COUNTING FREE ABELIAN ACTIONS

TAD WHITE

ABSTRACT. We consider the problem of counting commuting r-tuples of elements of the symmetric group S_n, i.e. computing $|\mathrm{Hom}(\mathbf{Z}^r, S_n)|$. The cases $r = 1, 2$ are well-known; a product formula for the case $r = 3$ was conjectured by Adams-Watters and later proved by Britnell. In this note we solve the problem for arbitrary r.

1. Introduction

In [2], Britnell proves the following product formula for the exponential generating function of the number $T(n)$ of ordered triples of commuting elements of the symmetric group S_n:

$$\sum_{n=0}^{\infty} \frac{T(n)}{n!} u^n = \prod_{j=1}^{\infty} (1 - u^j)^{-\sigma(j)} \tag{1}$$

where $\sigma(j)$ denotes the sum of the divisors of j. The right-hand side of (1) is the so-called Euler transform of the sequence $\{\sigma(j)\}$. The formula (1) had been conjectured by Adams-Watters, based on a comparison of sequences A079860 and A061256 in Sloane's Online Encyclopedia of Integer Sequences [6].

In this note we derive an analogous product formula which counts commuting r-tuples in S_n. As Britnell points out, the appearance of the number-theoretic function $\sigma(j)$ in (1) is surprising. The present proof not only yields a unified approach to the known results, but also illuminates the number-theoretic connections. The proof rests on a standard combinatorial technique for enumerating structures in terms of "connected" structures.

2. The result

For any integer $r \geq 0$, let $T_r(n)$ denote the number of r-tuples $\{g_1, \ldots, g_r\}$ in S_n such that $g_i g_j = g_j g_i$ for all i, j. We begin by observing that such tuples correspond precisely to homomorphisms from the group $\mathbf{Z}^r$ to S_n: we map the i-th standard basis vector to g_i. That is, $T_r(n) = |\mathrm{Hom}(\mathbf{Z}^r, S_n)|$.

Equivalently, $T_r(n)$ counts the number of actions of $\mathbf{Z}^r$ on the n-set $[n] = \{1, \ldots, n\}$. We let $T_r(n, k)$ denote the number of such actions with k orbits.

1991 *Mathematics Subject Classification.* 05A15 (Primary), 05E18, 11A25, 20B30 (Secondary).

Key words and phrases. Abelian group, group action, generating function, Euler transform.

For any integer $r \geq 1$, we denote by $\lambda_r(n)$ the number of index-n subgroups of $\mathbf{Z}^r$; for $r = 0$, it will be convenient to define $\lambda_0(n)$ to be 1 if $n = 1$, and 0 otherwise.

Theorem 1. *For any integer $r \geq 1$, we have*

$$\sum_{n,k=0}^{\infty} T_r(n,k)\frac{u^n}{n!}y^k = \prod_{j=1}^{\infty}(1-u^j)^{-y\lambda_{r-1}(j)}. \tag{2}$$

In particular, we can take $y = 1$ to ignore the orbit counts:

$$\sum_{n=0}^{\infty} T_r(n)\frac{u^n}{n!} = \prod_{j=1}^{\infty}(1-u^j)^{-\lambda_{r-1}(j)}. \tag{3}$$

It turns out that $\lambda_r(n)$ is quite tractable:

Lemma 2 (Counting subgroups)**.** *For any $r \geq 1$,*

$$\lambda_r(n) = \sum_{d_1 d_2 \cdots d_r = n} d_2 d_3^2 \cdots d_r^{r-1}.$$

Equivalently, $\{\lambda_r(n)\}$ is the Dirichlet convolution of the sequences $\{n^k\}$ for $0 \leq k < r$ [1].

Proof. Every subgroup of $\mathbf{Z}^r$ has a unique basis in Hermite normal form [3]. If the subgroup has index n in $\mathbf{Z}^r$, this normal form is an upper-triangular $r \times r$ matrix in which the product of the diagonal elements $d_1, \ldots, d_r$ is n, and the elements in the column above d_i lie between 0 and $d_i - 1$ inclusive. Every such matrix corresponds to a unique subgroup, so the lemma follows by counting the possible Hermite normal forms. □

We recover some known results when r is small:

- $r = 1$: The right-hand side of (3) is just $1/(1-u) = \sum_{n \geq 0} u^n$, in accordance with the trivial fact that $T_1(n) = |S_n| = n!$.
- $r = 2$: $\lambda_1(j) = 1$, as $\mathbf{Z}$ has a unique subgroup of each index j. So the right-hand side of (3) becomes

$$\prod_{j \geq 1}(1-u^j)^{-1} = \sum_{n \geq 0} p(n)u^n,$$

  where $p(n)$ is the number of integer partitions of n. Hence $T_2(n) = p(n)\,n!$. (Britnell points out that this result appears in Erdős and Turán [4]; it can also be derived easily by applying Burnside's lemma to the action of G on itself by conjugation.)
- $r = 3$: This is the case considered by Britnell. By Lemma 2, $\lambda_2(j) = \sum_{d|j} d = \sigma(j)$, so (1) follows.

In case $r = 4$, we have

$$\lambda_3(j) = \sum_{de|j} de^2 = \sum_{d|n} d^2\sigma(n/d), \tag{4}$$

which is A001001 in [6]. $T_4(n)/n!$ is the Euler transform of this sequence, namely $\{1, 1, 8, 21, 84, 206, \ldots\}$.

3. The proof

One frequently encounters objects which can be decomposed into a number of independent "connected" objects. The so-called exponential formula [7] is a general combinatorial principle asserting that the exponential generating function (egf) counting the labeled objects is the exponential of the egf counting the labeled connected objects.

