Pólya's enumeration theorem and the symbolic method

Marko R. Riedel

November 18, 2021

1 Introduction

Consider the problem of counting the number of different colorings of a necklace on n beads. Suppose we have χ different beads or colors, and we wish to investigate the asymptotics of this problem, i.e. we ask about the number of different colorings for large n.

The straightforward combinatorics of the problem identify it as a prime candidate for the symbolic method (consult [FS93] for more information). Indeed we may apply the cycle operator $\textsc{Cyc}$ to the generating function χz (there are χ atoms of unit size, namely the beads). The class $\mathcal{A}$ of χ-colored necklaces is the cycle class $\textsc{Cyc}\{\mathcal{B}\}$ where B is the size χ set of unit size beads. The respective generating functions are related by

$$A(z) = \sum_{n\geq 1} \frac{\phi(n)}{n} \log \frac{1}{1-B(z^n)} = \sum_{n\geq 1} \frac{\phi(n)}{n} \log \frac{1}{1-\chi z^n}.$$

The symbolic method translates relations between combinatorial classes into equations in the respective generating functions, which may then be treated by singularity analysis to obtain the asymptotics of their coefficients. These coefficients provide the desired statistic, e.g. in the present case we seek to evaluate

$$[z^n] \sum_{n\geq 1} \frac{\phi(n)}{n} \log \frac{1}{1-\chi z^n}.$$

It is characteristic of the symbolic method that the entire procedure may in many cases by carried out automatically.

There are exceptions, however. The function $A(z)$ has a natural boundary, i.e. the unit circle. Singularity analysis is not likely to be straightforward. Yet the solution is as intuitive as it is simple:

$$[z^n]A(z) \sim \frac{\chi^n}{n},$$

i.e. the majority of necklaces are not periodic and fall into equivalence classes of size n under rotation. (This one-term asymptotic expansion also implies that the dominant contribution to $[z^n]A(z)$ comes from $\log 1/(1-\chi z)$.)

The reader is asked to check this formula. The proof requires little else but algebraic manipulation, or so it might at first appear. A slight shift in perspective, i.e. if we regard the symbolic method as the outer layer of, or interface to, Pólya's theory of counting, reveals that said sequence of algebraic transformations is the equivalent of bypassing the interface to work directly with the underlying machinery. This is somewhat akin to coding a parser in a programming language like `C` rather than writing a grammar and letting `yacc` take care of the details. It is not always pleasant, but sometimes it is necessary.

Pólya's theory of counting may be used whenever a domain of locations is to be mapped to a range of objects and there is a permutation group that partitions the set of locations into equivalence classes. The generating function of the resulting class of composite objects is obtained by substituting the generating function of the object class into the so-called cycle polynomial of the group.

A necklace coloring maps bead positions to colors, or to colored beads. If we say that two necklaces are equivalent if they can be transformed into one another by a rigid motion in the plane, i.e. if we can rotate one to obtain the other, then the permutation group that acts on the set of positions is the cyclic group C_n. This is not the only plausible assumption. Physical necklaces are three-dimensional objects; two necklaces should also be equivalent if they are reflections of one another. Hence we might equally well have chosen the dihedral group D_n.

The cycle polynomial of the cyclic group is the polynomial

$$Z(C_n) = \frac{1}{n} \sum_{f|n} \phi(f) a_f^{n/f}.$$

This equation reflects the structure of the cyclic group C_n, which contains $\phi(f)$ permutations that consist of n/f cycles of length f, for every $f|n$, giving a total of n permutations. Note that $Z(C_n)$ is a polynomial in $\{a_f\}_{f|n}$.

The OGF $A(z)$ of the cycle class $\mathcal{A} = \textsc{Cyc}\{\mathcal{B}\}$ is then given by

$$\sum_{n\geq 1} \frac{1}{n} \sum_{f|n} \phi(f) B(z^f)^{n/f},$$

where $B(z)$ is the OGF of $\mathcal{B}$. (The next section provides a more detailed explanation of the substitution mechanism.) In the present case, $B(z) = \chi z$, and hence

$$[z^n]A(z) = \frac{1}{n} \sum_{f|n} \phi(f) \chi^{n/f} = \frac{\chi^n}{n} + \frac{1}{n} \sum_{f|n \wedge f<n} \phi(f) \chi^{n/f}.$$

We could have done without the cycle operator; in particular, neither the convergence of $A(z)$ nor the nature of the singularity at $z = 1$ of $A(z)$ need be considered.

