Constructing canonical bases of quantized enveloping algebras

Willem A. de Graaf
Mathematical Institute,
University of Utrecht,
Utrecht,
The Netherlands

Abstract

An algorithm for computing the elements of a given weight of the canonical basis of $U_q(\mathfrak{g})$ is described.

Define $U_q(\mathfrak{g})$, U^-, weight of an element, Weyl group, $s_i = s_{\alpha_i}$, $[m]!_\alpha$, Φ, Δ.

1 The canonical basis

We work in the subalgebra U^- of $U_q(\mathfrak{g})$. Let $w_0 = s_{i_1} \cdots s_{i_t}$ be a reduced expression of the longest element in the Weyl group. For $1 \leq k \leq t$ let $T_{i_k} = T_{\alpha_{i_k}} : U_q(\mathfrak{g}) \to U_q(\mathfrak{g})$ be the automorphism defined in [3], 8.13. Set $F_k = T_{i_1} \cdots T_{i_{k-1}}(F_{\alpha_{i_k}})$. Then F_k is an element of weight $\beta_k = s_{i_1} \cdots s_{i_{k-1}}(\alpha_{i_k})$. We also denote F_k by F_{β_k}. As usual we set $F_k^{(m)} = F_k^m/[k]!_{\alpha_{i_k}}$. Then the monomials

$$F_1^{(n_1)} \cdots F_t^{(n_t)} \qquad (1)$$

form a basis of U^-. This basis is called a PBW-type basis, and we call a monomial of the form (1) a PBW-monomial (relative to the chosen reduced expression of the longest element of the Weyl group). We have algorithms for writing the product of any two PBW-monomials as a linear combination of PBW-monomials ([2]).

Let x be a monomial of the form (1). Then to stress the dependency of x on the choice of reduced expression for the longest element of the Weyl group, we say that x is a w_0-monomial. We refer to the exponents $n_1, \dots, n_t$ as the first, second, ..., t-th exponent of x.

Let $\alpha \in \Delta$. The Kashiwara operators $\widetilde{F}_\alpha, \widetilde{E}_\alpha : U^- \to U^-$ are defined as follows. Let $w_0 = s_{i_1} \cdots s_{i_t}$ be a reduced expression of the longest element of the Weyl group, such that $\alpha_{i_1} = \alpha$. Let u be a w_0-monomial with exponents $n_1, \dots, n_t$. Then $\widetilde{F}_\alpha(u) = F_1^{(n_1+1)} \cdots F_t^{(n_t)}$, and $\widetilde{E}_\alpha(u) = F_1^{(n_1-1)} \cdots F_t^{(n_t)}$, if $n_1 > 0$, and $\widetilde{E}_\alpha(u) = 0$ otherwise. (Note that $F_1 = F_\alpha$.) The action of $\widetilde{F}_\alpha$, $\widetilde{E}_\alpha$ is extended to the whole of U^- by linearity. It can be shown that this definition does not depend on the choice of reduced expression of the longest element in the Weyl group (cf. [3], 10.1).

Let A be the ring consisting of all elements of $\mathbb{Q}(q)$ without pole at 0. Let $\mathcal{L}(\infty)$ be the A-lattice generated by the elements $\widetilde{F}_{\alpha_{k_1}} \cdots \widetilde{F}_{\alpha_{k_m}}(1)$, for $m \geq 0$. We consider the vector space $\mathcal{L}(\infty)/q\mathcal{L}(\infty)$, and we let $\mathcal{B}(\infty) \subset \mathcal{L}(\infty)/q\mathcal{L}(\infty)$ be the set of all nonzero cosets $\widetilde{F}_{\alpha_{k_1}} \cdots \widetilde{F}_{\alpha_{k_m}}(1) + q\mathcal{L}$. Then $\widetilde{F}_\alpha$ maps $\mathcal{B}(\infty)$ into itself and $\widetilde{E}_\alpha$ maps $\mathcal{B}(\infty)$ into $\mathcal{B}(\infty) \cup \{0\}$. Furthermore, $\widetilde{E}_\alpha \widetilde{F}_\alpha(b) = b$ for all $b \in \mathcal{B}(\infty)$. Also, if $\widetilde{E}(b) \neq 0$, then $\widetilde{F}_\alpha \widetilde{E}_\alpha(b) = b$ ([3], Proposition 10.12).

Now we let $^-$ be the unique automorpism of U^- (viewed as $\mathbb{Q}$-algebra) satisfying $\overline{q} = q^{-1}$ and $\overline{F}_{\alpha_i} = F_{\alpha_i}$. Elements that are invariant under $^-$ are said to be bar-invariant. The bar-invariant elements include all monomials $F_{\alpha_{i_1}}^{(n_1)} \cdots F_{\alpha_{i_r}}^{(n_r)}$.

Let $\pi : \mathcal{L}(\infty) \to \mathcal{L}(\infty)/q\mathcal{L}(\infty)$ denote the projection map. Then for each $b \in \mathcal{B}(\infty)$ there is a unique $G(b) \in \mathcal{L}(\infty)$ such that $\pi(G(b)) = b$, and $G(b)$ is bar-invariant (cf. [3], Theorem 11.10). The set of all $G(b)$ for $b \in \mathcal{B}(\infty)$ is denoted by $\mathbf{B}$. It forms a basis of U^-, called the canonical basis.

Now by results of Lusztig (e.g., [8] Theorem 42.1.10, [9], Proposition 8.2) we have that $\mathcal{L}(\infty)$ is spanned by all PBW-monomials (relative to any fixed reduced expression of the longest element in the Weyl group). Furthermore, $\mathcal{B}(\infty)$ consists of the cosets of the PBW-monomials. If $b \in \mathcal{B}(\infty)$ is the coset of the PBW-monomial x, then $G(b) = x + \sum_i \zeta_i x_i$, where the x_i are PBW-monomials, and $\zeta_i \in q\mathbb{Z}[q]$. We call x the *principal monomial* of $G(b)$.

