Invent. math. 133, 399–416 (1998)

Inventiones mathematicae

Quantum groups and quantum shuffles

Marc Rosso

I.R.M.A., Université Louis Pasteur et Institut Universitaire de France,
7, rue René Descartes, F-67084 Strasbourg Cedex, France

Oblatum 21-III-1997 & 12-IX-1997

Abstract. Let U_q^+ be the "upper triangular part" of the quantized enveloping algebra associated with a symetrizable Cartan matrix. We show that U_q^+ is isomorphic (as a Hopf algebra) to the subalgebra generated by elements of degree 0 and 1 of the cotensor Hopf algebra associated with a suitable Hopf bimodule on the group algebra of $\mathbf{Z}^n$. This method gives supersymetric as well as multiparametric versions of U_q^+ in a uniform way (for a suitable choice of the Hopf bimodule). We give a classification result about the Hopf algebras which can be obtained in this way, under a reasonable growth condition. We also show how the general formalism allows to reconstruct higher rank quantized enveloping algebras from $U_q sl(2)$ and a suitable irreducible finite dimensional representation.

Introduction

The quantized enveloping algebras $U_q\mathscr{G}$ associated with a symetrizable Kac-Moody algebra $\mathscr{G}$ are defined by generators and relations in terms of the Cartan matrix. It seems desirable to have a more intrinsic, or functorial understanding of them. (After all, we don't want, in order to define a simple complex Lie algebra, to have first to write down the list of all positive definite Cartan matrices...). By functorial, we mean something like the quantum double construction which allows to construct $U_q\mathscr{G}$ from its Hopf subalgebra U_q^+.

We shall restrict attention to U_q^+ (the remark we have just made allows to do that). There are already nice approaches to it, in terms of Hall algebras (Ringel [Ri]), or perverse sheaves (Lusztig [L2]). We want to have here a very pedestrian point of view. We shall show that U_q^+ can be seen as a sort of "quantum symetric algebra" (rather than a "quantum universal algebra").

The general formalism is as follows: starting with the data of a Hopf algebra H and a Hopf bimodule M over it, one constructs the "quantum shuffle Hopf algebra" as the cotensor Hopf algebra of M over H. It is naturally $\mathbf{N}$-graded, but is not generated by M and H. The sub-Hopf algebra generated by them is a natural generalization of the symetric algebra, and, for very specific examples (H being the group algebra of $\mathbf{Z}^n$), one gets exactly U_q^+.

It is very remarkable that these cotensor constructions were already done by W. Nichols ([N]) more than 20 years ago! What was missing at that time was interest in braids, and to realize that for each n, the braid group on n strands naturally acts on the homogenous component of degree n of the cotensor Hopf algebra.

As far as examples are concerned, we shall concentrate first on the case where H is the group algebra of an abelian group, and on Hopf bimodules reproducing the coproduct for the comodule structure. This leads to (multiparametric generalizations of) U_q^+. One interest of our approach of seeing U_q^+ as a subspace rather than a quotient is that it allows for very easy computations (the tensor coalgebra being a free left H-module with basis a tensor space over a linear space, it is easy to see when a element is zero or not). Extending classical results of Radford ([Ra]), we shall get information on bases for the quantum shuffle algebra and we shall provide a classification result on the "generalized U_q^+" under some growth conditions and genericity of the parameters.

Consider now the case where H is U_q^+. Natural examples of Hopf bimodules come from representations of $U_q\mathscr{G}$ (because $U_q\mathscr{G}$ is a quotient of the double of U_q^+). Choosing suitable irreducible $U_q\mathscr{G}$ modules, we shall construct, "by induction on the rank", the quantized enveloping algebras from the one associated with $sl(2)$. This is close in spirit to the construction of Kac-Moody Lie algebras from their local parts.

Let us explain roughly how this works on an example, refereeing to section 4 for details. Let V be an irreducible $U_q\mathscr{G}$ module. Then $U_q^+ \otimes V$ has a natural structure of a Hopf bimodule over U_q^+, and we can look at the "quantum symetric algebra" built on it. Assume to fix ideas that $\mathscr{G}$ is $sl(n)$ and that V is its natural n-dimensional representation. Then the "quantum symetric algebra" is nearly the "upper triangular part" of $U_q sl(n+1)$. The correct picture is obtained by extending U_q^+ by a grouplike element which acts diagonally on V. One observes in this case that elements of V belonging to a basis of weight vectors appear as analogues of root vectors of a Poincare-Birkhoff-Witt type basis.

The results of sections 1, 2, 3 were announced in [Ro 2] and explained at several conferences (Cours Peccot du Collège de France 1993, International Congress of Mathematical Physics Paris 1994, ...); the results of section 4 were announced in a course given at Les Houches Summer School in August 1995.

Notations

In all this paper, we denote by k a commutative field.

If H is a k-Hopf algebra, we denote by Δ its coproduct and by S its antipode. We shall use Sweedler's notation: for h in H, $\Delta(h) = \sum h_{(1)} \otimes h_{(2)}$. When we consider H with the opposite algebra structure, we denote it by H^{op}.

As we shall be dealing with tensor products between tensor powers of a given space, we shall often write $(x_1, \ldots, x_n)$ instead of $x_1 \otimes \cdots \otimes x_n$.

We denote by Σ_n the symetric group of $\{1, 2, \ldots, n\}$ and, for $i = 1, \ldots, n-1$, by s_i the transposition $(i, i+1)$. The braid group on n strands is denoted by B_n, and for $i = 1, \ldots, n-1$, the i-th generator by σ_i.

For $l_1 + \cdots + l_r = n$, the set of $(l_1, \ldots, l_r)$-shuffles, i.e. the set of permutations w such that $w(1) < w(2) < \cdots < w(l_1)$, $w(l_1+1) < w(l_1+2) < \cdots < w(l_1+l_2), \ldots, w(l_1 + \cdots + l_{r-1}+1) < \cdots < w(n)$, is denoted by $\Sigma_{(l_1,\ldots,l_r)}$.

The length of a permutation w, defined as the length of any reduced expression in terms of the standard generators s_i, is denoted by $l(w)$.

If w is in Σ_n, we denote by T_w the corresponding lift in B_n, defined as follows: if $w = s_{i_1} \ldots s_{i_k}$ is any reduced expression of w, then $T_w = \sigma_{i_1} \ldots \sigma_{i_k}$.

We put $\mathscr{B}_{(l_1,\ldots,l_r)} = \sum_{w \in \Sigma_{(l_1,\ldots,l_r)}} T_w$, and $\widetilde{\mathscr{B}}_{(l_1,\ldots,l_r)} = \Sigma_w - 1 \in \Sigma_{(l_1,\ldots,l_r)} T_w$.

For $q \in k$ different from 1 or -1, or q an indeterminate, and for all $n \in \mathbf{Z}$, we define $[n]_q = \frac{q^n - q^{-n}}{q - q^{-1}}$, and $[n]_q! = [n]_q [n-1]_q \cdots [1]_q$.

$\mathscr{G}$ will denote a finite dimensional complex simple Lie algebra, $\mathscr{H}$ a Cartan subalgebra, $(a_{i,j})_{1 \le i,j \le N}$ its Cartan matrix, $(\alpha_1, \ldots, \alpha_N)$ a set of simple roots, $(\,,\,)$ the inner product on the root lattice (so, we have: $a_{i,j} = 2\frac{(\alpha_i, \alpha_j)}{(\alpha_i, \alpha_i)}$).

