ON THE INJECTIVITY OF THE BRAID GROUP IN THE HECKE ALGEBRA

Gus I. Lehrer and Nanhua Xi.

Abstract. We show that the well known homomorphism from any Artin braid group to the Hecke algebra of the same type is injective for the universal Coxeter system and that the Burau representation is faithful for all finite Coxeter systems of rank two.

1. Introduction.

A Coxeter system (W, S) consists of a finite set S which generates the (possibly infinite) Coxeter group W subject to the following relations. For a subset of the pairs r, s of elements of S, there is a positive integer m_{rs} such that

(BR) $$rsr \cdots = srs \cdots \quad \text{,where both sides have } m_{rs} \text{ terms}$$

and secondly,

(Q) $$s^2 = 1 \quad \text{for any element} \quad s \in S$$

The *rank* of (W, S) is the cardinality of S. For each Coxeter system we have an associated generalised Artin braid group B_W and a Hecke algebra H_W over the ring $\mathbb{A} = \mathbb{R}[q, q^{-1}]$ of Laurent polynomials of the indeterminate q, which are defined as follows.

The Artin group B_W has generators $\{\sigma_s \mid s \in S\}$ which satisfy the braid relations (BR) above. The Hecke algebra $H_W = H_W(q)$ is generated as associative algebra by $\{T_s \mid s \in S\}$, subject to the relations (BR) and (Q*), the latter being the deformed quadratic relation

(Q*) $$(T_s - q)(T_s + q^{-1}) = 0 \qquad (s \in S)$$

1991 *Mathematics Subject Classification.* 20C08, 16A64, 20G05.

Key words and phrases. Hecke algebras, braid groups.

This work was carried out as part of the ARC funded project Group representations and cohomology of algebraic varieties.

N.X. was supported by the National Natural Science Foundation of China. N.X. also would like to thank the University of Sydney and Australian Research Council for financial support and hospitality during his visit there.

Typeset by $\mathcal{A}\mathcal{M}\mathcal{S}$-TEX

It is known that H_W is free as an $\mathbb{A}$ module, with basis $\{T_w \mid w \in w\}$, where, if $w \in W$ has reduced decomposition $w = s_1 s_2 \cdots s_\ell$, $(s_i \in S)$, then $T_w = T_{s_1} T_{s_2} \cdots T_{s_\ell}$. There is clearly a natural group homomorphism

$$\phi : B_W \longrightarrow H_W, \tag{1.1}$$

which takes σ_s to qT_s for $s \in S$. A natural and interesting (see, e.g. [Bi], [J], [Le]) question is whether this map is injective. For type A_2, it has been long known that the map is injective (see [Bi]), but for every other nontrivial case the question is still open. It is known that the Burau representation (to be defined shortly) is not injective for W of type A_n with $n \geq 4$ (see [B1, LP, Mo]). However even for type A_3, it is not known whether the map from the braid group to the Hecke algebra is injective.

When (W, S) is of finite type (i.e. W is finite), the braid group B_W has a "reduced Burau representation", described as follows. It is known that generically, i.e. over the quotient field $K \cong \mathbb{R}(q)$ of $\mathbb{A}$, the Hecke algebra $H_W(K) = H_W \otimes_{\mathbb{A}} K$ is isomorphic to the group algebra KW, and hence is a sum of two-sided ideals $H_W(K)_\lambda$, where λ runs over the irreducible KW modules. In particular, there is a surjection

$$\eta_\rho : H_W(K) \longrightarrow H_W(K)_\rho,$$

where ρ is the reflection representation of W. The reduced Burau representation of B_W is the composition

$$\psi = \eta_\rho \circ \phi. \tag{1.2}$$

In this short note we show that the map ψ (and therefore ϕ) is injective for all rank 2 cases.

The related (but weaker) question as to whether a braid group is linear (i.e. has a faithful finite dimensional linear representation) has been settled recently (see [B2, CW, D, K1, K2]) for W finite. In case W is crystallographic, it is shown in [D], that B_W has a faithful representation of degree equal to the number of positive roots.

