CANONICAL BASES FOR THE MINISCULE MODULES OF THE QUANTIZED ENVELOPING ALGEBRAS OF TYPES B AND D

1 Introduction

Let $\mathbf{g}$ be a finite-dimensional semisimple Lie algebra over $\mathbb{C}$, and let U be the q-analogue of its universal enveloping algebra defined by Drinfel'd [3] and Jimbo [5]. According to [7, 3.5.6, 6.2.3 & 6.3.4], for each dominant weight λ in the weight lattice of $\mathbf{g}$ there is an irreducible, finite-dimensional highest weight U-module $V(\lambda)$ with highest weight λ. Kashiwara [6] and Lusztig [7, 14.4.12] have independently shown the existence of a certain canonical basis $\mathbf{B}(\lambda)$ for $V(\lambda)$. For $1 \leq r \leq \text{rank}(\mathbf{g})$ let ω_r be the r-th fundamental weight (see §§2 and 3 for the numbering of the Dynkin diagrams we are using). Suppose that $\mathbf{g}$ is of type B_{n-1} or D_n ($n \geq 4$). In the former case, fix $r = n-1$, and in the latter case, fix $r \in \{1, n-1, n\}$. Let V_r be the fundamental U-module $V(\omega_r)$. Then V_r is miniscule (see [1, VIII,§7.3]). Let W^r be the set of distinguished left coset representatives in the Weyl group W of $\mathbf{g}$ with respect to the parabolic subgroup W_r generated by all of the fundamental generators $s_1, s_2, \ldots, s_n$ of W except s_r.

In this paper we show that there is a natural correspondence between W^r and the canonical basis of V_r. In §2, we concentrate on the D_n case. We examine the set W^r in detail and prove some properties of reduced expressions for its elements, which enable us to define a natural map ϕ_r from W^r to U^-, the minus part of U, which takes elements of W^r to monomials. This is extended to an injective map ψ_r from W^r to V_r whose image turns out to be the canonical basis of V_r. In §3, we prove similar results for V_{n-1} in the type B_{n-1} case, in a similar way. However in this case we first list the elements of W^{n-1} explicitly in order to prove properties for reduced expressions for them. This approach could have been used in cases A and D but was not necessary.

Note: Since completing this work, the author has learnt that in [7, 28.1], Lusztig proves a theorem which provides a description of the canonical basis for miniscule modules. It can be seen that the above bijection is a special case of this. Here, we provide an alternative proof, and the canonical basis is made explicit. Along the way, various results about W^r and V_r are shown which are both interesting in their own right and give reasons why the correspondence described above should be true. We now go into more detail.

We use the treatment in [7, §§1-3]. Let $\mathbf{g}$ be a semisimple Lie algebra of type B_n or D_n, with root system Φ, simple roots $\alpha_1, \alpha_2, \dots, \alpha_n$, and Killing form $(\ ,\ )$. Let $h_1, h_2, \dots, h_n$ be a basis for a Cartan subalgebra $\mathbf{h}$ of $\mathbf{g}$, satisfying $(h_i, h) = \alpha_i^*(h)$ for all h in $\mathbf{h}$ and all $i \in I = \{1, 2, \dots, n\}$. Let Y be the $\mathbb{Z}$-lattice spanned by $h_1, h_2, \dots, h_n$. Let $\omega_1, \omega_2, \dots, \omega_n$ be the fundamental weights of $\mathbf{g}$, defined by $\omega_i(h_j) = \delta_{ij}$, and let X be the $\mathbb{Z}$-lattice spanned by them (the weight lattice). Let d be the minimal positive integer so that $d(\alpha_i, \alpha_j)$ is always an integer and $d(\alpha_i, \alpha_i)$ is always even. If the largest common factor of the $d(\alpha_i, \alpha_j)$ and the $\frac{1}{2}d(\alpha_i, \alpha_i)$ is not 1, then replace d by d divided by this highest common factor. We then define $i \cdot j$ to be $d(\alpha_i, \alpha_j)$ for each $i, j \in I$, so $(I, \cdot)$ is a Cartan datum as in [7, 1.1.1]. For $\mu \in Y$ and $\lambda \in X$, define $\langle \mu, \lambda \rangle$ to be $\lambda(\mu)$. Define an imbedding of I into Y by $i \mapsto h_i$ and into X by $i \mapsto \alpha_i$ for all $i \in I$. We then have a root datum of type $(I, \cdot)$ as in [7, 2.2.1], with $\langle h_i, \alpha_j \rangle = \alpha_j(h_i) = A_{ij}$ the corresponding symmetrizable Cartan matrix. For each $i \in I$, we define d_i to be the integer $\frac{1}{2}d(\alpha_i, \alpha_i)$. Then $d_i A_{ij} = \frac{1}{2}d(\alpha_i, \alpha_i)\left(\frac{2(\alpha_i, \alpha_j)}{(\alpha_i, \alpha_i)}\right) = d(\alpha_i, \alpha_j)$ for each $i, j \in I$, and is thus a symmetric matrix over $\mathbb{Z}$.

Let $\mathbb{Q}(v)$ be the field of rational functions in an indeterminate v, and $\mathcal{A} \subseteq \mathbb{Q}(v)$ the ring $\mathbb{Z}[v, v^{-1}]$. For $N, M \in \mathbb{N}$ and $i \in I$ we put $v_i = v^{d_i}$ and define the following (which all lie in $\mathcal{A}$):

$$[N]_i = \frac{v_i^N - v_i^{-N}}{v_i - v_i^{-1}}, \quad [N]_i^! = [N]_i[N-1]_i \cdots [1]_i, \quad \begin{bmatrix} M \\ N \end{bmatrix}_i = \frac{[M]_i^!}{[N]_i^![M-N]_i^!}.$$

These are referred to as quantized integers, quantized factorials and quantized binomial coefficients, respectively. If v is specialized to 1 they specialize to the usual integers, factorials and binomial coefficients.

We define the quantized enveloping algebra U corresponding to the above data (as in [7, 3.1.1 & 33.1.5]) to be the $\mathbb{Q}(v)$-algebra U with generators $1, E_1, E_2, \dots, E_n$, $F_1, F_2, \dots, F_n$, and K_μ for $\mu \in Y$, subject to the relations: (for each $i, j \in I$ and

$\mu, \mu' \in Y$)

$$K_0 = 1,$$

$$K_\mu K_{\mu'} = K_{\mu+\mu'},$$

$$K_\mu E_i = v^{\alpha_i(\mu)} E_i K_\mu,$$

$$K_\mu F_i = v^{-\alpha_i(\mu)} F_i K_\mu,$$

$$E_i F_i - F_i E_i = \frac{\tilde{K}_i - \tilde{K}_i^{-1}}{v_i - v_i^{-1}},$$

$$E_i F_j - F_j E_i = 0, \quad i \neq j,$$

$$\sum_{p+p'=1-A_{ij}} (-1)^{p'} \left[\begin{array}{c} 1-A_{ij} \\ p' \end{array} \right]_i E_i^p E_j E_i^{p'} = 0, \quad i \neq j,$$

$$\sum_{p+p'=1-A_{ij}} (-1)^{p'} \left[\begin{array}{c} 1-A_{ij} \\ p' \end{array} \right]_i F_i^p F_j F_i^{p'} = 0, \quad i \neq j,$$

(where, for $i \in I$, we put $\tilde{K}_i = K_{d_i h_i}$ and $\tilde{K}_i^{-1} = K_{-d_i h_i}$). In the last two summations, p and p' are restricted to the non-negative integers.

We make the following definitions (see [7, 3.1.1 & 3.1.13]). For $M \in \mathbb{N}$, and $i \in I$, we put $E_i^{(M)} = E_i^M/[M]_i^!$, and $F_i^{(M)} = F_i^M/[M]_i^!$, which are called *divided powers*. We also put $K_i = K_{h_i}$ and $K_i^{-1} = K_{-h_i}$ for $i \in I$. Let $U_\mathcal{A}$ be the $\mathcal{A}$-subalgebra of U generated by the elements $E_i^{(N)}, F_i^{(N)}, K_\mu$ for $i \in I$, $N \in \mathbb{N}$ and $\mu \in Y$. It is called the *integral form* of U. Let U^+ be the $\mathbb{Q}(v)$-subalgebra of U generated by the E_i, $i \in I$, and $U_\mathcal{A}^+$ the $\mathcal{A}$-subalgebra of U generated by $E_i^{(N)}$, $i \in I, N \in \mathbb{N}$. Let U^- be the $\mathbb{Q}(v)$-subalgebra of U generated by the F_i, $i \in I$, and $U_\mathcal{A}^-$ the $\mathcal{A}$-subalgebra of U generated by $F_i^{(N)}$, $i \in I, N \in \mathbb{N}$. Let U^0 be the $\mathbb{Q}(v)$-subalgebra generated by the K_μ, $\mu \in Y$.

