Counting The Subgroups Of An Infinite Group

Michael Grady
Department of Mathematics and Computer Science
Georgia State University
Atlanta, GA 30303–3083 U.S.A.

Abstract. Dey's formula can be used to count the subgroups of finitely generated groups and to establish congruence properties of subgroup counting functions. We develop an algebraic technique based on this formula for counting the subgroups of given index in Hecke groups, and show how to streamline it for efficient computation modulo 2.

Introduction

Dey's formula (1) exhibits the fundamental enumerative relation between the subgroups and permutation representations of a finitely generated group and is a fascinating example of the ubiquitous "exponential formula" for labeled counting. This relation was discovered by Marshall Hall in connection with free groups [6], and later generalized to the case of free products by Ian Dey [2]. Kurt Wohlfahrt has given an insightful proof of its validity for all finitely generated groups in [13]. This reference is highly recommended, especially in conjunction with Wilf's lucid and relevant discussion of labeled counting [12, pp. 64–97].

A number of powerful and general theorems describe the behavior of subgroup counting functions for finite groups, those of Lagrange and Sylow being the most prominent. Are there analogous results for infinite groups? While no results of such consequence have yet surfaced, several interesting arithmetic patterns have been found. For instance, the number of subgroups of index n in the classical modular group is odd if and only if n is of the form $2^k - 3$ or $2(2^k - 3)$, [11]. To cite another example, the subgroup counting function for any free product containing the factor $C_p * C_p$ in its free product decomposition will be periodic modulo p, [5]. Further examples may be found in references [3],[4],[7] and [8].

In this paper we extend an algebraic technique, first suggested by Newman and the present author in [4], for counting the subgroups of given index in Hecke groups, and show how to streamline it for efficient computation modulo 2. Various parity patterns will be noted and two open problems stated.

Dey's Formula

For any finitely generated group G, let M denote the subgroup counting function and M_n the number of subgroups in G having index n. Let R denote the representation counting function and R_n the number of permutation representations of G on n symbols. Equivalently, this is the number of homomorphisms of G into the symmetric group S_n. Dey's formula reveals a remarkable connection between these two counting functions: $M_1 = 1$ and for indices greater than 1 we have

$$M_n = \frac{R_n}{(n-1)!} - \sum_{i=1}^{n-1} \frac{R_{n-i}M_i}{(n-i)!}. \tag{1}$$

In what follows, it will be advantageous to write (1) in terms of generating functions. Let $g(x)$ denote the ordinary generating function for the number of subgroups in G having index n:

$$g(x) = \sum_{n\geq 1} M_n x^n,$$

and let $f(x)$ denote the exponential generating function for the number of permutation representations of G on n symbols:

$$f(x) = \sum_{n\geq 0} \frac{R_n}{n!} x^n, \text{ with } R_0 = 1.$$

Then

$$g = \frac{xf'}{f}. \tag{2}$$

To illustrate the utility of (2) for obtaining congruence information, we now show that the number of subgroups of any given finite index in a free group is always odd. The number of permutation representations of C_∞, the infinite cyclic group, on n symbols is $n!$ since the generator may be mapped to any element of S_n. So a free group of rank t has $R_n = n!^t$, and

$$f(x) = \sum_{n\geq 0} n!^{t-1}x^n = \frac{1}{1-x} \text{ for } t = 1,$$

$$f(x) = \sum_{n\geq 0} n!^{t-1}x^2 \equiv 1 + x \pmod 2 \text{ for } t \geq 2.$$

giving

$$g(x) \equiv \frac{x}{1+x} \pmod 2,$$

by equation (2). Thus, all M_n are odd. Here, we are using the convention that whenever a function appears in a congruential expression, the congruence is meant to apply to the coefficients in the power series expansion of that function. This usage clearly requires that all such coefficients be integral.

Counting Subgroups of Hecke Groups Modulo 2

Hecke groups are free products of the form $C_2 * C_p$, where C_2 is the cyclic group of order 2 and C_p a cyclic group of prime order p. These groups, denoted H_p, are important in the field of analytic number theory [10, pp. 138–163]. The number of permutation representations of H_p on n symbols is simply $\tau_2(n)\tau_p(n)$, where $\tau_2(n)$ is the number of representations of C_2 and $\tau_p(n)$ the number of representations of C_p on n symbols. Since these numbers are easy to compute recursively, counting subgroups via Dey's formula (1) is a straightforward multiprecision computation [4, p. 432]. This method works reasonably well when n is small, but would be hopelessly inadequate for computing the parity of the first million values of the subgroup counting function for a group like H_{65537} (where $M_{1000000}$, for example, has approximately three million digits). We now describe an approach that will handle such a computation quite easily.

