# A Hecke Algebra Quotient and Some Combinatorial Applications 

\author{


#### Abstract

Let ( $W, S$ ) be a Coxeter group associated to a Coxeter graph which has no multiple bonds. Let $H$ be the corresponding Hecke Algebra. We define a certain quotient $\bar{H}$ of $H$ and show that it has a basis parametrized by a certain subset $W_{c}$ of the Coxeter group $W$. Specifically, $W_{c}$ consists of those elements of $W$ all of whose reduced expressions avoid substrings of the form $s t s$ where $s$ and $t$ are noncommuting generators in $S$. We determine which Coxeter groups have finite $W_{c}$ and compute the cardinality of $W_{c}$ when $W$ is a Weyl group. Finally, we give a combinatorial application (which is related to the number of reduced expressions for $w \in W_{c}$ ) of an exponential formula of Lusztig which utilizes a specialization of a subalgebra of $\bar{H}$.


}

Keywords: permutation, representation theory, non-commutative algebra, Lie theory, reductive group

## 1. Introduction

Let $(W, S)$ be a Coxeter group whose associated Coxeter graph $\Gamma$ is connected and has no multiple bonds. Let I be the set of vertices so that $S=\left\{s_{i}\right\}_{i \in \mathbf{I}}$. Let $l(w), w \in W$, be the smallest number $n$ such that $w$ is a product of $n$ generators. Let $H$ be the corresponding Hecke algebra over $\mathfrak{Q}\left[q, q^{-1}\right]$. Denote by $\left(T_{w}\right)_{w \in W}$ the standard basis. These satisfy the relations: (1) $T_{w} T_{w^{\prime}}=T_{w w^{\prime}}$, if $w, w^{\prime} \in W, l\left(w w^{\prime}\right)=l(w)+l\left(w^{\prime}\right),(2) T_{s}^{2}=(q-1) T_{s}+q$, if $s \in S$.

Let $I$ be the two-sided ideal generated by the elements
(*) $T_{s} T_{t} T_{s}+T_{s} T_{t}+T_{t} T_{s}+T_{s}+T_{t}+1$
where we have one such expression for each pair of non-commuting generators $s, t \in S$.
Let $\bar{H}=H / I$.
In the case where $W$ is a Coxeter group of type $A_{n}$, this has been studied by Jones [7], who attributes the notion to Temperley and Lieb [11]. For more details on this history, see [6, p. 104].

Let $W_{c}$ denote those elements of $W$ whose reduced expressions avoid substrings of the form sts where $s$ and $t$ are non-commuting generators in $S$. In Section 2, we show that $\bar{H}$ has a basis parametrized by $W_{c}$. In Section 3, we determine when $W_{c}$ is finite. In Section 4, we find explicit formulas for the cardinality of $W_{c}$ when $W$ is a Weyl group. Finally, in Section 5, we give an application of an exponential formula of Lusztig to derive some combinatorial identities.

Throughout this paper, we shall use a theorem of Iwahori and Tits which says that any reduced expression for $w \in W$ may be obtained from any other reduced expression for $w$ via a sequence of braid relations (see [3] for an explanation of braid relations and Coxeter groups).

I wish to thank George Lusztig, without whom this paper would not exist.
(Added April 21, 1995: It has come to the author's attention that Stembridge [10] has independently derived the formulas in section 4 using purely combinatorial methods and, after hearing about the results of this paper, generalized the results of section 3 to the non simply-laced case.)

## 2. The Hecke algebra quotient $\overline{\boldsymbol{H}}$

Let $(W, S)$ be as in the introduction. Depending on the context, we shall allow $T_{w}$ to mean $T_{w}$ or its canonical projection in $\bar{H}$.

Let $W_{c}$ be as defined in the introduction. For example, in type $A_{2}$, we have $W_{c}=$ $\{1, s, t, s t, t s\}$, where $S=\{s, t\}$.

Proposition 1 The elements $\left\{T_{w}\right\}_{w \in W_{c}}$ form a basis for the algebra $\bar{H}$.
The remainder of this section is devoted to a proof of Proposition 1.
Let $V$ be a free $\mathfrak{Q}\left[q, q^{-1}\right]$-module with basis $\left(X_{w}\right)_{w \in W_{c}}$.
Lemma 1 There exists an action of $\vec{H}$ on $V$ with the property that for any $w \in W_{c}$, we have $T_{w}\left(X_{1}\right)=X_{w}+$ (linear combination of $X_{w^{\prime}}, l\left(w^{\prime}\right)<l(w)$ ).

Before proving the lemma, we show how the lemma implies the proposition.
First, we claim that $\left\{T_{w}\right\}_{w \in W_{c}}$ spans $\bar{H}$. Let $H_{c} \subset \bar{H}$ be the $\mathbb{Q}\left[q, q^{-1}\right]$-module spanned by $\left\{T_{w}\right\}_{w \in W_{c}}$. We proceed by induction on the length. If $l(w)=1$, then $w=1$ and $T_{1} \in H_{c}$. Suppose $T_{w} \in H_{c}$ for all $w \in W, l(w)<m$. Choose $w \in W$ of length $m$. If $w \in W_{c}$, then $T_{w} \in H_{c}$. Otherwise, there is some reduced expression $s_{i_{1}} s_{i_{2}} s_{i_{3}} \cdots s_{i_{p}}$ of $w$ such that for some $p^{\prime}$, we have $s_{i_{p}^{\prime}}=s_{i_{p^{\prime}+2}}$ and $\left(s_{i_{p}^{\prime}} s_{i_{p^{\prime}+1}}\right)^{3}=1$. Thus,

$$
\begin{aligned}
T_{w} & =T_{s_{1}} \cdots T_{s_{p p}} \\
& =-T_{s_{s_{1}}} \cdots T_{s_{i_{p} p^{\prime}-1}}\left(T_{s_{i_{p}}} T_{s_{p^{\prime}+1}}+T_{s_{t_{p}+1}} T_{s_{p_{p}}}+T_{s_{i_{p}^{\prime}}}+T_{s_{s_{p^{\prime}+1}}}+1\right) T_{s_{i_{p^{\prime}}+3}} \cdots T_{s_{t_{p}}}
\end{aligned}
$$

This last expression is a linear combination of $T_{w^{\prime}}$ with $l\left(w^{\prime}\right)<l(w)$. By induction, we have $T_{w} \in H_{c}$. Since $\bar{H}$ is spanned by all $T_{w}, w \in W$, we see that $\bar{H}=H_{c}$.

To show linear independence of the $\left\{T_{w}\right\}_{w \in W_{c}}$, we again proceed by induction on length. Clearly, $\left\{T_{1}\right\}$ is a linearly independent set. Assume that $\left\{T_{w}\right\}_{w \in W_{c}, l(w)<n}$ is a linearly independent set. Suppose we have $\sum_{w \in W_{c}} c_{w} T_{w}=0$ where $c_{w}=0$ whenever $l(w)>n$. Then $\sum_{w \in W_{c}} c_{w} T_{w}\left(X_{1}\right)=\sum_{w \in W_{c}, l(w)=n} c_{w} X_{w}+\sum_{w \in W_{c}, l(w)<n} c_{w} X_{w}=0$. This implies that $c_{w}=0$ for all $w \in W_{c}, l(w)=n$. By the induction hypothesis, we must then have all $c_{w}=0$. Therefore the $\left\{T_{w}\right\}_{w \in W}$ form a basis of $\bar{H}$ and the proposition follows.

We prove Lemma 1.

