The construction of Hecke algebras associated to a Coxeter group

Bill Casselman
University of British Columbia
cass@math.ubc.ca

Hecke algebras associated to reductive groups over a finite field $\mathbb{F}_q$ were introduced in order to decompose representations of those groups induced from parabolic subgroups. They have subsequently become ubiquitous in representation theory, but often as algebras whose coefficients are polynomials, in which variables replace various powers of q.

The existence of these Hecke algebras with polynomial coefficients is not quite trivial. There are essentially two constructions in the literature. One originates in Exercices IV.22-25 of [Bourbaki:1968], and is apparently due originally to Jacques Tits. There are other accounts patterned after this argument, for example in [Humphreys:1990] and [Carter:1993]. My reaction to these is that they are clever but obscurely motivated—several tools used in the proof do not occur subsequently in the theory. There is a rather different, proof in [Eriksson:1994], which has much to be said for it. In this paper I offer a third, having something in common with each of these, but with what I consider to be a more direct approach. It was originally suggested in the course of writing programs for dealing with Hecke algebras.

I intend this paper to be largely self-contained, readable by novices. Before I present the proof of the general theorem, I recall the origins of the main theorem by looking at what happens for Hecke algebras of reductive groups defined over finite fields. Similar discussions are not difficult to find in the literature, but they are usually embedded in lengthier treatments. I include this section in order to motivate the later, more abstract, treatment.

Since many readers will be familiar only with finite Coxeter groups, I include a very brief summary of what parts of the subject I need.

Contents

1. The Hecke algebras of finite reductive groups

The standard reference for this section is Chapter 1 of [Carter:1972].

Let G be the group of $\mathbb{F}_q$-rational points on a Zariski-connected reductive group defined over $\mathbb{F}_q$. By a well known theorem of Serge Lang, it possesses a Borel subgroup B. A natural and classical question is, *how does the representation of G on the space $\mathbb{C}[B\backslash G]$ of $\mathbb{C}$-valued functions on the flag manifold $B\backslash G$ decompose into irreducible components?*

The first step in answering this is to describe the ring of operators on $I = \mathbb{C}[B\backslash G]$ commuting with G. Frobenius reciprocity tells us that

$$\mathrm{Hom}_G(I, I) \cong \mathrm{Hom}_B(I, \mathbb{C})\,.$$

The space on the right may be identified with functions in $\mathcal{H}(G//B)$, the space of complex-valued functions on G that are bi-invariant with respect to B. It is sometimes called the **Hecke algebra** of G with respect to B, for not very adequate historical reasons. Explicitly, F in $\mathcal{H}(G//B)$ corresponds to the operator L_F where

$$[L_F f](g) = \frac{1}{|B|} \sum_{x \in B\backslash G} F(x) f(x^{-1} g)\,.$$

This makes sense since the summand depends only on the image of x in $B\backslash G$.

The ring $\mathcal{H}(G//B)$ has convolution as its multiplication, and $L_{F_1F_2} = L_{F_1}L_{F_2}$. The characteristic function $\mathfrak{char}_B$ is the multiplicative identity. The following is immediate:

Lemma 1.1. *The map taking F to L_F is an identification of $\mathcal{H}(G//B)$ with the commutator of the right action of G in $\mathrm{End}\big(\mathbb{C}[B\backslash G]\big)$.*

If (π, V) is any representation of G, then $\mathcal{H}(G//B)$ acts on the subspace V^B of vectors fixed by B:

$$v \longmapsto \pi(F)v = \frac{1}{|B|}\sum_G F(g)\pi(g)v = \sum_{x\in G/B} F(x)\pi(x)v\,.$$

In the case above, π is the left-regular representation of G on itself.

Let T be a maximal torus contained in B, W the corresponding Weyl group $N_G(T)/T$. For w in W the double coset BwB is well defined, and the Bruhat decomposition asserts that G is the disjoint union of these as w ranges over W. If τ_w is the characteristic function $\mathfrak{char}_{BwB}$ of BwB, then the τ_w make up a basis of $\mathcal{H}(G//B)$. How can we compute the product $\tau_x\tau_y$ as a linear combination of the τ_w?