The numbers $\tau_2(n)$ and $\tau_p(n)$ are given by the exponential generating functions $e^{x+\frac{x^2}{2}}$ and $e^{x+\frac{x^p}{p}}$ respectively. (This can be shown as Wilf does in [12, p. 76], or alternatively, by solving (2) for f and noting that a cyclic group of prime order p has one subgroup of index 1 and one of index p). Thus,

$$\frac{\tau_p(n)}{n!} = \frac{1}{n!} + \frac{1}{p(n-p)!} + \frac{1}{2p^2(n-2p)!} + \ldots,$$

where the sum is finite and the general term is

$$\frac{1}{q!p^q(n-pq)!}, \; 0 \leq q \leq \lfloor \frac{n}{p} \rfloor.$$

Multiplying by $\tau_2(n)$ and summing over n gives

$$f = \sum_{n\geq 0} \frac{\tau_2(n)}{n!} + \frac{1}{p} \sum_{n\geq p} \frac{\tau_2(n)}{(n-p)!} x^n + \ldots,$$

where the general term is

$$\frac{1}{q!p^q} \sum_{n\geq pq} \frac{\tau_2(n)}{(n-pq)!} x^n.$$

Letting w denote the function $e^{x+\frac{x^2}{2}}$, and D the derivative operator, we have

$$f(x) = w + \frac{x^p}{p} D^p w + \frac{x^{2p}}{2p^2} D^{2p} w + \frac{x^{3p}}{3!p^3} D^{3p} w + \dots \tag{3}$$

If Q denotes the operator $e^{\frac{x^p}{p} D^p}$ then (3) has the interesting formulation: $f(x) = Q(w)$. Factoring out w yields

$$f(x) = w(1 + \frac{x^p}{p} C_p + \frac{x^{2p}}{2p^2} C_{2p} + \frac{x^{3p}}{3!p^3} C_{3p} + \dots) = wq(x), \tag{4}$$

where $C_n = \frac{1}{w} D^n w$ is a monic polynomial of degree n with positive integer coefficients, which shall be called the nth tau-2 polynomial.

We now give a formula for these polynomials.

Theorem 1. *The nth tau-2 polynomial is given by the formula*

$$C_n = \sum_{k=0}^{n} \binom{n}{k} \tau_2(k) x^{n-k}. \tag{5}$$

Proof:

$$C_{n+1} = \frac{1}{w} D^{n+1} w = \frac{1}{w} D(D^n w) = \frac{1}{w} D(wC_n) = \frac{1}{w}[(1+x)wC_n + wC_n'],$$

where the prime denotes the first derivative. This yields the recurrence

$$C_{n+1} = (1+x)C_n + C_n',$$

with initial values $C_0 = 1$, $C_1 = 1 + x$. Let

$$P(x,t) = \sum_{n \geq 0} \frac{C_n(x)}{n!} t^n$$

be the exponential generating function for the τ-2 polynomials. Then equation (5) implies

$$\sum_{n \geq 0} \frac{C_{n+1}(x)}{n!} t^n = (1+x) \sum_{n \geq 0} \frac{C_n(x)}{n!} t^n + \sum_{n \geq 0} \frac{C_n'(x)}{n!} t^n$$

which immediately yields the following differential equation:

$$\frac{dP}{dt} = (1+x)P + \frac{dP}{dx}.$$

Since the function $P(x,t) = e^{t+\frac{t^2}{2}} e^{xt}$ satisfies this equation and the initial conditions, it must be the required generating function. But the coefficient of $\frac{t^n}{n!}$ in the product of $e^{t+\frac{t^2}{2}}$ and e^{xt} is

$$C_n = \sum_{k=0}^{n} \binom{n}{k} \tau_2(k) x^{n-k}.$$

This completes the proof.

The τ-2 polynomials simplify enormously mod 2^s. That makes them very useful for parity computations. We state this explicitly in the next theorem.

Theorem 2. *Let s be a positive integer. Then $C_n \equiv \sum_{k=0}^{4s-3} \binom{n}{k} \tau_2(k) x^{n-k}$ mod 2^s.*

Proof: $\tau_2(n) \equiv 0 \; mod \, 2^s$ if $n > 4s-3$ [1, p. 334], so the result is immediate.

By equation (4) we have

$$\frac{xf'}{f} = x + x^2 + \frac{xq'(x)}{q(x)},$$

so we may restrict our attention to the series $q(x)$. A typical computation would proceed as follows. To find the parity of M_n for $n \leq kp$, use an appropriately truncated version of $q(x)$, take its reciprocal, (which will also be a series in the τ-2 polynomials), clear denominators and do computations mod 2^s, where 2^s is a higher power of 2 than appears in the denominators.

For example, the series giving the subgroup counting function exactly for the first $4p-1$ terms is

$$\begin{aligned} &x + x^2 + x^p B_p + \frac{x^{2p}}{p} B_{2p} - \frac{x^{2p}}{p} B_p C_p \\ &+ \frac{x^{3p}}{2p^2} B_{3p} - \frac{x^{3p}}{p^2} B_{2p} C_p + \frac{x^{3p}}{p^2} B_p C_p^2 - \frac{x^{3p}}{2p^2} B_p C_{2p}, \end{aligned} \tag{6}$$

where $B_{kp} = C_{kp} - xC_{kp-1}$. Since 2 is the highest power of 2 appearing in the denominator, the τ-2 polynomials may be computed mod 4. Multiplying by $2p^2$ clears the denominators, and the resulting polynomial is then reduced modulo 4. This computation will yield correct parity values for $n < 8p - 5$, due to the simplification mod 4. Table 1 gives the parity of the subgroup counting function for several Hecke groups. A number of patterns are evident and two of these are stated in the final section. We mention here the following result.