We change (Hecke algebra) generators from $T_{s}$ to $\tau_{s}=T_{s}+1$, for $s \in S$. These new generators satisfy the relations: (1) $\tau_{s}^{2}=(q+1) \tau_{s}$, (2) $\tau_{s} \tau_{t}=\tau_{t} \tau_{s}$ if $s t=t s$, and (3) $\tau_{s} \tau_{t} \tau_{s}-q \tau_{s}=\tau_{t} \tau_{s} \tau_{t}-q \tau_{t}$ if $(s t)^{3}=1$. (See [7, Section 11.6].)

The elements (*) are the elements $\tau_{s} \tau_{t} \tau_{s}-q \tau_{s}$.
Thus, $\bar{H}$ is a $\mathfrak{Q}\left[q, q^{-1}\right]$-algebra generated by the $\tau_{s}, s \in S$ satisfying the relations: (1) $\tau_{s}^{2}=(q+1) \tau_{s}$, (2) $\tau_{s} \tau_{t}=\tau_{t} \tau_{s}$ if $s t=t s$, and (3) $\tau_{s} \tau_{t} \tau_{s}=q \tau_{s}$ if $(s t)^{3}=1$.

Let $P_{n}$ denote the following six hypotheses (all $w$ are assumed to be in $W_{c}$ ):
(1) $\tau_{s}\left(X_{w}\right)$ is defined for all $s \in S, l(w) \leq n$.
(2) $\tau_{s}\left(\tau_{s}\left(X_{w}\right)\right)=(q+1) \tau_{s} X_{w}$, if $l(w) \leq n-1$.
(3) $\tau_{s}\left(\tau_{t}\left(X_{w}\right)\right)=\tau_{t}\left(\tau_{s}\left(X_{w}\right)\right)$ whenever $s t=t s$, and $l(w) \leq n-1$.
(4) $\tau_{s}\left(\tau_{f}\left(\tau_{s}\left(X_{w}\right)\right)\right)=q \tau_{s}\left(X_{w}\right)$ whenever $(s t)^{3}=1$ and $l(w) \leq n-2$.
(5) $X_{w}=\tau_{s_{i_{1}}}\left(\cdots\left(\tau_{s_{i_{p}}}\left(X_{1}\right)\right) \cdots\right)$ whenever $s_{i_{1}} s_{i_{2}} s_{i_{3}} \cdots s_{i_{p}}$ is a reduced expression for $w$ and $l(w) \leq n+1$.
(6) For any expression $s_{i_{1}} s_{i_{2}} s_{i_{3}} \cdots s_{l_{m}}, m \leq n+1$ (not necessarily reduced), $\tau_{s_{i_{1}}}\left(\cdots\left(\tau_{s_{l_{1}}}\right.\right.$ $\left.\left(X_{1}\right)\right) \cdots$ ) is a linear combination of $X_{w^{\prime}}$ with $l\left(w^{\prime}\right) \leq m$.

If $P_{n}$ holds for all $n$, Lemma 1 follows. To see this, note that for $w \in W_{c}$, it makes sense to define $\tau_{w}=\tau_{s_{t_{1}}} \cdots \tau_{s_{t_{n}}}$, where $s_{i_{1}} s_{i_{2}} s_{i_{3}} \cdots s_{t_{n}}$ is a reduced expression for $w$. Then, $T_{w}=\tau_{w}+\left(\right.$ linear combination of $\tau_{w^{\prime}}, l\left(w^{\prime}\right)<l(w)$ ). Therefore, by $P_{n}$, parts (5) and (6), Lemma 1 follows.

Let $s, t, u \in S, t \neq u$. Define $\tau_{s}\left(X_{1}\right)=X_{s}$. Define

$$
\tau_{s}\left(X_{t}\right)= \begin{cases}X_{s t} & \text { if } s \neq t \\ (q+1) X_{t} & \text { if } s=t\end{cases}
$$

Finally, define

$$
\tau_{s}\left(X_{t u}\right)= \begin{cases}X_{s t u} & \text { if } l(s t u)=3 \text { and } s t u \in W_{c} \\ (q+1) X_{t u} & \text { if } s=t, \\ (q+1) X_{t u} & \text { if } s=u \text { and } s t=t s \\ q X_{s} & \text { if } s=u \text { and }(s t)^{3}=1\end{cases}
$$

One can verify that with these definitions, $P_{2}$ is true.
Fix $n>2$ and assume that $P_{k}$ is true for $2 \leq k<n$. We shall establish the statement $P_{n}$.
Let $w \in W_{c}, l(w)=n$. We wish to define $\tau_{s}\left(X_{w}\right)$.
If $s w \in W_{c}$, then define

$$
\tau_{s}\left(X_{w}\right)= \begin{cases}X_{s w} & \text { if } l(s w)>l(w) \\ (q+1) X_{w} & \text { if } l(s w)<l(w)\end{cases}
$$

If $s w \notin W_{c}$, we proceed as follows.
First, note that $l(s w)>l(w)$. If not, we may write $w=s w^{\prime}$, with $l(w)=1+l\left(w^{\prime}\right)$. Since $w \in W_{c}$, we must have $w^{\prime}=s w \in W_{c}$, a contradiction.

Denote by $\operatorname{supp}(w)$ the set of generators $u \in S$ which appear in some (or any) reduced expression for $w$.

We need the following lemma.

Lemma 2 With $w$ and $s$ as above, i.e. $w \in W_{c}$ and $s w \notin W_{c}$, there exists a unique $t \in S$ such that every reduced expression of $w$ may be parsed uniquely as follows: $w=$ $w_{1} t w_{2} s w_{3}$, where $l(w)=l\left(w_{1}\right)+l\left(w_{2}\right)+l\left(w_{3}\right)+2,(s t)^{3}=1$, and $s$ commutes with every $u \in \operatorname{supp}\left(w_{1}\right) \cup \operatorname{supp}\left(w_{2}\right)$.

Assuming this lemma, we show how we define $\tau_{s}\left(X_{w}\right)$.
Let $s_{i_{1}} s_{i_{2}} s_{i_{3}} \cdots s_{i_{n}}$ be a reduced expresssion for $w$, and let $w_{1}, w_{2}, w_{3}$, and $t$ be as in the lemma. Thus, for some integers $f$ and $g$, we have $w_{1}=s_{i_{1}} s_{i_{2}} s_{i_{3}} \cdots s_{i_{f-1}}$ and $w_{2}=s_{i_{f+1}} s_{i_{f+2}} s_{i_{f+3}} \cdots s_{i_{g-1}}$. Furthermore, $s_{i_{f}}=t$ and $s_{i_{g}}=s$.

We define $Y_{\mathbf{i}}=\tau_{s_{1}}\left(\cdots\left(\tau_{s_{l_{-1}-1}}\left(\tau_{s}\left(X_{w_{2} w_{3}}\right)\right)\right) \cdots\right)$. By the uniqueness of $w_{1}, w_{2}$, and $w_{3}$, and the induction hypothesis $P_{n-1}$ parts (1) and (6), this is a well-defined construct. Note that $Y_{\mathrm{i}}$ is a linear combination of $X_{w}^{\prime}$ with $l\left(w^{\prime}\right) \leq n-1$. (This follows from the induction hypothesis $P_{n-1}$ parts (5) and (6).) Also, note that $l\left(w_{2} w_{3}\right)=l\left(w_{2}\right)+l\left(w_{3}\right)$.

We claim that $Y_{i}$ does not depend on $\mathbf{i}$. Since every reduced expression of $w$ can be obtained from any other via a sequence of commutation relations (recall that $w \in W_{c}$ ), it suffices to show that $Y_{i}=Y_{i^{\prime}}$, where $\mathbf{i}^{\prime}$ is obtained from $\mathbf{i}$ by switching two adjacent coordinates $i_{h}, i_{h+1}$ of i where $s_{i_{h}}$ and $s_{i_{h+1}}$ commute.

