ON NICHOLS ALGEBRAS OF LOW DIMENSION

MATÍAS GRAÑA

Abstract. This is a contribution to the classification program of pointed Hopf algebras. We give a generalization of the quantum Serre relations and propose a generalization of the Frobenius–Lusztig kernels in order to compute Nichols algebras of diagonal group type. With this, we classify Nichols algebras $\mathfrak{B}(V)$ with dimension < 32 or with dimension p^3, p a prime number, when V lies in a Yetter–Drinfeld category over a finite group. With the so called Lifting Procedure, this allows to classify pointed Hopf algebras of index < 32 or p^3.

1. Introduction, notation, preliminaries

1.1. **Introduction.** The "Lifting Procedure" (see [AS1]) is a method intended to classify finite dimensional pointed Hopf algebras. Among the achievements of this method, we mention the classification of pointed Hopf algebras of order p^3, p^4 (p a prime number) [AS1, AS3], the classification of pointed Hopf algebras whose group is of exponent p [AS4], the classification of pointed Hopf algebras of order p^5 [AS4, G2, G1], the classification of pointed Hopf algebras of index p, p^2 [G3], the answer, by the negative, to the tenth Kaplansky conjecture [AS2] (some of these results have been obtained independently by other methods, see for instance [BDG, Ge, D, CD, CDR, SvO, B]). The first step in this procedure is the classification of Nichols algebras, i.e., graded braided Hopf algebras with the base field in degree 0 and which are coradically graded and generated by its primitive elements (see 1.4.5). Being braided and graded, such an algebra gives a braiding $c : V \otimes V \to V \otimes V$, where V is the space of primitive elements (which turns out to coincide with the homogeneous component of degree 1). Furthermore, the pair (V, c) determines the Nichols algebra up to isomorphism. A major goal in the classification program of pointed Hopf algebras is thus to have an algorithm describing (and in particular giving the dimension of) a Nichols algebra starting out with the pair (V, c) as its space of primitive elements. Although any solution to the Braid Equation $c : V \otimes V \to V \otimes V$ gives rise to a Nichols algebra, the objects V arising in the application of the Lifting Procedure are objects of Yetter–Drinfeld categories over finite groups, and hence we shall restrict ourselves to those pairs (V, c) with this additional property (see 1.4.10).

The theory divides at this moment in two branches: the pair (V, c) is "of diagonal group type" (see 1.4.10) or it is not. In the first case, a substantial progress is made in [AS2] through the notion of "braiding of Cartan type", using the theory of Frobenius–Lusztig kernels. This notion applies to a large class of pairs (V, c) of diagonal group type. In this article we propose to enlarge the class of Frobenius–Lusztig kernels and we give the examples of type A_2 and B_2 (see 2.11 and 2.14). To

1991 *Mathematics Subject Classification.* Primary 16W30; Secondary 17B37.

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

compute the PBW bases of these generalized FL-kernels we use a generalized form of the quantum Serre relations. Though this generalized form can be found in [R] for the diagonal case, we prefer to derive it from an equality in the group algebra of the braid group, since this equality could provide quantum Serre relations for the general case (see 2.2 and 2.5).

In the non-diagonal case very little is known. In fact, up to now there were only two examples known to produce finite dimensional Nichols algebras (and hence, finite dimensional pointed Hopf algebras). The first one is 3-dimensional and it generates a 12-dimensional Nichols algebra (it is given for the first time in [MS] and was reproduced in [AG]). The second one is 6 dimensional and it is given also in [MS]. Another example given there, which is 4 dimensional, is proved in this article to be of diagonal group type (see 5.2.1).[1] In this article we propose some tools to classify all Yetter–Drinfeld modules of a given dimension over finite groups. We use these tools to parameterize those modules of dimension 3, 4 (sections 4, 5). As a consequence of this, we find a new example of a finite dimensional Nichols algebra with a 4-dimensional space of primitive elements which is of non-diagonal group type; its dimension is 72 (see 5.3.2). We also give some necessary conditions for an irreducible YD-module to be of "finite Nichols rank" (i.e., to give a finite dimensional Nichols algebra). This allows to focus the attention mainly on the specific cases $V = M(g, \chi)$ where χ is a character (see 3.1 for the condition, 1.4.7 for the definition of $M(g, \rho)$).

Finally, as a consequence of these methods together with those of [G3], we classify Nichols algebras over finite groups with dimension < 32. As said above, this is the first step in the classification of pointed Hopf algebras of index < 32. Specifically, we have:

Theorem 1.1.1. *Let $R \in {}^{\mathbf{k}\Gamma}_{\mathbf{k}\Gamma}\mathcal{YD}$ be a Nichols algebra, where Γ is a finite group and $\dim R < 32$. Let $V = \mathcal{P}R$ be its space of primitive elements. Then $\dim V \leq 4$ and either*

- *R is a Quantum Linear Space (see definition in 2.10), or*
- *R is of type A_2 (see remark 2.14), or*
- *R is of type $A_2 \times A_1$, or*
- *$V = V_{3,-1}$ and $\dim R = 12$ (see 4.1 for the definition), or*
- *$V = V_{3,-1} \oplus V'$, $\dim \mathfrak{B}(V') = 2$, $c^2 : V_{3,-1} \otimes V' \to V_{3,-1} \otimes V'$ is the identity, and $\dim R = 24$.*

1.2. **Acknowledgements.** I thank N. Andruskiewitsch for the careful reading of the material and for general and particular advice. I thank J. Fernández Bonder for a hint on 3.3. The referee has suggested the best terminology I have seen for the braided pairs that this article deals with. It has been a pleasure to read his comments. Thanks to A. Schüler, who pointed out a mistake in the published version for the relation $z_2 z_1 = q_{11} q_{12} q_{21}^2 q_{22}^2 z_1 z_2$ in the proof of 2.11. I thank also M. Lamas for many valuable conversations.

1.3. **Notation.** For a general reference on Hopf algebras see [M]. We fix an algebraically closed field $\mathbf{k}$ of characteristic 0. Most of the results of the article are still true for positive characteristic, as long as it does not divide the dimension of the

[1] After submitting the paper I was informed that a third module given in [MS] is known to produce a finite dimensional Nichols algebra (see [FK]).

Nichols algebras under consideration (see [G4]). In this case, the definition of $N(1)$ below must be given as $N(1) = \mathrm{char}(\mathbf{k})$.

All vector spaces, algebras, tensor products, homs are considered over $\mathbf{k}$ unless explicitly stated. If Γ is a group and $g \in \Gamma$, we denote by Γ_g the centralizer $\Gamma_g = \{x \in \Gamma \mid xg = gx\}$.

For a root of unity q, we denote by $N(q)$ its order if $q \neq 1$. If $q = 1$ or q is not a root of unity then we define $N(q) = \infty$. We recall the definition of q-numbers: for $\mathbf{q}$ an indeterminate and $n, m \in \mathbb{N}$, $n \geq m$, define

$$(n)_{\mathbf{q}} = 1 + \mathbf{q} + \mathbf{q}^2 + \cdots + \mathbf{q}^{n-1}, \quad (n)^!_{\mathbf{q}} = \prod_{i=1}^{n} (i)_{\mathbf{q}}, \quad \binom{n}{m}_{\mathbf{q}} = \frac{(n)^!_{\mathbf{q}}}{(m)^!_{\mathbf{q}}\,(n-m)^!_{\mathbf{q}}}.$$

All these expressions lie in $\mathbb{Z}[\mathbf{q}]$. For $q \in \mathbf{k}$ we evaluate them in $\mathbf{q} = q$ to get $(n)_q$, $(n)^!_q$ and $\binom{n}{m}_q$.

Let $\mathbb{S}_n$ be the symmetric group, presented with $n-1$ generators $\{\tau_1, \dots, \tau_{n-1}\}$ and relations $\tau_i\tau_j = \tau_j\tau_i$ if $|i-j| > 1$, $\tau_i\tau_{i+1}\tau_i = \tau_{i+1}\tau_i\tau_{i+1}$, $\tau_i^2 = 1$. We denote by $\mathbb{B}_n$ the braid group, with $n-1$ generators $\{\sigma_1, \dots, \sigma_{n-1}\}$ and relations

$$\sigma_i\sigma_j = \sigma_j\sigma_i \text{ if } |i-j| > 1, \quad \sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1}.$$

We consider the sequence of inclusions

$$\mathbb{B}_1 \hookrightarrow \mathbb{B}_2 \hookrightarrow \dots \hookrightarrow \mathbb{B}_n \hookrightarrow \mathbb{B}_{n+1} \hookrightarrow \dots$$

where $\sigma_i \mapsto \sigma_i$, and consider $\mathbb{B}_\infty$ the limit of this sequence.

Definition 1.3.2. For $m < n$, we denote by $\mathbb{B}_{m\text{-}n}$ the subgroup of $\mathbb{B}_n$ generated by $\sigma_m, \dots, \sigma_{n-1}$. We denote by $\iota_{m\text{-}n} : \mathbb{B}_{n-m+1} \to \mathbb{B}_n$ the inclusion $\sigma_i \mapsto \sigma_{i+m-1}$. Then $\mathbb{B}_{m\text{-}n} = \mathrm{Im}(\iota_{m\text{-}n})$. We may view all these groups as subgroups of $\mathbb{B}_\infty$. If x_1, x_2 are elements of $\mathbb{B}_{j_1}, \mathbb{B}_{j_2}$ respectively, then we denote

$$(x_1|x_2) = x_1 \cdot \iota_{(j_1+1)\text{-}(j_1+j_2)}(x_2) \in \mathbb{B}_{j_1+j_2},$$

and inductively we define

$$(x_1|\cdots|x_s) = (x_1|(x_2|\cdots|x_s)) \in \mathbb{B}_{j_1+\cdots+j_s}.$$

For instance, if $x_1 = \sigma_2\sigma_1 \in \mathbb{B}_3$ and $x_2 = \sigma_1 \in \mathbb{B}_2$, we have $(x_1|x_2) = \sigma_2\sigma_1\sigma_4 \in \mathbb{B}_5$. We extend (bi)linearly the definition of $(|)$ to the group algebra, i.e.

$$(|) : \mathbf{k}\mathbb{B}_{j_1} \otimes \mathbf{k}\mathbb{B}_{j_2} \to \mathbf{k}\mathbb{B}_{j_1+j_2}.$$

1.4. **Preliminaries.** We consider the canonical projection $\mathbb{B}_n \twoheadrightarrow \mathbb{S}_n$, $\sigma_i \mapsto \tau_i$. By [CuRe, 64.20] we have a section (of sets) $s : \mathbb{S}_n \to \mathbb{B}_n$ such that if $x = \tau_{i_1} \cdots \tau_{i_l}$, where $l = \ell(x)$ (i.e., x can not be written with fewer than l generators τ_i's), then $s(x) = \sigma_{i_1} \cdots \sigma_{i_l}$. Notice that if $\ell(xy) = \ell(x) + \ell(y)$ then $s(xy) = s(x)s(y)$.

We denote by $\mathbf{S}^n$ the element of the group algebra $\mathbf{k}\mathbb{B}_n$

$$\mathbf{S}^n = \sum_{x \in \mathbb{S}_n} s(x). \tag{1.4.3}$$

Let $i_1 + \cdots + i_r = n$. We denote by $Sh_{i_1,\dots,i_r} \subseteq \mathbb{S}_n$ the subset of $(i_1, \dots, i_r)$-shuffles, i.e.

$$Sh_{i_1,\dots,i_r} = \{x \in \mathbb{S}_n \mid x^{-1}(i_1 + \cdots + i_j + 1) < x^{-1}(i_1 + \cdots + i_j + 2) < \cdots$$
$$\cdots < x^{-1}(i_1 + \cdots + i_j + i_{j+1}) \text{ for } j = 0, \dots, r-1\}.$$

We consider also the elements

$$\mathbf{S}_{i_1,\dots,i_r} = \sum_{x\in Sh_{i_1,\dots,i_r}} s(x) \in \mathbf{k}\mathbb{B}_{i_1+\dots+i_r},$$
$$\mathbf{T}_{i_1,\dots,i_r} = \sum_{x^{-1}\in Sh_{i_1,\dots,i_r}} s(x) \in \mathbf{k}\mathbb{B}_{i_1+\dots+i_r},$$
$$\mathbf{S}^{j_1|j_2|\cdots|j_s} = (\mathbf{S}^{j_1}|\mathbf{S}^{j_2}|\cdots|\mathbf{S}^{j_s}) \in \mathbf{k}\mathbb{B}_{j_1+\dots+j_s}.$$

Notice that

$$\mathbf{S}^{i|j}\mathbf{S}_{i,j} = \mathbf{S}_{i+j} = \mathbf{T}_{i,j}\mathbf{S}^{i|j}.$$

Definition 1.4.4. 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. We say that (V, c) is a *rigid braided pair* (or RBP) if it is a finite dimensional BP such that $c^\flat \in \mathrm{End}(V^*\otimes V, V\otimes V^*)$ is an isomorphism (see for instance [T1] for the definition of $c^\flat$).

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. If V is an object of ${}_H^H\mathcal{YD}$ with braidings $c_{V,W} : V\otimes W \to W\otimes V$, then $(V, c = c_{V,V})$ is a braided pair. If V is moreover finite dimensional then $(V, c = c_{V,V})$ is an RBP.

