Bulletin of the Institute of Mathematics
Academia Sinica (New Series)
Vol. **7** (2012), No. 3, pp. 323-354

HECKE ALGEBRAS AND INVOLUTIONS IN WEYL GROUPS

GEORGE LUSZTIG[1,a] AND DAVID A. VOGAN, JR.[1,b]

[1]Department of Mathematics, M.I.T., Cambridge, MA 02139, USA.

[a]E-mail: gyuri@math.mit.edu

[b]E-mail: dav@math.mit.edu

0. Introduction and Statement of Results

0.1. Let W be a Weyl group with standard set of generators S; let $\leq$ be the Bruhat order on W. In [6], [7], certain polynomials $P_{y,w} = \sum_{i\geq 0} P_{y,w;i}u^i$ ($P_{y,w;i} \in \mathbf{N}$, u is an indeterminate) were defined and computed in terms of an algorithm for any $y \leq w$ in W. These polynomials are of interest for the representation theory of complex reductive groups, see [6]. Let $\mathbf{I} = \{w \in W; w^2 = 1\}$ be the set of involutions in W. In this paper we introduce some new polynomials $P^\sigma_{y,w} = \sum_{i\geq 0} P^\sigma_{y,w;i}u^i$ ($P^\sigma_{y,w;i} \in \mathbf{Z}$) for any pair $y \leq w$ of elements of $\mathbf{I}$. These new polynomials are of interest in the theory of unitary representations of complex reductive groups, see [1]; they are again computable in terms of an algorithm, see 4.5. For $y \leq w$ in $\mathbf{I}$ and $i \in \mathbf{N}$ there is the following relation between $P_{y,w;i}$ and $P^\sigma_{y,w;i}$: there exist $a_i, b_i \in \mathbf{N}$ such that $P_{y,w;i} = a_i + b_i$, $P^\sigma_{y,w;i} = a_i - b_i$.

Let $\mathcal{A} = \mathbf{Z}[u, u^{-1}]$ and let $\mathfrak{H}$ be the free $\mathcal{A}$-module with basis $(T_w)_{w\in W}$ with the unique $\mathcal{A}$-algebra structure with unit T_1 such that

(i) $T_wT_{w'} = T_{ww'}$ if $l(ww') = l(w) + l(w')$

($l : W \to \mathbf{N}$ is the standard length function) and $(T_s + 1)(T_s - u) = 0$ for all $s \in S$. Let $\mathfrak{H}'$ be the $\mathcal{A}$-algebra with the same underlying $\mathcal{A}$-module as $\mathfrak{H}$ but with multiplication defined by the rules (i) and

Received November 01, 2011 and in revised form December 29, 2011.

AMS Subject Classification: 20G40, 20C08.

Key words and phrases: Hecke algebra, Weyl group, involution.

Supported in part by National Science Foundation grants DMS-0758262, DMS-0967272.

(ii) $(T_s+1)(T_s-u^2)=0$ for all $s\in S$.

In the course of defining the polynomials $P_{y,w}$ in [6] a special role was played by the triple $(\mathfrak{H}\otimes\mathfrak{H}^{opp},\mathfrak{H},{}^-:\mathfrak{H}\to\mathfrak{H})$ where the middle $\mathfrak{H}$ is viewed as a $\mathfrak{H}\otimes\mathfrak{H}^{opp}$-module via left and right multiplication ($\mathfrak{H}^{opp}$ is the algebra opposed to $\mathfrak{H}$) and ${}^-:\mathfrak{H}\to\mathfrak{H}$ is a certain ring involution. To define the new polynomials $P^\sigma_{y,w}$ we shall instead need a triple

$$(\mathfrak{H}',M,{}^-:M\to M)$$

where M is the free $\mathcal{A}$-module with basis $(a_w)_{w\in\mathbf{I}}$ with a certain $\mathfrak{H}'$-module structure and ${}^-:M\to M$ is a certain $\mathbf{Z}$-linear involution which are described in the following theorem (here ${}^-:\mathfrak{H}'\to\mathfrak{H}'$ is the ring involution such that $\overline{u^nT_w}=u^{-n}T^{-1}_{w^{-1}}$ for all $w\in W,n\in\mathbf{Z}$).

Theorem 0.2. (a) *Consider for any $s\in S$ the $\mathcal{A}$-linear map $T_s:M\to M$ given by*

(i) $(T_s+1)(a_w)=(u+1)(a_w+a_{sw})$ *if* $w\in\mathbf{I},sw=ws>w$;

(ii) $(T_s+1)(a_w)=(u^2-u)(a_w+a_{sw})$ *if* $w\in\mathbf{I},sw=ws<w$;

(iii) $(T_s+1)(a_w)=a_w+a_{sws}$ *if* $w\in\mathbf{I},sw\ne ws>w$;

(iv) $(T_s+1)(a_w)=u^2(a_w+a_{sws})$ *if* $w\in\mathbf{I},sw\ne ws<w$.

(*Note that in* (iii) *we have automatically $sw>w$ and in* (iv) *we have automatically $sw<w$.*) *The maps T_s $(s\in S)$ define an $\mathfrak{H}'$-module structure on M.*

(b) *There exists a unique $\mathbf{Z}$-linear map ${}^-:M\to M$ such that $\overline{u^nm}=u^{-n}\overline{m}$ for all $m\in M$, $n\in\mathbf{Z}$, $\overline{a_1}=a_1$ and $\overline{(T_s+1)m}=u^{-2}(T_s+1)\overline{m}$ for all $m\in M,s\in S$. For any $w\in\mathbf{I}$ we have $\overline{a_w}=\sum_{y\in\mathbf{I};y\le w}r_{y,w}a_y$ where $r_{y,w}\in\mathcal{A}$ and $r_{w,w}=u^{-l(w)}$. For any $h\in\mathfrak{H}'$ and $m\in M$ we have $\overline{hm}=\overline{h}\overline{m}$. For any $m\in M$ we have $\overline{\overline{m}}=m$.*

The proof of (a) is given in 1.8. The proof of (b), given in 2.9, is based on a sheaf theoretic construction of M, some elements of which are inspired by the geometric construction of the plus part of a universal quantized enveloping algebra of non-simply laced type given in [10, Chap.12].)

Let $\underline{\mathcal{A}}=\mathbf{Z}[v,v^{-1}]$ where v is an indeterminate. We view $\mathcal{A}$ as a subring of $\underline{\mathcal{A}}$ by setting $u=v^2$. Let $\underline{M}=\underline{\mathcal{A}}\otimes_{\mathcal{A}}M$. We can view M as a $\mathcal{A}$-submodule of $\underline{M}$. We extend $^-: M \to M$ to a $\mathbf{Z}$-linear map $^-: \underline{M} \to \underline{M}$ in such a way that $\overline{v^n m} = v^{-n}\overline{m}$ for $m \in \underline{M}, n \in \mathbf{Z}$. Let $\underline{\mathfrak{H}} = \underline{\mathcal{A}} \otimes_{\mathcal{A}} \mathfrak{H}$, $\underline{\mathfrak{H}}' = \underline{\mathcal{A}} \otimes_{\mathcal{A}} \mathfrak{H}'$. These are naturally $\underline{\mathcal{A}}$-algebras containing $\mathfrak{H}, \mathfrak{H}'$ as $\mathcal{A}$-subalgebras. Note that the $\mathfrak{H}'$-module structure on M extends by $\underline{\mathcal{A}}$-linearity to an $\underline{\mathfrak{H}}'$-module structure on $\underline{M}$. We have the following result.

Theorem 0.3. (a) *For any $w \in \mathbf{I}$ there is a unique element*

$$A_w = v^{-l(w)} \sum_{y \in \mathbf{I}; y \le w} P^{\sigma}_{y,w} a_y \in \underline{M}$$

($P^{\sigma}_{y,w} \in \mathbf{Z}[u]$) such that $\overline{A_w} = A_w$, $P^{\sigma}_{w,w} = 1$ and for any $y \in \mathbf{I}$, $y < w$, we have $\deg P^{\sigma}_{y,w} \le (l(w) - l(y) - 1)/2$.

(b) *The elements A_w ($w \in \mathbf{I}$) form an $\underline{\mathcal{A}}$-basis of $\underline{M}$.*

The proof is given in 3.1, 3.2. In 3.3 we give an interpretation of $P^{\sigma}_{y,w}$ in terms of intersection cohomology.

0.4. For any $z \in \mathbf{Q} - \{0\}$ let $M_z = \mathbf{Q} \otimes_{\mathcal{A}} M$, $\mathfrak{H}'_z = \mathbf{Q} \otimes_{\mathcal{A}} \mathfrak{H}'$ where $\mathbf{Q}$ is viewed as an $\mathcal{A}$-algebra under $u \mapsto z$. For $w \in W$ we write $T_w \in \mathfrak{H}'_z$ instead of $1 \otimes T_w$; for $w \in \mathbf{I}$ we write $a_w \in M_z$ instead of $1 \otimes a_w$. Note that $\mathfrak{H}'_1$ can be identified with $\mathbf{Q}[W]$, the group algebra of W, so that for $w \in W$, T_w becomes w. Now specializing 0.2(a) with $u = 1$ we see that M_1 is a W-module such that

$s(a_w) = a_w + 2a_{sw}$ if $w \in \mathbf{I}, sw = ws > w$;

$s(a_w) = -a_w$ if $w \in \mathbf{I}, sw = ws < w$;

$s(a_w) = a_{sws}$ if $w \in \mathbf{I}, sw \ne ws$.

In §6 it is shown that the W-module M_1 is isomorphic to a direct sum of representations of W induced from one-dimensional representations of centralizers of involutions. The last direct sum has been studied in detail by Kottwitz [8]; in 6.4 we reformulate Kottwitz's results in terms of unipotent representations.

0.5. If X is a set and $f : X \to X$ is a map we write $X^f = \{x \in X; f(x) = x\}$. If X is a finite set we write $|X|$ for the cardinal of X.

Contents

1. Proof of Theorem 0.2(a)

1.1. Let $\mathbf{k}$ be an algebraic closure of the field $\mathbf{F}_p$ with p elements. (p is a prime number.) Let G be a connected semisimple simply connected algebraic group over $\mathbf{k}$. Let $\mathcal{B}$ be the variety of Borel subgroups of G. Then G acts on $\mathcal{B}\times\mathcal{B}$ by simultaneous conjugation and the set of orbits can be viewed naturally as a Coxeter group (the Weyl group of G); we shall assume that this Coxeter group is W of 0.1 with its standard set of generators. For $w\in W$ we write $\mathcal{O}_w$ for the corresponding G-orbit in $\mathcal{B}\times\mathcal{B}$. Let $\phi: G\to G$ be the Frobenius map for a split $\mathbf{F}_p$-structure on G.

Let $s\in\mathbf{Z}_{>0}$ and let $q=p^s$. Then $\phi':=\phi^s: G\to G$ is the Frobenius map for a split $\mathbf{F}_q$-structure on G (we denote by $\mathbf{F}_q$ the subfield of $\mathbf{k}$ of cardinal q). For any $s\in S$ the $\mathcal{A}$-linear map $T_s: M\to M$ defined in 0.2(i)-(iv) induces a $\mathbf{Q}$-linear map $M_q\to M_q$ denoted again by T_s; it is given by 0.2(i)-(iv) with u replaced by q.

Consider the $\mathbf{F}_q$-rational structure on $\mathcal{B}\times\mathcal{B}$ with Frobenius map

$$F:(B,B')\mapsto(\phi'(B'),\phi'(B)).$$

We have

$$(\mathcal{B}\times\mathcal{B})^F=\{(B,B')\in\mathcal{B}\times\mathcal{B}; B=\phi'(B'), B'=\phi'(B)\}.$$

If $(B,B')\in\mathcal{O}_w$ is fixed by F then $(\phi'(B'),\phi'(B))\in\mathcal{O}_w\cap\mathcal{O}_{w^{-1}}$ hence $w\in\mathbf{I}$. On the other hand if $(B,B')\in\mathcal{O}_w$, $w\in\mathbf{I}$ then $(\phi'(B'),\phi'(B))\in\mathcal{O}_w$ so that $\mathcal{O}_w$ is F-stable. We see that $(\mathcal{B}\times\mathcal{B})^F=\sqcup_{w\in\mathbf{I}}\mathcal{O}_w^F$. Now if $w\in\mathbf{I}$, then G acts transitively on $\mathcal{O}_w$ and this action is compatible with the $\mathbf{F}_q$-structure on $\mathcal{O}_w$ given by F and with the $\mathbf{F}_q$-structure on G given by $\phi':G\to G$. Hence, using Lang's theorem, we see that $\mathcal{O}_w^F\neq\emptyset$ and that the induced action of $G^{\phi'}$ on $\mathcal{O}_w^F$ is transitive (here we use also that the stabilizer in G of a point in $\mathcal{O}_w$ is connected). We see that the $G^{\phi'}$-orbits in $(\mathcal{B}\times\mathcal{B})^F$ are exactly the sets $\mathcal{O}_w^F$ with $w\in\mathbf{I}$. Let $\mathcal{F}_q$ be the vector space of functions $(\mathcal{B}\times\mathcal{B})^F\to\mathbf{Q}$ which are constant on the orbits of $G^{\phi'}$. Clearly we can identify M_q with $\mathcal{F}_q$ in such a way that for $w\in\mathbf{I}$, a_w becomes the function which is 1 on $\mathcal{O}_w^F$ and is 0 on $\mathcal{O}_{w'}^F$ for $w'\in\mathbf{I},w'\neq w$.

Next we consider the $\mathbf{F}_{q^2}$-rational structure on $\mathcal{B}\times\mathcal{B}$ with Frobenius map $(B,B')\mapsto(\phi'^2(B),\phi'^2(B'))$ denoted again by ϕ'^2. We have clearly $(\mathcal{B}\times\mathcal{B})^{\phi'^2}=\sqcup_{w\in W}\mathcal{O}_w^{\phi'^2}$ and this is exactly the decomposition of $(\mathcal{B}\times\mathcal{B})^{\phi'^2}$ into $G^{\phi'^2}$-orbits. Let $\mathcal{F}'_q$ be the vector space of functions $(\mathcal{B}\times\mathcal{B})^{\phi'^2}\to\mathbf{Q}$ which are constant on the orbits of $G^{\phi'^2}$. We define an (associative) algebra structure on $\mathcal{F}'_q$ by $h,h'\mapsto h*h'$ where

$$(h*h')(B_1,B_2)=\sum_{\beta\in\mathcal{B}^{\phi'^2}}h(B_1,\beta)h'(\beta,B_2).$$

Clearly we can identify $\mathfrak{H}'_q$ with $\mathcal{F}'_q$ as vector spaces in such a way that for $w\in W$, T_w becomes the function which is 1 on $\mathcal{O}_w^{\phi'^2}$ and is 0 on $\mathcal{O}_{w'}^{\phi'^2}$ for $w'\in W-\{w\}$. By Iwahori [5], this identification respects the algebra structures on $\mathcal{F}'_q,\mathfrak{H}'_q$.

