REPRESENTATIONS, CHARACTERS, AND COUNTING COLORINGS UNDER SYMMETRY

AMRITANSHU PRASAD

This article is an exposition of Polya's theory of counting colourings of structures under symmetry. It is based on a lecture given to the students of Amrita University on 16th September 2019 and at the inaugural talk of the Berchmans webinar series in Mathematics on 28th May 2020. For a deeper understanding of the topic, the reader is encouraged to read the book of Polya and Read [1].

1. Representations, Characters, and Invariant Vectors

Let G be a finite group and V be a finite-dimensional vector space over $\mathbf{C}$. Let $GL(V)$ denote the set of all invertible linear transformations $V \to V$. The set $GL(V)$ becomes a group under composition.

Definition 1.1 (Representation)**.** A *representation of G on V* is a function $\rho : G \to GL(V)$ such that

$$\rho(gh) = \rho(g)\rho(h) \text{ for all } g, h \in G.$$

In other words, ρ is a group homomorphism.

Given a linear transformation $T : V \to V$, we write $\operatorname{tr}(T; V)$ for the trace of T on V.

Definition 1.2 (Character)**.** The *character* of a representation $\rho : G \to GL(V)$ is the function $\chi_\rho : G \to \mathbf{C}$ defined by:

$$\chi_\rho(g) = \operatorname{tr}(\rho(g); V).$$

Exercise 1.3. *Show that, for any $g, h \in G$,*

$$\chi_\rho(ghg^{-1}) = \chi_\rho(h).$$

In other words, the function χ_ρ is constant on the conjugacy classes of G. A function that is constant on conjugacy classes is known as a class function *The above exercise shows that the character of a representation is a class function.*

Definition 1.4 (Invariant vector)**.** Let $\rho : G \to GL(V)$ be a representation. A vector $v \in V$ is said to be an *invariant vector* if

$$\rho(g)v = v \text{ for all } g \in G.$$

The set of invariant vectors is denoted V^G.

Exercise 1.5. *Show that V^G is a subspace of V.*

Theorem 1.6. *For any representation $\rho : G \to GL(V)$,*

$$\dim V^G = \frac{1}{|G|} \sum_{g \in G} \chi_\rho(g).$$

Proof. Define a linear map $P : V \to V$ by:

$$P(v) = \frac{1}{|G|} \sum_{g \in G} \rho(g) v.$$

We claim that

(1) $P^2 = P$ (in other words, P is *idempotent*),
(2) $P(V) = V^G$.

Since $P^2 = P$, $P(I - P) = 0$. It follows that the only eigenvalues of P are 0 and 1. Therefore the rank of P, which is the number of non-zero characteristic roots, is the multiplicity of 1 as a characteristic root, which is also the sum of characteristic roots, and hence the trace of P. Thus

$$\dim V^G = \text{rank} P = \text{tr} P = \frac{1}{|G|} \sum_{g \in G} \text{tr}(\rho(g); V),$$

as required. □

2. The Orbit-Counting Theorem

Definition 2.1 (G-set)**.** A G-set X is a set X, together with a function $G \times X \to X$ denoted by $(g, x) \mapsto g \cdot x$ (called the action function) such that, if we write $a(g, x)$ as $g \cdot x$, then

$$(gh) \cdot x = g \cdot (h \cdot x).$$

Given a G-set X and an element $x \in X$, the G-orbit of x, denoted $G \cdot x$ is the set of all elements that can be obtained from x by the action of G:

$$G \cdot x = \{g \cdot x \mid g \in G\}.$$

For $x, y \in X$, say that $x \sim_G y$ if y lies in the G-orbit of x. Then using the properties of groups and Definition 2.1, it is easy to show that $\sim_G$ is an equivalence relation on X. Its equivalence classes are the G-orbits of X. The set of G-orbits of X is denoted $G \backslash X$. For each $g \in G$, let X^g denote the points of X that are fixed by g, i.e.,

$$X^g = \{x \in X \mid g \cdot x = x\}.$$

The following theorem is popularly called *Burnside's lemma*, or the *Cauchy-Frobenius lemma*.

