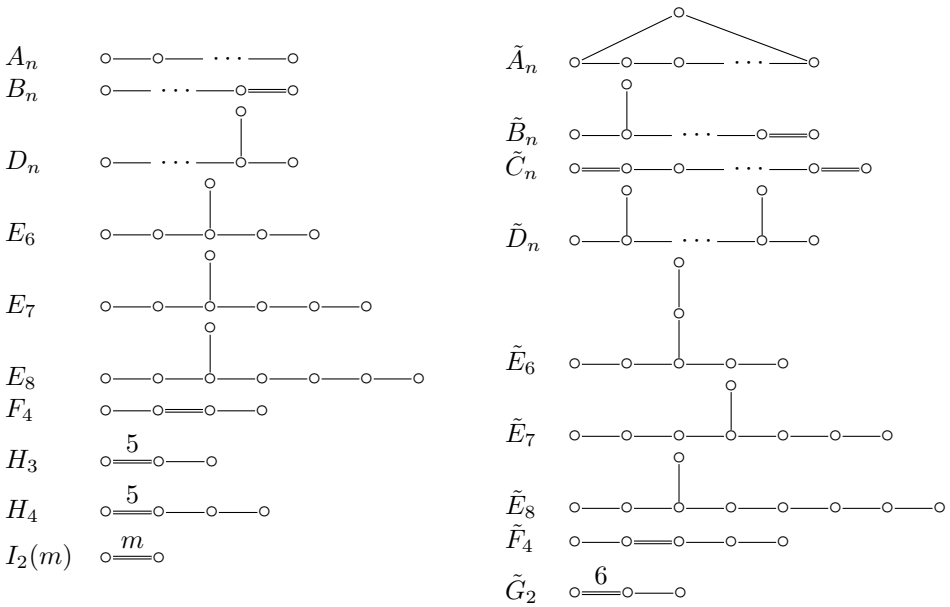
1 Last time: classification of finite Coxeter groups

Last time, we proved the following theorem, in two parts:

Theorem. The following Coxeter graphs correspond to the irreducible Coxeter groups whose geometric representations come with a positive definite or positive semidefinite bilinear form:



Among these, only the graphs in the left column correspond to finite Coxeter groups. The Coxeter graph of any irreducible finite Coxeter group is given by one of these.

Today, we introduce the *Iwahori-Hecke algebra* of a Coxeter system.

2 Iwahori-Hecke algebras

An Iwahori-Hecke algebra of a Coxeter system (W, S) will be a group ring RW for some commutative (usually, polynomial) ring R, but with a different multiplication than the usual one. We start with the most general construction, since the proofs are not much more difficult than in any particular case of interest.

Let A be a commutative ring with unit 1.

Let $\mathcal{H} = \mathcal{H}_{A,W}$ be the free A-module with basis $\{T_w : w \in W\}$. Here, each T_w is just a formal symbol used to distinguish basis elements of $\mathcal{H}$ from elements of W. Every element of $\mathcal{H}$ is a linear combination $h = \sum_{w \in W} h_w T_w$ with $h_w \in A$ and $h_w = 0$ for all but finitely many w. Alternatively, one can think of $h \in \mathcal{H}$ as a map $W \to A$ which sends all but finitely many elements to zero.

Choose elements $a_s, b_s \in A$ for $s \in S$ such that $a_s = a_t$ and $b_s = b_t$ if $s, t \in S$ are conjugate in W.

We'll spend the rest of today proving the following result:

Theorem. There is a unique associative A-algebra structure on $\mathcal{H}$ with unit T_1 and such that

$$T_s T_w = \begin{cases} T_{sw} & \text{if } \ell(sw) > \ell(w) \\ a_s T_w + b_s T_{sw} & \text{if } \ell(sw) < \ell(w) \end{cases} \qquad \text{if } s \in S \text{ and } w \in W. \tag{*}$$

We call this algebra a *generic (Hecke) algebra* of (W, S).

