ANNALI DELLA
SCUOLA NORMALE SUPERIORE DI PISA
Classe di Scienze

GIAN-CARLO ROTA
DAVID A. SMITH

Enumeration under group action

Annali della Scuola Normale Superiore di Pisa, Classe di Scienze 4e série, tome 4, nº 4 (1977), p. 637-646
<http://www.numdam.org/item?id=ASNSP_1977_4_4_4_637_0>

Enumeration Under Group Action.

GIAN-CARLO ROTA (*) - DAVID A. SMITH (**)

dedicated to Jean Leray

Polya's Theorem is a standard tool of enumerative combinatorial theory. The usual approach to proving it, an excellent exposition of which has been given by de Bruijn [1], relies heavily on the theory of permutation groups. We present here a proof of Polya's Theorem (and generalizations thereof) that requires only the most elementary facts about permutation groups, plus the concept of Möbius inversion on a lattice [3]. This is accomplished by establishing a Galois connection between the lattice of subgroups of a permutation group and the lattice of partitions of the set on which it acts (Section 1). The necessary computations are carried out in the smaller lattice of « closed » partitions and then transferred back to the permutation group. The central computation is actually a double Möbius inversion, and the Möbius function does not appear in the final result. Thus it does not have to be computed explicitly, which is usually the most difficult part of an application of Möbius inversion.

In Section 2 we introduce appropriate formal power series as « generating functions » for sets of functions (« colorings »), and also certain counting functions, one of which is an interesting generalization of the Euler φ function. The relationships among these functions are then explored, including the key inversion formulas. These formulas are then used in Section 3 to derive a generating function for equivalence classes of functions under a group action (Theorem 2). When this result is reformulated in terms of group elements, we arrive at a generalization of Polya's Theorem (Theorem 3).

(*) Massachusetts Institute of Technology.
(**) Duke University and Case Western Reserve University.
Pervenuto alla Redazione il 30 Novembre 1976.

We then note how the classical form of the theorem is obtained from Theorem 3, as well as certain of de Bruijn's generalizations.

Part of the formalism of generating functions and Möbius inversion on the closed partition lattice has been used before in another context to obtain a generalized Baxter-Bohnenblust-Spitzer formula [4]. The details are repeated here, however, to make this paper self-contained, and because slightly different notation will be used.

1. – A Galois theory for permutations and partitions.

Let G be a group of permutations of a set S, and let $L(G)$ be the lattice of subgroups of G, ordered by inclusion. Let $\Pi(S)$ be the lattice of partitions of S, ordered by refinement. Whenever it is convenient to do so, we will identify a partition of S with the corresponding equivalence relation on S.

Define a mapping $\eta: L(G) \to \Pi(S)$ as follows: If H is a subgroup of G, $\eta(H)$ is the partition whose blocks are the H-orbits in S, that is, $a \equiv b \bmod \eta(H)$ if and only if $b = g(a)$ for some $g \in H$. This partition is called the *period* of H. Now define a mapping $\theta: \Pi(S) \to L(G)$: If π is a partition of S, $\theta(\pi)$ is the set of group elements g which leave the blocks of π invariant (or, equivalently, for which the cycles of g are contained within blocks of π). It is clear that $\theta(\pi)$ is a subgroup of G.

One verifies immediately from the definitions that η and θ are increasing mappings, and

$$H \subseteq \theta\eta(H), \quad \text{for all } H \in L(G), \tag{1}$$

$$\pi \geqslant \eta\theta(\pi) \quad \text{for all } \pi \in \Pi(S). \tag{2}$$

These are the defining conditions for η to be a *residuated mapping* with *residual* θ. Alternatively, if we consider the lattice $\Pi(S)^*$ dual to $\Pi(S)$, then η and θ are decreasing mappings, and conditions (1) and (2) state that the pair (η, θ) is a *Galois connection* between $L(G)$ and $\Pi(S)^*$. It follows that $\theta\eta$ and $\eta\theta$ are *closure operators* on $L(G)$ and $\Pi(S)^*$ respectively, *i.e.* idempotent, increasing mappings $x \mapsto \bar{x}$ such that $\bar{x} \geqslant x$ for all x.