Fix a simple root α and consider the action of $\widetilde{F}_\alpha$ on $\mathcal{B}(\infty)$. We have that $\mathcal{B}(\infty)$ consists of the cosets of all PBW-monomials relative to a fixed reduced expression w_0 of the longest element of the Weyl group. Therefore, if x is a w_0-monomial, $\widetilde{F}_\alpha(x) = x' \bmod q\mathcal{L}(\infty)$, where x' is a certain w_0-monomial. We consider the problem of obtaining x' from x.

First we note that if w_0 happens to start with s_α, then x' is constructed from x by increasing the first exponent of x by 1. Now suppose that w_0 does not start with s_α. Let $\widetilde{w}_0$ be a different reduced expression for the longest element of the Weyl group. Then there is a $\widetilde{w}_0$-monomial $\tilde{x}$ such that $x = \tilde{x} \bmod q\mathcal{L}(\infty)$. In analogy with Lusztig's notation (see [8], [7]), we write $\tilde{x} = R_{w_0}^{\tilde{w}_0}(x)$. If we can find $\tilde{x}$ from x, then the problem of calculating $\widetilde{F}_\alpha(x)$ is solved. Indeed, let $\widetilde{w}_0$ be a reduced expression for the longest element of the Weyl group, starting with s_α. We find the $\tilde{x} = R_{w_0}^{\widetilde{w}_0}(x)$, and increase its first exponent by 1. Denote the resulting monomial by $\tilde{x}'$. Finally we construct $x' = R_{\widetilde{w}_0}^{w_0}(\tilde{x}')$. Then $\widetilde{F}_\alpha(x) = x' \bmod q\mathcal{L}(\infty)$.

We may assume that $\widetilde{w}_0$ can be obtained from w_0 by applying one braid relation. Suppose that this relation amounts to replacing $s_\alpha s_\beta \cdots$ by $s_\beta s_\alpha \cdots$, where both words are of length d. Then $d = 2, 3, 4$ or 6. Suppose that the first word occurs in w_0 on positions $p, p{+}1, \ldots, p{+}d{-}1$. Write $x = F_1^{(m_1)} \cdots F_t^{(m_t)}$ and $\tilde{x} = F_1^{(m_1')} \cdots F_t^{(m_t')}$ (where the F_i in $\tilde{x}$ are defined relative to $\widetilde{w}_0$). We obtain the m_i' from the m_i in the following way.

1. If $d = 2$, then $m_p' = m_{p+1}$ and $m_{p+1}' = m_p$.

2. If $d = 3$, then set $\mu = \min(m_p, m_{p+2})$, and $m_p' = m_{p+1} + m_{p+2} - \mu$, $m_{p+1}' = \mu$, $m_{p+2}' = m_p + m_{p+1} - \mu$.

3. If $d = 4$ then suppose that the move consists of replacing $s_\alpha s_\beta s_\alpha s_\beta$ by $s_\beta s_\alpha s_\beta s_\alpha$. Set $a = m_p$, $b = m_{p+1}$, $c = m_{p+2}$, $d = m_{p+3}$.

   (a) If α is short, then set $n_1 = \max(b, \max(b,d) + c - a)$, $n_2 = \max(a,c) + 2b$, $n_3 = \min(c + d, a + \min(b,d))$, $n_4 = \min(a,c)$. Set $\mu = \max(2n_3, n_2 + n_4)$ and $m_p' = n_1$, $m_{p+1}' = \mu - n_2$, $m_{p+2}' = n_2 + n_3 - \mu$, $m_{p+3}' = n_4 - 2n_3 + \mu$.

   (b) If α is long, then set $p_1 = \max(b, \max(b,d) + 2c - 2a)$, $p_2 = \max(a,c) + b$, $p_3 = \min(2c + d, \min(b,d) + 2a)$, $p_4 = \min(a,c)$. Set $\mu = \max(p_3, p_2 + p_4)$, and $m_p' = p_1$, $m_{p+1}' = \mu - p_2$, $m_{p+2}' = p_3 + 2p_2 - 2\mu$, $m_{p+3}' = p_4 - p_3 + \mu$.

4. If $d = 6$, then we consider the root system of type D_4, along with its diagram automorphism ϕ of order 3. Let α_2 be the simple root fixed by

ϕ, and $\alpha_1, \alpha_3, \alpha_4$ the other three. Set $v = s_1 s_3 s_4$. We use the following two reduced expressions for the longest element in the Weyl group: $v_0 = v s_2 v s_2 v s_2$ and $\widetilde{v}_0 = s_2 v s_2 v s_2 v$. Let $\widetilde{U}_q$ be the corresponding quantized enveloping algebra, in which we use the PBW-bases relative to v_0 and $\widetilde{v}_0$.

For simplicity assume that the root system of $U_q(\mathfrak{g})$ is of type G_2. Suppose that the braid relation amounts to replacing $w_0 = s_\alpha s_\beta s_\alpha s_\beta s_\alpha s_\beta$ by $\widetilde{w}_0 = s_\beta s_\alpha s_\beta s_\alpha s_\beta s_\alpha$, where α is long. Corresponding to a w_0-monomial x with exponents $m_1, \dots, m_6$ we construct the v_0-monomial $y = \psi_1(x)$ with exponents $m_1, m_1, m_1, m_2, m_3, m_3, m_3, m_4, m_5, m_5, m_5, m_6$. Furthermore, to a $\widetilde{w}_0$-monomial $\tilde{x}$ with exponents $m_1, \dots, m_6$ corresponds the $\widetilde{v}_0$-monomial $\tilde{y} = \psi_2(\tilde{x})$ with exponents $m_1, m_2, m_2, m_2, m_3, m_4, m_4, m_4, m_5, m_6, m_6, m_6$. Now starting with a w_0-monomial x we construct (using 1., and 2.) the $\widetilde{v}_0$-monomial $\tilde{y} = R_{v_0}^{\tilde{v}_0}(\psi_1(x))$. Then we have $R_{w_0}^{\tilde{w}_0}(x) = \psi_2^{-1}(\tilde{y})$.

