Computation of the cycle index polynomial of a Permutation Group CS497-report

Rohit Gurjar
Y5383
Supervisor: Prof Piyush P. Kurur
Dept. Of Computer Science and Engineering, IIT Kanpur

November 13, 2008

Abstract

Computing cycle index polynomial of a permutation group is known to be $\#P$-complete. In this report we give some introduction to the problem and describe some permutation groups for which the computation of cycle index polynomial is easy.

1 Introduction

Definition 1. *Cycle index polynomial of a group G of degree n is defined as*

$$P_G(z_1, z_2 \dots z_n) = \frac{1}{|G|} \sum_{g \in G} z_1^{c_1(g)} z_2^{c_2(g)} \dots z_n^{c_n(g)}$$

where $c_i(g)$ represents the number of cycles of length i in the disjoint cycle decomposition of g.

1.1 Application

Let G be a permutation group acting on $X = \{0, 1, \dots n-1\}$ and $\Omega = \{f \ : f \text{ is a function from } X \text{ to } C\}$, where C be a finite set of alphabet of cardinality k. We define a group action on the set Ω by

$$g(\phi)(x) = \phi(g^{-1}(x)) \ for \ each \ \phi \in \Omega$$

The action of G partitions Ω into a number of orbits, being the equivalence classes of Ω under the equivalence relation that identifies α and β whenever there exists $g \in G$ mapping α to β. Then we know the following theorem.

Theorem 1. *Let C, X and G be defined as above. Then the number of orbits of Ω under the action of G is*

$$P_G(k, k, \ldots k).$$

C can be a set of colors. Then the expression $P_G(k, k, \ldots k)$ gives the number of different color patterns of X.

Definition 2. *Let $w : C \to \mathbb{R}$ be a map which assigns a weight from $\mathbb{R}$ (or any ring) to each element of C. Then the weight of $\phi \in \Omega$, with respect to the weight function w is given by, $w(\phi) = \prod_{x \in X} w(\phi(x))$.*

Now, for each $g \in G$ and $\phi \in \Omega$,

$$w\left(g(\phi)\right) = \prod_{x \in X} w\left(g(\phi)(x)\right) = \prod_{x \in X} w\left(\phi(g^{-1}(x))\right) = \prod_{x \in X} w\left(\phi(x)\right) = w(\phi)$$

So, the elements of Ω in the same orbit, under the action of G, will have same weight. So we can define the following.

Definition 3. *Suppose $\Delta \subset \Omega$ be an orbit under the action of G. Then the weight of Δ, denoted $w(\Delta)$, is defined to be equal to $w(\phi)$ for any $\phi \in \Delta$.*

Theorem 2 (Polya's Enumeration Theorem)**.** *With the above definitions and notations*

$$I = \sum_{\Delta} w(\Delta) = P_G(x_1, x_2 \ldots x_n),$$

where the summation goes over distinct orbits of Ω under the action of G and $x_i = \sum_{c \in C} w(c)^i$.

We can see that cycle index polynomial of a permutation group G may be computed at a specified point, directly from definition(1) by explicit enumeration of the elements of G. In general, however, the order of G is exponentially larger than its input size, say a list of generators. Generally, degree n of the permutation group G is taken as the measure of input size. So, we want to compute the cycle index polynomial at a specified point in the time polynomial in degree n. It is known that the problem of computing cycle index polynomial for a group is $\#P$-complete. The proof (given in [1]) involves a polynomial-time reduction from finding number of independent sets in a graph(a $\#P$-complete problem) to computing cycle index polynomial of a permutation group. The proof suggests that that the problem of computing cycle index polynomial is $\#P$-complete even for abelian groups. Here we describe some special permutation groups for which the computation of cycle index polynomial is easy (can be computed in polynomial time).

2 Special Permutation Groups

Notation 1. *Let G be a permutation group with degree n. Consider the permutation $g \in G$, if g is the product of a cycle of length l_1, a cycle of length l_2 and so on till cycle of length l_k, then we say g has a cycle struture $P(g) = z_{l_1} z_{l_2} \dots z_{l_k}$.*

Notation 2. *Let G be a permutation group with degree n. Consider a set of permutations $H \subset G$, then we say*

$$P(H) = \sum_{g \in H} P(g)$$

2.1 Cyclic Groups

Suppose the cyclic group G with degree n acting on $\Omega = \{1, 2, \dots n\}$, is generated by g having cycle structure $P(g) = z_{l_1} z_{l_2} \dots z_{l_k}$ where $1 \leq l_i \leq n \ \forall i$. It is easy to see that $|G| = \text{lcm}\{l_1, l_2 \dots l_k\}$ which can be exponential in n. In general we do not see any easy way to compute cycle index polynomial for cyclic groups. But it is easy in some special cases given below.