Example. If $a_s = 0$ and $b_s = 1$ for all $s \in S$ then $\mathcal{H} = AW$ is the usual group ring.

Example. Let $P = \mathbb{Z}[x_1, x_2, \ldots, x_n]$. For $s_i = (i, i+1) \in S_n$ and $f \in P$, let $s_i f = f(\cdots, x_{i+1}, x_i, \cdots)$ be the polynomial given by interchanging x_i and x_{i+1}. Define

$$\partial_i f = \tfrac{f - s_i f}{x_i - x_{i+1}} \qquad \text{for } i \in [n-1].$$

The keyword for ∂_i is *divided difference operator*.

Claim. $\partial_i f \in P$ for $f \in P$

Proof. It suffice to check this when $f = x_i^a x_{i+1}^b$ for $a, b \in \mathbb{N}$. Then we have $\partial_i f = \frac{x_i^a x_{i+1}^b - x_{i+1}^a x_i^b}{x_i - x_{i+1}}$. This is a polynomial since $\frac{x_i^c - x_{i+1}^c}{x_i - x_{i+1}} \in P$ for all $c \in \mathbb{N}$. □

So we can view ∂_i as a map $P \to P$. These operators satisfy the braid relations for S_n:

Claim. $\partial_i^2 = 0$

Proof. If $f \in P$ then $(x_i - x_{i+1})\partial_i(\partial_i f) = \frac{f - s_i f}{x_i - x_{i+1}} - \frac{s f_i - f}{x_{i+1} - x_i} = 0$. □

Claim. $\partial_i \partial_j = \partial_j \partial_i$ if $|i - j| > 1$, and $\partial_i \partial_{i+1} \partial_i = \partial_{i+1} \partial_i \partial_{i+1}$ for $i \in [n-1]$.

Proof. The first identity is easy to deduce from the fact that $s_i s_j f = s_j s_i f$. The second identity follows from a very doable, but slightly tedious calculation (do this yourself!). □

We conclude that if $w = s_{i_1} s_{i_2} \cdots s_{i_k}$ is a reduced expression for $w \in S_n$ then the operator on polynomials $\partial_w = \partial_{i_1} \partial_{i_2} \cdots \partial_{i_k}$ is independent of the choice of reduced expression. This follows since, from the homework, we know that if $w = s_{i_1} \cdots s_{i_k} = s_{j_1} \cdots s_{j_k}$ are both reduced expressions, then one expression can be obtained from the other by a sequence of braid transformations, which also transform $\partial_{i_1} \cdots \partial_{i_k}$ to $\partial_{j_1} \cdots \partial_{j_k}$ without changing the value of the corresponding map $P \to P$.

Let $\mathcal{D} = \mathbb{Z}\text{-span}\{\partial_w : w \in S_n\}$ where ∂_1 is the identity map $P \to P$.

Claim. $\mathcal{D}$ is a free $\mathbb{Z}$-module, that is, the operators ∂_w for $w \in S_n$ are linearly independent.

Proof. We won't prove this fact here: the idea is to locate a family of homogeneous polynomials f_w of degree $\ell(w)$ for $w \in S_n$, such that $\partial_u f_v = \delta_{uv}$ if $\ell(u) \geq \ell(v)$. You can check that $\partial_u f_v$ is always homogeneous of degree $\ell(v) - \ell(u)$ or zero, and deduce the desired linear independence from this. We will return to this family of operators in more detail in a few lectures! □

Claim. $\mathcal{D}$ is a $\mathbb{Z}$-algebra, i.e., a ring.