2. The main theorem.

We shall prove

(2.1) Theorem. *Let (W, S) be a Coxeter system of rank 2. If W is finite, then the Burau representation ψ of B_W is faithful. In all cases, the homomorphism (1.1) from the braid group B_W to the Hecke algebra H_W is injective.*

Let $S = \{s, t\}$. Then (W, S) is determined by the integer $m = m_{st}$ of the relation (BR) above. We say $m = \infty$ if there is no such relation; in this case W is the infinite dihedral group, or the universal Coxeter group of rank 2.

The following result is useful, although we shall not be using its full force.

(2.2) Proposition.. *(i) For any positive integer n define the following elements of $\mathbb{A}_0 = \mathbb{Z}[q, q^{-1}]$: $\{n\}_q = \dfrac{q^n - (-q^{-1})^n}{q + q^{-1}}$ and $\alpha = q - q^{-1}$. Then*

$$\{n\}_q = \sum_{k \leq n-1,\ k \equiv n-1 (\mathrm{mod}\ 2)} b_{k,n} \alpha^k$$

where the $b_{k,n}$ are positive integers explicitly given as follows. If $n = 2m+1$ is odd and $k = 2r$ $(0 \leq r \leq k)$, then $b_{k,n} = \binom{m+r}{m-r}$. If $n = 2m+2$ is even and $k = 2r+1$ $(0 \leq r \leq k)$, then $b_{k,n} = \binom{m+r+1}{m-r}$.

(ii) Let T be one of the generators T_s of the Hecke algebra H_W. Then for any $n \in \mathbb{Z}$, we have

$$T^n = a_n + b_n T \tag{2.2.1}$$

where a_n and $b_n \in \mathbb{Z}[q, q^{-1}]$ are given given explicitly as follows. For $n \geq 1$, $a_n = \{n-1\}_q$ and $b_n = \{n\}_q$. For $n \leq -1$, $a_n = -\{-n+1\}_q$ and $b_n = \{-n\}_q$.

We omit the proof, which is an exercise in binomial identities.

(2.3) Proposition. *Let (W, S) be the "universal" Coxeter sysytem of any finite rank, i.e., assume that the set of relations (BR) is empty. Then the homomorphism (1.1) from the braid group B_W to the Hecke algebra H_W is injective.*

Proof. Any relation

$$T_{s_1}^{n_1} T_{s_2}^{n_2} T_{s_3}^{n_3} \cdots = q^{-\sum_i n_i}$$

translates, using (2.2)(ii) into

$$(a_{n_1} + b_{n_1} T_{s_1})(a_{n_2} + b_{n_2} T_{s_2})(a_{n_3} + b_{n_3} T_{s_3}) \cdots = q^{-\sum_i n_i}$$

Expressing the left side in the form $\sum_{w \in W} a_w T_w$, we see, since the expression $s_1 s_2 s_3 ...$ is reduced in W, that there is just one term with w of maximum length, and this term has coefficient $b_{n_1} b_{n_2} b_{n_3} ....$ It follows that $n_i = 0$ for all i. □

From now on we assume that $S = \{s, t\}$ and that the order of st is m. The case $m = \infty$ has just been dealt with and the case $m = 2$ of the theorem is trivial, although the construction of the Burau representation is different from that given below for $m \geq 3$.

We therefore assume henceforth that $m_{st} = m \neq 2, \infty$.

3. The reflection representation.

The reflection representation η_ρ of H_W may be realised as follows. Let M be the free $\mathbb{A}$-module with basis E_s, E_t. Define endomorphisms T_s, T_t of M by

$$T_s E_s = q E_s, \quad T_s E_t = -q^{-1} E_t + E_s,$$
$$T_t E_s = -q^{-1} E_s + 4\cos^2 \frac{\pi}{m} E_t, \quad T_t E_t = q E_t.$$

These equations (cf. [CIK, §8]) define an H-module structure on M. In matrix terms, T_s, T_t are represented respectively as left multiplication by the matrices

$$\begin{bmatrix} q & 1 \\ 0 & -q^{-1} \end{bmatrix}, \begin{bmatrix} -q^{-1} & 0 \\ c & q \end{bmatrix}, \tag{3.1}$$

where $c = 4\cos^2 \frac{\pi}{m}$.

