ON THE DISTRIBUTION OF THE NUMBER OF CYCLES OF ELEMENTS IN SYMMETRIC GROUPS

Don Zagier

Max-Planck-Institut für Mathematik, Bonn
and Universiteit Utrecht

Abstract. We give a formula for the number of elements in a fixed conjugacy class of a symmetric group whose product with a cyclic permutation has a given number of cycles. A consequence is a very short proof of the formula for the number $\varepsilon_g(n)$ of ways of obtaining a Riemann surface of given genus g by identifying in pairs the sides of a $2n$-gon. This formula, originally proved by a considerably more difficult method in [1], was the key combinatorial fact needed there for the calculation of the Euler characteristic of the moduli space of curves of genus g. As a second application, we show that the number of ways of writing an even permutation $\pi \in \mathfrak{S}_N$ as a product of two N-cycles always lies between $2(N-1)!/(N-r+2)$ and $2(N-1)!/(N-r+19/29)$, where r is the number of fixed points of π, and that both constants "2" and "19/29" are best possible.

Consider the following combinatorial problem. Let C be a conjugacy class in the symmetric group $\mathfrak{S}_N$ on N letters, and let $\sigma \in \mathfrak{S}_N$ denote a cyclic permutation. For $1 \le m \le N$ set

$$p_m(C) = \frac{1}{\#C} \cdot \#\{\pi \in C \mid \pi\sigma \text{ has } m \text{ cycles}\}\,,$$

so that $\sum_{m=1}^{N} p_m(C) = 1$. The problem is to give a closed formula for the numbers $p_m(C)$.

Theorem 1. *The numbers $p_m(C)$ are determined by*

$$\sum_{m=1}^{N} p_m(C)\,\Phi_m(X) = \frac{\chi(C,X)}{(1-X)^{N+2}}\,, \tag{1}$$

where $\chi(C,X) = \det(1-\pi X,\, V)$ is the characteristic polynomial of an element $\pi \in C$ acting on the permutation representation $V = \mathbb{C}^N$ of $\mathfrak{S}_N$ and

$$\Phi_1(X) = \frac{1}{(1-X)^2}\,, \quad \Phi_2(X) = \frac{1+X}{(1-X)^3}\,, \quad \Phi_3(X) = \frac{1+4X+X^2}{(1-X)^4}\,, \ \dots$$

are the polynomials in $\dfrac{1}{1-X}$ defined by $\Phi_m(X) = \sum_{k=1}^{\infty} k^m X^{k-1} \in \mathbb{Z}[[X]]$.

Before giving the proof of this theorem, we mention a few of its consequences.

Application 1. For $\pi \in \mathfrak{S}_N$ denote by $N_i(\pi)$ $(1 \le i \le N)$ and $N(\pi)$ the number of i-cycles and the total number of cycles, respectively, so that $\sum iN_i(\pi) = N$, $\sum N_i(\pi) = N(\pi)$. Since these

are conjugacy class invariants, we also denote them $N_i(C)$ and $N(C)$, where $C = C(\pi)$ is the conjugacy class of π. Then

$$\chi(C,X) = \prod_{i=1}^{N} (1-X^i)^{N_i(C)} \tag{2}$$

is divisible exactly by $(1-X)^{N(C)}$, so the right-hand side of (1) has a pole of order $N+2-N(C)$ at $X=1$. Since $\Phi_m(X)$ is a polynomial of degree $m+1$ in $(1-X)^{-1}$, it follows from (1) that

$$\mathrm{Max}\{m \mid p_m(C) \neq 0\} = N+1-N(C)\,,$$

and in particular, that $N(\pi)+N(\pi\sigma) \le N+1$ for every $\pi \in \mathfrak{S}_N$. This is a special case of the easily proved inequality $N(g_1)+N(g_2) \le N(g_1g_2)+N$, valid for all $g_1,\, g_2 \in \mathfrak{S}_N$.