For $h\in\mathcal{F}'_q,m\in\mathcal{F}_q$ we define $h*m\in\mathcal{F}_q$ by

$$(h*m)(B_1,B_2)=\sum_{\beta\in\mathcal{B}^{\phi'^2}}h(B_1,\beta)m(\beta,\phi'(\beta)).$$

(It may look strange that B_2 does not appear in the right hand side; but in fact it appears through B_1 since $B_2=\phi'(B_1)$.) If $h,h'\in\mathcal{F}'_q$, $m\in\mathcal{F}_q$ we have

$$((h*h')*m)(B_1,B_2)\;=\;\sum_{\beta\in\mathcal{B}^{\phi'^2}}(h*h')(B_1,\beta)m(\beta,\phi'(\beta))$$

$$
\begin{aligned}
&= \sum_{\beta,\beta'\in\mathcal{B}^{\phi'^2}} h(B_1,\beta')h'(\beta',\beta)m(\beta,\phi'(\beta))\\
&= \sum_{\beta'\in\mathcal{B}^{\phi'^2}} h(B_1,\beta')(h'*m)(\beta',\phi'(\beta'))\\
&= (h*(h'*m))(B_1,B_2).
\end{aligned}
$$

Thus $(h*h')*m = h*(h'*m)$ so that $h,m\mapsto h*m$ defines an $\mathcal{F}'_q$-module structure on $\mathcal{F}_q$. (Note that $T_1*m=m$ for $m\in\mathcal{F}_q$.)

1.2. Let $s\in S$, $w\in\mathbf{I}$. We have $T_s*a_w=\sum_{w'\in\mathbf{I}}N_{s,w,w'}a_{w'}$, where

$$
\begin{aligned}
N_{s,w,w'} &= |\{\beta\in\mathcal{B}^{\phi'^2};(\beta,\phi'(\beta))\in\mathcal{O}_w,(C,\beta)\in\mathcal{O}_s\}|\\
&= |\{(\beta,\beta')\in\mathcal{O}_w^F;(C,\beta)\in\mathcal{O}_s,(\beta',C')\in\mathcal{O}_s\}|
\end{aligned}
$$

for any $(C,C')\in\mathcal{O}^F_{w'}$. To simplify notation we write $N_{w'}$ instead of $N_{s,w,w'}$ since s,w are fixed. In 1.3-1.6 we compute the number $N_{w'}$ for a fixed $(C,C')\in\mathcal{O}^F_{w'}$, $w'\in\mathbf{I}$.

1.3. In this subsection we assume that $sw\neq ws>w$. Using [3, 1.6.4] we see that $l(sws)\neq l(w)$ hence $l(sws)=l(w)+2$. If $N_{w'}\neq 0$ then there exists $(\beta,\beta')\in\mathcal{O}_w$ such that $(C,\beta)\in\mathcal{O}_s,(\beta',C')\in\mathcal{O}_s$. Hence $w'=sws$. Conversely, assume that $w'=sws$. There is a unique $(\beta,\beta')\in\mathcal{O}_w$ such that $(C,\beta)\in\mathcal{O}_s,(\beta',C')\in\mathcal{O}_s$. We have $(\phi'(\beta'),\phi'(\beta))\in\mathcal{O}_w$, $(C,\phi'(\beta'))\in\mathcal{O}_s,(\phi'(\beta),C')\in\mathcal{O}_s$. (We use that $\phi'(C)=C'$, $\phi'(C)=C'$.) By uniqueness we must have $\phi'(\beta)=\beta'$, $\phi'(\beta')=\beta$. Thus $(\beta,\beta')\in\mathcal{O}^F_w$. We see that $N_{sws}=1$ so that $T_s*a_w=a_{sws}$.

1.4. In this subsection we assume that $sw=ws>w$. If $N_{w'}\neq 0$ then there exists $(\beta,\beta')\in\mathcal{O}_w$ such that $(C,\beta)\in\mathcal{O}_s,(\beta',C')\in\mathcal{O}_s$. Hence $(C,\beta')\in\mathcal{O}_{sw}$ (we use that $l(sw)>l(w)$) and $(C,C')\in\mathcal{O}_{sw}\cup\mathcal{O}_w$ (we use that $sws=w$); hence $w'=sw$ or $w'=w$.

Assume first that $w'=w$. We set

$$Z=\{(\beta,\beta')\in\mathcal{O}_w;(C,\beta)\in\mathcal{O}_s,(\beta',C')\in\mathcal{O}_s\}.$$

We claim that the first projection $Z\to Y:=\{\beta\in\mathcal{B};(C,\beta)\in\mathcal{O}_s\}$ is an isomorphism so that Z is an affine line. Let $\beta\in Y$. It is enough to show that there is a unique $\beta'\in\mathcal{B}$ such that $(\beta,\beta')\in\mathcal{O}_w,(\beta',C')\in\mathcal{O}_s$. Since

$l(ws) > l(w)$ it is enough to show that $(\beta, C') \in \mathcal{O}_{ws}$; but from $(\beta, C) \in \mathcal{O}_s, (C, C') \in \mathcal{O}_w$, $l(sw) > l(w)$ we do indeed deduce that $(\beta, C') \in \mathcal{O}_{ws}$, as desired. This proves our claim. Now the restriction of F to Z is an $\mathbf{F}_q$-rational structure on an affine line hence it has exactly q fixed points. It follows that $N_w = q$.

Assume next that $w' = sw = sw$. We set

$$Z' = \{(\beta, \beta') \in \mathcal{O}_w; (C, \beta) \in \mathcal{O}_s \cup \mathcal{O}_1, (\beta', C') \in \mathcal{O}_s \cup \mathcal{O}_1\}.$$

We claim that the first projection $Z' \to Y' := \{\beta \in \mathcal{B}; (C, \beta) \in \mathcal{O}_s \cup \mathcal{O}_1\}$ is an isomorphism so that Z' is a projective line. It is enough to show that for any $\beta \in Y'$ the set

$$\Xi_\beta = \{\beta' \in \mathcal{B}; (\beta, \beta') \in \mathcal{O}_w, (\beta', C') \in \mathcal{O}_s \cup \mathcal{O}_1\}$$

has exactly one element. Let C_1 be the unique element of $\mathcal{B}$ such that $(C, C_1) \in \mathcal{O}_s, (C_1, C') \in \mathcal{O}_w$ (we use that $(C, C') \in \mathcal{O}_{sw}$ and $l(sw) > l(w)$). Note that $C_1 \in Y'$. If $\beta = C_1$ then $C' \in \Xi_\beta$; if $\beta' \in \Xi_\beta - \{C'\}$ then $(\beta', C') \in \mathcal{O}_s$, $(C', C_1) \in \mathcal{O}_w$ hence $(\beta', C_1) \in \mathcal{O}_{sw}$ (since $l(sw) > l(w)$) contradicting $(\beta', \beta) \in \mathcal{O}_w$. Thus $|\Xi_{C_1}| = |\{C'\}| = 1$. Now assume that $\beta \in Y' - \{C_1\}$. From $\beta \neq C_1$, $(C, \beta) \in \mathcal{O}_s \cup \mathcal{O}_1$, $(C, C') \in \mathcal{O}_{sw}$ we deduce that $(\beta, C') \in \mathcal{O}_{sw}$. Hence there is a unique $\beta'_0 \in \mathcal{B}$ such that $(\beta, \beta'_0) \in \mathcal{O}_w$, $(\beta'_0, C') \in \mathcal{O}_s$. We have $\beta'_0 \in \Xi_\beta$. Conversely, if $\beta' \in \Xi_\beta$ we have $\beta' \neq C'$ (since $(\beta, C') \in \mathcal{O}_{sw}$); thus $\beta' = \beta'_0$. We see that $|\Xi_\beta| = |\{\beta'_0\}| = 1$. This proves our claim.

Now the restriction of F to Z' is an $\mathbf{F}_q$-rational structure on a projective line hence it has exactly $q+1$ fixed points. If $(\beta, \beta') \in Z^F$ then we have necessarily $C \neq \beta$ and $C' \neq \beta'$. Indeed, if $C = \beta$ then $\phi'(C) = \phi'(\beta)$ hence $C' = \beta'$ and $(\beta, \beta') = (C, C') \in \mathcal{O}_{sw}$ contradicting $(\beta, \beta') \in \mathcal{O}_w$. Similarly, if $C' = \beta'$ then $\phi'(C') = \phi'(\beta')$ hence $C = \beta$ and $(\beta, \beta') = (C, C') \in \mathcal{O}_{sw}$ contradicting $(\beta, \beta') \in \mathcal{O}_w$. Thus

$$q + 1 = |Z'^F| = |\{(\beta, \beta') \in \mathcal{O}_w^F; (C, \beta) \in \mathcal{O}_s, (\beta', C') \in \mathcal{O}_s\}| = N_{sw}.$$

We see that $T_s * a_w = qa_w + (q+1)a_{sw}$.

1.5. In this subsection we assume that $sw \neq ws < w$. Using [3, 1.6.4] we see that $l(sws) \neq l(w)$ hence $l(sws) = l(w) - 2$. We have $s(sws) \neq (sws)s >$

sws. Applying 1.3 to sws instead of w we obtain $T_s * a_{sws} = a_w$. Applying T_s to the last equality and using the equation $T_s^2 = (q^2-1)T_s+q^2 : \mathcal{F}_q \to \mathcal{F}_q$, we obtain

$$(q^2-1)T_s * a_{sws} + q^2 a_{sws} = T_s * a_w$$

that is, $T_s * a_w = (q^2-1)a_w + q^2 a_{sws}$.

1.6. In this subsection we assume that $sw = ws < w$. We have $s(sw) = (sw)s > sw$. Applying 1.4 to sw instead of w we obtain $T_s * a_{sw} = q a_{sw} + (q+1)a_w$. Applying T_s to the last equality and using the equation $T_s^2 = (q^2-1)T_s+q^2 : \mathcal{F}_q \to \mathcal{F}_q$ we obtain $(q^2-1)T_s*a_{sw}+q^2a_{sw} = qT_s*a_{sw}+(q+1)T_s*a_w$ that is

$$\begin{aligned}(q+1)T_s * a_w &= (q^2-1-q)T_s * a_{sw} + q^2 a_{sw}\\ &= (q^2-q-1)q a_{sw} + (q^2-q-1)(q+1)a_w + q^2 a_{sw}.\end{aligned}$$

Dividing by $q+1$ we obtain $T_s * a_w = (q^2-q-1)a_w + (q^2-q)a_{sw}$.

1.7. From the results in 1.3-1.6 we see that the operators $T_s : M_q \to M_q$ ($s \in S$) given by the formulas 0.2(i)-(iv) with u replaced by q define an $\mathfrak{H}'_q$-module structure on M_q.

1.8. We now prove 0.2(a). We shall use the following obvious fact.

(a) If $m \in M$ has zero image in M_{p^s} for $s = 1, 2, \ldots$ then $m = 0$.

Let $s, t \in S, s \neq t$ and let k be the order of st in W. Let $m \in M$. Let $m' = (T_sT_tT_s\cdots)m - (T_tT_sT_t\cdots)m \in M$ (both products have k factors). From 1.7 we see that m' has zero image in M_{p^s} for $s = 1, 2, \ldots$; hence by (a) we have $m' = 0$.

Now let $s \in S$ and let $m \in M$. Let $m' = T_s^2 m - (u^2-1)T_s m - u^2 m \in M$. From 1.7 we see that m' has zero image in M_{p^s} for $s = 1, 2, \ldots$; hence by (a) we have $m' = 0$.

We see that 0.2(a) holds.

2. Proof of Theorem 0.2(b)

2.1. We preserve the notation of 1.1. We fix a prime number $l \neq p$. For any complex $\mathfrak{K}$ of constructible $\mathbf{Q}_l$-sheaves on an algebraic variety we denote by $\mathcal{H}^i\mathfrak{K}$ the i-th cohomology sheaf of $\mathfrak{K}$ and by $D\mathfrak{K}$ the Verdier dual of $\mathfrak{K}$.

Let $\mathcal{C}_0$ be the category whose objects are the constructible G-equivariant $\mathbf{Q}_l$-sheaves on $\mathcal{B} \times \mathcal{B}$; the morphisms in $\mathcal{C}_0$ are morphisms of G-equivariant $\mathbf{Q}_l$-sheaves. Let Vec be the category of finite-dimensional $\mathbf{Q}_l$-vector spaces. If $\mathcal{S} \in \mathcal{C}_0$ and $x \in \mathcal{B} \times \mathcal{B}$, let $\mathcal{S}_x$ be the stalk of $\mathcal{S}$ at x; for any $w \in W$ there is a well defined object $V_w^{\mathcal{S}} \in Vec$ which is canonically isomorphic to $\mathcal{S}_x$ for any $x \in \mathcal{O}_w$. Note that $\mathcal{S} \mapsto V_w^{\mathcal{S}}$ is a functor $\mathcal{C}_0 \to Vec$. For $w \in W$ let $\mathbf{S}_w$ be the object of $\mathcal{C}_0$ which is $\mathbf{Q}_l$ on $\mathcal{O}_w$ and is 0 on $\mathcal{B} \times \mathcal{B} - \mathcal{O}_w$. For $w \in W$ let $\mathbf{S}_w^\sharp$ be the intersection cohomology complex of the closure $\bar{\mathcal{O}}_w$ of $\mathcal{O}_w$ with coefficients in $\mathbf{Q}_l$ (on $\mathcal{O}_w$) extended by zero on $\mathcal{B} \times \mathcal{B} - \bar{\mathcal{O}}_w$. We have $\mathcal{H}^i\mathbf{S}_w^\sharp \in \mathcal{C}_0$ ($i \in \mathbf{Z}$); moreover $\mathcal{H}^i\mathbf{S}_w^\sharp$ is zero for large i and is zero unless $i \in 2\mathbf{N}$, see [7, Thm. 4.2]. If $\mathcal{S} \in \mathcal{C}_0$, then $\mathcal{H}^iD\mathcal{S} \in \mathcal{C}_0$ ($i \in \mathbf{Z}$); moreover $\mathcal{H}^iD\mathcal{S}$ is zero for all but finitely many i.

Let $\mathcal{C}_1$ be the category whose objects are pairs $(\mathcal{S}, \Psi)$ where $\mathcal{S} \in \mathcal{C}_0$ and Ψ is an isomorphism $\phi^{2*}\mathcal{S} \xrightarrow{\sim} \mathcal{S}$ in $\mathcal{C}_0$. A morphism between two objects $(\mathcal{S}, \Psi), (\mathcal{S}', \Psi')$ of $\mathcal{C}_1$ is a morphism $\mathcal{S} \to \mathcal{S}'$ in $\mathcal{C}_0$ which is compatible with Ψ, Ψ'. If $(\mathcal{S}, \Psi) \in \mathcal{C}_1$ then for any $w \in W$, Ψ induces a linear isomorphism $\Psi_w : V_w^{\mathcal{S}} \to V_w^{\mathcal{S}}$ (Note that $V_w^{\phi^{2*}\mathcal{S}} = V_w^{\mathcal{S}}$ since $\mathcal{O}_w$ is ϕ-stable.) If $z \in \mathbf{Q}_l^*$ and $(\mathcal{S}, \Psi) \in \mathcal{C}_1$ then $(\mathcal{S}, z\Psi) \in \mathcal{C}_1$. If $(\mathcal{S}, \Psi) \in \mathcal{C}_1$ then for any i let $\Psi^{(i)} : \phi^{2*}\mathcal{H}^iD\mathcal{S} \xrightarrow{\sim} \mathcal{H}^iD\mathcal{S}$ be the inverse of the isomorphism $\mathcal{H}^iD\mathcal{S} \to \phi^{2*}\mathcal{H}^iD\mathcal{S}$ induced by D; thus $(\mathcal{H}^iD\mathcal{S}, \Psi^{(i)}) \in \mathcal{C}_1$.

