QFT Seminar - The Symmetric Group S_n

Zhao Yang Cai - 44092139
zhao.cai@uqconnect.edu.au

August 11, 2018

In this talk, we will place our focus on discussing the symmetric group S_n. The intent is to offer a basic introduction to the topic through this discussion of cycle structure (cycle notation and cycle types), partitions and conjugacy classes. A geometric analogue of the symmetric group will also be given through the consideration of reflection groups.

Further, we also relate symmetric groups to the idea of reflections groups. A key result in this section will be the fact that symmetric groups in fact arise from a Weyl group of type A.

Further, we will also discuss the relation of the symmetric group S_n to the braid group B_n; in particular their structural similarities will be the topic of our discussion.

Preliminaries

Definition 0.1. Let G be a group and S a non-empty subset of G. A *word* formed from S is either the identity element, or the finite product

$$\prod_{i=1}^{n} s_i^{n_i}, \quad s_i \in S, \quad n_i \in \mathbb{Z}, \quad m \geq 0,$$

where s_i are referred to as *letters*.

s

Definition 0.2. A **transposition** is an exchange of two elements of an ordered list with all others staying the same. That is, it is the permutation of two elements. It is often denoted (i, j), which means that i and j are swapped. Given a sequence of letters $1, \cdots i, \cdots, j, \cdots, n$ applying the

As an example, swapping 1 and 2 in 123 gives 213, and is a transposition. More generally, given a sequence of letters $1, \cdots i, \cdots, j, \cdots, n$ applying the transposition (i, j) swaps the positions of i and j to give $1, \cdots, j, \cdots, i, \cdots, n$.

Definition 0.3. An *adjacent transposition* is a transposition of the form $(i, i+1)$.

As an example, of this say, we have a sequence of numbers 1,2,3,4,5. Then,

$$(12), (23), (34), (45)$$

are its adjacent transpositions.

An Introduction to the Symmetric Group

The *symmetric group* S_n is the group consisting of all bijections from the set of letters $\{1, \cdots, n\}$ to itself with identity 1. The elements $\pi \in S_n$ are known as *permutations*, and the identity element $1 \in S_n$ is the *identity permutation*.

In this case, the operation that the group defines is $\circ$, denoting composition. So for two permutations π and σ, we write

$$\pi \circ \sigma$$

to denote the composition of the permutations. However, it is typical to employ shorthand notation by erasing the $\circ$ symbol and simply writing $\pi\sigma$ - which gives us a word. By convention, we "multiply" the permutations from right to left. That is, if we have a permutation $\pi\sigma$, we will apply σ first, and follow that with π.

We may verify that S_n is indeed a group since it is clear that $\pi \circ \sigma \in S_n$, as the result that we get from applying two permutations is still a permutation. Further, it is clear that there exists an inverse element π^{-1} for every permutation π. In fact, as we will soon see, every element is its own involution.

Definition 0.4. The **symmetric group** is the group generated by transpositions given by

$$S_n := \langle s_1, \cdots, s_{n-1} : s_i s_{i+1} s_i = s_{i+1} s_i s_{i+1},\ s_i s_j = s_j s_i \text{ for } |i-j| > 1 \text{ ,and } s_i^2 = 1 \rangle$$

where the conditions listed on the right-hand side of the colon are referred to as *relations*, and s_i represents *adjacent transpositions*.

We will see how this work in later examples, after we go through the notations that we use to represent permutations.

Remark. *The first two relations in the symmetric group are known as the braid group relations. This will be important later when we discuss morphisms between the braid group and symmetric group.*

By the above definition, we note that very element of the symmetric group s_i is its own involution (by the third relation). As such, there is no need to worry about inverses like with other groups. Combinatorially, it is quite easy to understand property **(iii)**, since if a permutation is applied on a set of letters, followed by applying the same permutation once more, we attain the same word from before the permutation.