The use of the symbolic method is not necessarily the most advantageous approach when we are concerned with necklace colorings. This observation suggests that we investigate the relation between Pólya's enumeration theorem and the symbolic method. The purpose of this document is to clarify this relation. We shall see that we can map sequences of permutation groups to sequences of cycle polynomials, and these in turn to combinatorial operators. The latter are likely to be of use when the underlying groups have a common, and reasonably simple structure, e.g. the identity group E_n corresponds to the sequence operator SEQ, and the symmetric group S_n to the multiset operator MSET. The structure of the cyclic group C_n depends critically on the prime factorization of n, and this accounts for the complexity of the corresponding operator CYC. In cases like this one we can profit from direct use of Pólya's theory.

Our reference for the symbolic method is [FS93]. The material on groups and Pólya's theory is from [Har69, p. 178-197].

2 Pólya's enumeration theorem

Let A be a permutation group of order m and degree d. (The group contains m elements, each of which is a permutation of, say, the set of integers $[d] = \{1, 2, 3 \ldots d.\}$)

Every $\alpha \in A$ has a unique decomposition into disjoint cycles. Say this decomposition contains $j_1(\alpha)$ cycles of length 1, $j_2(\alpha)$ cycles of length 2, etc. We may associate to every permutation α a sequence $j_1(\alpha), j_2(\alpha) \ldots j_d(\alpha)$ (a permutation of degree d does not contain any cycles longer than d), where $j_1(\alpha) + 2j_2(\alpha) + \ldots + dj_d(\alpha) = d$ and $0 \le j_k(\alpha) \le \lfloor d/k \rfloor$.

Introduce the sequence of variables $\{a_k\}_{k=1}^{d}$. We may use $\{j_k(\alpha)\}$ to map permutations to polynomials in $\{a_k\}_{k=1}^{d}$. In particular, we map $\alpha \in A$ to $\prod_{k=1}^{d} a_k^{j_k(\alpha)}$, i.e. the exponent of a_k indicates the number of k-cycles in α.

The *cycle polynomial* $Z(A)$ of A is then given by

$$Z(A) = \frac{1}{|A|} \sum_{\alpha \in A} \prod_{k=1}^{d} a_k^{j_k(\alpha)}.$$

Example. The cyclic group C_3 contains the permutations $[1, 2, 3] = (1)(2)(3)$, $[2, 3, 1] = (123)$, and $[3, 1, 2] = (321)$. Hence the cycle polynomial $Z(C_3)$ is

$$Z(C_3) = \frac{1}{3}\left(a_1^3 + 2a_3\right).$$

The alternating group A_3 includes all even permutations of three elements; hence A_3 coincides with C_3. (A permutation is even if it is the.product of an even number of transpositions.) The symmetric group S_3 contains all six permutations of three elements and

$$Z(S_3) = \frac{1}{6}\left(a_1^3 + 3a_2a_1 + 2a_3\right).$$

Consider the following enumeration problem. Given the OGF $C(z)$ of a combinatorial class $\mathcal{C}$ (i.e. the coefficient $[z^n]C(z)$ indicates the number of elements of size n) and a permutation group A of degree d, we wish to count the number of ways of distributing the elements of $\mathcal{C}$ into d bins. Two distributions are equivalent if one can be obtained from the other by permuting the bins according to some $\alpha \in A$. The size of a particular distribution is the sum of the sizes of its constituents.

The group A partitions the set of all possible distributions into equivalence classes, all of whose elements have the same size (the sum of the sizes of the contents of the d bins does not depend on the order of the bins). We seek to enumerate these equivalence classes.

Pólya's enumeration theorem applies. Let $D(z)$ be the OGF of the equivalence classes according to size, i.e. $[z^n]D(z)$ counts the number of equivalence classes of size n. We have

$$D(z) = Z(A)|_{a_1=C(z), a_2=C(z^2), \ldots, a_d=C(z^d)}.$$

(More general versions of this theorem exist. The present one will suffice for our purposes.)

3 The construction of symbolic operators

The theorem as stated concerns single permutation groups whose degree is fixed. Combinatorial operators such as the sequence operator $\textsc{Seq}$ enumerate composite objects with an arbitrary number of components.

Recall, however, that combinatorial operators such as $\textsc{Seq}$, $\textsc{Cyc}$ or $\textsc{Set}$ are in fact sums of fixed-degree operators, i.e.

$$\textsc{Cyc}\{\mathcal{A}\} = \bigcup_{n\geq 1} \textsc{Cyc}_{=n}\{\mathcal{A}\}, \quad \textsc{Seq}\{\mathcal{A}\} = \bigcup_{n\geq 0} \textsc{Seq}_{=n}\{\mathcal{A}\}$$
$$\text{or} \quad \textsc{Set}\{\mathcal{A}\} = \bigcup_{n\geq 0} \textsc{Set}_{=n}\{\mathcal{A}\} \text{ etc.}$$

This decomposition relates Pólya's enumeration theorem to symbolic operators, because the theorem applies to fixed-cardinality classes such as $\textsc{Cyc}\{\mathcal{A}; n\}$. Furthermore, there is a heuristic for the use of symbolic operators. If summing over the respective decomposition simplifies the computation of asymptotic expansions, use the symbolic operator, otherwise compute the expansion for fixed n.