Theorem 2.2 (Orbit-counting Theorem)**.** *For any G-set X,*

$$|G\backslash X| = \frac{1}{|G|}\sum_{g\in G}|X^g|.$$

Proof. Let V be a vector space with basis $\{1_x \mid x \in X\}$. For each $g \in G$, define a linear map $\rho(g) : V \to V$ by:

$$\rho(g)1_x = 1_{g\cdot x}.$$

Then ρ is a representation of G on V in the sense of Definition 1.1. With respect to the basis $\{1_x \mid x \in X\}$, the matrix of $\rho(g)$ has entries $\rho(g)_{xy} = \delta_{x,g\cdot y}$, where δ denotes the Kronecker delta function. We have:

$$\mathrm{tr}(\rho(g), V) = \sum_{x\in X}\rho(g)_{xx} = |\{x \in X \mid g\cdot x = x\}| = |X^g|.$$

Now let us determine V^G, the subspace of G-invariant vectors in V. Every vector $v \in V$ is of the form:

$$v = \sum_{x\in X}\alpha_x 1_x, \text{ for uniquely determined scalars } \alpha_x.$$

We have:

$$\rho(g)v = \sum_{x\in X}\alpha_x 1_{g\cdot x} = \sum_{x\in X}\alpha_{g^{-1}\cdot x}1_x.$$

Thus, if $\rho(g)v = v$, equating the coefficients of basis vectors shows that $\alpha_{g^{-1}\cdot x} = \alpha_x$ for all $x \in X$. So $v \in V^G$ if the function $x \mapsto \alpha_x$ is constant on G-orbits in X. Hence a vector in V^G is determined by specifying the coefficient of 1_x for one x in each G-orbit in X. In other words, $\dim V^G = |G\backslash X|$. Now we have:

$$\begin{aligned}|G\backslash X| &= \dim V^G\\ &= \frac{1}{|G|}\sum_{g\in G}\mathrm{tr}(\rho(g); V)\\ &= \frac{1}{|G|}\sum_{g\in G}|X^g|,\end{aligned}$$

completing the proof of the orbit-counting theorem. □

3. Colourings of a Set

Suppose we are given a set $C = \{c_1, \dots, c_r\}$ of colours. A colouring of a set X can be regarded as a function $f : X \to C$. Denote the set of all colourings of X by $C(X)$.

Definition 3.1 (Weight of a colouring)**.** To each colour $c_i \in C$, associate a variable t_i. The weight of a colouring $f \in C(X)$ is defined as:

$$w(f) = t_1^{\lambda_1} t_2^{\lambda_2} \cdots t_r^{\lambda_r},$$

where λ_i it the number of elements of X such that $f(x) = c_i$. Abbreviate $t_1^{\lambda_1} t_2^{\lambda_2} \cdots t_r^{\lambda_r}$ to t^λ.

To warm up, and illustrate how these weights will be used we first state a simple identity involving such weights:

$$\sum_{f \in C(X)} w(f) = (t_1 + \cdots + t_r)^{|X|}.$$

To prove this, observe that when the right hand side is expanded using distributivity we get:

$$(t_1 + \cdots + t_r)^{|X|} = \sum_{f \in C(X)} \prod_{x \in X} t_{f(x)},$$

which is the same as the left hand side.

Now suppose that X is a G-set.

Definition 3.2 (Equivalence of colourings)**.** The set $C(X)$ inherits an action of G from X. For $f \in C(X)$ and $g \in G$,

$$g \cdot f(x) = f(g^{-1} \cdot x).$$

To colourings $f_1, f_2 \in C(X)$ are said to be *equivalent* if they lie in the same G-orbit.

Obviously, equivalent colourings have the same weight. Let $\Lambda(X; r)$ denote the set of all vectors $(\lambda_1, \dots, \lambda_r)$ of vectors with non-negative integer coordinates that sum to $|X|$. For $\lambda \in \Lambda(X, r)$, let $C_\lambda(X)$ denote the colourings of X with weight t^λ.