Lemma 1.2. *If BxB is the disjoint union of right cosets x_iB and ByB is that of the y_jB, then*

$$\tau_x\tau_y = \sum_{i,j} x_iy_j\,\mathfrak{char}_B\,.$$

Here what I mean by $xy\mathfrak{char}_B$ is $\mathfrak{char}_{xyB}$.

Proof. If have identified $\mathcal{H}(G//B)$ with a subalgebra of the ring of endomorphisms of $\mathbb{C}[B\backslash G]$, so it suffices to show this for operators L_{τ_x}, L_{τ_y}. But for any representation (π, V) of G we have for any v in V^B

$$\pi(\tau_x)\pi(\tau_y)v = \sum_i \pi(x_i)\pi(\tau_y)v = \sum_{i,j}\pi(x_i)\pi(y_j)v\,.$$ ∎

Lemma 1.3. *Suppose G to have semi-simple rank one. Let N be the unipotent radical of B, and let $q_G = |N|$. Then*

$$\tau_s^2 = (q_G - 1)\tau_s + q_G\tau_1\,.$$

Proof. The Weyl group in this case has two elements, 1 and s. Let w be a representative in $N_G(T)$ of the non-trivial element s. The double coset BwB factors uniquely as NwB, so by the previous Lemma we can write

$$\tau_s^2 = \sum\nolimits_{x,y\in N} xw\cdot yw\,\mathfrak{char}_B$$

If $y = 1$ the product wyw lies in B, and the terms with $y = 1$ therefore contribute $q_G\tau_1$ to the product. But if $y \neq 1$ we have $wyw = n_yw_*b_y$, with $n_y \in N$, $b_y \in B$. Proving this reduces to an explicit calculation in one of the two possible semi-simple groups of rank one over $\mathbb{F}_q$, either $\mathrm{SL}_2(\mathbb{F}_q)$ or $\mathrm{SU}_3(\mathbb{F}_q)$. For example in SL_2 with $c \neq 0$

$$\begin{bmatrix} 0 & 1\\ -1 & 0\end{bmatrix}\begin{bmatrix} 1 & c\\ 0 & 1\end{bmatrix}\begin{bmatrix} 0 & 1\\ -1 & 0\end{bmatrix} = \begin{bmatrix} -1 & 0\\ c & -1\end{bmatrix}$$
$$= \begin{bmatrix} 1 & -1/c\\ 0 & 1\end{bmatrix}\begin{bmatrix} 0 & -1/c\\ c & 0\end{bmatrix}\begin{bmatrix} 1 & -1/c\\ 0 & 1\end{bmatrix}.$$

The terms with $y \neq 1$ therefore contribute $(q_G - 1)\tau_s$. ∎

Let Δ be the set of simple roots α determined by B and T. If T_α is the kernel of α in T, its centralizer G_α in G is a reductive group of semi-simple rank one containing T. The Weyl group of T in G_α contains a non-trivial involution s_α. The group W is a Coxeter group, generated by the s_α.

A representation of w as a product of s_α is said to be **reduced** if it is of minimal length $\ell(w)$. This is the same as the number of positive roots taken into negative ones by w. I write $ws > w$ if $\ell(ws) = \ell(w) + 1$ and similarly $sw > w$ if $\ell(sw) > \ell(w)$.

Let $q_\alpha = |N_\alpha|$. It only depends on the W-orbit of α, or equivalently on the conjugacy class of s_α in W.

Proposition 1.4. *Suppose w to be in W, $s = s_\alpha$ one of the simple generators. Then*

$$\begin{aligned} \tau_w\tau_s &= \tau_{ws} && ws > w \\ &= (q_\alpha - 1)\tau_w + q_\alpha\tau_{ws} && ws < w \\ \tau_s\tau_w &= \tau_{sw} && sw > w \\ &= (q_\alpha - 1)\tau_w + q_\alpha\tau_{sw} && sw < w \end{aligned}$$

Since W is generated by the s_α, these formulas determine completely the multiplication in $\mathcal{H}(G//B)$.

I'll sketch the *Proof.* Half of these claims follow from the more general claim that

$$\tau_x\tau_y = \tau_{xy}$$

if $\ell(xy) = \ell(x) + \ell(y)$, which I prove first.