1. The quantum shuffle Hopf algebra

We begin by recalling general facts, due to W. Nichols ([N]), about Hopf bimodules and the cotensor algebra. We complete them by clarifying the algebra structure in terms of the natural action of the braid group. This allows to give an abstract formulation in terms of the linearized braid category.

1.1 Hopf bimodules

Definition 1. *Let H be a k-Hopf algebra. A Hopf bimodule over H is a k-vector space M given with a H-bimodule structure, a H-bicomodule structure (i.e. left and right coactions $\delta_L : M \to H \otimes M$, $\delta_R : M \to M \otimes H$ which commute in the following sense: $(\delta_L \otimes id)\delta_R = (id \otimes \delta_R)\delta_L$, and such that δ_L and δ_R are morphisms of H-bimodules.*

This notion has also been considered by S. Woronowicz ([W]), under the name of bicovariant bimodule, in his work on non-commutative differential calculus on quantum groups.
W. Nichols shows that, taking tensor products over H, Hopf bimodules form a tensor category $\mathscr{E}$.
The structure of Hopf bimodules is clarified if one considers the subspaces of left or right coinvariants: $M^L = \{m \in M; \delta_L(m) = 1 \otimes m\}$ and $M^R = \{m \in M; \delta_R(m) = m \otimes 1\}$. In fact, a classical result of Sweedler says that M is isomorphic, as left module and comodule, to the trivial one $H \otimes M^L$, or, as a right module and comodule, to the trivial one $M^R \otimes H$. Furthermore, M^L is a sub-right comodule of M, and inherits a structure of right H-module given by:

$$m \cdot h = \sum S(h_{(1)}) m h_{(2)}$$

with $m \in M$ and $h \in H$. In the same way, M^R is a sub-left comodule of M, and inherits a left H-module action given by:

$$h \cdot m = \sum h_{(1)} m S(h_{(2)})$$

with $m \in M$ and $h \in H$.

Proposition 2. *With these two structures, M^R is a crossed module over H in the sense of Yetter* ([Y]); *and if H and M are finite dimensional, it is a module over the quantum double. Furthermore, a morphism of Hopf bimodules induces on the spaces of right coinvariants a morphism of crossed modules.*

Remark. This result gives a natural way to discover the quantum double (in particular its non trivial algebra structure) if one doesn't know it before.

In order to illustrate this remark, we shall sketch the proof in the finite dimensional context.

Proof. Assume that H and M are finite dimensional. Then M^R is a right module over the dual Hopf algebra H^*, and using the antipode or its inverse, we can make it a left module. So, for m in M^R and l in H^*, we have, writing $\delta_L(m) = \sum m_{(-1)} \otimes m_{(0)}$, $l \cdot m = \sum (S^{-1}(l), m_{(-1)}) m_{(0)}$. Now, we can compute how the actions of H and H^* commute. We have for h in H and l in H^*,

$$\begin{aligned} l \cdot (h \cdot m) = l \cdot \left(\sum h_{(1)} m S(h_{(2)}) \right) &= \sum (S^{-1}(l), h_{(1)} m_{(-1)} S h_{(3)}) h_{(2)} \cdot m_{(0)} \\ &= \sum (S^{-1}(l_{(3)}), h_{(1)}) (S^{-1}(l_{(1)}), S h_{(3)}) h_{(2)} \cdot (l_{(2)} \cdot m) \end{aligned}$$

This is also

$$\sum (S^{-1}(l_{(3)}), h_{(1)}) (l_{(1)}, h_{(3)}) h_{(2)} . (l_{(2)})$$

acting on m, and one recognizes the formula for the product in the quantum double.

1.2 Braidings

Woronowicz ([W]) introduced a remarkable braiding in the category of Hopf bimodules.

Proposition 3. *Let M and N be H-Hopf bimodules. There exists a unique morphism of H-bimodules $\sigma_{M,N} : M \otimes_H N \to N \otimes_H M$ such that, for $\omega \in M^L$ and $\eta \in M^R$ $\sigma_{M,N}(\omega \otimes \eta) = \eta \otimes \omega$. Furthermore, $\sigma_{M,N}$ is an invertible morphism of bicomodules and satisfies the following braid equation* (*where M, N and P are Hopf bimodules*):

$$(I_P \otimes \sigma_{M,N})(\sigma_{M,P} \otimes I_N)(I_M \otimes \sigma_{N,P}) = (\sigma_{N,P} \otimes I_M)(I_N \otimes \sigma_{M,P})(\sigma_{M,N} \otimes I_P) \ .$$

This makes $\mathscr{E}$ a braided tensor category.

One observes that $\sigma_{M,M}$ sends $M^R \otimes M^R$ into itself, and defines a representation T of the braid group B_n in $(M^R)^{\otimes n}$. An easy computation gives: $\sigma(x \otimes y) = \delta_L(x)(y \otimes 1)$, and so this representation is nothing but the one coming from the crossed module structure. More precisely, we have:

Proposition 4. *The functor sending M to M^R is an equivalence of braided tensor categories between $\mathscr{E}$ and the category of crossed modules.*

1.3 The cotensor Hopf algebra

The following construction generalizes the classical shuffle algebra.

Definition 5. (i) *Let M and N be H-Hopf bimodules. Their cotensor coproduct $M \sqcup N$ is the kernel of $\delta_R \otimes I_N - I_M \otimes \delta_L : M \otimes N \to M \otimes H \otimes N$.* (ii) *The cotensor coalgebra constructed on M is $T_H^c(M) = H \oplus \oplus_{n \geq 1} M^{\sqcup n}$.*

In fact, it is easy to see that $M \sqcup N$ is again a Hopf bimodule, and that $T_H^c(M)$ has a graded coalgebra structure given as follows: the component of bidegree (p, q) of the coproduct on $M^{\sqcup n}$ is given by the restriction of the map: $(x_1, \ldots, x_n) \mapsto (x_1, \ldots, x_p) \otimes (x_{p+1}, \ldots, x_n)$, for $p \geq 1$ and $q \geq 1$, and by $\delta_L \otimes id$ for $p = 0$, and $id \otimes \delta_R$ for $q = 0$.

Remark. The dual construction, i.e. the tensor algebra $T_H(M) = H \oplus \oplus_{n \geq 1} M^{\otimes_H n}$ is certainly more familiar. The product is given by concatenation over H; from its universal property, one deduces that $T_H(M)$ has a unique bialgebra structure such that the restriction of the coproduct to H is the one we started with and its restriction to M is the sum $\delta_L + \delta_R$. We shall elaborate a little bit on this to give a concrete description of the coproduct in terms of the braid group action. We begin by a more general result which is of independent interest.

Let A an H-bimodule algebra (i.e. A is an H bimodule, and left and right action of H respect its algebra structure: for all h in H, a and b in A,

$h(ab) = \sum h_{(1)}(a)h_{(2)}(b))$. Let f and g: $M \to A$ two H-bimodule maps. Then, by the universal property of the tensor product over H, the map: $f \cdot g : M \otimes_H M \to A$, sending $m \otimes_H n$ to $f(m)g(n)$ is well defined. More generally, one defines the product of n bimodule maps from M to A as a bimodule map from $M^{\otimes_H n}$ to A.

