H, so that $F(H) = |H|^n$. We see that

$$F(H) = \sum_{K \leq H} \phi_n(K)$$

since every n-tuple of H generates some subgroup K of H, and the number which generate K is $\phi_n(K)$. We deduce that $\phi_n(G)$ has the desired formula by applying the Möbius inversion formula over the lattice of subgroups of G, taking $f(H) = \phi_n(H)$.

□

We will now show a result that follows from knowing $\phi_n(G)$ for a finite *simple* group G. First, we will prove a lemma.

Lemma 3.2. *Let G be a non-abelian finite simple group, and let s be a positive integer. The only normal subgroups of G^s are direct products of the factors.*

Proof. Let $N \triangleleft G^s$. Suppose $\vec{g} = (g_1, \ldots, g_s) \in N$ with $g_j \neq e$. For any element $\vec{a} = (e, \ldots, e, a, e, \ldots, e)$ with a in position j,

$$\vec{a}\vec{g}\vec{a}^{-1} = \left(g_1, \ldots, ag_ja^{-1}, \ldots, g_s\right) \in N.$$

Multiplying by $\vec{g}^{-1}$ yields that $\left(e, \ldots, e, ag_ja^{-1}g_j^{-1}, e, \ldots, e\right) \in N$. Since G is non-abelian, we can find a so that $ag_ja^{-1}g_j^{-1} \neq e$. Since the conjugates of any non-identity element of G generate G, we see that

$$\{e\} \times \cdots \times \{e\} \times G \times \{e\} \times \cdots \times \{e\} < N.$$

Hence, we obtain that N is equal to the product of those factors G for which N has an element which is not e in that factor. This is a direct product of the factors, as required. $\square$

Now, we will prove one of our main results. Hall's paper implicitly uses this result, but he does not prove it.

Theorem 3.3. *Let G be a finite simple group that is not cyclic, and let n be a positive integer. The ratio*

$$d_n(G) := \frac{\phi_n(G)}{|\operatorname{Aut} G|}$$

is equal to the maximum power of G that can be generated by n elements.

Proof. First, we will show that this ratio is equal to the number of kernels for homomorphisms $F_n \to G$, where F_n is the free group with n generators. Such homomorphisms can be denoted $f_{(g_1,\ldots,g_n)}$, where $(g_1,\ldots,g_n)$ generates G and the homomorphism is determined by mapping variable x_i in the free group to g_i. Let $N_{f_{(g_1,\ldots,g_n)}} \lhd F_n$ be the kernel of $f_{(g_1,\ldots,g_n)}$. We have $F_n/N_{f_{(g_1,\ldots,g_n)}} \cong G$.

$\operatorname{Aut} G$ permutes ordered n-tuples that generate G freely with the action $\alpha \cdot (g_1,\ldots,g_n) = (\alpha g_1,\ldots,\alpha g_n)$ for $\alpha \in \operatorname{Aut} G$. The orbits all have size $|\operatorname{Aut} G|$. We will now prove that $(g_1,\ldots,g_n)$ and $(h_1,\ldots,h_n)$ lie in the same orbit if and only if $\ker f_{(g_1,\ldots,g_n)} = \ker f_{(h_1,\ldots,h_n)}$. From this point forward, we will denote $(g_1,\ldots,g_n)$ by $\vec{g}$ and $(h_1,\ldots,h_n)$ by $\vec{h}$.

For the forward direction, assume that $\vec{g}$ and $\vec{h}$ lie in the same orbit. Then, there exists $\alpha \in \operatorname{Aut} G$ such that $\alpha(\vec{g}) = \vec{h}$. We claim that $\alpha \circ f_{\vec{g}} = f_{\vec{h}}$. This follows immediately from the fact that $f_{\vec{h}}(x_i) = h_i$ and $\alpha \circ f_{\vec{g}} = \alpha(g_i) = h_i$. Hence, if $u \in F_n$, then $u \in \ker f_{\vec{h}}$ if and only if $f_{\vec{h}}(u) = e = \alpha \circ f_{\vec{g}}(u)$. This occurs if and only if $f_{\vec{g}}(u) = e$, namely, $u \in \ker f_{\vec{g}}$, as required.

To show the reverse direction, we assume that $\ker f_{\vec{g}} = \ker f_{\vec{h}} = N$. The First Isomorphism Theorem yields isomorphisms $\theta_{\vec{g}}, \theta_{\vec{h}} : F_n/N \to G$ given by $\theta_{\vec{g}}(uN) = f_{\vec{g}}(u)$ and $\theta_{\vec{h}}(uN) = f_{\vec{h}}(u)$. Let $\alpha = \theta_{\vec{h}} \circ \theta_{\vec{g}}^{-1}$. We see immediately that $\alpha \in \operatorname{Aut}(G)$. We claim that $\vec{h} = \alpha(\vec{g})$. We verify:

$$\alpha(g_i) = \theta_{\vec{h}} \circ \theta_{\vec{g}}^{-1}(g_i) = \theta_{\vec{h}}(x_i N) = h_i,$$

as required.