Finally, if α happens to be short, then we follow the same steps, in the reverse order.

First of all, 1., and 2. are proved in [8], 3. can be proved using [7], 12.5, and 4. follows in the same way (see also [1]). At the end of Section 3 we sketch a different proof of 2., 3.

2 The path method

We recall some facts on Littelmann's path model. For more details and proofs we refer to [5].

Let P denote the weight lattice, and let X be the vector space over $\mathbb{R}$ spanned by P. Let Π be the set of all piecewise linear paths $\xi : [0,1] \to X$, such that $\xi(0) = 0$. For $\alpha \in \Delta$ Littelmann defined operators $f_\alpha, e_\alpha : \Pi \to \Pi \cup 0$. Let λ be a dominant weight and let ξ_λ be the path joining λ and the origin by a straight line. Let Π_λ be the set of all $f_{\alpha_{i_1}} \cdots f_{\alpha_{i_m}}(\xi_\lambda)$ for $m \geq 0$. Then $\xi(1) \in P$ for all $\xi \in \Pi_\lambda$. Let $\mu \in P$ be a weight, and let $V(\lambda)$ be the highest-weight module over $U_q(\mathfrak{g})$ of highest weight λ. A theorem of Littelmann states that the number of paths in $\xi \in \Pi_\lambda$ such that $\xi(1) = \mu$ is equal to the dimension of the weight space of weight μ in $V(\lambda)$ ([5], Theorem 9.1).

Let $\nu = \sum_{i=1}^{l} k_i\alpha_i$ be a linear combination of simple roots, with non-negative integer coefficients. Set $\lambda = \sum_{i=1}^{l} k_i\lambda_i$ (where the λ_i are the fundamental weights). Then the dimension of the weight space of weight $\lambda - \nu$ in $V(\lambda)$ is equal to the dimension of $U^-_{-\nu}$. In particular, the dimension of $U^-_{-\nu}$ is equal to the number of paths $\xi \in \Pi_\lambda$ such that $\xi(1) = \lambda - \nu$.

Let $w_0 = s_{i_1}\cdots s_{i_t}$ be a fixed reduced expression of the longest element in the Weyl group. Let ν, λ be as in the preceding paragraph, and let $\xi \in \Pi_\lambda$ be such that $\xi(1) = \lambda - \nu$. We define a sequence of integers $\eta_\xi = (n_1, \dots, n_t)$ and a sequence of paths ξ_k in the following way. First we set $\xi_0 = \xi$. Suppose that the elements $\xi_0, \dots, \xi_{k-1}$ and $n_1, \dots, n_{k-1}$ are defined. Then let n_k be maximal such that $e^{n_k}_{\alpha_{i_k}}(\xi_{k-1}) \neq 0$, and set $\xi_k = e^{n_k}_{\alpha_{i_k}}(\xi_{k-1})$. Following [6] we call η_ξ the adapted string corresponding to ξ (relative to the fixed reduced expression of the longest element of the Weyl group). Let S_ν be the set of adapted strings corresponding to all $\xi \in \Pi_\lambda$ such that $\xi(1) = \lambda - \mu$.

Let $\eta = (n_1, \dots, n_t) \in S_\nu$ and set

$$M_\eta = F^{(n_1)}_{\alpha_{i_1}} \cdots F^{(n_t)}_{\alpha_{i_t}},$$

and

$$b_\eta = \widetilde{F}^{n_1}_{\alpha_{i_1}} \cdots \widetilde{F}^{n_t}_{\alpha i_t}(1) + q\mathcal{L}(\infty).$$

Let $<_{\text{lex}}$ be the lexicographical ordering on integer sequences of length t (i.e., $(m_1, \dots, m_t) <_{\text{lex}} (n_1, \dots, n_t)$ if there is a k such that $m_i = n_i$ for $i < k$, and $m_k < n_k$). Then [6] Proposition 10.4 states

$$M_\eta = G(b_\eta) - \sum_{\substack{\eta' >_{\text{lex}} \eta \\ \eta' \in S_\nu}} c_{\eta,\eta'} G(b_{\eta'}), \tag{2}$$

where $c_{\eta,\eta'} \in \mathbb{Z}[q, q^{-1}]$.

In the sequel we write $f^\eta(\xi_\lambda)$ instead of $f^{n_1}_{\alpha_{i_1}} \cdots f^{n_t}_{\alpha_{i_t}}(\xi_\lambda)$, where $\eta = (n_1, \dots, n_t)$.

3 Constructing canonical basis elements

Here we describe an algorithm for computing the elements of the canonical basis of a given weight.

By $<_{\text{lex}}$ we denote the lexicographic ordering on the PBW-monomials of U^- (i.e., $F_1^{(m_1)} \cdots F_t^{(m_t)} <_{\text{lex}} F_1^{(n_1)} \cdots F_t^{(n_t)}$ if and only if $(m_1, \dots, m_t) <_{\text{lex}} (n_1, \dots, n_t)$).

Let x be a PBW-monomial; then by b_x we denote the element of $\mathcal{B}(\infty)$ such that $G(b_x)$ has principal monomial x. Also by $\varepsilon_\alpha(x)$ we denote the maximal integer n such that $\widetilde{E}_\alpha^n(b_x) \neq 0$. Note that if x is a w_0-monomial, where w_0 starts with s_α, then $\varepsilon_\alpha(x)$ is equal to the first exponent of x.