For any $w \in W$ and any $z \in \mathbf{Q}_l^*$ we have $(\mathbf{S}_w, t_z) \in \mathcal{C}_1$ where $t_z : \phi^{2*}\mathbf{S}_w \xrightarrow{\sim} \mathbf{S}_w$ is multiplication by z (we have $\phi^{2*}\mathbf{S}_w = \mathbf{S}_w$).

Let $\mathcal{C}_2$ be the full subcategory of $\mathcal{C}_1$ whose objects are the pairs $(\mathcal{S}, \Psi) \in \mathcal{C}_1$ such that for any $w \in W$ all eigenvalues of $\Psi_w : V_w^{\mathcal{S}} \to V_w^{\mathcal{S}}$ are even powers of p. For example if $w \in W, k \in \mathbf{Z}$ then $(\mathbf{S}_w, t_{p^{2k}}) \in \mathcal{C}_2$.

Lemma 2.2. *For any $(\mathcal{S}, \Psi) \in \mathcal{C}_2$ and any $i \in \mathbf{Z}$ we have $(\mathcal{H}^iD\mathcal{S}, \Psi^{(i)}) \in \mathcal{C}_2$.*

It suffices to show that $(\mathcal{H}^iD\mathbf{S}_w, t_1^{(i)}) \in \mathcal{C}_2$ for any $w \in W, i \in \mathbf{Z}$. We can assume that $w \in W$ is fixed and that the statement in the previous sentence holds when w is replaced by any $w' \in W$, $w' < w$. Let $j^w : \phi^{2*}\mathbf{S}_w^\sharp \xrightarrow{\sim} \mathbf{S}_w^\sharp$ be the unique isomorphism such that the induced isomorphism $V_w^{\mathcal{H}^0\mathbf{S}_w^\sharp} \to V_w^{\mathcal{H}^0\mathbf{S}_w^\sharp}$ is the identity map. By [7, Thm. 4.2], j^w induces for any $h \in \mathbf{Z}$ an isomorphism $j^w_h : \phi^{2*}\mathcal{H}^h\mathbf{S}^\sharp_w \xrightarrow{\sim} \mathcal{H}^h\mathbf{S}^\sharp_w$ such that

(a) $(\mathcal{H}^h\mathbf{S}^\sharp_w, j^w_h) \in \mathcal{C}_2$.

Let K be the restriction of $\mathbf{S}^\sharp_w$ to $\bar{\mathcal{O}}_w - \mathcal{O}_w$ extended by 0 on the complement of $\bar{\mathcal{O}}_w - \mathcal{O}_w$. Now j^w induces an isomorphism $d : \phi^{2*}K \xrightarrow{\sim} K$. Let $d' : \phi^{2*}DK \xrightarrow{\sim} DK$ be the inverse of the isomorphism $DK \to \phi^{2*}DK$ induced by d; this induces isomorphisms $d'_h : \phi^{2*}\mathcal{H}^h DK \xrightarrow{\sim} \mathcal{H}^h DK$ for $h \in \mathbf{Z}$. Since $\mathrm{supp}(K) \subset \bar{\mathcal{O}}_w - \mathcal{O}_w$ we see using (a) and the induction hypothesis that

(b) $(\mathcal{H}^h DK, d'_h) \in \mathcal{C}_2$ for $h \in \mathbf{Z}$.

Now j^w induces an isomorphism $D\mathbf{S}^\sharp_w \to \phi^{2*}D\mathbf{S}^\sharp_w$ whose inverse is an isomorphism $j' : \phi^{2*}D\mathbf{S}^\sharp_w \xrightarrow{\sim} D\mathbf{S}^\sharp_w$. This induces for any $h \in \mathbf{Z}$ an isomorphism $j'_h : \phi^{2*}\mathcal{H}^h D\mathbf{S}^\sharp_w \xrightarrow{\sim} \mathcal{H}^h D\mathbf{S}^\sharp_w$. We can identify $D\mathbf{S}^\sharp_w = \mathbf{S}^\sharp_w[2m]$ for some $m \in \mathbf{Z}$ in such a way that j'_h becomes $p^{2m'} j^w_{h+2m}$ for some $m' \in \mathbf{Z}$. Using (a) we deduce that

(c) $(\mathcal{H}^h D\mathbf{S}^\sharp_w, j'_h) \in \mathcal{C}_2$.

Using (c), (b) and the long exact sequence of cohomology sheaves associated to the exact triangle consisting of $D\mathbf{S}_w, \Delta\mathbf{S}^\sharp_w, DK$ (which is obtained from the exact triangle consisting of $K, \mathbf{S}^\sharp_w, \mathbf{S}_w$) we deduce that $(\mathcal{H}^h D\mathbf{S}_w, t_1^{(h)}) \in \mathcal{C}_2$ for any $h \in \mathbf{Z}$. This completes the inductive proof. $\square$

2.3. Define $\sigma : \mathcal{B} \times \mathcal{B} \to \mathcal{B} \times \mathcal{B}$ by $(B, B') \mapsto (B', B)$. Then

$$\tilde{\phi} := \phi\sigma = \sigma\phi : \mathcal{B} \times \mathcal{B} \to \mathcal{B} \times \mathcal{B}$$

is the Frobenius map for an $\mathbf{F}_p$-rational structure on $\mathcal{B}\times\mathcal{B}$ such that $\tilde{\phi}^2 = \phi^2$.

Let $\mathcal{C}$ be the category whose objects are pairs $(\mathcal{S}, \Phi)$ where $\mathcal{S} \in \mathcal{C}_0$ and Φ is an isomorphism $\tilde{\phi}^*\mathcal{S} \to \mathcal{S}$ in $\mathcal{C}_0$ such that, setting $\Psi = \tilde{\phi}^*(\Phi)\Phi : \tilde{\phi}^{2*}\mathcal{S} \to \mathcal{S}$, we have $(\mathcal{S}, \Psi) \in \mathcal{C}_2$ (note that $\tilde{\phi}^{2*}\mathcal{S} = \phi^{2*}\mathcal{S}$). A morphism between two objects $(\mathcal{S}, \Phi), (\mathcal{S}', \Phi')$ of $\mathcal{C}$ is a morphism $\mathcal{S} \to \mathcal{S}'$ in $\mathcal{C}_0$ which is compatible with Φ, Φ'. Note that if $(\mathcal{S}, \Phi) \in \mathcal{C}$, then $(\mathcal{S}, -\Phi) \in \mathcal{C}$. For $(\mathcal{S}, \Phi) \in \mathcal{C}$ and $w \in \mathbf{I}$, Φ induces a linear isomorphism $\Phi_w : V^{\mathcal{S}}_w \to V^{\mathcal{S}}_w$. (Note that $V^{\tilde{\phi}^*\mathcal{S}}_w = V^{\mathcal{S}}_w$ since $\mathcal{O}_w$ is $\tilde{\phi}$-stable.)

For any $(\mathcal{S},\Psi)\in\mathcal{C}_2$ let $\Phi:\tilde{\phi}^*(\mathcal{S}\oplus\tilde{\phi}^*\mathcal{S})\to\mathcal{S}\oplus\tilde{\phi}^*\mathcal{S}$ (that is $\Phi:\tilde{\phi}^*\mathcal{S}\oplus\tilde{\phi}^{2*}\mathcal{S}\to\mathcal{S}\oplus\tilde{\phi}^*\mathcal{S}$) be the isomorphism whose restriction to $\tilde{\phi}^*\mathcal{S}$ is $0\oplus 1$ and whose restriction to $\tilde{\phi}^{2*}\mathcal{S}$ is $\Psi\oplus 0$. We set $\Theta(\mathcal{S},\Psi)=(\mathcal{S}\oplus\tilde{\phi}^*\mathcal{S},\Phi)$. Note that $\Theta(\mathcal{S},\Psi)\in\mathcal{C}$.

Let E be the subset of $\mathbf{Q}_l$ consisting of $p^n,-p^n$ $(n\in\mathbf{Z})$. For $w\in\mathbf{I}$, $z\in E$ let $\tau_z:\tilde{\phi}^*\mathbf{S}_w\xrightarrow{\sim}\mathbf{S}_w$ be the isomorphism such that $\Phi_w:V_w^{\mathbf{S}_w}\to V_w^{\mathbf{S}_w}$ is multiplication by z. We have $(\mathbf{S}_w,\tau_z)\in\mathcal{C}$.

Let $K(\mathcal{C})$ be the Grothendieck group of $\mathcal{C}$. We have the following result.

Lemma 2.4. *If $(\mathcal{S},\Phi)\in\mathcal{C}$ then in $K(\mathcal{C})$, $(\mathcal{S},\Phi)$ is a $\mathbf{Z}$-linear combination of elements $(\mathbf{S}_w,\tau_z)$ $(w\in\mathbf{I},z\in E)$ and of elements $\Theta(\mathcal{S},\Psi)$ for various $(\mathcal{S},\Psi)\in\mathcal{C}_2$.*

We can assume that the set $J:=\{w\in W;\mathcal{S}|_{\mathcal{O}_w}\neq 0\}$ consists either of (i) a single element of $\mathbf{I}$ or (ii) of two distinct elements w',w'' whose product is 1 and that for any $w\in J$ we have $\mathcal{S}|_{\mathcal{O}_w}=\mathbf{Q}_l$. In case (i) we have $(\mathcal{S},\Phi)=(\mathbf{S}_w,\tau_z)$ where $J=\{w\}$, $z\in E$; in case (ii) we have $(\mathcal{S},\Phi)\cong\Theta(\mathbf{S}_w,t_{p^{2n}})$ where $w\in J$ and $n\in\mathbf{Z}$. The lemma is proved. $\square$

2.5. Let $K'(\mathcal{C})$ be the subgroup of $K(\mathcal{C})$ generated by the elements of the form $\Theta(\mathcal{S},\Psi)$ for various $(\mathcal{S},\Psi)\in\mathcal{C}_2$ and by the elements of the form $(\mathcal{S},\Phi)+(\mathcal{S},-\Phi)$ with $(\mathcal{S},\Phi)\in\mathcal{C}$. Let $\bar{K}(\mathcal{C})=K(\mathcal{C})/K'(\mathcal{C})$. From 2.4 we see that

(a) *the abelian group $\bar{K}(\mathcal{C})$ is generated by the elements $(\mathbf{S}_w,\tau_{p^n})$ $(w\in\mathbf{I},n\in\mathbf{Z})$.*

We regard $K(\mathcal{C})$ as an $\mathcal{A}$-module where $u^n(\mathcal{S},\Phi)=(\mathcal{S},p^n\Phi)$ for $n\in\mathbf{Z}$. Then $K'(\mathcal{C})$ is an $\mathcal{A}$-submodule of $K(\mathcal{C})$ hence $\bar{K}(\mathcal{C})$ inherits an $\mathcal{A}$-module structure from $K(\mathcal{C})$.

2.6. Let s be an odd integer ≥ 1 and let $q=p^s$. Let

$$F=\phi^s\sigma=\sigma\phi^s=\tilde{\phi}^s:\mathcal{B}\times\mathcal{B}\to\mathcal{B}\times\mathcal{B}$$

be as in 1.1. For $(\mathcal{S},\Phi)\in\mathcal{C}$ we define a function $\chi_s(\mathcal{S},\Phi)\in\mathcal{F}_q$ (see 1.1) as follows. For $x\in(\mathcal{B}\times\mathcal{B})^F$, $\chi_s(\mathcal{S},\Phi)(x)$ is the trace of the composition

$$\mathcal{S}_x=\mathcal{S}_{\tilde{\phi}^s(x)}\xrightarrow{\Phi}\mathcal{S}_{\tilde{\phi}^{s-1}(x)}\xrightarrow{\Phi}\cdots\xrightarrow{\Phi}\mathcal{S}_{\tilde{\phi}(x)}\xrightarrow{\Phi}\mathcal{S}_x$$

or equivalently, the trace of $\Phi^s_w : V^{\mathcal{S}}_w \to V^{\mathcal{S}}_w$ where $w \in \mathbf{I}$ is such that $x \in \mathcal{O}^{\tilde{\phi}^s}_w$. Clearly, $(\mathcal{S}, \Phi) \mapsto \chi_s(\mathcal{S}, \Phi)$ defines a group homomorphism $\chi_s : K(\mathcal{C}) \to \mathcal{F}_q$ such that $\chi_s(u\xi) = p^s \chi_s(\xi)$ for all $\xi \in K(\mathcal{C})$ and such that $\chi_s(\mathbf{S}_w, \tau_1) = a_w$ for all $w \in \mathbf{I}$.

If $(\mathcal{S}, \Psi) \in \mathcal{C}_2$, the function $\chi_s(\Theta(\mathcal{S}, \Phi)) : (\mathcal{B} \times \mathcal{B})^F \to \bar{\mathbf{Q}}_l$ is 0 (its value at $x \in (\mathcal{B} \times \mathcal{B})^F$ is, from the definitions, the trace of a linear map of the form $A \oplus B \to A \oplus B$, $(a, b) \mapsto (T(b), T'(a))$ where $T : B \to A, T' : A \to B$ are linear maps). From the definition we see also that if $(\mathcal{S}, \Phi) \in \mathcal{C}$ then $\chi_s(\mathcal{S}, \Phi) + \chi_s(\mathcal{S}, -\Phi) = 0$. Thus, $\chi_s : K(\mathcal{C}) \to \mathcal{F}_q$ maps $K'(\mathcal{C})$ to 0 hence it induces a group homomorphism $\bar{K}(\mathcal{C}) \to \mathcal{F}_q$ denoted again by χ_s. It satisfies $\chi_s(u\xi) = p^s \chi_s(\xi)$ for all $\xi \in \bar{K}(\mathcal{C})$. We show:

(a) *if $\xi \in \bar{K}(\mathcal{C})$ is such that $\chi_s(\xi) = 0$ for all odd integers $s \geq 1$ then $\xi = 0$.*

By 2.4 we have $\xi = \sum_{w \in \mathbf{I}, n \in \mathbf{Z}} c_{w,n} (\mathbf{S}_w, \tau_{p^n})$ where $c_{w,n} \in \mathbf{Z}$ are zero for all but finitely many (w, n). Applying χ_s we obtain $0 = \sum_{w \in \mathbf{I}, n \in \mathbf{Z}} c_{w,n} p^{ns} a_w$. Since the a_w form a basis of $\mathcal{F}_{p^s}$ we deduce $\sum_{w \in \mathbf{I}, n \in \mathbf{Z}} c_{w,n} p^{ns} = 0$ for any $w \in \mathbf{I}$. Since this holds for $s = 1, 3, \ldots$ we see that $c_{w,n} = 0$ for any $w \in \mathbf{I}, n \in \mathbf{Z}$, proving (a).