Proof. Let $u, v \in S_n$. If $\ell(uv) = \ell(u) + \ell(v)$ then $\partial_u \partial_v = \partial_{uv} \in \mathcal{D}$. If $\ell(uv) < \ell(u) + \ell(v)$ then use the exchange condition to deduce that $\partial_u \partial_v = 0 \in \mathcal{D}$. It follows that $\mathcal{D}$ is closed under composition of operators, which is always an associative product. □

Observe that if $s \in S$ and $w \in W$ then

$$\partial_s \partial_w = \begin{cases} \partial_{sw} & \text{if } \ell(sw) > \ell(w) \\ 0 & \text{if } \ell(sw) < \ell(w). \end{cases}$$

Thus $\mathcal{D} = \mathcal{H}$ is the generic algebra with $A = \mathbb{Z}$, $W = S_n$, and $a_s = b_s = 0$ for all $s \in S$.

We now return to the task of proving the main theorem.

Lemma. If an associative A-algebra structure on $\mathcal{H}$ exists in which T_1 is the unit and (*) holds, then

$$T_w T_s = \begin{cases} T_{ws} & \text{if } \ell(ws) > \ell(w) \\ a_s T_w + b_s T_{ws} & \text{if } \ell(ws) < \ell(w) \end{cases} \qquad \text{if } s \in S \text{ and } w \in W. \tag{**}$$

Proof. Let $t \in S$. Suppose $\ell(wt) > \ell(w)$. We proceed by induction on $\ell(w)$. The result is clear if $w = 1$. Assume $w \neq 1$ and let $s \in S$ be such that $\ell(sw) < \ell(w)$. Then $\ell(swt)$ ib bounded above by $\ell(sw) + 1 = \ell(w)$ and below by $\ell(wt) - 1 = \ell(w)$, so $\ell(swt) = \ell(w)$. It holds by induction that $T_{sw}T_t = T_{swt}$. Since $T_s T_{sw} = T_w$, we get

$$T_w T_t = T_s T_{sw} T_t = T_s T_{swt} = T_{wt}.$$

Conclude that $T_w T_t = T_{wt}$ if $\ell(wt) > \ell(w)$. If $\ell(wt) < \ell(w)$, then the identity $T_w T_t = a_t T_w + b_t T_{wt}$ follows since $T_w T_t = T_{wt} T_t T_t = T_{wt}(a_t T_t + b_t T_1)$. □

Lemma. Assume there is an associative A-algebra structure on $\mathcal{H}$ with $T_1 = 1$ and $T_s T_w = T_{sw}$ for $s \in S$ and $w \in W$ with $\ell(sw) > \ell(w)$. The the following are then equivalent:

1. $T_s T_w = a_s T_w + b_s T_{sw}$ for $s \in S$ and $w \in W$ with $\ell(sw) < \ell(w)$.
2. $T_s^2 = a_s T_s + b_s T_1$ for $s \in S$.

Moreover, if these conditions hold then $T_w = T_{s_1} T_{s_2} \cdots T_{s_n}$ for any reduced expression $w = s_1 s_2 \cdots s_n$.

Proof. Clearly (1) implies (2). If (2) holds then (1) follows since if $w \in W$ and $s \in S$ have $\ell(sw) < \ell(w)$, then $T_s T_w = T_s T_s T_{sw} = (a_s T_s + b_s T_1) T_{sw} = a_s T_w + b_s T_{sw}$. The last claim holds since if $w = s_1 s_2 \cdots s_n$ is a reduced expression then $0 < \ell(s_n) < \ell(s_{n-1}s_n) < \ell(s_{n-2}s_{n-1}s_n) < \cdots < \ell(s_1 s_2 \cdots s_n)$. □

Corollary. If a given generic algebra structure on $\mathcal{H}$ exists (for a fixed choice of parameters a_s and b_s), then it is unique.

Proof. Multiplication of any two elements of $\mathcal{H}$ is completely determined by the products $T_u T_v$ for $u, v \in W$, and we have $T_u T_v = T_{s_1} \cdots T_{s_n} T_{t_1} \cdots T_{t_m}$ for any reduced expressions $u = s_1 \cdots s_n$ and $v = t_1 \cdots t_m$. The value of this product in turn is completely determined by the axiom (*). □

With this observation in hand, we just need to prove the existence of our generic algebra structure on $\mathcal{H}$. For this, we take a slightly clever approach which one also encounters when working with the universal enveloping algebra of a Lie algebra.