For each root λ let N_λ be the unipotent subgroup whose Lie algebra is the T-eigenspace $\mathfrak{g}_\lambda$, isomorphic to $\mathbb{F}_q$. Let N be the unipotent radical of B, which is isomorphic to the direct product

$$N = \prod_{\lambda>0} N_\lambda\,.$$

The product may be taken in any order, according to Lemme 3.3 of [Borel-Tits:1965]. Let $\overline{N}$ be the opposite subgroup, corresponding to negative roots. For any w in W we have the direct product factorization

$$N = (wNw^{-1} \cap N)(w\overline{N}w^{-1} \cap N)$$

with

$$\begin{aligned} wNw^{-1} \cap N &= \prod_{\substack{\lambda>0 \\ w^{-1}\lambda>0}} N_\lambda \\ w\overline{N}w^{-1} \cap N &= \prod_{\substack{\lambda>0 \\ w^{-1}\lambda<0}} N_\lambda \\ &= N_w \quad \text{(say)}\,. \end{aligned}$$

Since $N/(wNw^{-1} \cap N) \cong N_w$, we now have the very explicit formula

$$\tau_w = \sum_{n\in N_w} nw\,\mathfrak{char}_B\,.$$

Let Λ_w be the set of all positive roots λ such that $w^{-1}\lambda < 0$. If $\ell(xy) = \ell(x) + \ell(y)$ then

$$\Lambda_{xy} = x\Lambda_y \sqcup \Lambda_y$$

so the product map is a bijection of $N_x \times xN_yx^{-1}$ with N_{xy}. The number of roots in Λ_w is the same as the length of w^{-1}. But then

$$\tau_x\tau_y = \bigsqcup_{N_x\times N_y} (n_x x)(n_y y)B = \bigsqcup_{N_x\times N_y} (n_x)\,(xn_yx^{-1})\,xy)B = \bigsqcup_{N_{xy}} nxyB = \tau_{xy}$$

which proves the first assertion in the Proposition.

It remains to compute τ_{ws} when $ws < w$. If $ws < w$ then $w = ws{\cdot}s$ with $\ell(w) = \ell(ws) + 1$, so by the first part

$$\begin{aligned} T_w T_s &= (T_{ws} T_s) T_s \\ &= \tau_{ws} \tau_s^2 \\ \tau_s \tau_w &= \tau_s (\tau_s \tau_{ws}) \\ &= \tau_s^2 \tau_{ws} \end{aligned}$$

so both formulas we want follow from the single equation

$$\tau_s^2 = (q_\alpha - 1)\tau_s + q_\alpha \tau_1 \,,$$

which is Lemma 1.3. ∎

The use of associativity here in setting $(\tau_{ws}\tau_s)\tau_s = \tau_{ws}(\tau_s\tau_s)$ will be significant later on.

Knowing the structure of the Hecke algebra $\mathcal{H}(G/\!/B)$ is only a first basic step. Understanding the decomposition of $\mathbb{C}[B\backslash G]$ as a representation of G requires much more, eventually the theory of [Kazhdan-Lusztig:1979]. Similar algebras, called Iwahori-Hecke algebras, arise in the theory of unramified representations of a $\mathfrak{p}$-adic reductive group. For these, affine Weyl groups replace W.

In the theory of Kazhdan and Lusztig, as well as in answering other questions in representation theory, it is important to know that the prime powers q_α in the definition of the Hecke algebra may be replaced by variables. This is not so surprising, since the formulas for multiplication are polynomials in the q_α that do not depend on the particular value of q but only on the root structure of G. It ought not to be too surprising, either, that the Hecke algebras may also be defined for Kac-Moody groups or, in other words, crystallographic Coxeter groups. What is really remarkable is that a Hecke algebra may be defined for any Coxeter group, even the ones like H_3 or H_4 (the symmetry groups of the regular icosahedron and its four-dimensional analogue) that are not crystallographic and do not correspond to any algebraic group. This is the simplest example of the general rule that arbitrary Coxeter groups deserve to be treated as nicely as crystallographc ones. A more complicated one is that Kazhdan-Lusztig polynomials may be defined for all Coxeter groups, and truly astonishing is the conjecture that they always have non-negative coefficients.

The rest of this paper will present a new proof of the construction of the polynomial Hecke algebras for an arbitrary Coxeter group.

2. Coxeter groups

The standard references for this section are [Humphreys:1990] and [Bourbaki:1968].