Hence, different kernels from such homomorphisms are in bijection with $\operatorname{Aut} G$ orbits of ordered pairs. Hence, the total number is the ratio described before.

Let d be this ratio. Number the kernels of the homomorphism N_1 through N_d. We claim that $F_n/(N_1 \cap \cdots \cap N_d) \cong G^d$, thereby proving that G^d can be generated by n elements. After proving this, we will show that G^{d+1} cannot be generated by n elements, and that will complete the proof.

We will now prove that $F_n/(N_1 \cap \cdots \cap N_t) \cong G^t$ by induction on t. The case $t = 1$ is the First Isomorphism Theorem from group theory. Now, suppose $t > 1$ and the result is true for smaller values of t. Specifically, $F_n/(N_1 \cap \cdots \cap N_{t-1}) \cong G^{t-1}$. Let $H = \langle N_1 \cap \cdots \cap N_{t-1}, N_t \rangle$. We have $H \lhd F_n$, so $H/N_t \lhd F_n/N_t \cong G$. Since G is simple, we have $H/N_t \cong F_n/N_t$ or $H/N_t \cong N_t/N_t$, so $H = F_n$ or $H = N_t$.

We can exclude the second case. Assume for a contradiction that $H = N_t$. Then, $N_1 \cap \cdots \cap N_{t-1} < N_t$. Then we have that

$$N_t/(N_1 \cap \cdots \cap N_{t-1}) \lhd F_n/(N_1 \cap \cdots \cap N_{t-1}) \cong G^{t-1},$$

and the the quotient of these groups is isomorphic to G by the Third Isomorphism Theorem. By Lemma 3.2, the normal subgroup is the product of $t-2$ of the factors. Let the missing factor be the j^{th}, corresponding to kernel N_j. We will now show that $N_t = N_j$, which is a contradiction. First, both N_t and N_j contain $N_1 \cap \cdots N_{t-1}$. Also, both of their images in $F_n/(N_1 \cap \cdots \cap N_{t-1})$ have the property that upon factoring them out we obtain the j^{th} G factor. Hence, their images are equal, so $N_t = N_j$ by the one-to-one correspondence between subgroups of F_n containing $N_1 \cap \cdots \cap N_{t-1}$ and subgroups of $F_n/(N_1 \cap \cdots \cap N_{t-1})$ given by the First Isomorphism Theorem.

Now, by the Second Isomorphism Theorem, $N_t/(N_1 \cap \cdot \cap N_t) \cong G^{t-1}$ and $(N_1 \cap \cdots \cap N_{t-1})/(N_1 \cap \cdots \cap N_t) \cong G$. So, $F_n/(N_1 \cap \cdots \cap N_t)$ has two normal subgroups which generate F_n and intersect in 1. Therefore, $F_n/(N_1 \cap \cdots \cap N_t)$ is their direct product, namely G^t.

Finally, we show that G^{d+1} cannot be generated by n elements. If it can be, then there is a normal subgroup $J \lhd F_n$ so that $F_n/J \cong G^{d+1}$. Consider the $d+1$ projections $F_n \to G^{d+1} \to G$. The kernels are all different, with quotient G. This contradicts the fact that there are only d possible distinct kernels. Hence, G^{d+1} cannot be generated with n elements. □

We will now give two examples. First, let $G = A_5$. This, the alternating group on 5 letters (which has 60 elements), is the smallest non-abelian simple group. We have from [1] that $|\mathrm{Aut}\, A_5| = 120$. Hall's paper [2] gives the inversion formula of A_5 as

$$\phi(A_5) = \sigma(A_5) - 5\sigma(A_4) - 6\sigma(D_{10}) - 10\sigma(S_3) + 20\sigma(C_3) + 60\sigma(C_2) - 60\sigma(C_1).$$

Hall uses the notation σ for the function of each subgroup, because he considers functions that are more general than the number of generating n-tuples. Letting $\sigma(H) = |H|^n$ here, though, yields that

$$\begin{aligned} d_n(G_{168}) &= \frac{60^n - 5 \cdot 12^n - 6 \cdot 10^n - 10 \cdot 6^n + 20 \cdot 3^n + 60 \cdot 2^n - 60}{120} \\ &= 30 \cdot 60^{n-2} - 6 \cdot 12^{n-2} - 5 \cdot 10^{n-2} - 3 \cdot 6^{n-2} + \frac{3^{n-1}}{2} + 2^{n-1} - \frac{1}{2}. \end{aligned}$$

Substituting a given positive integer n into this formula gives the largest direct product of A_5 that can be generated with n elements. For $n = 2$, this is 19; for $n = 3$ it is 1668. Hence, the group A_5^{1668}, a group of order 60^{1668}, can be generated by only three elements! This is a group some 8.9×10^{2913} times larger than the Monster group [1].