Closed subgroups of G are called *periodic* and closed partitions of S are called *periods*. (The latter are precisely the partitions which are periods of subgroups of G.) We will be particularly interested in the periods, and it is convenient to use the abbreviation $\bar{\pi} = \eta\theta(\pi)$. Note that $\bar{\pi}$ refines π (inequality (2)), since $\pi \mapsto \bar{\pi}$ is a *coclosure* operator on $\Pi(S)$. We denote by $\mathcal{T}(G, S)$ the lattice of periods of G in S, *i.e.*

$$\mathcal{T}(G, S) = \{\pi \in \Pi(S) | \bar{\pi} = \pi\},$$

with the induced refinement ordering. (This need not be a sublattice of $\Pi(S)$.) As is the case with any Galois connection, η and θ are inverse order isomorphisms (with the original refinement ordering) between the lattice of periodic subgroups of G and $\mathcal{T}(G, S)$.

2. – Colorings and generating functions.

Polya theory has to do with enumeration of equivalence classes of « colorings » under the operation of groups of « symmetries » of the objects being colored. The set S of objects, henceforth assumed to be finite, and the group G of symmetries have already appeared in the previous section. Let X be another set, at most countable, which may be thought of as representing colors. Then colorings of S are functions $f\colon S \to X$. The kernel of each such function f is an equivalence relation on S, *i.e.* a partition. Its closure will be called the G-period of f in S, denoted per f. We have

$$\theta(\ker f) = \{g \in G | fg = f\} \tag{3}$$

and per f is the partion whose blocks are the orbits of $\theta(\ker f)$.

We associate with each $f \in X^S$ a *monomial*

$$M(f) = \prod_{i \in S} x_{f(i)}^{(i)}$$

in variables $x_j^{(i)}$, where i ranges over S and j over X. This is just a formal device for listing all the ordered pairs of the function. With any set $\mathcal{S}$ of functions we associate a *generating function*

$$M(\mathcal{S}) = \sum_{f \in \mathcal{S}} M(f)\,,$$

which of course is a formal power series in the indicated variables.

A set $\mathcal{F}$ of functions is called a *proper class* (with respect to G) if $fg \in \mathcal{F}$ whenever $f \in \mathcal{F}$ and $g \in G$. Examples of proper classes include: (a) X^S; (b) onto functions; (c) one-to-one functions; (d) the set of functions f such that $hf \in fG$, where h is some fixed permutation of X. With respect to a fixed proper class $\mathcal{F}$ and a partition π of S, we define the following generating functions:

$$A(\pi) = M(\{f \in \mathcal{F} | \ker f = \pi\})\,, \tag{4}$$

$$A_G(\pi) = M(\{f \in \mathcal{F} | \operatorname{per} f = \pi\})\,, \tag{5}$$

$$B(\pi) = M(\{f \in \mathcal{F} | \ker f \geqslant \pi\})\,. \tag{6}$$

Thus A, A_G, and B are functions on $\Pi(S)$ with values in $\mathbf{R}[\![\boldsymbol{x}]\!]$, the ring of formal power series in the variables $x_j^{(i)}$. Let $\mathcal{M}$ denote the additive group of functions $\Pi(S) \to \mathbf{R}[\![\boldsymbol{x}]\!]$, and let $\mathfrak{I}$ denote the incidence algebra ([3] or [5]) of $\Pi(S)$ over $\mathbf{R}[\![\boldsymbol{x}]\!]$. Then $\mathcal{M}$ is both a left and right $\mathfrak{I}$-module in the obvious way:

$$kF(\pi) = \sum_{\sigma \geqslant \pi} k(\pi, \sigma) F(\sigma)\,,$$

$$Fk(\pi) = \sum_{\sigma \leqslant \pi} F(\sigma) k(\sigma, \pi)\,,$$

where $k \in \mathfrak{I}$ and $F \in \mathcal{M}$.