Let W be the Weyl group of $\mathbf{g}$. So W is the group:

$$W = \langle s_1, s_2, \ldots, s_n \mid s_i^2 = 1, (s_i s_j)^{m_{ij}} = 1 \ (i \neq j) \rangle$$

where $m_{ij} = 2, 3, 4, 6$ if $A_{ij}A_{ji} = 0, 1, 2, 3$, respectively. For $r \in I$, let W^r be the set of distinguished left coset representatives of the parabolic subgroup W_r of W generated by $\{s_1, s_2, \ldots, s_n\} \setminus \{s_r\}$.

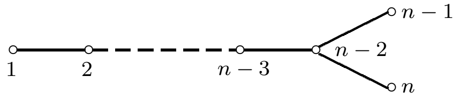
Let $X^+ \subseteq X$ be the set of dominant weights, i.e. those of the form $\lambda_1\omega_1 + \lambda_2\omega_2 + \cdots + \lambda_n\omega_n \in X$ where $\omega_1, \omega_2, \ldots, \omega_n$ are the fundamental weights of $\mathbf{g}$ and

$\lambda_1, \lambda_2, \ldots, \lambda_n \in \mathbb{N}$. If L is a U-module, $x \in L$ and $\lambda \in X$, we say that x has weight λ if $K_\mu x = v^{\lambda(\mu)} x$ for all $\mu \in Y$. We call the subspace of L consisting of all of the elements of weight λ the λ-*weight space* of L. As in [7, 3.4.1], we restrict our attention to U-modules which are direct sums of their weight spaces. We say that $x \in L$, $x \neq 0$, is a *highest* (respectively, *lowest*) weight vector if x has weight λ, for some $\lambda \in X$, $E_i x = 0$ (respectively, $F_i x = 0$) for each $i \in I$ and $U^- x = L$ (respectively, $U^+ x = L$). Such a vector is uniquely determined up to a non-zero scalar multiple. We say that L is a highest weight module with highest weight λ if it contains a highest weight vector of weight λ. Let $\lambda = \lambda_1\omega_1 + \lambda_2\omega_2 + \cdots + \lambda_n\omega_n$ be a dominant weight. We follow the construction in [7, 3.4.5 & 3.5.6]. Let J be the left ideal of U generated by the elements E_i for $i \in I$ and the elements $K_\mu - v^{(\lambda(\mu))}$ for $\mu \in Y$. Then the map from U^- to U/J taking $x \in U^-$ to $x + J$ is a $\mathbb{Q}(v)$-vector space isomorphism, which can be used to transfer the left U-module structure of U/J to U^-. The resulting U-module we denote by $M(\lambda)$; it is the called a *Verma module*. Let $T(\lambda)$ be the left ideal of $M(\lambda)$ (as a $\mathbb{Q}(v)$-algebra) generated by the elements $F_i^{\lambda_i+1}$, for $i \in I$, and let $V(\lambda)$ be the quotient module $M(\lambda)/T(\lambda)$. Then, by [7, 6.2.3 & 6.3.4], $V(\lambda)$ is an irreducible, finite-dimensional highest weight U-module with highest weight λ, unique up to isomorphism. We fix x_1 as the image of $1 \in M(\lambda)$ under the natural map from $M(\lambda)$ to $V(\lambda)$. Then x_1 is a highest weight vector for $V(\lambda)$. If λ and λ' are any two distinct dominant weights, then $V(\lambda)$ and $V(\lambda')$ are not isomorphic (see [7, 6.2.3(b)]). It is known that $V(\lambda)$ is the direct sum of its weight spaces (see [7, 3.4.1 & 3.5.6]). We also write $V(\lambda)_{\mathcal{A}} = U_{\mathcal{A}}^- x_1$, the integral form of $V(\lambda)$ (see [7, 19.3.1]). For $\mu \in Y$, we have $K_\mu V(\lambda)_{\mathcal{A}} \subseteq V(\lambda)_{\mathcal{A}}$, since K_μ always acts as an integral power of v on an element in a weight space and $V(\lambda)_{\mathcal{A}}$ is the direct sum of its weight spaces (see [7, 19.3.1]). Therefore, by [7, 19.3.2], $V(\lambda)_{\mathcal{A}}$ is a $U_{\mathcal{A}}$-module. For each $r \in I$ we denote by V_r the module $V(\omega_r)$ with highest weight ω_r. This is called the r-th *fundamental module* for U.

2 The Canonical Basis of the Miniscule Modules in Case D.

Throughout this section we assume that $\mathbf{g}$ is of type D_n and that $r \in \{1, n-1, n\}$. We recall here the Dynkin diagram of type D_n:

D_n



The V_r with r in this set are the only miniscule modules in type D_n (see [1, VIII,§7.3]). We note that $|W^1| = 2n$, $|W^{n-1}| = |W^n| = 2^{n-1}$, and that this is also the dimension of V_r over $\mathbb{Q}(v)$ in each case. We also note that if $s_{i_1}s_{i_2}\cdots s_{i_t}$ is a reduced expression for an element $w \in W^r \setminus \{1\}$ then $s_{i_1}w = s_{i_2}\cdots s_{i_t} \in W^r$. This follows immediately from the fact that

$$W^r = \{w \in W : \ell(ws_i) > \ell(w)\ \forall i \in I,\ i \neq r\},$$

where ℓ is the standard length function on W. We shall need the following:

Lemma 2.1 *Suppose that $s_{i_1}s_{i_2}\cdots s_{i_t} = s_{j_1}s_{j_2}\cdots s_{j_t}$ are two reduced expressions for an element $w \in W$. Then there exists a finite sequence of braid relations which, when applied to the first expression, in order, gives the second.*

Proof: This result is due to Matsumoto; see [2, 64.20]. □

The following lemma is a key step in pinning down the elements of W^r.

Lemma 2.2 *Suppose $s_{i_1}s_{i_2}\cdots s_{i_t}$ is a reduced expression for an element $w \in W^r$ of length at least 3. Then, in the list $i_1, i_2, \ldots, i_t$, there is no sequence p, q, p with $A_{pq} = -1$. So no long braid relation $s_ps_qs_p = s_qs_ps_q$ can be applied directly to this expression.*

Proof: We prove this in the same way as in type A (see Lemma [8, 2.1]). By the above remarks we can suppose that $w = s_ps_qs_ps_{i_4}\ldots s_{i_t}$ (and try to get a contradiction).

By [4, p14] we see that the following positive roots are all sent to negative roots by w:

$$\begin{aligned}\beta_1 &= s_{i_t}s_{i_{t-1}}\cdots s_{i_4}s_ps_q(\alpha_p),\\ \beta_2 &= s_{i_t}s_{i_{t-1}}\cdots s_{i_4}s_p(\alpha_q),\\ \beta_3 &= s_{i_t}s_{i_{t-1}}\cdots s_{i_4}(\alpha_p).\end{aligned}$$

Since $s_ps_q(\alpha_p) = \alpha_q$ and $s_p(\alpha_q) = \alpha_p + \alpha_q$, it is easily seen that $\beta_1 + \beta_3 = \beta_2$. However, we know that for $i \neq r$, $w(\alpha_i) > 0$ while $w(\alpha_r) < 0$. Hence if α is any positive root made negative by w, the coefficient of α_r in the expression of α as an integral combination of fundamental roots should be at least 1. We claim that by the structure of the root system of type D, this coefficient must be 1. The Lie algebra is of type D_n, so the positive roots are given by:

$$\begin{aligned}\alpha_i + \cdots + \alpha_{j-1};\ i < j,\\ \alpha_i + \cdots + \alpha_{n-2} + \alpha_n + \alpha_j + \cdots + \alpha_{n-1};\ i < j,\end{aligned}$$

(by [9, §2.14,p78]). Observing these, one can see that the coefficient of α_1, α_{n-1} or α_n is always at most 1, so the claim is shown. It is now clear that that the above situation cannot occur, since necessarily the coefficient of α_r in β_2 is 2. We have a contradiction and the lemma is proved. □

We return now to the fundamental modules V_r, $r = 1, 2, \ldots, n$. If x_1 is our fixed weight vector in V_r, it is clear from the definition of $V(\lambda)$, that in V_r, we have $F_ix_1 = 0$ if $i \neq r$ and $F_r^2x_1 = 0$.