Cycle Structure

Cycle Notation

Another way through which we can represent a permutation is through the use of *cycle notation*. Given a letter $i \in \{1, \cdots, n\}$, it's quite clear that the letters $i, \Pi(i), \Pi^2(i), \cdots$ cannot all be distinct. As such, we take the first power p such that $\Pi^p(i) = i$, which gives us the following cycle.

$$(i\Pi(i)\Pi^2(i)\Pi^3(i)\cdots\Pi^{p-1})$$

In this notation, we have i going to $\Pi(i)$, $\Pi(i)$ goes to $\Pi^2(i)$, and so on until we have $\Pi^{p-1}(i)$ going to $\Pi(i)^p$, which equals i, thus starting the entire cycle again. In general, any element $\Pi \in S_n$ can be written in terms of disjoint cycles. That is,

$$(i_1, \cdots, i_l) \cdots (i_{m+1}, \cdots, i_n)$$

Using our example from before, we may write the permutation in cycle notation as

$$\Pi = (1, 3)(2),$$

since 1 goes to 3, which then goes back to 1. 2 simply goes to itself, and is thus represented as a separate cycle. Note that $(1, 3)$ and (2) are disjoint cycles, and their product defines Π. Note that permuting the letters within a cycle does not change the permutation. That is,

$$(1, 3)(2) = (3, 1)(2) = (2)(3, 1) = (2)(1, 3)$$

In this case, the cycle (2) is called a *fixed point*, since it simply maps to itself. In general, any 1-cycle is called a *fixed point*.

An algorithmic approach to determing a cycle for a permutation is to pick a single element in the cycle containing i and interating this process until all members $\{1, \cdots, n\}$. A k-cycle, or cycle of *length* k is a cycle of k elements. For instance, our above example contains a 2-cycle and a 1-cycle.

Cycle Type

Now, the *cycle type*, or simply the *type* is an expression of the form

$$(1^{m_1}, 2^{m_2}, \cdots, n^{m_n})$$

where m_k is the number of cycles of length k in Π. Our above permutation thus has cycle type

$$(1^1, 2^1, 3^0)$$

Another way of representing the cycle type is through a *partition*, which is a sequence

$$\lambda = (\lambda_1, \cdots, \lambda_\ell)$$

where λ_i are a weakly decreasing sequence; that is,

$$\lambda_1 \leq \lambda_2 \leq \cdots \leq \lambda_\ell$$

and

$$\sum_{i=1}^{\ell} \lambda_i = n$$

As such, k would be repeated m_k times in the partition of the cycle type of Π. Using our above example, the partition would then be

$$(2, 1)$$

Example: S_2

The case of S_2 is a bit of a boring example, since it is simply given by

$$S_2 = \langle s_1 \rangle$$

and the only elements of the group are $\{\varepsilon, s_1\}$. The only possible cycle is the 2-cycle

$$\Pi = (1, 2)$$

which gives us the cycle type

$$(1^0, 2^1)$$

and the partition

$$(2)$$

Example: S_5

Consider $\pi \in S_5$ defined by

$$\pi(1) = 2, \quad \pi(2) = 3, \quad \pi(3) = 1, \quad \pi(4) = 4, \quad \pi(5) = 5$$

In cycle notation, we have

$$(1, 2, 3)(4)(5)$$

We note that there is one 3-cycle, and two fixed points. As such, our cycle type is

$$(1^2, 2^0, 3^1, 4^0, 5^0)$$

In our partition, 1 will be repeated 2 times, corresponding to the two fixed points in our cycle, and 3 will be repeated once, corresponding to the one 3-cycle. We order this in the form of a weakly decreasing sequence, as required, giving us

$$(3, 1, 1)$$

Conjugates and Conjugacy Classes

In any group G, elements g and h are *conjugates* if

$$g = khk^{-1}$$

for some $k \in G$. In fact, we may define an equivalence relation $\sim$ on G by $g \sim h$ if g and h are conjugate in G.

Proposition 1. *Let G be a group, and define the relation $\sim$ on G by $g \sim h$ if g and h are conjugate in G. Then, $\sim$ is an equivalence relation on G.*

Proof. We need to check that $\sim$ satisfies the properties of an equivalence relation. It is clear that $g \sim g$ since $ege^{-1} = g$ For $h, g \in G$ such that $xgx^{-1} = h$, we may re-arrange this to immediately obtain, $g = x^{-1}hx$. Then, we let $y = x^{-1}$ and so $g = yhy^{-1}$, and we have $h \sim g$. Now, let $g \sim h$ and $h \sim k$ for $g, h, k \in G$ and $y, z \in G$ such that $ygy^{-1} = h$ and $zhz^{-1} = k$. Then, $zygy^{-1}z^{-1} = (zy)g(zy)^{-1} = k$. And since $zy \in G$ by the closure of G, we have that $g \sim k$. Thus, $\sim$ is an equivalence relation.