In the present context, we wish to count actions of a group G on a set X. The appropriate notion of "connected" in this context is "transitive," since X is the union of its (connected) G-orbits. (Put another way, we can associate to each action a graph with vertex set X, joining two vertices by an edge if some group element sends one to the other. The connected components of this graph are just the orbits of the action; the graph is connected iff the action is transitive.)

Let d_n denote the number of transitive actions of a group G on $[n]$, and let

$$\mathcal{D}(u) = \sum_{n=0}^{\infty} d_n \frac{u^n}{n!}$$

be the egf of $\{d_n\}$. Let $h(n, k)$ denote the number of G-actions on $[n]$ containing k orbits. The exponential formula asserts in this case that:

$$\sum_{n,k=0}^{\infty} h(n,k) \frac{u^n}{n!} y^k = \exp\left(y\mathcal{D}(u)\right) \tag{5}$$

A direct derivation of this result can be found in Lubotzky [5, Prop. 1.10].

Our task is thus to compute $\mathcal{D}(u)$ when $G = \mathbf{Z}^r$, i.e. to enumerate the transitive actions of $\mathbf{Z}^r$ on $[n]$. We begin by observing that transitive actions have a very simple form (see also [5, Prop. 1.1]):

Lemma 3 (Transitive actions are coset actions)**.** *Let G act transitively on a set X. Then there exists a unique subgroup $K \subset G$ such that the given action is equivalent to the action of G on the cosets $K\backslash G$; that is, there is a bijection $f : X \to K\backslash G$ such that*

$$f(x)g = f(xg) \quad \text{for all } x \in X,\ g \in G. \tag{6}$$

Furthermore, there are precisely $|X|$ such bijections.

Proof. Choose a basepoint $* \in X$, and let $K = \mathrm{Stab}(*)$. By transitivity, for any $x \in X$, we can select $g_x \in G$ such that $*g_x = x$. Note that if g is another such choice, we have $*g_x g^{-1} = *$, so $Kg_x = Kg$. Thus the map $f : X \to K\backslash G$ given by $x \mapsto Kg_x$ is well-defined (independent of g_x), and (6) clearly holds.

The $|X|$ bijections arise from the $|X|$ possible choices of $*$: once $f(*)$ has been chosen, (6) determines f completely by transitivity. □

It follows that we can count transitive actions of $G = \mathbf{Z}^r$ on $[n]$ by counting the possible point stabilizers K. K must be an index-n subgroup of $\mathbf{Z}^r$. Given such a K, and the standard action of $\mathbf{Z}^r$ on $\mathbf{Z}^r/K$, we can use any bijection $f : [n] \to \mathbf{Z}^r/K$ to transfer the action to one on $[n]$. By Lemma 3, each action on $[n]$ arises in exactly n ways. Hence each possible K corresponds to $n!/n = (n-1)!$ actions. As there are $\lambda_r(n)$ choices for K, we see that the number of transitive actions of $\mathbf{Z}^r$ on $[n]$ is $(n-1)!\,\lambda_r(n)$.

We can now compute, for fixed $r > 0$, the egf $\mathcal{D}(u)$ for transitive actions of $\mathbf{Z}^r$ on $[n]$:

$$\begin{aligned}
\mathcal{D}(u) &= \sum_{n=0}^{\infty} (n-1)!\,\lambda_r(n)\frac{u^n}{n!} \\
&= \sum_{n=0}^{\infty} \lambda_r(n)\frac{u^n}{n} \\
&= \sum_{n=0}^{\infty} \frac{u^n}{n} \sum_{d_1 d_2 \cdots d_r = n} d_2\, d_3^2 \cdots d_r^{r-1} \quad \text{by Lemma 2} \\
&= \sum_{n=0}^{\infty} u^n \sum_{d_1 d_2 \cdots d_r = n} \frac{1}{d_1}\, d_3 d_4^2 \cdots d_r^{r-2} \\
&= \sum_{d_1, d_2, \ldots, d_r} d_3 d_4^2 \cdots d_r^{r-2}\, \frac{u^{d_1 \cdots d_r}}{d_1} \\
&= \sum_{j \geq 1} -\lambda_{r-1}(j) \log(1 - u^j) \quad \text{after taking } j = d_2 \cdots d_r.
\end{aligned}$$

Theorem 1 now follows immediately from the exponential formula. □

We remark that, while we have considered these power series formally, everything converges within the unit disk. From Lemma 2, since each d_i is at most n, we have $\lambda_r(n) < n^{r(r-1)/2}$, which is polynomial in n. Thus $\sum \lambda_r(n) u^n/n$ converges in the unit disk, and therefore so do the series on the left-hand sides of (2) and (3).

References

[1] T. M. Apostol. *Introduction to Analytic Number Theory.* Undergraduate Texts in Mathematics. Springer, 2010.

[2] J. R. Britnell. A formal identity involving commuting triples of permutations. arXiv:12035079 [math.CO].

[3] H. Cohen. *A Course in Computational Algebraic Number Theory.* Number 138 in Graduate Texts in Mathematics. Springer, 2010.

[4] P. Erdős and P. Turán. On some problems of statistical group theory IV. *Acta Mathematica Academia Scientiarum Hungaricae*, 19(3-4):413–435, 1968.

[5] A. Lubotzky. Counting finite index subgroups. In *Galway 1993, vol. 2*, number 212 in London Mathematical Society Lecture Note Series. Cambridge University Press, 1995.

[6] N. J. A. Sloane. Online Encyclopedia of Integer Sequences. `http://oeis.org`.

[7] H. Wilf. *generatingfunctionology*. A. K. Peters, 2006.

Department of Defense
E-mail address: tadwhite1@gmail.com