Second, let $G = G_{168} = GL(3, 2)$. This is the simple group of order 168. We have from [1] that $|\mathrm{Aut}\, G_{168}| = 2 \cdot 168 = 336$. Hall's paper [2] gives the inversion formula of G_{168} as

$$\begin{aligned} \phi(G_{168}) = \sigma(G_{168}) &- 14\sigma(S_4) - 8\sigma(M_{7,3}) + 21\sigma(D_8) \\ &+ 28\sigma(S_3) + 56\sigma(C_3) - 84\sigma(C_2) \end{aligned}$$

where in Hall's notation, $M_{7,3}$ is the non-abelian group of order 21. Letting $\sigma(H) = |H|^n$ yields that

$$\begin{aligned} d_n(G_{168}) &= \frac{168^n - 14 \cdot 24^n - 8 \cdot 21^n + 21 \cdot 8^n + 28 \cdot 6^n + 56 \cdot 3^n - 84 \cdot 2^n}{336} \\ &= 84 \cdot 168^{n-2} + 24^{n-1} + \frac{21^{n-1}}{2} + 4 \cdot 8^{n-2} + 3 \cdot 6^{n-2} + \frac{3^{n-1}}{2} + 2^{n-2}. \end{aligned}$$

Substituting a given positive integer n into this formula gives the largest direct product of G_{168} that can be generated with n elements. For $n = 2$, this is 57.

4 Growth Sequences of Finite Groups

A question that now comes to mind is, in general, given a finitely-generated group G and a positive integer n, what is the minimal number of generators for G^n. We will use the notation $d(G)$ to mean the minimal number of generators of G. As before, for simple G, $d_m(G)$ is the largest integer k such

PROOF. Since $M \cong F^n(M)$, there is a matrix $X \in GL_r(k)$ such that for all $g \in G$, $X\phi(g)X^{-1} = F^n\phi(g)$. By a theorem of Lang (see for example Srinivasan [**191**], p. 11), the map $Y \mapsto F^n(Y)^{-1}Y$ on $GL_r(k)$ is surjective, and so we may write $X = F^n(Y)^{-1}Y$ for some $Y \in GL_r(k)$. Then for all $g \in G$ we have $Y\phi(g)Y^{-1} = F^n(Y\phi(g)Y^{-1})$. Thus changing basis by means of Y, we see that the image of $G \to GL_r(k)$ lies in $GL_r(\mathbb{F}_{p^n})$ as required. □

COROLLARY 5.3.5. *Suppose k contains the primitive γth roots of unity, where γ is the p'-part of the exponent of G. Then the $\mathbb{Z}$-rank of $\mathcal{R}(kG)$ (i.e., the number of isomorphism types of p-modular irreducible representations of G) is equal to the number of conjugacy classes of p'-elements of G.* □

EXERCISE. Use the above arguments to count the number of isomorphism types of p-modular irreducible representations of G in case k does not contain the γth roots of unity.

COROLLARY 5.3.6. *The representation ring $A(G)$ decomposes as a direct sum of ideals*

$$A(G) = A(G,1) \oplus A_0(G,1).$$

The **Cartan homomorphism**

$$c : A(G,1) \hookrightarrow A(G) \twoheadrightarrow A(G)/A_0(G,1)$$

is an isomorphism. In particular, the Cartan matrix is non-singular. Thus projective kG-modules with the same Brauer character are isomorphic.

PROOF. By Lemmas 5.3.1 and 5.2.2, the t_g are linearly independent on $A(G,1)$, and so c is injective. But the number of isomorphism types of projective indecomposables is equal to the number of isomorphism types of irreducibles, so the dimensions of $A(G,1)$ and $A(G)/A_0(G,1)$ are equal, so c is an isomorphism. Letting $e = c^{-1}(1)$, we see that e is an idempotent, $A(G,1) = e.A(G)$, and $A_0(G,1) = (1-e).A(G)$. □

5.4. G-sets and the Burnside ring

We now go through the same process with permutation representations as we went through in the last two sections with linear representations. The result is called the Burnside ring. There is a natural homomorphism from the Burnside ring to the representation ring of RG for any coefficient ring R, and we shall use this fact to obtain information about representation rings (namely various "induction theorems") in Section 5.6.