We show:

(b) *The elements $(\mathbf{S}_w, \tau_1)$ $(w \in \mathbf{I})$ form an $\mathcal{A}$-basis of $\bar{K}(\mathcal{C})$.*

The fact that they generate the $\mathcal{A}$-module $\bar{K}(\mathcal{C})$ follows from 2.4. The fact that they are linearly independent over $\mathcal{A}$ follows from the proof of (a).

2.7. If $(\mathcal{S}, \Phi) \in \mathcal{C}$ then for any i let $\Phi^{(i)} : \tilde{\phi}^* \mathcal{H}^i D\mathcal{S} \xrightarrow{\sim} \mathcal{H}^i D\mathcal{S}$ be the inverse of the isomorphism $\mathcal{H}^i D\mathcal{S} \to \tilde{\phi}^* \mathcal{H}^i D\mathcal{S}$ induced by D. Note that if $z \in E$ (see 2.3) then $(z\Phi)^{(i)} = z^{-1} \Phi^{(i)}$. Moreover, setting $\Psi = \Phi \tilde{\phi}^*(\Phi) : \tilde{\phi}^{2*} \mathcal{S} \xrightarrow{\sim} \mathcal{S}$, we have that $\Phi^{(i)} \tilde{\phi}^*(\Phi^{(i)}) : \tilde{\phi}^{2*} \mathcal{S} \to \mathcal{S}$ is equal to $\Psi^{(i)}$ (as in 2.1). Using now 2.2 we see that

(a) $(\mathcal{H}^i D\mathcal{S}, \Phi^{(i)}) \in \mathcal{C}$.

Clearly there is a well defined $\mathbf{Z}$-linear map $\mathbf{D} : K(\mathcal{C}) \to K(\mathcal{C})$ such that

$$\mathbf{D}(\mathcal{S}, \Phi) = \sum_{i \in \mathbf{Z}} (-1)^i (\mathcal{H}^i D\mathcal{S}, \Phi^{(i)})$$

for any $(\mathcal{S}, \Phi) \in \mathcal{C}$. If $(\mathcal{S}, \Psi) \in \mathcal{C}_2$ and $\Theta(\mathcal{S}, \Psi) = (\mathcal{S} \oplus \tilde{\phi}^* \mathcal{S}, \Phi)$ then for any i we have $(\mathcal{H}^i D(\mathcal{S} \oplus \tilde{\phi}^* \mathcal{S}), \Phi^{(i)}) = \Theta(\mathcal{H}^i D\mathcal{S}, \Psi^{(i)})$ where $(\mathcal{H}^i D\mathcal{S}, \Psi^{(i)}) \in \mathcal{C}_2$

(see 2.2). Moreover if $(\mathcal{S},\Phi)\in\mathcal{C}$ then for any i we have $(\mathcal{H}^iD\mathcal{S},(-\Phi)^{(i)})=(\mathcal{H}^iD\mathcal{S},-\Phi^{(i)})$. It follows that $\mathbf{D}$ carries $K'(\mathcal{C})$ into itself hence it induces a $\mathbf{Z}$-linear map $\bar{K}(\mathcal{C})\to\bar{K}(\mathcal{C})$ denoted again by $\mathbf{D}$. Note that $\mathbf{D}(u^n\xi)=u^{-n}\mathbf{D}(\xi)$ for any $\xi\in\bar{K}(\mathcal{C})$ and any $n\in\mathbf{Z}$.

Since $\mathcal{O}_1$ is closed, smooth, of pure dimension $\nu:=\dim\mathcal{B}$, we have from the definitions

$$\mathbf{D}(\mathbf{S}_1,\tau_1)=u^{-\nu}(\mathbf{S}_1,\tau_1).$$

2.8. Now let $t\in S$. We have $\bar{\mathcal{O}}_t=\mathcal{O}_t\cup\mathcal{O}_1$. Let

$$Y=\{(B_1,B_2,B_3,B_4)\in\mathcal{B}^4;(B_1,B_2)\in\bar{\mathcal{O}}_t,(B_3,B_4)\in\bar{\mathcal{O}}_t\}.$$

Define $\tilde\phi:Y\to Y$ by

$$\tilde\phi(B_1,B_2,B_3,B_4)=(\phi(B_4),\phi(B_3),\phi(B_2),\phi(B_1)).$$

This is the Frobenius map for an $\mathbf{F}_p$-rational structure on Y. Define $\pi,\pi':Y\to\mathcal{B}\times\mathcal{B}$ by

$$\pi(B_1,B_2,B_3,B_4)=(B_2,B_3),\quad \pi'(B_1,B_2,B_3,B_4)=(B_1,B_4).$$

We have $\pi\tilde\phi=\tilde\phi\pi,\pi'\tilde\phi=\tilde\phi\pi'$. (The $\tilde\phi$ to the left of π or π' is as in 2.3.) For $\mathcal{S}\in\mathcal{C}_0$ and $i\in\mathbf{Z}$ let $\mathcal{S}^i=R^i\pi'_!\pi^*\mathcal{S}$; note that $\mathcal{S}^i\in\mathcal{C}_0$. Let $(\mathcal{S},\Psi)\in\mathcal{C}_2$. For $i\in\mathbf{Z}$, $\Psi:\phi^{2*}\mathcal{S}\to\mathcal{S}$ induces an isomorphism $\phi^{2*}\pi^*\mathcal{S}\to\pi^*\mathcal{S}$ (since $\pi\phi^2=\phi^2\pi$) and this induces for any i an isomorphism ${}^i\Psi:\phi^{2*}\mathcal{S}^i\to\mathcal{S}^i$ (since $\pi'\phi^2=\phi^2\pi'$). A standard argument shows that $(\mathcal{S}^i,{}^i\Psi)\in\mathcal{C}_2$. It follows that if $(\mathcal{S},\Phi)\in\mathcal{C}$ and $i\in\mathbf{Z}$, then the isomorphism ${}^i\Phi:\tilde\phi^*\mathcal{S}^i\to\mathcal{S}^i$ induced by Φ satisfies $(\mathcal{S}^i,{}^i\Phi)\in\mathcal{C}$. (Setting $\Psi=\tilde\phi^*(\Phi)\Phi:\tilde\phi^{2*}\mathcal{S}\xrightarrow{\sim}\mathcal{S}$, we have ${}^i\Psi=\tilde\phi^*({}^i\Phi)({}^i\Phi):\tilde\phi^{2*}\mathcal{S}\xrightarrow{\sim}\mathcal{S}$.) Hence there is a well defined $\mathbf{Z}$-linear map $\theta_t:K(\mathcal{C})\to K(\mathcal{C})$ such that $\theta_t(\mathcal{S},\Phi)=\sum_i(-1)^i(\mathcal{S}^i,{}^i\Phi)$ for all $(\mathcal{S},\Phi)\in\mathcal{C}$. From the definitions we have $\theta_t(u^n\xi)=u^n\theta_t(\xi)$ for any $\xi\in K(\mathcal{C})$, $n\in\mathbf{Z}$. From the known properties of Verdier duality we have that

$$\mathbf{D}(\theta_t(\xi))=u^{-2}\theta_t(\mathbf{D}(\xi))\text{ for all }\xi\in K(\mathcal{C}).$$

(We use that π' is proper and that π is smooth with connected fibres of dimension 2.)

If $(\mathcal{S},\Psi)\in\mathcal{C}_2$ and $\Theta(\mathcal{S},\Psi)=(\mathcal{S}\oplus\tilde\phi^*\mathcal{S},\Phi)$ then for any i we have

$$(\mathcal{S}\oplus\tilde\phi^*\mathcal{S})^i,{}^i\Phi)=\Theta(\mathcal{S}^i,{}^i\Psi).$$

Moreover if $(\mathcal{S},\Phi)\in\mathcal{C}$ then for any i we have

$$(\mathcal{S}^i,{}^i(-\Phi))=(\mathcal{S}^i,-{}^i\Phi).$$

It follows that θ_t carries $K'(\mathcal{C})$ into itself hence it induces an $\mathcal{A}$-linear map $\bar K(\mathcal{C})\to\bar K(\mathcal{C})$ denoted again by θ_t.

Now let s be an odd integer ≥ 1 and let $q=p^s$. We define a linear map $\theta_{t,s}:\mathcal{F}_q\to\mathcal{F}_q$ by $f\mapsto f'$ where

$$f'(B_1,B_4)=\sum_{(B_2,B_3)\in(\mathcal{B}\times\mathcal{B})^{\tilde\phi^s};(B_1,B_2)\in\bar{\mathcal{O}}_t,(B_3,B_4)\in\bar{\mathcal{O}}_t} f(B_2,B_3)$$

for any $(B_1,B_4)\in(\mathcal{B}\times\mathcal{B})^{\tilde\phi^s}$.

Let $(\mathcal{S},\Phi)\in\mathcal{C}$ and define $(\mathcal{S}^i,{}^i\Phi)\in\mathcal{C}$ as above. Using Grothendieck's sheaves-functions dictionary, we see that

$$\theta_{t,s}(\chi_s(\mathcal{S},\Phi))=\sum_i(-1)^i\chi_s(\mathcal{S}_i,{}^i\Phi).$$

It follows that

$$\theta_{t,s}(\chi_s(\xi))=\chi_s(\theta_t(\xi))$$

for any $\xi\in\bar K(\mathcal{C})$. From the definition of the $\mathfrak{H}'_q$-module structure on $\mathcal{F}_q$ in 1.1 we see that $\theta_{t,s}(m)=(T_t+1)(m)$ for any $m\in\mathcal{F}_q$. Thus for any $\xi\in\bar K(\mathcal{C})$ we have

$$\chi_s(\theta_t(\xi))=(T_t+1)(\chi_s(\xi)).$$

2.9. Using 2.6(b) we identify $M=\bar K(\mathcal{C})$ as $\mathcal{A}$-modules in such a way that for any $w\in\mathbf{I}$, the element $a_w\in M$ becomes the element $(\mathbf{S}_w,\tau_1)$ of $\bar K(\mathcal{C})$. Then $\mathbf{D}$ in 2.7 and θ_t in 2.8 become $\mathbf{Z}$-linear maps $M\to M$ (denoted again by $\mathbf{D},\theta_t$). From 2.8 we see that for any $s=1,3,5,\dots$ and any $m\in M$, the image of $\theta_t(m)$ in M_{p^s} is equal to the image of $(T_t+1)m$ in M_{p^s}. It follows that

$$\theta_t(m) = (T_t + 1)m \quad \text{in} \quad M.$$

Note also that $\theta_t : M \to M$ is $\mathcal{A}$-linear while $\mathbf{D}(u^n m) = u^{-n}\mathbf{D}(m)$ for all $m \in M$, $n \in \mathbf{Z}$. From 2.8 we see that $\mathbf{D}(\theta_t(m)) = u^{-2}\theta_t(\mathbf{D}(m))$ for all $m \in M$. Equivalently we have $\mathbf{D}((T_t + 1)(m)) = u^{-2}(T_t + 1)(\mathbf{D}(m))$ for all $m \in M$. (Here t is any element of S.) From 2.7 we have $\mathbf{D}(a_1) = u^{-\nu}a_1$. We now define $^- : M \to M$ by $m \mapsto u^\nu \mathbf{D}(m)$. This has the properties described in the first sentence of 0.2(b). Thus the existence part of that sentence is established. To prove the uniqueness part of that sentence it is enough to verify the following statement.

Let $f : M \to M$ be a $\mathbf{Z}$-linear map such that $f(u^n m) = u^{-n}\overline{m}$ for all $m \in M$, $n \in \mathbf{Z}$, $f(a_1) = 0$ and $f((T_t + 1)m) = u^{-2}(T_t + 1)f(m)$ for all $m \in M, t \in S$. Then $f = 0$.

We must show that $f(a_w) = 0$ for any $w \in \mathbf{I}$. We can assume that $w \neq 1$ and that $f(a_{w'}) = 0$ for any $w' \in \mathbf{I}$ such that $w' < w$. We can find $t \in S$ such that $wt < w$. If $tw \neq wt$ then applying 0.2(iii) with w, s replaced by twt, t we have

$$f(a_{twt} + a_w) = f((T_t + 1)(a_{twt})) = u^{-2}(T_t + 1)f(a_{twt}) = 0$$

(since $twt < w$) hence $f(a_w) = 0$. If $tw = wt$ then applying 0.2(i) with w, s replaced by wt, t we have

$$f((u + 1)(a_{wt} + a_w)) = f((T_t + 1)(a_{wt})) = 0$$

hence $(u^{-1} + 1)f(a_w) = 0$ so that $f(a_w) = 0$. This completes the proof of the first sentence in 0.2(b). The second sentence in 0.2(b) follows from the fact that $D\mathbf{S}_w$ has support contained in $\bar{\mathcal{O}}_w$ and from the fact that $\dim(\mathcal{O}_w) = l(w) + \nu$. We prove the third sentence in 0.2(b). Let $\mathfrak{H}'_0$ be the set of all $h \in \mathfrak{H}'$ such that $\overline{hm} = \overline{h}\overline{m}$ for any $m \in M$. Clearly $\mathfrak{H}'_0$ is an $\mathcal{A}$-subalgebra with 1 of $\mathfrak{H}'$. By definition, $\mathfrak{H}'_0$ contains $T_t + 1$ for any $t \in S$. Since the elements $T_t + 1$ generate $\mathfrak{H}'$ as an $\mathcal{A}$-algebra we see that $\mathfrak{H}'_0 = \mathfrak{H}'$, as desired. We prove the fourth sentence in 0.2(b). Define $f' : M \to M$ by $f'(m) = \overline{\overline{m}}$. This is an $\mathfrak{H}'$-linear map $M \to M$ such that $f'(a_1) = a_1$. We must show that $f' = 1$. It is enough to show that $f' = 1$ after the scalars are extended to $\mathbf{Z}[u, u^{-1}, (u + 1)^{-1}]$. But this follows the fact that

M (with scalars thus extended) is generated by a_1 as an $\mathfrak{H}'$-module. (We use the formulas in 0.2(a).) This completes the proof of 0.2(b) hence that of Theorem 0.2. $\square$