Lemma 2.3 *Suppose that* $\xi = F_i^2F_{i_1}F_{i_2}\cdots F_{i_t} \in U^-$. *Then* $\xi x_1 = 0$.

Proof: We start with the case when $r = 1$. Let $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n$ be the coordinate functions on the Cartan subalgebra $\mathbf{h}$ of the Lie algebra consisting of the diagonal matrices contained in the Lie algebra as in [9, §2.14]. These form a basis for $\mathbf{h}^*$. The following information can be found in [9, §§2.14 & 3.6]. The fundamental weights are $\lambda_i = \varepsilon_1 + \varepsilon_2 + \cdots + \varepsilon_i$ for $1 \leq i \leq n-2$, $\lambda_{n-1} = \frac{1}{2}(\varepsilon_1 + \varepsilon_2 + \cdots + \varepsilon_{n-1} - \varepsilon_n)$ and $\lambda_n = \frac{1}{2}(\varepsilon_1 + \varepsilon_2 + \cdots + \varepsilon_{n-1} + \varepsilon_n)$. The fundamental roots are given by $\alpha_i = \varepsilon_i - \varepsilon_{i+1}$, for $i \in [1, n-1]$, and $\alpha_n = \varepsilon_{n-1} + \varepsilon_n$. The weights of V_1 are given by

$$\{\pm\varepsilon_1, \pm\varepsilon_2, \ldots, \pm\varepsilon_n\}.$$

Suppose that $\xi x_1 \neq 0$ in V_1. Then, because of its monomial form, it is a weight vector of V_1, and has weight $\pm\varepsilon_k$ for some $k \in I$. Suppose first that $i \in [1, n-1]$. Then $\alpha_i = \varepsilon_i - \varepsilon_{i+1}$. If $F_i^2 F_{i_1} F_{i_2} \cdots F_{i_t} x_1 \neq 0$ then it is a weight vector of V_1 of weight $-2\alpha_i \pm \varepsilon_k = -2\varepsilon_i + 2\varepsilon_{i+1} \pm \varepsilon_k$ which is not a weight of V_1 — a contradiction. Suppose next that $i = n$. Then $\alpha_i = \varepsilon_{n-1} + \varepsilon_n$. If $F_i^2 F_{i_1} F_{i_2} \cdots F_{i_t} x_1 \neq 0$ then it is a weight vector of V_1 of weight $-2\alpha_i \pm \varepsilon_k = -2\varepsilon_{n-1} - 2\varepsilon_n \pm \varepsilon_k$ which is not a weight of V_1 — a contradiction. We are forced to conclude that $\xi x_1 = 0$.

We next consider the case $r = n$. (The case $r = n-1$ is very similar.) In this case the weights of V_n are precisely those sums of the form $\pm\frac{1}{2}\varepsilon_1 \pm \frac{1}{2}\varepsilon_2 \pm \cdots \pm \frac{1}{2}\varepsilon_n$ with an even number of minus signs (see [9, §3.9]). Suppose that $\xi x_1 \neq 0$ in V_n. Then $F_{i_1} F_{i_2} \cdots F_{i_t} x_1 \neq 0$ and therefore (as it is of monomial form) it has weight of the above form. But then $-2\alpha_i = -2\varepsilon_i + 2\varepsilon_{i+1}$ (if $i \in [1, n-1]$) and $-2\alpha_i = -2\varepsilon_{n-1} - 2\varepsilon_n$ (if $i = n$) so it is clear that $-2\alpha_i$ plus the weight of $F_{i_1} F_{i_2} \cdots F_{i_t} x_1$ is not a weight of V_n, whence $\xi x_1 = 0$ and we are done. □

Lemma 2.4 *Suppose that $\xi = F_{i_1} F_{i_2} \cdots F_{i_t} \in U^-$ is a monomial (with $t \geq 3$) such that in the list $i_1, i_2, \ldots, i_t$ there is a sequence of the form p, q, p with $A_{pq} = -1$. Then $F_{i_1} F_{i_2} \cdots F_{i_t} x_1 = 0$.*

Proof: Without loss of generality we can assume such a sequence occurs at the start, since if $F_{i_k} F_{i_{k+1}} \cdots F_{i_t} x_1 = 0$ for some $k \geq 1$ then $F_{i_1} F_{i_2} \cdots F_{i_t} x_1 = 0$. Since $A_{pq} = -1$ the following relation holds in U^-:

$$F_p^{(2)} F_q - F_p F_q F_p + F_q F_p^{(2)} = 0.$$

Therefore we have

$$\begin{aligned} F_{i_1} F_{i_2} \cdots F_{i_t} x_1 &= F_p F_q F_p F_{i_4} \cdots F_{i_n} x_1 \\ &= F_p^{(2)} F_q F_{i_4} \cdots F_{i_n} x_1 - F_q F_p^{(2)} F_{i_4} \cdots F_{i_n} x_1 \\ &= 0, \end{aligned}$$

by Lemma 2.3, as required. □

It is clear from Lemmas 2.3 and 2.4 that if $\xi = F_{i_1} F_{i_2} \cdots F_{i_t}$ is any monomial satisfying $\xi x_1 \neq 0$, then ξ must satisfy the following conditions:

(a) We have $F_{i_t} = F_r$. Also, after any commuting of F_i's, the expression for ξ must still end in F_r. This is clear from the action of U^- on x_1.

(b) There is no way of commuting F_i's to get a subsequence of the form p, p in the list $i_1, i_2, \ldots, i_t$.

(c) There is no way of commuting F_i's to get a subsequence of the form p, q, p with $A_{pq} = -1$ in the list $i_1, i_2, \ldots, i_t$.

We now define a map $\phi_r : W^r \to U^-$ in the following manner:
Suppose that $w = s_{i_1} s_{i_2} \cdots s_{i_t}$ is a reduced expression for an element $w \in W^r$. We put:

$$\phi_r(w) = F_{i_1} F_{i_2} \cdots F_{i_t} \in U^-.$$

In particular, $\phi_r(1) = 1 \in U^-$. This map is well-defined: if $s_{j_1} s_{j_2} \cdots s_{j_t}$ is another reduced expression for w, there exists a finite sequence of braid relations taking $s_{i_1} s_{i_2} \cdots s_{i_t}$ to $s_{j_1} s_{j_2} \cdots s_{j_t}$ (by Lemma 2.1). By Lemma 2.2, these relations must all be commutations. By applying the same commutations in U^-, we get equality of $F_{i_1} F_{i_2} \cdots F_{i_t}$ and $F_{j_1} F_{j_2} \cdots F_{j_t}$. The following three results have proofs exactly the same as in the case when U is of type A (see Lemma 2.6, Proposition 2.7 and Theorem 2.8 in [8]).

Lemma 2.5 *Suppose that $\xi = F_{i_1} F_{i_2} \cdots F_{i_t}$ is a monomial in the F_i's in U^-, satisfying $\xi x_1 \neq 0$. Then $\xi \in \mathrm{Im}(\phi_r)$.* □

Proposition 2.6 *The function ϕ_r, defined above, defines a bijection ψ_r from W^r onto a basis $\mathcal{B}_r$ for V_r, given by the formula:*
If $w = s_{i_1} s_{i_2} \cdots s_{i_t} \in W^r$ is a reduced expression, put

$$\psi_r(w) = \phi_r(w) x_1 = F_{i_1} F_{i_2} \cdots F_{i_t} x_1. \ \square$$

Theorem 2.7 *The basis $\mathcal{B}_r$ for V_r is in fact, up to sign, the canonical basis for V_r. So, up to sign, the canonical basis for V_r is:*

$$\{F_{i_1} F_{i_2} \cdots F_{i_t} x_1 \ : \ s_{i_1} s_{i_2} \cdots s_{i_t} \text{ is a reduced expression for an element in } W^r\},$$

where $F_{i_1} F_{i_2} \cdots F_{i_t} x_1 = F_{j_1} F_{j_2} \cdots F_{j_t} x_1$ if and only if $s_{i_1} s_{i_2} \cdots s_{i_t} = s_{j_1} s_{j_2} \cdots s_{j_t}$.