It instructive to consider the nature of the map that is used to construct a specific symbolic operator. We start with a combinatorial class $\mathcal{A}$, whose elements are to be distributed into bins, equivalence classes of distributions being defined by a permutation group Γ_n, where n is fixed. Pólya's theorem solves this enumeration problem; it reduces to the computation of the appropriate cycle polynomial $Z(\Gamma_n)$. We construct a fixed-cardinality operator $(\textsc{Id}(\Gamma_n), E)$ where

$$\textsc{Id}(\Gamma_n)\{\mathcal{A}\} = \mathcal{A}^n/\Gamma_n$$

and

$$E(\Gamma_n; A(z)) = Z(\Gamma_n)|_{a_1=A(z), a_2=A(z^2), \ldots, a_n=A(z^n)}$$

$$\{\Gamma_n\} \longrightarrow \{Z(\Gamma_n)\} \longrightarrow (\textsc{Id}, E)$$

Figure 1: The construction of symbolic operators.

and compute

$$[z^k]E(\Gamma_n, A(z)).$$

(Assume that we wish to count objects of size k. This k may or may not coincide with n.) It may not be necessary to go any farther.

Nonetheless it is possible to consider the following enumeration problem, i.e. given a sequence $\{\Gamma_n\}$ of permutation groups, compute the asymptotics of the number of equivalence classes of a given size k, where any number of bins may be used, or more generally, where the degrees n of $\{\Gamma_n\}$ range over a subset of the integers. This may be done in two different ways. A solution is given by

$$\sum_{n\geq 1}[z^k]E(\Gamma_n; A(z)).$$

It is especially useful when the number $e(k)$ of n such that $[z^k]E(\Gamma_n; A(z)) \neq 0$ is small. E.g. when $\Gamma_n = C_n$ and $A(z) = \chi z$, this number is constant, i.e. $e(k) = 1$.

Clearly

$$[z^k]\sum_{n\geq 1} E(\Gamma_n; A(z)).$$

provides a second solution. If the sum reduces the complexity of the problem, or more importantly, if $e(k)$ is a function of k, e.g. $e(k) = k$ when $\Gamma_n = E_n$ and $[z^k]A(z) > 0$ for all k, it may be appropriate to define an operator $(\textsc{Id}, E)$ where

$$\textsc{Id}\{\mathcal{A}\} = \bigcup_{n\geq 1} \textsc{Id}\left(\Gamma_n\right)\{\mathcal{A}\}$$

and

$$E(A(z)) = \sum_{n\geq 1} Z(\Gamma_n)|_{a_1=A(z), a_2=A(z^2), \ldots, a_n=A(z^n)}$$

and compute

$$[z^k]E(A(z)).$$

We now focus on the algorithmic aspects of this process, illustrated in Fig.1. There are two steps to the construction of a symbolic operator that reflects a sequence $\{\Gamma_n\}$ of permutation groups.

1. Compute the sequence of cycle polynomials $\{Z(\Gamma_n)\}$.
2. Evaluate
$$\sum_{n\geq 1} Z(\Gamma_n)\big|_{a_1=A(z),a_2=A(z^2),\ldots,a_n=A(z^n)}.$$

3.1 The evaluation of cycle indices

The identity group E_p. This group contains a single permutation that consists of p 1-cycles. Hence
$$Z(E_p) = a_1^p.$$

The cyclic group C_p. This group is generated by the rotation
$$\sigma = (1\ 2\ 3\ \ldots\ p)$$
(a single cycle) and consists of $\sigma^0 = e, \sigma^1, \sigma^2, \ldots \sigma^{p-1}$. We ask about the cycle structure of σ^j. We get p fixed points when we are not permuting at all i.e. for $j = 0$ we obtain a_1^p. When $j > 0$ for some element on the cycle we step along the cycle starting at that element making steps of length j and the first time we return to the start is after $\mathrm{lcm}(j, p)$ steps which means we have visited $\mathrm{lcm}(j, p)/j = p/\gcd(j, p)$ elements, which is the length of the cycle the element resides on. The number of cycles is thus given by $\gcd\{j, p\}$. This makes for a contribution of
$$a_{p/\gcd\{j,p\}}^{\gcd\{j,p\}}.$$

Observe that this gives the correct value for $j = 0$, the identity consisting of p fixed points, which with $\gcd\{0, p\} = p$ produces the term a_1^p. This is clearly the only such value for this GCD in the range $[0, p-1]$.

