THE PROBABILITY OF GENERATING SOME COMMON FAMILIES OF FINITE GROUPS

Vincenzo Acciaro

TR-227, SEPTEMBER 1993

School of Computer Science, Carleton University
Ottawa, Canada, KIS 5B6

The probability of generating some common families of finite groups

Vincenzo Acciaro *
(acciaro@scs.carleton.ca)
School of Computer Science, Carleton University
Ottawa, Canada, K1S 5B6
and
Dipartimento di Informatica, Bari, Italy

Abstract

Let G be a finite group. Define $e(G)$ to be the expected number of elements of G which have to be drawn at random with replacement from G before a set of generators is found. Define $\lambda_n(G)$ to be the probability that n elements drawn at random with replacement from G generate G. In this paper we discuss some general approaches to computing $e(G)$ and $\lambda_n(G)$. We apply these approaches to some common classes of finite groups, including the p-groups and the nilpotent groups.

1 Introduction

In [1] we describe a new algorithm for testing whether a group G generated by a given set of m permutations of degree n is regular – a transitive permutation group is said to be *regular* if its order and degree are equal: this condition is equivalent, for a transitive permutation group, to the fact that the stabiliser of each point is the identity (see [2] for a survey of algorithms to handle permutation groups). The expected execution time of this algorithm is $O(mn(\alpha(n) + e(G)))$, where $\alpha()$ represents the inverse of Ackerman's function and $e(G)$ the expected number of elements of G which have to be drawn at random, with replacement, before a set of generators is found.

In this paper we compute the function $e(G)$ for some common classes of groups, starting from the p-groups, i.e. those group whose order is the power of a prime p, and we prove that for these groups the quantity $e(G)$ is related

*Research supported in part by Natural Sciences and Engineering Research Council of Canada under Operating Grant A2415

exclusively to p and to the minimal number of elements needed to generate them.

Groups which are the direct product of groups of coprime order are also analysed and it is shown how to compute the function $e(G)$ for them.

With these two results at our disposition we can thoroughly analyse the class of nilpotent groups, i.e. those groups which are the direct product of their Sylow subgroups, which includes among others the class of abelian groups.

Some general approaches for computing the function $e(G)$ are given through the paper and, to show their validity, we employ them to compute $e(G)$ for all the groups of order less than sixteen.

2 Definitions

We start with some definitions, taken from [4]:

DEFINITION 1 *An n-basis of a group G is defined as an ordered set $(x_1, \ldots, x_n)$ of n elements, not necessarely distinct, of G which generates G: $\langle x_1, \ldots, x_n \rangle = G$.*

DEFINITION 2 *The number of distinct n-basis of G is denoted by $\phi_n(G)$ and is called the n^{th} Eulerian function of G.*

Two important cases must be noticed:

- If G cannot be generated by n elements then $\phi_n(G) = 0$.
- If G is cyclic of order m then $\phi_1(G) = \phi(m)$, where ϕ is the ordinary Eulerian function of an integer.

Obviously an n-tuple $(g_1, \ldots, g_n)$ of elements of G either generates G, that is $(g_1, \ldots, g_n)$ constitutes an n-basis of G, or it generates a proper subgroup H of G, in which case it constitutes an n-basis of H. The total number of n-tuples $(g_1, \ldots, g_n)$ of elements of G is $|G|^n$. We therefore have the *fundamental identity*:

$$|G|^n = \sum_{H \leq G} \phi_n(H) \tag{1}$$

DEFINITION 3 *Let $\lambda_n(G)$ denote the probability that n elements drawn at random, with replacement, from G generate G.*

It is easy to see that

$$\lambda_n(G) = \frac{\phi_n(G)}{|G|^n} \tag{2}$$

DEFINITION 4 *Let $e(G)$ denote the expected number of elements of G which have to be drawn at random, with replacement, before a set of generators is found.*

The probability that a sequence $g_1, \ldots, g_{d-1}, g_d$ of elements of G generates G and $g_1, \ldots, g_{d-1}$ does not is $\lambda_d(G) - \lambda_{d-1}(G)$. Therefore

$$e(G) = \sum_{d=1}^{\infty} d(\lambda_d(G) - \lambda_{d-1}(G)) \tag{3}$$

For the group of order one which is the base of our inductive construction it is easily seen that for any $n \in N$ we have $\phi_n(\{1\}) = 1$, $\lambda_n(\{1\}) = 1$ and therefore $e(\{1\}) = 0$.

3 Computation of the Eulerian function for some common families of groups.

In this section and in those to follow we will show how to compute the functions ϕ_n and e, introduced in Section 2, for some common classes of groups.

The Eulerian n^{th} function of a group G is computed recursively, by using the *fundamental identity* 1 which was introduced in Section 2.