4. Cycle Type of a Permutation

Let X be a finite set, and $g : X \to X$ be a bijection. Write $g \cdot x$ for the image of x under g. Take any element $x \in X$ and consider the sequence obtained by repeatedly applying g to x:

$$x, g \cdot x, g^2 \cdot x, \dots .$$

Since X is finite, there exist $0 \leq i < j$ such that $g^i \cdot x = g^j \cdot x$. Applying g^{-i} to both sides gives $x = g^{j-i} \cdot x$. Therefore there exists $d \geq 0$ such that $g^d \cdot x = x$. Assume further that for no $d' < d$, $g^{d'} \cdot x = x$. Then all the elements

$$x, g \cdot x, \ldots, g^{d-1} \cdot x$$

must be distinct. The set $\{x, g \cdot x, \ldots, g^{d-1} \cdot x\}$ is called a cycle of g. The cycles of g partition X into parts, say $X_1, \ldots, X_m$. Arrange these parts in decreasing order of cardinality. Let $\mu_1 \geq \mu_2 \geq \cdots \geq \mu_m$ denote the cardinalities of the cycles of g. The vector $\mu = (\mu_1, \ldots, \mu_m)$ is called the *cycle type* of g.

For any vector $\mu = (\mu_1, \ldots, \mu_m)$ of non-negative integers, let

$$p_\mu(t_1, \ldots, t_r) = \prod_{i=1}^{m} (t_1^{\mu_i} + \cdots + t_r^{\mu_i}).$$

The polynomial p_μ is called a *power sum symmetric function*.

Lemma 4.1. Let $g \in G$, and let $C_\lambda(X)^g$ denote the set of elements of $C_\lambda(X)$ fixed by g.

$$\sum_{\lambda \in \Lambda(X,r)} |C_\lambda(X)^g| t^\lambda = p_{\mu(g)}(t_1, \ldots, t_r).$$

Proof. When the right-hand side is expanded using distributivity, we get:

$$\sum_{i_1=1}^{r} \sum_{i_2=1}^{r} \cdots \sum_{i_m=1}^{r} \prod_{j=1}^{m} t_{i_j}^{\mu_i}.$$

Let $X_1, \ldots, X_m$ be the cycles of g in X. Each $(i_1, \cdots, i_m)$ determines a colouring of X as follows: colour all the elements of the cycle X_j with the colour i_j. The colouring so constructed is invariant under g since it is the same for all elements in a cycle of g. Conversely every G-invariant colouring arises in this manner. Moreover, the weight of this colouring is $\prod_{j=1}^{m} t_{i_j}^{\mu_i}$. Summing over all such $(i_1, \ldots, i_m)$ therefore gives the left hand side of the identity in Lemma 4.1. □

5. The Polya Enumeration Theorem

Theorem 5.1 (Polya Enumeration Theorem)**.**

$$\sum_{\lambda \in \Lambda(X,r)} |G \backslash C_\lambda(X)| t^\lambda = \frac{1}{|G|} \sum_{g \in G} p_{\mu(g)}(x_1, \ldots, x_r). \tag{1}$$

Proof. Applying the orbit-counting lemma to the action of G on $C_\lambda(X)$, we have:

$$|G\backslash C_\lambda(X)| = \frac{1}{|G|}\sum_{g\in G}|C_\lambda(X)^g|.$$

Now applying Lemma 4.1 gives

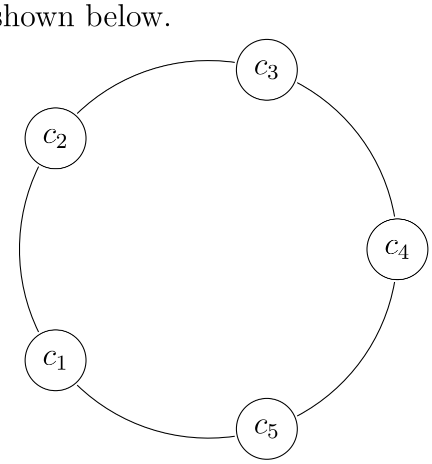
$$\begin{aligned}\sum_{\lambda\in\Lambda(X,r)}|G\backslash C_\lambda(X)|t^\lambda &= \frac{1}{|G|}\sum_{\lambda\in\Lambda(X,r)}\sum_{g\in G}|C_\lambda(X)^g|t^\lambda \\ &= \frac{1}{|G|}\sum_{g\in G}p_{\mu(g)}(t_1,\dots,t_r),\end{aligned}$$

as required. □

Call the symmetric polynomial on the right hand side of (1) the *Polya polynomial* of G. The following section discusses a standard class of examples.