3. Proof of Theorem 0.3

3.1. In this section we fix $w \in \mathbf{I}$. Recall that we have morphisms $\sigma, \phi, \tilde{\phi} = \sigma\phi = \phi\sigma$ of $\mathcal{B} \times \mathcal{B}$ into itself, see 2.3. Clearly there is a unique isomorphism $k^w : \sigma^* \mathbf{S}^\sharp_w \xrightarrow{\sim} \mathbf{S}^\sharp_w$, (resp. $m^w : \phi^* \mathbf{S}^\sharp_w \xrightarrow{\sim} \mathbf{S}^\sharp_w$, $i^w : \tilde{\phi}^* \mathbf{S}^\sharp_w \xrightarrow{\sim} \mathbf{S}^\sharp_w$) such that the induced isomorphisms

$$(k^w_h)_y : V_y^{\mathcal{H}^h \mathbf{S}^\sharp_w} \xrightarrow{\sim} V_y^{\mathcal{H}^h \mathbf{S}^\sharp_w}$$

$$\text{(resp. } (m^w_h)_y : V_y^{\mathcal{H}^h \mathbf{S}^\sharp_w} \xrightarrow{\sim} V_y^{\mathcal{H}^h \mathbf{S}^\sharp_w},\ (i^w_h)_y : V_y^{\mathcal{H}^h \mathbf{S}^\sharp_w} \xrightarrow{\sim} V_y^{\mathcal{H}^h \mathbf{S}^\sharp_w})$$

defined for any $y \in \mathbf{I}, y \le w$ and $h \in 2\mathbf{N}$ satisfy $(k^w_0)_w = 1$ (resp. $(m^w_0)_w = 1$, $(i^w_0)_w = 1$). We have $(i^w_h)_y = (k^w_h)_y (m^w_h)_y = (m^w_h)_y (k^w_h)_y$. By [7, Thm. 4.2], $(m^w_h)_y$ is equal to $p^{h/2}$ times a unipotent transformation. Clearly, $(k^w_h)_y$ has square equal to 1. In particular, for any $h \in 2\mathbf{N}$, we have

$$\text{(a)} \qquad \begin{aligned} &(\mathcal{H}^h \mathbf{S}^\sharp_w, i^w_h) \in \mathcal{C}, \\ &(\mathcal{H}^h \mathbf{S}^\sharp_w, i^w_h) = \sum_{y \in \mathbf{I}; y \le w} P^\sigma_{y,w;h/2} u^{h/2} \mathbf{S}_y, \\ &\sum_{h \in 2\mathbf{N}} (\mathcal{H}^h \mathbf{S}^\sharp_w, i^w_h) = \sum_{y \in \mathbf{I}; y \le w} P^\sigma_{y,w} \mathbf{S}_y \in \bar{K}(\mathcal{C}) \end{aligned}$$

where

$$\begin{aligned} P^\sigma_{y,w;h/2} &= \operatorname{tr}((k^w_h)_y : V_y^{\mathcal{H}^h \mathbf{S}^\sharp_w} \to V_y^{\mathcal{H}^h \mathbf{S}^\sharp_w}) \in \mathbf{Z}, \\ P^\sigma_{y,w} &= \sum_{h \in 2\mathbf{N}} P^\sigma_{y,w;h/2} u^{h/2} \in \mathbf{Z}[u]. \end{aligned}$$

From the definition of $\mathbf{S}^\sharp_w$ we have (with notation of 2.7):

$$\sum_{h \in 2\mathbf{N}} \sum_{j \in \mathbf{Z}} (-1)^j (\mathcal{H}^j D \mathcal{H}^h \mathbf{S}^\sharp_w, (i^w_h)^{(j)}) = u^{-l(w)-\nu} \sum_{h \in 2\mathbf{N}} (\mathcal{H}^h \mathbf{S}^\sharp_w, i^w_h) \in \bar{K}(\mathcal{C})$$

that is

$$\mathbf{D}(\sum_{h\in 2\mathbf{N}}(\mathcal{H}^h\mathbf{S}^\sharp_w, i^w_h) = u^{-l(w)-\nu}\sum_{h\in 2\mathbf{N}}(\mathcal{H}^h\mathbf{S}^\sharp_w, i^w_h)\in \bar{K}(\mathcal{C}).$$

Hence, setting

$$\mathfrak{A}_w = \sum_{h\in 2\mathbf{N}}(\mathcal{H}^h\mathbf{S}^\sharp_w, i^w_h)\in \bar{K}(\mathcal{C})$$

we have

$$\mathbf{D}(\mathfrak{A}_w) = u^{-l(w)-\nu}\mathfrak{A}_w$$

that is

$$\overline{\mathfrak{A}_w} = u^{-l(w)}\mathfrak{A}_w$$

where we identify $\bar{K}(\mathcal{C}) = M$ as in 2.9. Under this identification the element $\mathfrak{A}_w \in M$ becomes

$$\mathfrak{A}_w = \sum_{y\in\mathbf{I}; y\le w} P^\sigma_{y,w}a_y \in M.$$

From the definition of $\mathbf{S}^\sharp_w$ we have $\deg P^\sigma_{y,w} \le (l(w)-l(y)-1)/2$ (if $y\in \mathbf{I}, y<w$) and $P^\sigma_{w,w}=1$. We see that the existence part of 0.3(a) is verified by the element $A_w = v^{-l(w)}\mathfrak{A}_w \in \underline{M}$ (recall that $v^2=u$).

3.2. We prove the uniqueness part of 0.3(a). Assume that we have an element $A'_w = v^{-l(w)}\sum_{y\in\mathbf{I};y\le w} P'^\sigma_{y,w}a_y \in \underline{M}$ ($P'^\sigma_{y,w}\in\mathbf{Z}[u]$) such that $\overline{A'_w} = A'_w$, $P'^\sigma_{w,w} = 1$ and for any $y\in\mathbf{I}$, $y<w$, we have $\deg P'^\sigma_{y,w} \le (l(w)-l(y)-1)/2$. We must show that $\mathcal{P}_{z,w}=0$ where $\mathcal{P}_{z,w} = P'^\sigma_{z,w} - P^\sigma_{z,w}$ for all $z\in\mathbf{I}, z\le w$.

We already know that $\mathcal{P}_{w,w}=0$. We can assume that $z<w$ and that $\mathcal{P}_{y,w}=0$ for any $y\in\mathbf{I}$ such that $z<y\le w$. With the notation in 0.2(b) we have

$$v^{l(w)}\sum_{y\in\mathbf{I};y\le w}\overline{\mathcal{P}_{y,w}}\sum_{y'\in\mathbf{I};y'\le y} r_{y',y}a_{y'} = v^{-l(w)}\sum_{y\in\mathbf{I};y\le w}\mathcal{P}_{y,w}a_y$$

hence

$$v^{l(w)}\sum_{y\in\mathbf{I};z\le y\le w}\overline{\mathcal{P}_{y,w}}r_{z,y} = v^{-l(w)}\mathcal{P}_{z,w}.$$

Using our inductive assumption this becomes

$$v^{l(w)}\overline{\mathcal{P}_{z,w}} r_{z,z} = v^{-l(w)}\mathcal{P}_{z,w}.$$

Using $r_{z,z} = v^{-2l(z)}$ this becomes

$$v^{l(w)-l(z)}\overline{\mathcal{P}_{z,w}} = v^{-l(w)+l(z)}\mathcal{P}_{z,w}.$$

Here the right hand side is in $v^{-1}\mathbf{Z}[v^{-1}]$ and the left hand side is in $v\mathbf{Z}[v]$ (we use that $z < w$). Hence both sides are zero. Thus $\mathcal{P}_{z,w} = 0$. This completes the proof of 0.3(a). Now 0.3(b) is immediate. $\square$

In the course of this proof we have also verified the following result.

Proposition 3.3. *For any $y \in \mathbf{I}$, $y \le w$, the polynomial $P^\sigma_{y,w}$ defined in* 0.3 *satisfies*

$$P^\sigma_{y,w} = \sum_{h\in 2\mathbf{N}} \mathrm{tr}((k^w_h)_y : V_y^{\mathcal{H}^h\mathbf{S}^\sharp_w} \to V_y^{\mathcal{H}^h\mathbf{S}^\sharp_w})u^{h/2} \in \mathbf{Z}[u].$$

Note that, by [7], the polynomial $P_{y,w}$ of [6] satisfies (for y, w as in the proposition):

$$P_{y,w} = \sum_{h\in 2\mathbf{N}} \dim(V_y^{\mathcal{H}^h\mathbf{S}^\sharp_w})u^{h/2} \in \mathbf{Z}[u].$$

3.4. Let $s \in S$ be such that $sw < w$ or equivalently $ws < w$. Let $y \in \mathbf{I}$ be such that $y \le w$. Then we have also $sy \le w$; moreover, if $sy \ne ys$ we have $sys \le w$. We show:

(a) *If $sy = ys$ then $P^\sigma_{y,w} = P^\sigma_{sy,w}$.*

(b) *If $sy \ne ys$ then $P^\sigma_{y,w} = P^\sigma_{sys,w}$.*

Let $\mathcal{P}$ be the variety of parabolic subgroups P of G such that for any Borel subgroups B, B' in P we have $(B, B') \in \bar{\mathcal{O}}_s$ and for some Borel subgroups B, B' in P we have $(B, B') \in \mathcal{O}_s$. Let $\rho : \mathcal{B} \to \mathcal{P}$ be the morphism $B \mapsto P$ where $P \in \mathcal{P}$ contains B. Let $\tilde\rho = \rho\times\rho : \mathcal{B}\times\mathcal{B} \to \mathcal{P}\times\mathcal{P}$. This map commutes with the diagonal actions of G and $\tilde\rho\sigma = \sigma'\tilde\rho$ where $\sigma' : \mathcal{P}\times\mathcal{P} \to \mathcal{P}\times\mathcal{P}$ is $(P, P') \mapsto (P', P)$. We have $\bar{\mathcal{O}}_w = \tilde\rho^{-1}(X)$ where $X = \tilde\rho(\bar{\mathcal{O}}_w)$, a closed subvariety of $\mathcal{P}\times\mathcal{P}$. Let $X_0 = \tilde\rho(\mathcal{O}_w)$, the unique open G-orbit in X. Let K be the intersection cohomology complex of X with coefficients in $\mathbf{Q}_l$ (on

X_0) extended by 0 on $\mathcal{P}\times\mathcal{P}-X$. We have $\mathbf{S}_w^\sharp=\tilde{\rho}^*K$. Let $Z=\tilde{\rho}(\mathcal{O}_y)$; we have $\sigma'(Z)=Z$. For any $h\in 2\mathbf{N}$ there is a canonical vector space V' with a linear involutive σ'-action which is canonical isomorphic to the stalk of $\mathcal{H}^hK$ at any $z\in Z$. From the definitions we have canonically $V_y^{\mathcal{H}^h\mathbf{S}_w^\sharp}=V'$ and $V_{sy}^{\mathcal{H}^h\mathbf{S}_w^\sharp}=V'$ if $sy=ys$, (resp. $V_{sys}^{\mathcal{H}^h\mathbf{S}_w^\sharp}=V'$ if $sy\ne ys$); moreover under these identifications the operators $(k_h^w)_y$ and $(k_h^w)_{sy}$ if $sy=ys$ (resp. $(k_h^w)_{sys}$ if $sy\ne ys$) correspond to the σ'-action on V'. It follows that

$$\begin{aligned}&\mathrm{tr}((k_h^w)_y:V^{\mathcal{H}^h\mathbf{S}_w^\sharp}y\to V_y^{\mathcal{H}^h\mathbf{S}_w^\sharp})=\mathrm{tr}(\sigma':V'\to V')\\ &=\ \mathrm{tr}((k_h^w)_{sy}:V_{sy}^{\mathcal{H}^h\mathbf{S}_w^\sharp}\to V_{sy}^{\mathcal{H}^h\mathbf{S}_w^\sharp})\end{aligned}$$

if $sy=ys$ and

$$\begin{aligned}&\mathrm{tr}((k_h^w)_y:V^{\mathcal{H}^h\mathbf{S}_w^\sharp}y\to V_y^{\mathcal{H}^h\mathbf{S}_w^\sharp})=\mathrm{tr}(\sigma':V'\to V')\\ &=\ \mathrm{tr}((k_h^w)_{sys}:V_{sys}^{\mathcal{H}^h\mathbf{S}_w^\sharp}\to V_{sys}^{\mathcal{H}^h\mathbf{S}_w^\sharp})\end{aligned}$$

if $sy\ne ys$. This implies (a) in view of 3.3.

4. The Action of $u^{-1}(T_s+1)$ in the Basis (A_w)

4.1. Let $y,w\in\mathbf{I}$. We set $\delta_{y,w}=1$ if $y=w$, $\delta_{y,w}=0$ if $y\ne w$, $\delta'_{y,w}=1-\delta_{y,w}$. When $y\le w$ we set $\pi_{y,w}=v^{-l(w)+l(y)}P^\sigma_{y,w}$ so that $\pi_{y,w}\in v^{-1}\mathbf{Z}[v^{-1}]$ if $y<w$ and $\pi_{w,w}=1$; when $y\not\le w$ we set $\pi_{y,w}=0$. In any case we have

(a) $\pi_{y,w}=\delta_{y,w}+\mu'(y,w)v^{-1}+\mu''(y,w)v^{-2}\bmod v^{-3}\mathbf{Z}[v^{-1}]$
  where $\mu'(y,w)\in\mathbf{Z},\mu''(y,w)\in\mathbf{Z}$. Note that

(b) $\mu'(y,w)\ne 0\implies y<w,l(y)\ne l(w)\bmod 2$,

(c) $\mu''(y,w)\ne 0\implies y<w,l(y)=l(w)\bmod 2$.

For $w\in\mathbf{I}$ we set $a'_w=v^{-l(w)}a_w$ so that $A_w=\sum_{y\in\mathbf{I}}\pi_{y,w}a'_y$.

4.2. In this section we fix $s\in S$. We set $c_s=v^{-2}(T_s+1)\in\underline{\mathfrak{H}}'$. The formulas in 0.2(a) (with $w\in\mathbf{I}$) can be rewritten as follows.

$c_sa'_w=(v+v^{-1})a'_{sw}+(1+v^{-2})a'_w$ if $sw=ws>w$;

$c_sa'_w=(v-v^{-1})a'_{sw}+(v^2-1)a'_w$ if $sw=ws<w$;

$c_sa'_w=a'_{sws}+v^{-2}a'_w$ if $sw\ne ws>w$;

$c_s a'_w = a'_{sws} + v^2 a'_w$ if $sw \neq ws < w$.

4.3. For any $y, w \in \mathbf{I}$ such that $sy < y < sw > w$ we define $\mathcal{M}^s_{y,w} \in \underline{\mathcal{A}}$ by:

$$\mathcal{M}^s_{y,w} = \mu''_{y,w} - \sum_{x \in \mathbf{I}; y<x<w, sx<x} \mu'_{y,x}\mu'_{x,w} - \delta_{w,sws}\mu'_{y,sw} + \mu'_{sy,w}\delta_{sy,ys}$$

if $l(y) = l(w) \bmod 2$,

$$\mathcal{M}^s_{y,w} = \mu'_{y,w}(v + v^{-1})$$

if $l(w) \neq l(y) \bmod 2$.