Examples

(1) The case D_4. In this case we have:

$$W^1 = \{1,\ s_1,\ s_2s_1,\ s_3s_2s_1,\ s_4s_2s_1,\ s_4s_3s_2s_1,\ s_2s_4s_3s_2s_1,\ s_1s_2s_4s_3s_2s_1\}.$$

Therefore, in V_1,

$$\begin{aligned} \mathcal{B}_1 &= \{x_1,\ F_1x_1,\ F_2F_1x_1,\ F_3F_2F_1x_1,\ F_4F_2F_1x_1,\ F_4F_3F_2F_1x_1,\ F_2F_4F_3F_2F_1x_1, \\ &\quad F_1F_2F_4F_3F_2F_1x_1\}. \end{aligned}$$

(2) The case D_5. By calculating W^r in each case, we have:

$$\begin{aligned} \mathcal{B}_1 &= \{x_1, F_1x_1, F_2F_1x_1, F_3F_2F_1x_1, F_4F_3F_2F_1x_1, F_5F_3F_2F_1x_1, F_5F_4F_3F_2F_1x_1, \\ &\quad F_3F_5F_4F_3F_2F_1x_1, F_2F_3F_5F_4F_3F_2F_1x_1, F_1F_2F_3F_5F_4F_3F_2F_1x_1\} \end{aligned}$$

and $\mathcal{B}_5$ is given by the following elements:

$$x_1,$$

$$F_5x_1,$$

$$F_3F_5x_1,$$

$$F_2F_3F_5x_1,\ F_4F_3F_5x_1,$$

$$F_1F_2F_3F_5x_1,\ F_4F_2F_3F_5x_1,$$

$$F_4F_1F_2F_3F_5x_1,\ F_3F_4F_2F_3F_5x_1,$$

$$F_3F_4F_1F_2F_3F_5x_1,\ F_5F_3F_4F_2F_3F_5x_1,$$

$$F_2F_3F_4F_1F_2F_3F_5x_1,\ F_5F_3F_4F_1F_2F_3F_5x_1,$$

$$F_5F_2F_3F_4F_1F_2F_3F_5x_1,$$

$$F_3F_5F_2F_3F_4F_1F_2F_3F_5x_1,$$

$$F_4F_3F_5F_2F_3F_4F_1F_2F_3F_5x_1.$$

Note: It is possible to calculate W^r inductively on length, using the fact that if $s_{i_1}s_{i_2}\cdots s_{i_t}$ is a reduced expression for an element in W^r, then so is $s_{i_2}\cdots s_{i_t}$. We shall see later that in fact $\mathcal{B}_r$ is the canonical basis for V_r. Inspection of these examples gives us a hint of the general description of W^r.

Lemma 2.8 *For any n, we have:*

$$\begin{aligned} W^1 \;=\; &\{1,\ s_1,\ s_2s_1, \ldots ,\ s_{n-2}s_{n-3}\cdots s_1,\ s_{n-1}s_{n-2}s_{n-3}\cdots s_1, \\ &s_ns_{n-2}s_{n-3}\cdots s_1,\ s_ns_{n-1}s_{n-2}\cdots s_1,\ s_{n-2}s_ns_{n-1}s_{n-2}\cdots s_1, \\ &s_{n-3}s_{n-2}s_ns_{n-1}s_{n-2}\cdots s_1, \ldots ,\ s_1s_2\cdots s_{n-2}s_ns_{n-1}s_{n-2}\cdots s_1\}. \end{aligned}$$

Furthermore, each of these expressions is reduced.

Proof: It is clear that in each of the above expressions the only defining relations of the Weyl group that can be applied are commuting s_{n-1} and s_n. Therefore, each expression is reduced, and must end in s_1 (by Lemma 2.1)) unless it is equal to 1. Hence if X is the right-hand-side of the above equation, then $X \subseteq W^1$. The elements $s_{n-1}s_{n-2}\cdots s_1$ and $s_ns_{n-2}s_{n-3}\cdots s_1$ cannot be equal, since if they were we would have $s_{n-1} = s_n$ (which cannot happen; see [4, Prop. 5.3]). Since they are the only two expressions of the same length in the list, all of the elements listed are distinct and we have $|X| = 2n = |W^1|$, whence $X = W^1$ as required. □

The case when $r = n-1$ or n is a little harder. We consider only the case when $r = n$ since the case $r = n-1$ is very similar, and can be obtained from the case $r = n$ by applying the automorphism of W which exchanges s_{n-1} and s_n and keeps everything else fixed. There now follows a description of an algorithm which generates elements of the Weyl group W of type D_n. They will eventually be shown to constitute W^n.

For each sequence (of any length $k \geq 0$), $0 < m_1 < m_2, \cdots < m_k \leq n-1$, we construct a sequence $z_{m_1,m_2,\ldots m_k}$ as follows: put

$$a_1 = n,\ a_2 = n-2,\ a_3 = n-3,\ \ldots , a_{n-1} = 1,$$

$$b_1 = n-1,\ b_2 = n-2,\ b_3 = n-3,\ \ldots , b_{n-1} = 1.$$

Define:

$$z_{m_1,m_2,\ldots,m_k} = \ldots\ldots , a_{m_{k-2}}, \ldots , a_2, a_1, b_{m_{k-1}}, \ldots , b_2, b_1, a_{m_k}, \ldots , a_2, a_1,$$

so $z_{m_1,m_2,\ldots,m_k}$ is a concatenation of k subsequences, each of the form $a_{m_i}, \ldots , a_2, a_1$ or $b_{m_i}, \ldots , b_2, b_1$, taken alternately. Let $w_{m_1,m_2,\ldots,m_k}$ be the corresponding element of the Weyl group obtained by replacing each positive integer, d, in the sequence by the corresponding fundamental reflection s_d.

Example

Suppose we are in case D_5, and choose the sequence $0 < 1 < 2 < 3 < 4 \leq 5 - 1$. We obtain the following element of the Weyl group:

$$(s_4)(s_3 s_5)(s_2 s_3 s_4)(s_1 s_2 s_3 s_5). \tag{1}$$

To prove that these elements constitute W^n we shall need the following two lemmas:

Lemma 2.9 *Suppose that $i_1, i_2, \dots, i_t$ is a sequence generated by the algorithm, and that $i_k = i_1$ is the second appearance of i_1 in the sequence. Then in the set $\{i_m : 2 \leq m \leq k-1\}$ there are precisely two i_m's such that $A_{i_1, i_m} = -1$. Precisely which two occur is given by the following table:*

TABLE 1

i_1	*occurrences*
$2, \dots, n-3$	$i_1 - 1$ *and* $i_1 + 1$
$n-2$	$n-3$ *and exactly one of* $n-1$ *and* n
$n-1, n$	2 $(n-2)$*'s*