Proposition 6. *Let A be an H-bimodule algebra and f and $g : M \to A$ two bimodule maps. Assume that $g \cdot f = (f \cdot g) \circ \sigma$. Then the map $(f+g)^n : M^{\otimes_H n} \to A$ is given by*:

$$(f+g)^n = \sum_{k=0}^{n} (f^k \cdot g^{n-k}) \circ \widetilde{\mathscr{B}}_{k,n-k} \ .$$

where $\widetilde{\mathscr{B}}_{k,n-k} = \sum_{w^{-1} \in \Sigma_{k,n-k}} T_w$.

Proof. By induction on n:

$$\begin{aligned}(f+g)^{(n+1)} &= \sum_{k=0}^{n} (f^k \cdot g^{n-k}) \circ \widetilde{\mathscr{B}}_{k,n-k}.(f+g) \\ &= \sum_{k=0}^{n} (f^k \cdot g^{n-k}) \cdot (f+g) \circ (\widetilde{\mathscr{B}}_{k,n-k} \otimes Id) \ .\end{aligned}$$

Now, for all r, $g^r \cdot f = (f \cdot g^r) \circ \sigma_1 \ldots \sigma_r$; then the result follows from the observation that, for $w \in \Sigma_{k+1,n-k}$, either $w(n+1) = n+1$ or $w(k+1) = n+1$, and this implies that $\widetilde{\mathscr{B}}_{k+1,n-k} = \widetilde{\mathscr{B}}_{k+1,n-k-1} \otimes Id \ + Id^{\otimes k} \otimes \ (\sigma_1 \ldots \sigma_{n-k}) \circ (\widetilde{\mathscr{B}}_{k,n-k} \otimes Id)$.
We apply this to the following situation where $A = T_H(M) \otimes T_H(M)$, and the bimodule maps are δ_R and δ_L. This is possible because:

Lemma 7. *We have*: $\delta_L \cdot \delta_R = (\delta_R \cdot \delta_L) \circ \sigma$.

Proof. Denote, for $x \in H$, $\delta_L(x) = \sum x_{(-1)} \otimes x_{(0)}$ and $\delta_R(x) = \sum x_{(0)} \otimes x_{(1)}$. Then, for x and y in H, we have: $\delta_L(x) \cdot \delta_R(y) = \sum x_{(-1)}y_{(0)} \otimes x_{(0)}y_{(1)}$.

On the other hand, $\sigma(x \otimes_H y) = \sum x_{(-2)}y_{(0)}Sy_{(1)} \otimes Sx_{(-1)}x_{(0)}y_{(2)}$, and

$$\begin{aligned}(\delta_R \otimes \delta_L)(\sigma(x \otimes_H y)) &= \sum x_{(-5)}y_{(0)}Sy_{(3)}Sx_{(-2)}x_{(-1)}y_{(4)} \\ &\quad \otimes x_{(-4)}y_{(1)}Sy_{(2)}Sx_{(-3)}x_{(0)}y_{(5)} \\ &= \sum x_{(-1)}y_{(0)} \otimes x_{(0)}y_{(1)} \ .\end{aligned}$$

From Proposition 6 and Lemma 7, we get immediately:

Proposition 8. *The coproduct on $T_H(M)$ is given by*:

$$\text{for } (x_1, \ldots, x_n) \in M^{\otimes_H n}, \Delta(x_1, \ldots, x_n) = \sum_{k=0}^{n} (\delta_R^k \cdot \delta_L^{n-k}) \circ \widetilde{\mathscr{B}}_{k,n-k} \ .$$

Let us come back to the cotensor coalgebra. Nichols showed that this coalgebra has a universal property, from which one derives that it is a

Hopf algebra. The product is characterized as the unique coalgebra map $T_H^c(M) \otimes T_H^c(M) \to T_H^c(M)$ extending the given product on H and such that on elements of degree 1 in $T_H^c(M) \otimes T_H^c(M)$, i.e. on $H \otimes M + M \otimes H$, it is given by the left or right action of H on M.

When H and M are finite dimensional, it is very easy to understand the cotensor Hopf algebra: H^* is a Hopf algebra, M^* is a Hopf bimodule and the graded dual of the cotensor Hopf algebra $T_H^c(M)$ is the tensor Hopf algebra $T_{H^*}(M^*)$.

So, from Proposition 8, it should not be surprising that the algebra structure of $T_H^c(M)$ can made explicit in terms of the braid group action.

In order to simplify notations, let us put $V = M^R$. As $T_H^c(M)$ is a Hopf bimodule, it is a free right H-module over its subspace of right coinvariants, and this subspace is naturally but not trivially isomorphic to the tensor space $T(V)$ (see below). So, as a right H-module and right H-comodule, $T_H^c(M)$ is isomorphic to $T(V) \otimes H$. We are going to exhibit a Hopf algebra structure on $T(V) \otimes H$, and we shall show that it coincides (via the isomorphism above) with the one coming from the universal property.

Proposition 9. 1. *There is an associative algebra structure on $T(V)$, given by: for $x_1, \ldots, x_n$ in V,*

$$(x_1 \otimes \cdots \otimes x_p) \cdot (x_{p+1} \otimes \cdots \otimes x_n) = \sum_{w \in \Sigma_{p,n}} T_w(x_1 \otimes \cdots \otimes x_n)$$

where $\Sigma_{p,n-p}$ is the set of $(p, n-p)$-shuffles.

2. *The diagonal coaction of H on each $V^{\otimes n}$ gives $T(V)$ an H-comodule structure $\delta_L : T(V) \to H \otimes T(V)$, and δ_L is an algebra homomorphism.*

3. *For the diagonal action of H on each $V^{\otimes n}$, $T(V)$ is an H-module algebra, and $T(V) \otimes H$ inherits the crossed product algebra structure.*

4. *The following defines a coalgebra structure on $T(V) \otimes H$: for $(v_1, \ldots, v_n)$ in V and h in H,*

$$\Delta((v_1, \ldots, v_n) \otimes h) = \sum_{k=0}^{n} [(v_1, \ldots, v_k) \otimes v_{k+1(-1)} \cdots v_{n(-1)} h_{(1)}] \otimes [(v_{k+1(0)}, \cdots, v_{n(0)}) \otimes h_{(2)}] \ .$$

5. *The algebra structure of* 3 *and coalgebra structure of* 4 *are compatible and make $T(V) \otimes H$ a Hopf algebra.*

Proof. 1 In order to check associativity, we have to show that:

$$\mathscr{B}_{n,m-n} . \mathscr{B}_{k,n-k} = \mathscr{B}_{k,m-k} . \mathrm{shift}_k(\mathscr{B}_{n-k,m-n})$$

where $\mathrm{shift}_k . \mathscr{B}_{m-k} \to \mathscr{B}_m$ is the group homomorphism

given by: $\mathrm{shift}_k\ (\sigma_i) = \sigma_{i+k}\ \forall_i = 1, \ldots, m-k-1$.

When we expand in sums of products of braid group elements, all products $T_w \cdot T_{w'}$ which appear are such that $l(w \cdot w') = l(w) + l(w')$. So, all braid group elements are already written in terms of reduced expressions, and associativity follows from the independance in the reduced expression.