The *basic combinatorial identity* that we will use to simplify the computation of $e(G)$, as given by Formula 3, is the following:

$$\sum_{d=1}^{\infty} \frac{d}{x^{d-1}} = \left(\frac{x}{x-1}\right)^2 \tag{4}$$

where x is a real number strictly greater than one.

Before specializing our discussion to particular classes of finite groups, we state a lemma which is valid for arbitrary groups.

LEMMA 1 *Let G be an arbitrary group and $\Phi(G)$ its Frattini subgroup. Then r elements $x_1, \ldots, x_r$ of G generate G if and only if their images in $G/\Phi(G)$ generate $G/\Phi(G)$.*

PROOF See [3, problem 8.7]. □

In other words, given an arbitrary group G, we have $\lambda_n(G) = \lambda_n(G/\Phi(G))$, and therefore $\phi_n(G) = \lambda_n(G/\Phi(G)) \cdot |G|^n$.

3.1 P-groups

In this section we will address the problem of computing the probability of generating an arbitrary p-group. The next lemma shows how to reduce this problem to that of computing the probability of generating an elementary abelian p-group.

LEMMA 2 *If G is a p-group with minimal number of generators d then $G/\Phi(G)$ is an elementary abelian group of order p^d.*

PROOF See [3, problem 8.26]. □

We can now use the information contained in the two lemmas above to compute the probability of generating an arbitrary p-group with minimal number of generators d. To start, we recall the fact that an elementary abelian group of order p^d can be considered as a vector space of dimension d over $GF(p)$. In the light of this equivalence we introduce a new quantity:

DEFINITION 5 *Define $\mu_{r,s}$ as the probability that a sequence of r elements $x_1, \ldots, x_r$ drawn with replacement from a vector space of dimension d generates a subspace of dimension s.*

LEMMA 3

$$\mu_{r,s} = \begin{cases} p^{-rd} & \text{if } s = 0 \\ 0 & \text{if } r < s \\ \mu_{r-1,s}\frac{p^s}{p^d} + \mu_{r-1,s-1}(1 - \frac{p^{s-1}}{p^d}) & \text{otherwise} \end{cases}$$

PROOF

1. r elements chosen at random span a subspace of dimension zero in a space of dimension d over $GF(p)$ if and only if they are all equal to the null vector. But the probability that this event occurs is equal to $(\frac{1}{p^d})^r$.

2. it is obvious that r elements cannot generate a space of dimension s if $r < s$.

3. $$\begin{aligned} \mu_{r,s} &= \Pr(\dim\langle x_1, \ldots, x_r\rangle = s \ \wedge\ \dim\langle x_1, \ldots, x_{r-1}\rangle = s) \\ &\quad + \Pr(\dim\langle x_1, \ldots, x_r\rangle = s \ \wedge\ \dim\langle x_1, \ldots, x_{r-1}\rangle = s-1) \\ &= \Pr(\dim\langle x_1, \ldots, x_{r-1}\rangle = s \ \wedge\ x_r \in \langle x_1, \ldots, x_{r-1}\rangle) \\ &\quad + \Pr(\dim\langle x_1, \ldots, x_{r-1}\rangle = s-1 \ \wedge\ x_r \notin \langle x_1, \ldots, x_{r-1}\rangle) \\ &= \mu_{r-1,s}\frac{p^s}{p^d} + \mu_{r-1,s-1}\left(1 - \frac{p^{s-1}}{p^d}\right) \quad \square \end{aligned}$$

COROLLARY 1 $\mu_{s,s} = \prod_{i=d-s+1}^{d}(1 - p^{-i})$

PROOF
$$\begin{aligned} \mu_{s,s} &= \mu_{s-1,s-1}\left(1 - \frac{p^{s-1}}{p^d}\right) + \mu_{s-1,s}\frac{p^s}{p^d} \\ &= \mu_{s-1,s-1}\left(1 - \frac{p^{s-1}}{p^d}\right) \\ &= \mu_{s-1,s-1}\left(1 - p^{s-1-d}\right) \\ &= \mu_{s-2,s-2}\left(1 - p^{s-2-d}\right)\left(1 - p^{s-1-d}\right) \\ &= \left(1 - p^{-d}\right)\ldots\left(1 - p^{s-2-d}\right)\left(1 - p^{s-1-d}\right) \quad \square \end{aligned}$$

COROLLARY 2 $\mu_{s+k,s} = \frac{\mu_{s,s}}{p^{dk}} \prod_{i=1}^{k} \frac{p^{s+i}-1}{p^i-1}$