DEFINITION. Suppose S to be any finite set. A Coxeter matrix indexed by S is a symmetric matrix $M = (m_{s,t})$ with entries in $\{1, 2, 3, \ldots, \infty\}$ such that

(a) $m_{s,s} = 1$;
(b) $m_{s,t} \geq 2$ if $s \neq t$.

The Coxeter group W defined by these data is that with involutive generators in S and relations

$$s^2 = 1, \qquad st\ldots = ts\ldots \quad (m_{s,t} \text{ terms on each side if } m_{s,t} < \infty.)$$

This last is called a **braid relation**. These relations imply, and are implied by, the relations

$$(st)^{m_{s,t}} = 1$$

for all s, t.

GEOMETRIC REALIZATION. Let (α_s) be a basis of the vector space $V = \mathbb{R}^S$. Define on it an inner product:

$$\alpha_s \bullet \alpha_t = -2\cos(\pi/m_{s,t}) \,.$$

In particular, $\alpha_s \bullet \alpha_s = 1$, and for $s \neq t$ we have $\alpha_s \bullet \alpha_t \leq 0$. For each s in S define the linear transformation of V:

$$r_s\colon\ v \longmapsto v - 2(\alpha_s \bullet v)\alpha_s\,.$$

It is an orthogonal reflection, and the map $s \mapsto r_s$ determines a homomorphism from W to $\mathrm{GL}(V)$. Let

$$\begin{aligned} C &= \{v \in V \mid \alpha_s \bullet v > 0\} \\ \mathcal{C} &= \text{ the interior of the union of the transforms } \{w\overline{C} \mid w \in W\} \end{aligned}$$

Then W embeds into $\mathrm{GL}(V)$ and acts discretely on $\mathcal{C}$, which is a convex cone in V. (It is called the Tits cone, although it seems to have been independently discovered by Vinberg.) The closure $\overline{C}$ is a strict fundamental domain for the action of W on $\mathcal{C}$.

If W is finite, then $\mathcal{C}$ is all of V, but otherwise it is a proper subset. If W is an affine Weyl group, it is an open half-space. Otherwise, it is an acute cone.

The α_s are the simple roots of this realization of W, and the other roots λ are the transforms of these by elements of W. The transforms of C by elements of W make up the complement in $\mathcal{C}$ of the root hyperplanes $\lambda \bullet v = 0$.

EXCHANGE CONDITION. The fundamental relation between geometry and the combinatorics of W is that $sw > w$ if and only if C and wC lie in the half-plane $\alpha_s \bullet v > 0$. It follows easily from this that if w has the reduced expression

$$w = s_1 \dots s_n$$

and $sw < w$, then for some k

$$sw = s_1 \dots s_{k-1}\widehat{s}_k s_{k+1} \dots s_n\,.$$

This is the *Exchange Condition*. (See §IV.1.5 of [Bourbaki:1968], Lemme 1.4 of [Tits:1968].) The simple geometric fact underlying this is that if $sw < w$ then the path of neighbouring chambers

$$C,\ sC, ss_1C,\ ss_1s_2C, \dots, swC$$

first crosses and later recrosses the hyperplane $\alpha_s = 0$.

COSET REPRESENTATIVES. For this section, see §5.12 of [Humphreys:1990].

Given any subset $T \subseteq S$, let W_T be the subgroup generated by the s in T. It, too, is a Coxeter group, and cosets of $W_T\backslash W$ have special representatives in

$$[W_T\backslash W] = \{w \in W \mid tw > w \text{ for all } t \in T\}\,.$$

Every w in W may be written uniquely as $w_T w^T$ with $w_T \in W_T$, $w^T \in [W_T\backslash W]$, and $\ell(w) = \ell(w_T) + \ell(w^T)$. Similarly every double coset in $W_T\backslash W/W_U$ possesses an element w of minimal length such that $tw > w$ for all t in T, $wu > w$ for all u in U.

TITS' EQUIVALENCE THEOREM. According to the definition of a Coxeter group, two words in S give rise to the same element of W if and only if one of them can be obtained by a sequence of (a) deletion of a pair $s \circ s$; (b) insertion of a pair $s \circ s$; (3) replacement of one side of a braid relation inside a word by the other side. This criterion can be made somewhat more practical. The **descendants** of a word are all those obtained from it just by deletions and braid relations. Finding all descendants is a lengthy but finite process. The main result of [Tits:1968] is that two words are equivalent if and only their descendants overlap. This is discussed in §2.3.3 of [Abramenko-Brown:2009].