Theorem 4.4. *Recall that $s \in S$. Let $w \in \mathbf{I}$.*

(a) *If $sw = ws > w$ then $c_s A_w = (v + v^{-1})A_{sw} + \sum_{z \in \mathbf{I}; sz<z<sw} \mathcal{M}^s_{z,w} A_z$.*
(b) *If $sw \neq ws > w$ then $c_s A_w = A_{sws} + \sum_{z \in \mathbf{I}; sz<z<sw} \mathcal{M}^s_{z,w} A_z$.*
(c) *If $ws < w$ then $c_s A_w = (v^2 + v^{-2})A_w$.*

We prove (c). For $z \in \mathbf{I}, sz < z$ we set $\tilde{a}'_z = a'_z + v^{-1}a'_{sz}$ (if $sw = ws$) and $\tilde{a}'_z = a'_z + v^{-2}a'_{szs}$ (if $sz \neq zs$). By 3.4 we have

(d) $A_z = \tilde{a}'_z + \underline{\mathcal{A}}$-linear combination of elements $\tilde{a}'_y$ with $y \in \mathbf{I}$, $sy < y < z$.

It follows that the elements $A_z (z \in \mathbf{I}, sz < z)$ span the same $\underline{\mathcal{A}}$-submodule $\underline{M}'$ of $\underline{M}$ as the elements $\tilde{a}'_z (z \in \mathbf{I}, sz < z)$. To show (c) it is enough to show that $c_s - (v^2 + v^{-2})$ acts as 0 on $\underline{M}'$; hence it is enough to show that $(c_s - (v^2 + v^{-2}))\tilde{a}'_z = 0$ for any $z \in \mathbf{I}, sz < z$. But this follows from 4.2. This proves (c).

In the rest of the proof we assume that $sw > w$. Note that

$$c_s A_w = \sum_{y \in \mathbf{W}; y \leq w} \pi_{y,w} c_s a'_y$$

hence using 4.2, $c_s A_w$ is an $\underline{\mathcal{A}}$-linear combination of elements of the form $\tilde{a}'_z$ with $sz < z$ and with $z \leq sw$ (if $sw = ws$) or with $z \leq sws$ (if $sw \neq ws$). Using (d) it follows that $c_s A_w$ is an $\underline{\mathcal{A}}$-linear combination of elements of the form A_z with $sz < z$ and with $z \leq sw$ (if $sw = ws$) or with $z \leq sws$ (if $sw \neq ws$). For such z we have either $z = sw$ or $z = sws$ or $z < sw$. (To see this we can assume that $sw \neq ws$, $z < sws$. Then we must have $z \leq sw$ or $z \leq ws$; if $z \leq ws$ then taking inverses we obtain $z \leq sw$. Thus $z \leq sw$

in any case. We cannot have $z = sw$ since $sw \neq ws$; hence $z < sw$.) We see that $c_s A_w = \sum_{x \in \mathbf{I}; sx<x} m_x A_x$ where $m_x \in \underline{\mathcal{A}}$; moreover we have $m_x = 0$ unless $x = sw$ (if $sw = ws$), $x = sws$ (if $sw \neq ws$) or $x < sw$.

Since $\overline{c_s A_w} = c_s A_w$ we have $\sum_{x \in \mathbf{I}; sx<x} \bar{m}_x A_x = \sum_{x \in \mathbf{I}; sx<x} m_x A_x$ hence $\overline{m_x} = m_x$ for all $x \in \mathbf{I}$ such that $sx < x$. We have

$$\begin{aligned} c_s A_w = & \sum_{y \in \mathbf{I}; sy=ys>y} \pi_{y,w} c_s a'_y + \sum_{y \in \mathbf{I}; sy=ys<y} \pi_{y,w} c_s a'_y \\ & + \sum_{y \in \mathbf{I}; sy \neq ys>y} \pi_{y,w} c_s a'_y + \sum_{y \in \mathbf{I}; sy \neq ys<y} \pi_{y,w} c_s a'_y \end{aligned}$$

hence, using 4.2:

$$\begin{aligned} c_s A_w = & \sum_{y \in \mathbf{I}; sy=ys>y} \pi_{y,w}((v+v^{-1})a'_{sy} + (1+v^{-2})a'_y) \\ & + \sum_{y \in \mathbf{I}; sy=ys<y} \pi_{y,w}((v-v^{-1})a'_{sy} + (v^2-1)a'_y) \\ & + \sum_{y \in \mathbf{I}; sy \neq ys>y} \pi_{y,w}(a'_{sys} + v^{-2}a'_y) + \sum_{y \in \mathbf{I}; sy \neq ys<y} \pi_{y,w}(a'_{sys} + v^2 a'_y), \\ c_s A_w = & \sum_{y \in \mathbf{I}; sy=ys<y} \pi_{sy,w}(v+v^{-1})a'_y + \sum_{y \in \mathbf{I}; sy=ys>y} \pi_{y,w}(1+v^{-2})a'_y \\ & + \sum_{y \in \mathbf{I}; sy=ys>y} \pi_{sy,w}(v-v^{-1})a'_y + \sum_{y \in \mathbf{I}; sy=ys<y} \pi_{y,w}(v^2-1)a'_y \\ & + \sum_{y \in \mathbf{I}; sy \neq ys<y} \pi_{sys,w} a'_y + \sum_{y \in \mathbf{I}; sy \neq ys>y} \pi_{y,w} v^{-2} a'_y \\ & + \sum_{y \in \mathbf{I}; sy \neq ys>y} \pi_{sys,w} a'_y + \sum_{y \in \mathbf{I}; sy \neq ys<y} \pi_{y,w} v^2 a'_y. \end{aligned}$$

Thus,

$$\begin{aligned} c_s A_w = & \sum_{y \in \mathbf{I}; sy=ys<y} (\pi_{sy,w}(v+v^{-1}) + \pi_{y,w}(v^2-1))a'_y \\ & + \sum_{y \in \mathbf{I}; sy=ys>y} (\pi_{y,w}(1+v^{-2}) + \pi_{sy,w}(v-v^{-1}))a'_y \\ & + \sum_{y \in \mathbf{I}; sy \neq ys<y} (\pi_{sys,w} + \pi_{y,w} v^2)a'_y + \sum_{y \in \mathbf{I}; sy \neq ys>y} (\pi_{y,w} v^{-2} + \pi_{sys,w})a'_y. \end{aligned}$$

We have

$$\sum_{x\in\mathbf{I};sx<x} m_x A_x = \sum_{y\in\mathbf{I}}\sum_{x\in\mathbf{I};sx<x} m_x\pi_{y,x}a'_y.$$

It follows that for $y\in\mathbf{I}$ such that $ys<y$ we have

$$\begin{aligned}\sum_{x\in\mathbf{I};sx<x} m_x\pi_{y,x} &= \pi_{sy,w}(v+v^{-1})+\pi_{y,w}(v^2-1) \text{ if } sy=ys;\\ \sum_{x\in\mathbf{I};sx<x} m_x\pi_{y,x} &= \pi_{sys,w}+\pi_{y,w}v^2 \text{ if } sy\neq ys.\end{aligned}$$

For any $f\in\underline{\mathcal{A}}$ we define $f^+\in\mathbf{Z}[v]$ by $f-f^+\in v^{-1}\mathbf{Z}[v^{-1}]$. It follows that

$$\begin{aligned}\sum_{x\in\mathbf{I};sx<x}(m_x\pi_{y,x})^+ &= (\pi_{sy,w}(v+v^{-1}))^+ + (\pi_{y,w}(v^2-1))^+ \text{ if } sy=ys<y;\\ \sum_{x\in\mathbf{I};sx<x}(m_x\pi_{y,x})^+ &= \pi^+_{sys,w}+(\pi_{y,w}v^2)^+ \text{ if } sy\neq ys<y.\end{aligned}$$

Using 4.1(a) and that $y\neq w$ if $sy<y$ we deduce

$$\begin{aligned}&m_y^+ + \sum_{x\in\mathbf{I};sx<x,y<x}(m_x\pi_{y,x})^+ = \mu'_{sy,w}+\delta_{sy,w}v+\mu''_{y,w}+\mu'_{y,w}v \text{ if } sy=ys<y;\\ &\text{(e)}\\ &m_y^+ + \sum_{x\in\mathbf{I};sx<x,y<x}(m_x\pi_{y,x})^+ = \delta_{sys,w}+\mu''_{y,w}+\mu'_{y,w}v \text{ if } sy\neq ys<y.\end{aligned}$$

In particular we have

$$m_y^+ + \sum_{x\in\mathbf{I};sx<x,y<x}(m_x\pi_{y,x})^+ \in\mathbf{Z}+\mathbf{Z}v$$

for any $y\in\mathbf{I}$ such that $sy<y$. This shows by descending induction on $l(y)$ that $m_y^+\in\mathbf{Z}+\mathbf{Z}v$ for any $y\in\mathbf{I}$ such that $sy<y$. (Indeed, if we know that for $x\in\mathbf{I}$ such that $sx<x, y<x$ we have $m_x^+\in\mathbf{Z}+\mathbf{Z}v$, then $(m_x\pi_{y,x})^+\in\mathbf{Z}$.) Setting $m_y^+=m_y^0+m'_yv$ (with $m_y^0\in\mathbf{Z}$, $m'_y\in\mathbf{Z}$) for any $y\in\mathbf{I}$ such that $sy<y$, we can rewrite (e) as follows:

$$\begin{aligned}&m_y^0+m'_yv+\sum_{x\in\mathbf{I};sx<x,y<x} m'_x\mu'_{y,x}\\ &\quad= \delta_{sy,ys}\mu'_{sy,w}+\delta_{sy,ys}\delta_{sy,w}v+\delta'_{sy,ys}\delta_{sys,w}+\mu''_{y,w}+\mu'_{y,w}v.\end{aligned}$$

In particular,

$$m'_y = \mu'_{y,w} + \delta_{sy,ys}\delta_{sy,w}$$

for any $y \in \mathbf{I}$ such that $sy < y$. It follows that

$$\begin{aligned} m^0_y + \sum_{x\in\mathbf{I}; sx<x, y<x} (\mu'_{x,w} + \delta_{sx,xs}\delta_{sx,w})\mu'_{y,x} \\ = \delta_{sy,ys}\mu'_{sy,w} + \delta'_{sy,ys}\delta_{sys,w} + \mu''_{y,w}. \end{aligned}$$

Equivalently we have

$$\begin{aligned} m^0_y &= -\sum_{x\in\mathbf{I}; sx<x, y<x} \mu'_{y,x}\mu'_{x,w} - \delta_{w,sws}\mu'_{y,sw} \\ &\quad +\delta_{sy,ys}\mu'_{sy,w} + \delta'_{sy,ys}\delta_{sys,w} + \mu''_{y,w}. \end{aligned}$$

(We have used that $\sum_{x\in\mathbf{I}; sx<x,y<x} \delta_{sx,xs}\delta_{sx,w}\mu'_{y,x} = \delta_{w,sws}\mu'_{y,sw}$.) Since $\overline{m_y} = m_y$ we must have $m_y = m^0_y + m'_y(v+v^{-1})$ for $y \in \mathbf{I}, sy < y$. For $y \in \mathbf{I}$ such that $sy < y, l(w) \ne l(y) \bmod 2$ we deduce using 4.1(c) that

$$m_y = \mu'_{y,w}(v+v^{-1}) = \mathcal{M}^s_{y,w} \text{ if } y < sw, \quad m_y = v + v^{-1}$$

if $y = sw$, hence $ws = sw$. For $y \in \mathbf{I}$ such that $sy < y, l(w) = l(y) \bmod 2$ we deduce using 4.1(b),(c) that

$$m_y = \mu''_{y,w} - \sum_{x\in\mathbf{I}; sx<x, y<x} \mu'_{y,x}\mu'_{x,w} - \delta_{w,sws}\mu'_{y,sw} + \delta_{sy,ys}\mu'_{sy,w} + \delta'_{sy,ys}\delta_{sys,w}.$$

If $ws \ne sw$ and $y = sws$ we deduce that $m_y = 1$. If $y \in \mathbf{I}, sy < y, y < sw, l(y) = l(w) \bmod 2$ then

$$m_y = \mu''_{y,w} - \sum_{x\in\mathbf{I}; sx<x, y<x} \mu'_{y,x}\mu'_{x,w} - \delta_{w,sws}\mu'_{y,sw} + \delta_{sy,ys}\mu'_{sy,w} = \mathcal{M}^s_{y,w}.$$

We see that $m_y = \mathcal{M}^s_{y,w}$ for any $y \in \mathbf{I}$ such that $sy < y < sw$. We also see that $m_{sw} = v + v^{-1}$ if $sw = ws$ and $m_{sws} = 1$ if $sw \ne ws$. This completes the proof of the theorem. ☐

4.5. We now present an algorithm for compute the polynomials $P^\sigma_{y,w}$ for $y \le w$ in $\mathbf{I}$. It will be convenient to state this in terms of the elements

$\pi_{y,w} = v^{-l(w)+l(y)} P^{\sigma}_{y,w} \in \mathbf{Z}[v^{-1}]$ (see 4.1). Recall that $\pi_{y,w}$ is defined to be 0 if $y, w \in \mathbf{I}, y \not\leq w$.