Application 2. Another easy consequence of (1) is that $p_m(C) = 0$ unless $\mathrm{sgn}(\pi) = (-1)^{m-1}$ ($\pi \in C$). This is of course trivial anyway since $p_m(C) \neq 0$ implies that

$$(-1)^{N-m} = (-1)^{N-N(\pi\sigma)} = \mathrm{sgn}(\pi\sigma) = \mathrm{sgn}(\sigma)\,\mathrm{sgn}(\pi) = (-1)^{N-1}\,\mathrm{sgn}(\pi)$$

for some $\pi \in C$, but it also follows from (1) and (2) together with the observation that $X\Phi_m(X)$ is $(-1)^{m-1}$-symmetric under $X \mapsto 1/X$.

Application 3. In the special case when $\pi \in C$ is cyclic, the number $p_m(C)$ is the probability that a product of two cyclic permutations in $\mathfrak{S}_N$ has exactly m cycles, and (1) says that this number equals $\dfrac{1+(-1)^{N-m}}{(N+1)!}$ times the coefficient of x^m in $x(x+1)\cdots(x+N)$. For example, for N odd the probability that the product of two random cyclic permutations in $\mathfrak{S}_N$ is cyclic is $2/(N+1)$, as opposed to the probability $2/N$ that a random even element of $\mathfrak{S}_N$ is cyclic.

Application 4. The most interesting special case of (1), however, and the main reason for this note, is the case when $N = 2n$ and C is the conjugacy class of free involutions, i.e., any $\pi \in C$ has n cycles of length 2. Here $p_m(C) = 0$ if $m > n+1$ or $n+1-m$ is odd, by the observations in "Application 1" and "Application 2." The number $p_{n+1-2g}(C)$ equals $\varepsilon_g(n)/(2n-1)!!$, where $(2n-1)!! = |C| = 1\times 3\times\cdots\times(2n-1)$ and $\varepsilon_g(n)$ is the number of ways of identifying in pairs the sides of a $2n$-gon to obtain an oriented surface of genus g. (This is because any orientation-reversing pairwise gluing π of the sides gives an oriented surface of *some* genus g, and the resulting surface is triangulated with $N(\pi\sigma)$ vertices, n edges, and one 2-simplex, so that $2-2g = N(\pi\sigma)-n+1$ by Euler's formula.) On the other hand, $\chi(C,X) = (1-X^2)^n$ by (2), so (1) becomes

$$\frac{1}{(2n-1)!!} \sum_{0\le g\le n/2} \varepsilon_g(n)\,\Phi_{n+1-2g}(X) = \frac{(1+X)^n}{(1-X)^{n+2}} \tag{3}$$

or, comparing the coefficients of X^{k-1} on both sides,

$$\frac{1}{(2n-1)!!} \sum_{0\le g\le n/2} \varepsilon_g(n)\,k^{n+1-2g} = \mathrm{Coeff}_{X^{k-1}}\left[\frac{(1+X)^n}{(1-X)^{n+2}}\right] = \mathrm{Coeff}_{T^{n+1}}\left[\frac{1}{2}\left(\frac{1+T}{1-T}\right)^k\right], \tag{4}$$

where the last equality follows from the residue theorem or by computing in two ways the coefficient of $X^{k-1}T^{n+1}$ in $(1+T)/(1-T-X-XT)$.

Formula (4) was proved by a considerably more complicated method in [1] and was the main combinatorial ingredient in the calculation given there of the Euler characteristic of the moduli space of curves of genus g. Actually, the formula was used there in the form

$$\varepsilon_g(n) = \frac{2^{n-2g}\,(2n-1)!!}{(n+1-2g)!}\,\mathrm{Coeff}_{u^{2g}}\left[\left(\frac{u}{\sinh u}\right)^2\left(\frac{u}{\tanh u}\right)^n\right],$$

which can be obtained from (4) either by susbstituting $T = \tanh u$ and applying the residue theorem or else directly from (3) by observing that

$$e^{-x}\,\Phi_m\big(e^{-x}\big) = (-1)^m\,\frac{d^m}{dx^m}\left(\frac{1}{e^x-1}\right) = \frac{m!}{x^{m+1}} + \mathrm{O}(1) \qquad (x\to 0)$$

and then comparing coefficients of u^{2g-2-n} in both sides of (3) with $X = e^{-2u}$. The same method applies to the general case and leads to the following equivalent form of the main theorem:

$$p_m(C) = \frac{1}{m!}\,\mathrm{Coeff}_{x^{N+1-m}}\left[\left(\frac{x}{1-e^{-x}}\right)^{N+2} e^{-x}\,\chi\big(C,e^{-x}\big)\right]. \tag{5}$$