The elements T_{ts} and T_{st} are then represented by the matrices

$$(3.2) \qquad \begin{bmatrix} -1 & -q^{-1} \\ cq & c-1 \end{bmatrix}, \begin{bmatrix} c-1 & q \\ -cq^{-1} & -1 \end{bmatrix},$$

which both have eigenvalues $\zeta^{\pm 1}$, where $\zeta = e^{\frac{2\pi i}{m}}$. Now by calculating the corresponding eigenvectors and using the equation

$$c = \zeta + \zeta^{-1} + 2 = \frac{(\zeta+1)^2}{\zeta},$$

one easily calculates the matrices which represent all elements of W. For any integer k write

$$\begin{aligned}[k]_\zeta &= \frac{\zeta^k - \zeta^{-k}}{\zeta - \zeta^{-1}} \\ &= \zeta^{k-1} + \zeta^{k-3} + \cdots + \zeta^{-(k-1)} \quad if \quad k \geq 0.\end{aligned}$$

(3.3) Lemma. *The matrices representing the various elements of W are given by:*

$$T_{ts}^k = \begin{bmatrix} -[k]_\zeta - [k-1]_\zeta & -q^{-1}[k]_\zeta \\ cq[k]_\zeta & [k]_\zeta + [k+1]_\zeta \end{bmatrix},$$

$$T_{st}^k = \begin{bmatrix} [k]_\zeta + [k+1]_\zeta & q[k]_\zeta \\ -cq^{-1}[k]_\zeta & -[k]_\zeta - [k-1]_\zeta \end{bmatrix},$$

$$T_s T_{ts}^k = \begin{bmatrix} q([k]_\zeta + [k+1]_\zeta) & [k+1]_\zeta \\ -c[k]_\zeta & -q^{-1}([k]_\zeta + [k+1]_\zeta) \end{bmatrix},$$

$$T_t T_{st}^k = \begin{bmatrix} -q^{-1}([k]_\zeta + [k+1]_\zeta) & -[k]_\zeta \\ c[k+1]_\zeta & q([k]_\zeta + [k+1]_\zeta) \end{bmatrix}.$$

Using (3.3) one sees easily that $T_{w_0}^2$ acts on M as the identity, where w_0 is the longest element of W. More specifically, the action of T_{w_0} is given by

$$(3.3.1) \qquad T_{w_0} = \begin{cases} \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} & if \quad m \text{ is even,} \\ \begin{bmatrix} 0 & -[k]_\zeta \\ c[k+1]_\zeta & 0 \end{bmatrix} & if \quad m = 2k+1. \end{cases}$$

For any element $w \in W$, define $L(w) = \{r \in S \mid \ell(rw) < \ell(w)\}$ and similarly for $R(w)$. Let $Y = W \setminus \{w_0, e\}$, where e is the identity element of W. For $w \in Y$, clearly $L(w)$ and $R(w)$ each consist of a single element, and we shall abuse notation by writing $L(w), R(w)$ for these elements.

(3.4) Lemma. *Let $w \in Y$. Then for $r \in S$,*

$$T_w E_r = f_s E_s + f_t E_t,$$

where $f_s, f_t \in \mathbb{A} = \mathbb{R}[q, q^{-1}]$ and for $r_1 \in S$, degree(f_{r_1}) ≤ 0 unless $r = R(w)$ and $r_1 = L(w)$, in which case $f_{r_1} = \lambda q +$ lower degree terms, where $\lambda > 0$.

Lemma (3.4) follows immediately from inspection of the matrices in Lemma (3.3).