We can restate Theorem 4.4(a),(b) as follows. (Recall that $s \in S$, $w \in \mathbf{I}$, $sw > w$.)

$$\begin{aligned}
&\sum_{y\in\mathbf{I}; sy=ys<y} (\pi_{sy,w}(v+v^{-1}) + \pi_{y,w}(v^2-1))a'_y \\
&\quad + \sum_{y\in\mathbf{I}; sy=ys>y} (\pi_{y,w}(1+v^{-2}) + \pi_{sy,w}(v-v^{-1}))a'_y \\
&\quad + \sum_{y\in\mathbf{I}; sy\neq ys<y} (\pi_{sys,w} + \pi_{y,w}v^2)a'_y + \sum_{y\in\mathbf{I}; sy\neq ys>y} (\pi_{y,w}v^{-2} + \pi_{sys,w})a'_y \\
&= \sum_{y\in\mathbf{I}} \sum_{x\in\mathbf{I}; sx<x<sw} \mathcal{M}^s_{x,w}\pi_{y,x}a'_y \\
&\quad + \sum_{y\in\mathbf{I}} (v+v^{-1})\pi_{y,sw}\delta_{sw,ws}a'_y + \sum_{y\in\mathbf{I}} \pi_{y,sws}(1-\delta_{sw,ws})a'_y.
\end{aligned}$$

It follows that for any $y \in \mathbf{I}$, the expression

$$(v+v^{-1})\pi_{y,sw}\delta_{sw,ws} + \pi_{y,sws}\delta'_{sw,ws}$$

is equal to

$$\begin{aligned}
&-\sum_{x\in\mathbf{I}; sx<x<sw} \mathcal{M}^s_{x,w}\pi_{y,x} + \pi_{sy,w}(v+v^{-1}) + \pi_{y,w}(v^2-1) \text{ if } sy=ys<y, \\
&-\sum_{x\in\mathbf{I}; sx<x<sw} \mathcal{M}^s_{x,w}\pi_{y,x} + \pi_{y,w}(1+v^{-2}) + \pi_{sy,w}(v-v^{-1}) \text{ if } sy=ys>y, \\
&-\sum_{x\in\mathbf{I}; sx<x<sw} \mathcal{M}^s_{x,w}\pi_{y,x} + \pi_{sys,w} + \pi_{y,w}v^2 \text{ if } sy\neq ys<y, \\
&-\sum_{x\in\mathbf{I}; sx<x<sw} \mathcal{M}^s_{x,w}\pi_{y,x} + \pi_{y,w}v^{-2} + \pi_{sys,w} \text{ if } sy\neq ys>y.
\end{aligned}$$

We want show that the formulas above determine uniquely the quantities $\pi_{y,sw}$ (resp. $\pi_{y,sws}$) assuming that $y \in \mathbf{I}$ and that $sw = ws$ (resp. $sw \neq ws$) and assuming that the quantities $\pi_{y',w'}$ are known for any $w' \in \mathbf{I}$ such that $l(w') < l(ws)$ (resp. $l(w') < l(sws)$) and any $y' \in \mathbf{I}$. Then the quantities $\mathcal{M}^s_{x,w}$ in these formulas are also known except for a part of them given by $\delta_{ws,sw}\mu'_{x,sw}$ which is not known. If in the formulas above we replace the terms that are assumed to be known by a symbol $\spadesuit$ we obtain

(a) $$(v+v^{-1})\pi_{y,sw} = \sum_{x\in\mathbf{I}; sx<x<sw} \mu'_{x,sw}\pi_{y,x} + \spadesuit \text{ if } ws = sw.$$

$$\pi_{y,sws} = \spadesuit \text{ if } sw \neq ws.$$

We can now assume that $sw = ws$. In this case we determine the quantities $\pi_{y,sw}$ by descending induction on $l(y)$. (We can assume that $y < sw$ since $\pi_{y,sw} = 1$ for $y = sw$.) Thus we can assume that $\pi_{y,sw}$ (hence also $\mu'_{y,sw}$) is known when y is replaced by $x \in \mathbf{I}$ such that $y < x < sw$. Since in the sum over x in (a) we can restrict to those x such that $y \le x$ we see that (a) becomes

$$(v+v^{-1})\pi_{y,sw} - \mu'(y,sw) = \sum_{x\in\mathbf{I}; sx<x<sw, y<x} \mu'_{x,sw}\pi_{y,x} + \spadesuit$$

that is

$$(v+v^{-1})\pi_{y,sw} - \mu'(y,sw) = \spadesuit.$$

Let us write $\pi_{y,sw} = \sum_{n\ge1} c_n v^{-n}$ where $c_n \in \mathbf{Z}$ are zero for all but finitely many n; note that $c_1 = \mu'(y,sw)$. (Recall that $y < sw$.) It follows that

$$\sum_{n\ge1} c_n v^{-n+1} + \sum_{n\ge1} c_n v^{-n-1} - c_1 = \spadesuit$$

so that $c_2 = \spadesuit$, $c_1 + c_3 = \spadesuit$, $c_2 + c_4 = \spadesuit$, $c_3 + c_5 = \spadesuit$, $c_4 + c_6 = \spadesuit$, $\dots$. It follows that $c_{2k} = \spadesuit$ for $k = 1, 2, \dots$ and, since $c_{2t+1} = 0$ for large t we have also $c_{2k-1} = \spadesuit$ for $k = 1, 2, \dots$. Thus $c_i = \spadesuit$ for $i = 1, 2, \dots$ so that $\pi_{y,sw} = \spadesuit$.

The procedure above gives an algorithm to compute $\pi_{y,z}$ for any $y, z \in \mathbf{I}$ such that $y \le z$. Indeed, if $z = 1$ then $y = 1$ and $\pi_{y,z} = 1$. If $z \neq 1$ then we can find $s \in S$ such that $sz < z$. Setting $w = zs$ (if $zs = sz$) or $w = szs$ (if $zs \neq sz$) we see that $\pi_{y,z}$ is determined by the inductive procedure above.

5. Relation with Two-sided Cells

5.1. For any $w \in W$ let $\dot{c}_w = v^{-l(w)} \sum_{y\in W; y\le w} P_{y,w}(v^2)T_y \in \underline{\mathfrak{H}}$ (compare [6]); similarly let $c_w = u^{-l(w)} \sum_{y\in W; y\le w} P_{y,w}(u^2)T_y \in \underline{\mathfrak{H}}'$. The elements

$\dot{c}_w(w \in W)$ form an $\underline{\mathcal{A}}$-basis of $\underline{\mathfrak{H}}$; the elements $c_w(w \in W)$ form an $\underline{\mathcal{A}}$-basis of $\underline{\mathfrak{H}}'$. For z, w in W we write (in the algebra $\underline{\mathfrak{H}}$):

$$\dot{c}_z \dot{c}_w \dot{c}_{z^{-1}} = \sum_{w' \in W} h_{z,w,w'} \dot{c}_{w'}$$

where $h_{z,w,w'} \in \mathbf{N}[v, v^{-1}]$. For $z \in W, w \in \mathbf{I}$ we write (using the $\underline{\mathfrak{H}}'$-module structure on $\underline{M}$):

$$c_z A_w = \sum_{w' \in \mathbf{I}} f_{z,w,w'} A_{w'}$$

where $f_{z,w,w'} \in \underline{\mathcal{A}}$ are related to $h_{z,w,w'}$ as follows. For $z \in W$, $w, w' \in \mathbf{I}$ we write $h_{z,w,w'} = \sum_{n \in \mathbf{Z}} b_n v^n$, $f_{z,w,w'} = \sum_{n \in \mathbf{Z}} b'_n v^n$ where $b_n \in \mathbf{N}, b'_n \in \mathbf{Z}$ are zero for all but finitely many n. One can show that for each n we have $b_n = b_n^+ + b_n^-$, $b'_n = b_n^+ - b_n^-$ for some $b_n^+ \in \mathbf{N}, b_n^- \in \mathbf{N}$. (This is similar to the relation between $P_{y,w}$ and $P^\sigma_{y,w}$ for $y, w \in \mathbf{I}$. It is also analogous to the phenomenon described in [12, 16.3(a),(b)].) In particular,

(a) *If for some n we have $b_n = 0$, then $b'_n = 0$. Hence if $f_{z,w,w'} \neq 0$, then $h_{z,w,w'} \neq 0$.*

(b) *If for some n we have $b_n = 1$, then $b'_n = \pm 1$.*

5.2. Let c be a two-sided cell of W, see [6]. For $y, w \in W$ we shall write $y \preceq w$ instead of $y \leq_{LR} w$ ($\leq_{LR}$ is the preorder defined in [6]). For $y \in W$ we write $y \preceq c$ instead of: $y \preceq w$ for some $w \in c$. For $y \in W$ we write $y \prec c$ instead of: $y \preceq c$ and yc.

Let $\underline{\mathfrak{H}}'^{\preceq c}$ be the $\underline{\mathcal{A}}$-submodule of $\mathcal{H}'$ spanned by the elements $c_{w'}$ where $w' \in W$ is such that $w' \preceq c$. Let $\underline{\mathfrak{H}}'^{\prec c}$ be the $\underline{\mathcal{A}}$-submodule of $\underline{\mathfrak{H}}'$ spanned by the elements $c_{w'}$ where $w' \in W$ is such that $w' \prec c$. Note that $\underline{\mathfrak{H}}'^{\preceq c}, \underline{\mathfrak{H}}'^{\prec c}$ are two-sided ideals of $\underline{\mathfrak{H}}'$. Hence $\underline{\mathfrak{H}}'^{\preceq c}/\underline{\mathfrak{H}}'^{\prec c}$ is naturally an $\underline{\mathfrak{H}}'$-bimodule, in particular a left $\underline{\mathfrak{H}}'$-module.

Let $\underline{M}^{\preceq c}$ be the $\underline{\mathcal{A}}$-submodule of $\underline{M}$ spanned by the elements $A_{w'}$ where $w' \in \mathbf{I}$, $w' \preceq c$. Let $\underline{M}^{\prec c}$ be the $\underline{\mathcal{A}}$-submodule of $\underline{M}$ spanned by the elements $A_{w'}$ where $w' \in \mathbf{I}$, $w' \prec c$.

From 5.1(a) we see that for $z \in W$, $w \in \mathbf{I}$, the element $c_z A_w$ is an $\underline{\mathcal{A}}$-linear combination of elements $A_{w'}$ with $w' \in \mathbf{I}, w' \preceq w$. In particular, $\underline{M}^{\preceq c}, \underline{M}^{\prec c}$ are $\underline{\mathfrak{H}}'$-submodules of $\underline{M}$. Hence $\underline{M}^{\preceq c}/\underline{M}^{\prec c}$ is naturally an $\underline{\mathfrak{H}}'$-module.

Let $\alpha \in \mathbf{N}$ be the value of the $\mathbf{a}$-function [12, §13] on c. Let $\eta \in \mathbf{I} \cap c$. We define an $\underline{\mathfrak{H}}'$-linear map $\tau_\eta : \underline{\mathfrak{H}}'^{\preceq c} \to \underline{M}^{\preceq c}$ by $\xi \mapsto v^{2\alpha} \xi A_\eta$ (we use the $\underline{\mathfrak{H}}'$-module structure on $\underline{M}$). From 5.1(a) we see that if $\xi \in \underline{\mathfrak{H}}'^{\prec c}$ then $\xi A_\eta \in \underline{M}^{\prec c}$. Thus τ_η restricts to an $\underline{\mathfrak{H}}'$-linear map $\underline{\mathfrak{H}}'^{\prec c} \to \underline{M}^{\prec c}$ hence it induces an $\underline{\mathfrak{H}}'$-linear map $\underline{\mathfrak{H}}'^{\preceq c}/\underline{\mathfrak{H}}'^{\prec c} \to \underline{M}^{\preceq c}/\underline{M}^{\prec c}$ denoted again by τ_η. Let d be the unique distinguished involution in the same left cell as η (hence in the same right cell as η). From the known properties of distinguished involutions (see [12, §15]) we see that the following holds in $\underline{\mathfrak{H}}$.

$$v^{2\alpha}\dot{c}_d\dot{c}_\eta\dot{c}_d = \dot{c}_\eta + \xi + \xi'$$

where $\xi \in \sum_{x\in c} v\mathbf{Z}[v]\dot{c}_x$ and $\xi' \in \underline{\mathfrak{H}}^{\prec c}$. Using now the results in 5.1 we deduce that

$$v^{2\alpha}c_d A_\eta = \pm A_\eta + m_\eta + m'$$

where $m_\eta \in \sum_{x\in c\cap\mathbf{I}} v\mathbf{Z}[v]A_x$ and $m' \in \underline{M}^{\prec c}$. Thus we have

$$\tau_\eta(c_d) = \pm A_\eta + m_\eta$$

where m_η is as above. Now let $\tau : \oplus_{\eta\in c\cap\mathbf{I}}\underline{\mathfrak{H}}'^{\preceq c}/\underline{\mathfrak{H}}'^{\prec c} \to \underline{M}^{\preceq c}/\underline{M}^{\prec c}$ be the $\underline{\mathfrak{H}}'$-linear map whose restriction to the η-summand is τ_η. The image of this map contains the elements $\pm A_\eta + m_\eta$ ($\eta \in c\cap\mathbf{I}$) which clearly form a basis of $\mathbf{Z}[[v]] \otimes_{\underline{\mathcal{A}}} (\underline{M}^{\preceq c}/\underline{M}^{\prec c})$: the $(c\cap\mathbf{I}) \times (c\cap\mathbf{I})$ matrix whose η,η'-entry (in $\mathbf{Z}[v]$) is the $A_{\eta'}$-coordinate of $\pm A_\eta + m_\eta$ has determinant ± 1 plus an element in $v\mathbf{Z}[v]$, hence is invertible in $\mathbf{Z}[[v]]$. Thus after extension of scalars to $\mathbf{Z}[[v]]$, τ is surjective. Hence after extension of scalars to the quotient field of $\mathbf{Z}[[v]]$, or to the quotient field $\mathbf{Q}(v)$ of $\underline{\mathcal{A}}$, τ is surjective. We see that

(a) *the $\mathbf{Q}(v)\otimes_{\underline{\mathcal{A}}}\underline{\mathfrak{H}}'$-module $\mathbf{Q}(v)\otimes_{\underline{\mathcal{A}}}(\underline{M}^{\preceq c}/\underline{M}^{\prec c})$ is a direct sum of irreducible $\mathbf{Q}(v) \otimes_{\underline{\mathcal{A}}} \underline{\mathfrak{H}}'$-modules which appear in the $\mathbf{Q}(v) \otimes_{\underline{\mathcal{A}}} \underline{\mathfrak{H}}'$-module $\mathbf{Q}(v) \otimes_{\underline{\mathcal{A}}} (\underline{\mathfrak{H}}'^{\preceq c}/\underline{\mathfrak{H}}'^{\prec c})$ carried by the two-sided cell c.*

5.3. In this subsection we assume that W is a Weyl group of type A_{n-1}, $n \geq 2$. In this case for any two sided cell c, the $\mathbf{Q}(v)\otimes_{\underline{\mathcal{A}}}\underline{\mathfrak{H}}'$-module $\mathbf{Q}(v)\otimes_{\underline{\mathcal{A}}} (\underline{\mathfrak{H}}'^{\preceq c}/\underline{\mathfrak{H}}'^{\prec c})$ is known to be a direct sum of copies of a single simple module E_c. Hence from 5.2(a) we deduce that the $\mathbf{Q}(v) \otimes_{\underline{\mathcal{A}}} \underline{\mathfrak{H}}'$-module $\mathbf{Q}(v) \otimes_{\underline{\mathcal{A}}} (\underline{M}^{\preceq c}/\underline{M}^{\prec c})$ is a direct sum of say n_c copies of E_c. The dimension over $\mathbf{Q}(v)$ of this module is the number of involutions contained in c which is known to be equal to $\dim E_c$. It follows that $n_c = 1$. It follows that the $\mathbf{Q}(v) \otimes_{\underline{\mathcal{A}}} \underline{\mathfrak{H}}'$-module $\mathbf{Q}(v) \otimes_{\underline{\mathcal{A}}} \underline{M}$ is isomorphic to $\oplus_c E_c$ that is, is a "model representation" for the algebra $\mathbf{Q}(v) \otimes_{\underline{\mathcal{A}}} \underline{\mathfrak{H}}'$. (Each simple module of the algebra appears exactly once in it.)

6. The W-module M_1

6.1. Let $\underline{\mathbf{I}}$ be the set of conjugacy classes of W contained in $\mathbf{I}$. For any $w \in \mathbf{I}$ let $h(w)$ be the dimension of the fixed point set R^{-w} of $-w$ in the reflection representation R of W (over $\mathbf{Q}$). For any $C \in \underline{\mathbf{I}}$ we set $h(C) = h(w)$ where w is any element of C. We have the following result.