□

As such, we may define an equivalence class on g, known as the *conjugacy class of* g. We denote this by K_g, and write

$$K_g = \{kgk^{-1} : k \in G\}$$

We note that the distinct conjugacy classes partition G. Note especially that this partition is a *set* partition, as opposed to *integer* partitions described before. That is to say, the conjugacy class K_g is characterised by the cycle type, and the cycle types are parametrised by set partitions of size n.

Conjugacy Classes of Symmetric Groups

Let us now determine the conjugacy class of the symmetric group S_n.

Lemma 1. *Let $\alpha, \tau \in S_n$, where α is the k-cycle $(a_1, a_2, \cdots, a_k)$. Then,*

$$\tau\alpha\tau^{-1} = (\tau(a_1), \cdots, \tau(a_k))$$

Proof. Consider $\tau(a_i)$ such that $1 \leq i \leq k$. Then we have that $\tau^{-1}\tau(a_i) = a_i$ and $\alpha(a_i) = a_{i+1 \mod k}$. We have now that $(\tau\alpha\tau^{-1})(\tau(a_i) = \tau(a_{i+1 \mod k})$. Now, consider any $j \in \{1, \cdots, n\}$, but such that $j \neq a_i$ for any i. Then, $\alpha(j) = j$ since j is not in the k-cycle defining α. So, $\tau\alpha\tau^{-1}(\tau(j)) = \tau(j)$. So, what we see here is that $\tau\alpha\tau^{-1}$ fixes any number that is not of the form $\tau(a_i)$, which gives us

$$\tau\alpha\tau^{-1} = (\tau(a_1), \cdots, \tau(a_k))$$

□

Theorem 0.1. *The conjugacy classes of any S_n are determined by cycle type. That is, if σ has a cycle type $(1^{m_1}, \cdots, n^{m_n})$, then any conjugate of σ has cycle type $(1^{m_1}, \cdots, n^{m_n})$. And, if ρ is any other element of S_n with the same cycle type, then σ is conjugate to ρ :.*

Proof. Suppose that σ has cycle type $(\lambda_1 \cdots \lambda_\ell)$, so that σ can be written as a product of disjoint cycles $\sigma = \alpha_1, \cdots, \alpha_\ell$, where α_i denotes a λ_i-cycle. Now, let $\tau \in S_n$; then, we have

$$\tau\sigma\tau^{-1} = \tau\alpha_1 \cdots \alpha_\ell\tau^{-1} = (\tau\alpha_1\tau^{-1})(\tau(\alpha_2\tau^{-1}) \cdots (\tau\alpha_\ell\tau^{-1})$$

Then, for each $1 \leq i \leq n$, we have from **Lemma 1** that $\tau\alpha_i\tau^{-1}$ is also a λ_i-cycle. As such, for any $i, j \in \{1, 2, \cdots, \ell\}$ such that $i \neq j$, we have that α_i and α_j are disjoint, and so $\tau\alpha_i\tau^{-1}$ and $\tau\alpha_j\tau^{-1}$ must also be disjoint since τ is an bijective function. As such, the above product given by $\tau\sigma\tau^{-1}$ is written as a product of disjoint cycles. As such, any conjugate of σ has cycle type $(\lambda_1 \cdots \lambda_\ell)$.

Now, let $\sigma, \rho \in S_n$ both be of cycle type $(\lambda_1 \cdots \lambda_\ell)$. We will show that σ and ρ are conjugate. Let σ and τ be written as disjoint cycles as

$$\sigma = \alpha_1 \cdots \alpha_\ell \quad \text{and} \quad \rho = \beta_1 \cdots \beta_\ell$$

where α_i and β_i are λ_i-cycles. For each i, let us write

$$\alpha_i = (a_{i\lambda_1} \cdots a_{i\lambda_\ell}) \quad \text{and} \quad \beta_i = (b_{i1} \cdots b_{in^{m_n}})$$

Now define τ by $\tau(a_{ij}) = b_{ij}$ where $1 \leq i \leq n$ and $\lambda_1 \leq j \leq \lambda_\ell$. From **Lemma 1**, we then have that

$$\tau\alpha_i\tau^{-1} = \beta_i$$

, and thus

$$\tau\sigma\tau^{-1} = (\tau\alpha_1\tau^{-1})\cdots(\tau\alpha_\ell\tau^{-1}) = \beta_1\cdots\beta_\ell = \rho$$

□

Root Systems

We work over an Euclidean space E; that is, a finite dimensional vector space over $\mathbb{R}$ endowed with a positive definite symmetric bilinear form (α, β).