Let (V, c) be a BP. The group $\mathbb{B}_n$ acts on $V^{\otimes n}$ by $\sigma_i \mapsto (\mathrm{id}_{V^{\otimes i}} \otimes c \otimes \mathrm{id}_{V^{\otimes n-i-2}})$. We denote respectively by AV, CV the tensor algebra and the tensor coalgebra of V. As vector spaces, they coincide with $TV = \oplus_i V^{\otimes i} = \oplus_i A^iV = \oplus_i C^iV$. The (i, j)-component of the multiplication of AV is simply the identity map $m_{i,j} = \mathrm{id} : A^iV\otimes A^jV \to A^{i+j}V$. Dually, the (i, j)-component of the comultiplication 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. The comultiplication components of AV are nothing but $\mathbf{S}_{i,j} : A^{i+j}V \to A^iV\otimes A^jV$. Dually, the multiplication components of CV are $\mathbf{T}_{i,j} : C^iV\otimes C^jV \to C^{i+j}V$. The antipode in both cases is determined by $\mathcal{S}(x) = -x\ \forall x \in V$.

There exists a unique (graded) map of braided Hopf algebras which reduces to the identity $\mathrm{id} : V \to V$ in degree 1; we denote this map by $\mathbf{S}$. Its graded components are the maps $\mathbf{S}^n : A^nV \to C^nV$.

Definition 1.4.5. Let (V, c) be an RBP. We say that the image of

$$\mathbf{S} : AV \to CV$$

is the *Nichols algebra* generated by V and we denote it by $\mathfrak{B}(V)$ [2]. We say that $\dim(\mathfrak{B}(V))$ is the *Nichols rank* of V.

Remark 1.4.6. It can be proved that a finite dimensional braided pair (V, c) belongs to a braided category, and that an RBP (V, c) belongs to a rigid braided category. We warn that in [AS2] the term "Nichols algebra" is used for the case in which the rigid braided category is clearly defined. For the purpose of this article, it is more convenient not to emphasize the rigid braided category in which (V, c) lies. Furthermore, we shall often consider (V, c) as an object of different categories.

[2]If (V, c) is just a BP, the object $\mathfrak{B}(V)$ can be constructed in the same manner. In this general case, the result has been called a *Quantum Symmetric Algebra*.

We refer to [AG] for first properties of Nichols algebras. We refer to [G3] for further results, in particular the freeness result of Nichols algebras over certain Nichols subalgebras which we state in 2.7.

Definition 1.4.7. Let Γ be a finite group, $g \in \Gamma$, and $\rho \in \widehat{\Gamma_g}$ an irreducible representation of Γ_g. We denote by $M(g,\rho) \in {}^{\mathbf{k}\Gamma}_{\mathbf{k}\Gamma}\mathcal{YD}$ the object

$$M(g,\rho) = \operatorname{Ind}_{\Gamma_g}^{\Gamma} \rho = \mathbf{k}\Gamma \otimes_{\mathbf{k}\Gamma_g} \rho, \quad h \rightharpoonup (t \otimes x) = ht \otimes x, \quad \delta(t \otimes x) = tgt^{-1} \otimes (t \otimes x).$$

It has been proved in [DPR, W] and then more generally in [CiRo] in the language of Hopf bimodules (see also [AG]) that if one takes one element g in each conjugacy class of Γ and if ρ runs over all irreducible non-isomorphic representations of Γ_g, the objects $M(g,\rho)$ are a full set of irreducible non-isomorphic objects of ${}^{\mathbf{k}\Gamma}_{\mathbf{k}\Gamma}\mathcal{YD}$, which turns out to be a semisimple category.

Definition 1.4.8. Let $V = \oplus_{i=1}^{\theta} M(g_i,\rho_i)$, where $\rho_i : \Gamma_{g_i} \to \operatorname{Aut}(W_i)$ is an irreducible representation of Γ_{g_i}. Let $\{x_1^i, \dots, x_{r_i}^i\}$ be a basis of W_i and let $\{h_1^i, \dots, h_{s_i}^i\}$ be a set of representatives of left cosets Γ/Γ_{g_i}. We define $t_j^i = h_j^i g_i (h_j^i)^{-1}$ and $z_{jl}^i = h_j^i \otimes x_l^i \in \operatorname{Ind}_{\Gamma_i}^{\Gamma} W_i = M(g_i,\rho_i)$. Then $\{z_{jl}^i\}_{ijl}$ is a basis of V and the braiding is given by

$$c(z_{jl}^i \otimes z_{vw}^u) = (t_j^i h_v^u \otimes x_w^u) \otimes z_{jl}^i = t_j^i \rightharpoonup z_{vw}^u \otimes z_{jl}^i.$$

Definition 1.4.9. 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 c_{ij} the restriction $c_{ij} = c|_{V_i \otimes V_j}$. 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_{ii} of c then each (V_i, c_{ii}) becomes an RBP.

If Γ is a finite group and $V \in {}^{\mathbf{k}\Gamma}_{\mathbf{k}\Gamma}\mathcal{YD}$ is finite dimensional, then as noticed in 1.4.8 V can be decomposed as $V = \oplus_i M(g_i,\rho_i)$. 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 ${}^{\mathbf{k}\Gamma}_{\mathbf{k}\Gamma}\mathcal{YD}$, but since (V,c) is an RBP any decomposition gives a direct sum of RBP's.

Definition 1.4.10. Let (V,c) be a BP. We say that V is *of group type* (or *of GT*) if V has a basis $\{x_1, \dots, x_n\}$ and there exist $g_i \in \operatorname{GL}(V)$ $(i = 1, \dots, n)$ such that

$$c(x_i \otimes x_j) = g_i(x_j) \otimes x_i. \tag{1.4.11}$$

The terminology, introduced by the referee, comes from the fact that for V a finite dimensional object of ${}^{\mathbf{k}\Gamma}_{\mathbf{k}\Gamma}\mathcal{YD}$, one can find such a basis and maps in $\operatorname{GL}(V)$ (in fact, 1.4.8 tells explicitly how to do this when Γ is finite), and conversely, a BP which such a property is automatically an object of ${}^{\mathbf{k}\Gamma}_{\mathbf{k}\Gamma}\mathcal{YD}$, where $\Gamma \subset \operatorname{GL}(V)$ is the group generated by $\{g_1, \dots, g_n\}$. We further say that (V,c) is *of finite group type* (or *finite GT*) if the group Γ generated by $\{g_1, \dots, g_n\}$ is finite. We say that (V,c) is *of abelian group type* (or *abelian GT*) if Γ is abelian, and we finally say that (V,c) is *of diagonal group type* (or *diagonal GT*) if Γ acts in a diagonal way on V. It is clear that "diagonal" implies "abelian" and that the latter implies the former when $\mathbf{k}$ is algebraically closed of characteristic 0 (as we supposed it to be). It is clear also that "diagonal" means that there exist a basis $\{x_1, \dots, x_n\}$ and a matrix $(q_{ij}) \in (\mathbf{k}^\times)^{n\times n}$ such that

$$c(x_i \otimes x_j) = q_{ij} x_j \otimes x_i. \tag{1.4.12}$$

This condition is called "to come from the abelian case" in [AG], since for V in ${}^{\mathbf{k}\Gamma}_{\mathbf{k}\Gamma}\mathcal{YD}$, Γ finite abelian, it is fulfilled. The basis $\{x_1, \dots, x_n\}$ and the matrix (q_{ij}) verifying 1.4.12 will be called *the basis* and *the matrix* of (V, c).

In general, for a BP of group type (V, c), we say that $\{x_1, \dots, x_n\}$ is *a braided basis* if it verifies 1.4.11. The maps $\{g_1, \dots, g_n\}$ are called *the group-likes associated* to the basis. It can be seen that

$$g_i(x_j) \in V^{g_i g_j g_i^{-1}}, \tag{1.4.13}$$

where we denote $V^g := \operatorname{span}\{x_t \mid g_t = g\}$.

It is not hard to prove that a 2-dimensional BP of group type is always of abelian GT, and hence if it is moreover of finite GT, then it is of diagonal GT.

2. On the diagonal case

We prove an equality in the group algebra of the braid group $\mathbb{B}_n$. This equality will give information on the adjoint action. In particular, the quantum Serre relations will turn out to be a direct consequence of this equality. We denote by e the identity element in $\mathbb{B}_n$ and consider in $\mathbf{k}\mathbb{B}_n$ the following elements for $1 \le i \le j \le n$.

$$\begin{aligned}
U_i^j &= \sigma_j \sigma_{j-1} \cdots \sigma_i, \\
D_i^j &= \sigma_i \sigma_{i+1} \cdots \sigma_j, \\
R_i^j &= (e - \sigma_j\sigma_j)(e - D_{j-1}^j \sigma_j)(e - D_{j-2}^j \sigma_j) \cdots (e - D_i^j \sigma_j).
\end{aligned}$$

Lemma 2.1. *We have the following identities*

(1) *Let $y \in \mathbb{B}_n \hookrightarrow \mathbb{B}_{n+1}$ and let $x = \iota_{2\_(n+1)}(y)$. Then $U_1^n x = y U_1^n$ and $x D_1^n = D_1^n y$.*
(2) *Let $x \in \mathbb{B}_{2\_(n+1)}$. Then $x D_1^n U_1^n = D_1^n U_1^n x$.*
(3) *$U_1^j D_2^n \sigma_n = D_1^n \sigma_n U_1^{j-1}$ for $j < n$.*
(4) *$(e + U_1^1 + U_1^2 + \dots + U_1^{n-1} - D_n^n U_1^n - D_{n-1}^n U_1^n - \dots - D_1^n U_1^n) R_2^n = R_1^n (e + U_1^1 + U_1^2 + \dots + U_1^{n-1})$ for $n \ge 2$.*

Proof. (1) Since ι_{2_n} is a morphism, we prove it for the generators. Let $y = \sigma_{j-1}$, $2 \le j \le n$. Then $x = \sigma_j$, and we have

$$\begin{aligned}
U_1^n x = \sigma_n \cdots \sigma_1 \sigma_j &= (\sigma_n \cdots \sigma_{j+1}) \sigma_j \sigma_{j-1} \sigma_j (\sigma_{j-2} \cdots \sigma_1) \\
&= (\sigma_n \cdots \sigma_{j+1}) \sigma_{j-1} \sigma_j \sigma_{j-1} (\sigma_{j-2} \cdots \sigma_1) = \sigma_{j-1} \sigma_n \cdots \sigma_1 \\
&= y U_1^n,
\end{aligned}$$

and analogously for D_1^n.

(2) As the previous item, we can prove it for generators σ_j, $2 \le j \le n$. We have

$$\sigma_j D_1^n U_1^n = D_1^n \sigma_{j-1} U_1^n = D_1^n U_1^n \sigma_j.$$

(3) Simply

$$\begin{aligned}
U_1^j D_2^n \sigma_n = U_2^j D_1^n \sigma_n = \sigma_j \cdots \sigma_2 D_1^n \sigma_n = \sigma_j \cdots \sigma_3 D_1^n \sigma_1 \sigma_n = \dots \\
\dots = D_1^n \sigma_{j-1} \cdots \sigma_1 \sigma_n = D_1^n \sigma_n \sigma_{j-1} \cdots \sigma_1 = D_1^n \sigma_n U_1^{j-1}.
\end{aligned}$$

We remark that these equalities are easily understood with drawings.