We define the **Burnside ring** $b(G)$ to be the ring with generators the isomorphism classes $[X]$ of permutation representations of G on finite sets, and relations

$$[X] + [Y] = [X \dot{\cup} Y], \quad [X].[Y] = [X \times Y]$$

giving the addition and multiplication in terms of disjoint union and Cartesian product. The identity element of this ring corresponds to the one point set with trivial action, and the zero element corresponds to the empty set.

Now any permutation representation X of G may be expressed uniquely as a disjoint union of orbits. The isomorphism classes of transitive permutation representations are in one-one correspondence with the conjugacy classes of subgroups in such a way that the permutation representation G/H corresponds to the conjugacy class of H, which is characterised as the stabiliser of a point. So the additive structure of $b(G)$ is easy to describe. It is the free abelian group, with basis corresponding to the transitive permutation representations $[G/H]$, one for each conjugacy class of subgroups $H \leq G$.

EXAMPLE. Suppose G is the symmetric group $\mathcal{S}_3$. Then we shall denote the transitive permutation representations of G by 1, a, b and c, on 1, 2, 3 and 6 objects respectively. The multiplication table of $b(G)$ is as follows:

$\times$	1	a	b	c
1	1	a	b	c
a	a	$2a$	c	$2c$
b	b	c	$b+c$	$3c$
c	c	$2c$	$3c$	$6c$

What are the ring homomorphisms $f : b(G) \to \mathbb{C}$? Clearly for any such ring homomorphism we have $f(1) = 1$. Since $f(c)^2 = 6f(c)$, either $f(c) = 0$ or $f(c) = 6$.

Case (i): $f(c) = 6$. In this case $f(a)f(c) = 2f(c)$ implies that $f(a) = 2$, while $f(b)f(c) = 3f(c)$ implies that $f(b) = 3$.

Case (ii) : $f(c) = 0$ implies that $f(a)f(b) = 0$. In this case we have $f(a)^2 = 2f(a)$ and $f(b)^2 = f(b)$, and so we have either $f(a) = 0$, $f(b) = 1$, or $f(a) = 2$, $f(b) = 0$, or $f(a) = 0$, $f(b) = 0$.

We may summarise this information in the following table:

c	6	0	0	0
b	3	1	0	0
a	2	0	2	0
1	1	1	1	1

We can interpret this table in terms of the numbers of fixed points on subgroups as follows. If $H \leq G$, the map

$$f_H : b(G) \to \mathbb{Z} \subseteq C$$

sending a permutation representation X to $|X^H|$ is a ring homomorphism, since

$$|(X \dot{\cup} Y)^H| = |X^H| + |Y^H|, \quad |(X \times Y)^H| = |X^H||Y^H|.$$

Clearly if H is not conjugate to K then $f_H \neq f_K$ (evaluate on G/H and G/K).

LEMMA 5.4.1. *We have $f_H(G/K) \neq 0$ if and only if H is conjugate to a subgroup of K.* □

Let $B(G) = \mathbb{C} \otimes_{\mathbb{Z}} b(G)$. Then f_H extends in an obvious way to a $\mathbb{C}$-linear ring homomorphism

$$f_H : B(G) \to \mathbb{C}$$

THEOREM 5.4.2. *Every ring homomorphism $b(G) \to \mathbb{C}$ is of the form f_H for some $H \leq G$. The sum of these maps is an isomorphism after tensoring with $\mathbb{C}$:*

$$\sum f_H : B(G) \to \bigoplus_{H \leq_G G} \mathbb{C}.$$

PROOF. By Lemma 5.2.2, the f_H are linearly independent, and so the above map $\sum f_H$ is surjective. Since $\dim_{\mathbb{C}} B(G)$ is equal to the number of conjugacy classes of subgroups, it follows that it is an isomorphism. □

We write ε_H for the primitive idempotent corresponding to H in the right hand side of the above isomorphism, and e_H for the corresponding element of $B(G)$.

It follows from the above theorem that

$$\sum f_H : b(G) \to \bigoplus_{H \leq_G G} \mathbb{Z}$$

is injective with finite cokernel. How big is this cokernel? Choosing bases by listing subgroups in non-decreasing order of size, the matrix of $\sum f_H$ is

$$\begin{pmatrix} * & & \bigcirc \\ & \ddots & \\ * & & * \end{pmatrix}.$$

The diagonal entries are $f_H(G/H) = |N_G(H) : H|$, and so the size of the cokernel, which is the determinant of this matrix, is equal to

$$\prod_{H \leq_G G} |N_G(H) : H|.$$

REMARK. Burnside calls the above matrix the **table of marks**. In section 185 of his book [**44**], you will find the following table of marks for the alternating group A_4.