Proof: Note first that it is clear from the definition of the algorithm that the case $i_1 = 1$ cannot occur. We analyse the elements produced by the algorithm carefully. Firstly, suppose $1 \leq i_1 \leq n-3$. For this situation, one occurrence must be in a subsequence of the form $a_{m_s} \dots a_2 a_1$ and the other in one of the form $b_{m_t} \dots b_2 b_1$. Furthermore, since no i_1 can occur between them we must have $t = s \pm 1$. We assume that $t = s + 1$ (the argument in the case $t = s - 1$ is similar). The part of the sequence between the two occurrences of i_1 is thus of the form $(i_1 + 1) \cdots (n-2) n (b_{m_{s+1}}) \cdots (i_1 - 1)$ since $m_s < m_{s+1}$, and we see directly that the lemma holds in this case. Next, suppose $i_1 = n - 2$. The part of the sequence between the two occurrences of $n-2$ must be of the form $a_1 b_{m_s} \dots b_3$ or $b_1 a_{m_s} \dots a_3$ for some s. Since $n-2$ must appear in the subsequence corresponding to m_{s-1}, we must have $m_{s-1} \geq 2$, whence $m_s \geq 3$ so the a_3 or b_3 does actually occur. In the former case the lemma holds with $b_3 = n-3$ and $a_1 = n$. In the latter case the lemma holds with $a_3 = n-3$ and $b_1 = n-1$. Finally suppose that $i_1 = n$ (the case $i_1 = n-1$ is similar). Then the part of the sequence between the two occurrences of n is of the form $b_{m_{s-1}} \dots b_2 b_1 a_{m_s} \dots a_2$. Since here a_1 must appear in the subsequence corresponding to m_{s-2} we must have $m_{s-2} \geq 1$, whence $m_{s-1} \geq 2$ and $m_s \geq 2$, so the a_2 and b_2 do actually occur. The lemma is seen to hold in this case with $a_2 = b_2 = n - 2$. The lemma is proved. □

Lemma 2.10 *Suppose that $i_1, i_2, \dots, i_t$ is a sequence of length at least 2 generated by the algorithm, and that i_1 occurs in the sequence in the first place only. Then, in the set $\{i_m : 2 \leq m \leq t\}$, there is precisely one i_m such that $A_{i_1,i_m} = -1$, given by the following table:*

TABLE 2

i_1	*occurrence*
$1, \dots, n-3$	$i_1 + 1$
$n-2$	n
$n-1$	$n-2$

Proof: Note that the case $i_1 = n$ cannot occur since the length of the sequence is stipulated to be at least 2. We consider the various possibilities in the algorithm. Suppose first that $1 \leq i_1 \leq n-3$. The subsequence to the right of the last occurrence of i_1 (including i_1) must be $(i_1)(i_1+1)\cdots(n-2)(n)$ and we are done in this case. Suppose next that $i_1 = n-2$. Then the sequence to the right of i_1 must be $(n-2)(n)$ and the lemma holds in this case. Next suppose $i_1 = n-1$. The sequence to the right of i_1 then looks like $(n-1)(a_{m_k})\dots(a_2)(a_1)$ which is $(n-1)(a_{m_k})\dots(n-2)(n)$ and the lemma is seen to hold in this case. We are done. □

We can now prove the desired result:

Proposition 2.11 *The elements $w_{m_1,m_2,\dots,m_k}$ produced in the above algorithm exactly constitute the elements of W^n.*

Proof: We know that $|W^n| = 2^{n-1}$. We check that the number of sequences the algorithm generates is also 2^{n-1}. We use induction on n to do this. The base case is when $n = 4$. It is easy to check that in this case the algorithm produces 8 elements as required. Now assume the result to be true for n. To show the result for $n+1$ we need to count the possible sequences $0 < m_1 < m_2 \cdots < m_k \leq n$. By the inductive hypothesis, the number of sequences with $m_k \leq n-1$ is equal to 2^{n-1}. If $m_k = n$ (the only other possibility) then $0 < m_1 < m_2 \cdots < m_{k-1} \leq n-1$ so, as there is no restriction on k, there are also 2^{n-1} sequences of this type, whence the total number in case D_{n+1} is 2^n as required. By induction we see that $|W^n| = 2^n$ for $n = 4, 5, \ldots$.

Suppose now that $z_{m_1,m_2,\ldots,m_k}$ is a sequence generated by the algorithm, and that $w_{m_1,m_2,\ldots,m_k}$ is the corresponding element of the Weyl group, with expression determined by $z_{m_1,m_2,\ldots,m_k}$. Then, by Lemma 2.9, between every two occurrences of the same fundamental reflection s_i in this expression there are exactly two fundamental reflections which do not commute with s_i. It is clear that this will still be true even after commutations are applied to the expression. We conclude that no subexpression of the form $s_p s_q s_p$ with $A_{pq} = -1$ or of the form $s_p s_p$ can occur, even after commutations are applied. Therefore the expression for $w_{m_1,m_2,\ldots,m_k}$ produced by the algorithm must be reduced. Furthermore, by Lemma 2.10, if s_i occurs in the expression (for some $i \neq n$), and no s_i occurs further on in the expression, then s_i cannot be commuted to the end of the expression. It follows that, since commutations are the only defining relations of W that can be applied to the expression (we use Lemma 2.1), every reduced expression for $w_{m_1,m_2,\ldots,m_k}$ must end with the fundamental reflection s_n (unless $w_{m_1,m_2,\ldots,m_k} = 1$), whence $w_{m_1,m_2,\ldots,m_k} \in W^n$. Thus all the elements generated by the algorithm lie in W^n. Suppose that $z_{m_1,m_2,\ldots,m_k}$ and $z_{m'_1,m'_2,\ldots,m'_l}$ are two sequences generated by the algorithm, with corresponding elements $w_{m_1,m_2,\ldots,m_k}$ and $w_{m'_1,m'_2,\ldots,m'_l}$ which are equal. Since $a_1 = n$ and each $m_r \geq 1$, each subsequence of $z_{m_1,m_2,\ldots,m_k}$ of the form $a_{m_r} \cdots a_2 a_1$ must contain exactly one n. Similarly each subsequence of the form $b_{m_r} \cdots b_2 b_1$ must contain exactly one $n-1$. Therefore the whole sequence contains precisely k occurrences in total of $n-1$ and n, and so in total there are precisely k occurrences of s_{n-1} and s_n in the corresponding expression for $w_{m_1,m_2,\ldots,m_k}$. Similarly there are precisely l occurrences in total of s_{n-1} and s_n in the expression for $w_{m'_1,m'_2,\ldots,m'_l}$. Since both reduced expressions are equal in W and commutations are the only braid relations of W which can be applied to either expression, we have by Lemma 2.1 that $k = l$. Comparing the lengths of the expressions for $w_{m_1,m_2,\ldots,m_k}$ and $w_{m'_1,m'_2,\ldots,m'_l}$ (they must be the same) we see that $m_1 + m_2 + \cdots + m_k = m'_1 + m'_2 + \cdots + m'_k$. Since $0 < m_1 < m_2 < \cdots < m_k$ and $0 < m'_1 < m'_2 < \cdots < m'_k$ we must have $m_1 = m'_1,\ m_2 = m'_2, \ldots, m_k = m'_k$.

Therefore, all of the elements produced by the algorithm are distinct. Since there are $|W^n|$ of them and they all lie in W^n, we conclude that W^n is precisely the set of elements produced by the algorithm, and the proposition is proved. □

We now have:

Corollary 2.12 *Suppose that $r \in \{1, n\}$ and that $s_{i_1} s_{i_2} \cdots s_{i_t}$ is a reduced expression for an element $w \in W^r$, and that $s_{i_k} = s_{i_1}$ is the second appearance of s_{i_1} in the expression. Then in the set $\{s_{i_m} \; : \; 2 \leq m \leq k-1\}$ there are precisely two fundamental reflections which do not commute with s_{i_1}. Precisely which two occur is given by the following table:*

TABLE 3

i_1	*occurrences when $r = 1$*	*occurrences when $r = n$*
$1, \ldots, n-3$	$2 \ (i_1 + 1)$*'s*	$i_1 - 1$ *and* $i_1 + 1$
$n-2$	*one each of $n-1$ and n*	*$n-3$ and exactly one of $n-1$ and n*
$n-1, n$	—	$2 \ (n-2)$*'s*

If $r = 1$, we cannot have $i_1 = n-1$ or n; if $r = n$, we cannot have $i_1 = 1$.