(4) By induction. Notice first that

$$\begin{aligned}\sigma_i\sigma_{i+1}\sigma_{i+1}\sigma_i\sigma_{i+1}\sigma_{i+1} &= \sigma_i\sigma_{i+1}\sigma_i\sigma_{i+1}\sigma_i\sigma_{i+1} = \sigma_{i+1}\sigma_i\sigma_{i+1}\sigma_i\sigma_{i+1}\sigma_i\\ &= \sigma_{i+1}\sigma_{i+1}\sigma_i\sigma_{i+1}\sigma_{i+1}\sigma_i.\end{aligned}$$

For $n = 2$ we have

$$\begin{aligned}&(e+\sigma_1-\sigma_2\sigma_2\sigma_1-\sigma_1\sigma_2\sigma_2\sigma_1)(e-\sigma_2\sigma_2)\\ &\quad= e-\sigma_2\sigma_2+\sigma_1-\sigma_1\sigma_2\sigma_2-\sigma_2\sigma_2\sigma_1+\sigma_2\sigma_2\sigma_1\sigma_2\sigma_2-\sigma_1\sigma_2\sigma_2\sigma_1+\sigma_1\sigma_2\sigma_2\sigma_1\sigma_2\sigma_2\\ &\quad= e-\sigma_2\sigma_2+\sigma_1-\sigma_1\sigma_2\sigma_2-\sigma_2\sigma_2\sigma_1+\sigma_2\sigma_2\sigma_1\sigma_2\sigma_2-\sigma_1\sigma_2\sigma_2\sigma_1+\sigma_2\sigma_2\sigma_1\sigma_2\sigma_2\sigma_1\\ &\quad= (e-\sigma_2\sigma_2-\sigma_1\sigma_2\sigma_2+\sigma_2\sigma_2\sigma_1\sigma_2\sigma_2)(e+\sigma_1)\\ &\quad= (e-\sigma_2\sigma_2)(e-\sigma_1\sigma_2\sigma_2)(e+\sigma_1)\end{aligned}$$

Suppose the equality is true for n. Then

$$\begin{aligned}&(e+U_1^1+U_1^2+\cdots+U_1^n-D_{n+1}^{n+1}U_1^{n+1}-D_n^{n+1}U_1^{n+1}-\cdots-D_1^{n+1}U_1^{n+1})R_2^{n+1}\\ &\quad= R_2^{n+1}+(U_1^1+U_1^2+\cdots+U_1^n-D_{n+1}^{n+1}U_1^{n+1}-\cdots-D_2^{n+1}U_1^{n+1})R_2^{n+1}\\ &\qquad-D_1^{n+1}U_1^{n+1}R_2^{n+1}\\ &\quad= R_2^{n+1}+(e+U_2^2+\cdots+U_2^n-D_{n+1}^{n+1}U_2^{n+1}-\cdots-D_2^{n+1}U_2^{n+1})\sigma_1R_2^{n+1}\\ &\qquad-D_1^{n+1}U_1^{n+1}R_2^{n+1}\\ &\quad= R_2^{n+1}+(e+U_2^2+\cdots+U_2^n-D_{n+1}^{n+1}U_2^{n+1}-\cdots-D_2^{n+1}U_2^{n+1})\sigma_1R_3^{n+1}\\ &\qquad\times(e-D_2^{n+1}\sigma_{n+1})-R_2^{n+1}D_1^{n+1}U_1^{n+1}\ \text{(by 2)}\\ &\quad= R_2^{n+1}+(e+U_2^2+\cdots+U_2^n-D_{n+1}^{n+1}U_2^{n+1}-\cdots-D_2^{n+1}U_2^{n+1})R_3^{n+1}\sigma_1\\ &\qquad\times(e-D_2^{n+1}\sigma_{n+1})-R_2^{n+1}D_1^{n+1}U_1^{n+1}\ (R_3^{n+1}\in\mathbf{k}\mathbb{B}_{3\_n+2})\\ &\quad= R_2^{n+1}+\iota_{2\_(n+2)}((e+U_1^1+\cdots+U_1^{n-1}-D_n^nU_1^n-\cdots-D_1^nU_1^n)R_2^n)\sigma_1\\ &\qquad\times(e-D_2^{n+1}\sigma_{n+1})-R_2^{n+1}D_1^{n+1}U_1^{n+1}\\ &\quad= R_2^{n+1}+\iota_{2\_(n+2)}(R_1^n(e+U_1^1+U_1^2+\cdots+U_1^{n-1}))\sigma_1(e-D_2^{n+1}\sigma_{n+1})\\ &\qquad-R_2^{n+1}D_1^{n+1}U_1^{n+1}\ \text{(by IH)}\\ &\quad= R_2^{n+1}+R_2^{n+1}(e+U_2^2+U_2^3+\cdots+U_2^n)\sigma_1(e-D_2^{n+1}\sigma_{n+1})-R_2^{n+1}D_1^{n+1}U_1^{n+1}\\ &\quad= R_2^{n+1}[e+\sigma_1+U_2^2\sigma_1+\cdots+U_2^n\sigma_1-\sigma_1D_2^{n+1}\sigma_{n+1}\\ &\qquad-U_2^2\sigma_1D_2^{n+1}\sigma_{n+1}-\cdots-U_2^n\sigma_1D_2^{n+1}\sigma_{n+1}-D_1^{n+1}U_1^{n+1}]\end{aligned}$$

$$\begin{aligned}&= R_2^{n+1}(e+U_1^1+U_1^2+\cdots+U_1^n-D_1^{n+1}\sigma_{n+1}-U_1^2D_2^{n+1}\sigma_{n+1}-\cdots\\ &\qquad-U_1^nD_2^{n+1}\sigma_{n+1}-D_1^{n+1}\sigma_{n+1}U_1^n)\\ &= R_2^{n+1}(e+U_1^1+\cdots+U_1^n-D_1^{n+1}\sigma_{n+1}-D_1^{n+1}\sigma_{n+1}U_1^1-\cdots-D_1^{n+1}\sigma_{n+1}U_1^{n-1}\\ &\qquad-D_1^{n+1}\sigma_{n+1}U_1^n)\ \text{(by 3)}\\ &= R_2^{n+1}(e-D_1^{n+1}\sigma_{n+1})(e+U_1^1+U_1^2+\cdots+U_1^n)\\ &= R_1^{n+1}(e+U_1^1+U_1^2+\cdots+U_1^n).\end{aligned}$$

□

Proposition 2.2. $\mathbf{S}^{n+1}(e-U_1^n)(e-U_2^n)\cdots(e-U_n^n)=R_1^n\mathbf{S}^{n|1}$ *for* $n\geq 1$.

Proof. By induction, for $n=1$ being

$$\mathbf{S}^2(e-\sigma_1)=(e+\sigma_1)(e-\sigma_1)=e-\sigma_1\sigma_1.$$

If the equality holds for n, we have

$$\begin{aligned}
\mathbf{S}^{n+2}&(e-U_1^{n+1})(e-U_2^{n+1})\cdots(e-U_{n+1}^{n+1})\\
&=\mathbf{S}^{n+2}(e-U_2^{n+1})\cdots(e-U_{n+1}^{n+1})-\mathbf{S}^{n+2}U_1^{n+1}(e-U_2^{n+1})\cdots(e-U_{n+1}^{n+1})\\
&=\mathbf{T}_{1,n+1}\mathbf{S}^{1|n+1}(e-U_2^{n+1})\cdots(e-U_{n+1}^{n+1})\\
&\qquad-\mathbf{T}_{n+1,1}\mathbf{S}^{n+1|1}U_1^{n+1}(e-U_2^{n+1})\cdots(e-U_{n+1}^{n+1})\\
&=\mathbf{T}_{1,n+1}\mathbf{S}^{1|n+1}(e-U_2^{n+1})\cdots(e-U_{n+1}^{n+1})\\
&\qquad-\mathbf{T}_{n+1,1}U_1^{n+1}\mathbf{S}^{1|n+1}(e-U_2^{n+1})\cdots(e-U_{n+1}^{n+1})\ \text{(by 2.1,1)}\\
&=(\mathbf{T}_{1,n+1}-\mathbf{T}_{n+1,1}U_1^{n+1})\mathbf{S}^{1|n+1}(e-U_2^{n+1})\cdots(e-U_{n+1}^{n+1})\\
&=(\mathbf{T}_{1,n+1}-\mathbf{T}_{n+1,1}U_1^{n+1})\iota_{2_n+2}(\mathbf{S}^{n+1}(e-U_1^{n})\cdots(e-U_n^{n}))\\
&=(\mathbf{T}_{1,n+1}-\mathbf{T}_{n+1,1}U_1^{n+1})\iota_{2_n+2}(R_1^{n}\mathbf{S}^{n|1})\ \text{(by IH)}\\
&=(\mathbf{T}_{1,n+1}-\mathbf{T}_{n+1,1}U_1^{n+1})(R_2^{n+1}\mathbf{S}^{1|n|1})\\
&=(e+U_1^1+U_1^2+\cdots+U_1^{n+1}-U_1^{n+1}-D_{n+1}^{n+1}U_1^{n+1}-\cdots-D_1^{n+1}U_1^{n+1})\\
&\qquad\times R_2^{n+1}\mathbf{S}^{1|n|1}\\
&=(e+U_1^1+\cdots+U_1^{n}-D_{n+1}^{n+1}U_1^{n+1}-\cdots-D_1^{n+1}U_1^{n+1})R_2^{n+1}\mathbf{S}^{1|n|1}\\
&=R_1^{n+1}(e+U_1^1+\cdots+U_1^{n})\mathbf{S}^{1|n|1}\ \text{(by 2.1,4)}\\
&=R_1^{n+1}(\mathbf{T}_{1,n}|e_1)(\mathbf{S}^{1|n}|e_1)\quad (e_1\text{ the unique element of }\mathbb{B}_1)\\
&=R_1^{n+1}(\mathbf{S}^{n+1}|e_1)\\
&=R_1^{n+1}\mathbf{S}^{(n+1)|1}.
\end{aligned}$$

□

Definition 2.3. Let X be a vector space, $0\neq x\in X$ and $T\in\mathrm{End}(X)$ such that $T^n(x)=0$ for some n. The *nilpotency order* of T in x is the number $r+1$ such that $T^r(x)\neq 0$ and $T^{r+1}(x)=0$.

Definition 2.4. Let R be a braided Hopf algebra and $x\in R$. We denote by $\mathrm{Ad}_x\in\mathrm{End}(R)$ the (braided) adjoint of x, i.e.,

$$\mathrm{Ad}_x(y)=m(x_{(1)}\otimes m(c(\mathcal{S}(x_{(2)})\otimes y)),$$

where c is the braiding of R and m the multiplication map. Thus, if x is a primitive element, we have

$$\mathrm{Ad}_x(y)=xy-m(c(x\otimes y)).$$

The following result can be found in [R], but, as said in the introduction, we can obtain it directly from 2.2.

Theorem 2.5. *Let $x_1,x_2\in V$ be such that for some matrix (q_{ij}) the braiding verifies $c(x_i\otimes x_j)=q_{ij}x_j\otimes x_i$ for $i,j=1,2$. Let $N=N(q_{11})$ (see the beginning of 1.3) and let t be the least non-negative integer (if it exists) such that $q_{11}^t q_{12}q_{21}=1$. Let $r=\min\{t,N-1\}$. Then the nilpotency order of Ad_{x_1} on x_2 is exactly $r+1$.*

Proof. Let $n \in \mathbb{N}$. We consider $\mathrm{Ad}^n_{x_1}(x_2) = \mathbf{S}^{n+1}(\widetilde{\mathrm{Ad}}^n_{x_1}(x_2)) \in \mathfrak{B}(V)$, where $\widetilde{\mathrm{Ad}}$ is the adjoint in AV. It is easy to see by induction that this element is the action of the left hand side of 2.2 on $x_1^n x_2$. Now, the right hand side acts on $x_1^n x_2$ as a scalar, namely

$$(1-q_{12}q_{21})(1-q_{11}q_{12}q_{21})(1-q_{11}^2 q_{12}q_{21})\cdots(1-q_{11}^{n-1}q_{12}q_{21})(n)^!_{q_{11}}.$$

The assertion follows at once. □

Definition 2.6. 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 $B = \{x_1, \ldots, x_n\}$ is a basis of V, let $\{\partial_1, \ldots, \partial_n\}$ be the basis of V^* dual to B. We denote also by ∂_j, $j = 1, \ldots, n$ the operator ∂_{∂_j}. We warn that for the case $V \in {}^H_H\mathcal{YD}$, these are usually not morphisms in ${}^H_H\mathcal{YD}$, but only linear maps.

The following facts, which we shall use, are consequences of results in [G3].

Theorem 2.7. *Let $V = \oplus_{i=1}^n M(g_i, \rho_i) = \oplus_i V_i$, where $\rho_i \in \widehat{\Gamma_{g_i}}$. Let $q_i = \rho_i(g_i)$ (since g_i lies in the center of Γ_{g_i} and ρ_i is irreducible, $\rho_i(g_i)$ is a scalar) and let $N_i = N(q_i)$.*

(1) *Take a basis $\{z^i_{jl}\}$ of V as in 1.4.8 and $\{\partial^i_{jl}\}$ its dual basis. Let i, j, l be fixed, $K = \ker(\partial^i_{jl}) \subset \mathfrak{B}(V)$, and let $W = \mathrm{span}(x^i_{jl})$. Then for those i such that $N_i < \infty$ the multiplication map $K \otimes \mathfrak{B}(W) \to \mathfrak{B}(V)$ is an isomorphism. In particular, if $\{y_1, \ldots, y_k\}$ is a basis of K, then*

$$\{y_r (z^i_{jl})^s \mid 1 \le r \le k,\ 0 \le s < N_i\}$$

is a basis of $\mathfrak{B}(V)$.

(2) *If V is of finite Nichols rank, then*

$$N_i \mid \dim \mathfrak{B}(V_i) \mid \prod_i \dim \mathfrak{B}(V_i) \mid \dim \mathfrak{B}(V).$$

Furthermore, $\prod_i \dim \mathfrak{B}(V_i) = \dim \mathfrak{B}(V)$ iff $c_{ij} = \mathrm{id}_{V_i \otimes V_j}$ $\forall i \neq j$, where $c_{ij} = c|_{V_i \otimes V_j} : V_i \otimes V_j \to V_j \otimes V_i$.

(3) *$N_i^{\dim V_i} \le \dim \mathfrak{B}(V_i)$ $\forall i$. Furthermore, if $\{z^i_1, \ldots, z^i_{d_i}\}$ is a basis of V_i, then the set*

$$\{(z^1_1)^{i^1_1} \cdots (z^1_{d_1})^{i^1_{d_1}} (z^2_1)^{i^2_1} \cdots (z^n_{d_n})^{i^n_{d_n}} \mid 0 \le i^j_k < N_j\}$$

is linearly independent in $\mathfrak{B}(V)$.

