A FREENESS THEOREM FOR NICHOLS ALGEBRAS

MATÍAS GRAÑA

Abstract. We prove a freeness result for Nichols algebras over certain Nichols subalgebras. This result allows in particular to classify pointed Hopf algebras of prime and prime squared index.

1. Introduction and Notation

1.1. **Introduction.** Let V be a vector space and $c \in \operatorname{End}(V \otimes V)$ a solution of the braid equation

$$(c \otimes \mathrm{id})(\mathrm{id} \otimes c)(c \otimes \mathrm{id}) = (\mathrm{id} \otimes c)(c \otimes \mathrm{id})(\mathrm{id} \otimes c) \in \operatorname{End}(V \otimes V \otimes V).$$

Let AV and CV be respectively the tensor algebra and tensor coalgebra of V; they are both braided bialgebras. There exists a unique bialgebra map $\mathbf{S} : AV \to CV$ extending the identity $\mathrm{id} : V \to V$ in degree one. The image $\mathfrak{B}(V) := \operatorname{Im}(\mathbf{S}) \subset CV$ is a braided bialgebra usually called *quantum symmetric algebra*. If c is *rigid* (see definition in 1.3.1 below), then we say that $\mathfrak{B}(V)$ is a *Nichols algebra*. In such case it is known that $\mathfrak{B}(V)$ is a braided Hopf algebra in a rigid braided category.

In this article we consider a rigid solution (V, c) of the braid equation and a subspace $W \subset V$ such that $c(W \otimes W) = W \otimes W$. We identify the quantum symmetric algebra $\mathfrak{B}(W)$ with a subalgebra of $\mathfrak{B}(V)$. Under certain additional hypotheses it is a Nichols algebra, eventually in a different rigid braided category. Assume further that $\mathfrak{B}(W)$ is finite dimensional. Our main result, Theorem 3.8, shows then that $\mathfrak{B}(V)$ is free over $\mathfrak{B}(W)$. More precisely, we describe a graded subalgebra K of $\mathfrak{B}(V)$ (which is also a left coideal) such that $\mathfrak{B}(V) \simeq K \otimes \mathfrak{B}(W)$ as $(K, \mathfrak{B}(W))$-bimodules. Consequently, $P_{\mathfrak{B}(V)}(t) = P_K(t) P_{\mathfrak{B}(W)}(t)$, (where $P_A(t) = \sum_i \dim A_i t^i$ is the Hilbert polynomial of $A = \oplus_i A_i$) and in particular the dimension of $\mathfrak{B}(W)$ divides that of $\mathfrak{B}(V)$. Moreover, assume that there is a decomposition $V = \oplus_i V_i$ such that $c(V_i \otimes V_j) = V_j \otimes V_i$ for all i, j and that there exists for each i a (possibly trivial) subspace $W_i \subseteq V_i$ verifying the hypotheses of the first part. Then $\prod_i P_{\mathfrak{B}(W_i)}(t)$ divides $P_{\mathfrak{B}(V)}(t)$.

It was recently proved independently by Scharfschwerdt [Sf] and Takeuchi [T3] that the Nichols–Zoeller theorem [NZ] holds in Yetter–Drinfeld categories. In general, however, our algebras $\mathfrak{B}(V)$,

Date: September 1999.

This work was partially supported by CONICET, UBA, CONICOR and SeCyT-UNC.

$\mathfrak{B}(W)$ lie in different braided categories, and their result does not apply in the present situation (moreover, our result applies also to the case when $\mathfrak{B}(V)$ is infinite dimensional). We prove 3.8 using algebras of *quantum differential operators* $\mathcal{A}V \hookrightarrow \mathrm{End}(\mathfrak{B}(V))^{\mathrm{op}}$. To this end, we generalize the definition for the "abelian case" given, for instance, in [FG] (this algebra was considered also by Kashiwara and Lusztig). The author was not able to find this general notion in the literature.

As an application of our main result we classify, in 4.1 and 4.2, pointed Hopf algebras of index p and p^2 (p a prime number). This classification generalizes results from [D] and [AS2]. Here, for a pointed Hopf algebra A we define the index as the ratio $\dim A/\#G(A) =: [A : G(A)]$, where $G(A)$ is the group of group-likes of A.

The results of this article can be combined with a parameterization of Nichols algebras of ranks 3 and 4 in ${}^{\mathbf{k}\Gamma}_{\mathbf{k}\Gamma}\mathcal{YD}$ (Γ a finite group) in order to give a classification of Nichols algebras of dimension < 32. This, together with the "Lifting procedure" of [AS1], is a first step for the classification of pointed Hopf algebras of index < 32. These and related problems are considered in [G2].

The article is organized as follows: in Section 2 we state and prove some first results on Quantum Symmetric algebras and Nichols algebras. For $V \in {}^{\mathbf{k}\Gamma}_{\mathbf{k}\Gamma}\mathcal{YD}$, we define the subspaces that will play the rôle of W in the applications and study the behavior of the braiding with respect to these subspaces. We also prove in Section 2 a generalization of [AS1, 3.4-3.5] for general abelian braided categories. Section 3 is devoted to algebras of Quantum Differential Operators and to the main result. Finally, in Section 4 we classify all pointed Hopf algebras of prime index and all pointed Hopf algebras of prime squared index.

1.2. **Acknowledgements.** I thank N. Andruskiewitsch for his careful reading of the material and for the important suggestions he made. His contribution improved and made more clear the presentation of this work. I also thank him for the statement of 2.2.

I thank also the referee, who in particular pointed out the Remark 2.14, reducing the proof of 3.5.

1.3. **Notation.** We refer to [Mo] for notation on Hopf algebras. We fix $\mathbf{k}$ an algebraically closed field of characteristic 0. All vector spaces, algebras, tensor products, homs are considered over $\mathbf{k}$ unless explicitly stated. For comultiplication we use Sweedler's notation without summation symbol ($\Delta(z) = z_{(1)} \otimes z_{(2)}$).

It is worth noting that most of the results of this article (in particular, the main Theorem 3.8) are true in positive characteristic (with the same proofs). The results in section 4 also hold, assuming $\operatorname{char} \mathbf{k}$ does not divide $\dim A$.

We call a *braided pair* (or BP) a pair (V, c), where V is a vector space and $c : V \otimes V \to V \otimes V$ is a (bijective) solution of the braid equation. Throughout, V shall be finite dimensional. It is well known that there exists a braided category containing V as an object and such that c coincides with the braiding in the category, a construction due to [Ly] (see also [H, Sn]). Moreover, this category is abelian and has countable direct sums. Explicitly, one can take the category of comodules over the FRT bialgebra generated by (V, c) (see for instance [AA]).

When working in a non-symmetric braided category, one must distinguish between right and left duals. Since it is more convenient for our purposes, we shall use right duals, and hence consider evaluation and coevaluation maps as

$$e : V \otimes V^* \to \mathbf{k}, \qquad b : \mathbf{k} \to V^* \otimes V.$$

Let $f : X \otimes Y \to Y \otimes X$ be a map of finite dimensional vector spaces. It is custom to denote by $f^\flat : Y \otimes X^* \to X^* \otimes Y$ the morphism defined by

$$\langle (\mathrm{id} \otimes x), f^\flat(y \otimes \alpha)\rangle = \langle f(x \otimes y), (\alpha \otimes \mathrm{id})\rangle,$$

where we use the pairing $\langle (a \otimes b), (\beta \otimes \alpha)\rangle = \langle a, \alpha\rangle \langle b, \beta\rangle$.

Definition 1.3.1 ([Ly, Gu])**.** Let (V, c) be a braided pair such that V is finite dimensional. We say that c is *rigid* (or that (V, c) is an RBP) if $c^\flat$ is an isomorphism (it is proved in [LS] that this is equivalent to $(c^{-1})^\flat$ being an isomorphism).

When (V, c) is an RBP, we have isomorphisms

$$\begin{aligned} c_{V,V^*} &= (c^{-1})^\flat : V \otimes V^* \to V^* \otimes V, \\ c_{V^*,V} &= (c^\flat)^{-1} : V^* \otimes V \to V \otimes V^* \text{ and} \\ c_{V^*,V^*} &= c^* : V^* \otimes V^* \to V^* \otimes V^*, \end{aligned}$$

where we use the pairing above for the definition of c^*. Furthermore, in this case both V and V^* can be considered to be objects of one and the same braided category, and the evaluation and coevaluation maps $e : V \otimes V^* \to \mathbf{k}$ and $b : \mathbf{k} \to V^* \otimes V$ are maps in the category. Hence, the condition on c to be rigid is equivalent to the condition on V to lie in a rigid braided category.

Let (V, c) be a BP. Since c is a solution of the braid equation, the Artin braid group $\mathbb{B}_n$ acts on $V^{\otimes n}$ giving braidings

$$c_{V^{\otimes i}, V^{\otimes j}} : V^{\otimes i} \otimes V^{\otimes j} \to V^{\otimes j} \otimes V^{\otimes i}.$$

Let TV be the tensor space $TV = \oplus_n V^{\otimes n}$. This makes (TV, c) into a braided pair. If (V, c) is an RBP then c gives an action of $\mathbb{B}_n$ on $T^n(V \oplus V^*)$ and $(T(V \oplus V^*), c)$ becomes a BP.

Let (V, c) be a BP. We denote respectively by AV, CV the tensor algebra and the tensor coalgebra of V. As vector spaces, they coincide with TV. The multiplication components of AV are simply the identity maps $m_{i,j} = \mathrm{id} : A^iV \otimes A^jV \to A^{i+j}V$. Dually, the comultiplication components of CV are the identity maps $\Delta_{i,j} = \mathrm{id} : C^{i+j}V \to C^iV \otimes C^jV$. Both AV and CV are graded braided Hopf algebras. We denote the comultiplication components of AV and the multiplication components of CV by

$$\mathbf{S}_{i,j} : A^{i+j}V \to A^iV \otimes A^jV,$$
$$\mathbf{T}_{i,j} : C^iV \otimes C^jV \to C^{i+j}V,$$

(they are given by (i, j)-shuffles, we refer for instance to [AG] for the details). There exists a unique (graded) map of Hopf algebras $\mathbf{S} =: AV \to CV$ such that $\mathbf{S}|_V = \mathrm{id} : V \to V$. We denote by $\mathbf{S}^n$ the restriction of this map to A^nV.