Application 5. It is well-known that every even permutation $\pi \in \mathfrak{S}_N$ is the product of two N-cycles. Let $R(\pi)$ be the number of such representations. It is easy to see that

$$R(\pi) = (N-1)!\;p_1(\pi)\;. \tag{6}$$

On the other hand, it is also easy to verify that the average of $p_m(\pi)$ over all $\pi \in \mathfrak{S}_N$ for any $m \ge 1$ is just the coefficient of y^m in the polynomial $\binom{y+N-1}{N}$. For $m = 1$ this is $1/N$, so (6) gives

$$\mathrm{Average}\big\{R(\pi)\mid \pi\in\mathfrak{S}_N,\ \pi \text{ even}\big\} \;=\; \frac{2\,(N-1)!}{N}\;.$$

We will show that

$$\mathrm{Min}\big\{R(\pi)\mid \pi\in\mathfrak{S}_N,\ \pi \text{ even}\big\} \;\ge\; \frac{2\,(N-1)!}{N+2}\;,$$

so that the minimum value of $R(\pi)$ is only slightly less than its average value. In fact, we will prove the following stronger and rather amusing result.

Theorem 2. *Let $\pi \in \mathfrak{S}_N$ be an even permutation with r fixed points, $0 \le r \le N$. Then*

$$\frac{2\,(N-1)!}{N\,-\,r\,+\,2} \;\le\; R(\pi) \;\le\; \frac{2\,(N-1)!}{N\,-\,r\,+\,\frac{19}{29}} \tag{7}$$

and the constants 2 and $\frac{19}{29}$ appearing in the denominators are both best possible.

We now give the proofs of the two theorems.

Proof of Theorem 1. A well-known formula, valid for any finite group G and conjugacy classes A, B, $C \subseteq G$, says that

$$\#\big\{(a,b,c)\in A\times B\times C\mid abc=1\big\} = \frac{|A|\,|B|\,|C|}{|G|}\sum_{\chi\in\widehat{G}}\frac{\chi(A)\chi(B)\chi(C)}{\chi(1)}$$

(sum over the characters of the irreducible representations of G). An equivalent form of this is

$$\frac{1}{|C|}\sum_{c\in C}F(bc) = \sum_{\chi\in\widehat{G}}\frac{\chi(b)\chi(C)}{\chi(1)}\left(\frac{1}{|G|}\sum_{A}|A|\,\chi(A)\,F(A^{-1})\right) \tag{8}$$

for any $b \in G$ and any class invariant $F : G \to \mathbb{C}$. We apply it to $G = \mathfrak{S}_N$, $b = \sigma$, and $F(\pi) = \Phi_{N(\pi)}(X)$. Let V_0 denote the irreducible $(N-1)$-dimensional subrepresentation of $V = \mathbb{C}^N$ and χ_r $(0 \le r \le N-1)$ the character of the irreducible representation $\Lambda^r(V_0)$. Clearly

$$\sum_{r=0}^{N-1} \chi_r(\pi)\,(-T)^r = \det(1 - \pi\,T,\, V_0) = \frac{\chi(\pi,T)}{1-T} \qquad (\forall \pi \in G). \tag{9}$$

In particular, $\chi_r(\sigma) = (-1)^r$ since $\chi(\sigma,T) = 1 - T^N$ by (2). Hence

$$\sum_{r=0}^{N-1} |\chi_r(\sigma)|^2 = N = \frac{|G|}{|C(\sigma)|} = \sum_{\chi \in \widehat{G}} |\chi(\sigma)|^2$$