This allows to give a relation between the dimension and the Nichols rank of a BP of finite group type:

Definition 2.8. Let $n = \prod_{i=1}^R p_i^{v_i}$, where p_i are distinct primes, $v_i > 0$ and $p_i > p_1$ for $i > 1$. We define $r(n) = \log_{p_1}(n)$.

Remark 2.9. Applying 2.7 part 1 together with part 3, we get that if $\dim \mathfrak{B}(V) = n$, then $d = \dim V \le r(n)$. Applying 2.7 part 2, we get that if $V = \oplus_{i=1}^\theta V_i = \oplus_i M(g_i, \rho_i) \in {}^{\mathbf{k}\Gamma}_{\mathbf{k}\Gamma}\mathcal{YD}$ and $n = \dim(\mathfrak{B}(V))$, $n = \prod_{i=1}^R p_i^{v_i}$, then $\theta \le \sum_i v_i$.

Definition 2.10. If (V,c) is of diagonal GT with basis $\{x_1, \ldots, x_n\}$ and matrix (q_{ij}), we say, following [AS1], that $\mathfrak{B}(V)$ is a *Quantum Linear Space* (or QLS) if $q_{ij}q_{ji} = 1$ for $i \neq j$. It is proved in [AS1] (and it is also a consequence of 2.7 part 2), that in this case $\dim \mathfrak{B}(V) = \prod N(q_{ii})$.

In [AS3] the authors associate to some Nichols algebras of diagonal GT a Frobenius–Lusztig kernel with the same dimension. This association can be done whenever $q_{ij}q_{ji} = q_{ii}^{a_{ij}}$ $\forall i, j$ for a matrix (a_{ij}) with entries in $\mathbb{Z}$, where (q_{ij}) is the matrix of the braiding. The following proposition deals with general rank-2 Nichols algebras.

Proposition 2.11. *Let (V, c) be a 2 dimensional BP of finite GT (and thus of diagonal GT), with basis $\{x_1, x_2\}$ and matrix (q_{ij}), and let $N_j = N(q_{jj})$ for $j = 1, 2$. As in 2.5, let $r+1$ be nilpotency order of Ad_{x_2} on x_1. For $1 \le i \le r$ let $M_i = N(q_{11}(q_{12}q_{21})^i q_{22}^{i^2})$. Then*

$$\dim \mathfrak{B}(V) \ge N_1 N_2 \prod_{1\le i\le r} M_i.$$

Furthermore, suppose that the nilpotency order of Ad_{x_1} on x_2 is 2. We have:

1. *If $r = 1$ then the equality holds.*
2. *If $r = 2$, and $N(q_{11}) \ne 2$ or $N(q_{22}) \ne 3$ then the equality holds.*
3. *If $r = 2$, $N(q_{11}) = 2$ and $N(q_{22}) = 3$ then the equality holds if and only if*

$$q_{12}q_{21} = -1, \text{ or } q_{12}q_{21} = q_{22}, \text{ or } q_{12}q_{21} = -q_{22}.$$

Proof. Let $z_1 = \mathrm{Ad}_{x_2}(x_1) = x_2x_1 - q_{21}x_1x_2$, and define inductively $z_{i+1} = \mathrm{Ad}_{x_2}(z_i) = x_2z_i - q_{21}q_{22}^i z_i x_2$. Taking on $\mathfrak{B}(V)$ the bi-degree given by $\deg(x_1) = (1, 0)$, $\deg(x_2) = (0, 1)$, we have $z_i \in \mathfrak{B}^{1,i}(V)$. Furthermore, it is proved in 2.5 that $z_r \ne 0$ and $z_{r+1} = 0$. It is immediate to see by induction (it follows also from 2.2) that $\partial_{x_2}(z_i) = 0$, and $\partial_{x_1}(z_i) = d_{12}^1 d_{12}^2 \cdots d_{12}^i x_2^i$, where $d_{12}^j = (1 - q_{12}q_{21}q_{22}^{j-1})$. Thus, $\partial_{x_2}^i \partial_{x_1}(z_i) \ne 0$ if $i \le r$. We shall prove that the set $\{x_1^{n_1} z_1^{m_1} \cdots z_r^{m_r} \mid 0 \le n_1 < N_1,\ 0 \le m_i < M_i\}$ is linearly independent. To see this, we compute

$$\begin{aligned}
\partial_{x_2}^i \partial_{x_1}(z_i^m) &= \sum_{j=0}^{m-1} q_{12}^{ji} q_{11}^j d_{12}^1 \cdots d_{12}^j \partial_{x_2}^i (z_i^{m-1-j} x_2^i z_i^j) \\
&= d_{12}^1 \cdots d_{12}^j \sum_{j=0}^{m-1} q_{12}^{ji} q_{11}^j q_{21}^{ji} q_{22}^{ji^2} (i)_{q_{22}}^! \, z_i^{m-1} \\
&= d_{12}^1 \cdots d_{12}^j (m)_{q_{11} q_{12}^i q_{21}^i q_{22}^{i^2}} \, z_i^{m-1},
\end{aligned}$$

from where $z_i^m \ne 0$ if $m < N(q_{11}q_{12}^i q_{21}^i q_{22}^{i^2}) = M_i$. It is clear also that if $j > i$ then $\partial_{x_2}^j \partial_{x_1}(z_i^m) = 0$. Suppose inductively that for $s < r$, the set

$$\{x_1^{n_1} z_1^{m_1} \cdots z_s^{m_s} \mid 0 \le n_1 < N_1,\ 0 \le m_i < M_i\}$$

is linearly independent. Then we have that if there were a linear combination

$$\sum \alpha_{n_1, m_1, \ldots, m_{s+1}} x_1^{n_1} z_1^{m_1} \cdots z_{s+1}^{m_{s+1}} = 0,$$

we would get, applying $(\partial_{x_2}^{s+1} \partial_{x_1})^{M_{s+1}-1}$, a linear combination

$$\sum \tilde{\alpha}_{n_1, m_1, \ldots, m_s, M_{s+1}-1} x_1^{n_1} z_1^{m_1} \cdots z_s^{m_s} = 0,$$

where the $\tilde{\alpha}$'s are the α's multiplied by non-zero factors. By the inductive hypothesis, we have that $\alpha_{n_1, m_1, \ldots, m_s, M_{s+1}-1} = 0$. We apply now $[\partial_{x_2}^{s+1} \partial_{x_1}]^{M_{s+1}-2}$ and get that $\alpha_{n_1, m_1, \ldots, m_s, M_{s+1}-2} = 0$. Continuing in this way, we get that

$\alpha_{n_1,m_1,\dots,m_s,m_{s+1}} = 0$ for all m_{s+1}, proving the inductive thesis. Now the assertion follows at once noting that this set lies in $\ker(\partial_{x_2})$, and then by 2.7 part 1 the set

$$\{x_1^{n_1} z_1^{m_1} \cdots z_r^{m_r} x_2^{n_2} \mid 0 \le n_i < N_i,\ 0 \le m_i < M_i\} \tag{2.12}$$

is linearly independent in $\mathfrak{B}(V)$. Notice that we have not proved that $z_i^{M_i} = 0$.

Now, for the nilpotency order of Ad_{x_1} on x_2 to be 2 it can happen that $q_{11} = -1$ or that $q_{11}q_{12}q_{21} = 1$. In the first case we have $x_1^2 = 0$, and then

$$z_1 x_1 = -q_{21} x_1 x_2 x_1 = q_{11} q_{21} x_1 z_1.$$

In the second case it is easy to see using derivations that we also have

$$z_1 x_1 = q_{11} q_{21} x_1 z_1,$$

for ∂_{x_2} annihilates and ∂_{x_1} gives the same element in $\mathfrak{B}(V)$ when applied to both sides of the equality.

We consider now the three cases in the statement.

(1) We have $0 = \mathrm{Ad}_{x_2}(z_1) = x_2 z_1 - q_{21} q_{22} z_1 x_2$, whence $x_2 z_1 = q_{21} q_{22} z_1 x_2$. These equalities show how to write any monomial in $\mathfrak{B}(V)$ as a combination of the elements of the set $\{x_1^{n_1} z_1^{m_1} x_2^{n_2}\}$, from where we shall have $\dim \mathfrak{B}(V) \le N_1 N_2 M_1$ once we prove that $z_1^{M_1} = 0$, which we will do at the end of the proof.

(2) We have $z_2 = \mathrm{Ad}_{x_2}(z_1) = x_2 z_1 - q_{21} q_{22} z_1 x_2$, and hence

$$0 = \mathrm{Ad}_{x_2}(z_2) = x_2 z_2 - q_{21} q_{22}^2 z_2 x_2.$$

It can be seen, using derivations, that $z_2 x_1 = q_{21}^2 q_{11} x_1 z_2 + (q_{11} - q_{22}) q_{21} z_1^2$. Furthermore, it can also be seen that $z_2 z_1 = q_{11} q_{12} q_{21}^2 q_{22}^2 z_1 z_2$. We conclude now as in the previous case, since these equalities show how to write any monomial as a combination of those of (2.12).

(3) The same computations as in the previous case hold here, except for the relation between $z_2 z_1$ and $z_1 z_2$. We are looking for the condition on the matrix for (2.12) to be a basis of $\mathfrak{B}(V)$. For this to happen, we must be able to write $z_2 z_1$ as a linear combination of those elements; but now, the bi-degree of $z_2 z_1$ is $(3,2)$ and, moreover, it lies in the kernel of ∂_{x_2}. By 2.7 part 1, we have to write $z_2 z_1$ as a combination of the elements in (2.12) of bi-degree $(3,2)$ which also lie in $\ker \partial_{x_2}$, but there is only one such element: $z_1 z_2$. Hence we should have $z_2 z_1 = \lambda z_1 z_2$. Taking ∂_{x_1} in both sides, we are led to the equations

$$\begin{aligned} -\lambda(1-t) t q_{12} q_{22}^2 &= (1-t)(1+t-q_{22}t^2), \\ \lambda(1-t)(1-qt) &= -(1-t)(1-qt) t q_{21} q_{22}^2, \end{aligned}$$

for $t = q_{12} q_{21}$. Since $(1-t) \ne 0$ and $(1-qt) \ne 0$, these equations are equivalent to

$$0 = 1 + t - q_{22} t^2 - q_{22} t^3 = q_{22}(1+t)(q_{22} - t)(q_{22} + t),$$

from where the conditions we stated are clear.

We shall prove now that in these cases $z_i^{M_i} = 0$ for $i = 1, 2$. For this, we shall use that for $n \ge k \ge 0$ we have

$$\sum_{i=k}^{n} \mathbf{q}^i \binom{i}{k}_{\mathbf{q}} = \mathbf{q}^k \binom{n+1}{k+1}_{\mathbf{q}}, \tag{2.13}$$

which can easily be proved using that $\mathbf{q}^{n-i}\binom{n}{i}_{\mathbf{q}}+\binom{n}{i+1}_{\mathbf{q}}=\binom{n+1}{i+1}_{\mathbf{q}}$. We know that $\partial_2(z_i^n)=0\ \forall n>0$, and then we must prove that $\partial_1(z_i^{M_i})=0$. Let $Q_i=q_{11}(q_{12}q_{21})^i q_{22}^{i^2}$ (then $M_i=N(Q_i)$). Suppose $r=2$. We have, using the Leibniz rule for ∂_1 and the identities proved above,

$$\begin{aligned}
\partial_1(z_1^{M_1}) &= d_{12}^1\sum_{i=0}^{M_1-1}(q_{11}q_{12})^i z_1^{M_1-i-1}x_2z_1^i\\
&= d_{12}^1\sum_{i=0}^{M_1-1}(q_{11}q_{12})^i\left[(q_{21}q_{22})^i z_1^{M_1-1}x_2+\sum_{j=0}^{i-1}(q_{21}q_{22})^j z_1^{M_1-i+j-1}z_2z_1^{i-j-1}\right]\\
&= d_{12}^1\sum_{i=0}^{M_1-1}Q_1^i z_1^{M_1-1}x_1+d_{12}^1\sum_{0\le j<i\le M_1-1}Q_1^{2i-j-1}(q_{21}q_{22})^{-1}z_1^{M_1-2}z_2\\
&= d_{12}^1(M_1)_{Q_1}\,z_1^{M_1-1}x_1+d_{12}^1(q_{21}q_{22})^{-1}\Big(\sum_{i=0}^{M_1-1}Q_1^i(i)_{Q_1}\Big)z_1^{M_1-2}z_2\\
&= 0+d_{12}^1(q_{21}q_{22})^{-1}Q_1\binom{M_1}{2}_{Q_1}z_1^{M_1-2}z_2=0 \qquad \text{(by (2.13))},
\end{aligned}$$

since it is easy to see that if $M_1=2$ then $z_2=0$. If $r=1$ then $z_2=0$ and the same computation works. For $z_2^{M_2}$, we have

$$\begin{aligned}
\partial_1(z_2^{M_2}) &= d_{12}^1d_{12}^2\sum_{i=0}^{M_2-1}(q_{11}q_{12}^2)^i z_2^{M_2-i-1}x_2^2z_2^i = d_{12}^1d_{12}^2\sum_{i=0}^{M_2-1}Q_2^i z_2^{M_2-1}x_2^2\\
&= d_{12}^1d_{12}^2(M_2)_{Q_2}\,z_2^{M_2-1}x_2^2=0.
\end{aligned}$$

□

Remark 2.14. For (V,c) a BP of diagonal GT, let the matrix a_{ij} be defined by $a_{ii}=2$ and $a_{ij}=1-d_{ij}$ for $i\neq j$, with d_{ij} the nilpotency order of Ad_{x_i} on x_j. This is a generalized Cartan matrix. The proposition shows that if (a_{ij}) is of type A_2 then a PBW basis can be constructed for the Nichols algebra $\mathfrak{B}(V)$ in the same way as for Frobenius–Lusztig kernels of type A_2, though these matrices are not of Cartan type in general. It is natural to ask to what extent this method allows to compute the Nichols algebras as generalizations of Frobenius–Lusztig kernels. In part 3 we show that this does not give the general answer, and we find the conditions for this method to work in the case of type B_2.