Definition 1.3.2. Let (V, c) be a BP. We say that the image $\mathbf{S}(AV) \subseteq CV$ is a *Quantum Symmetric Algebra*, or QSA. It is a braided graded Hopf algebra and is determined by V. We denote it by $\mathfrak{B}(V)$. We denote also by $\mathfrak{B}^i(V)$ the homogeneous component of degree i, i.e. $\mathfrak{B}(V) = \oplus_i \mathfrak{B}^i(V)$. Notice that $\mathfrak{B}(V) \simeq TV/\ker(\mathbf{S})$.

Definition 1.3.3. If (V, c) is an RBP, then the quantum symmetric algebra generated by V will be called *Nichols algebra* and denoted also by $\mathfrak{B}(V)$. In this case, since V belongs to a rigid braided category, then V^* also does, and in particular it makes sense to consider $\mathfrak{B}(V^*)$, which is also a Nichols algebra.

Nichols algebras have some important properties that distinguish them from the general concept of QSA: they have a dual braided Hopf algebra (and in particular have non-zero spaces of integrals when they are finite dimensional). Moreover, finite dimensional Nichols algebras satisfy a Poincaré duality.

Let (V, c) be a BP. It is easy to see that the braiding commutes with the maps $\mathbf{S}^n$ (that is, $(\mathbf{S}^n \otimes \mathrm{id})c_{V,V^{\otimes n}} = c_{V,V^{\otimes n}}(\mathrm{id} \otimes \mathbf{S}^n))$, whence c gives a braiding $c_{\mathfrak{B}(V)} : \mathfrak{B}(V) \otimes \mathfrak{B}(V) \to \mathfrak{B}(V) \otimes \mathfrak{B}(V)$, and $(\mathfrak{B}(V), c_{\mathfrak{B}(V)})$ becomes a braided pair.

For a root of unity q, we denote by $N(q)$ its order if $q \neq 1$. If $q = 1$ then we define $N(q) = \infty$. We recall the definition of q-numbers: for $n, m \in \mathbb{N}$, $n \geq m$, define

$$(n)_q = \frac{q^n - 1}{q - 1} = 1 + q + q^2 + \cdots + q^{n-1}$$

$$(n)_q^! = \prod_{i=1}^{n} (i)_q \qquad \begin{pmatrix} n \\ m \end{pmatrix}_q = \frac{(n)_q^!}{(m)_q^! \, (n-m)_q^!}$$

Let H be a Hopf algebra with bijective antipode. We denote by ${}^H_H\mathcal{YD}$ the category of (left-left) Yetter–Drinfeld modules over H of arbitrary dimension. It is a braided category. The full subcategory of finite dimensional Yetter–Drinfeld modules is furthermore rigid. For an object $V \in {}^H_H\mathcal{YD}$, we shall denote by $\delta : V \to H \otimes V$ the H-coaction and by $\rightharpoonup: H \otimes V \to V$ the H-action. We sometimes denote the action by $h(v) := h \rightharpoonup v$.

2. First results on Nichols algebras

Definition 2.1. Let (V, c) be a BP, $V = \oplus_i V_i$. We say that this direct sum is a *decomposition of* (V, c) (and that (V, c) is *decomposable*) if $c|_{V_i \otimes V_j} : V_i \otimes V_j \to V_j \otimes V_i$. In this case we denote by b_{ij} the restriction $b_{ij} = c|_{V_i \otimes V_j}$. It is straightforward to see that if (V, c) is an RBP and $V = \oplus_i V_i$ is a decomposition of V as a BP, then this decomposition induces a decomposition of $V^* = \oplus_i V_i^*$ and taking the corresponding restrictions $c_i = b_{ii}$ of c then each (V_i, c_i) becomes an RBP.

If Γ is a finite group, $H = \mathbf{k}\Gamma$ and $V \in {}^H_H\mathcal{YD}$, then V can be decomposed as $V = \oplus_i M(g_i, \rho_i)$, where $\rho_i : \Gamma_{g_i} \to \operatorname{Aut}(Y_i)$ is an irreducible representation of the centralizer Γ_{g_i} of g_i (the definition of $M(g, \rho)$ is given in 2.15 below). However, sometimes it is possible to further decompose some of the summands, or to give a different decomposition. These decompositions usually fail to lie in ${}^H_H\mathcal{YD}$, but since (V, c) is an RBP any decomposition gives a direct sum of RBP's. For instance, it is proved in [AG, Prop. 3.1.11] that if V is 2-dimensional then it can be decomposed as a sum of two 1-dimensional subspaces. We say that (V, c) *comes from the abelian case* if V can be decomposed as a sum of 1-dimensional subspaces.

When $V = \oplus_i V_i$ is a decomposition of (V, c), then the knowledge of the QSA generated by the V_i's gives information on the QSA generated by V. The next result, which is a generalization of [AS1, Lemma 3.4 and Prop. 3.5] for the non-abelian case, gives a first relation between $\mathfrak{B}(V)$ and the $\mathfrak{B}(V_i)$'s.

Theorem 2.2. *Let (V,c) be a braided pair and suppose it is decomposable as $V = \oplus_{i=1}^n V_i$ such that $\mathfrak{B}(V_i)$ is finite dimensional $\forall i$. Then $\dim \mathfrak{B}(V) \geq \prod_{i=1}^n \dim \mathfrak{B}(V_i)$. Furthermore, the equality holds if and only if $b_{ij} = b_{ji}^{-1}$ $\forall i \neq j$.*

Proof. Let $\{v_i^1, \dots, v_i^{N_i}\}$ be a set of homogeneous vectors of $T(V_i)$ such that the set

$$\{\mathbf{S}^{d_i^1}(v_i^1), \dots, \mathbf{S}^{d_i^{N_i}}(v_i^{N_i})\}$$

is a basis of $\mathfrak{B}(V_i)$, where d_i^k is the degree of v_i^k. The set

$$\mathcal{B} = \{v_1^{k_1} \otimes \cdots \otimes v_n^{k_n} \in T(V_1) \otimes \cdots \otimes T(V_n) \mid 1 \leq k_i \leq N_i\}$$

is linearly independent in $T(V)$, and has $(\prod_i \dim \mathfrak{B}(V_i))$ elements. Note that the set

$$\{\mathbf{S}^{d_1^{k_1}} v_1^{k_1} \otimes \cdots \otimes \mathbf{S}^{d_n^{k_n}} v_n^{k_n} \mid 1 \leq k_i \leq N_i\}$$

is also linearly independent. It is enough for the first part to prove that $\mathcal{B}$ remains linearly independent after applying $\mathbf{S}$ to it. Then, suppose that a linear combination $\sum \lambda_{k_1,\dots,k_n} v_1^{k_1} \otimes \cdots \otimes v_n^{k_n}$ lies in $\ker \mathbf{S}$. Now, the space $T(V)$ can be decomposed in homogeneous components with respect of the V_i's, and the hypothesis made on c (namely, that c behaves well with the decomposition $V = \oplus_i V_i$) guarantees that c is a homogeneous morphism. Hence, the linear combination of above can be treated for each homogeneous component, and we consequently may suppose that there exist $d_1, \dots, d_n$ such that $\lambda_{k_1,\dots,k_n} = 0$ if $d_i^{k_i} \neq d_i$ for some i. Let $m = d_1 + \cdots + d_n$.

Now, by (2.8), for $m = i + j$ we have

$$(\mathbf{S}^i \otimes \mathbf{S}^j) \circ \mathbf{S}_{i,j} = \mathbf{S}^m = \mathbf{T}_{i,j} \circ (\mathbf{S}^i \otimes \mathbf{S}^j).$$

This implies that

$$\begin{aligned} 0 &= \mathbf{S}^m\big(\sum \lambda_{k_1,\dots,k_n} v_1^{k_1} \otimes \cdots \otimes v_n^{k_n}\big) \\ &= \mathbf{T}_{d_1,\dots,d_n}(\mathbf{S}^{d_1} \otimes \cdots \otimes \mathbf{S}^{d_n}) \left(\sum \lambda_{k_1,\dots,k_n} v_1^{k_1} \otimes \cdots \otimes v_n^{k_n}\right) \\ &= \sum_{x^{-1} \in Sh_{d_1,\dots,d_n}} s(x)(\mathbf{S}^{d_1} \otimes \cdots \otimes \mathbf{S}^{d_n}) \left(\sum \lambda_{k_1,\dots,k_n} v_1^{k_1} \otimes \cdots \otimes v_n^{k_n}\right), \end{aligned} \tag{2.3}$$

where $Sh_{d_1,\dots,d_n} \subset \mathbb{S}^m$ is the shuffle. Furthermore, the homogeneous component with degrees $(d_1, \dots, d_n)$ of CV can be decomposed as a direct sum taking all the possible orders for d_i tensorands of V_i. Explicitly, let

$$Z_{d_1,\dots,d_n} = \{f : \{1, \dots, m\} \to \{1, \dots, n\} \mid \#(f^{-1}(i)) = d_i \ \forall 1 \leq i \leq n\}.$$

The decomposition just stated is nothing but

$$(\text{the } (d_1,\dots,d_n) \text{ component of } CV) = \bigoplus_{f\in Z_{d_1,\dots,d_n}} V_{f(1)}\otimes V_{f(2)}\otimes\cdots\otimes V_{f(m)} = \bigoplus_{f\in Z_{d_1,\dots,d_n}} V_f.$$

It is clear that there exists a bijection $\gamma : (Sh_{d_1,\dots,d_n})^{-1} \to Z_{d_1,\dots,d_n}$ such that for $x \in (Sh_{d_1,\dots,d_n})^{-1}$ the image of $s(x)|_{V_1^{\otimes d_1}\otimes\cdots\otimes V_n^{\otimes d_n}}$ lies in $V_{\gamma(x)}$. Hence (2.3) implies, for each $x \in (Sh_{d_1,\dots,d_n})^{-1}$, that

$$0 = s(x)(\mathbf{S}^{d_1}\otimes\cdots\otimes\mathbf{S}^{d_n})\left(\sum \lambda_{k_1,\dots,k_n} v_1^{k_1}\otimes\cdots\otimes v_n^{k_n}\right),$$

but since $s(x)$ is an isomorphism for each $x\in\mathbb{S}_n$, this implies that

$$0 = (\mathbf{S}^{d_1}\otimes\cdots\otimes\mathbf{S}^{d_n})\left(\sum \lambda_{k_1,\dots,k_n} v_1^{k_1}\otimes\cdots\otimes v_n^{k_n}\right) = \sum \lambda_{k_1,\dots,k_n}(\mathbf{S}^{d_1}v_1^{k_1}\otimes\cdots\otimes\mathbf{S}^{d_n}v_n^{k_n}),$$

which in turn implies that $\lambda_{k_1,\dots,k_n} = 0$ $\forall k_1,\dots,k_n$. This proves the first part.