PROOF By induction on k. For $k = 0$ the result follows from the last corollary. For $k > 0$ we can write:

$$\begin{aligned}
\mu_{s+k+1,s} &= \mu_{s+k,s}\frac{p^s}{p^d} + \mu_{s+k,s-1}\left(1 - \frac{p^{s-1}}{p^d}\right) \\
&= \frac{p^s}{p^d}\frac{\mu_{s,s}}{p^{dk}}\prod_{i=1}^{k}\frac{p^{s+i}-1}{p^i-1} + \left(1-p^{s-1-d}\right)\frac{\mu_{s-1,s-1}}{p^{d(k+1)}}\prod_{i=1}^{k+1}\frac{p^{s-1+i}-1}{p^i-1} \\
&= \frac{p^s\mu_{s,s}}{p^{d(k+1)}}\prod_{i=1}^{k}\frac{p^{s+i}-1}{p^i-1} + \frac{\mu_{s,s}}{p^{d(k+1)}}\prod_{i=1}^{k+1}\frac{p^{s-1+i}-1}{p^i-1} \\
&= \frac{\mu_{s,s}}{p^{d(k+1)}}\prod_{i=1}^{k}\frac{p^{s+i}-1}{p^i-1}\left(p^s + \frac{p^s-1}{p^{k+1}-1}\right) \\
&= \frac{\mu_{s,s}}{p^{d(k+1)}}\prod_{i=1}^{k+1}\frac{p^{s+i}-1}{p^i-1} \quad \square
\end{aligned}$$

The lemma that follows is the most important of this section. In fact, it allows us to effectively compute the probability that some elements chosen independently and at random generate a p-group with minimal number of generators d.

LEMMA 4 *If G is a p-group with minimal number of generators d, then*

- $\lambda_d(G) = \prod_{i=1}^{d}\left(1-p^{-i}\right)$
- *if* $k \geq 0$ *then* $\lambda_{d+k}(G) = \lambda_d(G)\prod_{i=1}^{k}\frac{p^i-p^{-d}}{p^i-1}$

PROOF The first part follows from the fact that $\lambda_d(G) = \mu_{d,d}$ and the second part from the fact that $\lambda_{d+k}(G) = \mu_{d+k,d}$. □

The formulae given above are quite complicated: the next theorem gives a handy estimate for $\lambda_d(G)$, and also shows that $\lim_{p\to\infty}\lambda_d(G) = 1$

THEOREM 1 *If G is a p-group with minimal number of generators d, then*

$$\frac{p-1}{p} \geq \lambda_d(G) \geq 1 - p^{-1} - p^{-2}$$

PROOF The upper bound follows from the expression for $\lambda_d(G)$ given in Lemma 4. To prove the lower bound, we see that :

$$\lambda_d(G) = \prod_{i=1}^{d}\left(1-p^{-i}\right) \geq \prod_{n=1}^{\infty}\left(1-p^{-n}\right)$$

By Euler's formula :

$$\prod_{n=1}^{\infty}\left(1-z^n\right) = 1 - z - z^{-2} + z^5 + z^7 - z^{12} - z^{15} + \ldots = \sum_{-\infty<j<\infty}(-1)^j z^{\frac{3j^2+j}{2}}$$

if we put $z = p^{-1}$ we obtain :

$$\prod_{n=1}^{\infty}\left(1-p^{-n}\right) = 1 - p^{-1} - p^{-2} + p^{-5} + p^{-7} - p^{-12} - p^{-15} + \ldots$$

this can be considered as an alternating series, if we collect each even term with the consecutive one; if we take the first three terms by Liebniz's theorem the error will be negative and less than $p^{-5} + p^{-7}$ in absolute value. □

NOTE 1 The lower bound for $\lambda_d(G)$ given in Theorem 1 is also valid for $\lambda_{d+k}(G)$, since $\lambda_d(G) = \mu_{d,d} \leq \mu_{d+k,d} = \lambda_{d+k}(G)$

EXAMPLE 1 To see the numerical effectiveness of this approximation, consider a four generator p-group with $p = 7$: by Lemma 4 we have $\lambda_4(G) = \frac{236390400}{282475249} \approx 0.8368$, while Theorem 1 gives $0.8367 \approx \frac{41}{49} \leq \lambda_4(G) \leq \frac{6}{7} \approx 0.8571$.

3.2 Computation of a presentation for $G/\Phi(G)$ when G is a p-group given by generators and relations

Let us suppose that G is a p-group, for which a presentation is given. We would like to compute the quotient group of G with respect to its Frattini subgroup. The following theorems will prove very useful.