Now for some $d|p$ how many q are there such that $\gcd\{q, p\} = d$? This requires $\gcd\{q/d, p/d\} = 1$ and is given by $\phi(p/d)$, where we use p to represent the identity, working with $[1, p]$. We therefore obtain
$$Z(C_p) = \frac{1}{p}\sum_{d|p} \phi(p/d)a_{p/d}^d$$

The cycle index is alternatively
$$Z(C_p) = \frac{1}{p}\sum_{k|p} \phi(k)a_k^{p/k}.$$

The dihedral group D_p. This group is generated by $g_1 = (12\ldots p)$ and $g_2 = (1p)(2\ p-1)(3\ p-2)\ldots$ It includes C_p as a subgroup.

We need to enumerate the elements of D_p. Note that D_p is isomorphic to the group of additive functions $f : \mathbb{Z}_p \mapsto \mathbb{Z}_p$ that is generated by $g_1 = (z \mapsto z + 1)$ and $g_2 = (z \mapsto p - 1 - z)$, with function composition being the group operation and $\mathbf{1} = (z \mapsto z)$. This group is the union of the two sets $\{z \mapsto z + k\}_{k=0}^{p-1}$

and $\{z \mapsto k - z\}_{k=0}^{p-1}$, and hence $|D_p| = 2p$. The elements of $\{z \mapsto z + k\}_{k=0}^{p-1}$ constitute the subgroup that is isomorphic to C_p. We require the disjoint cycle decomposition of the permutation of $\mathbb{Z}_p$ that is induced by f, where $f \in \{z \mapsto k - z\}_{k=0}^{p-1}$. The fixed points of $(z \mapsto k - z)$ are the solutions of $2z = k$.

There are two cases.

- p *odd.* There is one fixed point and $(p-1)/2$ 2-cycles in all cases.
- p *even.* There are two fixed points when k is even, namely $k/2$ and $(p+k)/2$, and $(p-2)/2$ 2-cycles. There are no fixed points when k is odd, i.e. f consist of $p/2$ 2-cycles.

(We have used the fact that $(z \mapsto k - z)^2 = \mathbf{1}$; hence no cycle in the disjoint cycle decomposition of $f = (z \mapsto k - z)$ can be longer than two.)

We conclude that

$$Z(D_p) = \frac{1}{2p} \sum_{\alpha \in D_p} \prod_{k=1}^{p} a_k^{j_k(\alpha)} = \frac{1}{2} Z(C_p) + \begin{cases} \frac{1}{2} a_1 a_2^{(p-1)/2} & p \text{ odd} \\ \frac{1}{4}\left(a_1^2 a_2^{(p-2)/2} + a_2^{p/2}\right) & p \text{ even.} \end{cases}$$

Example. Define a generalized necklace, (p, b)-necklace for short, as the product of a cycle C_p and the line graph L_b, where $p, b > 1$. One such necklace is shown in Fig. 2. We ask about the number of χ-colorings of this necklace, where two colorings are considered equivalent if the underlying graph has an automorphism that maps one to the other.

Let F_b be the group generated by $g = (1b)(2\ b-1)(3\ b-2)\dots$ so that $Z(F_b) = \frac{1}{2}\left(a_1^b + a_2^{b/2}\right)$ if b is even, and $Z(F_b) = \frac{1}{2}\left(a_1^b + a_1 a_2^{(b-1)/2}\right)$ if b is odd. Let $N_{p,b} = D_p \times F_b$. We require the cycle polynomial $Z(N_{p,b})$.

Start with the contribution from D_p, which acts on the p linked lines of length b. There are two contributions that correspond to C_p and $D_p - C_p$, i.e.

$$\sum_{k|p} \phi(k) a_k^{bp/k} \quad \text{and} \quad \begin{cases} p\, a_1^b a_2^{b(p-1)/2} & p \text{ odd} \\ \frac{p}{2}\left(a_1^{2b} a_2^{b(p-2)/2} + a_2^{bp/2}\right) & p \text{ even.} \end{cases}$$

Note that $g^2 = 1$; hence the remaining elements of $D_p \times F_b$ fall into two categories, i.e. rotations and reflections from D_p that are multiplied by g, understood to act on the b cycles of length p.

We treat reflections first. There are two cases.

b *even.* The length b lines are either fixed under the reflection, or paired with opposite lines; g will split the first type into 2-cycles; the second type consists of line pairs with opposite orientations; these form 2-cycles also. All p permutations consist entirely of 2-cycles and contribute $a_2^{bp/2}$ each to the cycle polynomial.

b *odd.* A line that is fixed by the reflection splits into a single fixed point and $(b-1)/2$ 2-cycles. The remaining lines form pairs that contribute 2-cycles only. Hence we have p permutations of type $a_1 a_2^{(b-1)/2} a_2^{b(p-1)/2} = a_1 a_2^{(bp-1)/2}$ when p is odd. There are $p/2$ permutations of type $a_1^2 a_2^{b-1} a_2^{b(p-2)/2} = a_1^2 a_2^{bp/2-1}$ and $p/2$ permutations of type $a_2^{bp/2}$ when p is even.