Define $\mathrm{End}\mathcal{H}$ as the set of A-linear maps $\mathcal{H} \to \mathcal{H}$. $\mathrm{End}\mathcal{H}$ is already an A-algebra with respect to pointwise addition and composition of functions. It's hard to show that the product on $\mathcal{H}$ is associative directly. The idea is to instead locate a subalgebra of $\mathrm{End}\mathcal{H}$ isomorphic to $\mathcal{H}$ as an A-module, and then check that in this subalgebra (*) holds.

Define $\lambda_s \in \mathrm{End}\mathcal{H}$ as the linear map with $T_w \mapsto \begin{cases} T_{sw} & \text{if } \ell(sw) > \ell(w) \\ a_s T_w + b_s T_{sw} & \text{if } \ell(sw) < \ell(w) \end{cases}$.

Define $\rho_s \in \mathrm{End}\mathcal{H}$ as the linear map with $T_w \mapsto \begin{cases} T_{ws} & \text{if } \ell(ws) > \ell(w) \\ a_s T_w + b_s T_{ws} & \text{if } \ell(ws) < \ell(w) \end{cases}$.

The key property of these endomorphisms is that they commute. To show this, we need a technical lemma about Coxeter groups:

Lemma. Let $w \in W$ and $s, t \in S$. If $\ell(swt) = \ell(w)$ and $\ell(sw) = \ell(wt)$, then $sw = ws$.

Proof. Let $w = s_1 \cdots s_r$ be a reduced expression. There are two cases:

(a) Suppose $\ell(sw) > \ell(w)$.

Then $\ell(w) = \ell((sw)t) < \ell(sw)$ so the exchange condition implies that $sw = w't$ where w' is either w or $ss_1 \cdots \widehat{s_i} \cdots s_r$ for some i. The second case would imply that $w = s(sw) = s_1 \cdots \widehat{s_i} \cdots s_r t$ so $wt = s_1 \cdots \widehat{s_i} \cdots s_r t < w$, contradicting the fact that $\ell(wt) = \ell(sw) > \ell(w)$. Therefore $sw = wt$.

(b) Suppose $\ell(sw) < \ell(w) = \ell(s(sw))$.

Applying (a) with sw in place of w gives $s(sw) = (sw)t$ so again $sw = wt$.

□

Proposition. For all $s, t \in S$, it holds that $\lambda_s \rho_t = \rho_t \lambda_s \in \mathrm{End}\mathcal{H}$.

Proof. This is the most difficult part of the proof of the main theorem, and reduces mostly to a rather long, technical calculation.

Fix $w \in W$. We will compute $\lambda_s(\rho_t(T_w))$ and $\rho_t(\lambda_s(T_w))$ and show that in either case we get the same thing. There are six (!) cases according to the relative lengths of w, sw, wt, and swt. This looks a little intimidating at first, but (*) and (**) will let us compute each case explicitly, and then lemma will let us handle any ambiguities.

1. If $\ell(w) > \ell(wt) = \ell(sw) < \ell(swt)$ then $\lambda_s \rho_t(T_w) = \lambda_s(T_{wt}) = T_{swt} = \rho_t \lambda_s(T_w)$.
2. If $\ell(swt) < \ell(wt) = \ell(sw) < \ell(w)$ then

$$\begin{aligned} \lambda_s \rho_t T_w &= \lambda_s(a_t T_w + b_t T_{wt}) = a_t \lambda_s(T_w) + b_t \lambda_s(T_{wt}) \\ &= a_t(a_s T_w + b_s T_{sw}) + b_t(a_s T_{wt} + b_s T_{swt}) \\ &= a_s a_t T_w + a_t b_s T_{sw} + a_s b_t T_{wt} + b_s b_t T_{swt}. \end{aligned}$$

   It follows by symmetric that this is equal to $\rho_t \lambda_s(T_w)$.