For the second part, suppose there exist i, j, $i\neq j$ such that $b_{ji}b_{ij}\neq \mathrm{id}$, and let $v\in V_i$, $w\in V_j$ such that $b_{ji}b_{ij}(v\otimes w)\neq (v\otimes w)$. Consider the element $z\in T(V)$ given by $z = (\mathrm{id} - b_{ij})(v\otimes w)$. Since the linear span of the set $\mathbf{S}(\mathcal{B}) = \{\mathbf{S}(y), y\in\mathcal{B}\}$ is a subspace of $\mathfrak{B}(V)$ with dimension $\prod_l \dim\mathfrak{B}(V_l)$, it is sufficient to prove that $\mathbf{S}(z)$ does not lie in this linear span. Note that since $\deg z = 2$, $\mathbf{S}(z) = (\mathrm{id} + c)(z)$. Suppose that

$$\mathbf{S}(z) = \mathbf{S}\left(\sum \lambda_{k_1,\dots,k_n} v_1^{k_1}\otimes\cdots\otimes v_n^{k_n}\right).$$

Looking at the homogeneous components, we must have $\lambda_{k_1,\dots,k_n} = 0$ if $(d_1^{k_1},\dots,d_n^{k_n})\neq e_i + e_j$, where $e_l = (0,\dots,0,1,0,\dots,0)$ with the 1 in the l-coordinate. In other words, if $i<j$ there exist $u_1,\dots,u_s\in V_i$, $u'_1,\dots,u'_s\in V_j$ and $\lambda_1,\dots,\lambda_s\in\mathbf{k}$ such that

$$\mathbf{S}(z) = \mathbf{S}(\sum_t \lambda_t u_t\otimes u'_t)$$

(if $i>j$ we have $\mathbf{S}(z) = \mathbf{S}(\sum_t \lambda_t u'_t\otimes u_t)$ and it is analogous). Now, since $z = (1-c)(v\otimes w)$ and $\mathbf{S}(z) = (1+c)(z)$, we have

$$(1-c^2)(v\otimes w) = (1+c)(\sum_t \lambda_t u_t\otimes u'_t),$$

but the component in $V_j\otimes V_i$ in the left hand side vanish, and hence we have $c(\sum_t \lambda_t u_t\otimes u'_t) = 0$. Since c is an isomorphism, we must have $\sum_t \lambda_t u_t\otimes u'_t = 0$, but this implies that the $V_i\otimes V_j$ component in the right hand side vanish, whence $c^2(v\otimes w) = (v\otimes w)$, a contradiction.

It only remains to prove that if $b_{ij}b_{ji} = \mathrm{id}$ $\forall i\neq j$ then $\mathbf{S}(\mathcal{B})$ is a basis of $\mathfrak{B}(V)$. This is the same as saying that $\mathcal{B}$ generates $T(V)$ modulo $\ker\mathbf{S}$. Let $\{w_i^1,\dots,w_i^{M_i}\}$ be a basis of V_i. Let

$$\tilde{\mathcal{B}} = \{w_{a_1}^{r_1}\otimes\cdots\otimes w_{a_m}^{r_m} \mid m\in\mathbb{N},\ 1\leq r_t\leq M_{a_t} \text{ and } a_1\leq a_2\leq\ldots\leq a_m\}.$$

Since, modulo $\ker(\mathbf{S})$, the elements of $\tilde{\mathcal{B}}$ are linear combinations of the elements of $\mathcal{B}$, it remains to prove that $\tilde{\mathcal{B}}$ generates $T(V)$ modulo $\ker(\mathbf{S})$. To see this, it suffices to prove that if $i < j$ and $1 \le r_i \le M_i$, $1 \le r_j \le M_j$, then $w_j^{r_j} \otimes w_i^{r_i}$ can be expressed in terms of elements in $\tilde{\mathcal{B}}$. Let $z = (1-c)(w_j^{r_j} \otimes w_i^{r_i})$. Since $b_{ij}b_{ji} = \mathrm{id}$, we have $\mathbf{S}(z) = (1+c)(z) = 0$, which gives the relation

$$w_j^{r_j} \otimes w_i^{r_i} = b_{ji}(w_j^{r_j} \otimes w_i^{r_i}) \bmod \ker(\mathbf{S}).$$

Now, $b_{ji}(w_j^{r_j} \otimes w_i^{r_i}) \in V_i \otimes V_j$, and it can be written as a linear combination of elements in $\tilde{\mathcal{B}}$. $\square$

From now on, we concentrate on Nichols algebras. Let (V, c) be an RBP. Since V and V^* belong to a braided category $\mathcal{C}$, we have that $V^{\otimes n}$ and $(V^*)^{\otimes m}$ also belong to $\mathcal{C}$, and it is easy to see that the map $\mathbf{S} : AV \to CV$ is a map in the category, whence both $\mathfrak{B}(V)$ and $\mathfrak{B}(V^*)$ lie in $\mathcal{C}$, and in particular they lie in one and the same braided category.

We shall use the bilinear form $(|) : T^nV \otimes T^nV^* \to \mathbf{k}$ given by

$$(z_1 z_2 \cdots z_n | w_1 w_2 \cdots w_n) = \prod_{1 \le i \le n} \langle z_i, w_{n+1-i}\rangle = \langle z_1, w_n\rangle \cdots \langle z_n, w_1\rangle, \tag{2.4}$$

where $z_1, z_2, \cdots, z_n \in T^n(V)$, $w_1, w_2, \cdots, w_n \in T^n(V^*)$ and $\langle\cdot,\cdot\rangle$ is the evaluation map. We define also $(z|w) = 0$ if $z \in T^n(V)$, $w \in T^m(V^*)$ and $n \ne m$. It is easy to see that c_{V^*,V^*} is the transpose of $c_{V,V}$ when one identifies $(V \otimes V)^* \simeq V^* \otimes V^*$ with this form. Furthermore, as proved in [AG, Prop. 3.2.20], this bilinear form satisfies for $z \in T^n(V)$, $w \in T^n(V^*)$,

$$(\mathbf{S}^n z|w) = (z|\mathbf{S}^n w), \tag{2.5}$$

from where $\mathbf{S}^n : T^nV^* \to T^nV^*$ is the transpose of $\mathbf{S}^n : T^nV \to T^nV$ with respect to the pairing $(|)$. We thus have proved:

Lemma 2.6. *Let (V, c) be an RBP. Then $\mathfrak{B}^n(V^*) \simeq (\mathfrak{B}^n(V))^*$ for all $n \ge 0$. If $\mathfrak{B}(V)$ is finite dimensional then $\mathfrak{B}(V^*) \simeq (\mathfrak{B}(V))^*$ and $(\mathfrak{B}(V), c_{\mathfrak{B}(V),\mathfrak{B}(V)})$ is an RBP.* $\square$

Definition 2.7. Let (V, c) be an RBP. For $y \in V^*$, we denote by ∂_y the operator

$$\partial_y = (\mathrm{id} \otimes y) \circ \Delta^{i-1,1} : \mathfrak{B}^i(V) \to \mathfrak{B}^{i-1}(V).$$

If $B = \{x_1, \dots, x_n\}$ is a basis of V, let $\{\partial_1, \dots, \partial_n\}$ be the basis of V^* dual to B. We denote also by ∂_j, $j = 1, \dots, n$ the operator ∂_{∂_j}. We warn that for the case $V \in {}^H_H\mathcal{Y}D$, usually these are not morphisms in ${}^H_H\mathcal{Y}D$.

Because of the coassociativity of AV, we have for $i_1, i_2, i_3 \in \mathbb{N}$

$$(\mathbf{S}_{i_1,i_2} \otimes \mathrm{id})\mathbf{S}_{i_1+i_2,i_3} = \mathbf{S}_{i_1,i_2,i_3} = (\mathrm{id} \otimes \mathbf{S}_{i_2,i_3})\mathbf{S}_{i_1,i_2+i_3}, \tag{2.8}$$

which has the following consequence:

Proposition 2.9. *Let (V, c) be an RBP. Consider the map $\partial : V^* \to \operatorname{End}\mathfrak{B}(V)$ given in 2.7, and denote by $\bar{\partial} : T(V^*) \to (\operatorname{End}\mathfrak{B}(V))^{\mathrm{op}}$ the (unique) algebra map extending ∂ to the tensor algebra. Then $\bar{\partial}$ factors through $\mathfrak{B}(V^*)$ as*

$$\bar{\partial} = T(V^*) \xrightarrow{\pi} \mathfrak{B}(V^*) \xhookrightarrow{\iota} (\operatorname{End}\mathfrak{B}(V))^{\mathrm{op}}.$$

Proof. We use the bilinear form $(|)$ of 2.4. Notice that if $z \in T^n(V)$, $z' \in T^m(V)$, $w \in T^n(V^*)$, $w' \in T^m(V^*)$, then

$$(z \cdot z'|w' \cdot w) = (z'|w')(z|w). \tag{2.10}$$

For $w \in T^n(V^*)$, $z \in T^m(V)$ we take the pairing $z \otimes w \mapsto (\mathbf{S}^n z|w)$. By definition this pairing gives a functional $w \in (\mathfrak{B}(V))^*$, and we define the operator $h(w) \in \operatorname{End}\mathfrak{B}(V)$ by $h(w)(x) = w \rightharpoonup x$, i.e. $h(w)(x) = x_{(1)}w(x_{(2)})$. In other terms, if $z \in T^m(V)$ then $\mathbf{S}(z) \in \mathfrak{B}^m(V)$ and we have, using (2.5),

$$h(w)(\mathbf{S}(z)) = \mathbf{S}(z_{(1)})w(\mathbf{S}(z_{(2)})) = (\mathbf{S}(z_{(1)}))(z_{(2)}|\mathbf{S}^n w) = (\mathbf{S}^{m-n} \otimes (\,\cdot\,|\mathbf{S}^n w))\mathbf{S}_{m-n,n}(z). \tag{2.11}$$