Case 1

When $k = 1$ i.e., $g = (1, 2, 3 \dots n)$ and $|G| = n$. So, the cycle index polynomial can be computed very easily. It is given by

$$\frac{1}{n} P(G) = \frac{1}{n} \sum_{d|n} \phi(d) z_d^{n/d}$$

.

Case 2

$|G| = p^m$, where p is a prime, this case is also easy. Because $|G| = \text{lcm}\{l_1, l_2 \dots l_k\} = p^m$ so, $\exists l_i$ s.t. $l_i = p^m$. Hence $|G| = p^m \leq n$. The cycle index polynomial is given by

$$\frac{1}{p^m} P(G) = \frac{1}{p^m} \sum_{i=1}^{m} \phi(p^{m-i}) P(g^{p^i})$$

.

Case 3

If $l_i \neq l_j$ then $\gcd\{l_i, l_j\} = 1 \ \forall i, j \in \{1, 2 \dots k\}$, i.e., distinct l_is are pairwise relatively prime. Let us assume that all l_is are distinct. The results can be easily generalised to the other case.

Let $S_i \subset \Omega$ be the set of elements in the l_i-cycle of g. Consider the subgroup $H_0 = \langle g^{l_1} \rangle$ of group G. This is the subgroup of all permutations in G, which fixes all elements in S_1. Let right cosets of H_0 in G be $\{H_0, H_1, \dots H_{l_1 - 1}\}$ and

the corresponding representatives are $\{g^0, g^1 \dots g^{l_1-1}\}$. It is easy to see that $P(G) = \sum_{i=0}^{l_1-1} P(H_i)$

Let G_1 and G_1' be permutation groups acting on S_1 and $\Omega \backslash S_1$ respectively and for every $h \in G$ we can write $h = h_1 \times h_1'$ where, $h_1 \in G_1$ and $h_1' \in G_1'$, s.t. $h_1(i) = h(i)\ \forall i \in S_1$ and $h_1'(i) = h(i)\ \forall i \in \Omega \backslash S_1$. Let $g = g_1 \times g_1'$, where $g_1 \in G_1$ and $g_1' \in G_1'$. Now, we can see that $H_0 = \langle g^{l_1} \rangle \approx \langle {g_1'}^{l_1} \rangle$. Now, because $\forall j \in \{1, 2, \dots k\}$ l_1 and l_j are relatively prime, $\langle {g_1'}^{l_1} \rangle = G_1'$. So, $G_1' \approx H_0$.
Now,

$$H_i = g^i H_0$$

$$H_i = (g_1^i \times {g_1'}^i) H_0$$

$$H_i = (g_1^i \times {g_1'}^i) G_1'$$

${g_1'}^i \in G_1'$, so ${g_1'}^i G_1' = G_1'$. Hence,

$$H_i = g_1^i \times G_1'$$

So,

$$P(G) = \left(\sum_{i=0}^{l_1-1} P(g_1^i) \right) \times P(G_1')$$

$$P(G) = P(G_1) \times P(G_1')$$

Inductively, $P(G) = P(G_1) \times P(G_2) \cdots \times P(G_k)$, where for every $j \in \{1, 2 \dots k\}$, G_j be permutation group acting on S_j, and for every $h \in G$ we can write $h = h_1 \times h_2 \cdots \times h_k$ where, $h_j \in G_j$ s.t. $h_j(i) = h(i)\ \forall i \in S_j$.
Now, $|G_j| = l_j \leq n$, so $P(G_j)$ can be computed easily for all $j \in \{1, 2 \dots k\}$. Then the cycle index polynomial will be given by

$$\frac{1}{|G|} P(G) = \frac{1}{|G|} \left(P(G_1) \times P(G_2) \cdots \times P(G_k) \right)$$

2.2 Symmetric Group

Computing cycle index polynomial for symmetric group(whole permutation group) can be done easily because of its symmetry. Let G be the symmetric group acting on $\Omega = \{a_1, a_2, \dots a_n\}$. Consider the following definition for group $G\ \forall i \in \{1, 2, \dots n\}$,

$$P_i(G) = \sum_{\substack{g \in G \\ a_n \text{ is in a} \\ i-\text{cycle in } g}} P(g)$$

We can see that $P(G) = \sum_{i=1}^{n} P_i(G)$. Consider the subgroup H_0 of all permutations in G which fixes a_n. Consider $H \approx H_0$ as acting on $\Omega \backslash \{a_n\}$. For H,

$P_i(H)$, would be defined like this,

$$P_i(H) = \sum_{\substack{g \in H \\ a_{n-1} \ is \ in \ a \\ i-cycle \ in \ g}} P(g)$$

Note that $P_n(H) = 0$. Because in any $g \in H$ maximum length of a cycle can be $n-1$.
We give the following recursive algorithm for computing cycle index polynomial for a symmetric group at the point $(z_1, z_2 \dots z_n)$.