(orthogonality relation for characters!), so $\chi(\sigma) = 0$ for all $\chi \notin \{\chi_0, \dots, \chi_{N-1}\}$ and (8) becomes

$$\frac{1}{|C|} \sum_{\pi \in C} \Phi_{N(\pi\sigma)}(X) = \sum_{r=0}^{N-1} \frac{(-1)^r\,\chi_r(C)}{\binom{N-1}{r}} \left(\frac{1}{N!} \sum_A |A|\,\chi_r(A)\,\Phi_{N(A)}(X) \right). \tag{10}$$

But by formulas (9) and (2) we have

$$\begin{aligned} \sum_{r=0}^{N-1} \left(\frac{1}{N!} \sum_A |A|\,\chi_r(A)\,k^{N(A)} \right) (-T)^r &= \sum_{N_1+2N_2+\cdots=N} \frac{k^{N_1+N_2+\cdots}\,(1-T)^{N_1}(1-T^2)^{N_2}\cdots}{1^{N_1}2^{N_2}\cdots N_1!N_2!\cdots(1-T)} \\ &= \frac{1}{1-T}\,\mathrm{Coeff}_{u^N}\left[\prod_{j=1}^{\infty} \sum_{n=0}^{\infty} \frac{k^n(1-T^j)^n u^{nj}}{j^n\,n!} \right] = \frac{1}{1-T}\,\mathrm{Coeff}_{u^N}\left[\left(\frac{1-uT}{1-u} \right)^k \right]. \end{aligned}$$

Multiplying by X^{k-1} and summing over all $k \ge 1$, we find

$$\sum_{r=0}^{N-1} \left(\frac{1}{N!} \sum_A |A|\,\chi_r(A)\,\Phi_{N(A)}(X) \right) (-T)^r = \frac{1}{1-T}\,\mathrm{Coeff}_{u^N}\left[\frac{1-uT}{1-u-X+uXT} \right] = \frac{(1-XT)^{N-1}}{(1-X)^{N+1}}$$

or, comparing the coefficients of $(-T)^r$ on both sides,

$$\frac{1}{N!} \sum_A |A|\,\chi_r(A)\,\Phi_{N(A)}(X) = \binom{N-1}{r} \frac{X^r}{(1-X)^{N+1}}\,.$$

Substituting this into (10) and using (9) again, we obtain the desired formula (1).

Proof of Theorem 2. Write N_i for $N_i(\pi)$, so that $r = N_1$, and denote by $f_\pi(k)$ the polynomial $\sum_{m=1}^{N} p_m(\pi) k^m$. Theorem 1 can be expressed in terms of f_π by the generating function

$$\phi_\pi(y) = \sum_{k=1}^{\infty} f_\pi(k)\,y^{k-1} = \frac{\chi(\pi,y)}{(1-y)^{N+2}} = \frac{1}{(1-y)^{N+2}} \prod_{i=1}^{N} (1-y^i)^{N_i} \tag{11}$$

and we want to compute $p_1(\pi) = f'_\pi(0)$. For this we use:

Lemma. *Let $f(k)$ be a polynomial with $f(0) = 0$ and $\phi(y) = \sum_{k=1}^{\infty} f(k) y^{k-1} \in \mathbb{C}\big[\frac{1}{1-y}\big]$. Then*

$$f'(0) = \int_0^\infty \phi(-t)\, dt\ .$$

Proof. We may assume $f(k) = \binom{k+r-1}{r}$ for some $r \geq 1$, since any polynomial with zero constant term is a linear combination of these. Then $\int_0^\infty \phi(-t)dt = \int_0^\infty (1+t)^{-r-1}dt = 1/r = f'(0)$.