Let $w_{1}^{\prime}, w_{2}^{\prime}, w_{3}^{\prime}$, and $t$ be associated to $i^{\prime}$ as in the lemma.
If $f<h$, then $w_{1}^{\prime}=w_{1}$ and $w_{2}^{\prime} w_{3}^{\prime}=w_{2} w_{3}$. Thus, $Y_{\mathrm{i}}=Y_{\mathrm{i}^{\prime}}$ because both are defined by the same expression.

If $h<f-1$, then $w_{k}^{\prime}=w_{k}$, but the expressions which define $Y_{i}$ and $Y_{i^{\prime}}$ differ by the switching of $\tau_{s_{1_{h}}}$ and $\tau_{s_{t_{n+1}}}$. In this case, the induction hypothesis $P_{n-1}$ parts (3) and (6) imply $Y_{i}=Y_{i^{\prime}}$.

The remaining two cases, namely $h=f-1$ and $h=f$, are similar. We treat the case where $h=f-1$. In this case, $Y_{i^{\prime}}=\tau_{s_{i_{1}}}\left(\cdots\left(\tau_{s_{i_{f-2}}}\left(\tau_{s}\left(X_{s_{i_{f-1}}} w_{2} w_{3}\right)\right)\right) \cdots\right)$. Using the induction hypothesis $P_{n-1}$ parts (3), (5), and (6), this can be seen to be the same as $Y_{i}$.

Because $Y_{i}$ is independent of $i$, we can define

$$
\tau_{s}\left(X_{w}\right)=q Y_{i}
$$

for any choice of reduced expression for $w$.
We now prove Lemma 2.
Let $s_{i_{1}} s_{i_{2}} s_{i_{3}} \cdots s_{i_{n}}$ be a reduced expression for $w$. Since $w \in W_{c}$, every reduced expression for $w$ may be obtained from this one via a sequence of commutation relations. Therefore every reduced expression of $w$ is of the form $s_{i_{\pi(1)}} s_{i_{\pi(2)}} s_{i_{\pi(3)}} \cdots s_{i_{\pi(n)}}$ where $\pi$ is a permutation of the letters $1, \ldots, n$.

We remark that if $s_{i_{k}}$ does not commute with $s_{i l}$, with $k<l$, then $\pi^{-1}(k)<\pi^{-1}(l)$.
Let $s_{i_{0}}=s$. Since $s w \notin W_{c}$, we can apply a sequence of commutation relations to $s_{i_{0}} s_{i_{1}} s_{i_{2}} \cdots s_{i_{n}}$ and obtain some expression $s_{i_{\sigma(0)}} s_{i_{\sigma(1)}} s_{i_{\sigma(2)}} \cdots s_{i_{\sigma(n)}}$, where $\sigma$ is a permutation of the letters $0, \ldots, n$, and there exists some $m$ where $s_{i_{\sigma(m)}}=s_{i_{\sigma(m+2)}}$ and $\left(s_{i_{\sigma(m)}} s_{i_{\alpha(m+1)}}\right)^{3}=1$.

We claim that $\sigma(m)=0$. First note that by the remark, $\sigma(m+1) \neq 0$ and $\sigma(m+2) \neq 0$. (There are non-commuting generators to the left of these.) If $\sigma(m) \neq 0$, then by the remark, we can move $s_{i_{0}}$ back to its original place. That is, if we set $z=\sigma^{-1}(0)$, then $s s_{\left.i_{\sigma(0)}\right)} s_{i_{\sigma(1)}} s_{i_{\sigma(2)}} \cdots s_{i_{\sigma(2-1)}} s_{i_{\sigma(2+1)}} s_{i_{\sigma(z+2)}} s_{i_{\sigma(2+3)}} \cdots s_{i_{\sigma(t)}}$ is a reduced expression for $s w$. However, this yields a reduced expression for $w$ which is plainly not in $W_{c}$, a contradiction. Therefore $\sigma(m)=0$.

We also have $s_{t \sigma(m+2)}=s$ and $s_{i_{\sigma(m+1)}}=t$ for some $t \in S$, such that $(s t)^{3}=1$.
Let $f=\sigma(m+1)$ and $g=\sigma(m+2)$. Notice that, by the remark, $f$ and $g$ are uniquely determined by i. Indeed, $s_{i_{g}}=s$ is characterized by being the first occurrence of $s$ in $s_{i_{1}} s_{l_{2}} s_{i_{3}} \cdots s_{i_{n}}$ (reading from left to right), and $s_{i_{f}}=t$ is the only generator occurring before $s_{i_{g}}$ which does not commute with $s$. (If more than one such element existed, the reduced expression obtained via $\sigma$ would not be possible.) Now set $w_{1}=s_{t_{1}} s_{t_{2}} s_{i_{3}} \cdots s_{l_{f-1}}$, $w_{2}=s_{i_{f+1}} s_{i_{f+2}} s_{i_{f+3}} \cdots s_{i_{g-1}}$, and $w_{3}=s_{i_{8+1}} s_{i_{g+2}} s_{t_{8+3}} \cdots s_{i_{n}}$.

All that remains to show is that $t$ is independent of the choice of reduced expression for $w$. Let $s_{t_{1}^{\prime}} s_{i_{2}^{\prime}} s_{t_{3}^{\prime}} \cdots s_{t_{n}^{\prime}}$ be another reduced expression for $w$. Let $t^{\prime}$ be the unique generator which does not commute with $s$ and which occurs before the first occurrence of $s$ (which must necessarily occur) in this reduced expression. From the remark, since $t$ appears before the first occurrence of $s$ in $s_{i_{1}} s_{i_{2}} s_{l_{3}} \cdots s_{i_{n}}$, we must have that $t$ appears before the first occurrence of $s$ in $s_{t_{1}} s_{i_{2}^{\prime}} s_{i_{3}^{\prime}} \cdots s_{t_{n}^{\prime}}$ as well. Therefore, we must have $t^{\prime}=t$.

The lemma follows.
By construction, it follows that $P_{n}$ parts (1), (5), and (6) hold.
We shall use the following immediate consequence of Lemma 2.

Lemma 3 Let $w \in W_{c}, s \in S$. If $s \notin W_{c}$, then we may write $w=w_{1} t s w_{2}$, where $l(w)=l\left(w_{1}\right)+l\left(w_{2}\right)+2, s$ commutes with all $u \in \operatorname{supp}\left(w_{1}\right)$, and $(s t)^{3}=1$. Furthermore, if $w=w_{1}^{\prime} t^{\prime}$ s $w_{2}^{\prime}$ is another such expression, then $t=t^{\prime}$.

We now check $P_{n}$, part (2).
Let $w \in W_{c}, l(w)=n-1$.
Case 1. Suppose $s w \in W_{c}$. If $w<s w$, then $\tau_{s}\left(\tau_{s}\left(X_{w}\right)\right)=(q+1) X_{s w}$ and $(q+1)$ $\tau_{s}\left(X_{w}\right)=(q+1) X_{s w}$. If $w>s w$, then $\tau_{s}\left(\tau_{s}\left(X_{w}\right)\right)=(q+1)^{2} X_{w}$ and $(q+1) \tau_{s}\left(X_{w}\right)=$ $(q+1)^{2} X_{w}$.

Case 2. Suppose $s w \notin W_{c}$. Write $w=w_{1} t s w_{2}$, as in the lemma.
We have $\tau_{s}\left(\tau_{s}\left(X_{w}\right)\right)=\tau_{s}\left(q \tau_{w_{1}}\left(\tau_{s}\left(X_{w_{2}}\right)\right)\right)=q(q+1) \tau_{w_{1}}\left(\tau_{s}\left(X_{w_{2}}\right)\right)$. On the other hand, we have $(q+1) \tau_{s}\left(X_{w}\right)=(q+1)\left(q \tau_{w_{1}}\left(\tau_{s}\left(X_{w_{2}}\right)\right)\right)$.