6. Necklace colourings

Consider a necklace with n beads, which are allowed to be of r possible colours, $c_1,\dots,c_r$. Thus a typical necklace can be described by a list of colours: $c_{i_1}, c_{i_2},\dots,c_{i_n}$, describing the colours of the beads starting at some particular bead and going clockwise around the necklace. The case $n = 5$ is shown below.



There is an ambiguity in the choice of the first bead whose colour is listed. Thus the necklace $c_{i_1}, c_{i_2},\dots,c_{i_n}$ is the same as the necklace $c_{i_2}, c_{i_3},\dots,c_{i_n}, c_{i_1}$. This situation can be modelled as a group action as follows: let G be the group $\mathbf{Z}/n\mathbf{Z}$, the group of residue classes of integers modulo n, also known as the cyclic group of order n. The group G acts on itself by the translation action $g\cdot x = g + x$.

For every integer n, let $\phi(n)$ denote the number of integers $0 \leq i < n$ that are coprime to n. The function ϕ is the well-known *Euler totient function*, and $\phi(n)$ can also be interpreted as the number of generators of $\mathbf{Z}/n\mathbf{Z}$. For each $d|n$, $\mathbf{Z}/n\mathbf{Z}$ has exactly one subgroup of order d, generated by the residue class of n/d. This subgroup has $\phi(d)$ generators. Thus $\mathbf{Z}/n\mathbf{Z}$ has $\phi(d)$ elements that generate this subgroup. Since every element of $\mathbf{Z}/n\mathbf{Z}$ generates a unique such subgroup, we get the identity:

$$n = \sum_{d|n} \phi(d).$$

The orbit of $0 \in \mathbf{Z}/n\mathbf{Z}$ under $r \in \mathbf{Z}/n\mathbf{Z}$ is the subgroup generated by r. If d is the gcd of n and r, then this subgroup is $d\mathbf{Z}/n\mathbf{Z} \cong \mathbf{Z}/(n/d)\mathbf{Z}$. The orbit of an element $i \in \mathbf{Z}/m\mathbf{Z}$ under r is a coset of this subgroup. Thus the cycle type or r is $(n/d, n/d, \ldots, n/d)$ (with d repetitions). The number of elements of $\mathbf{Z}/n\mathbf{Z}$ which generate its cyclic subgroup of order n/d is given by $\phi(n/d)$. Thus the Polya polynomial for this group action in r variables is:

$$\phi_{\mathbf{Z}/n\mathbf{Z}}(t_1, \ldots, t_r) = \frac{1}{n} \sum_{d|n} \phi(n/d)(t_1^{n/d} + \cdots t_r^{n/d})^d.$$

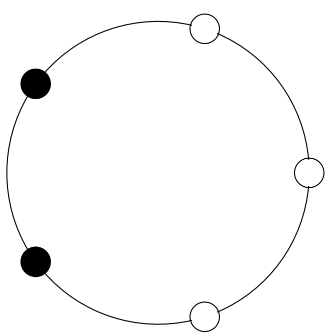
If n is a prime this takes a simpler form:

$$\phi_{\mathbf{Z}/n\mathbf{Z}}(t_1, \ldots, t_r) = \frac{(n-1)(t_1^n + \cdots + t_r^n) + (t_1 + \cdots + t_r)^n}{n}.$$

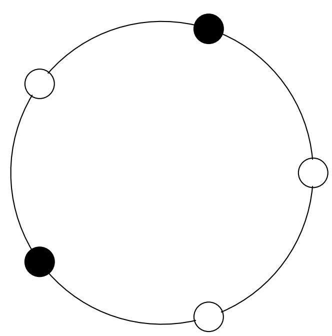
Taking $n = 5$ and $r = 2$ we get:

$$\begin{aligned}\phi_{\mathbf{Z}/5\mathbf{Z}}(t_1, t_2) &= \frac{4(t_1^5 + t_2^5) + (t_1 + t_2)^5}{5} \\ &= t_1^5 + t_1^4 t_2 + 2t_1^3 t_2^2 + 2t_1^2 t_2^3 + t_1 t_2^4 + t_2^5.\end{aligned}$$