Concrete examples of these algebras over specific groups can be found in [N, §3]. There, the author presents algebras over abelian groups, all of which can be computed with 2.11. For instance, if $\Gamma=C_4$ the cyclic group of order 4 with generator σ, take $V=M(\sigma,\chi)\oplus M(\sigma^2,\chi)$, where $i=\chi(\sigma)$ is a primitive fourth root of unity. Then the matrix of c is $\begin{pmatrix}-1 & i\\ -1 & i\end{pmatrix}$. Here $N_1=2$, $N_2=4$, $r=1$ and the nilpotency order of Ad_{x_1} on x_2 is 2. Then $\mathfrak{B}(V)$ is of type A_2, and $M_1=N(-1)=2$, whence $\dim\mathfrak{B}(V)=16$. The pointed Hopf algebra $\mathfrak{B}(V)\#\mathbf{k}C_4$ is hence 64-dimensional. As another example, borrowed from [N], take $\Gamma=C_6$ with generator σ, and take $V=M(\sigma,\chi^3)\oplus(\sigma,\chi^2)$, where $N(\chi(\sigma))=6$, i.e. χ is a generator of $\widehat{\Gamma}$. Then the matrix of c is $\begin{pmatrix} -1 & \omega \\ -1 & \omega \end{pmatrix}$, where $\omega = \chi^2(\sigma)$ is a third root of unity. This braiding is of type B_2 and fits in the part 3 of the proposition, with $q_{12}q_{21} = -q_{22}$. We have $N_1 = 2$, $N_2 = 3$, $M_1 = 3$, $M_2 = 2$, and hence $\mathfrak{B}(V)$ is 36 dimensional. More examples can be found in [G1].

3. On the non-diagonal case

We give some necessary conditions a Yetter–Drinfeld module over a finite group algebra must verify to produce a finite dimensional Nichols algebra. As said in 1.4.10, such a module is of group type. We want, however, to keep track of the structure of the group.

Lemma 3.1. *Let Γ be a finite group, $g \in \Gamma$ and $\rho \in \widehat{\Gamma_g}$ an irreducible representation of Γ_g. Let $q = \rho(g)$ (as noticed in 2.7, it is a scalar) and let $N = N(q)$. Let $V = M(g, \rho)$ and suppose V is of finite Nichols rank. Then*

1. *if $\deg \rho \geq 3$ then $N = 2$ (i.e. $q = -1$);*
2. *if $\deg \rho = 2$ then $2 \leq N \leq 3$ (i.e. $q = -1$ or it is a third root of unity).*

Proof. Let W be the space of the representation ρ. For $x \in W$ we denote also by x the element $1 \otimes x \in \operatorname{Ind}_{\Gamma_g}^{\Gamma} W = V$. Let $\{x_1, \dots, x_d\}$ be a basis of W. We have $\delta(x) = g \otimes x \ \forall x \in W$, and hence $c(x_i \otimes x_j) = g \rightharpoonup x_j \otimes x_i = q x_j \otimes x_i$. We have an inclusion $\mathfrak{B}(W) \hookrightarrow \mathfrak{B}(V)$ (in fact, $\mathfrak{B}(V)$ is free as a right $\mathfrak{B}(W)$-module by [G3, Th. 3.11]) and hence $\mathfrak{B}(W)$ is finite dimensional. Now, W is of diagonal GT with matrix (q_{ij}), $q_{ij} = q \ \forall i, j$, and thus it is of Cartan type. Hence, the Cartan matrix of this braiding has 2 in the main diagonal and $2 - N$ outside the main diagonal. Since by a result of Lusztig (see [AS2, Thm. 3.1]) this matrix must correspond to a finite datum, the condition on N follows. □

As a consequence of this, we see that Nichols algebras which do not come from the abelian case are usually infinite dimensional. In the same vein, we have the following result which appeared as a conjecture in a former version of [AS2].

Proposition 3.2. *If Γ has odd order, then there are finitely many modules in ${}^{\mathbf{k}\Gamma}_{\mathbf{k}\Gamma}\mathcal{YD}$ of finite Nichols rank.*

Proof. Since ${}^{\mathbf{k}\Gamma}_{\mathbf{k}\Gamma}\mathcal{YD}$ has a finite number of simple modules up to isomorphism, it is enough to see that each simple module $M(g, \rho)$ can appear no more than n times (n depending on $M(g, \rho)$) in a module V for it to be of finite Nichols rank. Let then W be the space affording ρ, $0 \neq x \in W$ and q such that $g \rightharpoonup x = qx$. Suppose $V = n \cdot M(g, \rho) + \cdots$ $(n > 0)$. Then we take $Y = \operatorname{span}\{x_1, \dots, x_n\}$, where x_i is the element of the i-th copy of $M(g, \rho)$ corresponding to x. It is immediate to see that Y is of diagonal GT with matrix (q_{ij}), $q_{ij} = q \ \forall i, j$. Now, $q \neq 1$ since $M(g, \rho)$ is of finite Nichols rank (since so is V), and $q \neq -1$ since Γ is of odd order. The same argument as in the previous lemma tells that $1 \leq n \leq 2$ if $N(q) = 3$ and $n = 1$ if $N(q) > 3$. □

Without the odd-order assumption the result is known to be false (for instance, for $\Gamma = C_2$).

Let now Γ be a finite group and $\mathcal{O}_g$ the conjugacy class of $g \in \Gamma$. Let $\rho : \Gamma_g \to \operatorname{Aut}(W)$ be an irreducible representation, and take a basis of $M(g, \rho)$ as follows: let $\{h_1, \dots, h_s\}$ be a set of representatives of left cosets of Γ/Γ_g and let $\{x_1,\dots,x_r\}$ be a basis of W. We consider the basis $\{z_{jl}=h_j\otimes x_l\}$. By the definition of the braiding, it is useful to take into account the way in which $\mathcal{O}_g$ acts on itself by conjugation. To do this, we name $t_i=h_igh_i^{-1}$ and define the morphism

$$f_g:\Gamma\to\mathbb{S}_s,\quad f_g(k)(i)=j \text{ if } kt_ik^{-1}=t_j.$$

Notice that $f_g(k)$ fixes i iff k commutes with t_i; in particular $f_g(t_i)(i)=i$ for all i.

Remark 3.3. Let $f:G\to H$ be a morphism between two groups. For $g\in G$, the conjugacy class $\mathcal{O}_g$ has cardinality the index $s=[G:G_g]$. Let $\tilde{G}=f^{-1}H_{f(g)}$. It is straightforward to see that the set $f(\mathcal{O}_g)$ has cardinality the index $n=[G:\tilde{G}]$ and that for any $h\in f(\mathcal{O}_g)$ the fiber $f^{-1}(h)\cap\mathcal{O}_g$ has cardinality the index $m=[\tilde{G}:G_g]$, whence the cardinality of the orbit $\mathcal{O}_g$ can be factorized by $s=nm$.

Remark 3.4. Let $V=M(g,\rho)$ where $\rho:\Gamma_g\to\mathrm{Aut}(W)$ and let $x\in W$. Let $q=\rho(g)$ (as noticed in 2.7, g acts by a scalar, on W). In particular, $c(x\otimes x)=g\rightharpoonup x\otimes x=qx\otimes x$. Let $t\notin\Gamma_g$ and $y=t\rightharpoonup x$. Thus $\delta(y)=tgt^{-1}\otimes y$ and tgt^{-1} acts on y by q, since

$$tgt^{-1}\rightharpoonup y=tgt^{-1}t\rightharpoonup x=tg\rightharpoonup x=qt\rightharpoonup x=qy.$$

Thus, $c(y\otimes y)=qy\otimes y$.

The preceding paragraphs suggest a different approach for classifying braided pairs of finite group type, as follows:

Definition 3.5. Let X be a finite set and $\triangleright:X\times X\to X$ a function. We say that $(X,\triangleright)$ is a *crossed set* if

(1) for each $i\in X$, the function $i\triangleright\bullet:X\to X$, $j\mapsto i\triangleright j$, is a bijection,
(2) $i\triangleright i=i$ $\forall i\in X$,
(3) $j\triangleright i=i$ whenever $i\triangleright j=j$, and
(4) $i\triangleright(j\triangleright k)=(i\triangleright j)\triangleright(i\triangleright k)$ $\forall i,j,k\in X$.

The example we come from is X being a union of conjugacy classes of a finite group Γ and $\triangleright$ the conjugation, $i\triangleright j=iji^{-1}$.

A crossed set provides a set-theoretical solution to the Braid Equation by

$$c:X\times X\to X\times X,\quad c(i,j)=(i\triangleright j,i). \tag{3.6}$$

We remark that c being a solution to the Braid Equation is equivalent to the condition 4 in the above definition. The condition 1 is given to guarantee the bijectivity of c, and the conditions 2 and 3 are necessary conditions for X to be "injective", in the language of [So].

Notice that any set-theoretical solution to the Braid Equation c gives rise to a (set-theoretic) representation of the braid group $\mathbb{B}_n$, namely, $X^n=X\times\cdots\times X$ (n times), where σ_i acts by c in the coordinates i and $i+1$.

Although [So, LYZ] consider more general set-theoretical solutions, in both articles the authors prove that any bijective solution $(i,j)\mapsto({}^ij,i^j)$ is, in some sense, equivalent to a solution as in (3.6). Specifically, for any solution $\tilde{c}$ there exists a solution c as in (3.6) and a collection of bijective maps $J_n:X^n\to X^n$ which intertwine the representations of $\mathbb{B}_n$ associated to $\tilde{c}$ and c.

Let $(X, \triangleright)$ be a crossed set and $n \geq 0$. We define $C^n(X) := \{f : X^n \to \mathbf{k}^\times\}$ (X^0 is a singleton). Let $\delta^n : C^n(X) \to C^{n+1}(X)$ be given by

$$\delta^0 = 0$$

$$\delta^n(f)(x_0, \dots, x_n) = \prod_{i=0}^{n-1} f(x_0, \dots, x_{i-1}, x_{i+1}, \dots, x_n)^{(-1)^i} \times f(x_0, \dots, x_{i-1}, x_i \triangleright x_{i+1}, \dots, x_i \triangleright x_n)^{(-1)^{i+1}}.$$

It is easy to prove that $(C^\bullet(X), \delta)$ is a cochain complex (we remark that an analog definition for a general set-theoretical solution of the Braid Equation does not yield a complex). We define then the cohomology $H^n(X) = H^n(C^\bullet(X), \delta) = \ker(\delta^n)/\operatorname{Im}(\delta^{n-1})$.

Let $f \in C^2(X)$. We define a map $c^f : \mathbf{k}X \otimes \mathbf{k}X \to \mathbf{k}X \otimes \mathbf{k}X$ by

$$c^f(i \otimes j) = f(i, j) i \triangleright j \otimes i,$$

and extend it linearly. We denote by $\text{Braidings}(X)$ the subset

$$\text{Braidings}(X) = \{f \in C^2(X) \mid c^f \text{ verifies the Braid Equation}\}.$$

We then have

Proposition 3.7. *Let $(X, \triangleright)$ be a crossed set and $(C^n(X), \delta)$ be given as before. Then*

1. *$H^1(X) = \mathbf{k}^{\pi_0(X)}$, where $\pi_0(X)$ is the set of equivalence classes of the relation generated by $j \sim i \triangleright j$.*
2. *$H^2(X) = \text{Braidings}(X)$ modulo change of basis of the form $i \mapsto \lambda_i i$ for $\lambda_i \in \mathbf{k}^\times$ $\forall i \in X$.*

Proof. Straightforward (see [G4]). □

Notice that we always have an inclusion $\mathbf{k}^\times \hookrightarrow H^2(X)$ by $q \mapsto (f(i,j) = q)$.