Since a reduced word is not equivalent to a shorter one, two reduced words give rise to the same group element if and only if one can be obtained from the other by a sequence of braid relations. This is proven directly in the course of the proof of Tits' proof in [Tits:1968]. This result does not lead to a practical algorithm for telling whether two elements of W, expressed as products from W, are the same are not, but nonetheless it ought to be considered one of the fundamental results about Coxeter groups.

There do exist very efficient algorithms for computing in Coxeter groups. The best ones are purely combinatorial, and are based on the main theorem of [Brink-Howlett:1994], which asserts that a Coxeter group is automatic.

3. The Hecke algebra of a Coxeter group

Let (W, S) be any Coxeter group, say with Coxeter matrix $(m_{s,t})$. Suppose assigned to each s in S a parameter q_s. This assignment will be called **consistent** if $q_s = q_t$ whenever s and t are conjugate in W. Consistency is relatively easy to check, because s and t will be conjugate in W if and only if they are conjugate in the dihedral group $W_{s,t}$ generated by them ([Bourbaki:1968], p. 12). More explicitly, they will be conjugate if and only if $m_{s,t}$ is odd.

The proof of the next result is based on a practical algorithm, which requires that every element of W be assigned a unique expression as a product of elements of S. There is one most frequently used, its `ShortLex` expression. Assume S to be ordered. The expression

$$w = s_1 s_2 \dots s_n$$

is said to be in `ShortLex` form if s_1 is the least s in S such that $sw < w$ and the expression $s_2 \dots s_n$ is the `ShortLex` form for $s_1 w$. Such an expression is as **short** as possible, and **lex**icographically least among reduced expressions for w. Every w can be represented uniquely by its `ShortLex` expression, so this offers a purely combinatorial way to represent elements of W in a computer program. Every strict subexpression of a `ShortLex` word is also a `ShortLex` word.

Theorem 3.1. *If $s \mapsto q_s$ is an assignment of parameters in a ring R, then there exists an associative algebra $\mathcal{H}(W, S)$ which is free over R with basis T_w, indexed by elements of W, and identity T_1, such that*

$$\begin{aligned} T_w T_s &= T_{ws} && ws > w \\ &= (q_s - 1)T_w + q_s T_{ws} && ws < w \\ T_s T_w &= T_{sw} && sw > w \\ &= (q_s - 1)T_w + q_s T_{sw} && sw < w \end{aligned}$$

if and only if the parameters are consistent. It is unique up to isomorphism.

Induction then implies

$$T_x T_y = T_{xy}$$

if $\ell(xy) = \ell(x) + \ell(y)$.

Proof. Necessity first. The elements s, t in S are conjugate in W if and only if $m_{s,t}$ is odd and hence

$$tw = ws \quad \left(w = (st)^{(m_{s,t}-1)/2}\right),$$

with $sw = wt > w$. But then $s(sw) = w = (wt)t$ so that assuming the formulas of the Theorem to be true

$$T_s T_{sw} = q_s T_w + (q_s - 1)T_{sw} = T_{wt} T_t = q_t T_w + (q_t - 1)T_{wt},$$

requiring $q_s = q_t$.

The more difficult half is sufficiency.

Let $\mathcal{H} = \mathcal{H}(W, S)$ be the free module over R with basis T_w ($w \in W$). Define a product on $\mathcal{H}$ by an inductive formula. First of all, let T_1 be the multiplicative identity. Next I define multiplication by T_s ($s \in S$) on the left by the formulas

$$T_s T_w = \begin{cases} T_{sw} & \text{if } sw > w \\ (q_s - 1)T_w + q_s T_{sw} & \text{otherwise.} \end{cases}$$

To define products $T_w T_x$ in general, I use a notion arising in computation with Coxeter groups.