Proof: What happens when $r = 1$ is easily checked directly, using Lemma 2.8. The case $r = n$ follows from Proposition 2.11 and Lemma 2.9. □

Corollary 2.13 *Suppose that $r \in \{1, n\}$ and that $s_{i_1} s_{i_2} \cdots s_{i_t}$ is a reduced expression for an element $w \in W^r$ of length at least 2 with s_{i_1} occurring in the expression in the first factor only. Then, in the set $\{s_{i_m} \; : \; 2 \leq m \leq t\}$, there is precisely one fundamental reflection which does not commute with s_{i_1}, given by the following table:*

TABLE 4

i_1	*occurrences when $r = 1$*	*occurrences when $r = n$*
1	—	2
$2, \ldots, n-3$	$i_1 - 1$	$i_1 + 1$
$n-2$	$n-3$	n
$n-1$	$n-2$	$n-2$
n	$n-2$	—

Proof: Again the case $r = 1$ is easy to check directly using Lemma 2.8. Note that the case $i_1 = 1$ cannot occur since the length of the word is stipulated to be at least 2. The case $r = n$ follows from Proposition 2.11 and Lemma 2.10. □

These two results give us the following useful result about $\mathcal{B}_r$:

Lemma 2.14 *Suppose that* $r \in \{1, n\}$ *and that* $s_{i_1} s_{i_2} \cdots s_{i_t}$ *is a reduced expression for an element* $w \in W^r$*. Let* $\xi = \phi_r(w)$*, so* ξx_1 *is the corresponding element of* $\mathcal{B}_r$*. Then:*

$$K_{i_1}(F_{i_2} \cdots F_{i_t} x_1) = v F_{i_2} \cdots F_{i_t} x_1.$$

Proof: We use 2.12 and 2.13 in the same way as in the proof of Lemma 2.11 in [8]. □

There is, as in type A (see [8, 2.12]), a converse result, for which the proof is the same as in type A:

Lemma 2.15 *Suppose that* $r \in \{1, n\}$ *and that* $s_{i_1} s_{i_2} \cdots s_{i_t}$ *is a reduced expression for an element* $w \in W^r$*. Let* $\xi = \phi_r(w)$*, so* ξx_1 *is the corresponding element of* $\mathcal{B}_r$*. Suppose also that* $K_i(\xi x_1) = v \xi x_1$*. Then* $F_i F_{i_1} F_{i_2} \cdots F_{i_t} x_1 \neq 0$*. Equivalently,* $s_i s_{i_1} s_{i_2} \cdots s_{i_t} \in W^r$*.* □

We put these two results together to get:

Proposition 2.16 *Suppose* $r \in \{1, n\}$*. If* $F_{i_1} F_{i_2} \cdots F_{i_t} x_1 \neq 0$ *in* V_r*, then*

$$K_i(F_{i_1} F_{i_2} \cdots F_{i_t} x_1) = v F_{i_1} F_{i_2} \cdots F_{i_t} x_1 \text{ if and only if } F_i F_{i_1} F_{i_2} \cdots F_{i_t} x_1 \neq 0. \ \square$$

Corollary 2.17 *Suppose that* $r \in \{1, n\}$ *and* $s_{i_1} s_{i_2} \cdots s_{i_t}$ *is a reduced expression for an element* $w \in W^r$*. Let* $\xi = \phi_r(w) = F_{i_1} F_{i_2} \cdots F_{i_t}$ *and suppose* F_{i_u} *cannot be commuted to the start of the expression. Then* $F_{i_1} F_{i_2} \cdots \widehat{F_{i_u}} \cdots F_{i_t} x_1 = 0$ *in* V_r*.*

Proof: See the proof of Corollary 2.14 in [8]. □

We are finally nearing our goal. We shall use the Kashiwara operators, $\widetilde{F}_i$, for $i \in I$ (see [6, 2.2]). Suppose that $V(\lambda)$ is the irreducible finite-dimensional highest weight module for U with highest weight λ. Fix $i \in I$. Any element $x \in V(\lambda)$ can be written uniquely $x = \sum_{0 \le l \le l'} F_i^{(l)} x_{l,l'}$, where the $x_{l,l'}$ satisfy $E_i x_{l,l'} = 0$ and $K_i x_{l,l'} = v^{l'} x_{l,l'}$. We then define $\widetilde{F}_i(x) = \sum_{0 \le l \le l'} F_i^{(l+1)} x_{l,l'}$.

If $b \in \mathcal{B}_r$, then by the definition of $\mathcal{B}_r$ (see Proposition 2.6), b satisfies condition (1) of [8, 2.15] (which is the corrected version of the first part of [7, 19.3.5]). So, by [8, 2.15], if $b \in \mathcal{B}_r$ and $b = \widetilde{F}_{j_1} \widetilde{F}_{j_2} \cdots \widetilde{F}_{j_k} x_1$ for some $j_1, j_2, \ldots, j_k$ in I, then in fact b lies in the canonical basis. The proof of the following is exactly the same as that for [8, 2.16]:

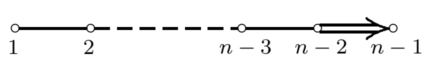
Theorem 2.18 *For $r \in \{1, n\}$, the basis $\mathcal{B}_r$ for V_r is the canonical basis of V_r.* □

Lemmas 2.14 and 2.15, Proposition 2.16, Corollary 2.17 and Theorem 2.18 can all easily be seen to hold for $r = n-1$ by similar arguments. Note that it is now easy to see explicitly what the canonical basis is in each case by using Lemmas 2.8 and 2.11, along with Proposition 2.6 and Theorem 2.18.

3 The Canonical Basis of the Miniscule Module in Type B

Here we use the above results for the quantized spin modules in case D to prove similar results for the fundamental module V_{n-1} (the quantized version of the spin module in the unquantized case) in case B_{n-1} (for $n \ge 4$). This is the only miniscule module in this case. Throughout this section we assume that the Lie algebra is of type B_{n-1} and that W is the corresponding Weyl group. We denote by W' the Weyl group of type D_n. We recall here the Dynkin diagram of type B_{n-1}:

B_{n-1}



Let x_1 be our fixed highest weight vector in V_{n-1}. We have $|W^{n-1}| = 2^{n-1}$, since $|W| = 2^{n-1}(n-1)!$, W_{n-1} is a Weyl group of type B_{n-2} and $|W| = |W_{n-1}||W^{n-1}|$. Note that $\dim_{\mathbb{Q}(v)}(V_{n-1})$ is also 2^{n-1}. We would like to prove a result similar to Lemma 2.2 but the same proof will not work (because of the structure of the root system in this case). Instead we find W^{n-1} explicitly. Firstly we describe an algorithm which generates a subset of W. This subset will eventually be seen to be W^{n-1}. For every sequence of integers $0 < m_1 < m_2 < \cdots < m_k \leq n-1$ (of arbitrary length $k \geq 0$), define $z_{m_1,m_2,\ldots,m_k}$ to be the sequence:

$$n-m_1, n-m_1+1, \ldots, n-1,\ n-m_2, n-m_2+1, \ldots, n-1, \ldots$$

$$\ldots, n-m_k, n-m_k+1, \ldots, n-1,$$

and $w_{m_1,m_2,\ldots,m_k}$ to be the corresponding element of W obtained by replacing each positive integer d with the corresponding fundamental reflection s_d.

Remark 3.1 The sequences produced by this algorithm are precisely those sequences obtained by replacing every occurrence of n with $n-1$ in the sequences produced by the algorithm used in type D, described just before Lemma 2.9.

We need the following two lemmas:

Lemma 3.2 *Suppose that $i_1, i_2, \ldots, i_t$ is a sequence generated by the algorithm, and that $i_k = i_1$ is the second appearance of i_1 in the sequence. Then the following table lists exactly those i_m's in the set $\{i_m : 2 \leq m \leq k-1\}$ satisfying $A_{i_1,i_m} \neq 0$:*

TABLE 5

i_1	*occurrences*
$2, \ldots, n-2$	$i_1 - 1$ *and* $i_1 + 1$
$n-1$	$n-2$

The case $i_1 = 1$ cannot occur.