Lemma 3.8. *Let $(X, \triangleright)$ be a crossed set and f a 2-cocycle in $C^2(X)$. If f takes values on the roots of unity then $(\mathbf{k}X, c)$ is of finite GT.*

Proof. We have to prove that the group-likes associated with the basis X of $\mathbf{k}X$ generate a finite group. These group-likes are nothing but $g_i \in GL(\mathbf{k}X)$, $g_i(j) = f(i,j) i \triangleright j$. Let $N_{ij} = N(f(i,j))$, let N be the least common multiple of the N_{ij}'s and let $G \subset \mathbf{k}^\times$ be the group of N-roots of unity. Let $Y = X \times G$ and $\mathbb{S}_Y$ the symmetric group on the (finite) set Y. It is clear then that there is an inclusion of the group generated by the g_i's into $\mathbb{S}_Y$. □

We can state 3.4 in this setting: if f is a 2-cocycle and $k \triangleright i = j$, then we have $f(i,i) = f(j,j)$. To see this, just compute

$$1 = \delta(f)(k, i, i) = f(i,i) f(j,j)^{-1} f(k,i)^{-1} f(k,i).$$

4. Rank 3 Nichols algebras

In this section we show that if V is a 3-dimensional BP of GT, then it is either of diagonal GT or $V \simeq V_{3,q}$, q a root of unity (we give the definition of $V_{3,q}$ in 4.1).

Let (V, c) be a 3-dimensional BP of group type which is not of abelian group type. Let $\{\bar{x}_0, \bar{x}_1, \bar{x}_2\}$ be a basis as in (1.4.11) and $g_i \in \mathrm{GL}(V)$ the associated automorphisms ($i = 0, 1, 2$). If two of the g_i's were equal then (V, c) would be of abelian GT. For, suppose $g_1 = g_2$. If $g_0 = g_1$, the assertion is obvious. If not, $g_0(\bar{x}_1) \in \operatorname{span}\{\bar{x}_0\}$ or $g_0(\bar{x}_1) \in \operatorname{span}\{\bar{x}_1, \bar{x}_2\}$. In the first case, we have $g_0 g_1 g_0^{-1} = g_0$ (which would imply that $g_0 = g_1$), while in the second case we have $g_0 g_1 g_0^{-1} = g_1$ (which would imply that g_0 commutes with g_1 and hence the assertion). Therefore, $\#\{g_0, g_1, g_2\} = 3$. Consider now the subindices of the g_i's and the x_i's to be in $\mathbb{Z}/3$. We have $g_i g_j g_i^{-1} = g_{-i-j}$, for if not we would fall in one of the contradictions of before. Furthermore, (1.4.13) implies that $c(\bar{x}_i \otimes \bar{x}_j) = f(i,j)\bar{x}_{-i-j} \otimes \bar{x}_i$ for some $f : \{0,1,2\} \times \{0,1,2\} \to \mathbf{k}^\times$. That is, (V,c) can be constructed as in 3.5. Take $q = f(0,0)$ (i.e., $g_0(\bar{x}_0) = q\bar{x}_0$), and define $x_0 = \bar{x}_0$, $qx_1 = g_2(x_0)$, $qx_2 = g_0(x_1)$. Then it can be seen by hand that $c(x_i \otimes x_j) = qx_{-i-j} \otimes x_i$. To see this, we must compute $g_r(x_s)$ for $r, s \in \mathbb{Z}/3$, but this can be accomplished just by using the definition of the x_i's and the relations $g_i g_j g_i^{-1} = g_{-i-j}$. Alternatively, we can verify that $H^2(X) = \mathbf{k}^\times$ for $X = \mathbb{Z}/3$ and $i \triangleright j = -i-j$.

Definition 4.1. We denote this space by $V_{3,q}$. That is, $V_{3,q}$ has a basis $\{x_0, x_1, x_2\}$ (the subindices in $\mathbb{Z}/3$) and the braiding is given by

$$c(x_i \otimes x_j) = qx_{-i-j} \otimes x_i.$$

Notice that $c^3 = q^3$, from where the eigenvalues of c belong to $\{q, \xi q, \xi^2 q\}$ for ξ a root of unity of order 3.

As a consequence, we have a classification of 3-dimensional BP of group type:

Lemma 4.2. *Let (V,c) be a 3-dimensional BP of GT. Then either*

- *(V,c) is of abelian GT, or*
- *$(V,c) = V_{3,q}$ for some $q \in \mathbf{k}^\times$.*

Then, if Γ is a finite group and $V \in {}^{\mathbf{k}\Gamma}_{\mathbf{k}\Gamma}\mathcal{YD}$ is 3-dimensional, we have a basis $\{x_0, x_1, x_2\}$ such that either

- *$c(x_i \otimes x_j) = q_{ij} x_j \otimes x_i$ for roots of unity q_{ij}, or*
- *$c(x_i \otimes x_j) = qx_{-i-j} \otimes x_i$ (the subindices in $\mathbb{Z}/3$) for q a root of unity.*

The algebra $\mathfrak{B}(V_{3,-1})$ has been studied in [MS] and is also included in [AG]; it is 12-dimensional and can be presented with generators $\{x_0, x_1, x_2\}$ and relations

$$x_i^2 = 0 \ (i = 0,1,2), \quad x_0x_1 + x_1x_2 + x_2x_0 = 0, \quad x_0x_2 + x_1x_0 + x_2x_1 = 0.$$

Let q be a root of unity of order 3. By the remarks given above on the eigenvalues of c, the morphism $1 + c$ is injective, and hence $\mathfrak{B}^2(V_{3,q})$ has dimension 9. Since the image of ∂_0 restricted to $\mathfrak{B}^2(V_{3,q})$ has dimension 3, its kernel has dimension 6. Furthermore, 2.7 part 3 says that the set $\{x_1^i x_2^j, 0 \le i,j < 3,\ i+j > 2\}$ is linearly independent and it is clearly contained in $\ker \partial_0$. Taking into account the vectors $1, x_1, x_2$ which lie also in $\ker \partial_0$, we see that the Hilbert polynomial of $\ker \partial_0$ has coefficients greater or equal to $P(t) = 1 + 2t + 6t^2 + 2t^3 + t^4$, and then 2.7 part 1 says that $\dim \mathfrak{B}(V_{3,q}) \ge 3P(1) = 36$.

Remark 4.3. By 2.7 part 3, $\dim(\mathfrak{B}(V_{3,q})) \ge N(q)^3$, but the same result says that the equality does not hold. In fact, $\dim(\mathfrak{B}(V_{3,-1})) > N(-1)^3$. Suppose then $q \neq -1$. If we had $\dim(\mathfrak{B}(V_{3,q})) = N(q)^3$, then 2.7 part 3 would tell that $\dim \mathfrak{B}^2(V_{3,1}) = 6$, or equivalently, that $\dim \ker \mathbf{S}^2 = 3$. This is easily seen to be false, since for $N(q) \neq 6$ we have $\ker \mathbf{S}^2 = \ker(1+c) = \{0\}$, and for $N(q) = 6$ we have

$$\ker \mathbf{S}^2 = \operatorname{span}\{x_0x_1 - qx_2x_0 + q^2x_1x_2,\ x_1x_0 - qx_2x_1 + q^2x_0x_2\}.$$

The unique Nichols algebra of rank 3 which does not come from the abelian case and whose dimension is < 32 is hence $\mathfrak{B}(V_{3,-1})$. In particular, by 2.7 part 3 we see that it is the lowest dimensional Nichols algebra which does not come from the abelian case.

5. Rank 4 Nichols algebras

We classify now 4-dimensional braided pairs of finite GT. Let $V \in {}^{\mathbf{k}\Gamma}_{\mathbf{k}\Gamma}\mathcal{YD}$ be 4-dimensional and suppose $V = \oplus_i M_i = \oplus_i M(g_i, \rho_i)$ is its decomposition as a sum of irreducible modules.

If $M(g,\rho)$ is 2-dimensional, then it is of abelian GT. If it is 1-dimensional then g is central in Γ. Thus, a sum of 1-dimensional modules and at most one 2-dimensional module in ${}^{\mathbf{k}\Gamma}_{\mathbf{k}\Gamma}\mathcal{YD}$ is of abelian GT. We have the following possibilities:

1. $4 = 1+1+1+1$, i.e. a sum of four 1-dimensional modules. It is of abelian GT.
2. $4 = 1+1+2$, it is also of abelian GT.
3. $4 = 1+3$. If the module of dimension 3 is of abelian GT, then V is of abelian GT. The possibility we must consider is that the 3-dimensional module be $V_{3,q}$ for some q.
4. $4 = 2+2$. Here V is of abelian GT unless ρ_1 and ρ_2 be characters and g_1 do not commute with g_2.
5. $4 = 4$. $V = M(g,\rho)$ is irreducible. There are three sub-cases:
   (a) g is central and $\deg\rho = 4$. It is of abelian GT (furthermore, by 3.1, $\rho(g) = -1$ and $\dim\mathfrak{B}(V) = 16$).
   (b) $[\Gamma : \Gamma_g] = 2$ and $\deg\rho = 2$. It is of abelian GT (furthermore, by 3.1, $N(\rho(g)) = 2$ or 3. If $N(\rho(g)) = 3$ we have by 2.7 part 2 that $\dim\mathfrak{B}(V) \geq 27^2$).
   (c) $[\Gamma : \Gamma_g] = 4$ and ρ is a character.

We consider as before the situations which are not of abelian GT.

5.1. **Case 3.** Let $V = V_1 \oplus V_{3,q}$ with $\dim V_1 = 1$, $V_1 = M(g,\chi)$. By 2.7 part 2, we have

$$\dim\mathfrak{B}(V) \geq \dim\mathfrak{B}(V_1)\dim\mathfrak{B}(V_{3,q}) \geq 36$$

unless $\chi(g) = q = -1$, case in which $\dim\mathfrak{B}(V) \geq 24$. We denote by χ', g' the character and the element of Γ giving $V_{3,-1}$, i.e. $V = M(g,\chi) \oplus M(g',\chi')$. Since g is central, it acts on $V_{3,-1}$ by a scalar, say q_{12}. We denote $q_{21} = \chi(g')$. Let $\sigma := q_{12}q_{21}$. By 2.7 part 2, $\dim\mathfrak{B}(V) = 24$ iff $\sigma = 1$. If $\sigma \neq 1$, we consider x a generator of the space affording χ and x_0, x_1, x_2 a basis of $M(g',\chi')$ as in section 4, and define for $i = 0,1,2$

$$z_i = \mathrm{Ad}_{x_i}(x) = x_i x - q_{21} x x_i.$$

Let $N = N(\sigma)$. It is straightforward (though tedious) to see, using derivations, that the set

$$\{x^i z_0^{j_0} \mid 0 \leq i < 2,\ 0 \leq j_0 < N\}$$

is linearly independent. With this, we see also using derivations that the set

$$\{x^i z_0^{j_0} z_1^{j_1} \mid 0 \leq i < 2,\ 0 \leq j_0, j_1 < N\}$$

is linearly independent, and finally we see that the set

$$\{x^i z_0^{j_0} z_1^{j_1} z_2^{j_2} \mid 0 \leq i < 2,\ 0 \leq j_0, j_1, j_2 < N\}$$

is linearly independent. Furthermore, it is clear that this set is contained in K, the intersection of the kernels of $\partial_{x_0}, \partial_{x_1}, \partial_{x_2}$. Thus, by 2.7 part 1 (taking $W = V_{3,q}$), we see that $\dim \mathfrak{B}(V) \geq 2N^3 \times 12 \geq 192$. Henceforth, in section 6 we shall not consider these cases, except for $\sigma = 1$.

5.2. **Case 4.** We have $V = M_1 \oplus M_2 = M(g_1, \rho_1) \oplus M(g_2, \rho_2)$, ρ_1, ρ_2 are characters, g_1, g_2 do not commute, and $[\Gamma : \Gamma_{g_1}] = [\Gamma : \Gamma_{g_2}] = 2$. Let $g_1' = g_2 g_1 g_2^{-1}$, $g_2' = g_1 g_2 g_1^{-1}$. The conjugacy class of g_i is then $\{g_i, g_i'\}$ and, by [AG, Lemma 3.1.9], $[g_i, g_i'] = 1$. Let H be the subgroup of Γ generated by g_1, g_1', which is commutative. Let $\sigma \in \operatorname{Aut} H$ be the restriction of the adjoint $\sigma(h) = g_2 h g_2^{-1}$. We have $\sigma^2 = \mathrm{id}$, and let $t = g_1' g_1^{-1}$. Notice that

$$g_2' = g_1 g_2 g_1^{-1} = g_2 g_2^{-1} g_1 g_2 g_1^{-1} = g_2 g_1' g_1^{-1} = g_2 t,$$
$$g_2 = g_1 g_2' g_1^{-1} = g_2' g_1' g_1^{-1} = g_2' t = g_2 t^2,$$

whence $t^2 = 1$. Let then $q_1 = \rho_1(g_1)$, $q_2 = \rho_2(g_2)$, $\eta_1 = \rho_1(t)$, $\eta_2 = \rho_2(t)$ (thus $\eta_1 = \pm 1$, $\eta_2 = \pm 1$), and $\alpha_1 = \rho_1(g_2^2)$, $\alpha_2 = \rho_2(g_1^2)$. We have then the bases $\{x_1, x_1' = g_2 \rightharpoonup x_1\}$ for M_1 and $\{x_2, x_2' = g_1 \rightharpoonup x_2\}$ for M_2, and the braidings are given respectively by

$$\text{matrix of } c \text{ in } M_1 = \begin{pmatrix} q_1 & \eta_1 q_1 \\ \eta_1 q_1 & q_1 \end{pmatrix}, \qquad \text{matrix of } c \text{ in } M_2 = \begin{pmatrix} q_2 & \eta_2 q_2 \\ \eta_2 q_2 & q_2 \end{pmatrix},$$

and on the other monomials the braiding acts as

$$\begin{aligned} c(x_1 \otimes x_2) &= x_2' \otimes x_1, & c(x_2 \otimes x_1) &= x_1' \otimes x_2, \\ c(x_1 \otimes x_2') &= \alpha_2 x_2 \otimes x_1, & c(x_2 \otimes x_1') &= \alpha_1 x_1 \otimes x_2, \\ c(x_1' \otimes x_2) &= \eta_2 x_2' \otimes x_1', & c(x_2' \otimes x_1) &= \eta_1 x_1' \otimes x_2', \\ c(x_1' \otimes x_2') &= \eta_2 \alpha_2 x_2 \otimes x_1', & c(x_2' \otimes x_1') &= \eta_1 \alpha_1 x_1 \otimes x_2'. \end{aligned}$$

We notice that, as in the proof of 3.1, the modules M_i $(i = 1, 2)$ are of Cartan type with associated matrices $\begin{pmatrix} 2 & 2 - N_i \\ 2 - N_i & 2 \end{pmatrix}$, where $N_i = N(q_i)$. Thus $\mathfrak{B}(V)$ is infinite dimensional if $N_1 > 3$ or $N_2 > 3$. Furthermore, if $N_1 = 3$ then $\mathfrak{B}(M_1)$ has dimension 27 and analogously for M_2, whence, by 2.7 part 2, if $N_1 > 2$ or $N_2 > 2$ then $\dim \mathfrak{B}(V) \geq 4 \times 27 = 108$.