Geometrically, a reflection in the space E sends any vector α orthogonal to a hyperplane to its negative. To each vector α is associated a *reflecting hyperplane* $P_\alpha := \{\beta \in E : (\beta, \alpha) = 0\}$ From this, we may write down an explicit equation for the reflection:

$$\sigma_\alpha(\beta) = \beta - \frac{2(\beta,\alpha)}{(\alpha,\alpha)}\alpha$$

Definition 0.5. A subset Φ of the Euclidean space E is called a *root system* if the following axioms are satisfies:

(R1) Φ is finite, spans E and does not contain 0

(R2) If $\alpha \in \Phi$, the only multiples of α in Φ are $\pm\alpha$.

(R3) If $\alpha \in \Phi$, the reflection σ_α leaves Φ invariant.

(R4) If $\alpha, \beta \in \Phi$, then

$$\sigma_\alpha(\beta) = \beta - \frac{2(\beta,\alpha)}{(\alpha,\alpha)}\alpha \in \mathbb{Z}$$

Simple Roots

Definition 0.6. A subset Δ of Φ is called a *base* if

(B1) Δ is a basis of E.

(B2) Each root β can be written as

$$\beta = \sum_{\alpha\in\Delta} k_\alpha\alpha$$

with integral coefficients k_α all nonnegative or all nonpositive.

And the elements of Δ are known as the *simple roots*.

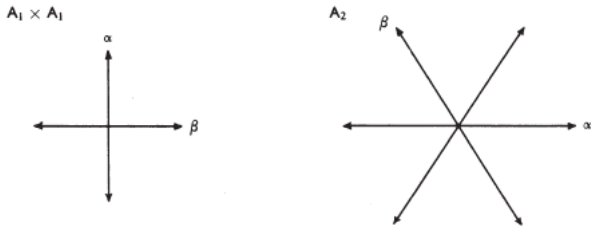
Weyl Group

Now, let Φ be a root system in E. Then, we denote by W the subgroup of $\mathrm{GL}_n(E)$ generated by the reflections σ_α with $\alpha \in \Phi$. Then, by (R3), W permutes the set Φ, which by (R1) is finite and spans E. This allows us to identify W as the subgroup of the symmetric group on Φ. W is called the *Weyl group* of Φ.

We may represent these root systems pictorially. For our purposes today, we will only consider root systems of type A. Let $\ell := \dim E$ denote the *rank* of the root system Φ. When $\ell \leq 2$, we can describe Φ by simply drawing a picture. By (R2), there is only one possibility for the case where $\ell = 1$, which we call A_1:

And indeed, this is a root system with Weyl group of order 2.

In the case of rank 2, there are much more opportunities. As aforementioned, we're most interested in considering Weyl groups of type A, because that's what is going to connect us to the symmetric group. As an example, consider the root systems $A_1 \times A_1$ and A_2.



S_n and the Braid Group B_n

Definition 0.7. The Artin Braid Group on n letters, B_n, is a finitely-generated group with generators $b_1, \cdots, b_{n-1}$ with

$$B_n := \langle b_1, \cdots, b_{n-1} : \text{relations} \rangle$$

satisfying the following relations:

$$b_i b_j = b_j b_i \quad \text{for} \quad |i-j| > 2, i, j \in \{1, \cdots, n-1\}$$

$$b_i b_{i+1} b_i = b_{i+1} b_i b_{i+1} \quad \text{for} \quad i \in \{1, \cdots, n-2\},$$

called the *braid relations*.

We define the braid group to be a group with the identity ε. As such, we have by definition that $B_1 = \{\varepsilon\}$ is a trivial group. The group B_2 is generated by a single generator b_1 and an empty set of relations.

Definition 0.8. A group is called a *free group* if no relation exists between its group generators other than the relationship between an element and its inverse.

As an example, the additive group of integers $(\mathbb{Z}, +)$ is free with generator 1 and its inverse, -1.