Algorithm 1 cycle-index(G)

Require: A symmetric group G with degree n.
Ensure: $P(G)$ and $P_i(G)$ $\forall i \in \{1, 2, \dots n\}$ at the point $(z_1, z_2 \dots z_n)$

```
if n == 1 then
    return {z_1, z_1}
else
    {P(H), P_1(H), P_2(H) ... P_{n-1}(H)} ← cycle-index(H)
    P_1(G) ← z_1 P(H)
    for i ← 2 to n do
        P_i(G) ← (n − 1) (z_i / z_{i−1}) P_{i−1}(H)
    end for
    P(G) ← P_1(G) + P_2(G) ··· + P_n(G)
    return {P(G), P_1(G), P_2(G) ... P_n(G)}
end if
```

Then the cycle index polynomial of G will be given by $\frac{1}{n!}P(G)$.
We can see that the algorithm takes $O(n^2)$ time.

Theorem 3. *With the notations given above,* $P_1(G) = z_1 P(H)$ *and* $P_i(G) = (n-1)\left(\frac{z_i}{z_{i-1}}\right) P_{i-1}(H)$ $\forall i \in \{2, 3, \dots n\}$. *And hence, the algorithm is correct.*

Proof. Consider the case when $i = 1$. Note that, $\{g \in G | a_n \ is \ in \ a \ 1 - cycle \ in \ g\} = \{g \in G | g \ fixes \ a_n\} = H_0$. So, $P_1(G) = P(H_0) = z_1 P(H)$. Now, when $i \geq 2$, let us say the right cosets of H_0 in G are $\{H_0, H_1, H_2 \dots H_{n-1}\}$ and the corresponding representatives are $\{I, (a_n, a_1), (a_n, a_2) \dots (a_n, a_{n-1})\}$, where I is the identity element of G. Now, we can see that, $P(G) = \sum_{j=0}^{n-1} P(H_j)$.
We can also write that

$$P_i(G) = \sum_{j=0}^{n-1} P_i(H_j) \tag{1}$$

where $P_i(H_j) = \sum_{\substack{g \in H_j \\ a_n \ is \ in \ a \\ i-cycle \ in \ g}} P(g)$.

We know that $H_{n-1} = H_0 g_{n-1}$, where $g_{n-1} = (a_n, a_{n-1})$. We can easily see that

$$(b, c, d, e \dots).(a, b) = (a, b, c, d, e \dots)$$

So, suppose $h \in H_0$ s.t. $P(h) = z_1 z_{l_1} z_{l_2} \dots z_{l_k}$, and a_{n-1} is in l_1-cycle. Then $P(hg_{n-1}) = z_{l_1+1} z_{l_2} \dots z_{l_k}$. So, it is clear that $\forall i \geq 2$

$$P_i(H_0 g_{n-1}) = \left(\frac{z_i}{z_{i-1}}\right) P_{i-1}(H)$$

$$P_i(H_{n-1}) = \left(\frac{z_i}{z_{i-1}}\right) P_{i-1}(H) \tag{2}$$

Notation 3. *For any $g \in G$, let*

$$P_i(g) = \begin{cases} P(g) & \text{if } a_n \text{ is in a } i\text{-cycle in } g \\ 0 & \text{otherwise.} \end{cases}$$

So, we can say that $P_i(H_j) = \sum_{g \in H_j} P_i(g)$.

Let $h \in H_{n-1}$, consider the function f s.t. $f(h) = (a_j, a_{n-1}) h (a_j, a_{n-1})$ for some $j \in \{1, 2 \dots n-2\}$. For some $h_0 \in H_0$, we can write $h = h_0(a_n, a_{n-1})$, and so $f(h) = (a_j, a_{n-1}) h_0 (a_n, a_{n-1})(a_j, a_{n-1}) = (a_j, a_{n-1}) h_0 (a_j, a_{n-1})(a_n, a_j) = h_0'(a_n, a_j)$. It is easy to see that $h_0' = (a_j, a_{n-1}) h_0 (a_j, a_{n-1}) \in H_0$. So, $f(h) \in H_j$. The cycle structures of h and $f(h)$ are same, except that the positions of a_{n-1} and a_j are swapped. So, we can say that $P_i(h) = P_i(f(h)) \; \forall i \in \{1, 2, \dots n\}$. Also, it is easy to see that $f : H_{n-1} \to H_j$ is a bijection. So,

$$\begin{aligned} P_i(H_{n-1}) &= \sum_{h \in H_{n-1}} P_i(h) \\ &= \sum_{h \in H_{n-1}} P_i(f(h)) \\ &= \sum_{h' \in H_j} P_i(h') \\ &= P_i(H_j) \; \forall j \in \{1, 2, \dots n-2\} \end{aligned} \tag{3}$$