Proposition 1 *Let $w = s_{\alpha_{i_1}} \cdots s_{\alpha_{i_r}}$ be a reduced word in the Weyl group of Φ. Let w_0 be any reduced expression for the longest element in the Weyl group starting with w. Let*

$$x = F_{\alpha_{i_1}}^{(n_1)} T_{\alpha_{i_1}}(F_{\alpha_{i_2}})^{(n_2)} \cdots (T_{\alpha_{i_1}} \cdots T_{\alpha_{i_{r-1}}})(F_{\alpha_{i_r}})^{(n_r)}$$

be a PBW-monomial in U^-. Then $G(b_x)$ is equal to x plus a $q\mathbb{Z}[q]$-linear combination of w_0-monomials y such that $y >_{\rm lex} x$.

In the proof we use two direct sum decomposition of U^- relative to a simple root α:

$$U^- = U^- \cap T_\alpha(U^-) \oplus F_\alpha U^-, \tag{3}$$

$$U^- = U^- \cap T_\alpha^{-1}(U^-) \oplus U^- F_\alpha, \tag{4}$$

(cf. [3], 8.25, [9]). We have the corresponding projection maps $\pi_\alpha^+ : U^- \to U^- \cap T_\alpha(U^-)$ and $\pi_\alpha^- : U^- \to U^- \cap T_\alpha^{-1}(U^-)$ (cf. [9]). These maps can be described as follows. Let $w_0 = s_{\alpha_{i_1}} \cdots s_{\alpha_{i_t}}$ be a reduced expression for the longest element in the Weyl group, where $\alpha_{i_1} = \alpha$. We have that $U^- \cap T_\alpha(U^-)$ is the linear span of all w_0-monomials y, such that the first exponent of y is zero. Now let $u \in U^-$ and write u as a linear combination of w_0-monomials. Then $u = u_1 + u_2$, where u_1 consists of w_0-monomials with first exponent zero, and u_2 is a linear combination of w_0-monomials with first exponent ≥ 1. Hence $\pi_\alpha^+(u) = u_1$.

Set $v = s_{\alpha_{i_2}} \cdots s_{\alpha_{i_t}}$, and let β be a simple root such that $v(\beta) > 0$. We set $\widetilde{w}_0 = v s_\beta$; then $\widetilde{w}_0$ is also a reduced expression for the longest element of the Weyl group. We have $v(\beta) > 0$, but $s_\alpha v(\beta) < 0$, so that $v(\beta) = \alpha$. Hence $T_v(F_\beta) = F_\alpha$ (cf. [3], Proposition 8.20). Furthermore, $U^- \cap T_\alpha^{-1}(U^-)$ is the linear span of all $\widetilde{w}_0$-monomials with t-th exponent zero. This means that we can decompose $u \in U^-$ according to the decomposition (4) by writing $u = u_1 + u_2$, where u_1 is a linear combination of $\widetilde{w}_0$-monomials with t-th exponent zero, and u_2 consists of $\widetilde{w}_0$-monomials with t-th exponent ≥ 1. Then $\pi_\alpha^-(u) = u_1$.

We have that $B_\alpha^+ = \pi_\alpha^+(\mathbf{B} \setminus \mathbf{B} \cap F_\alpha U^-)$ is a basis of $U^- \cap T_\alpha(U^-)$, and $B_\alpha^- = \pi_\alpha^-(\mathbf{B} \setminus \mathbf{B} \cap U^- F_\alpha)$ is a basis of $U^- \cap T_\alpha^{-1}(U^-)$ (cf. [9]). Now [9], Theorem 1.2 states that

$$T_\alpha(B_\alpha^-) = B_\alpha^+. \tag{5}$$

Proof. (Of Proposition 1). We use induction on r. Note that the result is trivial for $r = 1$ as in that case $x = F_{\alpha_{i_1}}^{(n_1)}$ and $G(b_x) = x$. Set $\alpha = \alpha_{i_1}$ and

$$x' = T_{\alpha_{i_1}}(F_{\alpha_{i_2}})^{(n_2)} \cdots (T_{\alpha_{i_1}} \cdots T_{\alpha_{i_{r-1}}})(F_{\alpha_{i_r}})^{(n_r)},$$

$$x'' = F_{\alpha_{i_2}}^{(n_2)} T_{\alpha_{i_2}}(F_{\alpha_{i_3}})^{(n_3)} \cdots (T_{\alpha_{i_2}} \cdots T_{\alpha_{i_{r-1}}})(F_{\alpha_{i_r}})^{(n_r)}.$$

(So that $x' = T_\alpha(x'')$.) We define $\widetilde{w}_0$ as above. Then x'' is a $\widetilde{w}_0$-monomial and by induction $G(b_{x''})$ is equal to x'' plus a $q\mathbb{Z}[q]$-linear combination of $\widetilde{w}_0$-monomials that are lexicographically bigger than x''. By the description of π_α^- we see that the same holds for $\pi_\alpha^-(G(b_{x''}))$. Now, by (5) we have that $T_\alpha(\pi_\alpha^-(G(b_{x''}))) = \pi_\alpha^+(G(b_y))$ for some $G(b_y) \in \mathbf{B} \setminus \mathbf{B} \cap F_\alpha U^-$. But $T_\alpha(\pi_\alpha^-(G(b_{x''})))$ is equal to $T_\alpha(x'') = x'$ plus a $q\mathbb{Z}[q]$-linear combination of w_0-monomials, and therefore $y = x'$. It follows that $\pi_\alpha^+(G(b_{x'}))$ is equal to x' plus a $q\mathbb{Z}[q]$-linear combination of w_0-monomials that are lexicograpically bigger than x'. From the description above of the map π_α^+ we now see that $G(b_{x'})$ is equal to $\pi_\alpha^+(G(b_x'))$ plus a linear combination of w_0-monomials with non-zero first exponent, and these are lexicographically bigger than x'. Now by [3] 11.12(1), we have that $G(b_x) = F_\alpha^{(n_1)} G(b_{x'}) + R$ where R is a linear combination of elements $G(b_z)$, with $\varepsilon_\alpha(z) > n_1$. By [3], 11.3(2), 11.12(3) we have that $G(b_u) \in F_\alpha^{(\varepsilon_\alpha(u))} U^-$ for all PBW-monomials u. In particular, all w_0-monomials occurring in R have first exponent $> n_1$, and therefore they are bigger than x in the lexicographical ordering. □