Thus, $P_{n}$, part (2) is established.
We now check $P_{n}$, part (3).
Let $r, s \in S$ commute and pick $w \in W_{c}, l(w)=n-1$.
Case 1. Suppose $r s w \in W_{c}$. We have four possibilities depending on whether $w$ is shortened or lengthened by $r$ and $s$. The proof for each case is similar. We consider only
the case where $r w<w$ and $s w>w$. We have $\tau_{s}\left(\tau_{r}\left(X_{w}\right)\right)=\tau_{s}\left((q+1) X_{w}\right)=(q+1) X_{s w}$. On the other hand, $\tau_{r}\left(\tau_{s}\left(X_{w}\right)\right)=\tau_{r}\left(X_{s w}\right)=(q+1) X_{s w}$.

Case 2. Suppose $r w \in W_{c}$, but $s w \notin W_{c}$. Write $w=w_{1} t s w_{2}$, as in the lemma. If $r w<w$, we have $\tau_{s}\left(\tau_{r}\left(X_{w}\right)\right)=\tau_{s}\left((q+1) X_{w}\right)=q(q+1) \tau_{w_{1}}\left(\tau_{s}\left(X_{w_{2}}\right)\right)$. On the other hand, $\tau_{r}\left(\tau_{s}\left(X_{w}\right)\right)=\tau_{r}\left(q \tau_{w_{1}}\left(\tau_{s}\left(X_{w_{2}}\right)\right)\right)=q(q+1) \tau_{w_{1}}\left(\tau_{s}\left(X_{w_{2}}\right)\right)$. Note that if $r w<w$, then $r w_{1} s w_{2}<w_{1} s w_{2}$, since $t \neq r$. The case $r w>w$ follows similar lines.

Case 3. Suppose $r w, s w \notin W_{c}$. We have two possibilities. Either we can write $w=$ $w_{1} \operatorname{tr} s w_{2}$ where $t$ does not commute with $r$ or $s$ but both $r$ and $s$ commute with all $u \in$ $\operatorname{supp}\left(w_{1}\right)$, or we can write $w=w_{1} t s w_{2} v r w_{3}$, where $t$ does not commute with $s, v$ does not commute with $r$, but $s$ commutes with all $u \in \operatorname{supp}\left(w_{1}\right)$ and $r$ commutes with all $u \in \operatorname{supp}\left(w_{1} t s w_{2}\right)$. We treat only the latter case.

We have then, $\tau_{s}\left(\tau_{r}\left(X_{w}\right)\right)=\tau_{s}\left(q \tau_{w_{1} t s w_{2}}\left(\tau_{r}\left(X_{w_{3}}\right)\right)\right)=q^{2} \tau_{w_{1}}\left(\tau_{s}\left(\tau_{w_{2}}\left(\tau_{r}\left(X_{w_{3}}\right)\right)\right)\right.$ ). To arrive at this, we have made extensive use of induction hypothesis $P_{n-1}$. On the other hand, $\tau_{r}\left(\tau_{s}\left(X_{w}\right)\right)=\tau_{r}\left(q \tau_{w_{1}}\left(\tau_{s}\left(\tau_{w_{2} v r w_{3}}\left(X_{1}\right)\right)\right)\right)=q^{2} \tau_{w_{1}}\left(\tau_{s}\left(\tau_{w_{2}}\left(\tau_{r}\left(X_{w_{3}}\right)\right)\right)\right)$.

This exhausts the possibilities and establishes $P_{n}$, part (3).
The establishment of $P_{n}$, part (4) follows similar lines. Let $w \in W_{c}, l(w)=n-2$. Fix $s, r \in S$ such that $(s r)^{3}=1$.

Case 1. Suppose $l(r s w)<l(s w)<l(w)$. Note that $l(s r s w)=l(w)-1$. We must then have $w=s r w^{\prime}$ where $l(w)=l\left(w^{\prime}\right)+2$. We find, $\tau_{s}\left(\tau_{r}\left(\tau_{s}\left(X_{w}\right)\right)\right)=(q+1) \tau_{s}\left(\tau_{r}\left(X_{s r} w^{\prime}\right)\right)=$ $q(q+1) \tau_{s}\left(\tau_{r}\left(X_{w^{\prime}}\right)\right)$. On the other hand, $q \tau_{s}\left(X_{w}\right)=q(q+1)\left(X_{w}\right)=q(q+1) \tau_{s}\left(\tau_{r}\left(X_{w^{\prime}}\right)\right)$, as desired.

Case 2. Suppose $l(s w)<l(w), l(r s w)=l(w)$. Here, $w=s w^{\prime}$ where $l(w)=l\left(w^{\prime}\right)+1$. Then, $\tau_{s}\left(\tau_{r}\left(\tau_{s}\left(X_{w}\right)\right)\right)=(q+1) \tau_{s}\left(\tau_{r}\left(X_{s w^{\prime}}\right)\right)=(q+1) \tau_{s}\left(\tau_{r}\left(\tau_{s}\left(X_{w^{\prime}}\right)\right)\right)=q(q+1) \tau_{s}\left(X_{w^{\prime}}\right)$, by $P_{n-1}$ part (4). On the other hand, $q \tau_{s}\left(X_{w}\right)=q(q+1)\left(X_{w}\right)$ as desired.

Case 3. Suppose $l(s w)>l(w)$ and both $s w, r s w \in W_{c}$. Note that necessarily, $l(r s w)>$ $l(s w)$. We have $\tau_{s}\left(\tau_{r}\left(\tau_{s}\left(X_{w}\right)\right)\right)=\tau_{s}\left(X_{r s w}\right)=q \tau_{s}\left(X_{w}\right)$ as desired.

Case 4. Suppose $l(s w)>l(w), s w \in W_{c}$, and $r s w \notin W_{c}$. In this case, we see that we may write $w=r w_{1}$. This follows since by lemma $3, s w=w_{1}^{\prime} t r w_{2}^{\prime}$. According to Lemma 3, $t$ is the unique generator occurring to the left of $r$ which fails to commute with $r$, but this is just $s$. By the remark on ordering, we see that $s w=s w_{1}^{\prime} r w_{2}^{\prime}=s r w_{1}^{\prime} w_{2}^{\prime}$. We take $w_{1}=w_{1}^{\prime} w_{2}^{\prime}$. We then find $\tau_{s}\left(\tau_{r}\left(\tau_{s}\left(X_{w}\right)\right)\right)=\tau_{s}\left(q \tau_{r}\left(X_{w_{1}}\right)\right)=q\left(\tau_{s}\left(X_{r w_{1}}\right)\right)$, as desired.

Case 5. Suppose $s w \notin W_{c}$, In this case, write $w=w_{1} t s w_{2}$ as in the lemma. $\tau_{s}\left(X_{w}\right)=$ $q \tau_{w_{1}}\left(\tau_{s}\left(X_{w_{2}}\right)\right)=q \tau_{s}\left(\tau_{w_{1}}\left(X_{w_{2}}\right)\right)$. Recall that $s$ commutes with all $u \in \operatorname{supp}\left(w_{1}\right)$. Since this last expression is a linear combination of $X_{w^{\prime}}$ with $l\left(w^{\prime}\right) \leq n-3$, we can write $\tau_{s}\left(\tau_{r}\left(q \tau_{s}\left(\tau_{w_{1}}\left(X_{w_{2}}\right)\right)\right)\right)=q^{2} \tau_{s}\left(\tau_{w_{1}}\left(X_{w_{2}}\right)\right)$, which is just $q \tau_{s}\left(X_{w}\right)$, as desired.