From (1),

$$\begin{aligned} P_i(G) &= \sum_{j=0}^{n-1} P_i(H_j) \\ &= \sum_{j=1}^{n-1} P_i(H_j) \quad \{\because H_0 \text{ fixes } a_n \\ &= (n-1) P_i(H_{n-1}) \quad \{\text{from (3)} \\ &= (n-1) \left(\frac{z_i}{z_{i-1}}\right) P_{i-1}(H) \quad \{\text{from (2)} \end{aligned}$$

□

2.3 Alternating Group

Let G be a permutation group with degree n and H be a subset of G such that $H = \{g | g \in G$ and g is an even permutation$\}$. It is easy to see that H is a subgroup of G. So, consider the following

Lemma 1.

$$|G| = 2 \times |H|$$

Proof. Let the left cosets of H in G be $\{H, H_1, H_2 \dots H_k\}$ and their representatives are $\{I, a_1, a_2 \dots a_k\}$ respectively. It is easy to see that a_i is an odd permutation for all $1 \leq i \leq k$. So, for all $1 \leq i, j \leq k$, the element $a_i a_j^{-1}$, will be an even permutation and so $a_i a_j^{-1} \in H$. Hence a_i and a_j are in same coset. And this is true for all $1 \leq i, j \leq k$. So $k = 1$, and there are only two left cosets of H in G. Hence, $|G| = 2 \times |H|$. □

Theorem 4.

$$P_H(z_1, z_2 \dots z_n) = P_G(z_1, z_2 \dots z_n) + P_G(x_1, x_2 \dots x_n)$$

where $x_i = (-1)^{i-1} z_i$.

Proof.

$$\begin{aligned} P_G(x_1, x_2 \dots x_n) &= \frac{1}{|G|} \sum_{g \in G} x_1^{c_1(g)} x_2^{c_2(g)} \dots x_n^{c_n(g)} \\ &= \frac{1}{|G|} \sum_{g \in G} (-1)^{\sum_i c_i(g)(i-1)} z_1^{c_1(g)} z_2^{c_2(g)} \dots z_n^{c_n(g)} \\ &= \frac{1}{|G|} \sum_{g \in G} \mathrm{sgn}(g) z_1^{c_1(g)} z_2^{c_2(g)} \dots z_n^{c_n(g)} \end{aligned}$$

where

$$\mathrm{sgn}(g) = \begin{cases} 1 & \text{if } g \text{ is an even permutation,} \\ -1 & \text{if } g \text{ is an odd permutation.} \end{cases}$$

Now, it is easy to see that

$$\begin{aligned} P_G(x_1, x_2 \dots x_n) + P_G(z_1, z_2 \dots z_n) &= 2 \times \frac{1}{|G|} \sum_{g \in H} z_1^{c_1(g)} z_2^{c_2(g)} \dots z_n^{c_n(g)} \\ &= \frac{1}{|H|} \sum_{g \in H} z_1^{c_1(g)} z_2^{c_2(g)} \dots z_n^{c_n(g)} \\ &= P_H(z_1, z_2 \dots z_n) \end{aligned}$$

□

So, cycle index polynomial at any point for the alternating group can be computed by computing the cycle index polynomial for the symmetric group at two points.

3 Another Approach

The problem of counting the number of matchings in a graph is also known to be $\#P$-complete. Another version of this problem is to find the sum of weights of all matchings of a weighted graph, where weight of a matching is the product of weights of edges in the matching. In the special case, when the graph is planar, the problem is easy and known to be in class NC. Now, computing the sum of weights of all matchings of a weighted graph and computing cycle index polynomial of a permutation group can be reduced to each other. So, the idea is to see for which groups the cycle index problem reduces to the matching problem with the planar graph case. For those groups computing cycle index polynomial will be easy.

For example consider the graph G_1 with vertex set $V = \{v_1, v_2 \dots v_{2n}\}$, and edge set $E = \{(v_i, v_{n+i}) | 1 \leq i \leq n\}$, with all the weights z_1. It is easy to see that computing cycle index polynomial for the trivial group reduces to the matching problem for G_1.

However the reduction does not look easy for any nontrivial group even in very simple cases. And any such nontrivial groups could not be found.

4 Acknowledgements

I would like to sincerely thank Prof. Piyush P. Kurur, for his constant encouragement and guidance throughout this work.

References

[1] Mark Jerrum, *Computational Pólya Theory*, In Surveys in combinatorics (1995), 103-118.

[2] A.K. Lal, *Lecture Notes on Discrete Mathematics*, available at `http://home.iitk.ac.in/~arlal/book/mth202.pdf`

[3] Peter J. Cameron, *Notes on Counting*, available at `http://www.maths.qmw.ac.uk/~pjc/notes/counting.pdf`