It remains to examine rotations that are multiplied by g. There is a central cycle that is fixed by g when b is odd. The remaining cycles form pairs that contain an inner

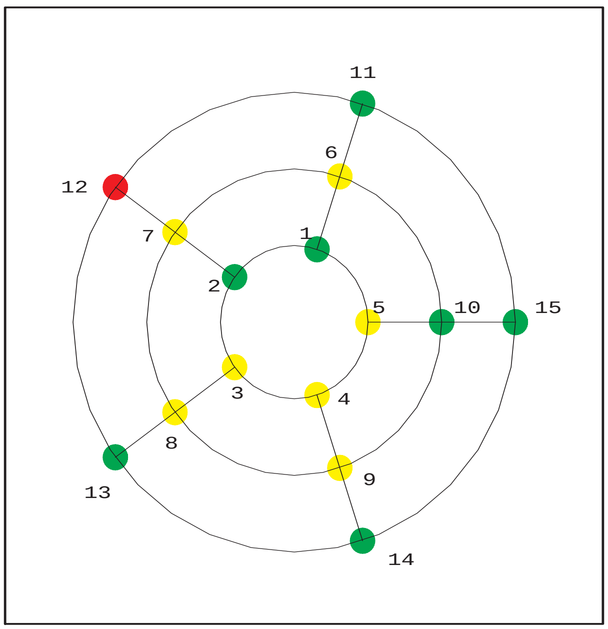

Figure 2: Random coloring of the $(5,3)$-necklace, whose automorphism group is $D_5 \times (S_2 + E_1)$.

and an outer cycle. Any sequence of rotations that contains a g factor necessarily maps nodes on the inner cycle to nodes on the outer one and vice versa. A rotation that is not multiplied by g consists of p/k k-cycles, where $k|p$. A map that does include the g factor runs through two k-cycles simultaneously, one from the inner, and the other from the outer cycle, alternating between the two. If k is even, the map returns to the starting point after k steps, having omitted $k/2$ elements of both cycles. These elements form a k-cycle of their own. If k is odd, we miss the starting point on the first return, and reach it on the second. The inner and the outer cycle merge to form a single cycle of length $2k$.

Therefore the contribution from rotations that are multiplied by g is

$$\sum_{k=2m|p} \phi(k) a_k^{bp/k} + \begin{cases} \sum_{k=2m+1|p} \phi(k) a_{2k}^{bp/2k} & b \text{ even} \\ \sum_{k=2m+1|p} \phi(k) a_k^{p/k} a_{2k}^{(b-1)p/2k} & b \text{ odd.} \end{cases}$$

Let $p = 2n+1$ and $b = 2n$ to obtain

$$\begin{aligned} Z(N_{p,b}) &= \frac{1}{4p} \left(\sum_{k|p} \phi(k) a_k^{bp/k} + p\, a_1^b a_2^{b(p-1)/2} + p\, a_2^{bp/2} + \sum_{k=2m+1|p} \phi(k) a_{2k}^{bp/2k} \right) \\ &= \frac{1}{4} \left(a_1^b a_2^{b(p-1)/2} + a_2^{bp/2} \right) + \frac{1}{4p} \left(\sum_{k|p} \phi(k) \left(a_k^{bp/k} + a_{2k}^{bp/2k} \right) \right). \end{aligned}$$

The number of χ-colorings of the $(2n+1, 2n)$-necklace is given by the value of $Z(N_{p,b})$ at $\{a_k = \chi\}$; asymptotically there are $\chi^{pb}/4p$ such colorings, which reflects the fact that the majority of colorings have no symmetry.

We conclude by pointing out that the above computation is a special case of a more general result, namely the formula

$$Z(A \times B) = \frac{1}{|A|\,|B|} \sum_{(\alpha,\beta) \in A \times B} \prod_{(r,s) \in [d] \times [e]} a_{\mathrm{lcm}\{r,s\}}^{\gcd\{r,s\}\, j_r(\alpha) j_s(\beta)},$$

where d and e are the degrees of the two permutation groups A and B.