	1	C_2	C_3	V_4	A_4
1	12	0	0	0	0
C_2	6	2	0	0	0
C_3	4	0	1	0	0
V_4	3	3	0	3	0
A_4	1	1	1	1	1

CONGRUENCES AND IDEMPOTENTS IN $b(G)$. The idempotents in $B(G)$ are the elements

$$\sum_{H \in \mathcal{H}} e_H$$

where $\mathcal{H}$ is a collection of representatives of distinct conjugacy classes of subgroups.

QUESTION 5.4.3. *When is* $\sum_{H\in\mathcal{H}} e_H$ *in* $b(G)$*?*

More generally, if S is a set of primes, we can look at the localised Burnside ring $b(G)_{(S)}$, obtained by allowing denominators coprime to S. Thus for example if $S = \{p\}$, we write $b(G)_{(p)}$ for the p-local Burnside ring, and if S is the set of all primes other than p, we write $b(G)_p$ for $\mathbb{Z}[1/p] \otimes_{\mathbb{Z}} b(G)$. All these rings may be thought of as subrings of $B(G)$.

QUESTION 5.4.4. *When is* $\sum_{H\in\mathcal{H}} e_H$ *in* $b(G)_{(S)}$*?*

LEMMA 5.4.5 (Burnside). *The number of orbits of* G *on* X *is equal to*

$$\frac{1}{|G|}\sum_{g\in G}|X^{\langle g\rangle}|$$

and in particular

$$\sum_{g\in G}|X^{\langle g\rangle}| \equiv 0 \pmod{|G|}.$$

PROOF. Count $\{(x,g) \mid xg = x\}$ in two ways. □

Hence, if $H \trianglelefteq K \leq G$, then the quotient group K/H acts on X^H, and we have

$$\sum_{\bar{k}\in K/H}|X^{\langle H,k\rangle}| \equiv 0 \pmod{|K/H|}.$$

Here, k denotes any pre-image of $\bar{k}$ in K, and the group $\langle H,k\rangle$ is clearly independent of this choice.

We can obtain a complete set of congruences (i.e., characterising the image of $b(G)$ under the map $\sum f_H$) by taking $K = N_G(H)$ for each conjugacy class of subgroups H of G.

These congruences are independent since they form a lower triangular matrix of congruences with ones on the diagonal. For example, in the case of the example above from Burnside's book, the congruences say that

$$\begin{pmatrix} 12 & 0 & 0 & 0 & 0 \\ 6 & 2 & 0 & 0 & 0 \\ 4 & 0 & 1 & 0 & 0 \\ 3 & 3 & 0 & 3 & 0 \\ 1 & 1 & 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 3 & 1 & 0 & 0 & 0 \\ 8 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 2 & 1 \end{pmatrix} \equiv 0 \pmod{\begin{pmatrix} 12 & 2 & 1 & 3 & 1 \end{pmatrix}}.$$

The second matrix in the above equation has its rows and columns labelled by the conjugacy classes of subgroups of G, and has a non-zero entry if and only if the subgroup H corresponding to the column is contained normally in a conjugate of the subgroup K corresponding to the row, with cyclic quotient. The entry is the number of times conjugates of K appear in the above congruence for $N_G(H)/H$; namely the sum, over the subgroups K in

the given G-conjugacy class that contain H normally with cyclic quotient, of the number of generators of the cyclic group K/H.

These congruences therefore define an additive subgroup of $\sum_{H\leq_G G}\mathbb{Z}$ of the same index as $b(G)$, which therefore *is* $b(G)$. We have therefore proved the following theorem of Dress [**86**] (our presentation follows tom Dieck [**72**]).

THEOREM 5.4.6. *The image of the map*

$$\sum f_H : b(G) \to \bigoplus_{H\leq_G G} \mathbb{Z}$$

is given by the congruences

$$\sum_k |\{\text{generators of } K/H\}|.f_H(x) \equiv 0 \pmod{|N_G(H):H|}$$

where the sum runs over the subgroups $K \leq G$ with $H \trianglelefteq K$ and K/H cyclic. □

Note that we can separate these congruences into p-primary components by using the pairs of groups $H \trianglelefteq N \leq G$ with $N/H \in \mathrm{Syl}_p(N_G(H)/H)$.