A simple non-abelian example of a free group would be the Galois field $GF(2)$ with the generating set $S = \{a, b\}$.

Lemma 2. *If $s_1, \cdots, s_{n-1}$ be elements of some group G satisfying the braid relations. Then, there is a unique group homomorphism $f : B_n \to G$ such that $s_i = f(b_i)$ for all $i = 1, 2, \cdots, n-1$.*

Proof. Let F_n be the free group generated by the set $\{b_1, \cdots, b_{n-1}\}$. There is a unique group homomorphism $\bar{f} : \bar{F_n} \to$ such that $\bar{f}(\sigma_i) = s_i$ for all $i = 1, 2, \cdots, n-1$. This homomorphism induces a group homomorphism $f : B_n \to G$ provided $\bar{f}(r^{-1}r') = \varepsilon$, or equivalently that $\bar{f}(r) = \bar{f}(r')$ for all braid relations $r = r'$. For the first braid relation we have:

$$\bar{f}(b_i b_j) = \bar{f}(b_i)\bar{f}(b_j) = s_i s_j = s_j s_i = \bar{f}(b_j)\bar{f}(b_i) = \bar{f}(b_j b_i)$$

And for the second braid relation, we have

$$\bar{f}(b_i b_{i+1} b_i) = s_i s_{i+1} s_i = s_{i+1} s_i s_{i+1} = \bar{f}(b_i b_{i+1} b_i),$$

as required.

□

From this lemma, we will prove that there is an epimorphism from the braid group B_n to S_n. But first, let us gain some intuition of why this should be the case.

In fact, if we discard the notion of strands twisting and crossing in the braid group and instead consider a "flat braid", then every braid of n strands determines a permutation on n elements.

A close inspection of both the braid group B_n and the symmetric group S_n shows us that both groups have the same amount of generators, and that the generators also of S_n also satisfy the braid relations, as well as the extra condition that $s_i^2 = 1$. This implies that the assignment $b_i \mapsto s_i$ is structure-preserving and thus defines a homomorphism

$$\varphi : B_n \to S_n, \quad b_i \mapsto s_i$$

And finally, since $\varphi(B_n)$ contains all the generators of S_n by our construction, φ is thus surjective. As such, φ is an epimorphism.

Now, we apply the previous lemma with $G = S_n$. We are able to do this as S_n satisfies the braid relations by definition. As we have already seen, an element of S_n is merely the permutation of the set $\{1, \cdots, n\}$. So, if we let $\{s_1, \cdots, s_{n-1}\}$ be the transpositions that we defined before, then the mapping

$$\varphi : B_n \to S_n, \quad b_i \to s_i$$

is a group homomorphism.

To justify the surjectivity of φ, let us consider another group homomorphism

$$\theta : G \to G'$$

where $\{g_1, \cdots g_d\}$ are generators of G and $\{\theta(g_1), \cdots, \theta(g_d)\}$ are generators for G'. Then, it follows that θ is a surjection since for each $g' \in G$, there exists a $g \in G$ such that

$$\theta(g) = g'$$

And so, by this construction, it follows that since b_i is a generator for B_n, and since $\varphi(b_i) = s_i$ is also a generator for S_n, we have that φ is surjective, and thus an epimorphism.

And in fact, it is possible to construct an isomorphism between the braid group B_n and the symmetric group S_n by imposing some extra structure on the braid group. Consider

$$\Theta : B_n/\langle s_i^2 \rangle \to S_n, \quad b_i\langle s_i^2 \rangle \mapsto s_i$$

It follows that $\ker\Theta = \langle s_i^2 \rangle$. And since the map φ has been shown to be a group epimorphism, it follows from the first isomorphism theorem that $B_n/\langle s_i^2 \rangle$ is isomorphic to S_n. That is, Θ is an isomorphism and thus

$$B_n/\langle s_i^2 \rangle \cong S_n$$

- Introduction to Lie Algebras and Representation Theory (chapter 3)
- number of conjugacy classes is equal to the number of partitions of n
- Schur polynomial for partitions
- Realise that S_n is the Weyl group of A_n
- build the A_n group system (yellow humphrey boi), use A_2 as an example
- define a root system in reflection groups part
- define simple roots
- define the weyl group W, and then show that $W \cong S_n$ in type A
- You get more semidirect products on type B and C
- include the signed permutation signs