E.g. suppose we wished to verify our earlier claim that all reflections that are multiplied by g produce a permutation of the form $a_2^{bp/2}$ when b is even. The formula yields

$$a_{\mathrm{lcm}\{1,2\}}^{\gcd\{1,2\}\, b/2} a_{\mathrm{lcm}\{2,2\}}^{\gcd\{2,2\}\, b/2\, (p-1)/2} = a_2^{bp/2}$$

when p is odd and

$$a_{\mathrm{lcm}\{1,2\}}^{\gcd\{1,2\}\, 2\, b/2} a_{\mathrm{lcm}\{2,2\}}^{\gcd\{2,2\}\, b/2\, (p-2)/2} = a_2^{bp/2} \quad \text{or} \quad a_{\mathrm{lcm}\{2,2\}}^{\gcd\{2,2\}\, b/2\, p/2} = a_2^{bp/2}$$

when p is even.

The symmetric group S_p. This group includes all permutations of p elements.

Let $J = \{\mathbf{j} \mid \sum_{k=1}^{p} k j_k = p\}$. Note that the disjoint cycle decomposition $\prod_{k=1}^{p} a_k^{j_k(\alpha)}$ occurs

$$\frac{p!}{\prod_{k=1}^{p} (k!)^{j_k(\alpha)}} \prod_{k=1}^{p} \left(\frac{k!}{k} \right)^{j_k(\alpha)} \prod_{k=1}^{p} \frac{1}{j_k(\alpha)!}$$

times. (Partition the p elements into subsets, one for each cycle. A subset of size k generates $k!/k$ cycles. The same size $j_k(\alpha)$ set of k-cycles may be chosen in $j_k(\alpha)!$ different ways.)

Hence

$$Z(S_p) = \sum_{\mathbf{j} \in J} \frac{1}{\prod_{k=1}^{p} k^{j_k} j_k!} \prod_{k=1}^{p} a_k^{j_k}.$$

The alternating group A_p. This group includes all even permutations of p elements; its order is $p!/2$.

Let $v(\alpha)$ be the number of inversions of $\alpha \in S_n$ and recall that the parity $\sigma(\alpha)$ of α is defined to be $(-1)^{v(\alpha)}$. We have

$$\sigma(\alpha) = \prod_{n \geq i > j \geq 1} \frac{\alpha(i) - \alpha(j)}{i - j},$$

because (i, j) occurs as $i - j$ in the denominator and as $i - j$ in the numerator if $\alpha^{-1}(i)$ is larger than $\alpha^{-1}(j)$, i.e. if i and j are in order, and as $j - i$ otherwise. An additional property of σ is

$$\sigma(\alpha\beta) = \sigma(\beta\alpha) = \sigma(\beta)\sigma(\alpha),$$

which holds because

$$\prod_{n \geq i > j \geq 1} \frac{(\beta \circ \alpha)(i) - (\beta \circ \alpha)(j)}{i - j} = \prod_{n \geq i > j \geq 1} \frac{(\beta \circ \alpha)(i) - (\beta \circ \alpha)(j)}{\beta(i) - \beta(j)} \frac{\beta(i) - \beta(j)}{i - j}.$$

A transposition $\tau = (c\; c+d)$ has $(d-1)+d = 2d-1$ inversions; hence $\sigma(\tau) = -1$. The product of an even number of transpositions has parity 1, and the product of an odd number of transpositions has parity -1.

A factorization into transpositions of $\gamma = (cc_1 \cdots c_{k-1})$ where $k \geq 2$ is given by $(cc_1)(cc_2) \cdots (cc_{k-1})$. Therefore $\sigma(\gamma) = (-1)^{k-1}$ and

$$\sigma(\alpha) = \prod_{k=1}^{p} \left((-1)^{k-1}\right)^{j_k(\alpha)}.$$

We finally obtain

$$Z(A_p) = Z(S_p) + \sum_{\mathbf{j} \in J} \frac{1}{\prod_{k=1}^{p} k^{j_k} j_k!} \prod_{k=1}^{p} \left((-1)^{k-1} a_k\right)^{j_k}$$

by cancellation of odd permutations.

3.2 Operators from cycle polynomials

We present examples of the second step in the symbolic operator construction, i.e. the substitution into the sequence $\{Z(\Gamma_n)\}$ of the generating function $A(z)$ associated to a combinatorial class $\mathcal{A}$ and the subsequent simplification that

Group Γ	Cycle polynomial $Z(\Gamma)$
E_p	a_1^p
C_p	$\frac{1}{p}\sum_{k\mid p}\phi(k)a_k^{p/k}$
D_p	$\frac{1}{2}Z(C_p)+\begin{cases}\frac{1}{2}a_1a_2^{(p-1)/2} & p \text{ odd}\\ \frac{1}{4}\left(a_1^2a_2^{(p-2)/2}+a_2^{p/2}\right) & p \text{ even.}\end{cases}$
S_p	$\sum_{\mathbf{j}\in J}\frac{1}{\prod_{k=1}^p k^{j_k(\alpha)}j_k(\alpha)!}\prod_{k=1}^p a_k^{j_k(\alpha)}$
A_p	$Z(S_p)+\sum_{\mathbf{j}\in J}\frac{1}{\prod_{k=1}^p k^{j_k(\alpha)}j_k(\alpha)!}\prod_{k=1}^p\left((-1)^{k-1}a_k\right)^{j_k(\alpha)}$
—	$Z(A_p)-Z(S_p)$