We use the standard notation for the important elements of the incidence algebra, namely, the Kronecker delta function (multiplicative identity element):

$$\delta(x, y) = 1 \quad \text{if } x = y,\ 0 \text{ otherwise;} \tag{7}$$

the characteristic function of the ordering:

$$\zeta(x, y) = 1 \quad \text{if } x \leqslant y,\ 0 \text{ otherwise;} \tag{8}$$

and the Möbius function μ defined by

$$\mu\zeta = \delta\,. \tag{9}$$

The incidence algebra of $\mathcal{T}(G, S)$ is naturally imbedded in $\mathfrak{I}$ [6, p. 17], and the corresponding functions for $\mathcal{T}(G, S)$ are denoted $\delta_{\mathcal{T}}$, $\zeta_{\mathcal{T}}$, $\mu_{\mathcal{T}}$. We also define

$$\bar{\delta}(\pi, \sigma) = \delta(\pi, \bar{\sigma})\,, \qquad \pi, \sigma \in \Pi(S)\,. \tag{10}$$

Then [7, Theorem 1]:

$$\bar{\delta} = \mu_{\mathcal{T}}\zeta\,. \tag{11}$$

(The reversal of factors from the order given in [7] is because the bar represents a coclosure rather than a closure.) Also note that an immediate consequence of the definitions (4) and (6) is:

$$B = \zeta A\,. \tag{12}$$

The important relationships among the generating functions are summarized in the following result.

THEOREM 1 [4, p. 332]. *For any proper class* $\mathcal{F}$,

$$A_G = \mu_{\mathcal{F}} B = \bar{\delta} A \,. \tag{13}$$

That is, for any $\pi \in \Pi(S)$,

$$A_G(\pi) = \sum_{\sigma \geqslant \pi} \mu_{\mathcal{F}}(\pi, \sigma) B(\sigma) = \sum_{\bar{\tau} = \pi} A(\tau) \,. \tag{14}$$

PROOF. By (5) and (4),

$$\begin{aligned} A_G(\pi) &= \sum_{\operatorname{per} f = \pi} M(f) \\ &= \sum_{\bar{\tau} = \pi} \left[\sum_{\ker f = \tau} \right] M(f) \\ &= \sum_{\bar{\tau} = \pi} A(\tau) \,. \end{aligned}$$

Thus $A_G = \bar{\delta} A = \mu_{\mathcal{F}} \zeta A = \mu_{\mathcal{F}} B$, by (11) and (12). ■

Next we introduce two counting functions, one of which is a generalization of the Euler φ-function of number theory. For each period π, let

$$\nu(\pi) = |\theta(\pi)| \,, \tag{15}$$

that is, the number of group elements g whose cycles are contained in blocks of π, and

$$\varphi(\pi) = |\{g \in G | \text{ cycles of } g \textit{ are } \text{blocks of } \pi\}| \,. \tag{16}$$

These functions may be extended to all of $\Pi(S)$ by defining then to be zero if π is not a period. Then it is convenient to treat them as elements of the module $\mathcal{M}$ in the obvious way, by identifying their values (integers) with constant power series. By comparing the definitions (15) and (16), we see that

$$\nu = \varphi \zeta_{\mathcal{F}} \,, \tag{17}$$

so

$$\varphi = \nu \mu_{\mathcal{F}} \,. \tag{18}$$

EXAMPLE. Let G be the cyclic group generated by a single cyclic permutation $g = (1, 2, 3, \ldots, n)$. Then $L(G)$ is isomorphic to the lattice of divisors of n. A typical subgroup has the form (g^m) where $m|n$. The closure of (g^m) is the subgroup of powers of g leaving invariant the cycles of g^m.