THEOREM 2 *If N is the minimal normal subgroup with the property that G/N is elementary abelian, then $N = \Phi(G)$*

PROOF Let M be maximal in G. Then M is normal, since G is a p-group, so G/M is elementary abelian, and then by hypothesis $N \leq M$. This shows that N is contained in the Frattini subgroup of G, since it is contained in all the maximal subgroups of G.
Conversely, consider $G/N = A_1/N \times \ldots \times A_k/N$, where each A_i/N has order p. Let $B_i/N = \times_{j \neq i} A_j/N$. This group is easily seen to be maximal. Clearly $\cap B_i/N$ is equal to the identity in G/N, from which it follows that $\cap B_i = N$. But then N contains the Frattini subgroup of G. □

THEOREM 3 *A presentation for $G/\Phi(G)$ is obtained by adding the relations $[x, y] = 1$ and $x^p = 1$, where x and y range over all the generators of G, to the given presentation of G.*

PROOF Let K be the minimal normal subgroup containing $[x, y]$ and x^p for all generators x and y. G/K is elementary abelian, since $[xK, yK] = 1$ in G/K and $(xK)^p = x^pK = 1$ in G/K. But then $\Phi(G) \leq K$, since by the previous theorem $\Phi(G)$ is the minimal normal subgroup N of G with the property that G/N is elementary abelian.
Conversely, since $G/\Phi(G)$ is elementary abelian, $[x, y] \in \Phi(G)$, $x^p \in \Phi(G)$. This shows that $K \leq \Phi(G)$. □

3.3 On the direct product of two groups

The theorem which follows can be applied to any finite group which is the direct product of two groups to compute its Frattini subgroup.

THEOREM 4 *If a finitely generated group M is the direct product of two subgroups G and H then the Frattini subgroup of M is isomorphic to the direct product of the Frattini subgroup of G and the Frattini subgroup of H.*

PROOF See [3, problem 8.22] □

If the two groups have coprime order we can say much more, namely:

THEOREM 5 *Let G and H be two finite groups of coprime order. Let $x_i = (g_i, h_i)$, $g_i \in G$, $h_i \in H$. Then $x_1, \ldots, x_d$ generate $G \times H$ if and only if $g_1, \ldots, g_d$ generate G and $h_1, \ldots, h_d$ generate H.*

PROOF The if part is true even without the assumption that $|G|$ and $|H|$ are coprime, since the homomorphism that maps an x_i into the corresponding g_i (resp h_i), i.e. the projection homomorphism, is onto.
Conversely let $x_i = (g_i, h_i)$, $g_i \in G$, $h_i \in H$. Then $x_i^{k_i} = (g_i^{k_i}, h_i^{k_i})$. We can choose k_i so that k_i is the order of g_i, and by hypothesis k_i is coprime with the order of h_i. But then h_i and $h_i^{k_i}$ generate the same group, and therefore $\left\langle x_i^{k_i} \right\rangle = \langle h_i \rangle$. It follows that $\langle x_1, \ldots, x_d \rangle \geq \left\langle x_1^{k_1}, \ldots, x_d^{k_d} \right\rangle = \langle h_1, \ldots, h_d \rangle = H$. Using the same argument it is possible to prove that $\langle x_1, \ldots, x_d \rangle \geq G$. By combining the two inclusions it is shown that $\langle x_1, \ldots, x_d \rangle \geq G \times H$. Since it is obvious that $\langle x_1, \ldots, x_d \rangle \leq G \times H$, the theorem follows. □

COROLLARY 3 *If G and H are two finite groups of coprime order then $\phi_d(G \times H) = \phi_d(G)\phi_d(H)$ and $\lambda_d(G \times H) = \lambda_d(G)\lambda_d(H)$*

COROLLARY 4 *If G is a nilpotent group of order $p_1^{e_1} \ldots p_k^{e_k}$ then $\phi_n(G) = \phi_n(G_{p_1}) \cdots \phi_n(G_{p_k})$ and $\lambda_n(G) = \lambda_n(G_{p_1}) \cdots \lambda_n(G_{p_k})$, where G_{p_i} is the p_i-Sylow subgroup of G.*

The last corollary in conjunction with the results about p-groups in Section 3.1 allows one to effectively compute the functions $\phi_n(G)$ and $\lambda_n(G)$ when G is a finite nilpotent group.

3.4 Cyclic groups

Although a finite cyclic group is necessarely nilpotent and therefore it could be analyzed using the results of Section 3.3, its very simple structure allows one to reduce the work needed to compute the Eulerian function. It is well known, in fact, that a cyclic group of order n has one (cyclic) subgroup of order m for each divisor m of n. Therefore the Identity 1 becomes $n^d = \sum_{m|n} \phi_d(C_m)$, from which it follows, by applying the Möbius inversion formula, that

$$\phi_d(C_n) = \mu(m)\frac{n^d}{m^d} = n^d \prod_{p|n} \left(1 - \frac{1}{p^d}\right)$$

where $\mu(m)$ stands for the ordinary Möbius function of an integer, and p ranges over all the prime divisors of n.