Thus, $P_{n}$, part (4) is established.
This completes the proof of Proposition 1.

## 3. Classification of finite $\boldsymbol{W}_{\boldsymbol{c}}$

By $E_{n}$ we mean the extended $E$ series which is defined for $n \geq 5$ and consists of a string of $n-1$ nodes which comprise a graph of type $A_{n-1}$, along with an additional node which is connected by a single edge to the third node of the string counting from one end. Note that $E_{9}=\tilde{E}_{8}$.

Proposition 2 If $W$ is of type $A_{n}, D_{n}$, or $E_{n}$, then $W_{c}$ is finite. Otherwise, $W_{c}$ is infinite.
Proof: Suppose that $\Gamma$ has a subgraph of type $\tilde{A}_{n}$ for some $n \geq 2$. Denote by $s_{0}, s_{1}$, $s_{2}, \ldots, s_{n}$ the corresponding generators such that $s_{i}$ and $s_{j}$ commute unless $i-j=$ $\pm 1 \bmod n+1$. Let $w=s_{0} s_{1} s_{2} \cdots s_{n}$. We see that $w^{t} \in W_{c}$ for any $t>0$.

Therefore, if $W_{c}$ is finite, $\Gamma$ has no loops.
Suppose that $\Gamma$ has a subgraph of type $\tilde{D}_{n}$ for some $d \geq 4$. Label the associated generators as follows:


Let $w=s_{1} s_{2} s_{3} \cdots s_{n-4} b_{1} b_{2} s_{n-4} s_{n-5} s_{n-6} \cdots s_{1} a_{1} a_{2}$. We see that $w^{t} \in W_{c}$ for any $t>0$.
Therefore, if $W_{c}$ is finite, $\Gamma$ can have at most one branch point, and this branch cannot have more than three arms.

Suppose that $\Gamma$ has a subgraph of type $\tilde{E}_{6}$. Label the associated generators as follows:


Let $w=m a_{2} a_{1} b_{1} m b_{2} b_{1} c_{1} m c_{2} c_{1} a_{1}$. One can check that $w^{t}$ has the property that between any two occurrences of a generator $s$ in $w^{t}$, there occur two generators which do not commute with $s$. Therefore, $w^{t} \in W_{c}$ for any $t>0$.

Therefore, if $W_{c}$ is finite and $\Gamma$ has a branch point, then the three arms cannot all extend a distance of two or more from the branch point.

Suppose that $\Gamma$ has a subgraph of type $\tilde{E}_{7}$. Label the associated generators as follows:


Let $w=m a_{2} a_{1} b_{1} m a_{3} a_{2} a_{1} c_{1} m b_{1} c_{2} c_{1} m a_{1} c_{3} c_{2} c_{1}$. One can check that $w^{t}$ has the property that between any two occurrences of a generator $s$ in $w^{t}$, there occur two generators which do not commute with $s$. Therefore, $w^{t} \in W_{c}$ for any $t>0$.

Therefore, if $W_{c}$ is finite and $\Gamma$ has a branch point, then no two arms can extend a distance of three or more from the branch point.

The above considerations eliminate all graphs except those of type $A_{n}, D_{n}$, or $E_{n}$. Since $W$ itself is finite in case $A_{n}, D_{n}, E_{6}, E_{7}$, and $E_{8}$, it suffices to check the case $E_{n}, n>8$.

Assume $\Gamma=E_{n}, n>8$. We shall proceed by induction on $n$. Let $L$ denote the longest possible length of a reduced expression in $W_{c}$ for the Coxeter group of type $E_{n-1}$. Label the generators as follows:


We group all generators of type $a_{k}$ together into one family called $\alpha$. Similarly, define families $\beta$ and $\gamma$. Note that elements from different families commute.

Lemma 4 Let $w \in W_{c}$. In any reduced expression for $w$, we claim that:
(1) Between any two occurrences of $b_{1}$, there must be at least two occurrences of $m$.
(2) Between any two occurrences of $m$, there must be generators from at least two of the three families $\alpha, \beta$, and $\gamma$.
(3) For any four consecutive occurrences of $m$, at least one consecutive pair of these $m$ 's must be separated by generators other than $a_{1}$.
(4) Between any two occurrences of $c_{n-4}$, there must be an occurrence of two m's separated by generators of type $\alpha$ and $\beta$ only.

Proof: Note that $b_{1}$ commutes with all other generators except $m$. Therefore, if there are two occurrences of $b_{1}$ separated by one or fewer occurrences of $m$, we may perform a series of commutations until either $b_{1} b_{1}$ or $b_{1} m b_{1}$ appears. Then either our expression is not reduced, or $w \notin W_{c}$. This proves (1).

Suppose we have two occurrences of $m$ separated by generators from family $\gamma$ only. Since $m$ commutes with all but one member of $\gamma$, namely $c_{1}$, there must be two occurrences of $c_{1}$ between these $m$ 's. Two consecutive occurrences of $c_{1}$ must be separated by at least two occurrences of $c_{2}$. Of these, we can find two consecutive occurrences of $c_{2}$. These must be separated by at least two occurrences of $c_{3}$, etc. We continue this argument until we have two consecutive occurrences of $c_{n-4}$ which must be separated by at least two occurrences of generators which do not exist, an impossibility. A similar argument applies to the other families. This proves (2).

Suppose we have four consecutive occurrences of $m$, such that between any two consecutive $m$ 's there exists an occurrence of $a_{1}$. We may arrange that $a_{1}$ is the only generator of type $\alpha$ between the middle consecutive pair of $m$ 's by commuting $a_{2}$ as necessary. If this is not possible, it means there is an occurrence of $a_{2}$ surrounded by $a_{1}$ 's which contradicts $w \in W_{c}$. Since this lone $a_{1}$ can be commuted to be adjacent to either of the two middle
$m$ 's, $a_{2}$ must be the first generator of family $\alpha$ which appears reading from the second $m$ to the left, and $a_{2}$ must be the first generator of family $\alpha$ which appears reading from the third $m$ to the right. In this case, we may commute these $a_{2}$ 's so that they lie between the two middle $m$ 's. But this allows us to form an occurrence of $a_{2} a_{1} a_{2}$, contradicting $w \in W_{c}$. This proves (3).

For (4), we proceed in a similar way as in the proof of (2). If we have two occurrences of $c_{n-4}$, we can find two consecutive such occurrences. These must be separated by at least two occurrences of $c_{n-5}$. Of these, we pick two consecutive occurrences, and so on, until we arrive at two consecutive occurrences of $m$ separated by no member of family $\gamma$. This proves (4).

This completes the proof of Lemma 4.

Now assume $W_{c}$ is infinite. We shall expose a contradiction.
Note that any element in $W_{c}$ of length $p(L+1), p$ a positive integer, must involve at least $p$ occurrences of $c_{n-4}$, by definition of $L$. Removing the vertex corresponding to $m$ from $\Gamma$ results in a Coxeter graph of type $A_{1} \times A_{2} \times A_{n-4}$. The corresponding Coxeter group has a longest element, say, of length $L_{0}$. Thus, any element in $W_{c}$ of length $p\left(L_{0}+1\right)$ must involve at least $p$ occurrences of $m$.

Since we are assuming that $W_{c}$ is infinite, there must occur elements in $W_{c}$ with reduced expression of arbitrary length. Let $w \in W_{c}$ be an element of length greater than $2(L+1)$ $\left(L_{0}+1\right)$. Then any reduced expression for $w$ must have $2(L+1)$ occurrences of $m$. Between the first and last of these occurrences of $m$, there must occur at least 2 occurrences of $c_{n-4}$. By Lemma 4, part (4), between these two occurrences of $c_{n-4}$ there occurs two $m$ 's separated by generators from families $\alpha$ and $\beta$, but not $\gamma$. By construction, there occur four consecutive $m$ 's of which the middle two $m$ 's are precisely the aforementioned $m$ 's. From now on, we shall refer only to these four $m$ 's.