2 It follows from the fact that the braid group elements act as left comodule morphisms.

3 and 4 are simple computational checkings, and 5 is a consequence of 2

Proposition 10. 1. *There is a natural embedding ϕ of $T(V)$ in $T_H^c(M)$ given on homogeneous elements of degree n by*:

$$\phi(v^1, \dots, v^n) = \sum v^1 v^2_{(-1)} v^3_{(-2)} \cdots v^n_{(-n+1)} \otimes v^2_{(0)} v^3_{(-1)} \cdots v^n_{(-n+2)} \otimes \cdots \otimes v^n_{(0)}$$

whose image is the subspace of right coinvariants. In fact, one has an isomorphism of right module and comodule $\hat{\phi} : T(V) \otimes H \to T_H^c(M)$

$$\begin{aligned} \hat{\phi}[(v^1, \dots, v^n) \otimes h] = \sum & v^1 v^2_{(-1)} v^3_{(-2)} \cdots v^n_{(-n+1)} h_{(1)} \\ & \otimes v^2_{(0)} v^3_{(-1)} \cdots v^n_{(-n+2)} h_{(2)} \otimes \cdots \otimes v^n_{(0)} h_{(n)} \end{aligned}$$

2. *The subspace of right coinvariants is a subalgebra of $T_H^c(M)$.*

Proof. 1. One checks immediately that $\phi(v^1, \dots, v^n)$ is in $M^{\sqcup n}$ and that it is right coinvariant. Let $\psi : M^{\otimes n} \to M^{\otimes n}$ be the map given by:

$$\psi(w^1, \dots, w^n) = (w^1 S(w^2_{(-1)}), w^2_{(0)} S(w^3_{(-1)}), \dots, w^n_{(0)}) \ .$$

(Observe that, on the subspace of right coinvariants of $M^{\sqcup n}$, ψ is given by $P_R^{\otimes n}$, where P_R is the projection from M onto V.) By computation, one sees that $\psi \circ \phi$ is the identity. Surjectivity follows by counting dimensions if V is finite dimensional; it holds in general because a (bi)comodule is the direct sum of its finite dimensional subcomodules.

2. This follows from the fact that the product is a morphism of right comodules.

Theorem 11. *The map $\hat{\phi}$ is a Hopf algebra isomorphism.*

Proof. It is enough to show that it is a coalgebra isomorphism. Indeed, once we have seen this, we transport, by $\hat{\phi}$, the product of $T(V) \otimes H$ on $T_H^c(M)$, and we just have to check that it has the characteristic property of the multiplication on $T_H^c(M)$, i.e. that it is a coalgebra morphism (which immediate, because ϕ is a coalgebra morphism and $T(V) \otimes H$ is a Hopf algebra), and that it gives the good answer on degree one elements of $T_H^c(M) \otimes T_H^c(M)$, which is a simple checking. Now, that $\hat{\phi}$ is a coalgebra morphism is seen by inspection on the defining formulas.

1.4 The quantum symetric algebra

The sub-Hopf algebra $S_H(M)$ of $T_H^c(M)$ generated by H and M has very remarkable properties. It is again a Hopf bimodule and its subspace of right coinvariants is isomorphic, via ϕ, to the subalgebra of $T(V)$ generated by V. We shall denote this subalgebra by $S_\sigma(V)$. It can be considered as a quantum version of the symetric algebra and, as an algebra, $S_H(M)$ is nothing but the crossed product of H by $S_\sigma(V)$.
This Hopf algebra was introduced by W. Nichols under the name bialgebra (or Hopf algebra) of type one. The name quantum symetric algebra is deserved for at least two reasons:

1. The product, on the subspace of right coinvariants $S_\sigma(V)$ is given by applying the braid version of the total symetrization.
2. (A Milnor-Moore type property) A classical result of Milnor and Moore ([M-M]) states that for a connected, graded Hopf algebra A, if the subspace of primitive elements is isomorphic to the (quotient) space of indecomposable elements, then, A is both commutative and cocommutative (in the graded sense). We have a very similar situation here: Let $B = B_0 \oplus B_1 \oplus \cdots$ be a graded bialgebra or Hopf algebra. Let us call primitive an element of x in B such that $\Delta(x) \in B_0 \otimes B \oplus B \otimes B_0$. Note that B_1 is a B_0 Hopf bimodule. Then ([N]) B is isomorphic to $S_{B_0}(B_1)$ if and only if
(i) $B_0 \oplus B_1$ is exactly the space of primitive elements,
(ii) $(\bigoplus_{i=1}^{i=\infty} B_i)^2 = \bigoplus_{i=2}^{i=\infty} B_i$, i.e. B_1 is isomorphic to the space of indecomposable elements.

In fact, one can recover Milnor and Moore characterization of (graded) symetric bialgebras from this.

1.5 Universal construction in the Braid category

All the results above suggest that, given a vector space V with an automorphism σ of $V \otimes V$ which satisfies the braid equation in $V^{\otimes 3}$ (a so called "braided vector space"), one can define interesting algebra and coalgebra structures on the tensor space $T(V)$. In fact, using σ to construct a representation of the braid group B_n in $V^{\otimes n}$, one can define a (graded) multiplication *sh* by the same formula as in Proposition 6 and a comultiplication Δ by the usual formula for the coproduct (as in Definition 5, but with the two coactions trivial) in the classical shuffle algebra to provide it with a coalgebra structure. However these two structures are not compatible. In order to make (e.g.) the coproduct a morphism of algebras, one has to change the product in $T(V) \otimes T(V)$. One proceeds as follows:

Proposition 12. *Let (V, σ) be a braided vector space.*
1. *The following defines an associative algebra structure on $T(V) \otimes T(V)$: for p and q two positive integers, let $w_{p,q}$ be the permutation*:

$$\begin{pmatrix} 1 & 2 & \dots & q & q+1 & \dots & p+q \\ p+1 & p+2 & \dots & p+q & 1 & \dots & p \end{pmatrix},$$

and let $T_{w_{p,q}}$ be the associated element in the braid group B_{p+q}: it acts in $V^{\otimes p+q}$ and can be seen as a "generalized flip" from $V^{\otimes p} \otimes V^{\otimes q}$ to $V^{\otimes q} \otimes V^{\otimes p}$. Then the product sends $(V^{\otimes n} \otimes V^{\otimes p}) \otimes (V^{\otimes q} \otimes V^{\otimes m})$ to $(V^{\otimes n+q} \otimes V^{\otimes p+m})$ and it is the composition: $(sh \otimes sh) \circ (Id \otimes T_{w_{p,q}} \otimes Id)$ where sh denotes the product on $T(V)$ defined above.

2. *Then $\Delta : T(V) \to T(V) \otimes T(V)$ is an algebra homomorphism.*

Proof. The idea is the same as for the proof of the first statement of Proposition 9. One observes that all the maps involved are given by the action of certain elements of the group algebra of the braid group. The identities to be checked involve sums of products of braid group elements, and all products $T_w \cdot T_{w'}$ appearing are such that $l(w \cdot w') = l(w) + l(w')$. So, all braid group elements are already written in terms of reduced expressions, and both statements follow from the independance in the reduced expression.

One can formulate these twisted bialgebras structures in a unifom way using a universal construction in the Braid category (cf [Ka]) made linear . Recall that objects in the braid category $\mathscr{B}$ are the "direct sums" of positive integers n, and that the morphisms $\mathrm{Mor}(n, m)$ are 0, if $n \neq m$, and the group algebra of B_n otherwise. It is a braided monoidal category, the monoidal structure being given by addition. Its universal property says that, given a braided vector space (V, σ), there is unique monoidal functor from $\mathscr{B}$ to the category of vector spaces, sending 1 to V and the generator of B_2 to σ.