We prove now that $h = \bar{\partial}$. In degree 1 this is just the definition of h, so it is enough to prove that h is multiplicative. Let $w_i \in T^{n_i}(V^*)$ for $i = 1, 2$ and $z \in T^{n_1+n_2+n_3}(V)$. Then

$$\begin{aligned}
(h(w_1) \cdot_{\mathrm{op}} h(w_2))\,(pz) &= h(w_2)(pz_{(1)})w_1(z_{(2)}) = pz_{(1)}w_2(z_{(2)})w_1(z_{(3)}) \\
&= \mathbf{S}^{n_3}(z_{(1)})(z_{(2)}|\mathbf{S}^{n_2}w_2)(z_{(3)}|\mathbf{S}^{n_1}w_1) \text{ by (2.11)} \\
&= (\mathbf{S}^{n_3} \otimes w_2 \otimes w_1)(\mathrm{id} \otimes \mathbf{S}^{n_2} \otimes \mathbf{S}^{n_1})(\mathbf{S}_{n_3,n_2,n_1}(z)) \\
&= (\mathbf{S}^{n_3} \otimes w_1 \cdot w_2)(\mathrm{id} \otimes \mathbf{S}^{n_2+n_1})(\mathbf{S}_{n_3,n_2+n_1}(z)) \text{ by (2.10)} \\
&= (\mathbf{S}^{n_3} \otimes \mathbf{S}^{n_2+n_1}(w_1 \cdot w_2))(\mathbf{S}_{n_3,n_2+n_1}z) \\
&= h(w_1 \cdot w_2)(pz) \text{ by (2.11)}.
\end{aligned}$$

The factorizability through $\mathfrak{B}(V^*)$ is now a consequence of (2.11). The injectivity of ι follows immediately from the non-degeneracy of $(|)$. $\square$

As a first consequence of this result, we have

Corollary 2.12. *Let $\partial_0 \in V^*$ be such that $c(\partial_0 \otimes \partial_0) = q\partial_0 \otimes \partial_0$, where $q \neq 1$ is a root of unity of order N. Then $(\partial_0)^N = 0$ as an operator of $\mathfrak{B}(V)$.* □

Definition 2.13. We shall denote by $[,]$ the action given by $\bar{\partial}$, i.e. for $\mathbf{S}^n z \in \mathfrak{B}^n(V)$, $\mathbf{S}^m w \in \mathfrak{B}^m(V^*)$ $(n \geq m)$,

$$[\mathbf{S}^n z, \mathbf{S}^m w] = \mathbf{S}^{n-m}(z_{(1)})(\mathbf{S}^m z_{(2)}|w) \in \mathfrak{B}^{n-m}(V).$$

We characterize now the RBP's (V, c) arising in Yetter–Drinfeld categories over group algebras. The following remark is due to the referee.

Remark 2.14. Let V be a finite dimensional module in ${}^{\mathbf{k}\Gamma}_{\mathbf{k}\Gamma}\mathcal{YD}$, where Γ is a group. As a $\mathbf{k}\Gamma$-comodule, V can be decomposed as $V = \oplus_{g\in\Gamma} V^g$, where $\delta(x) = g \otimes x$ $\forall x \in V^g$. Then, for $x \in V^g$, $y \in V$ we have $c(x \otimes y) = g \rightharpoonup y \otimes x \in V \otimes x$. Thus V has a basis $\{x_1, \dots, x_n\}$ such that $c(x_i \otimes V) = V \otimes x_i$. Conversely, let (V, c) be a BP with a basis $\{x_1, \dots, x_n\}$ such that $c(x_i \otimes V) = V \otimes x_i$. Let $g_i \in \mathrm{Aut}(V)$ be defined by

$$c(x_i \otimes y) = g_i(y) \otimes x_i,$$

and let Γ be the subgroup of $\mathrm{Aut}(V)$ generated by $\{g_1, \dots, g_n\}$. Then V is an object of ${}^{\mathbf{k}\Gamma}_{\mathbf{k}\Gamma}\mathcal{YD}$. In particular, it is an RBP.

Proof. The comodule structure is determined by $\delta(x_i) = g_i \otimes x_i$. The module structure is given by $g_i \rightharpoonup y = g_i(y)$. We must prove the YD-compatibility condition between $\rightharpoonup$ and δ, which reads as $\delta(g \rightharpoonup y) = gy_{(-1)}g^{-1} \otimes gy_{(0)}$, with $g \in \Gamma$, $\delta(y) = y_{(-1)} \otimes y_{(0)}$. It is sufficient to prove it for $y = x_i$ and $g = g_j$, which is equivalent to prove that $g_j(x_i) \in V^{g_j g_i g_j^{-1}}$. Let $g_j x_i = \sum_k c_k x_k$. The braid equation applied to $x_j \otimes x_i \otimes y$ implies that

$$\sum_k g_j g_i(y) \otimes c_k x_k \otimes x_j = \sum_k g_k g_j(y) \otimes c_k x_k \otimes x_j,$$

which tells that $c_k = 0$ if $g_j g_i \neq g_k g_j$. □

Remark 2.15. Let $V \in {}^{\mathbf{k}\Gamma}_{\mathbf{k}\Gamma}\mathcal{YD}$, Γ a finite group. Then $V = \oplus_i M(g_i, \rho_i)$, where $\rho_i : \Gamma_{g_i} \to \mathrm{Aut}(Y_i)$ is an irreducible representation of Γ_{g_i}, and

$$M(g_i, \rho_i) = \mathrm{Ind}_{\Gamma_{g_i}}^{\Gamma} \rho_i = \mathbf{k}\Gamma \otimes_{\mathbf{k}\Gamma_{g_i}} Y_i,$$

with comodule structure $\delta(h \otimes y) = hg_ih^{-1} \otimes (h \otimes y)$. Let $\{x_1^i, \dots, x_{r_i}^i\}$ be a basis of Y_i and let $\{h_1^i, \dots, h_{s_i}^i\}$ be a set of representatives of left coclasses in Γ/Γ_{g_i}. Then $M(g_i, \rho_i)$ has basis $\{z_{jl}^i = h_j^i \otimes x_l^i,\ 1 \leq j \leq s_i,\ 1 \leq l \leq r_i\}$, and consequently $\{z_{jl}^i\}_{i,j,l}$ is a basis of V. Let $\{\partial_{jl}^i\}_{i,j,l}$ be the dual basis. Let $t^i_j = h^i_j g_i (h^i_j)^{-1}$ (thus, the conjugacy class of g_i is $\{t^i_1, \dots, t^i_{s_i}\}$), and note that $\delta(z^i_{jl}) = t^i_j \otimes z^i_{jl}$. Let $W'^i_{jl} = \operatorname{span}\{z^{i_2}_{j_2 l_2} \mid (i,j,l) \neq (i_2, j_2, l_2)\}$. Then W'^i_{jl} is a $\mathbf{k}\Gamma$-subcomodule of V. For further use, we compute:

$$(\mathrm{id} \otimes \partial^{i_1}_{j_1 l_1}) c(z^{i_2}_{j_2 l_2} \otimes z^{i_3}_{j_3 l_3}) = (\mathrm{id} \otimes \partial^{i_1}_{j_1 l_1})(t^{i_2}_{j_2} \rightharpoonup z^{i_3}_{j_3 l_3} \otimes z^{i_2}_{j_2 l_2}) = \delta_{i_1, i_2} \delta_{j_1, j_2} \delta_{l_1, l_2} (t^{i_1}_{j_1} \rightharpoonup z^{i_3}_{j_3 l_3}).$$

Moreover,

$$(\partial^{i_1}_{j_1 l_1} \otimes \mathrm{id}) c(z^{i_1}_{j_1 l_1} \otimes z^{i_2}_{j_2 l_2}) = \partial^{i_1}_{j_1 l_1}(t^{i_1}_{j_1} \rightharpoonup z^{i_2}_{j_2 l_2}) z^{i_1}_{j_1 l_1} = \delta_{i_1, i_2} \partial^{i_1}_{j_1 l_1}(t^{i_1}_{j_1} \rightharpoonup z^{i_1}_{j_2 l_2}) z^{i_1}_{j_1 l_1}. \tag{2.16}$$

Now, we have $\delta(t^{i_1}_{j_1} \rightharpoonup z^{i_1}_{j_2 l_2}) = (t^{i_1}_{j_1} t^{i_1}_{j_2} (t^{i_1}_{j_1})^{-1}) \otimes t^{i_1}_{j_1} \rightharpoonup z^{i_1}_{j_2 l_2}$, whence (2.16) vanishes if $t^{i_1}_{j_1} t^{i_1}_{j_2} (t^{i_1}_{j_1})^{-1} \neq t^{i_1}_{j_1}$, i.e. if $t^{i_1}_{j_2} \neq t^{i_1}_{j_1}$, but for the definition of t^i_j and h^i_j this is equivalent to $j_1 \neq j_2$. Moreover, for $y \in Y_{i_1}$, $t^{i_1}_{j_1} \rightharpoonup (h^{i_1}_{j_1} \otimes y) = h^{i_1}_{j_1} g_{i_1} (h^{i_1}_{j_1})^{-1} h^{i_1}_{j_1} \otimes y = h^{i_1}_{j_1} \otimes \rho_{i_1}(g_{i_1})(y) = q_{i_1} h^{i_1}_{j_1} \otimes y$, from where (2.16) vanishes if $l_1 \neq l_2$. Then, we have proved

- $c(z^i_{jl} \otimes z^i_{jl}) = q_i z^i_{jl} \otimes z^i_{jl}$,
- $c(z^i_{jl} \otimes W'^i_{jl}) = W'^i_{jl} \otimes z^i_{jl}$,
- $\delta(W'^i_{jl}) \subseteq \mathbf{k}\Gamma \otimes W'^i_{jl}$.