By Lemma 4, part (1), the first and third consecutive pairs of $m$ 's are not separated by any occurrence of $b_{1}$, since $b_{1}$ already occurs between the middle pair of $m$ 's. By Lemma 4, part (2), we must then have the first and third consecutive pairs of $m$ 's separated by generators from both families $\alpha$ and $\gamma$, and only these families. By Lemma 4, part (3), between some consecutive pair of these four $m$ 's there cannot occur $a_{1}$. The middle pair must be separated by an occurrence of $a_{1}$ because these two $m$ 's must be separated by at least two of $a_{1}$ and $b_{1}$, and $b_{1}$ cannot occur twice (by Lemma 4, part (1)). Thus, between the first or third pair of $m$ 's there cannot occur $a_{1}$. Between the pair which excludes $a_{1}$, there must be two occurrences of $c_{1}$. Grouping together the generators of family $\gamma$ between this pair yields an element of the $W_{c}$ associated with a graph of type $A_{n-4}$ with two occurrences of $c_{1}$. The argument for Lemma 4, part (2) shows that this is impossible. Proposition 2 follows.

## 4. Some explicit formulas

In this section, let $C_{n}=\frac{1}{n+1}\binom{2 n}{n}$, the $n$th Catalan number. We adopt the convention that $\binom{n}{k}=0$ whenever $k \notin\{0,1,2, \ldots, n\}$.

Proposition 3 For the simply laced Weyl groups, the cardinality of $W_{c}$ is given by:

$$
\#\left|W_{c}\right|= \begin{cases}C_{n+1} & \text { in type } A_{n} \\ \frac{n+3}{2} C_{n}-1 & \text { in type } D_{n} \\ 662 & \text { in type } E_{6}, \\ 2,670 & \text { in type } E_{7}, \\ 10,846 & \text { in type } E_{8}\end{cases}
$$

We remark that for type $A_{n}$, the above result is well-known as the number of 321avoiding permutations (permutations $\pi$ such that there does not exist $a<b<c$ such that $\pi(a)>\pi(b)>\pi(c)$ ), see for example [2, Section 2], and also [7, Section 11].

Proof: By Proposition 1, $W_{c}$ parametrizes a basis of $\bar{H}$. When $W$ is a Weyl group, this algebra is semi-simple since it is the quotient of a semi-simple algebra. Thus, the cardinality of $W_{c}$ is the sum of the squares of the dimensions of those representations of $H$ which factor through to $\bar{H}$. These, in turn, are in one to one correspondence with representations of $W$ on which the elements (*) (interpreted as elements of the group algebra of $W$ ) act as 0 . Equivalently, this condition is given by: $\left(\operatorname{Res}_{A_{2}}^{W} \chi, 1_{A_{2}}\right)_{A_{2}}=0$, where $A_{2}$ is some (or any) parabolic subgroup of $W$ of type $A_{2}$. We call this restriction property $(R)$.

Note that any two parabolic subgroups of type $A_{2}$ are conjugate. Because $\Gamma$ is connected, this statement follows from the following observation: If $\{s, t, u\} \subset S$ generate a subgroup of type $A_{3}$ where $s u=u s$, then the parabolic subgroup $\langle s, t\rangle$ can be conjugated to $\langle t, u\rangle$ using the element sutsut.

Case 1. The representations of $A_{n}$ are parametrized by diagrams with $n+1$ squares. Let $h=n+1$. The ones which satisfy the restriction property $(R)$ are precisely those with two or fewer columns (where we take the single column diagram to be the sign representation.)

Using the hook length formula for dimension, we have:

$$
\begin{aligned}
\#\left|W_{c}\right| & =\sum_{k=0}^{\left[\frac{h}{2}\right]} \frac{h!(h-2 k+1)!}{k!(h-2 k-2)!(h-k+1)!} \\
& =\sum_{k=0}^{\left[\frac{h}{2}\right]}\left(\binom{h}{k}-\binom{h}{k-1}\right)^{2}=\frac{1}{2} \sum_{k=0}^{h+1}\left(\binom{h}{k}-\binom{h}{k-1}\right)^{2} \\
& =\frac{1}{2} \sum_{k=0}^{h+1}\left(\binom{h}{k}^{2}+\binom{h}{k-1}^{2}-2\binom{h}{k}\binom{h}{k-1}\right) \\
& =\binom{2 h}{h}-\sum_{k=0}^{h+1}\binom{h}{h-k}\binom{h}{k-1}=\binom{2 h}{h}-\binom{2 h}{h-1}=\left(1-\frac{h}{h+1}\right)\binom{2 h}{h} \\
& =C_{h} .
\end{aligned}
$$

Case 2. Let $n \geq 4$.

The irreducible representations of $W$ of type $D_{n}$ arise from certain pairs of diagrams. For details of this correspondence, we refer the reader to [8, Sections 4.5, 4.6]. Briefly, let $r+\tilde{r}=n, r \geq \tilde{r} \geq 0$. Let $\chi_{1}$ (resp. $\chi_{2}$ ) be the character of an irreducible representation $E_{1}$ (resp. $E_{2}$ ) of the symmetric group $S_{r}$ (resp. $S_{r}$ ). There are two natural ways in which $W$ is a subgroup of $W_{n}^{\prime}$, the Weyl group of type $B_{n}$, though the choice of the imbedding is immaterial for our purposes, so we fix one. The symmetric group $S_{n}$ is naturally a quotient of $W_{n}^{\prime}$. Thus, $E_{1} \otimes E_{2}$, a representation of $S_{r} \times S_{\bar{r}}$, can be lifted to a representation $E_{1,2}$ of $W_{r}^{\prime} \times W_{r}^{\prime}$. Inducing this latter representation to $W_{n}^{\prime}$ and then restricting to $W$ gives us a representation $E$, with character $\chi$, of $W$. If $E_{1}$ and $E_{2}$ are not given by the same diagram, then $E$ is irreducible. Otherwise, $E$ is a direct sum of two irreducible representations of the same dimension.

We have the following formulae:

$$
\begin{aligned}
& \chi(1)=\binom{n}{r} \chi_{1}(1) \chi_{2}(1) \\
& \chi(s)=\chi(t)=\chi(s t s)=\binom{n-2}{r-2} \chi_{1}(s) \chi_{2}(1)+\binom{n-2}{\tilde{r}-2} \chi_{1}(1) \chi_{2}(s) \\
& \chi(s t)=\chi(t s)=\binom{n-3}{r-3} \chi_{1}(s t) \chi_{2}(1)+\binom{n-3}{\tilde{r}-3} \chi_{1}(1) \chi_{2}(s t) .
\end{aligned}
$$