Definition and Proposition 13. 1. *The shuffle algebra $\mathscr{S}$ in $\mathscr{B}$ is, as an object, the direct sum of all objects n.*

2. *The product is given by the direct sum of its "homogenous components": for all n and m in* $\mathbf{N}$, *one has a component in* $\mathrm{Mor}(n \otimes m, n+m)$ *which is the sum of $T_w \in B_{n+m}$, w ranging in the set of (n, m)- shuffles of Σ_{n+m}.*

3. *The coalgebra structure is also given by the direct sum of its "homogenous components": for all n, p, q in* $\mathbf{N}$ *such that $p + q = n$, the component in* $\mathrm{Mor}(n, p \otimes q)$ *is the canonical morphism $n \to p \otimes q$.*

4. *These product and coproduct are compatible if we give $\mathscr{S} \otimes \mathscr{S}$ the algebra structure deduced from the one on $\mathscr{S}$ by first twisting by the braiding: $(Id \otimes T_{w_{p,q}} \otimes Id) : (n+p) \otimes (q+m) \to (n+q) \otimes (p+m)$.*

The proof is the same as before: simply observe that we are only using actions of linear combinations of braid group elements, which are precisely the morphisms in $\mathscr{B}$.

2. The examples from abelian group algebras

We are going to apply the preceding machinery to a very simple situation, but which leads to interesting examples.

Let $H = k[G]$ be the group algebra of an abelian group G, written as a product $\mathbf{Z}^r \times \mathbf{Z}/l_1 \times \mathbf{Z}/l_2 \times \cdots \times \mathbf{Z}/l_p$. We shall fix generators $K_1, \ldots, K_N$ of G $(N = r + p)$. As H is both commutative and cocommutative, the structure of the subspace V of right coinvariants of a Hopf bimodule M is just that of a left module and a left comodule, with trivial compatibility condition. We shall consider the following family of examples: V is a k-vector space of dimension N, with a left coaction of H reproducing the coproduct of H, and a left action of H which is completely reducible. So, there is a basis $(e_1, \ldots, e_N)$ of V and N^2 non zero scalars q_{ij} such that: $\delta(e_i) = K_i \otimes e_i$, $K_i(e_j) = q_{ij} e_j$.

Note that the braiding in $V \otimes V$ is given by: $\sigma(e_i \otimes e_j) = q_{ij}(e_j \otimes e_i)$. The adjoint action in $S_H(M)$ is completely described as follows: for any x in $S_H(M)$ and any $i = 1, \ldots, N$, $ade_i(x) = e_i x - K_i(x) e_i$; so $ad(e_i)(S_\sigma(V)) \subset (S_\sigma(V))$

In order to study the structure of $S_H(M)$, the following lemma will be very useful.

Lemma 14.

(a) *for all* $i = 1, \ldots, N$ *and* $r \in \mathbf{N}$, $e_i^r = \prod_{k=1}^r \left(\frac{q_{ii}^k - 1}{q_{ii} - 1}\right) e_i^{\otimes r}$

(b) *for* $i \neq j$ *and* $r \in \mathbf{N}$,

$$ad(e_i)^r(e_j) = \prod_{k=1}^{r} \left(\frac{q_{ii}^k - 1}{q_{ii} - 1}\right) \prod_{k=0}^{r-1} \left(1 - q_{ii}^k q_{ij} q_{ji}\right) e_i^{\otimes r} \otimes e_j \quad .$$

Proof. By induction on r.

Example 1. Assume that the coefficients q_{ij} satisfy: for $i \neq j$, $q_{ij} q_{ji} = 1$. One gets from Lemma 14 that, for $i \neq j$, $ade_i(e_j) = 0$, i.e. $e_i e_j = q_{ij} e_j e_i$. The algebra $S_\sigma(V)$ is the "algebra of functions" on the quantum hyperplane of Manin ([Mn]).

Example 2. Let $A = (a_{ij})_{1 \leq i,j \leq N}$ be a symetrizable generalized Cartan matrix, $(d_1, \ldots, d_N)$ positive integers relatively prime such that $(d_i a_{ij})$ is symetric. Take for G either $\mathbf{Z}^N$ or $(\mathbf{Z}/l)^N$. Let $q \in \mathbf{C}$ and define $q_{ij} = q^{d_i a_{ij}}$. (For $G = (\mathbf{Z}/l)^N$, q has to be an l-th root of unity.)

One gets immediately from Lemma 14. that:

(a) if q is a root of unity of order l, then for all $i = 1, \ldots, N$, $e_i^l = 0$.

(b) if q is generic, then for $i \neq j$ there is a smallest integer r such that $ad(e_i)^r(e_j) = 0$, and it is given by: $(r-1) d_i a_{ii} + 2 d_i a_{ij} = 0$, i.e. $r = 1 - a_{ij}$. In fact, we have:

Theorem 15. *In the situation of Example* 2,

1. *For* $G = \mathbf{Z}^N$, *if* q *is not a root of unity, then the Hopf algebra* $S_H(M)$ *is isomorphic, as a Hopf algebra, to the sub Hopf algebra* U_q^+ *of the quantized universal enveloping algebra associated with* A.

2. *For $G = (\mathbf{Z}/l)^N$, if q is a primitive l-th root of unity, $S_H(M)$ is isomorphic to the quotient of the restricted quantized enveloping algebra u_q^+ of Lusztig* ([L1]) *by the two-sided Hopf ideal generated by the elements $(K_i^l - 1)$, $i = 1, \dots, N$.*

Proof. Observe that, giving the degree 0 to H and 1 to the e_i's, U_q^+ or u_q^+ is a graded Hopf algebra, generated by its elements of degree 0 and 1. Furthermore, any primitive element of degree at least 2 would be in the kernel of the Hopf pairing between U_q^+ and U_q^- or between u_q^+ and u_q^-, and we know that this Hopf pairing is nondegenerate. (This is the "raison d'être" of the universal R-matrix). So the theorem follows from the "Milnor-Moore type property" of Section 1.4.

Remark 1. The computations of Lemma 14 give a very simple way to check that the quantized Serre relations hold. In fact, for our framework, they give a little more: one sees that the coefficients q_{ij} occur only via the symetrized expression $q_{ij}q_{ji}$. This leaves the freedom to chose the antisymetric part. If one introduces an antisymetric matrix (r_{ij}) and put $q_{ij} = q^{d_i a_{ij} + r_{ij}}$, $S_H(M)$ is isomorphic to the dual of the "multiparametric versions" of U_q^+ introduced by Reshetikhin ([Re]) via twistings.

Remark 2. Supersymetric versions are constructed by putting an $\mathbf{Z}/2$ copy in G to make some e_i's odd. More precisely, take $G = \mathbf{Z}^N \times \mathbf{Z}/2$ and call ϵ the generator of $\mathbf{Z}/2$. Let $J \subset \{1, \dots, N\}$ the subset of indices i for which e_i must be odd. For $i \in J$, put $\delta(e_i) = \epsilon K_i \otimes e_i$, and $\epsilon(e_i) = -e_i$; for i not in J, δ is as before and $\epsilon(e_i) = e_i$.

3. A classification result

We keep the same notations as in the preceeding section. All the structure of $S_\sigma(V)$ is encoded in the $N \times N$ matrix (q_{ij}), and we saw that some particular choices led to familiar examples. The question that we address now is: are there other interesting examples? We begin by the construction of "multiplicative" bases for the quantum shuffle algebra: this is a generalization of a result of Radford ([Ra]) on bases for the classical shuffle algebra.