THEOREM 5.4.7 (Dress). (i) *An idempotent $\sum_{H\in\mathcal{H}} e_H \in B(G)$ lies in $b(G)$ if and only if, whenever $H \trianglelefteq H'$ with cyclic quotient, $H \in \mathcal{H} \Leftrightarrow H' \in \mathcal{H}$.*

(ii) *An idempotent $\sum_{H\in\mathcal{H}} e_H \in B(G)$ lies in $b(G)_{(S)}$ if and only if, whenever $H \trianglelefteq H'$ of index $p \in S$, H is conjugate to a subgroup in $\mathcal{H}$ if and only if H' is.*

PROOF. Suppose $\sum_{H\in\mathcal{H}} e_H \in b(G)_{(S)}$ and $H \trianglelefteq H'$ with cyclic quotient of order $p \in S$. Then the congruence $|X^H| \equiv |X^{H'}| \bmod |H':H|$ implies that for all $x \in b(G)_{(S)}$, $f_H(x) \equiv f_{H'}(x)$. Since $0 \not\equiv 1 \bmod p$, $H \in \mathcal{H} \Leftrightarrow H' \in \mathcal{H}$. Conversely, by the above theorem, if these congruences are satisfied then $\sum_{H\in\mathcal{H}} e_H \in b(G)_{(S)}$. □

COROLLARY 5.4.8 (Dress). (i) *The primitive idempotents in $b(G)$ are of the form*

$$\sum_{H^{(\infty)}=H_0} e_H$$

where H runs through representatives of conjugacy classes of subgroups of G for which $H^{(\infty)}$ is a given perfect subgroup H_0 of G.

In particular, G is soluble if and only if the only idempotents in $b(G)$ are 0 and 1.

(ii) *The primitive idempotents in $b(G)_{(p)}$ are of the form*

$$\sum_{O^p(H)=H_0} e_H$$

where H runs through representatives of conjugacy classes of subgroups of G for which $O^p(H)$ is a given p-perfect subgroup H_0 of G (i.e., subgroup with no normal subgroup of index p). □

ILLINOIS JOURNAL OF MATHEMATICS
Volume 25, Number 1, Spring 1981

IDEMPOTENT FORMULA FOR THE BURNSIDE ALGEBRA WITH APPLICATIONS TO THE p-SUBGROUP SIMPLICIAL COMPLEX

BY
DAVID GLUCK

1. Introduction

The Burnside ring $\Omega(G)$ of a finite group G is the Grothendieck ring of the category of finite G-sets. This ring has important algebraic and topological applications. A striking result of Dress [3] shows that there is a correspondence between the non-trivial primitive idempotents of $\Omega(G)$ and the conjugate classes of perfect subgroups of G. To shed some light on these idempotents one can pass to the Burnside *algebra* $\mathbf{Q} \otimes_{\mathbf{Z}} \Omega(G)$ which we denote $B[G]$. The primitive idempotents of $\Omega(G)$ are of course sums of primitive idempotents in $B[G]$, so a formula for the latter idempotents is of interest.

A recent paper of Quillen [6] examines the simplicial complex associated with the poset of non-trivial p-subgroups of a finite group. This study is motivated in part by a result of K. Brown that the Euler characteristic of this complex is congruent to one modulo the p-part of the group order.

In the final section of this paper we use our idempotent formula to give a very short, purely algebraic and combinatorial proof of the above result. In fact, the idempotent formula shows that the congruence property for the Euler characteristic is a consequence of the results of Dress [3] on the prime ideals of $\Omega(G)$.

2. Möbius functions of partially ordered sets

For the convenience of the reader we include a brief description of the Möbius function of a partially ordered set. See [7] for more information on this subject and for proofs of the following statements.

An interval $[a, b]$ in a partially ordered set S consists by definition of all c in A such that $a \leq c \leq b$. S is called locally finite if all intervals in S are finite. Any locally finite partially ordered set S has a Möbius function $\mu\colon S \times S \to \mathbf{Z}$ which is uniquely defined by the condition that

$$\sum_{c \in [a,b]} \mu(c, b) = \begin{cases} 1 & \text{if } a = b \\ 0 & \text{if } a \neq b. \end{cases}$$

When S is the set of natural numbers partially ordered by divisibility, $\mu(a, b) = \mu(b/a)$; the latter μ denotes the ordinary Möbius function of number theory.

Received February 7, 1979.

© 1981 by the Board of Trustees of the University of Illinois
Manufactured in the United States of America

Two properties of the Möbius function are important in this paper: the inversion formula and the alternating sum formula.

To state the first we let S be a locally finite partially ordered set and let f and g be functions from S to an abelian group such that $g(x) = \sum_{y \leq x} f(y)$. Then

$$f(x) = \sum_{y \leq x} \mu(y, x) g(y).$$

The alternating sum formula states that $\mu(a, b) = \sum_i (-1)^i c_i$ where c_i is the number of chains from a to b of length i. A chain of length i means one involving $i + 1$ elements of S.

Of course the inversion formula generalizes classical Möbius inversion while the alternating sum formula reminds one of Euler characteristics.

3. The idempotent formula

We refer the reader to Solomon [8] for the basic facts about $B[G]$. Our notation will be slightly different, however. We shall denote by $L(G)$ the lattice of subgroups of G and by $L^*(G)$ a set of representatives of conjugate classes of subgroups of G.