Thus every subgroup is closed (periodic). It follows that η is an isomorphism between $L(G)$ and $\mathcal{T}(G, S)$, with the image of (g^m) being the partition whose blocks are the cycles of g^m. If π is that partition, π has m blocks, each with n/m elements. The group elements having the same period are the generators of (g^m), so $\varphi(\pi) = \varphi(n/m)$, where the latter refers to the classical Euler function. The Möbius function $\mu_{\mathcal{T}}$, thought of as defined on the lattice of divisors of n, is essentially the classical Möbius function [3, pp. 346, 350], and $\nu(\pi) = n/m$, the number of distinct powers of g^m. Equation (18) in this context is the familiar relation between Euler and Möbius functions:

$$\varphi(n) = \sum_{d|n} d\mu\left(\frac{n}{d}\right).$$

3. – Polya theory.

We continue to focus on a fixed proper class $\mathcal{F}$ of functions $f: X \to S$, which may be thought of as « admissible colorings ». The group G acts on $\mathcal{F}$ by composition: $f \mapsto fg$. The orbit of f under this action is denoted fG. The following lemma uses the only fact about permutation group theory needed to obtain Polya's theorem.

LEMMA 1. *If* $f_1G = f_2G$, *then* $\operatorname{per} f_1 = \operatorname{per} f_2$.

PROOF. For $i = 1, 2$, let $H_i = \theta(\ker f_i) = \{g \in G | f_i g = f_i\}$. We have $f_2 = f_1 g_0$ for some g_0, and thus $H_1 = g_0 H_2 g_0^{-1}$. Since conjugate subgroups have the same orbits, $\operatorname{per} f_1 = \eta(H_1) = \eta(H_2) = \operatorname{per} f_2$, as desired. ■

LEMMA 2. *If* $\pi = \operatorname{per} f$, *the number of distinct functions in* fG *is* $[G: \theta(\pi)]$, *and thus depends only on* π.

PROOF. $fg_1 = fg_2$ if and only if $g_1 g_2^{-1} \in \theta(\pi)$, so the elements of fG are in one-to-one correspondence with the right cosets of $\theta(\pi)$. ■

The functions having a given period π are represented by the generating function $A_G(\pi)$. According to Lemmas 1 and 2, the formal power series $A_G(\pi)/[G: \theta(\pi)]$ represents the G-equivalence classes of functions with period π. By summing over all periods π, we get a generating function for G-classes of functions in $\mathcal{F}$. The following result indicates how to evaluate that generating function, and is a generalization of Polya's Theorem.

THEOREM 2.

$$\sum_{\pi \in \mathcal{T}(G,S)} \frac{A_G(\pi)}{[G: \theta(\pi)]} = \frac{1}{|G|} \sum_{\sigma \in \mathcal{T}(G,S)} \varphi(\sigma) B(\sigma). \tag{19}$$

PROOF. We have

$$\sum_{\pi} \frac{A_G(\pi)}{[G:\theta(\pi)]} = \frac{1}{|G|} \sum_{\pi} \nu(\pi) A_G(\pi) , \qquad \text{by (15)}$$

$$= \frac{1}{|G|} \sum_{\pi} \nu(\pi) \mu_{\mathcal{T}} B(\pi) , \qquad \text{by (13)}$$

$$= \frac{1}{|G|} \sum_{\pi} \sum_{\sigma \geqslant \pi} \nu(\pi) \mu_{\mathcal{T}}(\pi, \sigma) B(\sigma)$$

$$= \frac{1}{|G|} \sum_{\sigma} \sum_{\pi \leqslant \sigma} \nu(\pi) \mu_{\mathcal{T}}(\pi, \sigma) B(\sigma)$$

$$= \frac{1}{|G|} \sum_{\sigma} \nu \mu_{\mathcal{T}}(\sigma) B(\sigma)$$

$$= \frac{1}{|G|} \sum_{\sigma} \varphi(\sigma) B(\sigma) , \qquad \text{by (18)} .$$

The significance of Theorem 2 lies in the fact that the right hand member of (19) is relatively easy to evaluate as soon as the group G is known: $\varphi(\sigma) = 0$ unless the blocks of σ are the cycles of an element of G. Thus, it is not necessary to know what other partitions are periods. Notice also that the theorem was proved by a double Möbius inversion on the lattice $\mathcal{T}(G, S)$, but $\mu_{\mathcal{T}}$ is not involved in the final result, and therefore need not be known explicitly.