Proof: This follows straight away from Lemma 2.9 and Remark 3.1. □

Lemma 3.3 *Suppose that $i_1, i_2, \ldots, i_t$ is a sequence of length at least 2 generated by the algorithm, and that i_1 occurs in the sequence in the first place only. Then, in the set $\{i_m : 2 \leq m \leq t\}$, there is precisely one i_m such that $A_{i_1,i_m} \neq 0$, and this is $i_1 + 1$. (Note that the case $i_1 = n - 1$ cannot occur here.)*

Proof: This follows straight away from Lemma 2.10 and Remark 3.1. □

We can now prove the desired result:

Proposition 3.4 *The elements $w_{m_1,m_2,\ldots,m_k}$ produced in the above algorithm exactly constitute the elements of W^{n-1}.*

Proof: By Remark 3.1, it is clear that the algorithm generates 2^{n-1} elements, which is the number of elements in W^{n-1}. Suppose now that $z_{m_1,m_2,\ldots,m_k}$ is a sequence generated by the algorithm, and that $w_{m_1,m_2,\ldots,m_k}$ is the corresponding element of the Weyl group, with expression determined by $z_{m_1,m_2,\ldots,m_k}$. Then, if $i \neq n-1$, by Lemma 3.2, between every two occurrences of the same fundamental reflection s_i in this expression there are exactly two fundamental reflections which do not commute with s_i. It is clear that this will still be true even after commutations are applied to the expression. We conclude that no subexpression of the form $s_p s_q s_p$ with $A_{pq}A_{qp} = 1$ or of the form $s_p s_p$ can occur, even after commutations are applied. Also, by Lemma 3.2, between every two occurrences of s_{n-2} in the expression there must be an s_{n-3}. Thus there can be no subexpression of the form $s_{n-2}s_{n-1}s_{n-2}s_{n-1}$ or $s_{n-1}s_{n-2}s_{n-1}s_{n-2}$. This will be true even after commutations so we conclude that no subexpression of the form $s_p s_q s_p s_q$ with $A_{pq}A_{qp} = 2$ can occur, even after commutations are applied, since in this situation we must have $\{p, q\} = \{n-2, n-1\}$. Therefore the expression for $w_{m_1,m_2,\ldots,m_k}$ produced by the algorithm must be reduced. Furthermore, by Lemma 3.3, if s_i occurs in the expression (for some $i \neq n-1$), and no s_i occurs further on in the expression, then s_i cannot be commuted to the end of the expression. It follows from Lemma 2.1, since commutations are the only defining relations of W that can be applied to the expression, that every reduced expression for $w_{m_1,m_2,\ldots,m_k}$ must end with the fundamental reflection s_{n-1} (unless $w_{m_1,m_2,\ldots,m_k} = 1$), whence $w_{m_1,m_2,\ldots,m_k} \in W^{n-1}$. Thus all the elements generated by the algorithm lie in W^{n-1}. The argument used in Proposition 2.11 can be used to show that all of the elements generated by the algorithm are distinct, except that instead of counting occurrences of $n-1$ and n together we just count occurrences of $n-1$. The proposition follows. □

Corollary 3.5 *Suppose $s_{i_1}s_{i_2}\cdots s_{i_t}s_r$ is a reduced expression for an element $w \in W^{n-1}$ of length at least 3. Then, in the list $i_1, i_2, \ldots, i_r$, there is no sequence p, q, p with $A_{pq}A_{qp} = 1$, nor any sequence p, q, p, q with $A_{pq}A_{qp} = 2$. So no braid relation of the form $s_ps_qs_p = s_qs_ps_q$ or of the form $s_ps_qs_ps_q = s_qs_ps_qs_p$ can be applied directly to this expression.*

Proof: This follows from Proposition 3.4 and its proof. □

Next we have:

Lemma 3.6 *Suppose that $\xi = F_{i_1}F_{i_2}\cdots F_{i_t} \in U^-$ is such that in the sequence $i_1, i_2, \ldots, i_t$, there is a subsequence of one of the following forms:*
(a) a subsequence p, p,
(b) a subsequence p, q, p with $A_{pq}A_{qp} = 1$,
(c) a subsequence p, q, p, q with $A_{pq}A_{qp} = 2$.
Then $\xi x_1 = 0$ in V_{n-1}.

Proof: Let $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{n-1}$ be the coordinate functions on the Cartan subalgebra $\mathbf{h}$ of the Lie algebra consisting of the diagonal matrices contained in it as in [9, §2.14]. (Note that here the rank is $n-1$). These form a basis for $\mathbf{h}^*$. The following information can be found in [9, §§2.14 & 3.6]. The fundamental weights are $\lambda_i = \varepsilon_1 + \varepsilon_2 + \cdots + \varepsilon_i$ for $1 \leq i \leq n-2$ and $\lambda_{n-1} = \frac{1}{2}(\varepsilon_1 + \varepsilon_2 + \cdots + \varepsilon_{n-1})$. The fundamental roots are given by $\alpha_i = \varepsilon_i - \varepsilon_{i+1}$, for $i \in [1, n-2]$, and $\alpha_{n-1} = \varepsilon_{n-1}$. The weights of V_{n-1} are precisely the elements of the weight lattice of the form $\pm\frac{1}{2}\varepsilon_1 \pm \frac{1}{2}\varepsilon_2 \pm \ldots \pm \frac{1}{2}\varepsilon_{n-1}$ (see [9, §3.9]). As in Lemma 2.2 we can assume the given subsequence is at the start of the sequence. Suppose the subsequence is of length u. Then, as $F_{i_{u+1}}F_{i_{u+2}}\cdots F_{i_t}x_1 \neq 0$, $F_{i_{u+1}}F_{i_{u+2}}\cdots F_{i_t}x_1$ has a weight which is a weight of V_{n-1} and thus of the form $\pm\frac{1}{2}\varepsilon_1 \pm \frac{1}{2}\varepsilon_2 \pm \ldots \pm \frac{1}{2}\varepsilon_{n-1}$. But the weight of $F_{i_1}F_{i_2}\cdots F_{i_u}$ (i. e. the sum $\alpha_{i_1} + \alpha_{i_2} + \cdots + \alpha_{i_u}$) for each type of subsequence is as follows:

(a) $-2\varepsilon_p + 2\varepsilon_{p+1}$ if $p \neq n-1$, $-2\varepsilon_{n-1}$ if $p = n-1$,

(b) $-2\varepsilon_p + \varepsilon_{p+1} + \varepsilon_{p+2}$ if $q = p+1$, $-\varepsilon_{p-1} - \varepsilon_p + 2\varepsilon_{p+1}$ if $q = p-1$, (these are the only possibilities for (b)),

(c) $-2\varepsilon_{n-1}$, since we must have $\{p,q\} = \{n-2, n-1\}$.

It is clear that in each case, the weight of $F_{i_1}F_{i_2}\cdots F_{i_t}x_1$, which is the weight of $F_{i_1}F_{i_2}\cdots F_{i_u}$ plus the weight of $F_{i_{u+1}}F_{i_{u+2}}\cdots F_{i_t}x_1$, is not a weight of V_{n-1}, whence $F_{i_1}F_{i_2}\cdots F_{i_t}x_1 = 0$ in V_{n-1} and we are done. □

From Lemma 3.6 it is clear that any monomial $\xi = F_{i_1}F_{i_2}\cdots F_{i_t} \in U^-$ satisfying $\xi x_1 \neq 0$ in V_{n-1} must satisfy the following conditions:

(a) We have $F_{i_t} = F_r$. Also, after any commuting of F_i's, the expression for ξ must still end in F_r. This is clear from the action of U^- on x_1.

(b) There is no way of commuting F_i's to get a subsequence of the form p, p in the list $i_1, i_2, \ldots, i_t$.

(c) There is no way of commuting F_i's to get a subsequence of the form p, q, p with $A_{pq}A_{qp} = 1$ in the list $i_1, i_2, \ldots, i_t$.

(d) There is no way of commuting F_i's to get a subsequence of the form p, q, p, q with $A_{pq}A_{qp} = 2$ in the list $i_1, i_2, \ldots, i_t$.

We can now define a map ϕ_{n-1} exactly as in case D (see just before Lemma 2.5) and the following results all follow (as in case A — see Lemma 2.6, Proposition 2.7 and Theorem 2.8 in [8]).