Proposition (1) yields the following algorithm for constructing elements of the canonical basis. From (2) we get

$$G(b_\eta) = M_\eta + \sum_{\eta' <_{\mathrm{lex}} \eta} c_{\eta,\eta'} G(b_{\eta'}). \tag{6}$$

The M_η, $G(b_\eta)$ are all bar-invariant, and the latter form a basis of $U_{-\nu}^-$, hence the $c_{\eta,\eta'}$ are bar-invariant as well.

Let $\eta \in S_\nu$, and suppose that we have already constructed the elements $G(b_{\eta'})$ for $\eta' >_{\mathrm{lex}} \eta$. In order to construct $G(b_\eta)$ we need to know the coefficients $c_{\eta,\eta'}$ in (6). For $b_1, b_2 \in \mathcal{B}(\infty)$ we write $b_1 <_{\mathrm{lex}} b_2$ if the principal monomial of $G(b_1)$ is smaller with respect to $<_{\text{lex}}$ than the principal monomial of $G(b_2)$. Order the elements occuring in the sum on the right hand side of (6) as $b_{\eta_1} <_{\text{lex}} b_{\eta_2} <_{\text{lex}} \cdots <_{\text{lex}} b_{\eta_r}$. We define a sequence of elements $G_k \in U^-$. First set $G_0 = M_\eta$. Suppose that $G_0, \ldots, G_{k-1}$ are defined. Let ζ_k be the coefficient of the principal monomial of $G(b_{\eta_k})$ in G_{k-1}, and let ζ'_k be the unique bar-invariant element of $\mathbb{Z}[q, q^{-1}]$ such that $\zeta_k + \zeta'_k \in q\mathbb{Z}[q]$. Set $G_k = G_{k-1} + \zeta'_k G(b_{\eta_k})$. By induction on k, and Proposition 1 we have that $c_{\eta,\eta_k} = \zeta'_k$. Hence $G_r = G(b_\eta)$.

Example 2 We consider the root system of type B_2, with simple roots α, β, where α is long. We use the reduced expression $s_\alpha s_\beta s_\alpha s_\beta$ of the longest element in the Weyl group. The generators of the corresponding PBW-type basis of U^- are F_α, $F_{\alpha+\beta}$, $F_{\alpha+2\beta}$, F_β. Let $\nu = 3\alpha + 2\beta$; we compute the elements of the canonical basis of weight ν.

The set S_ν consists of the adapted strings $\eta_1 = (3, 2, 0, 0)$, $\eta_2 = (2, 2, 1, 0)$, $\eta_3 = (2, 1, 1, 1)$, $\eta_4 = (1, 2, 2, 0)$ (in lexicographical order). First of all $M_{\eta_1} = F_\alpha^{(3)} F_\beta^{(2)} = G(b_{\eta_1})$. Now we consider η_2. Using the algorithms to compute products of PBW-monomials in U^- ([2]), we get

$$M_{\eta_2} = F_\alpha^{(2)} F_\beta^{(2)} F_\alpha = F_\alpha^{(2)} F_{\alpha+2\beta} + q F_\alpha^{(2)} F_{\alpha+\beta} F_\beta + (1 + q^4 + q^8) F_\alpha^{(3)} F_\beta^{(2)}.$$

Here the coefficient of $F_\alpha^{(3)} F_\beta^{(2)}$ is not contained in $q\mathbb{Z}[q]$. We repair this situation, and we get that

$$G(b_{\eta_2}) = M_{\eta_2} - G(b_{\eta_1}) = F_\alpha^{(2)} F_{\alpha+2\beta} + q F_\alpha^{(2)} F_{\alpha+\beta} F_\beta + (q^4 + q^8) F_\alpha^{(3)} F_\beta^{(2)}.$$

Thirdly, $M_{\eta_3} = F_\alpha^{(2)} F_{\alpha+\beta} F_\beta + (q^{-3} + q^{-1} + q + q^3 + q^5 + q^7) F_\alpha^{(3)} F_\beta^{(2)}$. Here we get

$$G(b_{\eta_3}) = M_{\eta_3} - (q^{-3} + q^{-1} + q + q^3) G(b_{\eta_1}) = F_\alpha^{(2)} F_{\alpha+\beta} F_\beta + (q^5 + q^7) F_\alpha^{(3)} F_\beta^{(2)}.$$

Finally, $M_{\eta_4} = F_\alpha F_{\alpha+\beta}^{(2)} + (1 + q^4) F_\alpha^{(2)} F_{\alpha+2\beta} + (q + q^5) F_\alpha^{(2)} F_{\alpha+\beta} F_\beta + (q^4 + q^8 + q^{12}) F_\alpha^{(3)} F_\beta^{(2)}$. Here the coefficient of $F_\alpha^{(2)} F_{\alpha+2\beta}$ does not lie in $q\mathbb{Z}[q]$. So we have to subtract the element of the canonical basis with that principal monomial, i.e., $G(b_{\eta_2})$. We get

$$G(b_{\eta_4}) = M_{\eta_4} - G(b_{\eta_2}) = F_\alpha F_{\alpha+\beta}^{(2)} + q^4 F_\alpha^{(2)} F_{\alpha+2\beta} + q^5 F_\alpha^{(2)} F_{\alpha+\beta} F_\beta + q^{12} F_\alpha^{(3)} F_\beta^{(2)}.$$