To see that Polya's Theorem is a consequence of Theorem 2, we turn our attention to generating functions which contain less information than the ones introduced thus far, namely, formal power series in variables x_j indexed by X alone. We have an obvious algebra homomorphism T from the one formal power series algebra to the other determined by $T(x_j^{(i)}) = x_j$. We define the *weight* of a function f to be the monomial

$$W(f) = \prod_{i=1}^{n} x_{f(i)} = T(M(f)) ,$$

where $n = |S|$. Clearly, functions in the same G-class have the same weight, so we define $W(fG) = W(f)$. If $\mathcal{S}$ is a set of functions (subset of $\mathcal{F}$), the *inventory* of $\mathcal{S}$ is the formal power series

$$W(\mathcal{S}) = \sum_{f \in \mathcal{S}} W(f) = T(M(\mathcal{S})) .$$

Similarly, the *inventory* of a set of G-classes is the sum of the weights of the classes. (This terminology agrees with that of de Bruijn [1].) The central problem of the Polya theory is to determine the inventory of the set of all classes.

Let $g \in G$ and $\pi = \eta((g))$. We write $B'(g) = T(B(\pi))$. Thus $B'(g)$ is the inventory of the set of $f \in \mathcal{F}$ which are constant on the cycles of g, or, equivalently, for which $fg = f$.

THEOREM 3. *The inventory of the set of all G-classes is*

$$\frac{1}{|G|}\sum_{g\in G} B'(g)\,. \tag{20}$$

PROOF. The desired inventory is

$$\begin{aligned}\sum_{\text{classes } fG} W(fG) &= \sum_{\pi}\sum_{\{fG \mid \text{ker } f=\pi\}} W(fG)\\ &= \sum_{\pi}\frac{1}{[G:\theta(\pi)]}\sum_{\{f \mid \text{ker } f=\pi\}} T(M(f))\,, \quad \text{by Lemma 2}\\ &= T\left[\sum_{\pi}\frac{A_G(\pi)}{[G:\theta(\pi)]}\right]\\ &= T\left[\frac{1}{|G|}\sum_{\pi}\varphi(\pi)B(\pi)\right], \quad \text{by Theorem 2}\\ &= \frac{1}{|G|}\sum_{g\in G} B'(g),\end{aligned}$$

since $\varphi(\pi)$ is the number of distinct elements of G whose cycles are the blocks of π. ■

The standard derivation of Polya's Theorem is based on Burnside's Lemma, which bears a superficial resemblance to Theorem 3. An equivalent of Burnside's Lemma is an immediate corollary, since $B'(g)$ is the inventory of fixed points of g acting on $\mathcal{F}$. If X is finite, we may set all $x_j = 1$ and obtain:

COROLLARY 1. *The number of G-classes in $\mathcal{F}$ is*

$$\frac{1}{|G|}\sum_{g\in G}(\text{number of fixed points of } g)\,.$$

If $\mathcal{F}$ is the proper class X^S of all functions, the inventory of classes may be given more explicitly than in Theorem 3. If $\pi = \eta((g))$, write $\pi = \{\pi_1, \pi_2, \ldots, \pi_k\}$, where $k =$ the number of blocks of π (cycles of g).