Theorem 3. *The first four odd values of the subgroup counting function for H_p will occur at indices 1, 2, $2p-1$ and $4p-2$.*

Proof: It follows from Theorem 1 that $C_n \equiv x^n + x^{n-1}$ (mod 2) for odd n and $C_n \equiv x^n$ for even n, giving

$$B_n \equiv x^{n-1} \; mod\; 2.$$

Truncating equation (6) to permit mod 2 computation gives

$$\begin{aligned} &x + x^2 + x^p B_p + \frac{x^{2p}}{p} B_{2p} + x^{2p} B_p C_p \\ &\equiv x + x^2 + x^p x^{p-1} + x^{2p} x^{2p-1} + x^{2p}(x^p + x^{p-1}) \\ &\equiv x + x^2 + x^{2p-1} + x^{4p-2}, \text{ (mod 2)}, \end{aligned}$$

proving the theorem.

Open Problems

1. **Parity patterns.** The author has computed the parity of the subgroup counting function for Hecke groups H_p, $p < 100$, for all indices less than $16p$. For primes less than or equal to 17 the data was extended to include indices less than 1000. These computations support the following conjectures.

   Conjecture 1: If n is odd, then M_n and M_{2n} have the same parity.

   Conjecture 2: M_{4k} is even for all positive k.

2. **A remarkable property of the function Q(w).** Let Q^{-1} denote the operator $e^{\frac{-x^p}{p}D^p}$. $Q^{-1}(w^{-1})$ is not the reciprocal of $Q(w)$, an assertion which is easily confirmed by computing each series to a few terms. However, for parity computations it behaves as if it were this reciprocal. Computations for the groups listed in problem 1, and in the same ranges, support the following conjecture.

   Conjecture 3.: The series $x[Q(w)]'[Q^{-1}(w^{-1})]$ has integral coefficients and is congruent to $\frac{xf'}{f}$ *mod* 2.

   Since both $Q(w)$ and $Q^{-1}(w^{-1})$ are efficiently computed, this would bypass the need to find the reciprocal of f in the usual way.

Table 1. The subgroup counting function for H_p is odd at these indices only, for $n < 16p$.

Small primes:

H_3:	1	2	5	10	13	26	29
H_7 :	1	2	13	26	37	61	74
H_{11} :	1	2	21	42	61	122	141
H_{13} :	1	2	25	50	121		

Fermat primes:

H_5:	1	2	9	18	41
H_{17}:	1	2	33	66	
H_{257}:	1	2	513	1026	
H_{65537}:	1	2	131073	262146	

Mersenne primes:

H_{127}	1	2	253	506	757	1261	1514
H_{8191}	1	2	16381	32762	49141	81901	98282

References

[1] S. Chowla, I. Herstein, K. Moore, On recursions connected with symmetric groups, *Canad. J. Math*, **3** (1951), 328–334.

[2] I.M.S. Dey, Schrier systems in free products, *Proc. Glasgow Math. Assoc.*, **7** (1965), 61–79.

[3] M. Grady and M. Newman, Some divisibility properties of the subgroup counting function for free products, *Math. Comp.* **58** (1992), 347–353.

[4] M. Grady and M. Newman, Counting subgroups of given index in Hecke groups, *Contemp. Math, Amer. Math. Soc.*, **Vol. 143**, (1993), 431–436.

[5] M. Grady and M. Newman, Residue periodicity in subgroup counting functions, *Proc. of the Rademacher Conference on Number Theory*, (to appear).

[6] M. Hall, Subgroups of finite index in free groups, *Canad. J. Math.* **1** (1949), 187–190.

[7] C. Godsil, W. Imrich, and R. Razen, On the number of subgroups of given index in the modular group, *Monatsh. Math.* **87** (1979), 273–280.

[8] W. Imrich, On the number of subgroups of a given index in $SL_2(Z)$, *Arch. Math*, **31** (1978), 224–231.

[9] M. Newman, Asymptotic formulas related to free products of cyclic groups, *Math. Comp.*, **30** (1976), 839–846.

[10] M. Newman, *Integral matrices*, Academic Press, New York(1972).

[11] W.W. Stothers, The number of subgroups of given index in the modular group, *Proc. Roy Soc. Edinburgh Sect. A*, **78** (1977), 105–112.

[12] H. Wilf, *generatingfunctionology*, Academic Press, San Diego (1990).

[13] K. Wohlfahrt, Uber einen Satz von Dey und die Modulgruppe, *Arch. Math*, **29** (1977), 455–457.