We then consider $q_1 = q_2 = -1$. There are two cases: $(\eta_1, \eta_2) = (1, 1)$ and $(\eta_1, \eta_2) \neq (1, 1)$. In the case $(\eta_1, \eta_2) = (1, 1)$, we define for $\epsilon = \pm 1$ the vectors

$$z_\epsilon = \sqrt{\alpha_1} x_1 + \epsilon x_1', \quad z_\epsilon' = \sqrt{\alpha_2} x_2 + \epsilon x_2',$$

which give a basis of V. It is straightforward to compute the braiding in this basis, which is given by

$$\begin{aligned} c(z_\epsilon \otimes z_{\epsilon'}) &= -z_{\epsilon'} \otimes z_\epsilon, \\ c(z_\epsilon \otimes z_{\epsilon'}') &= \sqrt{\alpha_2} \epsilon' z_{\epsilon'}' \otimes z_\epsilon, \\ c(z_{\epsilon'}' \otimes z_\epsilon) &= \sqrt{\alpha_1} \epsilon z_\epsilon \otimes z_{\epsilon'}', \\ c(z_\epsilon' \otimes z_{\epsilon'}') &= -z_{\epsilon'}' \otimes z_\epsilon', \end{aligned}$$

from where we see that $\mathfrak{B}(V)$ comes from the abelian case. If we take as a subspace $M_{\epsilon,\epsilon'}$ to be the linear span of $\{z_\epsilon, z_{\epsilon'}'\}$ we have that the braiding has the matrix

$\begin{pmatrix} -1 & \sqrt{\alpha_2}\epsilon' \\ \sqrt{\alpha_1}\epsilon & -1 \end{pmatrix}$. By virtue of 2.11, $\mathfrak{B}(M_{\epsilon,\epsilon'})$ has dimension $4N(\epsilon\epsilon'\sqrt{\alpha_1}\sqrt{\alpha_2})$, from where

$$\dim(\mathfrak{B}(V)) \geq \dim(\mathfrak{B}(M_{\epsilon,\epsilon'}))\dim(\mathfrak{B}(M_{-\epsilon,-\epsilon'})) = 16(N(\epsilon\epsilon'\sqrt{\alpha_1}\sqrt{\alpha_2}))^2 \geq 64,$$

taking ϵ, ϵ' in such a way that $\epsilon\epsilon'\sqrt{\alpha_1}\sqrt{\alpha_2} \neq 1$. Thus we will not be interested in these algebras in section 6.

Remark 5.2.1. A Nichols algebra as these can be found in [MS], where the authors consider a 4-dimensional Yetter–Drinfeld module over $\mathbf{k}\mathbb{D}_4$ which can be decomposed as a sum of two 2-dimensional ones. That algebra is associated to the constants $q_1 = q_2 = -1$, $\eta_1 = \eta_2 = 1$, $\alpha_1 = \alpha_2 = 1$. It can be seen taking $M_{+,-}$ and $M_{-,+}$ that each $\mathfrak{B}(M_{\pm,\mp})$ is of type A_2 and hence 8-dimensional, and that for the elements of $M_{\pm,\mp} \otimes M_{\mp,\pm}$ the braiding verifies $c^2 = \mathrm{id}$, from where, by 2.7 part 2, $\dim\mathfrak{B}(V) = 64$.

If $(\eta_1, \eta_2) \neq (1, 1)$, we suppose $\eta_1 = -1$ (if $(\eta_1, \eta_2) = (1, -1)$ we interchange M_1 and M_2). We take z'_ϵ as before, and define

$$t_+ = \mathrm{Ad}_{x_1} z'_+ = x_1 z'_+ - \sqrt{\alpha_1} z'_+ x_1,$$
$$t_- = \mathrm{Ad}_{x_1} z'_- = x_1 z'_- + \sqrt{\alpha_1} z'_- x_1.$$

It is straightforward (but tedious) to see using derivations that t_+, t_- are linearly independent, and that the set $\{t_+^{i_+} t_-^{i_-} (z'_+)^{j_+} (z'_-)'^{j_-} \mid 0 \leq i_+, i_-, j_+, j_- < 2\}$ is l.i. too. Since this set is contained in $\ker \partial_{x_1} \cap \ker \partial_{x'_1}$, it is immediate by a generalization of 2.7 part 1 (see [G3]) that the set

$$\{t_+^{i_+} t_-^{i_-} (z'_+)^{j_+} (z'_-)^{j_-} (x_1)^{t_1} (x'_1)^{t_2} \mid 0 \leq i_+, i_-, j_+, j_-, t_1, t_2 < 2\}$$

is linearly independent, whence $\dim\mathfrak{B}(V) \geq 64$. Hence, in section 6 we shall not consider these algebras.

5.3. **Case 5c.** We have $V = M(g, \rho)$, with $\mathcal{O}_g = \{t_0 = g, t_1, t_2, t_3\}$ and ρ a character. We consider as in the paragraph preceding 3.3, $f_g : \Gamma \to \mathbb{S}_4$. By 3.3 we have that the cardinality of $f_g(\mathcal{O}_g)$ may be $1, 2, 4$. If $\# f_g(\mathcal{O}_g) = 1$ then $\mathcal{O}_g$ generates a commutative subgroup and hence V is of abelian GT.

If $\# f_g(\mathcal{O}_g) = 2$ we may index the t_i's in such a way that

$$f_g(t_0) = f_g(t_1) = (2\ 3), \qquad f_g(t_2) = f_g(t_3) = (0\ 1)$$

(since $f_g(t_0) = f_g(t_1)$ then t_0 commutes with t_1, whence either $f_g(t_0) = \mathrm{id}$ –which would imply $\# f_g(\mathcal{O}_g) = 1$– or $f_g(t_0) = (2\ 3)$. Analogously for $f_g(t_2)$.). Let $h \in \Gamma$ be such that $h t_0 h^{-1} = t_2$; then $f_g(h)(0) = 2$. It is easy to see (multiplying h by the t_i's on both sides if necessary) that $\exists h' \in \Gamma$ such that $f_g(h') = (0\ 2)(1\ 3)$. Let x_0 be a generator of the space affording ρ, $x_1 = t_2 \rightharpoonup x_0$, $x_2 = h' \rightharpoonup x_0$, $x_3 = t_0 h' \rightharpoonup x_0$. It is straightforward to see that $\mathfrak{B}(V)$ is a particular case of the algebras of 5.2. In fact, if $q = \rho(t_0)$, $\eta = \rho(t_0^{-1} t_1)$ and $\alpha = \rho(t_2^2)$ then $\mathfrak{B}(V) \simeq \mathfrak{B}(M_{q,q,\eta,\eta,\alpha,\alpha})$, and then $\dim\mathfrak{B}(V) \geq 64$. We shall not consider them in section 6.

If $\# f_g(\mathcal{O}_g) = 4$, then $f_g(t_i)$ fixes i and does not fix j for $j \neq i$, and then it is a tri-cycle. We may index the t_i's in such a way that $f_g(t_0) = (1\ 2\ 3)$. It can be seen that the hypothesis $f_g(t_1) = (0\ 2\ 3)$ leads to a contradiction, and thence we have $f_g(t_1) = (0\ 3\ 2)$. This implies $f_g(t_2) = (0\ 1\ 3)$ and $f_g(t_3) = (0\ 2\ 1)$. Take $h = t_2 t_1 t_0^{-2}$. Then $f_g(h) = \mathrm{id}$, and thus h commutes with $\mathcal{O}_g$ (notice that for the same reason t_i^3 commutes with $\mathcal{O}_g$ for $i=0,1,2,3$). We note that $t_1^3 = t_2 t_0^3 t_2^{-1} = t_0^3$, and in the same way we see that $t_i^3 = t_j^3$. Notice also that

$$\begin{aligned} h &= t_2 t_1 t_0^{-2} = t_0^{-2} t_0^2 (t_2 t_1) t_0^{-2} = t_0^{-2} t_1 t_3, \text{ and} \\ h^2 &= t_0^{-2} t_1 t_3 t_2 t_1 t_0^{-2} = t_0^{-2} t_1 t_3 t_2 t_3^{-2} t_1 = t_0^{-2} t_1 t_1 t_3 t_3^{-2} t_1 \\ &= t_0^{-2} t_1^2 t_3^{-1} t_1 = t_0^{-2} t_0^{-1} t_1^2 t_1 = t_0^{-3} t_1^3 = 1. \end{aligned}$$

Take x_0 a generator of the space affording ρ, let $q=\rho(g)$ and take $qx_1 = t_2 \rightharpoonup x_0$, $qx_2 = t_0 \rightharpoonup x_1$, $qx_3 = t_0 \rightharpoonup x_2$. Let $\alpha = \rho(h) = \pm 1$; we compute

$$\begin{aligned}
& t_0 \rightharpoonup x_0 = qx_0, \quad t_0 \rightharpoonup x_1 = qx_2, \quad t_0 \rightharpoonup x_2 = qx_3, \\
& t_0 \rightharpoonup x_3 = q^{-2} t_0^3 \rightharpoonup x_1 = q^{-3} t_0^3 t_2 \rightharpoonup x_0 = q^{-3} t_2 t_0^3 \rightharpoonup x_0 = t_2 \rightharpoonup x_0 = qx_1, \\
& t_1 \rightharpoonup x_0 = t_0^2 t_2 t_0^{-2} \rightharpoonup x_0 = q^{-2} t_0^2 t_2 \rightharpoonup x_0 = q^{-1} t_0^2 \rightharpoonup x_1 = qx_3, \\
& t_1 \rightharpoonup x_1 = qx_1 \text{ by 3.4}, \\
& t_1 \rightharpoonup x_2 = t_2^{-1} t_2 t_1 t_0^{-2} t_0^2 \rightharpoonup x_2 = q^2 t_2^{-1} h \rightharpoonup x_1 = q^2 \alpha t_2^{-1} \rightharpoonup x_1 = q\alpha x_0, \\
& t_1 \rightharpoonup x_3 = t_0^2 t_0^{-2} t_1 t_3 t_3^{-1} \rightharpoonup x_3 = q^{-1} \alpha t_0^2 \rightharpoonup x_3 = q\alpha x_2, \\
& t_2 \rightharpoonup x_0 = qx_1, \\
& t_2 \rightharpoonup x_1 = t_2 t_1 t_0^{-2} t_0^2 t_1^{-1} \rightharpoonup x_1 = q^{-1} t_2 t_1 t_0^{-2} t_0^2 \rightharpoonup x_1 = q\alpha x_3, \\
& t_2 \rightharpoonup x_2 = qx_2 \text{ by 3.4}, \\
& t_2 \rightharpoonup x_3 = t_2^3 t_2^{-2} \rightharpoonup x_3 = q^{-1} \alpha^{-1} t_2^3 t_2^{-1} \rightharpoonup x_1 = q^{-2} \alpha^{-1} t_2^3 \rightharpoonup x_0 \\
& \qquad = q^{-2} \alpha t_0^3 \rightharpoonup x_0 = q\alpha x_0, \\
& t_3 \rightharpoonup x_0 = t_0 t_2 t_0^{-1} \rightharpoonup x_0 = t_0 \rightharpoonup x_1 = qx_2, \\
& t_3 \rightharpoonup x_1 = t_0 t_2 t_0^{-1} \rightharpoonup x_1 = q^{-1} t_0 t_2 \rightharpoonup x_3 = \alpha t_0 \rightharpoonup x_0 = q\alpha x_0, \\
& t_3 \rightharpoonup x_2 = t_0 t_2 t_0^{-1} \rightharpoonup x_2 = q^{-1} t_0 t_2 \rightharpoonup x_1 = \alpha t_0 \rightharpoonup x_3 = q\alpha x_1, \\
& t_3 \rightharpoonup x_3 = qx_3 \text{ by 3.4}.
\end{aligned}$$

We shall denote by $V_{4,q,\alpha}$ the 4-dimensional module generated by $\{x_0, x_1, x_2, x_3\}$ with the braiding of above. By 2.7 part 3, we have $\dim(\mathfrak{B}(V_{4,q,\alpha})) \geq 81$ if $N(q) \geq 3$, whence we will be interested in the case $q=-1$.