We close this section with a useful bound for dimension of Nichols algebras:

Lemma 2.17. *Let $V \in {}^{\mathbf{k}\Gamma}_{\mathbf{k}\Gamma}\mathcal{YD}$, Γ finite, V finite dimensional. Then by 2.15, we have a basis $\{x_1, \dots, x_n\}$ of V such that $c(x_i \otimes V) = V \otimes x_i$ and $c(x_i \otimes x_i) = q_i x_i \otimes x_i$, q_i a root of unity. Let $N_i = N(q_i)$. Then $\prod_i N_i \leq \dim(\mathfrak{B}(V))$.*

Proof. Let $\{\partial_1, \dots, \partial_n\}$ be the basis of V^* dual to $\{x_1, \dots, x_n\}$. Note first that $x_i^{N_i - 1} \neq 0$ because $\mathfrak{B}(\mathbf{k}x_i) \hookrightarrow \mathfrak{B}(V)$, or simply by direct computation, since $\partial_i(x_i^j) = (j)_{q_i} x_i^{j-1}$ and thence $(\partial_i)^j(x_i^j) = (j)^!_{q_i}$, which is nonzero if $j < N_i$ (we use the Leibniz rule to make the computations, see 3.5 below). We prove now that the set $\{x_1^{j_1} \cdots x_n^{j_n} \mid 0 \leq j_i < N_i\}$ is linearly independent. We do it by induction: suppose that the subset with $j_m = 0$ for $m \geq m_0$ is l.i. and consider a linear combination

$$\sum_{j_1, \dots, j_{m_0}} \alpha_{j_1, \dots, j_{m_0}} x_1^{j_1} \cdots x_{m_0}^{j_{m_0}} = 0.$$

Applying $(\partial_{m_0})^{N_{m_0} - 1}$ we get

$$\sum_{j_1, \dots, j_{m_0 - 1}} \alpha_{j_1, \dots, j_{m_0 - 1}, N_{m_0} - 1} (N_{m_0} - 1)^!_{q_{m_0}} x_1^{j_1} \cdots x_{m_0 - 1}^{j_{m_0 - 1}} = 0,$$

from where the coefficients $\alpha_{j_1,\dots,j_{m_0-1},N_{m_0}-1}$ vanish. We can apply then $(\partial_{m_0})^{N_{m_0}-2}$, and get that the coefficients $\alpha_{j_1,\dots,j_{m_0-1},N_{m_0}-2}$ vanish. Proceeding in this way, we see that all the coefficients $\alpha_{j_1,\dots,j_{m_0}} = 0$, and the inductive thesis follows. □

Corollary 2.18. *If $V = \oplus_j M(g_j,\rho_j) \in {}^{\mathbf{k}\Gamma}_{\mathbf{k}\Gamma}\mathcal{YD}$ (Γ a finite group) and $d_j = \dim M(g_j,\rho_j)$, $q_j = \rho_j(g_j)$, $N_j = N(q_j)$, then $\prod_j N_j^{d_j} \le \dim(\mathfrak{B}(V))$.*

3. Main result

Definition 3.1. We say that a finite dimensional braided Hopf algebra (R,c) is *rigid* if R is a Hopf algebra in a rigid braided category. This is equivalent to (R,c) being an RBP and the structure morphisms of R commuting with the braiding. In particular replacing P by R and by R^* we have

$$c_{P,R}(\mathrm{id}\otimes m_R) = (m_R\otimes \mathrm{id})c_{P,(R\otimes R)} : P\otimes R\otimes R \to R\otimes P,$$
$$(c_{R,P})^{-1}(\mathrm{id}\otimes m_R) = (m_R\otimes \mathrm{id})(c_{(R\otimes R),P})^{-1} : P\otimes R\otimes R \to R\otimes P,$$

and analogous equalities for $\Delta, u, \varepsilon, \mathcal{S}$.

For rigid braided Hopf algebras, most of the "classic" results on finite dimensional Hopf algebras can be stated *mutatis mutandis* in a braided sense, and we refer to [T2] for this. We shall use the existence of a non-zero integral (in R and R^*) and the non-degenerate bilinear form given by it.

Definition 3.2. Let (V,c) be an RBP such that $\mathfrak{B}(V)$ is finite dimensional. We have seen that $\mathfrak{B}(V^*) \simeq (\mathfrak{B}(V))^*$ and that $(\mathfrak{B}(V), c_{\mathfrak{B}(V)})$ is an RBP. It is straightforward to see by the definitions of the structure morphism in $\mathfrak{B}(V)$ that it is a rigid braided Hopf algebra. Then $\mathfrak{B}(V)$ has a one-dimensional space of integrals, which is easily seen to be homogeneous. We denote by $\mathrm{top}(V)$ the degree of the integral of $\mathfrak{B}(V)$. We further denote by $\Lambda_{\mathfrak{B}(V)}$ a nonzero integral of $\mathfrak{B}(V)$.

The non-degenerate bilinear form gives the Poincaré duality found by Nichols (see e.g. [AG, Prop. 3.2.2]), namely, that $\dim \mathfrak{B}^i(V) = \dim \mathfrak{B}^{\mathrm{top}(V)-i}(V)$; in particular, $\dim \mathfrak{B}^{\mathrm{top}(V)}(V) = 1$ and $\mathfrak{B}^{\mathrm{top}(V)+i}(V) = 0\ \forall i>0$.

The following lemma, which we have mostly proved, is an addendum to this duality

Lemma 3.3. *Let (V,c) be an RBP.*

1. *$\mathfrak{B}^n(V^*) \simeq (\mathfrak{B}^n(V))^*$ via the form $[,]$ of 2.13.*
2. *If $\mathfrak{B}(V)$ is finite dimensional and $n \le \mathrm{top}(V)$, then $[\Lambda_{\mathfrak{B}(V)}, \mathfrak{B}^{\mathrm{top}(V)-n}(V^*)] = \mathfrak{B}^n(V)$.*

Proof. 1. It is part of the content of 2.6, once we see the definition of $[,]$.

2. If $D \in \mathfrak{B}^{\mathrm{top}(V)-n}(V^*)$ is such that $[\Lambda_{\mathfrak{B}(V)}, D] = 0$, we can take $D' \in \mathfrak{B}^n(V^*)$ such that $\Lambda_{\mathfrak{B}(V^*)} = DD'$, and then $[\Lambda_{\mathfrak{B}(V)}, \Lambda_{\mathfrak{B}(V^*)}] = [[\Lambda_{\mathfrak{B}(V)}, D], D'] = 0$, which contradicts 1. Then we have a monomorphism $\mathfrak{B}^{\mathrm{top}(V)-n}(V^*) \hookrightarrow \mathfrak{B}^n(V)$. Since by 1 and the Poincaré duality both spaces have the same dimension, we are done.

□

Definition 3.4. Let (V, c) be an RBP and consider the map $\iota : \mathfrak{B}(V^*) \to \operatorname{End}\mathfrak{B}(V)^{\mathrm{op}}$ of 2.9. Given $x \in \mathfrak{B}(V)$, we denote also by x the map in $\operatorname{End}\mathfrak{B}(V)^{\mathrm{op}}$ given by right multiplication by x. We have hence $\mathfrak{B}(V)$ and $\mathfrak{B}(V^*)$ acting on $\mathfrak{B}(V)$. We define the *quantum differential operators algebra* $\mathcal{A}V$ as the subalgebra of $\operatorname{End}\mathfrak{B}(V)^{\mathrm{op}}$ generated by $\mathfrak{B}(V)$ and $\mathfrak{B}(V^*)$.

When $V \in {}^{\mathbf{k}\Gamma}_{\mathbf{k}\Gamma}\mathcal{YD}$, it can be given a nice basis of $\mathcal{A}V$.

Lemma 3.5. *Let $V \in {}^{\mathbf{k}\Gamma}_{\mathbf{k}\Gamma}\mathcal{YD}$ be finite dimensional.*

1. *Let $\{x_1, \dots, x_n\}$ be a basis of V such that $\delta(x_i) = g_i \otimes x_i$. Let $\{\partial_1, \dots, \partial_n\}$ be the basis of V^* dual to $\{x_1, \dots, x_n\}$. Then $\mathcal{A}V$ can be presented with generators $\{\partial_1, \dots, \partial_n, x_1, \dots, x_n\}$ and relations*
   - $\ker \mathbf{S}^m : TV \to \mathfrak{B}(V)$, *$m \geq 0$, i.e. the relations in $\mathfrak{B}(V)$,*
   - $\ker \mathbf{S}^m : TV^* \to \mathfrak{B}(V^*)$, *$m \geq 0$, i.e. the relations in $\mathfrak{B}(V^*)$, and*
   - $x_i\partial_j = \delta_{ij} + \partial_j g_j(x_i)$ *for $1 \leq i, j \leq n$.*

   Furthermore, for $m \geq 0$ take $\{z_1^m, \dots, z_{d_m}^m\}$ a basis of $\mathfrak{B}^m(V)$, and let $\{w_1^m, \dots, w_{d_m}^m\}$ be the dual basis of $\mathfrak{B}^m(V^*)$ (given by the duality in 3.3). Then the set

$$\{w_k^i z_l^j \mid i, j \geq 0,\ 1 \leq k \leq d_i,\ 1 \leq l \leq d_j\}$$

   is a basis of $\mathcal{A}V$.

2. *Suppose $W \subset V$ is a $\mathbf{k}\Gamma$-subcomodule which is Γ'-stable, where $\Gamma' \subset \Gamma$ is the smallest subgroup such that $\delta(W) \subseteq \mathbf{k}\Gamma' \otimes W$. Then $c(W \otimes W) = W \otimes W$, the pair $(W, c_W = c_V|_{W\otimes W})$ is an RBP and it makes sense to consider $\mathfrak{B}(W)$. Suppose furthermore that $V = W \oplus W'$, where W' is a $\mathbf{k}\Gamma$-subcomodule and a $\mathbf{k}\Gamma'$-submodule. Let $W^* \hookrightarrow V^*$ be the map given by the identification $W^* = (W')^\perp$. Then there is a monomorphism of algebras*

$$\mathcal{A}W \hookrightarrow \mathcal{A}V,$$

   induced by $W \hookrightarrow V$ and $W^* \hookrightarrow V^*$.