Operator ID	OGF $E(\{\Gamma\};A(z))$
SEQ	$\frac{1}{1-A(z)}$
CYC	$\sum_{k\geq 1}\frac{\phi(k)}{k}\log\frac{1}{1-A(z^k)}$
DHD	$\frac{1}{2}E(\{C_p\};A(z))+\frac{1}{4}\frac{2A(z)+A(z)^2+A(z^2)}{1-A(z^2)}$
MSET	$\exp\left(\sum_{l\geq 1}\frac{A(z^l)}{l}\right)$
ALT	$E(\{S_p\};A(z))+\exp\left(\sum_{l\geq 1}(-1)^{l-1}\frac{A(z^l)}{l}\right)$
SET	$\exp\left(\sum_{l\geq 1}(-1)^{l-1}\frac{A(z^l)}{l}\right)$

Figure 3: The map from permutation groups to generating functions.

produces an operator that encapsulates the cycle polynomials $\{Z(\Gamma_n)\}$ and may be applied to $A(z)$ itself. A summary of the material in this section may be found in Fig. 3.

The sequence operator Seq. A length n sequence of objects that are chosen from a given combinatorial class $\mathcal{A}$ is one of the unit-size equivalence classes that constitute $\mathcal{A}^n/E_n$, or the empty sequence if $n = 0$. Hence

$$\textsc{Seq}\{\mathcal{A}\} = \{\lambda\} \cup \bigcup_{n \geq 1} \textsc{Id}\,(E_n)\,\{\mathcal{A}\}$$

and

$$S(A(z)) = 1 + \sum_{n \geq 1} Z(E_n)\big|_{a_1=A(z),a_2=A(z^2),\ldots,a_n=A(z^n)}.$$

But $Z(E_n) = a_1^n$ and hence

$$S(A(z)) = 1 + \sum_{n \geq 1} A(z)^n = \frac{1}{1 - A(z)}.$$

The cycle operator Cyc. This construction was outlined in the introduction.

$$\textsc{Cyc}\{\mathcal{A}\} = \bigcup_{n \geq 1} \textsc{Id}\,(C_n)\,\{\mathcal{A}\}$$

and

$$\begin{aligned} C(A(z)) &= \sum_{n \geq 1} \frac{1}{n} \sum_{k|n} \phi(k) A(z^k)^{n/k} \\ &= \sum_{k \geq 1} \phi(k) \sum_{m \geq 1} \frac{1}{mk} A(z^k)^m = \sum_{k \geq 1} \frac{\phi(k)}{k} \log \frac{1}{1 - A(z^k)}. \end{aligned}$$

The dihedral operator Dhd. This operator counts equivalence classes of $\mathcal{A}^n/D_n$, i.e. two length n sequences are considered equivalent if one can be obtained from the other by a rotation or a lateral reflection in an element if n is odd, and in an element or inter-element gap if n is even.

$$\textsc{Dhd}\{\mathcal{A}\} = \bigcup_{n \geq 1} \textsc{Id}\,(D_n)\,\{\mathcal{A}\}$$

and

$$\begin{aligned} D(A(z)) &= \frac{1}{2} C(A(z)) \\ &+ \frac{1}{2} \sum_{m \geq 0} A(z) A(z^2)^m + \frac{1}{4} \sum_{m \geq 1} \left(A(z)^2 A(z^2)^{m-1} + A(z^2)^m \right) \\ &= \frac{1}{2} C(A(z)) + \frac{1}{4} \frac{2A(z) + A(z)^2 + A(z^2)}{1 - A(z^2)}. \end{aligned}$$

The multiset operator MSET. If n elements of $\mathcal{A}$ are to be distributed into n bins, where repetion is allowed, and two distributions are considered equivalent if we can obtain one from the other by permuting, without restriction, the bins of the first, the distributions so obtained are multisets of elements drawn from $\mathcal{A}$, which must not contain a size zero element. Hence we are counting equivalence classes of $\mathcal{A}^n$ with respect to S_n and

$$\textsc{Mset}\{\mathcal{A}\} = \bigcup_{n\geq 0} \textsc{Id}\,(S_n)\,\{\mathcal{A}\}.$$

We follow [Lov79, p. 199]. Express $Z(S_n)$ recursively by factoring terms according to the size l of the cycle that contains n. There are $\binom{n-1}{l-1}$ ways to choose the remaining $l-1$ elements of the cycle. Every such choice generates $l!/l$ different cycles.

$$Z(S_n) = \frac{1}{n!}\sum_{\alpha\in S_n}\prod_{k=1}^{n} a_k^{j_k(\alpha)} = \frac{1}{n!}\sum_{l=1}^{n}\binom{n-1}{l-1}\frac{l!}{l}\,a_l\,(n-l)!Z(S_{n-l})$$

or

$$Z(S_n) = \frac{1}{n}\sum_{l=1}^{n} a_l Z(S_{n-l})$$

where we define $Z(S_0) = 1$.