3.1 Multiplicative bases in the quantum shuffle algebra

3.1.1 Let V be a finite dimensional vector space. We begin with some combinatorics in the tensor space $T(V)$, borrowed to Radford.

Fix $(e_1, \dots, e_N)$ a basis of V, and a total ordering (e.g. $1 < 2 < \dots < N$). Then the set S of tensor products $e_{i_1} \otimes \dots \otimes e_{i_k}$ of these basis elements provide a basis of $T(V)$.

Definition 16. 1. *A total ordering $\le$ on the set S is defined by lexicographic ordering, with the convention that $a \otimes b \le a$ for a and b in S.*

2. *An element p in S is said to be a prime if, for any splitting $p = a \otimes b$, with a and b in S, one has: $b < p$.*

One can show that any $a \in S$ has a unique prime factorization, i.e. can be written in a unique way as a (tensor) product of primes with minimal number of primes. In fact, if $a = p_1 \cdots p_r$ is a product of primes, $p_1 \cdots p_r$ is its prime factorization if and only if $p_1 \le p_2 \le \cdots \le p_r$.

3.1.2 Assume now that (V, σ) is a finite dimensional braided vector space, with σ given by the $N \times N$ matrix (q_{ij}).

Proposition 17. *Let $a \in S$ and $a = p_1^{\otimes n_1} \otimes p_2^{\otimes n_2} \otimes \cdots \otimes p_s^{\otimes n_s}$ be its prime factorization. Define $X_a = p_1^{n_1} p_2^{n_2} \cdots p_s^{n_s}$ (i.e. we replace tensor products between p_i's by quantum shuffle multiplication). Then $X_a, a \in S$ form a basis of $T(V)$, and the change of basis with respect to a is triangular: there exist $\alpha_{ab} \in k$, with $\alpha_{aa} \neq 0$ such that: $X_a = \sum_{a \le b} \alpha_{ab} b$.*

Proof. We adapt Radford's one to our situation; this is possible because of the special form of the braiding (usual permutation up to a scalar). Let l_i be the length (or degree) of the tensor p_i. Then $X_a = \mathscr{B}_{(l_1,\ldots,l_s)}\ (p_1^{\otimes n_1} \otimes p_2^{\otimes n_2} \otimes \cdots \otimes p_s^{\otimes n_s})$. As shown by Radford, for $w \in \Sigma_{(l_1,\ldots,l_s)}$, $w(a) \ge a$ and $w(a) = a$ if and only if w is in the subgroup $\Sigma_{n_1} \times \cdots \times \Sigma_{n_s}$ of "block permutations", permuting only the p_i's among themselves for each i. Formula $X_a = \sum_{a \le b} \alpha_{ab} b$ follows immediately, as T_w, up to a non-zero scalar, acts as w. Furthermore α_{aa} is a product of q-factorials: for $1 \le i \le s$ let $p_i = (e_{j_1}, \ldots, e_{j_{m_i}})$ and $Q_i = \prod_{k,l \in \{e_{j_1},\ldots,e_{j_{m_i}}\}} q_{kl}$. Then $\alpha_{aa} = [n_1]_{Q_1}! \cdots [n_s]_{Q_s}!$.

Corollary 18. *Let $i \neq j$ in $1, \ldots, N$. There is a total ordering for which $i > j$. Then, for each n, $e_i^{\otimes n} \otimes e_j$ is a prime, and the ordered quantum shuffle products, $(e_i^{\otimes n_1} \otimes e_j)(e_i^{\otimes n_2} \otimes e_j) \cdots (e_i^{\otimes n_r} \otimes e_j)$, for $n_1 \le n_2 \le \cdots \le n_r$, are linearly independent.*

Remark. Assume that $q_{ij} = q^{a_{ij}}$, with (a_{ij}) a Cartan matrix of type A. Then the multiplicative basis (X_a) of $T(V)$ has the following remarkable property:

Given a in S, either X_a is in the subalgebra $S_\sigma(V)$, or it is not; and those which are in $S_\sigma(V)$ form a basis of $S_\sigma(V)$, which is, up to a scalar, nothing but the Poincare-Birkhoff-Witt basis.

To see this, recall that, for each positive root $\alpha = \alpha_i + \cdots + \alpha_j$, on may construct a "root vector" $e_\alpha = ad(e_i)ad(e_{i+1}) \cdots ad(e_{j-1})(e_j)$ (for the A-series, this is equivalent to the construction using Lusztig's braid automorphisms). The same computations as in Lemma 14 give: $e_\alpha = (1 - q^{-2})^{j-i-1} e_i \otimes e_{i+1} \otimes \cdots \otimes e_j$, and this is a prime element.

3.2 Consequences of growth conditions

We want to show that reasonable growth conditions on the dimensions of the homogenous components of $S_\sigma(V)$ imply the existence of Serre type relations, which in turn imply the existence of a symetrizable generalized Cartan matrix from which $S_\sigma(V)$ is constructed as in Example 2 of Section 2.

Lemma 19. *Suppose there are $i \neq j$ in $\{1, \ldots, N\}$ such that, for all $r \in \mathbf{N}^*$, $(ade_i)^r(e_j) \neq 0$. Then, for n big enough, the dimension of the homogenous component of degree n satisfies*: $\dim S_\sigma(V)(n) \geq \frac{e^{\sqrt{n}}}{n} \cdot \frac{1}{\pi e^2}$

Proof. One has, from Lemma 14, that if $(ade_i)^r(e_j)$ is not 0, then $e_i^{\otimes r} \otimes e_j$ is in $S_\sigma(V)$. So, if for all $r \in \mathbf{N}^*$, $(ade_i)^r(e_j) \neq 0$, then for all $n_1 \leq n_2 \leq \cdots \leq n_r$ $(e_i^{\otimes n_1} \otimes e_j)(e_i^{\otimes n_2} \otimes e_j) \cdots (e_i^{\otimes n_r} \otimes e_j)$ is in $S_\sigma(V)$. From Corollary 18, one gets that, for $r < n$, $\dim S_\sigma(V)(n)$ is at least the number of partitions $P(n-r, r)$ of $n - r$ in r parts. Using standard minorations for $P(n, m)$ and Stirling's formula, the result follows.

Lemma 19 implies immediately the following.

Lemma 20. *If the Gelfand-Kirillov dimension of $S_\sigma(V)$ is finite, or its Borho-Kraft dimension* ([*B-K*]) *is strictly smaller than* $1/2$, *then necessarily, for all $i \neq j$ there exists n_{ij} in $\mathbf{N}$ such that*: $(ade_i)^{n_{ij}}(e_j) = 0$.

Recall that a matrix $(b_{ij})_{1 \leq i,j \leq N}$ is said to be indecomposable if $\forall k$, $l \in \{1, \ldots, N\}$ there exists $i_1 = k, i_2, \ldots, i_r = l$ such that $\forall 1 \leq s \leq r,\ b_{i_s i_{s+1}} \neq 0$.

We shall say that a matrix $(q_{ij})_{1 \leq i,j \leq N}$ with non zero entries is exp-indecomposable if for all $k, l \in \{1, \ldots, N\}$ there exists $i_1 = k, i_2, \ldots, i_r = l$ such that $\forall 1 \leq s \leq r, \quad q_{i_s i_{s+1}} \neq 1$.