As a first application of the algorithm for constructing elements of the canonical basis we give an inefficient algorithm for constructing highest-weight modules. Let λ be a dominant weight. Let v_λ be a highest-weight vector of the highest weight module $V(\lambda)$. Then according to [3], Theorem 11.10 (d), the set $\{G(b)\cdot v_\lambda \mid b\in\mathcal{B}(\infty)\}\setminus\{0\}$ is a basis of $V(\lambda)$. Using the path method it is straightforward to decide which $b\in\mathcal{B}(\infty)$ satisfy $G(b)\cdot v_\lambda=0$. Let $b=b_\eta$ for some adapted string η. Then $G(b)\cdot v_\lambda=0$ if and only if $f^\eta\xi_\lambda=0$ (this will be the content of Lemma 4). Furthermore, we only have to check $b\in\mathcal{B}(\infty)$ of weight ν such that the multiplicity of $\lambda-\nu$ in $V(\lambda)$ is non-zero. By a standard algorithm we can calculate the set of all those ν (using the path method for example). Now the nonzero $G(b)\cdot v_\lambda$ form a basis of the highest-weight module, and we use the $G(b)$ such that $G(b)\cdot v_\lambda=0$ to rewrite all other vectors to linear combinations of basis elements. We remark that this algorithm is rather inefficient because the dimension of $U^-_{-\nu}$ grows quickly as the level of ν increases. A more efficient algorithm for constructing highest-weight modules is indicated in [2].

Example 3 We use the same notation as in Example 2. Let $\lambda=\lambda_1$ be the first fundamental weight. Then $V(\lambda)$ has a weight space of weight $-\lambda_1=\lambda-2\alpha-2\beta$. The elements of the canonical basis of weight $2\alpha+2\beta$ are

$$\begin{aligned}
G(b_1) &= F_\alpha^{(2)}F_\beta^{(2)}\\
G(b_2) &= F_\alpha F_{\alpha+\beta}F_\beta+(q^3+q^5)F_\alpha^{(2)}F_\beta^{(2)}\\
G(b_3) &= F_\alpha F_{\alpha+2\beta}+qF_\alpha F_{\alpha+\beta}F_\beta+(q^2+q^6)F_\alpha^{(2)}F_\beta^{(2)}\\
G(b_4) &= F_{\alpha+\beta}^{(2)}+q^2F_\alpha F_{\alpha+2\beta}+q^3F_\alpha F_{\alpha+\beta}F_\beta+q^8F_\alpha^{(2)}F_\beta^{(2)}.
\end{aligned}$$

They correspond to the strings $\eta_1=(2,2,0,0)$, $\eta_2=(1,1,1,1)$, $\eta_3=(1,2,1,0)$ and $\eta_4=(0,2,2,0)$ respectively. Now only $f^{\eta_3}\xi_\lambda\neq 0$. So $G(b_i)\cdot v_\lambda=0$ for $i=1,2,4$. Let x_i denote the principal monomial of $G(b_i)$. We see that $x_i\cdot v_\lambda=0$ for $i=1,2$, and $x_4\cdot v_\lambda=-q^2x_3\cdot v_\lambda$.

We end this section with a sketch of a proof of case 3. of the formulas for the exponents m_i' in Section 1. We have to study the case where the root system is of type B_2. We let α,β be the simple roots, where β is long. First suppose that we use the reduced expression $s_\alpha s_\beta s_\alpha s_\beta$. Then by [6], Corollary 2, the set $C_1^{s,r}$ of adapted strings of weight $s\alpha+r\beta$ consists of all $\eta_{l,m}=(s-m,r-l,m,l)$, such that $0\le m\le s$, $0\le l\le r$ and

$2(r-l)\geq m\geq 2l$. Here we have $\eta_{l,m}>_{\rm lex}\eta_{l',m'}$ if $m<m'$ or $m=m'$ and $l<l'$.

Now

$$F_\alpha^{(s-m)}F_\beta^{(r-l)}F_\alpha^{(m)}F_\beta^{(l)}=\sum_{\substack{i,j\geq 0\\ i+j\leq r-l\\ 2i+j\leq m}} q^{(m-2i-j)(2r-2l-2i-j)+2(r-l-i-j)i}$$
$$\begin{bmatrix} s-2i-j\\ s-m\end{bmatrix}_\alpha \begin{bmatrix} r-i-j\\ l\end{bmatrix}_\beta F_\alpha^{(s-2i-j)}F_{2\alpha+\beta}^{(i)}F_{\alpha+\beta}^{(j)}F_\beta^{(r-i-j)}.$$

By studying the coefficients in this expression, and following the algorithm for computing elements of the canonical bases it can be shown that the principal monomial of $G(b_{\eta_{l,m}})$ is $F_\alpha^{(s-m)}F_{2\alpha+\beta}^{(l)}F_{\alpha+\beta}^{(m-2l)}F_\beta^{(r-m+l)}$ if $m\leq r$, and $F_\alpha^{(s-m)}F_{2\alpha+\beta}^{(m+l-r)}F_{\alpha+\beta}^{(2r-2l-m)}F_\beta^{(l)}$ if $m\geq r$.

Now suppose that we use the reduced expression $s_\beta s_\alpha s_\beta s_\alpha$. In this case the set $C_2^{s,r}$ of adapted strings of weight $s\alpha+r\beta$ consists of all $\zeta_{l,m}=(r-m,s-l,m,l)$ such that $0\leq l\leq s$, $0\leq m\leq r$, $s-l\geq m\geq m$ (cf. [6], Corollary 2). We have that $\zeta_{l,m}<_{\rm lex}\zeta_{l',m'}$ if $m<m'$ or $m=m'$ and $l<l'$. In this case the principal monomial of $G(b_{\zeta_{l,m}})$ is $F_\beta^{(r-m)}F_{\alpha+\beta}^{(2m-s+l)}F_{2\alpha+\beta}^{(s-l+m)}F_\alpha^{(l)}$ if $s\leq 2m$, and $F_\beta^{(r-m)}F_{\alpha+\beta}^{(l)}F_{2\alpha+\beta}^{(m-l)}F_\alpha^{(s+l-2m)}$ if $s\geq 2m$.