Introduce the function

$$M_1(A(z), y) = \sum_{n\geq 0} y^n\; Z(S_n)\big|_{a_1=A(z), a_2=A(z^2),\ldots,a_n=A(z^n)}$$

so that $M(A(z)) = M_1(A(z), 1)$.

The recurrence relation shows that

$$\begin{aligned}
\frac{\partial}{\partial y}M_1(A(z), y) &= \sum_{n\geq 1}\sum_{l=1}^{n} A(z^l)y^{n-1}\left[y^{n-l}\right]M_1(A(z), y)\\
&= \sum_{l\geq 1} A(z^l)y^{l-1}\sum_{n=l} y^{n-l}\left[y^{n-l}\right]M_1(A(z), y)\\
&= \left(\sum_{l\geq 1} A(z^l)y^{l-1}\right)M_1(A(z), y)
\end{aligned}$$

or

$$\frac{\partial}{\partial y}\log M_1(A(z), y) = \sum_{l\geq 1} A(z^l)y^{l-1} \quad\text{and}\quad \log M_1(A(z), y) = \sum_{l\geq 1} A(z^l)\frac{y^l}{l}$$

because $\log M_1(A(z), 0) = \log Z(S_0) = 0$. This yields

$$M(A(z)) = \exp\left(\sum_{l\geq 1}\frac{A(z^l)}{l}\right).$$

The alternating operator Alt. This operator counts equivalence classes of $\mathcal{A}^n$ with respect to A_n, i.e. two distributions are equivalent if one can be obtained from the other by an even number of bin swaps. The principal use of this operator is in the construction of the set operator Set.

We have

$$Z(A_n) = Z(S_n) + Z(S_n)|_{\cdots, a_k := (-1)^{k-1} a_k, \cdots}$$

and hence

$$L(A(z)) = M(A(z)) + \exp\left(\sum_{l \geq 1} (-1)^{l-1} \frac{A(z^l)}{l}\right).$$

The set operator Set. Pólya's enumeration theorem counts equivalence classes of maps from a domain of locations to a range of objects with respect to a permutation group that acts on the domain. It does not distinguish bijections.

The problem of enumerating sets of objects that are drawn from a given combinatorial class is however precisely the problem of counting the number of equivalence classes with respect to the symmetric group of bijective maps from locations to objects. Therefore we cannot expect to use the theorem as stated.

Consider the following observation instead. The multiset operator Mset counts both proper multisets and ordinary sets. There is one equivalence class for every multiset, proper or not. We ask about the relation between these and the equivalence classses that are counted by Alt. An equivalence class with respect to S_n that represents a proper multiset remains the same under A_n, because if we require an odd number of bin transpositions to turn a certain element into another, we may append an extra transposition of two bins that contain the same object. These two bins exist because we assumed that the equivalence class corresponds to a proper multiset. An equivalence class with respect to S_n that represents a set is isomorphic to the set of all size n permutations itself, and splits into two different classes, one isomorphic to the set of size n even permutations, the other to size n odd permutations. Hence

$$\textsc{Set} = \textsc{Alt} - \textsc{Mset}$$

and

$$P(A(z)) = \exp\left(\sum_{l \geq 1} (-1)^{l-1} \frac{A(z^l)}{l}\right).$$

The exponential formula for the set operator Set and the multiset operator Mset are computed and used in [Rie17].

References

[FS93] Philippe Flajolet and Robert Sedgewick. The average case analysis of algorithms: Complex asymptotics and generating functions. Research Report 2026, Institut National de Recherche en Informatique et en Automatique, 1993. 100 pages.

[Har69] Frank Harary. *Graph theory.* Addison-Wesley Publishing Company, 1969. 274 pages. (ISBN 0-201-02787-9).

[Lov79] László Lovász. *Combinatorial problems and exercises.* Akadémiai Kiadó, Publishing House of the Hungarian Academy of Sciences, Budapest, 1979. 551 pages. (ISBN 0-444-85219-0).

[Rie17] Marko Riedel. Cycle indices from the exponential formula and subset / multiset sums divisible by a parameter. Exponential formula PDF, 2017.