4 Some worked examples

In this section we employ the results of the previous sections to show how to compute the Eulerian function for some common classes of groups.

4.1 Groups of prime order

The only subgroup of a group of prime order p is the trivial one. The identity 1 becomes $p^d = \phi_d(1) + \phi_d(C_p) = 1 + \phi_d(C_p)$ from which it follows that $\phi_d(C_p) = p^d - 1$. The application of the Identities 3 and 4 yields $e(C_p) = \frac{p}{p-1}$.

4.2 Groups of order p^2, p prime

It is well known that a group of order p^2 must be abelian. Furthermore, such a group can be either cyclic or the direct product of two cyclic groups of order p. Because of the difficulty of applying Lemma 4, in what follows we will compute the Eulerian function by the using the general formula 1.

- **Cyclic groups of order p^2**
  From the results of Section 3.4 we obtain $\phi_d(C_{p^2}) = p^d(p^d - 1)$. The application of the Identities 3 and 4 yields $e(C_{p^2}) = \frac{p}{p-1}$
- **Elementary abelian groups of order p^2**
  Besides the trivial subgroup an elementary abelian group of order p^2 has only $p + 1$ subgroups, of order p. By applying the identity 1 we obtain $\phi_d(C_p \times C_p) = p^{2d} - p^{d+1} - p^d + p$. The application of the Identities 3 and 4 yields $e(C_p \times C_p) = 2 + \frac{p+2}{p^2-1}$.

4.3 Groups of order pq, p and q primes

A group of order pq, with p and q primes, q less than p, must be either cyclic or non abelian and metacyclic. The second case can happen only if q divides $p - 1$, i.e. a group of order pq, with p and q primes, q less than p, and q not dividing $p - 1$ must be necessarily cyclic.

- **Cyclic groups of order pq**
  By using the result of Section 3.4 we obtain $\phi_d(C_{pq}) = (p^d - 1)(q^d - 1)$. The application of the Identities 3 and 4 yields $e(C_{pq}) = 1 + \frac{1}{p-1} + \frac{1}{q-1} - \frac{1}{pq-1}$
- **Non abelian groups of order pq**
  If M_{pq} is a non abelian group of order pq, with $q < p$, then in addition to the trivial subgroup, it has a normal subgroup of order p and p subgroups of order q. By applying the identity 1 we obtain $\phi_d(M_{pq}) = (pq)^d - p^d - p \cdot q^d + p$. The application of the Identities 3 and 4 yields $e(M_{pq}) = 2 + \frac{1}{q-1} + \frac{1}{p-1} - \frac{p}{pq-1}$

4.4 Groups of small order

In this section we will show that it is possible to compute the functions ϕ_d, λ_d and e for all the groups of order less than sixteen by using the methods discussed in the previous sections. In fact, the group of order 1 is dealt with in Section 2, the groups of order 2, 3, 5, 7, 11, 13 are dealt with in Section 4.1, the groups of order 4, 9 are dealt with in Section 4.2 and the groups of order 6, 10, 14, 15 are dealt with in Section 4.3. We are left now with the groups of order 8 and 12.

It is known that there are five groups of order eight, and they are: C_8, $C_4 \times C_2$, the Quaternion group Q, D_8 and $C_2 \times C_2 \times C_2$.

The first group that we consider is C_8: this is a 2-group with minimal number of generators equal to one. Therefore its behaviour is the same as C_2.

The next three groups, $C_4 \times C_2$, the quaternion group Q and the dihedral group D_8 are 2-groups with minimal number of generators equal to two. Therefore the behaviour of each of these group is the same as V_4.

The last group considered, the elementary abelian group of order eight, is known to have seven subgroups of order two and seven subgroups of order four, isomorphic to the Klein four group, in addition to the trivial subgroup. By applying the Identity 1 we obtain $\phi_d(C_2 \times C_2 \times C_2) = 8^d - 7 \cdot 4^d + 14 \cdot 2^d - 8$. By applying the Identities 3 and 4 we obtain $e(C_2 \times C_2 \times C_2) = \frac{94}{21}$

It is known that there are five groups of order twelve, and they are: C_{12}, $C_2 \times C_2 \times C_3$, A_4, D_{12} and the group $T = \langle a, b \mid a^6 = 1, b^2 = a^3 = (ab)^2 \rangle$.

Let us consider first the cyclic group of order twelve. Since $C_{12} \cong C_4 \times C_3$ according to Theorem 4 we have $\Phi(C_{12}) = \Phi(C_4 \times C_3) \cong \Phi(C_4) \times \Phi(C_3) \cong C_2 \times \{1\} = C_2$ and $C_{12}/\Phi(C_{12}) \cong C_6$. Therefore, by Lemma 4 $\lambda_d(C_{12}) = \lambda_d(C_6)$.