Suppose x in W, with `ShortLex` expression $x = s_1 \dots s_n =$ (say) $s_1 y$. Define recursively

$$T_x T_w = T_{s_1}(T_y T_w).$$

This is consistent with the earlier definition since an element of S has exactly one reduced expression. We can unravel the induction to some extent:

$$T_x T_w = T_{s_1}(T_{s_2}(\dots(T_{s_n}T_w)\dots))\,.$$

This can be rephrased, since because strict subexpressions of a `ShortLex` expression are `ShortLex`:

Lemma 3.2. *If z has* `ShortLex` *expression $s_1 \dots s_n$ and*

$$x = s_1 \dots s_m, \quad y = s_{m+1} \dots s_n$$

then

$$T_z T_w = T_x(T_y T_w)\,.$$

The problem now is to show that *this product is associative*.

Lemma 3.3. *If $\ell(xy) = \ell(x) + \ell(y)$ then*

$$T_x T_y = T_{xy}\,.$$

Proof. By induction on $\ell(x)$. For $\ell(x) = 0$ it is trivial, and if $\ell(x) = 1$ then $x = s$, so it is a matter of definition.

It is straightforward even in general. Suppose x to have the `ShortLex` expression

$$x = s_1 s_2 \dots\ s_n = \text{ (say) } s_1 z\,.$$

Then by definition

$$T_x T_y = T_{s_1}(T_z T_y)$$

and by the induction assumption

$$T_{s_1}(T_z T_y) = T_{s_1} T_{zy} = T_{s_1 zy} = T_{xy}\,. \blacksquare$$

Lemma 3.4. *We have*

$$T_x T_s = \begin{cases} T_{xs} & \text{if } xs > x \\ (q_s - 1)T_x + q_s T_{xs} & \text{otherwise.} \end{cases}$$

Proof. If $\ell(x) = 0$ there is nothing to prove, and if $\ell(x) = 1$ it is a matter of definition. So assume $\ell(x) \geq 2$.

If $xs > x$ then $T_x T_s = T_{xs}$ by the previous Lemma. Otherwise let the `ShortLex` expression for x be $s_n \dots\ s_1$. The induction hypothesis is that the Lemma is true for y with $\ell(y) < \ell(x) = n$. Let m be least such that

$$s_m \dots\ s_1 s < s_m \dots\ s_1\,.$$

That is to say, if $u = s_{m-1} \dots\ s_1$ then $us > u$ but $s_m us < us$. By the Exchange Condition we have

$$s_m \dots\ s_1 s = s_{m-1} \dots\ s_1 s \text{ or } s_m us = u\,.$$

If $v = s_n \dots\ s_{m+1}$ then

$$x = v s_m u, \text{ so } xs = v s_m us = vu\,.$$

Because $us = s_m u$, the elements s and s_m are conjugate, hence $q_s = q_{s_m}$. At first I take $v = 1$, $x = s_m u$. Then because strict subexpressions of a `ShortLex` expression are `ShortLex`:

$$\begin{aligned}
T_x T_s &= T_{s_m u} T_s \\
&= T_{s_m s_{m-1} \dots s_1} T_s) && (u = s_{m-1} \dots s_1) \\
&= T_{s_m}(T_{s_{m-1}}(\dots(T_{s_1}T_s)\dots)) && \text{(definition)} \\
&= T_{s_m} T_{us} && \text{(Lemma 3.3)} \\
&= (q_{s_m} - 1)T_{s_m u} + q_{s_m} T_{s_m us} && \text{(definition)} \\
&= (q_{s_m} - 1)T_{s_m u} + q_{s_m} T_u && (s_m us = u) \\
&= (q_s - 1)T_{s_m u} + q_s T_u && (q_s = q_{s_m}) \\
&= (q_s - 1)T_x + q_s T_{xs}\,.
\end{aligned}$$

Now take v arbitrary. Then

$$\begin{aligned} T_x T_s &= T_{vs_m u} T_s \\ &= T_v (T_{s_m u} T_s) \quad \text{(by Lemma 3.2)} \\ &= T_v ((q_s - 1) T_{s_m u} + q_s T_u) \\ &= (q_s - 1) T_x + q_s T_{xs} \,. \end{aligned}$$

The last step is by Lemma 3.3, since the hypotheses imply that $\ell(vus) = \ell(v) + \ell(us)$ and $\ell(vu) = \ell(v) + \ell(u)$. □

The following is a special case of associativity, and the crux of the proof of associativity in general.