Suppose that the braid relation consists of replacing $s_\alpha s_\beta s_\alpha s_\beta$ by $s_\beta s_\alpha s_\beta s_\alpha$. We start with a PBW-monomial $x=F_\alpha^{(a)}F_{2\alpha+\beta}^{(b)}F_{\alpha+\beta}^{(c)}F_\beta^{(d)}$. We form the adapted string η such that $G(b_\eta)$ has principal monomial x. By the description of the principal monomials above we have that $\eta=(a,c+\max(b,d),2b+c,\min(b,d))$. Now we use the bijection $\phi: C_1^{s,r}\to C_2^{s,r}$, such that $f^\theta=f^{\phi(\theta)}$ for all $\theta\in C_1^{s,r}$. According to [6], Proposition 2.4 it is given by $\phi(\eta)=(n_1,n_2,n_3,n_4)$, where $n_1=\max(b,\max(b,d)+c-a)$, $n_2=\max(a,c)+2b$, $n_3=\min(c+d,a+\min(b,d))$, $n_4=\min(a,c)$. Now $\phi(\eta)$ corresponds to the PBW-monomial $F_\beta^{(n_1)}F_{\alpha+\beta}^{(2n_3-n_2)}F_{2\alpha+\beta}^{(n_2-n_3)}F_\alpha^{(n_4)}$ if $n_2+n_4\leq 2n_3$, and to $F_\beta^{(n_1)}F_{\alpha+\beta}^{(n_4)}F_{2\alpha+\beta}^{(n_3-n_4)}F_\alpha^{(n_2+2n_4-2n_3)}$ if $n_2+n_4\geq 2n_3$. This implies the formulas in the case 3(a); the case 3(b) is similar.

Also the formula in case 2. can be proved this way.

4 Canonical bases of modules

Let λ be a dominant weight, and $V(\lambda)$ the corresponding highest-weight module over U_q. For $\alpha\in\Delta$ we have the Kashiwara operators $\widetilde{F}_\alpha,\widetilde{E}_\alpha$:

$V(\lambda) \to V(\lambda)$ defined by [3], 9.2(2), (3). Let v_λ be a fixed highest-weight vector, and let $\mathcal{L}(\lambda)$ be the A-module spanned by all $\widetilde{F}_{\alpha_{i_1}} \cdots \widetilde{F}_{\alpha_{i_r}}(v_\lambda)$, for $r \geq 0$. Furthermore, $\mathcal{B}(\lambda)$ is the set of non-zero cosets $\bmod q\mathcal{L}(\lambda)$ of these elements ([3], §9.5).

Let $U_{\mathbb{Z}}^-$ be the $\mathbb{Z}$-form of U^-. It is spanned over $\mathbb{Z}[q, q^{-1}]$ by all PBW-monomials (2). Let $\varphi_\lambda : U_{\mathbb{Z}}^- \to V(\lambda)$ be the map defined by $\varphi_\lambda(u) = uv_\lambda$, and set $V_{\mathbb{Z}}(\lambda) = \varphi_\lambda(U_{\mathbb{Z}}^-)$. We consider the $\mathbb{Z}[q]$-module $\mathcal{L}_{\mathbb{Z}}(\lambda) = \mathcal{L}(\lambda) \cap V_{\mathbb{Z}}(\lambda)$ (cf., [3], §11.1 - 11.6). In this section we describe an algorithm for obtaining a basis of $\mathcal{L}_{\mathbb{Z}}(\lambda)$, along with a set of coset representatives for the elements of $\mathcal{B}(\lambda)$.

We have that φ_λ induces a map (which we denote by the same symbol) $\varphi_\lambda : \mathcal{L}(\infty)/q\mathcal{L}(\infty) \to \mathcal{L}_{\mathbb{Z}}(\lambda)/q\mathcal{L}_{\mathbb{Z}}(\lambda)$. By [3], Theorem 10.10 we have that $\varphi_\lambda(\mathcal{B}(\infty)) \setminus \{0\} = \mathcal{B}(\lambda)$. Furthermore, [3], Theorem 11.10 states that the set of $\varphi_\lambda(G(b))$, where $b \in \mathcal{B}(\infty)$ is such that $\varphi(b) \neq 0$ is a basis over $\mathbb{Z}[q]$ of $\mathcal{L}_{\mathbb{Z}}(\lambda)$. So we can find a basis of $\mathcal{L}_{\mathbb{Z}}(\lambda)$ by computing elements of the canonical basis of U^-, and taking their image under φ_λ. However, many of these images will be zero. Here we describe a more direct approach for computing $\varphi_\lambda(G(b))$, without computing $G(b)$ first.

Let $\eta = (n_1, \dots, n_t)$ be an adapted string, relative to the reduced expression $w_0 = s_{\alpha_{i_1}} \cdots s_{\alpha_{i_t}}$. Then we write $\widetilde{F}^\eta$ for $\widetilde{F}_{\alpha_{i_1}}^{n_1} \cdots \widetilde{F}_{\alpha_{i_t}}^{n_t}$ (where the $\widetilde{F}_{\alpha_k}$ are the Kashiwara operators on U^- or the Kashiwara operators on $V(\lambda)$).