The next group to consider is $C_2 \times C_2 \times C_3$. This group is nilpotent, since it is the direct product of its Sylow subgroups, which are isomorphic to V_4 and C_3. Therefore, according to the results of Section 3.3 we obtain $\phi_d(V_4 \times C_3) = 12^d - 3 \cdot 6^d - 4^d + 2 \cdot 3^d + 3 \cdot 2^d - 2$. By applying the Identities 3 and 4 we obtain $e(V_4 \times C_3) = 6 + \frac{3}{2} - \frac{8}{3} + \frac{24}{11} - \frac{18}{5}$.

The third group to consider is the alternating group on four symbols. The subgroup structure of A_4 is well known: besides the trivial subgroups, A_4 has four subgroups of order three, one subgroup isomorphic to the Klein four group, and three subgroups of order two. By applying the Identity 1 we obtain $\phi_d(A_4) = 12^d - 4 \cdot 3^d - 4^d + 4$. By applying the Identities 3 and 4 we obtain $e(A_4) = \frac{246}{100}$

The fourth group to consider is the dihedral group of order twelve: this group is known to have, besides the trivial subgroups: one cyclic subgroup of order six, two dihedral subgroups of order six, one subgroup of order three, seven subgroups of order two and three subgroups of order four isomorphic to the Klein four-group. By applying the Identity 1 we obtain $\phi_d(D_{12}) = 12^d - 3 \cdot 6^d + 2 \cdot 3^d - 3 \cdot 4^d + 9 \cdot 2^d - 6$. By applying the Identities 3 and 4 we obtain $e(D_{12}) = \frac{1181}{330}$

The last group of order twelve to consider is the group T, isomorphic to the group generated by the two matrices $\begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$ and $\begin{pmatrix} \epsilon & 0 \\ 0 & \epsilon^2 \end{pmatrix}$ where $i = \sqrt{-1}$ and ϵ is a non real complex cubic root of the unity. Besides the trivial subgroups T has three cyclic subgroups of order four, a cyclic subgroup of order six, a cyclic subgroup of order two and a cyclic subgroup of order three. By applying the Identity 1 we obtain $\phi_d(T) = 12^d - 6^d - 3 \cdot 4^d + 3 \cdot 2^d$. By applying the Identities 3 and 4 we obtain $e(T) = \frac{29}{10}$ The results of this section are summarized in Table 1.

4.5 A nontrivial example: $PSL_2(7)$

We conclude our paper with a nontrivial example, $PSL_2(7)$. The structure of the groups $PSL_2(p)$, p prime is given in [4]. In particular, $PSL_2(7)$ has, in addition to the trivial subgroups, 21 subgroups isomorphic to C_2, 21 subgroups isomorphic to C_4, 7 subgroups isomorphic to V_4, 21 subgroups isomorphic to D_8, 28 subgroups isomorphic to C_3, 8 subgroups isomorphic to C_7, 8 noncyclic subgroups of order 21, 28 subgroups isomorphic to S_3, 14 subgroups isomorphic to A_4, 14 subgroups isomorphic to S_4.

Since all these groups, with the exception of S_4, are dealt with in the previous sections, we need to compute only $\phi_d(S_4)$. The structure of S_4 is well known: besides the trivial subgroups S_4 has one subgroups isomorphic to A_4, three subgroups isomorphic to D_8, four subgroups isomorphic to S_3, three subgroups isomorphic to C_4, four subgroups isomorphic to V_4, four subgroups isomorphic to C_3 and nine subgroups isomorphic to C_2. By applying the Identity 1 we obtain $\phi_d(S_4) = 24^d - 12^d - 3 \cdot 8^d - 4 \cdot 6^d + 3 \cdot 4^d + 4 \cdot 3^d + 12 \cdot 2^d - 12$.

For the group $PSL_2(7)$ therefore we obtain $\phi_d(PSL_2(7)) = 168^d - 14 \cdot 24^d - 8 \cdot 21^d + 21 \cdot 8^d + 28 \cdot 6^d + 7 \cdot 4^d + 56 \cdot 3^d - 105 \cdot 2^d + 14$.