If $f g = f$, then

$$T(M(f)) = \prod_{i=1}^{k} x_{f(\pi_i)}^{|\pi_i|}. \tag{21}$$

All possible k-tuples in X occur as subscripts in (21) for such functions f, so

$$\begin{aligned} B'(g) &= \sum_{(j_1,\dots,j_k)} \prod_{i=1}^{k} x_{j_i}^{|\pi_i|} \\ &= \prod_{i=1}^{k} \sum_{j\in X} x_j^{|\pi_i|}. \end{aligned}$$

This last expression depends only on the lengths of the cycles in g, so we introduce the *type* of g, the n-tuple $(b_1, b_2, \dots, b_n)$, where b_i is the number of cycles of length i.

COROLLARY 2 (Polya's Theorem). *If $\mathcal{F} = X^S$, the inventory of G-classes of functions is*

$$\frac{1}{|G|}\sum_{g\in G}\Big(\sum x_j\Big)^{b_1}\Big(\sum x_j^2\Big)^{b_2}\dots\Big(\sum x_j^n\Big)^{b_n}, \tag{22}$$

where, for each g, $(b_1, b_2, \dots, b_n)$ is the type of g.

Several generalizations of Polya's Theorem have been given by de Bruijn (e.g. in [1], [2], and elsewhere), and it is of interest to note how these are related to Theorem 3.

Suppose h is a fixed permutation of X and we want the inventory of classes fG which are h-invariant, i.e. for which $hfG = fG$. As noted above, the set $\mathcal{F}_h$ of functions f such that $hf \in fG$ is a proper class. Clearly, $f \in \mathcal{F}_h$ if and only if fG is h-invariant. Thus, the desired inventory is given by (20), but not in the explicit form given by de Bruijn [2].

Now suppose that X is finite and H is a group of permutations of X. We define a new equivalence relation $\equiv$ on functions $f\colon S \to X$, namely, $f_1 \equiv f_2$ if and only if $hf_1 = f_2 g$ for some $h \in H$ and $g \in G$. The equivalence classes are the sets HfG, so G-equivalence refines $\equiv$. In the terminology introduced above, it doesn't make sense to determine the inventory of these classes (one needs yet another power series algebra and another homomorphism), so we content ourselves with determining the number of $\equiv$ classes. H acts as a permutation group on the G-classes fG, and the classes HfG are the orbits. By Burnside's Lemma, the number of orbits is

$$\frac{1}{|H|}\sum_{h\in H}(\text{number of fixed points of } h).$$

Now fG is a fixed point for h if and only if $f \in \mathcal{F}_h$, so the number of $\equiv$ classes is

$$\frac{1}{|H|}\sum_{h \in H}(\text{number of } G\text{-classes in } \mathcal{F}_h)\,.$$

A similar argument [2] shows that the inventory of $\equiv$ classes, suitably defined, is similarly related to the inventories for the $\mathcal{F}_h$.

REFERENCES

[1] N. G. DE BRUIJN, *Polya's theory of counting*, in Applied Combinatorial Mathematics, ed. by E. F. BECKENBACH, Wiley, 1964, pp. 144-184.

[2] N. G. DE BRUIJN, *Colour patterns which are invariant under a given permutation of the colours*, J. Combinatorial Theory, **2** (1967), pp. 418-421.

[3] G.-C. ROTA, *On the foundations of combinatorial theory*, I: *Theory of Möbius functions*, Z. Wahrscheinlichkeitstheorie, **2** (1964), pp. 340-368.

[4] G.-C. ROTA, *Baxter algebras and combinatorial identities, II*, Bull. Amer. Math. Soc., **75** (1969), pp. 330-334.

[5] D. A. SMITH, *Incidence functions as generalized arithmetic functions, I*, Duke Math. J., **34** (1967), pp. 617-634.

[6] D. A. SMITH, *Incidence functions as generalized arithmetic functions, II*, Duke Math. J., **36** (1969), pp. 15-30.

[7] D. A. SMITH, *Multiplication operators on incidence algebras*, Indiana Univ. Math. J., **20** (1970), pp. 369-383.