$B[G]$ is a commutative semisimple algebra over $\mathbf{Q}$, isomorphic to a direct sum of $|L^*(G)|$ copies of $\mathbf{Q}$. It has a natural basis element u_H for each $H \in L^*(G)$. Here u_H denotes the G-set of left cosets of H. The primitive idempotents e_H of $B[G]$ are also in one-to-one correspondence with the elements of $L^*(G)$. By [8, Theorem 4] each such idempotent can be written in the form

$$e_H = (|H|/|N_G(H)|)u_H + \sum_{K<H} \alpha_{KH} u_K$$

where the α_{KH} are rational numbers. We allow distinct subgroups K on the right to be conjugate in G, so a basis element u_K may appear more than once in the sum.

To get a more explicit formula for the e's in terms of the u's, we first express the u's in terms of the e's. We denote by $\langle \ , \ \rangle$ the natural bilinear form on $B[G]$ defined by the e's.

LEMMA 1. *For $H, K \in L^*(G)$ we have $\langle e_K, u_H \rangle = c_{KH}|N_G(K)|/|H|$ where c_{KH} is the number of conjugates of K contained in H. Consequently*

$$u_H = \sum_{K \leq H} (|N_G(K)|/|H|)e_K$$

the sum being taken over all subgroups K of H.

Proof. For $J, L \in L^*(G)$ define $\phi_J(u_L)$ to be the number of left cosets of L which are fixed by every element of J. By remarks preceeding Lemma 1 of [3], ϕ_J extends to an algebra homomorphism from $B[G]$ onto $\mathbf{Q}$, and all such homomorphisms arise in this way. Thus $\phi_J(\cdot) = \langle e_{J'}, \cdot \rangle$ for some $J' \in L^*(G)$.

To show that $J' = J$ we evaluate at $u_{J'}$ and get $\phi_J(u_{J'}) \neq 0$. It follows from the

definition of ϕ_J that J is conjugate to a subgroup of J'. In particular $|J| \leq |J'|$. Thus $G' = G$ and by downward induction on $|J|$ we have $J = J'$ for all $J \in L^*(G)$.

Thus $\langle e_K, u_H \rangle = \phi_K(u_H)$ is the number of left cosets gH such that $KgH = gH$, or equivalently $g^{-1}Kg \leq H$. Let $S = \{g \in G \mid g^{-1}Kg \leq H\}$. The number of fixed left cosets we want to find is $|S|/|H|$. But S is the union of c_{KH} right cosets of $N_G(K)$. The statement of the lemma follows.

Remark. Each e_H is an integral linear combination of the distinct u_K's but the numbers $|N_G(K)|/|H|$ need not be integers.

The idempotent formula follows.

We denote by μ the Möbius function of $L(G)$.

PROPOSITION. *For $H \in L^*(G)$, $e_H = (|N_G(H)|)^{-1} \sum_{K \leq H} \mu(K, H)|K|u_K$, the sum being taken over all subgroups of H.*

Proof. For $H \in L(G)$ let $f_H = |N_G(H)|e_H$ and let $v_H = |H|u_H$. By Lemma 1, $v_H = \sum_{K \leq H} f_K$, the sum being taken over all subgroups of H. We think of v and f as functions from $L(G)$ to the abelian group $B[G]$. By Möbius inversion $f_H = \sum_{K \leq H} \mu(K, H)v_K$ which translates into the statement of the proposition.

We remark that the above formula generalizes the "Brauer Coefficient Formula"; see [1, Satz 1]. A special case of our formula appears in [8] and a closely related formula appears in a different context in [5].

4. The p-subgroup simplicial complex

Let $S_p(G)$ denote the simplicial complex considered in [6]. The vertices of $S_p(G)$ are the non-trivial p-subgroups of G and the n-simplices are the chains of p-subgroups of G of length n.

Two subgroups H and K of G are said to be p-equivalent if $O^p(H)$ is G-conjugate to $O^p(K)$, where $O^p(H)$ denotes the smallest normal subgroup of H having p-power index. For $H \in L^*(G)$ let $\tilde{e}_H$ denote the sum $\sum e_K$ in $B[G]$ where K ranges over all subgroups in $L^*(G)$ which are p-equivalent to H. Let $\mathbf{Z}_p$ be the integers localized at p and let $\Omega(G)_p$ be $\mathbf{Z}_p \otimes_{\mathbf{Z}} \Omega(G)$. Finally let $P(G)$ be the set of p-subgroups of G and let $P^*(G) = P(G) \cap L^*(G)$.

LEMMA 2. *The distinct $\tilde{e}_H$ are the primitive idempotents of $\Omega(G)_p$.*

Proof. This is implicit in [3], and a fuller description may be found in [4, p. 54]. We shall sketch the proof for the reader's convenience.