Before giving the proof, we note that if Γ is finite, 2.15 tells that the conditions of the second part are fulfilled taking, for i,j,l fixed, $W=\operatorname{span}\{z^i_{jl}\}$ and $W'=W'^i_{jl}$.

Proof. 1. The relations in $\mathfrak{B}(V)$ hold in $\mathcal{A}V$ because it acts by the regular representation. The relations in $\mathfrak{B}(V^*)$ hold in $\mathcal{A}V$ because of 2.9. Of course, AV, CV and $\mathfrak{B}(V)$ lie in ${}^{\mathbf{k}\Gamma}_{\mathbf{k}\Gamma}\mathcal{YD}$, whence we may consider g_i acting on $\operatorname{Aut}(\mathfrak{B}(V))$. It is immediate to see from the definition that the derivations ∂_i verify the Leibniz rule

$$\partial_i(ab)=\partial_i(a)g_i(b)+a\partial_i(b),$$

which implies at once the last set of relations taking $b=x_j$.

Thus, if B is the algebra defined with generators $\{\partial_1,\dots,\partial_n,x_1,\dots,x_n\}$ and the stated relations, we have a surjection $B\twoheadrightarrow\mathcal{A}V$. Moreover, the last set of relations implies that any monomial in B can be written in the form $\sum_r a_rb_r$, where the a_r's are generated by the ∂_i's and the b_r's are generated by the x_i's. Now, the first and second set of relations imply that we can choose a_r and b_r to be respectively in the sets $\{w^i_k\}$ and $\{z^j_l\}$. The last thing to be proved is the linear independence of the set $\{w^i_kz^j_l\}$. Since $\mathcal{A}V$ is generated by $\{x_i\}$ and $\{\partial_i\}$, which act on $\mathfrak{B}(V)$ in a graded way, then $\mathcal{A}V$ is a graded algebra with degrees given by $\deg(x_i)=1$ and $\deg(\partial_i)=-1$, and then it is enough to prove the linear independence of the subsets with the same degree. Let then

$$T=\sum_{\substack{-i+j=n\\k,l}}\alpha_{ijkl}w^i_kz^j_l=0,$$

and suppose some of the $\alpha_{ijkl}\neq0$. We take $m=\min\{i\mid\exists j,k,l\text{ s.t. }\alpha_{ijkl}\neq0\}$ and let

$$\tilde{T}=\sum_{\substack{j=n+m,\,i=m\\k,l}}\alpha_{ijkl}w^i_kz^j_l.$$

Since T and $T-\tilde{T}$ act trivially on $\mathfrak{B}^m(V)$ then $\tilde{T}$ also does. Thus, for any k' we have

$$\begin{aligned}0=\tilde{T}(z^m_{k'})&=[z^m_{k'},\sum_k w^m_k]\sum_l\alpha_{m,n+m,k,l}z^{n+m}_l\\&=\sum_l\alpha_{m,n+m,k',l}z^{n+m}_l,\end{aligned}$$

but then the linear independence of the set $\{z^{n+m}_l\}_l$ implies that $\alpha_{m,n+m,k,l}=0\ \forall k,l$, which contradicts the definition of m.

2. The pair (W, c_W) is an RBP thanks to 2.14. Let $\{x_1, \dots, x_m\}$ be a basis of W such that $\delta(x_i) = g_i \otimes x_i$. We consider $\{\partial_1, \dots, \partial_m\}$ the dual basis of W^* and extend it by $\partial_i|_{W'} = 0$ (i.e., $W^* \hookrightarrow V^*$ as $W^* = (W')^\perp$). The condition on W' to be a $\mathbf{k}\Gamma$-subcomodule implies that in $\mathcal{A}V$ we have $x_i \partial_j = \delta_{ij} + \partial_j g_j(x_i)$ for $1 \le i, j \le m$. The condition on W' to be a $\mathbf{k}\Gamma'$-submodule implies that $c_{V^*}(W^* \otimes W^*) = W^* \otimes W^*$, and it is easy to see that the restriction $c_{V^*}|_{W^* \otimes W^*}$ coincides with c_{W^*}, the braiding given by considering W^* as an object of ${}^{\mathbf{k}\Gamma'}_{\mathbf{k}\Gamma'}\mathcal{YD}$. Thus,

$$\ker(\mathbf{S}^n : (W^*)^{\otimes n} \to (W^*)^{\otimes n}) = \ker(\mathbf{S}^n : (V^*)^{\otimes n} \to (V^*)^{\otimes n}) \cap (W^*)^{\otimes n}.$$

Since clearly

$$\ker(\mathbf{S}^n : W^{\otimes n} \to W^{\otimes n}) = \ker(\mathbf{S}^n : V^{\otimes n} \to V^{\otimes n}) \cap W^{\otimes n},$$

by the first part this gives a well defined morphism of algebras $\mathcal{A}W \to \mathcal{A}V$. We must prove that this map is injective, but this is also a consequence of the first part, for if we take $\{z_i\}$ a basis of $\mathfrak{B}(W)$ and $\{w_j\}$ a basis of $\mathfrak{B}(W^*)$ then the set $\{w_j z_i\}$ is a basis of $\mathcal{A}W$, and it is linearly independent in $\mathcal{A}V$ (completing the bases to bases of $\mathfrak{B}(V)$ and $\mathfrak{B}(V^*)$). The assertion follows. $\square$

Example 3.6. If $V = \mathbf{k}x$ and $c(x \otimes x) = qx \otimes x$, let $\partial \in V^*$ such that $\partial(x) = 1$. Then $\mathcal{A}V$ has basis $\{\partial^i x^j \mid 0 \le i, j < N(q)\}$, and it can be seen by induction that the relation $x\partial = q\partial x + 1$ implies that for $i, j \ge 0$ we have

$$x^i \partial^j = \sum_{l \ge 0} \binom{i}{l}_q \binom{j}{l}_q (l)_q^! \, q^{(j-l)(i-l)} \partial^{j-l} x^{i-l}.$$

Remark 3.7. Let $V \in {}^{\mathbf{k}\Gamma}_{\mathbf{k}\Gamma}\mathcal{YD}$. We note that the relations in $\mathcal{A}V$ imply that if $\partial \in V^*$ is such that $\partial|_{V^h} = 0 \ \forall h \neq g$ and $z \in \mathfrak{B}(V)$, then $z\partial = [z, \partial] + \partial g(z)$ in $\mathcal{A}V$. Thus, if $w \in \mathfrak{B}(V^*)$, we have

$$zw = [z, w] + \text{terms beginning with elements of positive degree in } \mathfrak{B}(V^*).$$

Now, for a finite dimensional graded space $A = \oplus_{i=0}^n A_i$ we denote the Hilbert polynomial $P_A(t) = \sum_{i=0}^n \dim(A_i) t^i$. We are in position to prove the main theorem.

Theorem 3.8. *Let $V \in {}^{\mathbf{k}\Gamma}_{\mathbf{k}\Gamma}\mathcal{YD}$ be finite dimensional.*

1. *Suppose there exists W as in 3.5 part 2 such that $\mathfrak{B}(W)$ is finite dimensional. Take the basis $\{x_1, \dots, x_m\}$ of W and the dual basis $\{\partial_1, \dots, \partial_m\}$ of $W^* \subset V^*$ (extend them to V by $\partial_i|_{W'} =$*

$0\ \forall i$). *Consider then the* ∂_i*'s as operators on* $\mathfrak{B}(V)$ *and let* $K = \cap_{i=1}^m \ker(\partial_i)$. *Then* $\mathfrak{B}(V) \simeq K \otimes \mathfrak{B}(W)$ *as right* $\mathfrak{B}(W)$*-modules and as left* K*-modules. In particular,*

$$P_{\mathfrak{B}(V)}(t) = P_K(t) P_{\mathfrak{B}(W)}(t),$$

and thus $\dim \mathfrak{B}(W)$ *divides* $\dim \mathfrak{B}(V)$.

2. *Suppose that* $\mathfrak{B}(V)$ *is finite dimensional and* $V = V_1 \oplus \cdots \oplus V_\theta$ *is a decomposition of* (V, c) *(that is,* $c(V_i \otimes V_j) = V_j \otimes V_i$*). For each* $1 \le i \le \theta$*, let* $W_i \subseteq V_i$ *be a (possibly zero) subspace of* V_i *as in 3.5 part 2, i.e., for each* i*,* W_i *is a* $\mathbf{k}\Gamma_i'$*-comodule for* $\Gamma' \subseteq \Gamma$ *a subgroup, it is* $\mathbf{k}\Gamma_i'$*-stable and there exists* $W_i' \subseteq V$ *a* $\mathbf{k}\Gamma$*-subcomodule and a* $\mathbf{k}\Gamma_i'$*-submodule such that* $V = W_i \oplus W_i'$*. Thus, if* $P_i(t)$ *is the Hilbert polynomial of* $\mathfrak{B}(W_i)$*, then the product* $\prod_{i=1}^\theta P_i(t)$ *divides* $P_{\mathfrak{B}(V)}(t)$ *and the quotient lies in* $\mathbb{Z}[t]$*. In particular,* $\prod_{i=1}^\theta \dim \mathfrak{B}(W_i)$ *divides* $\dim \mathfrak{B}(V)$.