(3.5) Corollary. *Let $w_1, w_2, \cdots, w_p$ be a sequence of elements of Y. Then for $r \in S$,*

$$T_{w_1} T_{w_2} \cdots T_{w_p} E_r = h_s E_s + h_t E_t,$$

where $h_s, h_t \in \mathbb{A} = \mathbb{R}[q, q^{-1}]$ and for $r_1 \in S$, degree$(h_{r_1}) \leq p - 1$ unless $r = R(w_p)$, $r_1 = L(w_1)$ and $L(w_i) = R(w_{i-1})$ for $i = 2, 3, \cdots, p$. In case these three conditions hold, $h_{r_1} = \alpha q^p +$ lower degree terms, where $\alpha > 0$.

This follows immediately by repeated application of Lemma (3.4).

4. Proof of the theorem.

We shall prove

(4.1) Proposition. *Let (W, S) be a Coxeter system of rank 2 with $m_{st} = m$ satisfying $3 \leq m < \infty$. Let M be the $\mathbb{A}-$space defined in §3 above and define the reduced Burau representation $\psi : B_W \longrightarrow GL(M)$ as in (1.2), with T_s, T_t acting as in §3 and $\psi(\sigma_s) = qT_s$, etc. Then ψ is injective.*

We begin with some reductions which apply whenever W is finite (and of arbitrary rank). Let B_W^+ be the braid monoid; this is the monoid generated by $\{\sigma_s,\ s \in S\}$, subject to the braid relations (BR). It is known (cf. [Mi, 3.2]) that B_W^+ embeds (injectively) in B_W and that there is a canonical injection, denoted here by $w \mapsto \sigma_w$, from W to B_W^+ whose image we denote by $\sigma(W)$. The elements of B_W^+ have a unique "normal decomposition" ([Mi, §4]) $\sigma = \sigma_{w_1} \sigma_{w_2} \cdots \sigma_{w_p}$, where $R(w_i) \supset L(w_{i+1})$ for $i = 1, 2, \cdots, p-1$. If w_0 is the longest element of W, write σ_0 for σ_{w_0}. Then σ_0^2 is central in B_W, and for any element $b \in B_W$, there is a power σ_0^N such that $\sigma_0^N b \in B_W^+$. From this one deduces that any element $b \in B_W$ may be written uniquely in the form $b = \sigma_1^{-1} \sigma_2$, where $\sigma_i \in B_W^+$ and the σ_i have no common left divisor in $\sigma(W)$.

Suppose that D is any B_W module. It follows from the above remarks that to prove D faithful, it suffices to prove that if $\sigma_1, \sigma_2 \in B_W^+$, then $\sigma_1 m = \sigma_2 m$ for all $m \in D$ implies that $\sigma_1 = \sigma_2$; in fact it suffices to show that σ_1, σ_2 have a non-trivial common left divisor in $\sigma(W)$.

Now consider the situation of (4.1), where $S = \{s, t\}$, W is finite of order $2m$, and $M = \langle E_s, E_t \rangle_{\mathbb{A}}$ is the reduced Burau representation, with σ_s, σ_t acting as qT_s, qT_t above.

(4.2) Lemma. *Let W and M be as just described. Suppose σ and τ are elements of B_W^+ such that for all $E \in M$, we have $\sigma E = \tau E$. Then either $\sigma = \tau = 1$ or σ and τ have a non-trivial common left divisor in $\sigma(W)$*

Proof. Let $\sigma = \sigma_{x_1} \sigma_{x_2} \cdots \sigma_{x_k}$ and $\tau = \sigma_{y_1} \sigma_{y_2} \cdots \sigma_{y_l}$ be the unique normal decompositions of σ and τ. First suppose that $x_j = w_0$ for some j; then the condition $R(x_i) \supset L(x_{i+1})$ implies that $x_1 = w_0$, and hence the result, unless $l = 0$. But if $l = 0$, then since det$\sigma_w = \pm q^{2\ell(w)}$, we have $k = 0$ and so $\sigma = \tau = 1$. Thus we may suppose that for all i, j, x_i and y_j are in $Y = W \setminus \{e, w_0\}$. But then by Corollary (3.5), if $\sigma(E_s + E_t) = h_s E_s + h_t E_t$, with $h_s, h_t \in \mathbb{A}$, the coefficient of E_r has greater degree if $r = L(x_1)$. Applying the same argument to the right side, we see that $L(x_1) = L(y_1)$ and the Lemma is proved. $\square$

Proposition 4.1 is immediate from the Lemma, since if $b \in B_W$ acts on M as the identity, then writing $b = \sigma^{-1} \tau$, where $\sigma, \tau \in B_W^+$ have no common left divisor in

$\sigma(W)$, we have the situation of Lemma 4.2, and deduce that $\sigma = \tau = 1$, whence $b = 1$. Theorem 2.1 is immediate.