Condition ( $R$ ) requires:

$$
\begin{aligned}
0= & \chi(1)+3 \chi(s)+2 \chi(s t) \\
= & \binom{n}{r} \chi_{1}(1) \chi_{2}(1)+3\left(\binom{n-2}{r-2} \chi_{1}(s) \chi_{2}(1)+\binom{n-2}{\tilde{r}-2} \chi_{1}(1) \chi_{2}(s)\right) \\
& +2\left(\binom{n-3}{r-3} \chi_{1}(s t) \chi_{2}(1)+\binom{n-3}{\tilde{r}-3} \chi_{1}(1) \chi_{2}(s t)\right) \\
= & \chi_{1}(1) \chi_{2}(1)\left(\binom{n-3}{r-3}+3\binom{n-3}{r-2}+3\binom{n-3}{r-1}+\binom{n-3}{r}\right) \\
& +3 \chi_{1}(s) \chi_{2}(1)\left(\binom{n-3}{r-2}+\binom{n-3}{r-3}\right)+3 \chi_{1}(1) \chi_{2}(s)\left(\binom{n-3}{\tilde{r}-2}+\binom{n-3}{\tilde{r}-3}\right) \\
& +2 \chi_{1}(s t) \chi_{2}(1)\binom{n-3}{r-3}+2 \chi_{1}(1) \chi_{2}(s t)\binom{n-3}{\tilde{r}-3} \\
= & \binom{n-3}{r-3} \chi_{2}(1)\left(\chi_{1}(1)+3 \chi_{1}(s)+2 \chi_{1}(s t)\right) \\
& +3\binom{n-3}{r-2} \chi_{2}(1)\left(\chi_{1}(1)+\chi_{1}(s)\right)+3\binom{n-3}{\tilde{r}-2} \chi_{1}(1)\left(\chi_{2}(1)+\chi_{2}(s)\right) \\
& +\binom{n-3}{r} \chi_{1}(1)\left(\chi_{2}(1)+3 \chi_{2}(s)+2 \chi_{2}(s t)\right) .
\end{aligned}
$$

If $\tilde{r} \geq 2$, this last expression can be 0 if and only if $\chi_{1}(s)=-\chi_{1}(1)$ and $\chi_{2}(s)=$ $-\chi_{2}(1)$. Because any normal subgroup of the symmetric group which contains all simple transpositions must be the whole group, we see that this is possible if and only if $E_{1}$ and $E_{2}$ are the respective sign representations of $S_{r}$ and $S_{\bar{r}}$.

If $\tilde{r}=1$, we must have $\chi_{1}(s)=-\chi_{1}(1)$. Therefore, $E_{1}$ is the sign representation and $E_{2}$ is the trivial representation.

If $\tilde{r}=0$, we must have $\chi_{1}(1)+3 \chi_{1}(s)+2 \chi_{1}(s t)=0$, which means that $E_{1}$ is parametrized by a diagram with two or fewer columns.

Note that if $E_{1}$ and $E_{2}$ are given by the same diagram, that is, if $r=\tilde{r}$ and $E_{1}$ and $E_{2}$ are both sign representations, then the two irreducible summands of $E$ both satisfy the restriction condition ( $R$ ) because if one did not, neither could $E$.

We compute

$$
\begin{aligned}
\#\left|W_{c}\right| & =C_{n}+\sum_{r=1}^{\left[\frac{n-1}{2}\right]}\binom{n}{r}^{2}+\cos ^{2}\left(\frac{\pi n}{2}\right) \frac{1}{2}\binom{n}{n / 2}^{2} \\
& =C_{n}-1+\frac{1}{2} \sum_{r=0}^{n}\binom{n}{r}^{2} \\
& =\frac{n+3}{2} C_{n}-1 .
\end{aligned}
$$

By inspection, this formula is valid also when $n=2$ and $n=3$.
Case 3. For $E_{6}, E_{7}$, and $E_{8}$ we consulted [1] to determine which representations contain an $A_{2}$ fixed vector. We shall follow the notation in [8] for the irreducible representations.

For $E_{6}$, the representations are $1_{p}^{\prime}, 6_{p}^{\prime}, 15_{q}^{\prime}$, and $20_{p}^{\prime}$.
For $E_{7}$, the representations are $1_{a}^{\prime}, 7_{a}^{\prime}, 15_{a}^{a}, 21_{b}, 27_{a}^{\prime}$, and $35_{b}^{\prime}$.
For $E_{8}$, the representations are $1_{x}^{\prime}, 8_{z}^{\prime}, 35_{x}^{\prime}, 50_{x}^{\prime}$, and $84_{x}^{\prime}$.
This completes the proof of Proposition 3.

## 5. Application of an exponential formula of Lusztig

In this section, we assume that $(W, S)$ is the Weyl group of a reductive algebraic group $G$ defined over $\mathfrak{C}$. Let $\mathfrak{g}$ be the Lie algebra of $G$. We continue to assume $\mathfrak{g}$ is simple of type $A, D$, or $E$. Fix a Cartan subalgebra $\mathfrak{h}$ and a root decomposition of $\mathfrak{g}$. Let $R$ be the set of roots. Choose a set of simple roots $\Pi=\left\{\alpha_{i}\right\}_{i \in \mathbf{I}}$. Let $h t(\phi), \phi \in R$ denote the sum of the coefficients of $\phi$ when written as a linear combination of simple roots. Here, $s_{i} \in S$ corresponds to the reflection in the root $\alpha_{t}$. Let $w_{0} \in W$ be the unique element for which $2 l\left(w_{0}\right)=\operatorname{card}(R)$. For each $i \in \mathbf{I}$, fix some $E_{\imath} \in \mathfrak{g}_{\alpha_{1}}, E_{i} \neq 0$. Let $\mathfrak{u}^{+}$be the nilpotent subalgebra of $\mathfrak{g}$ generated by the $E_{\imath}$ and let $U^{+}=\exp \left(\mathfrak{u}^{+}\right)$.

The following exponential formula was conjectured by Lusztig [9, Section 11.4] and proven in [4].

Proposition 4 Choose $\left(i_{1}, \ldots, i_{N}\right) \in \mathbf{I}^{N}$ so that $s_{i_{1}} s_{i_{2}} s_{i_{3}} \cdots s_{i_{N}}$ is a reduced expression for $w_{0}$. Let $h_{k}=h t\left(s_{i_{1}} s_{i_{2}} s_{i_{3}} \cdots s_{i_{k-1}}\left(\alpha_{i_{k}}\right)\right)$. For each $i \in \mathbf{I}$, let $n_{i}=\sum_{i_{k}=t} h_{k}$. Then

$$
\exp \left(h_{1} E_{i_{1}}\right) \exp \left(h_{2} E_{i_{2}}\right) \cdots \exp \left(h_{N} E_{i_{N}}\right)=\exp \left(\sum_{i \in \mathbf{I}} n_{i} E_{i}\right)
$$

For any $w \in W$, we denote by $\mathbf{J}(w)$ the set of $\mathbf{i}$ for which $s_{l_{1}} s_{l_{2}} s_{i_{3}} \cdots s_{i_{n}}$ is a reduced expression for $w$.

For each $z \in W$, we shall define a map $f_{z}: W \mapsto \mathfrak{N}$.
Fix $w \in W$ and pick some $\mathbf{j} \in \mathbf{J}(w)$.
For each $1 \leq k \leq l(w)$, let $h_{k}=h t\left(s_{j_{1}} \cdots s_{j k-1}\left(\alpha_{j k}\right)\right)$. Let $n=l(z)$.
Now define

$$
f_{z}^{\prime}(\mathbf{j})=\sum_{\substack{1 \leq p_{1}<\\\left(U_{p_{1}}, \ldots, j_{n}\right) \in p_{n} \leq(z)}} h_{p_{1}} h_{p_{2}} \cdots h_{p_{n}} .
$$

We claim that this definition is independent of the choice of $\mathbf{j}$. The proof can be achieved using the theorem of Iwahori and Tits referred to in the introduction. We omit the proof. We remark that in the case where $w \in W_{c}$, this will follow from Proposition 5.

We define

$$
f_{z}(w)=f_{z}^{\prime}(\mathbf{j})
$$

for any choice of $\mathbf{j} \in \mathbf{J}(w)$.
Note that for $w \in W_{c}$, the number of times a given generator occurs in a reduced expression is independent of the reduced expression. Therefore, it makes sense to define $c_{z}=\frac{1}{n_{11} \cdot n_{t(z)}} f_{z}\left(w_{0}\right), z \in W_{c}, \mathbf{i} \in \mathbf{J}(z)$. Here, the $n_{i}$ are as defined in the statement of Proposition 4.