Proof. 1. Since $\mathfrak{B}(W)$ is finite dimensional, we can fix $\Lambda_{\mathfrak{B}(W)}$ and $\Lambda_{\mathfrak{B}(W^*)}$ integrals such that

$$[\Lambda_{\mathfrak{B}(W)}, \Lambda_{\mathfrak{B}(W^*)}] = 1.$$

Let $\{z_1, \dots, z_n\}$ be a basis of homogeneous elements of $\mathfrak{B}(W)$, and let $\{\tilde{z}_1, \dots, \tilde{z}_n\}$ be the dual basis with respect to the Poincaré duality, i.e. $[\tilde{z}_i z_j, \Lambda_{\mathfrak{B}(W^*)}] = \delta_{ij}$. Let $p_i \in \mathcal{A}W$ be defined by $p_i = z_i \Lambda_{\mathfrak{B}(W^*)} \tilde{z}_i$. Now, by 3.7 we have that if $z \in \mathfrak{B}(W)$ and $w \in \mathfrak{B}(W^*)$ then

$$\Lambda_{\mathfrak{B}(W^*)} z w = \Lambda_{\mathfrak{B}(W^*)} [z, w].$$

Thus, by definition we have $p_i p_j = \delta_{ij} p_i$, i.e., the p_i's are mutually orthogonal idempotents. Furthermore, let $z \in \mathfrak{B}(W)$, $z = \sum_j \alpha_j \tilde{z}_j$. Then

$$(\sum_i p_i)(z) = \sum_{i,j} \alpha_j [\tilde{z}_j z_i, \Lambda_{\mathfrak{B}(W^*)}] \tilde{z}_i = \sum_j \alpha_j \tilde{z}_j = z,$$

whence $\sum_i p_i = 1$. Because of the immersion $\mathcal{A}W \hookrightarrow \mathcal{A}V$, the equality $\sum_i p_i = 1$ also holds in $\mathcal{A}V$. Now, since the image of $\Lambda_{\mathfrak{B}(W^*)}$ lies in K, we have that

$$\mathfrak{B}(V) = \sum_i \mathfrak{B}(V) z_i \Lambda_{\mathfrak{B}(W^*)} \tilde{z}_i \subseteq \sum_i K \tilde{z}_i.$$

This tells that the canonical map $\mu : K \otimes \mathfrak{B}(W) \to \mathfrak{B}(V)$ given by multiplication is surjective. We shall prove that the sum is direct and that μ restricted to $K \otimes \tilde{z}_i$ is injective $\forall i$, which completes the proof. To see this, if $0 = \sum_i k_i \tilde{z}_i$ with $k_i \in K$, then for each j we have

$$\begin{aligned} 0 &= p_j(\sum_i k_i \tilde{z}_i) \\ &= \sum_i k_i \tilde{z}_i z_j \Lambda_{\mathfrak{B}(W^*)} \tilde{z}_j \\ &= \sum_i k_i \left([\tilde{z}_i z_j, \Lambda_{\mathfrak{B}(W^*)}] + \text{ terms beginning with elements of positive degree in } \mathfrak{B}(W^*) \right) \tilde{z}_j \\ &= k_j \tilde{z}_j. \end{aligned}$$

This proves that the sum is direct. Now, if $k \in K$ and, for some i, $k\tilde{z}_i = 0$, then let d be the degree of $\tilde{z}_i$ and let w_i be an element in $\mathfrak{B}^d(W^*)$, such that $[\tilde{z}_i, w_i] = 1$. We have

$$0 = k\tilde{z}_i w_i = k[\tilde{z}_i, w_i] + k\,(\text{terms beginning with elements of positive degree in } \mathfrak{B}(W^*)) = k,$$

which implies the injectivity of μ.

2. Consider in $\mathfrak{B}(V)$ the multi-degree given by the decomposition $V = \oplus_i V_i$. The condition on the V_i's implies that the map $\mathbf{S}^n$ is (multi-)graded for each n, whence we can take the Hilbert polynomial of $\mathfrak{B}(V)$ in $\mathbb{Z}[t_1, \dots, t_\theta]$, i.e.

$$P_{\mathfrak{B}(V)}(t_1, \dots, t_\theta) = \sum_{i_1, \dots, i_\theta} \dim \mathfrak{B}^{i_1, \dots, i_\theta}(V) t_1^{i_1} \cdots t_\theta^{i_\theta}$$

($\mathfrak{B}^{i_1, \dots, i_\theta}(V)$ the homogeneous component of degree $(i_1, \dots, i_\theta)$). If $K_i \subset \mathfrak{B}(V)$ is the intersection of the kernels of ∂ for all $\partial \in W_i^*$, then we can take also the Hilbert polynomial of K_i in $\mathbb{Z}[t_1, \dots, t_\theta]$ since the elements in W_i^* act in an homogeneous way. By the first part, we have that $P_{\mathfrak{B}(V)} = P_{K_i} P_{\mathfrak{B}(W_i)}$, where $P_{\mathfrak{B}(W_i)} \in \mathbb{Z}[t_i]$. Thus, for each i the polynomial $P_{\mathfrak{B}(W_i)}$ divides $P_{\mathfrak{B}(V)}$, and since these polynomials are coprime, their product also divides $P_{\mathfrak{B}(V)}$. Moreover, since the product is a monic polynomial (because $\dim \mathfrak{B}^{\mathrm{top}(W_i)}(W_i) = 1$) the quotient lies in $\mathbb{Z}[t_1, \dots, t_\theta]$. The result follows taking $t_1 = \cdots = t_\theta = t$.

□

Remark 3.9. In the situation of the first part of the theorem, the Leibniz rule tells immediately that K is a subalgebra of $\mathfrak{B}(V)$. It is in general not a coalgebra, but with the help of (2.8) it is easy to see that it is a left coideal. The fact that the morphism $K \otimes \mathfrak{B}(W) \to \mathfrak{B}(V)$ is the multiplication of $\mathfrak{B}(V)$ shows that they are isomorphic as $(K, \mathfrak{B}(W))$-bimodules.

Remark 3.10. Let $V = \oplus_i M(g_i, \rho_i)$ a module in ${}^{\mathbf{k}\Gamma}_{\mathbf{k}\Gamma}\mathcal{YD}$, Γ finite. Let $z = z_{jl}^i \in M(g_i, \rho_i)$ be as in 2.15. Then $c(z \otimes z) = qz \otimes z$, where $q = \rho_i(g_i)$. By the first part of Theorem 3.8 (taking $W' = W_{jl}^{\prime i}$), we have that $N(q)$ divides $\dim \mathfrak{B}(V)$. Furthermore, a basis of $\mathfrak{B}(V)$ is given by $\{y_a z^b \mid 0 \leq b < N(q)\}$, where $\{y_a\}$ is a basis of $\ker \partial^i_{jl}$.

Taking one element $z^i_{j_i l_i}$ in each $M(g_i, \rho_i)$ and $q_i = \rho_i(g_i)$, $N_i = N(q_i)$, by the second part of Theorem 3.8 (W_i being the subspace generated by $z^i_{j_i l_i}$ and $W'_i = W'^i_{j_i l_i}$) we have that $\prod_i N_i$ divides $\dim \mathfrak{B}(V)$.

Remark 3.11. We notice the difference between this result, 2.2 and 2.17. Let Γ be finite and $V \in {}^{\mathbf{k}\Gamma}_{\mathbf{k}\Gamma}\mathcal{YD}$ be finite dimensional, $V = \oplus_i M(g_i, \rho_i) = \oplus_i V_i$. Let $d_i = \dim(V_i)$, $q_i = \rho_i(g_i)$, $N_i = N(q_i)$, let $D_i = \dim(\mathfrak{B}(V_i))$. Then by 2.2 we have $\dim(\mathfrak{B}(V)) \geq \prod_i D_i$ and by 2.17 we have $D_i \geq N_i^{d_i}$. Finally, 3.8 tells that if $\dim(\mathfrak{B}(V))$ is finite, then it can be divided by $\prod_i N_i$.

We warn that it is not in general true that $\dim(\mathfrak{B}(V))$ is divisible by $\prod_i N_i^{d_i}$. For instance taking V with basis $\{x_0, x_1, x_2\}$ and braiding $c(x_i \otimes x_j) = -x_{-i-j} \otimes x_i$ (we take the subindices in $\mathbb{Z}/3$), then $d = 3$ and $N = 2$, but $\dim(\mathfrak{B}(V)) = 12$ (it is computed in [MS], see also [AG]).

This example shows also why 3.8 is not a consequence of a braided version of the Nichols–Zoeller theorem. Taking $W = \operatorname{span}(x_0)$, we have $c(V \otimes W) \not\subset (W \otimes V)$, and in particular $c(\mathfrak{B}(V) \otimes \mathfrak{B}(W)) \not\subset (\mathfrak{B}(W) \otimes \mathfrak{B}(V))$, from where $\mathfrak{B}(W)$ is not a *categorical braided Hopf subalgebra* of $\mathfrak{B}(V)$ in the sense of [T3], which is one of the hypotheses of Nichols–Zoeller theorem for braided Hopf algebras.

4. Applications

As a consequence of the main theorem, we have a generalization of [D] and [AS2, Lemma 7.4]:

Corollary 4.1. *Let A be a finite dimensional pointed Hopf algebra, let $\Gamma = G(A)$ be its group of group-like elements, and let $[A : \Gamma]$ be the index of Γ in A. If $[A : \Gamma] = p$ is a prime number, then there exists $g \in Z(\Gamma)$, $\chi \in \hat{\Gamma}$ a character and $\lambda \in \{0, 1\}$ such that*

- *$\chi(g)$ is a primitive p-th root of unity*
- *$\lambda = 0$ if $\chi^p \neq 1$ or $g^p = 1$,*

and the algebra A is isomorphic to the algebra generated by $G(A)$ plus an element x with relations

$$x^p = \lambda(g^p - 1),$$

$$hx = \chi(h)xh.$$

The coalgebra structure is given by $\Delta(x) = g \otimes x + x \otimes 1$.