Theorem 21. *Assume that the ground field k is the field of complex numbers* $\mathbf{C}$, *that the symetrized matrix $(q_{ij}q_{ji})_{1 \leq i,j \leq N}$ is exp-indecomposable and that the coefficients q_{ij} are strictly positive. Then $S_\sigma(V)$ is of finite Gelfand-Kirillov dimension, or of Borho-Kraft dimension strictly smaller than* $1/2$ *if and only if there exists q in $\mathbf{C}^*$, relatively prime positive integers $(d_1, \ldots, d_N)$ and a Cartan matrix $A = (a_{ij})$ such that*:

$$q_{ii} = q^{d_i} \qquad q_{ij}q_{ji} = q^{-d_i a_{ij}} = q^{-d_j a_{ji}} \quad .$$

The Hopf algebra $S_H(M)$ is then isomorphic to the multiparametric version of the "upper triangular subalgebra U_q^+" of the quantized enveloping algebra associated with A.

Proof. According to Lemma 20, for all $i \neq j$ there exists a smallest integer n_{ij} such that: $(ade_i)^{n_{ij}}(e_j) = 0$. As q_{ii} is not a root of unity, necessarily, we have: $1 - q_{ii}^{n_{ij}} q_{ij}q_{ji} = 0$, so: $q_{ii}^{-n_{ij}} = q_{jj}^{-n_{ji}} = q_{ij}q_{ji}$. This formula suggests to define $n_{ii} = -2$. Observe that $n_{ij} = 0$ implies $n_{ji} = 0$. The hypothesis on (q_{ij}) implies that the matrix $N = (n_{ij})$ is indecomposable. Put $q_{ii} = e^{x_i}, x_i \in \mathbf{R}$. Note that $x_i \neq 0$ and that x_i's are all of the same sign. Then $n_{ij}x_i = n_{ji}x_j$, from which follows that there exists $x \in \mathbf{R}$ and $(d_1, \ldots, d_N)$ positive integers such that $x_i = xd_i$; we may choose x in such a way that the d_i's are relatively prime. Then, the matrix $N = (n_{ij})$ is the opposite of a symetrizable generalized Cartan matrix.

4. Inductive construction of higher rank quantized enveloping algebras

The data needed to perform the quantum shuffle construction is that of a Hopf algebra and a Hopf bimodule on it. Representations of quantized enveloping algebras essentially provide such a Hopf bimodule for their sub-Hopf algebra U_q^+.

Recall (cf [DC-K-P]) that for each lattice M between the root lattice Q and the weight lattice P, one has a version $U_q(M)$ of $U_q\mathcal{G}$ (loosely speaking, one adds grouplike elements K_v for all v in the lattice M). This can be slightly generalized as follows: assume that the weight lattice is an orthogonal direct summand of a bigger lattice P', i.e. $P' = P \oplus S$ with S a sublattice orthogonal to P. Then, for any sublattice M of P' containing Q, one has a version $U_q(M)$ of $U_q\mathcal{G}$, where the defining relations involving K_v, $v \in M$ only use the orthogonal projection of v onto P.

We are going to show that, if we take a suitable irreducible representation of a suitable version of $U_q\mathcal{G}$, what we construct is the "plus part" of a quantized enveloping algebra associated with a Lie algebra containing $\mathcal{G}$ and of rank equal to $rk(\mathcal{G}) + 1$.

In order to increase the rank by 1, we extend U_q^+ by a grouplike element, which acts and coacts diagonally on the module. This amounts to extend the weight lattice by a vector orthogonal to it, and then take a suitable sublattice. This was suggested to us by a very interesting construction of Kac-Moody algebras by Benkart, Kang and Misra ([B-K-M]). These authors start with a finite dimensional simple Lie algebra of classical type $\mathcal{G}$ and its fundamental representation V. They trivially extend $\mathcal{G}$ by a central element c, and make c act by a non zero scalar on V (and dually on V^*). Given a certain $\mathcal{G}$-equivariant linear map $\phi : V^* \otimes V \to \mathcal{G}$, they construct the minimal graded Lie algebra with local part $V^* \oplus \mathcal{G} \oplus V$ and show that it is isomorphic to a Kac-Moody Lie algebra whose Cartan matrix is obtained from that of $\mathcal{G}$ by adding a line and a column of a certain form. In fact, our work may be seen as a sort of quantization of theirs, with the benefit that we do not need to use any pairing ϕ: it automatically appears when we do the quantum double.

4.1 General construction

Let $\mathcal{G}$ be finite dimensional complex Lie algebra with an $n \times n$ Cartan matrix A, and V an irreducible finite dimensional $U_q\mathcal{G}$ module with lowest weight λ.

If we consider here the version where M is the sublattice of P generated by Q and λ, V is a Yetter crossed module on $U_q^+(M)$: it is generated, as a module, by a lowest weight vector v and the coaction of $U_q^+(M)$ on V is completely determined by : $\delta(v) = K_\lambda \otimes v$ (due to twisted compatibility between action and coaction). Extend the lattice M by an element μ orthogonal to it and with square length $(\mu, \mu) = c$. Let Q' the sub-lattice generated by Q and $\lambda + \mu$. The modification of U_q^+ that we use is the Hopf algebra $U = U_q(Q')^+$.

Indeed, V is a Yetter crossed module on U: one extends the U_q^+-module structure by making $K_{\lambda+\mu}$ act diagonally in a basis of weight vectors of V, the eigenvalues being completely specified by: $K_{\lambda+\mu}(v) = q^{(\lambda,\lambda)+(\mu,\mu)}v$, and one defines the coaction of U on V by $\delta(v) = K_{\lambda+\mu} \otimes v$.

Proposition 22. Assume that the scalar $c = (\mu, \mu)$ is such that: for all $i \in \{1, \ldots, n\}$, $2\frac{(\lambda,\alpha_i)}{((\lambda,\lambda)+c)}$ is a non positive integer. Then the quantum symetric algebra $S_U(V \otimes U)$ is isomorphic to the "plus part" of the quantum generalized Kac-Moody algebra $\widetilde{U}_q$ whose Cartan matrix (a_{ij}) is obtained from A by adding a line and a column with: $a_{i,n+1} = 2\frac{(\lambda,\alpha_i)}{(\alpha_i,\alpha_i)}$, $a_{n+1,i} = 2\frac{(\lambda,\alpha_i)}{((\lambda,\lambda)+c)}$.

Proof. We know that $S_U(V \otimes U)$ is generated by U and V. The same computations as Lemma 14 lead to: $ad(e_i)^r(v) = 0$ for $r \geq 1 - 2\frac{(\lambda,\alpha_i)}{(\alpha_i,\alpha_i)}$ and $ad(v)^s(e_i) = 0$ for $s \geq 1 - 2\frac{(\lambda,\alpha_i)}{((\lambda,\lambda)+c)}$. So, clearly, $S_U(V \otimes U)$ is a Hopf algebra quotient of $\widetilde{U}_q^+$. The kernel is a two-sided ideal and coideal, homogenous with respect to the gradation by the root lattice, and which does not meet the subspace spanned by the elements having for degree a simple root. If it is not zero, it has to contain an element of minimal degree . But such an element is then necessarily nearly primitive, which is impossible due to the non degeneracy of the Hopf pairing between the "plus" and "minus" parts ([Ro1]).