Proposition 5 Proposition 4 is equivalent to the set of equations:

$$
c_{z}=\frac{\operatorname{card}(\mathbf{J}(z))}{l(z)!}
$$

where $z \in W_{c}$.
Proof: Let $\mathbf{U}^{+}$be the universal enveloping algebra of $\mathfrak{u}^{+}$. Define

$$
\tilde{\mathbf{U}}^{+}=\frac{\mathbf{U}^{+}}{\sum_{i \in \mathbf{I}} \mathbf{U}^{+} E_{i}^{2} \mathbf{U}^{+}}
$$

Let $\bar{E}_{l}$ denote the image of $E_{i}$ in $\overline{\mathbf{U}}^{+}$. The Serre relation $2 E_{l} E_{i} E_{i}=E_{1}^{2} E_{2}+E_{2} E_{1}^{2}$ implies that $\bar{E}_{t} \bar{E}_{j} \bar{E}_{t}=0$ in $\overline{\mathbf{U}}^{+}$whenever $\left(s_{i} s_{j}\right)^{3}=1$.

We now return to the algebra $\bar{H}$. Let $e_{s}=q \tau_{s}$. We see that $\bar{H}$ is the algebra generated by the $e_{s}, s \in S$ with the following relations: (1) $e_{s_{-}}^{2}=q(q+1) e_{s}$, (2) $e_{s} e_{t}=e_{t} e_{s}$, if $s t=t s$, and (3) $e_{s} e_{t} e_{s}=q^{3} e_{s}$, if $(s t)^{3}=1$. Let $\bar{H}_{\mathfrak{Q}_{[q]}}$ be the $\mathfrak{Q}[q]$-subalgebra of $\bar{H}$ generated by the $e_{s}$. As a $\mathfrak{Q}[q]$-module, this is free with basis $e_{w}=q^{l(w)} \tau_{w}, w \in W_{c}$. Let $\bar{H}_{0}=\bar{H}_{\mathfrak{Q}[q]} \otimes_{\mathfrak{Q}[q]} \mathfrak{C}$ where $q$ acts as 0 on the $\mathfrak{Q}[q]$-module $\mathfrak{C}$. This is the the specialization of $\bar{H}_{Q_{[q]}}$ to $q=0$ with base field extended to $\mathfrak{C}$.

By construction, we have an algebra isomorphism $\psi: \bar{H}_{0} \cong \overline{\mathbf{U}}^{+}$where $\psi\left(e_{s_{1}}\right)=\bar{E}_{i}$.
For any $\mathbf{i}=\left(i_{1}, \ldots, i_{n}\right) \in \mathbf{I}^{n}$, denote by $\bar{E}_{\mathbf{i}}$ the monomial $\bar{E}_{i_{1}} \cdots \bar{E}_{i_{n}}$. By convention, when $n=0$ we set $\bar{E}_{\mathbf{i}}=1$. For each $z \in W_{c}$, choose $\mathbf{i}(z) \in \mathbf{J}(z)$.

Lemma 5 The set of monomials $\left\{\bar{E}_{\mathbf{i}}(z) \mid z \in W_{c}\right\}$ form a basis for the algebra $\overline{\mathbf{U}}^{+}$.
Proof: Via the isomorphism $\psi$, this is equivalent to showing that $\left\{e_{w}\right\}_{w \in W_{c}}$ is a basis of $\bar{H}_{0}$. Since $\bar{H}_{\mathfrak{Q}_{[q]}}$ is free over $\mathfrak{Q}[q]$, we see that $\operatorname{dim}_{\mathfrak{C}}\left(\bar{H}_{0}\right)=\operatorname{dim}_{\mathfrak{Q}_{[q]}} \bar{H}_{\mathfrak{Q}_{[q]}}$. The lemma follows.

Lemma 6 There exists a unique injective group homomorphism $\iota: U^{+} \hookrightarrow\left(\overline{\mathbf{U}}^{+}\right)^{*}$ such that $\exp \left(a E_{i}\right) \mapsto 1+a \bar{E}_{i}$ where $a \in \mathfrak{C}$.

Proof: Because $U^{+}$is unipotent, $\exp : \mathfrak{u}^{+} \mapsto U^{+}$is a bijection. Observe that $\overline{\mathbf{U}}^{+}=$ $\mathfrak{C} \oplus \operatorname{rad}\left(\overline{\mathbf{U}}^{+}\right)$. Therefore $\exp : \operatorname{rad}\left(\overline{\mathbf{U}}^{+}\right) \mapsto 1+\operatorname{rad}\left(\overline{\mathbf{U}}^{+}\right) \subset\left(\overline{\mathbf{U}}^{+}\right)^{*}$ is an injection into $\overline{\mathbf{U}}^{+}$.

By the Poincare-Birkoff-Witt theorem, the natural map ${ }^{-}: \mathfrak{u}^{+} \mapsto \overline{\mathbf{U}}^{+}$is injective because $\overline{\mathbf{U}}^{+}$is obtained from $\mathbf{U}^{+}$by reducing modulo elements of homogeneity 2.

Using functoriality of the exponential map between nilpotent Lie algebras and unipotent groups, we get the desired map $\iota$. One can check that $\iota\left(\exp \left(a E_{i}\right)\right)=1+a \bar{E}_{i}$ and the lemma follows.

By Lemma 6, Proposition 4 holds if and only if the formula holds in $\overline{\mathbf{U}}^{+}$via the homomorphism $\iota$.

Direct computation reveals that the formula becomes

$$
\sum_{z \in W_{c}} c_{z} \bar{E}_{\mathbf{i}(\mathrm{z})}=\sum_{z \in W_{c}} \frac{\operatorname{card}(\mathbf{J}(z))}{l(z)!} \bar{E}_{\mathrm{i}(\mathbf{z})}
$$

when interpreted as a formula in $\overline{\mathbf{U}}^{+}$.
By Lemma 5, this equality can occur if and only if the various coefficients are equal, whence the proposition.

## References

1. D. Alvis, "Induce/restrict matrices for exceptional Weyl groups," Manuscript.
2. S.C. Billey, W. Jockusch, and R.P. Stanley, "Some combinatorial properties of Schubert polynomials," J. Alg. Combin. 2 (1993), 345-374.
3. N. Bourbaki, Groupes et algèbres de Lie, Chapitres 4, 5, et 6, Masson, Paris, 1981.
4. C.K. Fan and G. Lusztig, "Factorization of certain exponentials in Lie groups," to appear in Tribute to R.W. Richardson.
5. J.S. Frame, "The characters of the Weyl group $E_{8}$," Computational Problems in Abstract Algebra (Oxford conference, 1967), ed. J. Leech, 111-130.
6. V.F.R. Jones, "A polynomial invariant for knots via Von Neumann algebras," Bulletin of the Amer. Math. Soc. 12(1) (1985), 103-111.
7. V.F.R. Jones, "Hecke algebra representations of braid groups and link polynomials," Annals of Mathemattcs 126 (1987), 335-388.
8. G. Lusztig, "Characters of reductive groups over a finite field," Annals of Mathematical Studies No. 107, Princeton University Press, 1984.
9. G. Lusztig, "Total positivity in reductive groups," in Lie Theory and Geometry (In Honor of Bertram Kostant), Birkhaüser, Boston, 1994.
10. J.R. Stembridge, "On the fully commutative elements of Coxeter groups," to appear in Journal Alg. Combin.
11. H.N.V. Temperley and E.H. Lieb, "Relations between the percolation and colouring problem. . ," Proceedings of the Royal Society of London (1971), 251-280.