Proof. The lifting procedure (see [AS1]) applied to A, we get R a coradically graded Hopf algebra in ${}^{\mathbf{k}\Gamma}_{\mathbf{k}\Gamma}\mathcal{YD}$ of dimension p. Let R' be the subalgebra generated by $R(1)$. By the Nichols–Zoeller theorem

[NZ], $R' = R$, and thus R is a Nichols algebra. Take x a non-zero element in $R(1)$. The algebra generated by x in R is isomorphic to $\mathbf{k}[x]/x^t$, but by 3.8 and 3.10 we must have $t = p$, and then $R = \mathbf{k}[x]/x^p$. The equality $x^p = \lambda(g^p - 1)$ is a straightforward computation of the lifting procedure, as done for instance in [G1]. □

Corollary 4.2. *Let A be a pointed Hopf algebra, let $\Gamma = G(A)$ be its group of group-like elements, and let $[A : \Gamma]$ be the index of Γ in A. If $[A : \Gamma] = p^2$ is a square prime, then either*

1. *the situation is the same as in 4.1, replacing each occurrence of "p" by "p^2",*
2. *there exist two elements $g_1, g_2 \in Z(\Gamma)$, two characters $\chi_1, \chi_2 \in \hat{\Gamma}$ and $\lambda_1, \lambda_2, \lambda_3 \in \mathbf{k}$ such that*
   - *$\chi_i(g_i)$ are p-th roots of unity,*
   - *$\chi_1(g_2)\chi_2(g_1) = 1$*
   - *$\lambda_i = 0 \quad (i = 1, 2)$ if $\chi_i^p \neq 1$ or $g_i^p = 1$,*
   - *$\lambda_3 = 0$ if $\chi_1\chi_2 \neq 1$ or $g_1g_2 = 1$,*

   and the algebra A is isomorphic to the algebra generated by $\Gamma(A)$ plus two elements x_1, x_2 with relations
   $$\begin{aligned} &x_i^p = \lambda_i(g_i^p - 1), i = 1, 2; \quad x_1x_2 - \chi_2(g_1)x_2x_1 = \lambda_3(g_1g_2 - 1); \\ &hx_i = \chi_i(h)x_ih. \end{aligned}$$
   The coalgebra structure is given by
   $$\Delta(x_i) = g_i \otimes x_i + x_i \otimes 1,$$
3. *$p = 2$, there exists an element $g \in Z(\Gamma)$ and ρ an irreducible representation of Γ of degree 2 such that $\rho(g) = -\operatorname{id}$; there exists a Γ-invariant quadratic form $\lambda : \operatorname{span}\{x_1, x_2\} \to \mathbf{k}$ such that $\lambda = 0$ if $g^2 = 1$, and the algebra A is isomorphic to the algebra generated by Γ plus two elements x_1, x_2 with relations*
   $$\left.\begin{aligned} hxh^{-1} &= \rho(h)(x) \\ x^2 &= \lambda(x)(g^2 - 1) \end{aligned}\right\} \text{ for } x \in \operatorname{span}\{x_1, x_2\}.$$
   The coalgebra structure is given by $\Delta(x) = g \otimes x + x \otimes 1$, or
4. *there exists an element $g \in Z(\Gamma)$ with $[\Gamma : \Gamma_g] = 2$, and A may be presented as an extension*
$$\mathbf{k} \to B \to A \to \mathbf{k}(\Gamma/H) \to \mathbf{k}, \tag{4.3}$$
   where H is the subgroup of Γ generated by $\mathcal{O}_g$ and B fits into the case 2.

Proof. Take R' and R as in the proof of 4.1. Then the dimension of R' may be p or p^2. If it were equal to p, then 3.8 tells that the rank of R' is 1, and thus by [AS1, Thm. 3.2] $R = R'$, a contradiction. Then $R = R' = \mathfrak{B}(V)$, and R is a Nichols algebra. If $\dim V = 1$, then $V = M(g,\chi)$ and we are in case 1. If $\dim V = 2$, then either $V = M(g_1,\chi_1) \oplus M(g_2,\chi_2)$ and we are in case 2, $V = M(g,\rho)$ with $\deg\rho = 2$ and we are in case 3 ($\rho(g) = -\operatorname{id}$ is an equivalent condition for $\mathfrak{B}(V)$ to be p^2-dimensional, because of 2.2, the condition on λ to be Γ-invariant follows computing hx^2h^{-1}), or $V = M(g,\rho)$ with $[\Gamma : \Gamma_g] = 2$, and then by [AG, Lemma 3.1.9] $R\#\mathbf{k}\Gamma$ is an extension as 4.3 and we are in case 4. The rank of R is necessarily ≤ 2 because of 2.17. $\square$

As a last application of 3.8, we classify Nichols algebras of dimension p^3 that arise in Yetter–Drinfeld categories over finite groups. Together with the lifting procedure of [AS1], this is a first step in order to classify finite dimensional pointed Hopf algebras of index p^3.

Let then $V \in {}^{\mathbf{k}\Gamma}_{\mathbf{k}\Gamma}\mathcal{YD}$ be such that $\dim\mathfrak{B}(V) = p^3$. By 2.17 and 3.8, we have $\dim V \leq 3$. It can be proved (see [G2]) that if (V,c) does not come from the abelian case then $\dim\mathfrak{B}(V) > p^3$.

If $\dim V = 3$, $\mathfrak{B}(V)$ is a QLS because of 2.2 and 3.8, i.e. V has a basis $\{x_1,x_2,x_3\}$ such that the set $\{x_1^{n_1}x_2^{n_2}x_3^{n_3} \mid 0 \leq n_i < p\}$ is a basis of $\mathfrak{B}(V)$.

If $\dim V = 2$ then c has a matrix $\begin{pmatrix} q_{11} & q_{12} \\ q_{21} & q_{22} \end{pmatrix}$ where the q_{ii}'s are either p-roots or p^2-roots of unity. If one of them has order p^2, say q_{22}, then $N(q_{11}) = p$ and $\mathfrak{B}(V)$ is a QLS. If $N(q_{11}) = N(q_{22}) = p$ then by the results in [G2] we have two possibilities:

1. $p = 2$ and $q_{12}q_{21} \neq 1$. Furthermore, for $\mathfrak{B}(V)$ to be 8-dimensional $q_{12}q_{21} = -1$. The algebra $\mathfrak{B}(V)$ is of type A_2.
2. $p > 2$ and $q_{12}q_{21}q_{22} = 1$. Interchanging q_{11} with q_{22} we see that $q_{12}q_{21}q_{11} = 1$, whence $q_{11} = q_{22}$ and $\mathfrak{B}(V)$ is of type A_2.

Thus we reach in both cases to the same situation. The algebra $\mathfrak{B}(V)$ has a PBW basis given by $\{x_1^{m_1}z^nx_2^{m_2} \mid 0 \leq m_1,m_2,n < p\}$, $z = x_2x_1 - q_{21}x_1x_2$.

The last case is $\dim V = 1$. We have simply $\{x\}$ a basis of V such that $c(x\otimes x) = qx\otimes x$, $N(q) = p^3$. Thus $\mathfrak{B}(V) = \mathbf{k}[x]/(x^{p^3})$.

References

[AA] A. Abella & N. Andruskiewitsch, *Compact quantum groups arising from the FRT-construction*, Boletín de la Acad. Nac. Cs. Córdoba, Argentina **63** (1999), 15–44. Also in `www.mate.uncor.edu/andrus/articulos.html`.

[AG] N. Andruskiewitsch & M. Graña, *Braided Hopf algebras over non abelian finite groups*, Boletín de la Acad. Nac. Cs. Córdoba, Argentina **63** (1999), 45–78. Also in `www.mate.uncor.edu/andrus/articulos.html`.

[AS1] N. Andruskiewitsch & H.-J. Schneider, *Lifting of quantum linear spaces and pointed Hopf algebras of order* p^3, J.Algebra **209** (1998), 659–691.

[AS2] N. Andruskiewitsch & H.-J. Schneider, *Finite quantum groups and Cartan matrices*, to appear in Adv. Math.

[AS3] N. Andruskiewitsch & H.-J. Schneider, *Lifting of Nichols algebras of type* A_2 *and pointed Hopf algebras of order* p^4, Proc. Coll. Hopf algs. & quantum gps., ed. S. Caenepeel, M. Dekker. Brussels (1998), 1–18.

[D] S. Dăscălescu, *Pointed Hopf algebras with large coradical*, Commun. Alg. **27**, 10 (1999), 4827–4851.

[FG] Fronsdal & Galindo, *The ideals of free differential algebras*, `q-alg 9806069`.

[Gu] D. Gurevich, *Algebraic Aspects of the Quantum Yang–Baxter Equation*, Leningrad J. of Math. **2** (1991), 801–828.

[G1] M. Graña, *Pointed Hopf algebras of dimension 32*, Commun. Alg., to appear.

[G2] M. Graña, *Nichols algebras of low dimension*, Contemp. Math., to appear.

[H] M. Hayashi, *Quantum groups and quantum semigroups*, J. Algebra **204** (1998), 225–254.

[Ly] V. Lyubashenko, *Hopf algebras and vector symmetries*, Russian Math. Surveys **41** (1986), 153–154.

[LS] V. Lyubashenko, A Sudbery, *Quantum supergroups of* $GL(n|m)$ *type: differential forms, Koszul complexes and berezinians*, Duke Math. J. **90** (1997), 1–62.

[MS] A. Milinski and H.-J. Schneider, *Pointed Indecomposable Hopf Algebras over Coxeter Groups*, preprint.

[Mo] S. Montgomery, *Hopf algebras and their actions on rings*, AMS, CBMS **82** (1993).

[NZ] W. D. Nichols and M. B. Zoeller, *A Hopf algebra freeness theorem*, Amer. J. Math. **111** (1989), 381–385.

[Sf] B. Scharfschwerdt, Talk at *Colloquium on Quantum Groups and Hopf Algebras*, La Falda, (1999).

[Sn] P. Schauenburg, *On Coquasitriangular Hopf algebras and the Quantum Yang–Baxter equation*, Algebra Berichte **67** (1992), 1–76, Verlag R. Fischer, München.

[T1] M. Takeuchi, *The coquasitriangular Hopf algebra associated with a rigid Yang–Baxter coalgebra*, Proc. Coll. Hopf algs. & quantum gps., ed. S. Caenepeel, M. Dekker. Brussels (1998), 251–270.

[T2] M. Takeuchi, *Finite Hopf algebras in braided tensor categories* J. P. App. Alg. **138** (1999), 59–82.

[T3] M. Takeuchi, *The Nichols–Zoeller theorem for braided Hopf algebras*, (1999) preprint.

Matías Graña: Departamento de Matemática, FCEyN, Pab. I,
(1428) Ciudad Universitaria, Buenos Aires, Argentina

E-mail address: `matiasg@dm.uba.ar`