Applying the lemma to the polynomial $f = f_\pi$, we find

$$p_1(\pi) = f'_\pi(0) = \int_0^\infty \phi_\pi(-t)\, dt = 2\int_0^1 \phi_\pi(-t)\, dt\ ,$$

where the last identity follows from the fact that $y\phi_\pi(y)$ is invariant under $y \mapsto 1/y$ since π is even (cf. "Application 3" above). Now substitute $t = x/(1-x)$ and use (11) to get

$$p_1(\pi) = 2\int_0^{1/2} \phi_\pi\big(\frac{-x}{1-x}\big)\, \frac{dx}{(1-x)^2} = 2\int_0^{1/2} \prod_{i=2}^{N} \big[(1-x)^i - (-x)^i\big]^{N_i}\, dx\ . \tag{12}$$

The lower bound in the theorem follows easily. Indeed, for $i \geq 2$ we have

$$(1-x)^i - (-x)^i \ \geq\ \big[(1-2x) + x^2\big]^{i/2} - (x^2)^{i/2} \ \geq\ (1-2x)^{i/2}\ ,$$

so

$$p_1(\pi) \ \geq\ 2\int_0^{1/2} (1-2x)^{(N-N_1)/2}\, dx \ =\ \frac{2}{N - N_1 + 2}$$

with equality if $N = N_1 + 2N_2$, and in view of (6) this is equivalent to the lower bound in equation (7). (Recall that $r = N_1$.) For the other direction, we use the estimates

$$(1-3x+3x^2)^{2/3} = \big[(1-2x)^3 + 2(2x^2-x)^2 + (x^2-x)^2\big]^{1/3} \ \geq\ 1-2x \ =\ (1-x)^2 - x^2$$
$$(1-3x+3x^2)^{i/3} = \big[(1-x)^3 + x^3\big]^{i/3} \ \geq\ (1-x)^i + x^i \ \geq\ (1-x)^i - (-x)^i \qquad \text{if} \quad i \geq 3$$

to get

$$p_1(\pi) \ \leq\ 2\int_0^{1/2} (1-3x+3x^2)^{(N-N_1)/3}\, dx \ =:\ A(N-N_1)\ .$$

An easy analysis shows that $A(k) = 2/(k + c_k)$ where c_k decreases monotonically from $c_2 = 1.24409\ldots$ to $c_8 = 0.64164\ldots$ and then increases monotonically to a limiting value of 1 as $k \to \infty$, with $c_9 = \frac{19}{29}$ and $c_k \geq \frac{19}{29}$ for all k except 7 and 8. This proves the second inequality in (7) for all cases except $N = N_1 + 7$ or $N = N_1 + 8$ and shows also that it is best possible. (Take π with $r = N - 9$ fixed points and three 3-cycles; then (12) shows that $p_1(\pi) = A(9) = 2/(N - r + \frac{19}{29})$.) Finally, for the two cases where $k = N - r$ has the value 7 or 8 we must look at the finite list of partitions of k as $\sum_{i\geq 2} iN_i$ and for each one check that the value of the integral in (12) is $\leq 2/(k + \frac{19}{29})$. (The integrand in (12) is a polynomial, so the ten integrals in question are easy to compute). This completes the proof of the theorem.

Remarks. The author would like to thank Professor T.A. Springer for helpful conversations and in particular for the observation that only the characters χ_r contribute to the calculation of $p_m(C)$. The observation that the combinatorial result in [1] could in principle also be obtained by calculating the numbers $p_m(C)$ for the conjugacy class of free involutions in $\mathfrak{S}_{2n}$ was made to me shortly after [1] appeared by A. Odlyzko, and an explicit calculation along these lines is given in the paper [3] by D.M. Jackson, but with a longer derivation than the one here. Another proof of the combinatorial formula in question was given by Itzykson and Zuber [2], and a completely different proof of the Euler characteristic formula, not relying on a triangulation of the moduli space, by Kontsevich [4].

References

[1] J. Harer and D. Zagier, *The Euler characteristic of the moduli space of curves*, Invent. math. **85** (1986) 457–485

[2] C. Itzykson and J-B. Zuber, *Matrix integration and combinatorics of modular groups*, Comm. Math. Phys. **134** (1990) 197–207

[3] D.M. Jackson, *Counting cycles in permutations by group characters, with an application to a topological problem*, Trans. AMS **299** (1987) 785–801

[4] M. Kontsevich, *Intersection theory on the moduli space of curves and the matrix Airy function*, Comm. Math. Phys. **147** (1992) 1–23