The application of the Identities 3 and 4 yields $e(PSL_2(7)) = \frac{49}{3} + \frac{64}{7} - \frac{21^2}{20} - \frac{28^2}{27} - 7 \cdot \frac{42}{41} - \frac{56^2}{55} + 105 \cdot \frac{84}{83} - 14 \cdot \frac{168}{167} \cong 2.38$

G	$\lambda_d(G)$	$e(G)$
$\{1\}$	1	0
C_2	$(2^d - 1)/2^d$	2
C_3	$(3^d - 1)/3^d$	3/2
C_4	$(2^d - 1)/2^d$	2
$C_2 \times C_2$	$(4^d - 3 \cdot 2^d + 2)/4^d$	10/3
C_5	$(5^d - 1)/5^d$	5/4
C_6	$(6^d - 2^d - 3^d + 1)/6^d$	23/10
D_6	$(6^d - 3 \cdot 2^d - 3^d + 3)/6^d$	29/10
C_7	$(7^d - 1)/7^d$	7/6
C_8	$(2^d - 1)/2^d$	2
$C_4 \times C_2$	$(4^d - 3 \cdot 2^d + 2)/4^d$	10/3
$C_2 \times C_2 \times C_2$	$(8^d - 7 \cdot 4^d + 14 \cdot 2^d - 8)/8^d$	94/21
Q	$(4^d - 3 \cdot 2^d + 2)/4^d$	10/3
D_8	$(4^d - 3 \cdot 2^d + 2)/4^d$	10/3
C_9	$(3^d - 1)/3^d$	3/2
$C_3 \times C_3$	$(9^d - 3^{d+1} - 3^d + 3)/9^d$	21/8
C_{10}	$(10^d - 2^d - 5^d + 1)/10^d$	77/36
D_{10}	$(10^d - \cdot 2^d - 5^d + 5)/10^d$	97/36
C_{11}	$(11^d - 1)/11^d$	11/10
C_{12}	$(6^d - 2^d - 3^d + 1)/6^d$	23/10
$C_2 \times C_2 \times C_3$	$(12^d - 3 \cdot 6^d - 4^d + 2 \cdot 3^d + 3 \cdot 2^d - 2)/12^d$	1127/330
A_4	$(12^d - 4 \cdot 3^d - 4^d + 4)/12^d$	246/100
D_{12}	$(12^d - 3 \cdot 6^d + 2 \cdot 3^d - 3 \cdot 4^d + 9 \cdot 2^d - 6)/12^d$	1181/330
T	$(6^d - 3 \cdot 2^d - 3^d + 3)/6^d$	29/10
C_{13}	$(13^d - 1)/13^d$	13/12
C_{14}	$(14^d - 2^d - 7^d + 1)/14^d$	163/78
D_{14}	$(14^d - 7 \cdot 2^d - 7^d + 7)/14^d$	205/78
C_{15}	$(15^d - 3^d - 5^d + 1)/15^d$	47/28

Table 1: Groups of order less than sixteen

Acknoledgements

I would like to thank Prof. M.D. Atkinson for his helpful remarks and for suggesting the problem. Helpful discussions with Prof. J.D. Dixon are gratefully acknoledged.

References

[1] V. Acciaro and M.D. Atkinson. *A new algorithm for testing the regularity of a permutation group.* Congressum Numerantium 90 (1992), 151-160

[2] M.D. Atkinson. *A survey of algorithms for handling permutation groups.* School of Computer Science Technical Report SCS-TR-164, Carleton University, Ottawa, January 1990

[3] J.D. Dixon. *Problems in group theory.* Blaisdell Publishing Company, 1967

[4] P. Hall. *The Eulerian functions of a group.* Quart. J. Math., Ox. Series 7 (1936), 134-151

School of Computer Science, Carleton University
Recent Technical Reports

TR-186 **Reduced Constants for Simple Cycle Graph Separation**
Hristo N. Djidjev and Shankar M. Venkatesan, February 1991

TR-187 **Multisearch Techniques for Implementing Data Structures on a Mesh-Connected Computer**
Mikhail J. Atallah, Frank Dehne, Russ Miller, Andrew Rau-Chaplin, and Jyh-Jong Tsay, February 1991

TR-188 **Generating and Sorting Jordan Sequences**
Alan Knight and Jörg-Rüdiger Sack, March 1991

TR-189 **Probabilistic Estimation of Damage from Fire Spread**
Charles C. Colbourn, Louis D. Nel, T.B. Boffey and D.F. Yates, April 1991

TR-190 **Coordinators: A Mechanism for Monitoring and Controlling Interactions Between Groups of Objects**
Wilf R. LaLonde, Paul White, and Kevin McGuire, April 1991

TR-191 **Towards Decomposable, Reusable Smalltalk Windows**
Kevin McGuire, Paul White, and Wilf R. LaLonde, April 1991

TR-192 **PARASOL: A Simulator for Distributed and/or Parallel Systems**
John E. Neilson, May 1991

TR-193 **Realizing a Spatial Topological Data Model in a Relational Database Management System**
Ekow J. Otoo and M.M. Allam, August 1991

TR-194 **String Editing with Substitution, Insertion, Deletion, Squashing and Expansion Operations**
B John Oommen, September 1991

TR-195 **The Expressiveness of Silence: Optimal Algorithms for Synchronous Communication of Information**
Una-May O'Reilly and Nicola Santoro, October 1991