Lemma 4 *Let η be an adapted string, and set $b = \widetilde{F}^\eta(1) \bmod q\mathcal{L}(\infty)$. Then $\varphi_\lambda(b) = 0$ if and only if $f^\eta(\xi_\lambda) = 0$.*

Proof. By [4], Theorem 4.1 we have that $f^\eta \xi_\lambda = 0$ if and only if $\widetilde{F}^\eta b_\lambda = 0$, where $b_\lambda = \varphi_\lambda(1)$. By [3], Proposition 10.9 this is equivalent to $\varphi_\lambda(\widetilde{F}^\eta(1)) = 0$, which, by [3], Theorem 11.10(d) is equivalent to $G(b_\eta) \cdot v_\lambda = 0$. □

For an adapted string η we denote by x_η the PBW-monomial with the property $\widetilde{F}^\eta(1) = x_\eta \bmod q\mathcal{L}(\infty)$. Note that we can compute x_η by usingthe algorithm for computing the action of $\widetilde{F}_\alpha$, described at the end of Section 1.

Corollary 5 *$\mathcal{B}(\lambda)$ consists of all cosets $x_\eta \cdot v_\lambda \bmod q\mathcal{L}(\infty)$, where η runs over all adapted strings with $f^\eta(\xi_\lambda) \neq 0$.*

Proof. This follows immediately from Lemma 4, along with $\phi_\lambda(\mathcal{B}(\infty)) \setminus \{0\} = \mathcal{B}(\lambda)$. □

We note that this corollary gives an immediate algorithm for constructing a set of coset representatives for the elements of $\mathcal{B}(\lambda)$.

By $^{-}$ we denote the involution of $V(\lambda)$ defined by $\overline{u \cdot v_\lambda} = \overline{u} \cdot v_\lambda$, for $u \in U^-$.

Lemma 6 *Let $b \in \mathcal{B}(\lambda)$. Then there is a unique element $v(b) \in \mathcal{L}_{\mathbb{Z}}(\lambda)$ such that $v(b) = b \bmod q\mathcal{L}(\lambda)$ and $\overline{v(b)} = v(b)$. Let $b' \in \mathcal{B}(\infty)$ be such that $\varphi_\lambda(b') = b$; then $v(b) = \varphi(G(b'))$.*

Proof. It is clear that $\varphi(G(b'))$ has the listed properties. Suppose that the element $v \in \mathcal{L}_{\mathbb{Z}}(\lambda)$ also has these properties. Then we write v as a linear combination of elements $\varphi_\lambda(G(b''))$. Because v is bar-invariant, the coefficients in this expression must be bar-invariant as well. Because the $\varphi_\lambda(G(b''))$ form a basis of $\mathcal{L}_{\mathbb{Z}}(\lambda)$ over $\mathbb{Z}[q]$, the coefficients must lie in $\mathbb{Z}[q]$. This means that the coefficients are elements of $\mathbb{Z}$. Since $v = b \bmod q\mathcal{L}(\lambda)$ we have that the only $\varphi_\lambda(G(b''))$ that has a non-zero coefficient is $\varphi_\lambda(G(b'))$. $\square$

Now the algorithm is straightforward. Let ν be a weight such that $\lambda - \nu$ is a weight of $V(\lambda)$. Let $\xi_1, \ldots, \xi_r$ be the paths in Π_λ such that $\xi_k(1) = \lambda - \nu$. Let $\eta_1, \ldots, \eta_r$ be the corresponding adapted strings (relative to some fixed reduced expression for the longest element in the Weyl group). Suppose that they are ordered so that $\eta_i <_{\text{lex}} \eta_{i+1}$. Set $u_i = x_{\eta_i} \cdot v_\lambda$, and $w_i = M_{\eta_i} \cdot v_\lambda$. Suppose that $v_1 = v(b_{\eta_1}), \ldots, v_k = v(b_{\eta_k})$ are already constructed. Write $v_i <_{\text{lex}} v_j$ if $x_{\eta_i} <_{\text{lex}} x_{\eta_j}$.

Now write $w_{k+1} = \sum_{j=1}^{r} \zeta_{ij} u_j$, where $\zeta_{ij} \in \mathbb{Z}[q, q^{-1}]$. We go through the v_m, starting with the one which is biggest in the $<_{\text{lex}}$ ordering. If the coefficient of a u_m in the expression for w_{k+1} does not lie in $\mathbb{Z}[q]$, then we add a suitable bar-invariant multiple of v_m to remedy this situation. Proposition 1 implies that this algorithm terminates with the correct result.

References

[1] R. W. Carter. Canonical bases, reduced words, and Lusztig's piecewise-linear function. In *Algebraic groups and Lie groups*, pages 61–79. Cambridge Univ. Press, Cambridge, 1997.

[2] W. A. de Graaf. Computing with quantized enveloping algebras: PBW-type bases, highest-weight modules, R-matrices. J. of Symbolic Computation, to appear.

[3] J. C. Jantzen. *Lectures on Quantum Groups*, volume 6 of *Graduate Studies in Mathematics*. American Mathematical Society, 1996.

[4] M. Kashiwara. Similarity of crystal bases. In *Lie algebras and their representations (Seoul, 1995)*, pages 177–186. Amer. Math. Soc., Providence, RI, 1996.

[5] P. Littelmann. Paths and root operators in representation theory. *Ann. of Math. (2)*, 142(3):499–525, 1995.

[6] P. Littelmann. Cones, crystals, and patterns. *Transform. Groups*, 3(2):145–179, 1998.

[7] G. Lusztig. Introduction to quantized enveloping algebras. In *New developments in Lie theory and their applications (Córdoba, 1989)*, pages 49–65. Birkhäuser Boston, Boston, MA, 1992.

[8] G. Lusztig. *Introduction to quantum groups*. Birkhäuser Boston Inc., Boston, MA, 1993.

[9] G. Lusztig. Braid group action and canonical bases. *Adv. Math.*, 122(2):237–261, 1996.