So when there are two colours, (say black and white), there are two distinct necklaces with five beads, of which two are black and three are white. These are:



and



When $n = 6$ and $r = 2$, the possible values of $d|6$ are $1, 2, 3, 6$, which ϕ-values $1, 1, 2, 2$, respectively. We get

$$\begin{aligned}\phi_{\mathbf{Z}/6\mathbf{Z}}(t_1, t_2) &= \frac{2(t_1^6 + t_2^6) + 2(t_1^3 + t_2^3)^2 + (t_1^2 + t_2^2)^3 + (t_1 + t_2)^6}{6} \\ &= t_1^6 + t_1^5 t_2 + 3t_1^4 t_2^2 + 4t_1^3 t_2^3 + 3t_1^2 t_2^4 + t_1 t_2^5 + t_2^6.\end{aligned}$$

Thus, for example, there are four distinct necklaces with three white and three black beads. Can you list them?

7. Implementation in Sage

The open-source mathematical software system Sage has two modules which make it almost trivial to compute the Polya polynomial for a group action: it has an interface with GAP for permutation groups and a module for symmetric functions.

A permutation group is nothing but an abstract group expressed as a subgroup of S_n for some n. A permutation group is no different from a group action. Indeed if G acts on X, a set of order n, then labelling the elements of X by integers $1, \ldots, n$ allows us to think of each element of G as a permutation of n letters. Thus the cyclic group group of order 6 is naturally realized as a subgroup of S_6 in Sage:

```
sage: C = CyclicPermutationGroup(6)
sage: list(C)
[(),
 (1,2,3,4,5,6),
 (1,3,5)(2,4,6),
 (1,4)(2,5)(3,6),
 (1,5,3)(2,6,4),
 (1,6,5,4,3,2)]
```

The reader is encouraged to explore permutation groups in Sage with the help of the documentation at `http://doc.sagemath.org/html/en/reference/groups/sage/groups/perm_gps/permgroup.html`.

The other module on symmetric functions makes it very easy to construct the power sum symmetric functions p_μ and expand them in a specified number of variables:

```
sage: def polya_poly(G,r):
....:       S = SymmetricFunctions(QQ)
....:       P = S.powersum()
....:       p = sum([P[w.cycle_type()] for w in G])/G.order()
....:       return p.expand(r)
```

Using this code, the example of Section 6 can be obtained as follows:

```
sage: polya_poly(CyclicPermutationGroup(5),2)
x0^5 + x0^4*x1 + 2*x0^3*x1^2 + 2*x0^2*x1^3 + x0*x1^4 + x1^5
sage: polya_poly(CyclicPermutationGroup(6),2)
x0^6 + x0^5*x1 + 3*x0^4*x1^2 + 4*x0^3*x1^3 + 3*x0^2*x1^4 +
x0*x1^5 + x1^6
```

It is easy to do much fancier things. For example, the number of colourings of the vertices of a dodecahedron in two colours up to its self-isometries can be computed as follows:

```
sage: D = graphs.DodecahedralGraph()
sage: G = D.automorphism_group()
sage: polya_poly(G,2)
x0^20 + x0^19*x1 + 5*x0^18*x1^2 + 15*x0^17*x1^3 +
58*x0^16*x1^4 + 149*x0^15*x1^5 + 371*x0^14*x1^6 +
693*x0^13*x1^7 + 1135*x0^12*x1^8 + 1466*x0^11*x1^9
+ 1648*x0^10*x1^10 + 1466*x0^9*x1^11 +
1135*x0^8*x1^12 + 693*x0^7*x1^13 + 371*x0^6*x1^14
+ 149*x0^5*x1^15 + 58*x0^4*x1^16 + 15*x0^3*x1^17
+ 5*x0^2*x1^18 + x0*x1^19 + x1^20
```

showing that, for example, there are 1648 inequivalent colourings of the vertices of the dodecahedron with ten vertices coloured black and ten vertices coloured white.

Acknowledgements. I thank Dr. K. Somasundaram for inviting me to Amrita University to deliver a lecture on this topic to the students. I thank Mr. S. Prajnanaswaroopa for his comments on a preliminary version of these notes. I thank Ms. Jinu Mary Jameson of St. Berchmans college for inviting me to deliver the inaugural talk of the Berchmans webinar series in Mathematics.

References

[1] G. Polya and R. C. Read. *Combinatorial enumeration of groups, graphs, and chemical compounds*. Springer, 2012.