Remarks: 1. Our basic lemma (3.4) is reminiscent of a property of the a-function introduced by Lusztig, see [L1-2].

2. Let (W, S) be as in Theorem 2.1. Let ϕ' be the map from B_W to H_W which takes σ_r to T_r for all $r \in S$ and let $\psi' = \eta_\rho \circ \phi'$. Then using (3.3.1), one sees that ψ' is not injective; but clearly ϕ' is injective whenever ϕ is injective. To see this, suppose $T_{s_1}^{n_1} T_{s_2}^{n_2} T_{s_3}^{n_3} \cdots = 1$. Substituting $T_s = q$, we see $\sum_i n_i = 0$, whence $(qT_{s_1})^{n_1} (qT_{s_2})^{n_2} (qT_{s_3})^{n_3} \cdots = 1$.

3. We believe that the analogue of Theorem 2.1 may be true for type A_3.

References

[B1] Bigelow, S., *The Burau representation is not faithful for $n = 5$,* Geometry and Topology **3** (1999), 397-404.

[B2] Bigelow, S., *Braid groups are linear,* Jour. Amer. Math. Soc. **14**, No. 2 (2001), 471-486.

[Bi] Birman, J., *Braids, links, and mapping class groups*, Ann. of Math. Studies, **82** , Princeton Univeristy Press, Princeton, N. J., 1974.

[CIK] Curtis, C. W.; Iwahori, N.; Kilmoyer, R. *Hecke algebras and characters of parabolic type of finite groups with (B, N)-pairs*, Inst. Hautes Études Sci. Publ. Math. **40** (1971), 81–116.

[CW] Cohen, A. J., and Wales, D. B., *Linearity of Artin groups of finite type,* preprint, ArXiv: math.GR/0010204.

[D] Digne, F. *On the linearity of Artin braid groups,* preprint, 2001.

[J] Jones, V.F.R., *Hecke algebra representations of braid groups and link polynomials*, Ann. of Math. (2) **126** (1987), no. 2, 335–388

[K1] Krammer, D., *The braid group B_4 is linear*, Invent. Math. **142** (2000), 451-486.

[K2] Krammer, D., *Braid groups are linear*, Preprint, 2000.

[Le] Lehrer, G. I. *A survey of Hecke algebras and the Artin braid groups*, Braids (Santa Cruz, CA, 1986), 365–385, Contemp. Math., **78**, Amer. Math. Soc., Providence, RI, 1988.

[LP] Long, D. D., and Paton, M., *The Burau representation is not faithful for $n \geq 6$,* Topology **32** (1993), No. 2, 439-447.

[L1] Lusztig,G., *Cells in affine Weyl groups*, in "Algebraic Groups and Related Topics", Advanced Studies in Pure Math., **6**, Kinokunia and North Holland, 1985, pp. 255-287 .

[L2] Lusztig,G., *Cells in affine weyl groups, II*, J. Alg. **109** (1987), 536-548.

[Mi] Michel J., *A note on words in braids monoids,* J. Alg. **215** (1999), 366-377.

[Mo] Moody, J. A., *The Burau representation of the braid group B_n is unfaithful for large n,* Bull. Amer. Math. Soc. (N. S.) **25** (1991), No. 2, 379-384.

School of Mathematics and Statistics, University of Sydney, NSW 2006, Australia

E-mail address: `gusl@maths.usyd.edu.au`

Institute of Mathematics, Chinese Academy of Sciences,Beijing 100080, China

E-mail address: `nanhua@math08.math.ac.cn`