3. If $\ell(wt) = \ell(sw) < \ell(swt) = \ell(w)$ then it follows by the lemma that $sw = wt$ so s and t are conjugate in W, hence $a_s = a_t$ and $b_s = b_t$, and so we compute that the expressions

$$\begin{aligned} \lambda_s \rho_t(T_w) &= a_s a_t T_w + a_t b_s T_{sw} + b_t T_{swt}, \\ \rho_t \lambda_s(T_w) &= a_s a_t T_w + a_s b_t T_{wt} + b_s T_{swt} \end{aligned}$$

   are equal.

4. If $\ell(wt) < \ell(w) = \ell(swt) < \ell(sw)$ then $\lambda_s \rho_t(T_w) = a_s T_{sw} + b_t T_{swt} = \rho_t \lambda_s(T_w)$.
5. If $\ell(sw) < \ell(w) = \ell(swt) < \ell(wt)$ then $\lambda_s \rho_t(T_w) = a_s T_{wt} + b_s T_{swt} = \rho_t \lambda_s(T_w)$.
6. Finally, if $\ell(w) = \ell(swt) < \ell(sw) = \ell(wt)$ then, using the lemma, we similarly compute

$$\lambda_s \rho_t(T_w) = a_s T_{wt} + b_s T_{swt} = a_t T_{sw} + b_t T_{swt} = \rho_t \lambda_s(T_w).$$

□

We can now prove the existence of part of the main theorem.

Proof of main theorem. Let $\mathcal{L} = \langle \lambda_s : s \in S \rangle \subset \mathrm{End}\mathcal{H}$ be the subalgebra generated by the left-translation operators λ_s. Define $\phi : \mathcal{L} \to \mathcal{H}$ as the clearly linear map with $\phi(\lambda) = \lambda(T_1)$.

This map is surjective since $\phi(\lambda_{s_1} \cdots \lambda_{s_n}) = T_{s_1} \cdots T_{s_n} = T_w$ for any reduced expression $w = s_1 \cdots s_n$.

To show that ϕ is injective, suppose $\phi(\lambda) = 0$ for some $\lambda \in \mathcal{L}$. We want to show that $\lambda = 0$. For this it suffices to show that $\lambda(T_w) = 0$ for all $w \in W$. This holds by definition for $w = 1$.

If $w \neq 1$, let $t \in S$ be such that $\ell(wt) < \ell(w)$. Then

$$\lambda(T_w) = \lambda(T_{(wt)t}) = \lambda(\rho_t(T_{wt})) = \rho_t(\lambda(T_{wt})) = 0$$

by induction, using the preceding proposition in the third equality.

Thus $\phi : \mathcal{L} \to \mathcal{H}$ is an isomorphism of A-modules. It follows that $\mathcal{L}$ is free with an A-basis given by $\lambda_w = \phi^{-1}(T_w) = \lambda_{s_1} \cdots \lambda_{s_n}$ for any reduced expression $w = s_1 \cdots s_n \in W$.

Let $s \in W$ and $w \in W$. If $\ell(sw) > \ell(w)$ then $\lambda_s \lambda_w = \lambda_{sw}$ by definition. Likewise, we have

$$\lambda_s^2(T_w) = \begin{cases} \lambda(T_{sw}) = a_s \lambda_s(T_w) + b_s T_w & \text{if } sw > w \\ \lambda_s(a_s T_w + b_s T_{sw}) = a_s \lambda_s(T_w) + b_s T_w & \text{if } sw < w. \end{cases}$$

Thus $\lambda_s^2 = a_s \lambda_s + b_s \lambda_1$. Setting $TT' = \phi\left(\phi^{-1}(T)\phi^{-1}(T')\right)$ for $T, T' \in \mathcal{H}$ defines an associative product on $\mathcal{H}$ since composition of functions is always associative, and what we have just shown proves that this product satisfies (*), which completes our proof. □