Lemma 3.5. *For s, t in S, w in W, $(T_s T_w) T_t = T_s (T_w T_t)$.*

Proof. For any u in S let $W_u = \{1, u\}$. The group W decomposes into a disjoint union of double cosets $W_s w W_t$, on each of which the product $W_s \times W_t$ acts by left and right multiplication. There are two kinds of cosets, according to what the isotropy group is. Suppose w to be of minimal length in the coset (as in [Bourbaki:1968], Exercice 3 of IV.1). In one case, the isotropy group is trivial, and the coset is $\{w < sw, wt < wst\}$. In the otehr, it has two elements and the coset is $\{w < sw = wt\}$.

Let λ_s be left multiplication by T_s, ρ_t right multiplication by T_t. Associativity means that λ_s and ρ_t commute. On $\{w, sw, wt, swt\}$ this is straightforward. On a double coset $\{w, sw = wt\}$ the calculation is also straightforward, using the consistency of the parameters and the previous lemma. □

From this to a full proof of associativity is a straightforward induction argument. □

Corollary 3.6. *For each pair s, t in S*

$$T_s T_t \ldots = T_t T_s \ldots \qquad (m_{s,t} \text{ terms on each side}) \,.$$

Proof. Immediate from Lemma 3.3 and the braid relations in W. □

4. Generators and relations

It is important in representation theory to know that the Hecke algebra is defined by the equations in Theorem 3.1.

Define now $H(W, S)$ to be the associative algebra defined by generators τ_s ($s \in S$) with relations

$$\begin{aligned} \tau_s^2 &= (q_s - 1)\tau_s + q_s \tau_1 \\ \tau_s \tau_t \ldots &= \tau_t \tau_s \ldots \qquad (m_{s,t} \text{ terms on each side}) \,. \end{aligned}$$

The map $\tau_s \mapsto T_s$ defines a homomorphism from $H(W, S)$ to $\mathcal{H}(W, S)$.

Theorem 4.1. *This homomorphism is an isomorphism of $H(W, S)$ with $\mathcal{H}(W, S)$.*

Proof. From Tits' result, we can derive an algorithm to express any product $\tau_{s_1} \ldots \tau_{s_n}$ as a linear combination of such products for which the sequence is `ShortLex`. First of all, we repeatedly apply braid relations to make a list of all products of the same length. If the product is reduced, then by Tits' theorem one of them will be the `ShortLex` expression. If the product is not reduced, then by Tits' theorem at least one of them will include a duplication $\tau_s \tau_s$, which may be reduced to a sum of two products of lower degree. So an induction argument will work. □

Tits' result does not give us a practical algorithm for finding a `ShortLex` expression, but of course here that doesn't matter.

Corollary 4.2. *If V is a vector space and we are given operators e_s for each s in S such that*

$$\begin{aligned} e_s^2 &= (q_s - 1) e_s + q_s I \\ e_s e_t \ldots &= e_t e_s \ldots \quad (m_{s,t} \text{ terms on each side}) \end{aligned}$$

then $T_s \mapsto e_s$ defines V as a module over $\mathcal{H}(W, S)$.

5. References

1. Armand Borel and Jacques Tits, 'Groupes réductifs', *Publications Mathématiques de lÍnstitut des Hautes Études Scientifiques* **27** | (1965), 55–150.

2. N. Bourbaki, Chapitres IV, V, and VI of **Groupes et algèbres de Lie**, Hermann, 1968.

3. Brigitte Brink and Robert Howlett, 'A finiteness property and an automatic structure for Coxeter groups', *Math. Ann.* **296** (1993), 179–190.

4. Ken Brown, **Buildings**, first edition, Springer, 1989. The second edition, appearing in 2008, was co-authored with Peter Abramenko.

5. Roger Carter, **Finite groups of Lie type**, Wiley, 1993.

6. Kimmo Eriksson, 'A combinatorial proof of the existence of the generic Hecke algebra and R-polynomials', *Mathematica Scandinavica* **75** (1994), 169–177.

7. James E. Humphreys, **Reflection groups and Coxeter groups**, Cambridge University Press, 1990.

8. David Kazhdan and George Lusztig, 'Representations of Coxeter groups and Hecke algebras', *Inventiones Mathematicae* **53** (1979), 165–184.

9. Jacques Tits, 'Le problème de mots dans les groupes de Coxeter', *Symposia Math.* **1** (1968), 175–185.