5.3.2. If $\alpha = -1$, it is easy to see that for $V_{4,-1,-1}$ the restriction of c to the linear span of $\{x_i \otimes x_j \mid i \neq j\}$ verifies $c^3 = 1$, from where

$$\ker \mathbf{S}^2 = \ker(1+c) = \operatorname{span}\{x_i^2,\ i=0,1,2,3\}.$$

This implies that $\dim \mathfrak{B}^2(V_{4,-1,-1}) = 12$. Now, since the image of the map $\partial_0 : \mathfrak{B}^2(V_{4,-1,-1}) \to \mathfrak{B}^1(V_{4,-1,-1})$ is 3-dimensional (we have $x_0 \notin \operatorname{Im}(\partial_0)$ because $x_0^2 = 0$), we have $\dim(\ker(\partial_0) \cap \mathfrak{B}^2(V_{4,-1,-1})) = 9$. Thus, the Hilbert polynomial of $\mathfrak{B}(V_{4,-1,-1})$ verifies

$$P_{\mathfrak{B}(V_{4,-1,-1})}(t) \geq (1+t)(1+3t+9t^2+3t^3+t^4)$$

by virtue of 2, whence $\dim \mathfrak{B}(V_{4,-1,-1}) \geq 34$. We shall not consider this algebra in section 6.

For the module $V_{4,-1,1}$, it is easy to find the relations in degree 2:

$$\begin{aligned} &x_i^2 = 0,\ i = 0,1,2,3 \\ &x_0x_1 + x_2x_0 + x_1x_2 = 0, \\ &x_0x_2 + x_3x_0 + x_2x_3 = 0, \\ &x_0x_3 + x_1x_0 + x_3x_1 = 0, \\ &x_1x_3 + x_2x_1 + x_3x_2 = 0. \end{aligned}$$

With the order $x_0 > x_1 > x_2 > x_3$, to give a Gröbner basis of the ideal generated we have to add the relations

$$\begin{aligned} &x_1x_2x_1 - x_2x_1x_2 = 0, \\ &x_2x_3x_2 - x_3x_2x_3 = 0. \end{aligned}$$

It is not so easy[3] to see that there is one more relation for $\mathfrak{B}(V_{4,-1,1})$:

$$x_2x_3x_4x_2x_3x_4 + x_3x_4x_2x_3x_4x_2 + x_4x_2x_3x_4x_2x_3 = 0.$$

With this, it is straightforward (though a little bit tedious) to see that the dimension of $\mathfrak{B}^i(V_{4,-1,1})$ is $1,4,8,11,12,12,11,8,4,1$ for $i = 0,1,2,3,4,5,6,7,8,9$ respectively, and hence $\dim(\mathfrak{B}(V_{4,-1,1})) = 72$. We thus shall not consider this algebra.

6. Classification of Nichols algebras of dimension < 32

The Nichols algebras (and also their liftings) of dimension p and p^2 are classified in [G3]. We shall consider now the other possibilities.

Let (V,c) be a BP of finite GT with Nichols rank p^3. We have $r(n) = 3$ (see 2.8 for the definition of $r(n)$), from where $\dim V \le 3$. By the results in section 4, V is of abelian GT, for, if not, we would have $V = V_{3,q}$, but then by 2.7 part 2, $N(q) = p$ and by 4.3, the Nichols rank of V would be $> p^3$, a contradiction. Hence, if $\dim V = 3$, $\mathfrak{B}(V)$ is a QLS because of 2.7 part 2, i.e., V has a basis $\{x_1,x_2,x_3\}$ such that the set $\{x_1^{n_1}x_2^{n_2}x_3^{n_3} \mid 0 \le n_i < p\}$ 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 2.11 we have two possibilities:

(1) $p = 2$ and $q_{12}q_{21} \ne 1$. Furthermore, for $\mathfrak{B}(V)$ to be 8-dimensional we must have $q_{12}q_{21} = -1$. 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 also $q_{12}q_{21}q_{11} = 1$, whence $q_{11} = q_{22}$ and $\mathfrak{B}(V)$ is also 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 $\{x_1^{m_1}z^nx_2^{m_2} \mid 0 \le m_1,m_2,n < p\}$, $z = x_2x_1 - q_{21}x_1x_2$. The last case to be considered 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 $\mathfrak{B}(V) = \mathbf{k}[x]/(x^{p^3})$.

We then have proved:

---

[3] I used a computer program by E. Müller [Mü] to see that there should be one more relation in degree 6.

Theorem 6.1. *Let (V, c) be a BP of finite group type with Nichols rank p^3 (p a prime number). Then V is of diagonal GT and it fits in one of the following possibilities:*

$\dim V$	*Type*
3	*QLS*, $N(q_{11}) = N(q_{22}) = N(q_{33}) = p$
2	*QLS*, $N(q_{11}) = p,\ N(q_{22}) = p^2$
2	$A_2,\ q_{11} = q_{22} = (q_{12}q_{21})^{-1},\ N(q_{11}) = p$
1	*QLS*, $N(q_{11}) = p^3$

□

Let $n = p_1p_2$ a product of two distinct primes such that $p_1 < p_2 < p_1^2$. Then $r(n) < 3$, whence $\dim V \leq 2$ and it is of abelian GT. If $\dim V = 2$ and c has matrix $\begin{pmatrix} q_{11} & q_{12} \\ q_{21} & q_{22} \end{pmatrix}$, then by 2.7 part 2 we must have (reversing the basis if necessary) $N(q_{11}) = p_1$, $N(q_{22}) = p_2$, and $q_{12}q_{21} = 1$, i.e., $\mathfrak{B}(V)$ is a QLS with PBW basis $\{x_1^{m_1}x_2^{m_2} \mid 0 \leq m_i < p_i,\ i = 1, 2\}$. If $\dim V = 1$ then as before x generates V, $c(x \otimes x) = qx \otimes x$ with $N(q) = p_1p_2$ and $\mathfrak{B}(V) = \mathbf{k}[x]/(x^{p_1p_2})$.

Since we have computed the dimension of $\mathfrak{B}(V_{3,-1})$, together with the fact that we have shown that $\dim \mathfrak{B}(V_{3,q}) \geq 32$ if $q \neq -1$ and $\dim \mathfrak{B}(V) \geq 32$ for V a 4-dimensional BP of finite GT which is not of abelian GT, this last argument applies also for $p_1 = 2$ and $p_2 < 16$ (i.e., $n = 10$, $n = 14$, $n = 22$ and $n = 26$). In these cases, if $\dim V$ were 3, then V would be of abelian GT because if not $V = V_{3,-1}$, which would give a Nichols algebra of dimension 12, a contradiction. Then remark 2.9 applies and $\dim V \leq 2$.

We have hence the classification of the Nichols algebras of dimensions $1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 13, 14, 15, 17, 19, 21, 22, 23, 25, 26, 27, 29, 31$. For the remaining dimensions it is routine to make the computations, and we refer to [G4]. The result can be stated as follows:

Type	Dimensions
QLS, rank 1	All dimensions
QLS, rank 2	$\neq p$
QLS, rank 3	8, 12, 16, 18, 20, 24, 27, 28, 30
QLS, rank 4	16, 24
A_2	8, 12, 16, 20, 27, 28
$A_2 \times A_1$	16, 24
$V_{3,-1}$	12
$V_{3,-1} \times A_1$	24

When applying the lifting procedure, the computations in the previous section are the first step in order to classify pointed Hopf algebras of index < 32. The following lemmas, which can be proved as in [AS4, Lemma 7.2] or [G1, §7] and are referred to [G4], show that any such Hopf algebra is generated by group-likes and skew-primitive elements, completing the second step of the procedure.

Lemma 6.2. *Let $(V = (x_1, x_2), c)$ be an BP of abelian GT with matrix (q_{ij}), and suppose* $\dim \mathfrak{B}(V) < 32$. *If S is a graded braided Hopf algebra between TV and $\mathfrak{B}(V)$, i.e.*

$$TV \twoheadrightarrow S \twoheadrightarrow \mathfrak{B}(V),$$

with graded maps and categorical maps (that is, there exists a braided category such that TV, S and $\mathfrak{B}(V)$ belong to it and the projections are maps in the category), then either $S = \mathfrak{B}(V)$ or $\dim S \geq 32$. □

Lemma 6.3. *Let S be a finite dimensional graded braided Hopf algebra with graded maps $T(V_{3,-1}) \twoheadrightarrow S \overset{p}{\twoheadrightarrow} \mathfrak{B}(V_{3,-1})$. Then p is an isomorphism.* □

References

[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 `q-alg 9802074`.

[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] ______ & ______, *Finite quantum groups and Cartan matrices*, to appear in Adv. Math.

[AS3] ______ & ______, *Lifting of Nichols algebras of type A_2 and Pointed Hopf algebras of order p^4*, in "Hopf algebras and quantum groups", Proceedings of the colloquium in Brussels 1998, ed. Caenepeel, 1–18.

[AS4] ______ & ______, *Finite quantum groups over abelian groups of prime exponent*, (1999), preprint. Available at `www.mate.uncor.edu/andrus/articulos.html`.

[B] M. Beattie *An isomorphism theorem for Ore extension Hopf algebras*, to appear in Comm. Alg.

[BDG] M. Beattie, S. Dăscălescu & L. Grünenfelder, *On the number of types of finite-dimensional Hopf algebras*, Inventiones Math. **136** (1999), 1–7.

[CD] S. Caenepeel & S. Dăscălescu, *Pointed Hopf algebras of dimension p^3*, J. Algebra **209** (1998), 622–634.

[CDR] S. Caenepeel, S. Dăscălescu & Ş. Raianu, *Classifying pointed Hopf algebras of dimension 16*, to appear in Comm. Alg.

[CiRo] C. Cibils & M. Rosso, *Algèbres des chemins quantiques*, Adv. in Math. **125** (1997), 171–199.

[CuRe] C.W. Curtis & I. Reiner, *Methods of representation theory*, volume II. J. Wiley, 1994.

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

[DPR] R. Dijkgraaf, V. Pasquier & P. Roche, *Quasi Hopf algebras, group cohomology and orbifold models*, Integrable systems and quantum groups. Ed: M. Carfora et al., Papers from the workshop, Pavia, Italy, March, (1990). Singapore: World Scientific. 75–98.

[FK] S. Fomin & A. Kirillov, *Quadratic algebras, Dunkl elements, and Schubert calculus*, Advances in geometry, J.-L. Brylinski (Ed.), Progress in Mathematics **172**, (1998) Birkäuser.

[Ge] S. Gelaki, *On pointed Hopf algebras and Kaplansky's tenth conjecture*, J.Algebra, **209** (1998), 635–657.

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

[G2] ______, *On pointed Hopf algebras of dimension p^5*, to appear in Glasgow Math. J.

[G3] ______, *A freeness theorem for Nichols algebras*, to appear in J. Algebra.

[G4] ______, *Doctoral Thesis*, in preparation.

[LYZ] Jiang-Hua Lu, Min Yan & Yong-Chang Zhu, *On Set-theoretical Yang–Baxter equation*, to appear in Duke Math. J.

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

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

[Mü] E. Müller, *A computer program for Nichols algebras*, available at `www.mate.uncor.edu/andrus/articulos`

[N] W.D. Nichols, *Bialgebras of type one*, Comm. in Alg. **6** (1978), 1521–1552.

[R] M. Rosso, *Quantum groups and quantum shuffles*, Inventiones Math. **133** (1998), 399–416.

[S] B. Scharfschwerdt, talk at *Colloquium on quantum groups and Hopf algebras*, La Falda (1999).

[So] A. Soloviev, *Non-unitary set-theoretical solutions to the quantum Yang–Baxter equation*, `q-alg 0003194`.

[SvO] D. Stefan & F. van Oystaeyen, *Hochschild cohomology and coradical filtration of pointed Hopf algebras*, J. Algebra **210** (1998), 535–556.

[T1] M. Takeuchi, *The coquasitriangular Hopf algebra associated with a rigid Yang–Baxter coalgebra*, in "Hopf algebras and quantum groups", Proceedings of the colloquium in Brussels 1998, ed. Caenepeel.

[T2] ———, *The Nichols–Zoeller theorem for braided Hopf algebras*, preprint.

[W] S. J. Witherspoon, *The representation ring of the quantum double of a finite group*, J. Algebra **179** (1996), 305–329.

Matías Graña
Depto. de Matemática
Pab I, FCEyN, Ciudad Universitaria
(1428) Buenos Aires, Argentina
E-mail address: matiasg@dm.uba.ar