Lemma 6.2. *Let $s \in S$, $w \in \mathbf{I}$ be such that $sw = ws > w$. Then $h(sw) > h(w)$.*

From our assumptions it follows that the line R^{-s} is contained in R^w, the fixed point set of w, and R^{-w} is contained in R^s, the fixed point set of s. It follows that R^{-s} and R^{-w} are contained in R^{-sw} hence $R^{-s} \oplus R^{-w}$ is contained in R^{-sw}. Thus $h(sw) \geq h(w) + 1$. The lemma is proved. $\square$

6.3. In the setup of 0.4 for any $i \in \mathbf{N}$ let $M_1^{\geq i}$ be the subspace of M_1 spanned by $\{a_w; h(w) \geq i\}$. From the formulas for the W-action in 0.4 and from 6.2 we see that for any $i \in \mathbf{N}$, $M_1^{\geq i}$ is a W-submodule of M_1. This induces a W-module structure on $M_1^i := M_1^{\geq i}/M_1^{\geq i+1}$. Let $gr(M_1) = \oplus_{i \in \mathbf{N}}(M_1^{\geq i}/M_1^{\geq i+1})$. This is naturally a W-module. By complete reducibility we have $M_1 \cong gr(M_1)$ as W-modules. For any $w \in \mathbf{I}$ we denote by $\tilde{a}_w$ the image of a_w under the projection $M_1^{\geq h(w)} \to M_1^{\geq h(w)}/M_1^{\geq h(w)+1}$. The elements $\tilde{a}_w (w \in \mathbf{I})$ form a $\mathbf{Q}$-basis of $gr(M_1)$ in which the W-action is as follows. (Here $s \in S$.)

$s(\tilde{a}_w) = -\tilde{a}_{sws}$ if $w \in \mathbf{I}, sw = ws < w$;

$s(\tilde{a}_w) = \tilde{a}_{sws}$ for all other $w \in \mathbf{I}$.

It follows that for any $x \in W, w \in \mathbf{I}$ we have $x(\tilde{a}_w) = \epsilon_{x,w}\tilde{a}_{xwx^{-1}}$ where $\epsilon_{x,w} \in \{1, -1\}$ satisfies $\epsilon_{xy,w} = \epsilon_{x,ywy^{-1}}\epsilon_{y,w}$ for all $x, y \in W, w \in \mathbf{I}$. In particular, if x, y are in $Z(w)$, the centralizer of $w \in \mathbf{I}$, in W then $\epsilon_{xy,w} = \epsilon_{x,w}\epsilon_{y,w}$. Thus, $x \mapsto \epsilon_{x,w}$ is a homomorphism $\epsilon_w : Z(w) \to \{1, -1\}$ and it is clear that for any $C \in \underline{\mathbf{I}}$, the subspace of $gr(M_1)$ spanned by $\{\tilde{a}_w; w \in C\}$ is a W-submodule of $gr(M_1)$ isomorphic to the representation of W induced from the character ϵ_w of $Z(w)$ where w is any element of C. We see that

(a) $M_1 \cong \oplus_w \mathrm{Ind}_{Z(w)}^W(\epsilon_w)$

as a W-module; here w runs over a set of representatives for the various $C \in \underline{\mathbf{I}}$. The multiplicities of the various irreducible W-modules in the W-module given by the right hand side of (a) were first described explicitly in [4] for W of type A_{n-1} and later by Kottwitz [8] for any irreducible W; for example, if W is irreducible of classical type then an irreducible representation E of W appears in the right hand side of (a) if and only if it is special in the sense of [9, (4.1.4)] and then its multiplicity is the integer f_E in [9, 4.1.1] (in type A_{n-1} this follows also from 5.3).

6.4. Kottwitz's formula for the W-module grM_1 in the right hand side of 6.3(a) is in terms of the nonabelian Fourier transform matrix of [9, 4.14]. We shall reformulate that formula in terms of unipotent representations, by using [9, 4.23] which relates unipotent representations with the nonabelian Fourier transform matrix. One advantage of this reformulation is that unlike in [8] we need not consider separately the "exceptional" representations of W of type E_7, E_8. (In the remainder of this section we assume that G is almost simple and that q, ϕ' are as in 1.1.) Let $IrrG^{\phi'}$ be a set of representatives for the isomorphism classes of irreducible representations of $G^{\phi'}$ over $\bar{\mathbf{Q}}_l$. For any $\rho \in IrrG^{\phi'}$ let $\epsilon(\rho) \in \{0, 1, -1\}$ be the Frobenius-Schur indicator of ρ; thus $\epsilon(\rho) = 1$ (resp. $\epsilon(\rho) = -1$) if ρ admits a nondegenerate $G^{\phi'}$-invariant symmetric (resp. antisymmetric) bilinear form $\rho \times \rho \to \bar{\mathbf{Q}}_l$ and $\epsilon(\rho) = 0$ if ρ is not isomorphic to its dual representation. It is known (Frobenius-Schur) that the dimension of the virtual representation $\sum_{\rho \in \mathrm{Irr}G^{\phi'}} \epsilon(\rho)\rho$ is equal to the number of $g \in G^{\phi'}$ such that $g^2 = 1$. Let us now consider the part $\Theta := \sum_{\rho \in \mathcal{U}} \epsilon(\rho)\rho$ of the virtual representation above coming from the set $\mathcal{U}$ of unipotent representations of $G^{\phi'}$.

Let $\mathcal{X}$ be the set of all triples $(\mathcal{F}, y, r)$ where $\mathcal{F}$ is a family [9, 4.2] of irreducible representations of W (with an associated finite group $\mathcal{G}_{\mathcal{F}}$, see [9, Chap. 4]), y is an element of $\mathcal{G}_{\mathcal{F}}$ defined up to conjugacy and r is an irreducible representation of the centralizer of y in $\mathcal{G}_{\mathcal{F}}$ defined up to isomorphism. In [9, 4.23], $\mathcal{X}$ is put in a bijection $(\mathcal{F}, y, r) \leftrightarrow \rho_{\mathcal{F},y,r}$ with $\mathcal{U}$. If $(\mathcal{F}, y, r) \in \mathcal{X}$ then we have $\epsilon(\rho_{\mathcal{F},y,r}) \in \{0, 1\}$; moreover, $\epsilon(\rho_{\mathcal{F},y,r}) = 1$ in exactly the following cases:

(i) $|\mathcal{F}| \neq 2$ and y acts on r by the scalar ± 1;

(ii) $|\mathcal{F}| = 2$ and $y = 1$.

(This follows from results in [11, Sec. 1] where it is shown that in case (i) $\rho_{\mathcal{F},y,r}$ is actually defined over $\mathbf{Q}$. On the other hand, in case (ii), $\rho_{\mathcal{F},y,r}$ is defined over $\mathbf{Q}[\sqrt{q}]$.) In particular, if W is of classical type, we have $\epsilon(\rho_{\mathcal{F},y,r}) = 1$ for any $(\mathcal{F}, y, r) \in \mathcal{X}$.

For each W-module E we define

$$R_E = |W|^{-1} \sum_{w \in W} \mathrm{tr}(w, E) \sum_i (-1)^i H_c^i(X_w, \bar{\mathbf{Q}}_l)$$

where X_w is the variety associated to G, ϕ', w in [3]. We view R_E as an element of $\mathbf{Q}[\mathcal{U}]$, the vector space of $\mathbf{Q}$-linear combinations of elements of $\mathcal{U}$ with its symmetric inner product $(,)$ in which $\mathcal{U}$ is an orthonormal basis.

Using the above description of $\epsilon(\rho_{\mathcal{F},y,r})$ and [9, 4.23] we can rewrite Kottwitz's formula in the form

(a) $\sum_{\rho \in \mathcal{U}; \epsilon(\rho)=1} (\rho, R_E) = (R_{grM_1}, R_E)$ *for any irreducible W-module E.*

Using the isomorphism $M_1 \cong grM_1$ we can rewrite (a) as follows.

(b) *We have $\Theta = R_{M_1} + \xi$ where $\xi \in \mathbf{Q}[\mathcal{U}]$ is orthogonal to R_E for any irreducible W-module E.*

Note that if G is of type $\neq F_4, E_8$ then $(\xi, \xi) = 0$ hence $\xi = 0$; if G is of type F_4 or E_8 then $(\xi, \xi) = 1$.

6.5. Let c be a two-sided cell of W. Let $M_1^{\preceq c}$ be the subspace of M_1 spanned by the elements $A_{w'}$ where $w' \in \mathbf{I}$, $w' \preceq c$. Let $M_1^{\prec c}$ be the subspace of M_1 spanned by the elements $A_{w'}$ where $w' \in \mathbf{I}$, $w' \prec c$. Then $M_1^{\preceq c}, M_1^{\prec c}$ are W-submodules of M_1 and $M_1^{\preceq c}/M_1^{\prec c}$ is naturally a W-module. From 5.2(a) we see that this last W-module is a direct sum of irreducible representations E of W which appear in c (which we write as $E \dashv c$). Since M_1 is isomorphic as a W-module to $\oplus_{c'} M_1^{\preceq c'}/M_1^{\prec c'}$ (c' runs over the two-sided cells of W) we see that $M_1^{\preceq c}/M_1^{\prec c} \cong \oplus_{E; E \dashv c} E^{\oplus (E:M_1)}$ where $(E : M_1)$ is the multiplicity of E in the W-module M_1. Note that $\dim(M_1^{\preceq c}/M_1^{\prec c}) = |c \cap \mathbf{I}|$. It follows that

(a) $|c \cap \mathbf{I}| = \oplus_{E; E \dashv c} (E : M_1) \dim(E)$.

This determines explicitly the number $|c \cap \mathbf{I}|$ since the multiplicities $(E : M_1) = (E : grM_1)$ are known from [8]. In particular, if W is of classical type we have

(b) $|c \cap \mathbf{I}| = f_E \dim(E)$

where E is the special representation such that $E \dashv c$ and f_E is as in 6.3. We thus recover a known result from [9, 12.17]).

7. Some Extensions

7.1. In this subsection we assume that W is irreducible and that $w \mapsto w^\diamond$ is a nontrivial automorphism of W (as a Coxeter group) such that $(w^\diamond)^\diamond = w$ for all $w \in W$. Let $\mathbf{I}_\diamond = \{w \in W; w^\diamond = w^{-1}\}$ be the set of "$\diamond$-twisted" involutions of W. Let $M_\diamond$ be the free $\mathcal{A}$-module with basis $(a_w)_{w \in \mathbf{I}_\diamond}$. Replacing M by $M_\diamond$, $\mathbf{I}$ by $\mathbf{I}_\diamond$, ws, sws by $ws^\diamond, sws^\diamond$ in Theorem 0.2 we obtain a true statement. The proof is along the same lines as that in §1,§2: we replace ϕ' in §1 or ϕ in §2 by a not necessarily split Frobenius map $G \to G$ which induces $w \mapsto w^\diamond$ on W (if G is not of type B_2, G_2 or F_4) or by a Chevalley exceptional isogeny, see [2, 21.4, 23.7], (if G is of type B_2, G_2 or F_4 and $p = 2, 3, 2$ respectively). Note that in this last situation, only cases (iii),(iv) appear in 0.2(a). (Indeed, in this situation, for $s \in S$, $s, s^\diamond$ are not conjugate in W hence $sw \neq ws^\diamond$ for any $w \in W$; this guarantees that the formulas in 0.2(a) specialized with u equal to an odd power of $\sqrt{p}$ involve only integer coefficients.) The statement obtained from Theorem 0.3 by replacing $\mathbf{I}$ by $\mathbf{I}_\diamond$, $\underline{M}$ by $\underline{M}_\diamond = \underline{\mathcal{A}} \otimes_{\mathcal{A}} M_\diamond$ and $P^\sigma_{y,w}$ by $P^{\sigma;\diamond}_{y,w}$ remains true with essentially the same proof. The description of the W-module $M_{\diamond,1} = \mathbf{Q} \otimes_{\mathcal{A}} M_\diamond$ (with $\mathbf{Q}$ viewed as an $\mathcal{A}$-algebra under $u \mapsto 1$) given in 0.4 with $\mathbf{I}$ replaced by $\mathbf{I}_\diamond$ and ws, sws replaced by $ws^\diamond, sws^\diamond$) remains valid. The statement of 4.4 remains valid if $\mathbf{I}$ is replaced by $\mathbf{I}_\diamond$ and ws, sws are replaced by $ws^\diamond, sws^\diamond$. (The quantities $\mathcal{M}^s_{z,w}$ are defined as in 4.3 with the same replacements.) The analogue of 5.2(a) continues to hold. The analogues of 6.2, 6.3 continue to hold.

7.2. Theorems 0.2 and 0.3 remain valid if W is replaced by an affine Weyl group. The proofs are essentially the same but use instead of $\mathcal{B}$ the affine flag manifold associated to $G(\mathbf{k}((\epsilon)))$ (here ϵ is an indeterminate). We note that although $\mathbf{D}$ and multiplication by u^ν (in 2.9) do not make sense separately, their composition $m \mapsto u^\nu \mathbf{D}(m)$ does. The results in §4 also remain valid. The results in §6 remain valid as far as $gr(M_1)$ is concerned but one cannot assert that $M_1 \cong gr(M_1)$. The generalizations of 0.2,0.3,§4 involving $w \mapsto w^\diamond$

(as in 7.1) also remain valid if W is replaced by an affine Weyl group and $w \mapsto w^\diamond$ is any automorphism of order ≤ 2 of W (as a Coxeter group).

7.3. Theorem 0.2(a) (and its variant for twisted involutions) remains valid if W is replaced by any Coxeter group. The main part of the proof involves the case where W is a dihedral group. It is likely that Theorem 0.2(b) (and then automatically Theorem 0.3) also extend to the case of Coxeter groups.

References

1. J. Adams, M.van Leeuwen, P. Trapa, D.A. Vogan and W.L. Yee, Unitary representations of real reductive groups, in preparation.
2. C. Chevalley, *Classification des Groupes Algébriques Semi-simples*, Springer, 2005.
3. P. Deligne and G. Lusztig, Representations of reductive groups over finite fields, *Ann. Math.*, **103** (1976), 103-161.
4. N. F.Inglis, R. W. Richardson and J. Saxl, An explicit model for the complex representations of S_n, *Arch. Math.* (Basel), **54** (1990), 258-259.
5. N. Iwahori, On the structure of the Hecke ring of a Chevalley group over a finite field, *J. Fac. Sci. Univ. Tokyo Sect.* 1, **10** (1964), 215-236.
6. D. Kazhdan and G. Lusztig, Representations of Coxeter groups and Hecke algebras, *Inv. Math.*, **53** (1979), 165-184.
7. D. Kazhdan and G. Lusztig, Schubert varieties and Poincaré duality, *Proc. Symp. Pure Math.*, **36** (1980)(Amer. Math. Soc.), 185-203.
8. R. Kottwitz, Involutions in Weyl groups, *Represent. Th.*(electronic), **4** (2000), 1-15.
9. G. Lusztig, Characters of reductive groups over a finite field, *Ann. Math. Studies*, **107**, Princeton Univ. Press, 1984.
10. G. Lusztig, *Introduction to Quantum Groups*, Progr. in Math., **110** Birkhäuser Boston, 1993.
11. G. Lusztig, Rationality properties of unipotent representations, *J. Alg.*, **258** (2002), 1-22.
12. G. Lusztig, *Hecke Algebras with Unequal Parameters*, CRM Monograph Ser., **18** Amer. Math. Soc., 2003.