The prime ideals of $\Omega(G)_p$ are of two types. There are minimal prime ideals $\mathfrak{p}(H, 0)$ defined by $\{x \in \Omega(G)_p \mid \langle e_H, x \rangle = 0\}$ and there are maximal ideals $\mathfrak{p}(H, p)$ defined by $\{x \in \Omega(G)_p \mid \langle e_H, x \rangle \equiv 0 \bmod p\}$. The $\mathfrak{p}(H, 0)$ are distinct for distinct $H \in L^*(G)$ but $\mathfrak{p}(H, p) = \mathfrak{p}(K, p)$ if and only if H and K are p-

equivalent. Each p-equivalence class thereby determines a connected component of Spec $\Omega(G)_p$ consisting of one maximal ideal $\mathfrak{p}(H, p)$ and the minimal prime ideals $\mathfrak{p}(K, 0)$ for those K in $L^*(G)$ which are p-equivalent to H. All the above $\mathfrak{p}(K, 0)$ are contained in $\mathfrak{p}(H, p)$.

On the other hand, for any commutative ring R the connected components of Spec R correspond to the primitive idempotents of R; the connected component of Spec R corresponding to a primitive idempotent e in R consists of all prime ideals of R which contain $1 - e$. So if e is the primitive idempotent of $\Omega(G)_p$ corresponding to the connected component of Spec $\Omega(G)_p$ described in the previous paragraph, $1 - e$ is contained in $\mathfrak{p}(K, 0)$ if and only if K is p-equivalent to H. The statement of the lemma follows.

We can now prove the result mentioned in the introduction.

THEOREM (K. Brown). *The Euler characteristic of $S_p(G)$ is congruent to one modulo $|G|_p$.*

Proof. First observe that the Euler characteristic equals $\sum_{i=0}(-1)^i c_i$ where c_i is the number of chains of non-trivial p-subgroups of G of length i. There is an obvious correspondence between all chains in $S_p(G)$ and all non-trivial chains in $P(G)$ whose smallest element is 1. A chain in $S_p(G)$ of length i corresponds to a chain in $P(G)$ of length $i + 1$.

Let d_i denote the number of chains with smallest element 1 and length i in $P(G) \subset L(G)$. By the alternating sum formula for the Möbius function, $\sum_{i=0}(-1)^i d_i = \sum_{P \in P(G)} \mu(1, P)$. Since $\sum_{i=0}(-1)^i c_i$ omits the chain from 1 to 1 in $L(G)$, which corresponds to $\mu(1, 1)$ in $\sum \mu(1, P)$, the Euler characteristic of $S_p(G)$ equals $1 - \sum_{P \in P(G)} \mu(1, P)$. Thus it suffices to show that

$$\sum_{P \in P(G)} \mu(1, P) \equiv 0 \mod |G|_p.$$

The idempotent formula gives, after one "uncollects" conjugate subgroups,

$$|G|^{-1} \sum_{P \in P(G)} \mu(1, P)$$

as the coefficient of u_1 in $\sum_{P \in P^*(G)} e_P$. Since $P^*(G)$ is the set of subgroups in $L^*(G)$ which are p-equivalent to 1, the idempotent $\sum_{P \in P^*(G)} e_P$ lies in $\Omega(G)_p$ by Lemma 2, so its coefficients are p-integral, which completes the proof.

REFERENCES

1. R. BRAUER, *Beziehungen zwischen Klassenzahlen von Teilkörpern eines galoisschen Körpers*, Math. Nachr., vol. 4 (1951), pp. 158–174.
2. K. BROWN, *Euler characteristics of groups: The p-fractional part*, Invent. Math., vol. 29 (1975), pp. 1–5.
3. A. DRESS, *A characterization of solvable groups*, Math, Zeitschr., vol. 110 (1969), pp. 213–217.
4. A. DRESS and M. KÜCHLER, *Zur Darstellungstheorie Endlicher Gruppen I* (preliminary edition), Bielefeld, 1970.

5. R. GILMAN, *A combinatorial identity with applications to representation theory*, Illinois J. Math., vol. 17 (1973), pp. 347–351.
6. D. QUILLEN, *Homotopy properties of the poset of nontrivial p-subgroups of a group*, Advances in Math., vol. 28 (1978), pp. 101–128.
7. G.-C. ROTA, *On the foundations of combinatorial theory*, Z. Wahrscheinlichkeitstheorie und Verw. Gebielte, vol. 2 (1964), pp. 340–368.
8. L. SOLOMON, *The Burnside algebra of a finite group*, J. Combinatorial Theory, vol. 2 (1967), pp. 603-615.

UNIVERSITY OF ILLINOIS
URBANA, ILLINOIS