TR-196 **Lights, Walls and Bricks**
J. Czyzowicz, E. Rivera-Campo, N. Santoro, J. Urrutia and J. Zaks, October 1991

TR-197 **A Brief Survey of Art Gallery Problems in Integer Lattice Systems**
Evangelos Kranakis and Michel Pocchiola, November 1991

TR-198 **On Reconfigurability of Systolic Arrays**
Amiya Nayak, Nicola Santoro, and Richard Tan, November 1991

TR-199 **Constrained Tree Editing**
B. John Oommen and William Lee, December 1991

TR-200 **Industry and Academic Links in Local Economic Development: A Tale of Two Cities**
Helen Lawton Smith and Michael Atkinson, January 1992

TR-201 **Computational Geometry on Analog Neural Circuits**
Frank Dehne, Boris Flach, Jörg-Rüdiger Sack, Natana Valiveti, January 1992

TR-202 **Efficient Construction of Catastrophic Patterns for VLSI Reconfigurable Arrays**
Amiya Nayak, Linda Pagli, Nicola Santoro, February 1992

TR-203 **Numeric Similarity and Dissimilarity Measures Between Two Trees**
B. J. Oommen, K. Zhang and W. Lee, February 1992 (Revised July 1993)

TR-204 **Recognition of Catastrophic Faults in Reconfigurable Arrays with Arbitrary Link Redundancy**
Amiya Nayak, Linda Pagli, Nicola Santoro, March 1992

TR-205 **The Permutational Power of a Priority Queue**
M.D. Atkinson and Murali Thiyagarajah, April 1992

TR-206 **Enumeration Problems Relating to Dirichlet's Theorem**
Evangelos Kranakis and Michel Pocchiola, April 1992

TR-207 **Distributed Computing on Anonymous Hypercubes with Faulty Components**
Evangelos Kranakis and Nicola Santoro, April 1992

TR-208 **Fast Learning Automaton-Based Image Examination and Retrieval**
B. John Oommen and Chris Fothergill, June 1992

TR-209 **On Generating Random Intervals and Hyperrectangles**
Luc Devroye, Peter Epstein and Jörg-Rüdiger Sack, July 1992

TR-210 **Sorting Permutations with Networks of Stacks**
M.D. Atkinson, August 1992

TR-211 **Generating Triangulations at Random**
Peter Epstein and Jörg-Rüdiger Sack, August 1992

TR-212 **Algorithms for Asymptotically Optimal Contained Rectangles and Triangles**
Evangelos Kranakis and Emran Rafique, September 1992

TR-213 **Parallel Algorithms for Rectilinear Link Distance Problems**
Andrzej Lingas, Anil Maheshwari and Jörg-Rüdiger Sack, September 1992

TR-214 **Camera Placement in Integer Lattices**
Evangelos Kranakis and Michel Pocchiola, October 1992

TR-215 **Labeled Versus Unlabeled Distributed Cayley Networks**
Evangelos Kranakis and Danny Krizanc, November 1992

TR-216 **Scalable Parallel Geometric Algorithms for Coarse Grained Multicomputers**
Frank Dehne, Andreas Fabri and Andrew Rau-Chaplin, November 1992

TR-217 **Indexing on Spherical Surfaces Using Semi-Quadcodes**
Ekow J. Otoo and Hongwen Zhu, December 1992

TR-218 **A Time-Randomness Tradeoff for Selection in Parallel**
Danny Krizanc, February 1993

TR-219 **Three Algorithms for Selection on the Reconfigurable Mesh**
Dipak Pravin Doctor and Danny Krizanc, February 1993

TR-220 **On Multi-label Linear Interval Routing Schemes**
Evangelos Kranakis, Danny Krizanc, and S.S. Ravi, March 1993

TR-221 **Note on Systems of Polynomial Equations over Finite Fields**
Vincenzo Acciaro, March 1993

TR-222 **Time-Message Trade-Offs for the Weak Unison Problem**
Amos Israeli, Evangelos Kranakis, Danny Krizanc and Nicola Santoro, March 1993

TR-223 **Anonymous Wireless Rings**
Krzysztof Diks, Evangelos Kranakis, Adam Malinowski, and Andrzej Pelc, April 1993

TR-224 **A consistent model for noisy channels permitting arbitrarily distributed substitutions, insertions and deletions**
B.J. Oommen and R.L. Kashyap, June 1993

TR-225 **Mixture Decomposition for Distributions from the Exponential Family Using a Generalized Method of Moments**
S.T. Sum and B.J. Oommen, June 1993

TR-226 **Switching Models for Non-Stationary Random Environments**
B. John Oommen and Hassan Masum, July 1993

TR-227 **The Probability of Generating Some Common Families of Finite Groups**
Vincenzo Acciaro, September 1993