Lemma 3.7 *Suppose that $\xi = F_{i_1}F_{i_2}\cdots F_{i_t}$ is a monomial in the F_i's in U^-, satisfying $\xi x_1 \neq 0$. Then $\xi \in \mathrm{Im}(\phi_{n-1})$.* □

Proposition 3.8 *The function ϕ_{n-1} defined above defines a bijection ψ_{n-1} from W^{n-1} onto a basis $\mathcal{B}_{n-1}$ for V_{n-1}, given by the formula:*
If $w = s_{i_1}s_{i_2}\cdots s_{i_t} \in W^{n-1}$ is a reduced expression, put

$$\psi_{n-1}(w) = \phi_{n-1}(w)x_1 = F_{i_1}F_{i_2}\cdots F_{i_t}x_1. \ \Box$$

Theorem 3.9 *The basis $\mathcal{B}_{n-1}$ for V_{n-1} is in fact, up to sign, the canonical basis for V_{n-1}. So, up to sign, the canonical basis for V_{n-1} is:*

$$\{F_{i_1}F_{i_2}\cdots F_{i_t}x_1 : s_{i_1}s_{i_2}\cdots s_{i_t} \text{ is a reduced expression for an element in } W^{n-1}\},$$

where $F_{i_1}F_{i_2}\cdots F_{i_t}x_1 = F_{j_1}F_{j_2}\cdots F_{j_t}x_1$ if and only if $s_{i_1}s_{i_2}\cdots s_{i_t} = s_{j_1}s_{j_2}\cdots s_{j_t}$. □

Example

Remark 3.1 implies that W^{n-1} can be obtained from $(W')^n$ by taking each expression in turn, replacing each s_n with s_{n-1}, and interpreting the resulting expression as an element of W. Similarly, by Proposition 3.8, Proposition 2.6 and Theorem 2.18, $\mathcal{B}_{n-1}$ (and thus, it will be seen, the canonical basis for V_{n-1}) can be obtained from the canonical basis for the n-th fundamental module in type D by taking each expression in turn as a monomial times x_1, replacing each F_n with F_{n-1}, and interpreting the expression as a monomial times x_1 in V_{n-1}. Note that there will be no duplication during this process, since we have $|(W')^n| = |W^{n-1}| = 2^{n-1}$. Using this, and the second example given after Lemma 2.7, we obtain that, in case B_4, $\mathcal{B}_4$ is given by the following elements:

$$x_1,$$

$$F_4x_1,$$

$$F_3F_4x_1,$$

$$F_2F_3F_4x_1,\ F_4F_3F_4x_1,$$

$$F_1F_2F_3F_4x_1,\ F_4F_2F_3F_4x_1,$$

$$F_4F_1F_2F_3F_4x_1,\ F_3F_4F_2F_3F_4x_1,$$

$$F_3F_4F_1F_2F_3F_4x_1,\ F_4F_3F_4F_2F_3F_4x_1,$$

$$F_2F_3F_4F_1F_2F_3F_4x_1,\ F_4F_3F_4F_1F_2F_3F_4x_1,$$

$$F_4F_2F_3F_4F_1F_2F_3F_4x_1,$$

$$F_3F_4F_2F_3F_4F_1F_2F_3F_4x_1,$$

$$F_4F_3F_4F_2F_3F_4F_1F_2F_3F_4x_1.$$

Lemma 3.10 *Suppose that* $s_{i_1}s_{i_2}\cdots s_{i_t}$ *is a reduced expression for an element* $w \in W^{n-1}$*, and that* $s_{i_k} = s_{i_1}$ *is the second appearance of* s_{i_1} *in the expression. Then the following table gives those* s_{i_m}*'s in the set* $\{s_{i_m} : 2 \leq m \leq k-1\}$ *which do not commute with* s_{i_1}*.*

TABLE 6

i_1	*occurrences*
$2, \ldots, n-2$	$i_1 - 1$ *and* $i_1 + 1$
$n-1$	$n-2$

The case $i_1 = 1$ *cannot occur.*

Proof: This follows from Proposition 3.4 and Lemma 3.2. □

Lemma 3.11 *Suppose that* $s_{i_1}s_{i_2}\cdots s_{i_t}$ *is a reduced expression for an element* $w \in W^{n-1}$ *of length at least 2, and that* s_{i_1} *occurs in the expression in the first factor only. Then, in the set* $\{s_{i_m} : 2 \leq m \leq t\}$*, there is precisely one fundamental reflection which does not commute with* s_{i_1}*, which is* s_{i_1+1}*. (Note that the case* $i_1 = n-1$ *cannot occur here.)*

Proof: This follows from Proposition 3.4 and Lemma 3.3. □

Lemma 3.12 *Suppose that* $s_{i_1}s_{i_2}\cdots s_{i_t}$ *is a reduced expression for an element* $w \in W^{n-1}$*, and* $\xi = \phi_{n-1}(w)$*, so* ξx_1 *is the corresponding element of* $\mathcal{B}_{n-1}$*. Then:*

$$K_{i_1}(F_{i_2}\cdots F_{i_t}x_1) = vF_{i_2}\cdots F_{i_t}x_1.$$

Proof: We use Lemmas 3.10 and 3.11 in the same way as in the proof of Lemma 2.11 in [8]. □

Lemma 3.13 *Suppose that* $s_{i_1}s_{i_2}\cdots s_{i_t}$ *is a reduced expression for an element* $w \in W^{n-1}$*, and* $\xi = \phi_{n-1}(w)$*, so* ξx_1 *is the corresponding element of* $\mathcal{B}_{n-1}$*. Suppose that* $K_i(\xi x_1) = v\xi x_1$*. Then* $F_iF_{i_1}F_{i_2}\cdots F_{i_t}x_1 \neq 0$*. Equivalently,* $s_is_{i_1}s_{i_2}\cdots s_{i_t} \in W^{n-1}$*.*

Proof: We use Lemma 3.7 and argue as in Lemma 2.12 in [8]. □

We put these two results together to get:

Proposition 3.14 *If* $F_{i_1}F_{i_2}\cdots F_{i_t}x_1 \neq 0$ *in* V_{n-1}*, then*

$$K_i(F_{i_1}F_{i_2}\cdots F_{i_t}x_1) = vF_{i_1}F_{i_2}\cdots F_{i_t}x_1 \text{ if and only if } F_iF_{i_1}F_{i_2}\cdots F_{i_t}x_1 \neq 0. \ \square$$

Corollary 3.15 *Suppose that* $s_{i_1}s_{i_2}\cdots s_{i_t}$ *is a reduced expression for an element* $w \in W^{n-1}$*. Let* $\xi = \phi_{n-1}(w) = F_{i_1}F_{i_2}\cdots F_{i_t}$ *and suppose that* F_{i_u} *cannot be commuted to the start of the expression. Then* $F_{i_1}F_{i_2}\cdots \widehat{F_{i_u}}\cdots F_{i_t}x_1 = 0$ *in* V_{n-1}*.*

Proof: See the proof of Corollary 2.14 in [8]. □

Using the Kashiwara operators as in the proof of Theorem 2.16 in [8], we finally obtain:

Theorem 3.16 *The basis* $\mathcal{B}_{n-1}$ *for* V_{n-1} *is the canonical basis for* V_{n-1}*.* □

Note that it is now easy to see explicitly what the canonical basis for V_{n-1} is by using Lemma 3.4, along with Proposition 3.8 and Theorem 3.16.

ACKNOWLEDGMENTS

This paper was written while the author was supported by a grant from the Engineering and Physical Science Research Council, and supervised by Professor R. W. Carter at the University of Warwick.

REFERENCES

[1] N. Bourbaki. *Groupes et algèbres de Lie, Chapitres 7 et 8.* Hermann, Paris, 1975.

[2] C. W. Curtis and I. Reiner. *Methods of Representation Theory with Applications to Finite Groups and Orders*, volume II. Wiley, New York, 1987.

[3] V. G. Drinfel'd. Hopf algebras and the Yang–Baxter equation. *Soviet Math. Dokl.*, 32:254–258, 1985.

[4] J. E. Humphreys. *Reflection Groups and Coxeter Groups*. C.U.P., Cambridge, 1992.

[5] M. Jimbo. A q-difference analogue of $U(\mathbf{g})$ and the Yang–Baxter equation. *Lett. Math. Phys.*, 10:63–69, 1985.

[6] M. Kashiwara. On crystal bases of the q-analogue of universal enveloping algebras. *Duke Math. J.*, 63(2):465–516, 1991.

[7] G. Lusztig. *Introduction to Quantum Groups*. Birkhäuser, Boston, 1993.

[8] R. J. Marsh. Canonical bases for fundamental modules of quantized enveloping algebras of type A. *Comm. Algebra*, 25(5):1365–1386, 1997.

[9] H. Samelson. *Notes on Lie Algebras*. Springer–Verlag, New York, 1990.