4.2 Examples

We now explain how to obtain step by step, and starting with $sl(2)$, all quantized enveloping algebras associated with finite dimensional simple Lie algebras or with affine Kac-Moody Lie algebras. For roots and weights, we use the notations from Bourbaki ([Bo]). In particular, the root lattice and the weight lattice are realized as sublattices of an euclidian lattice with orthonormal basis (ϵ_i).

The choice of the element μ in Proposition 22 is made as follows: one works over $\mathbf{Q}$ (i.e. μ has rational coordinates in the basis (ϵ_i)), and one chooses the euclidean space in which it lives to be of the smallest possible dimension.

(a) The A_n series.

Take $\mathcal{G} = sl(n)$ and V the fundamental representation, with lowest weight $-\omega_{n-1}$. Let $\mu = \frac{1}{n}(\epsilon_1 + \cdots + \epsilon_n) - \epsilon_{n+1}$. Then we get $sl(n+1)$.

(b) The B_n series.

Take again $\mathcal{G} = sl(n)$ and V the fundamental representation, with lowest weight $-\omega_{n-1}$, but choose now $\mu = \frac{1}{n}(\epsilon_1 + \cdots + \epsilon_n)$. Then we get $so(2n+1)$.

(c) The C_n series.

Take $\mathcal{G} = sl(n)$ and V the "symetric square" of the fundamental representation, with lowest weight $-2\omega_{n-1}$. Choose $\mu = \frac{2}{n}(\epsilon_1 + \cdots + \epsilon_n)$. Then we get $sp(2n)$.

(d) The D_n series.

Take $\mathcal{G} = sl(n)$ and V the second exterior power of the fundamental representation, with lowest weight $-\omega_{n-2}$. Choose $\mu = \frac{2}{n}(\epsilon_1 + \cdots + \epsilon_n)$. Then we get $so(2n)$.

(e) The case of F_4.

Take $\mathcal{G} = so(7)$ and V the irreducible module with lowest weight $-\omega_3$ (the spin representation) Choose $\mu = \frac{1}{2}\epsilon_4$.

(f) The case of G_2.

Take $\mathcal{G} = sl(2)$, and V the spin $\frac{3}{2}$ representation. Choose $\mu = \frac{-1}{2}(\epsilon_1 + \epsilon_2) + \epsilon_3$.

(g) In the same way, E_6 is obtained from $so(10)$ and one of the half-spin representation, then E_7 from E_6 and E_8 from E_7.

(h) The quantum affine untwisted Kac-Moody algebras.

Let $\mathcal{G}$ be a finite dimensional simple complex Lie algebra and $V = \mathcal{G}$ the adjoint representation, with lowest weight $-\theta$. Here μ has to be of length 0, and orthogonal to Q. So we take $\mu = \delta$.

4.3 Application

The isomorphism of $S_U(V \otimes U)$ with $S_\sigma(V) \otimes U$ allows for an inductive construction of bases. Let us show that, in the A-series case, this leads very simply to the Poincaré-Birkhoff-Witt basis and consequently to the "q-exponential formula" for the universal R-matrix. Indeed, we assume by induction that we have constructed a Poincaré-Birkhoff-Witt basis for A_n; then we need a basis of $S_\sigma(V)$. We observe that the braid group action is given by application of the R-matrix of A_{n-1}-type in the fundamental representation, twisted by the scalar q^c (due to the effect of $k_{\lambda+N}$ in the coaction). Here $c = 1 + \frac{1}{n}$, and the scalar q^c combines with the factor $q^{-\frac{1}{n}}$ appearing from direct application of the universal R (see comments in [C-P] p. 277), to give that the braid group representation in the tensor powers of the fundamental representation factorizes through the Hecke algebra, with eigenvalues of the generators 1 and $-q^2$. Then, calling $(v_1, \ldots, v_n)$ the standard basis of V, we have: for $i < j$, $v_i \cdot v_j = q^2 v_j \cdot v_i$, so $S_\sigma(V)$ is a twisted polynomial algebra (i.e. the algebra of functions on a quantum hyperplane). Furthermore, looking at weights with respect to the new lattice Q', we see that v_i's are root vectors, v_i being associated with the root $\alpha_i + \cdots + \alpha_n$. So, the given ordering on the v_i's is a convex ordering and we get a Poincaré-Birkhoff-Witt basis.

References

[B-K-M] G. Benkart, S-J. Kang, K. Misra: Indefinite Kac-Moody algebras of classical type, Advances in Math. **105**, 76–110 (1994)

[B-K] W. Borho, H. Kraft: Über die Gelfand-Kirillov Dimension, Math. Ann. **220**, 1–⊠ (1976)

[Bo] N. Bourbaki: Groupes et algèbres de Lie, Ch. 4, 5, 6, (1968), Hermann

[C-P] V. Chari, A. Pressley: A guide to quantum groups, (1994), Cambridge University Press

[D] V. Drinfeld: Quantum Groups, Proc.Int. Cong. Math., Berkeley, 798–820 (1986)

[DC-K-P] C. De Concini, V. Kac, C. Procesi: Quantum coadjoint action, J. Amer. Math. Soc. **5**, 151–190 (1992)

[J] M. Jimbo: A q-difference analoque of $U(\mathscr{G})$ and the Yang-Baxter equation, Lett. Math. Phys. **10**, 63–69 (1986)

[Ka] Ch. Kassel: Quantum Groups, Graduate Texts in Mathematics **155** (1995), Springer Verlag, Berlin Heidelberg New York

[K-L] G. Krause, T. Lenagan: Growth of algebras and Gelfand-Kirillov dimension, Research Notes in Mathematics **116**, Pitman, Boston (1988)

[L1] G. Lusztig: Quantum groups at a root of 1, Geom. Dedic. **35**, 89–114 (1990)

[L2] G. Lusztig: Quivers, perverse sheaves and quantized enveloping algebras, J. Amer. Math. Soc. **4**, 365–421 (1991)

[Mj] S. Majid: Doubles of quasitriangular Hopf algebras, Comm. Alg **19**, 3061–3073 (1991)

[Mn] Y. Manin: Some remarks on Koszul algebras and quantum groups, Ann. Inst. Fourier **37**, 191–205 (1987)

[M-M] J. Milnor, C. Moore: On the structure of Hopf algebras, Ann. of Math. **81**, 211–264 (1965)

[N] W. Nichols: Bialgebras of type I, Comm. Alg **15**, 1521–1552 (1978)

[Ra] D. Radford: A natural ring basis for the Shuffle Algebra and an application to group schemes, J. of Alg. **58**, 432–454 (1979)

[Ri] C. Ringel: Hall algebras and quantum groups, Inv. Math. **101**, 583–592 (1990)

[Re] N. Reshetikhin: Multiparameter quantum groups and twisted quasitriangular Hopf algebras, Lett. Math. Phys. **20**, 331–335 (1990)

[Ro1] M. Rosso: Certaines formes bilineaires sur les groupes quantiques et une conjecture de Schechtman et Varchenko, C. R. Acad. Sc. Paris (I), **314**, 5–8 (1992)

[Ro2] M. Rosso: Groupes quantiques et algèbres de battage quantiques, C. R. Acad. Sc. Paris I, **320**

[S] M. Sweedler: Hopf algebras, W. A. Benjamin Inc., New York (1969)

[W] S. Woronowicz: Differential calculus on compact matrix pseudogroups (quantum groups, Commun. Math. Phys. **122**, 125–170 (1989)

[Y] D. Yetter: Quantum groups and representations of monoidal categories, Math. Proc. Camb. Phil. Soc. **108**, 261–290 (1990)