Finite Quantum Groups and Cartan Matrices

Nicolás Andruskiewitsch and Hans-Jürgen Schneider

February 2, 2000

Abstract. We consider a class of Hopf algebras having as an invariant a generalized Cartan matrix. For a Hopf algebra of this kind, we prove that it is finite dimensional if and only if its generalized Cartan matrix is actually a finite Cartan matrix (under some mild hypothesis). These results allow to classify all the finite dimensional coradically graded pointed Hopf algebras whose coradical has odd prime dimension p. We also characterize coradically graded pointed Hopf algebras of order p^4.

§1. Introduction.

We shall work over an algebraically closed field $\Bbbk$ of characteristic 0. In this article, we are concerned with the classification problem of finite dimensional pointed Hopf algebras over $\Bbbk$. Our references for the theory of Hopf algebras are [Mo1], [Sw].

1.1 The general method. Let us recall that a Hopf algebra is *pointed* if all its simple subcoalgebras are one-dimensional, that is spanned by a group-like element. The class of pointed Hopf algebras includes many important examples such as group algebras, enveloping algebras, quantized enveloping algebras and Frobenius-Lusztig kernels. In fact, any Hopf algebra generated by group-like and skew-primitive elements is pointed.

Finite dimensional cocommutative Hopf algebras over $\Bbbk$ are necessarily group algebras; it is also known that pointed semisimple Hopf algebras are just group algebras. The main known examples of finite dimensional pointed and non-cocommutative Hopf algebras are the Frobenius-Lusztig kernels [L1], [L2].

Recently, the classification problem of finite dimensional Hopf algebras, or according to Drinfeld, finite quantum groups, attracted the interest of many specialists. Whereas there were several important contributions in the semisimple case (see the survey [Mo2]), only few results are known in the non-semisimple case. Pointed non-semisimple Hopf algebras of dimension p^3 are classified in [AS2], [CD], [SvO]; infinite families of pointed non-semisimple Hopf algebras of dimension p^4 were constructed in [AS2], [BDG], [G]. The full classification was worked out for some small dimensions– see [Mo2]; also, pointed Hopf algebras of order 16 and 32 were respectively classified in [CDR], [Gr1]. Still less is known in the non-pointed non-semisimple case, see however [AS1].

This work was partially supported by CONICET, CONICOR, DAAD, the Graduiertenkolleg of the Math. Institut (Universität München), TWAS (Trieste) and Secyt (UNC).

Our approach to the classification problem is in the spirit of Lie theory and is based on our previous paper [AS2], which can be viewed as a continuation of the work of Nichols [N].

Let A be a pointed Hopf algebra, let Γ be the group of its group-like elements and let $A_0 = \Bbbk\Gamma \subseteq A_1 \subseteq \dots$ be its coradical filtration. Then the associated graded coalgebra $\operatorname{gr} A = \oplus_{n\geq 0} \operatorname{gr} A(n)$ is a pointed graded Hopf algebra; $\Bbbk\Gamma \simeq \operatorname{gr} A(0)$ is a Hopf subalgebra and the projection $\pi : \operatorname{gr} A \to \operatorname{gr} A(0)$ with kernel $\oplus_{n>0} \operatorname{gr} A(n)$, is a Hopf algebra map and a retraction of the inclusion. Let R be the algebra of coinvariants of π.

We denote by ${}^{\Bbbk\Gamma}_{\Bbbk\Gamma}\mathcal{YD}$ the braided category of Yetter-Drinfeld modules over $\Bbbk\Gamma$, see [Mo1]. Yetter-Drinfeld modules over Γ were already considered by Whitehead under the name of "crossed Γ-modules".

Then R is a braided Hopf algebra in ${}^{\Bbbk\Gamma}_{\Bbbk\Gamma}\mathcal{YD}$ and $\operatorname{gr} A$ can be reconstructed from R and $\Bbbk\Gamma$ as a biproduct [Ra]:

$$\operatorname{gr} A \simeq R\#\Bbbk\Gamma.$$

This reconstruction is called bosonization, see [Mj1]. The passage from A to the biproduct $R\#\Bbbk\Gamma$ is a substitute of the well-known Cartier-Kostant-Milnor-Moore theorem for cocommutative Hopf algebras. Notice that in the finite dimensional case, $\dim A = \dim \operatorname{gr} A = \dim R \operatorname{ord} \Gamma$.

The "infinitesimal part" R satisfies the following conditions:

(1.1) $R = \oplus_{n\geq 0} R(n)$ is a graded braided Hopf algebra.
(1.2) $R(0) = \Bbbk 1$ (hence the coradical is trivial, *cf.* [Sw, Chapter 11]).
(1.3) $R(1) = P(R)$ (the space of primitive elements of R).

A first rough invariant of such R is the dimension of $P(R)$ and we call this the *rank* of R. It is in general not true that a braided Hopf algebra R satisfying (1.1), (1.2) and (1.3) also satisfies

(1.4) R is generated as an algebra over $\Bbbk$ by $R(1)$.

The subalgebra R' of R generated by $R(1)$, a Hopf subalgebra of R satisfying (1.1), (1.2), (1.3) and (1.4), is an invariant of our initial Hopf algebra A. We call a braided Hopf algebra satisfying (1.1), (1.2), (1.3) and (1.4) a *Nichols algebra* since the notion appears for the first time in the article [N]. It can be shown that a Nichols algebra with prescribed space of primitive elements is unique up to isomorphisms; that is, the notions of "Nichols algebra" and "Yetter-Drinfeld module" are naturally equivalent. We shall denote by $\mathfrak{B}(V)$ the Nichols algebra whose space of primitive elements is isomorphic to the Yetter-Drinfeld module V.

This notion, or the related one of "quantum shuffle algebras" was considered by several authors under various presentations; see [L3], [Mü], [Ro2], [Ro3], [CR], [Rz], [BD], [Sbg], [W]. We refer to the survey article [AG] for details and further references.

Now we can describe our method for classifying finite dimensional pointed Hopf algebras over $\Bbbk$. We fix a finite group Γ. Then

(a) Determine all finite dimensional Yetter-Drinfeld modules V over Γ such that $\mathfrak{B}(V)$ is finite dimensional.
(b) For V as in step (a), compute the braided Hopf algebra $\mathfrak{B}(V)$.

(c) For $\mathfrak{B}(V)$ as in step (b), compute all Hopf algebras A such that $\operatorname{gr} A \simeq \mathfrak{B}(V)\#\Bbbk\Gamma$ ("lifting") up to isomorphism.
(d) Investigate whether any finite dimensional braided Hopf algebra R in ${}^{\Bbbk\Gamma}_{\Bbbk\Gamma}\mathcal{YD}$ satisfying (1.1), (1.2) and (1.3) is generated by its primitive elements, that is also fulfills (1.4).

As to step (a), it is in general very difficult to decide when $\mathfrak{B}(V)$ is finite dimensional since an efficient description of the defining relations of $\mathfrak{B}(V)$ is not known. Step (c) should be possible once the answer to step (b) is known, as the experience seems to indicate [AS2]. Condition (d) means that any pointed finite dimensional Hopf algebra with coradical $\Bbbk\Gamma$ is generated by group-like and skew-primitive elements.

In this paper we mainly contribute to (a) and (d).

1.2 The main results. Let us assume from now on that Γ is a fixed finite abelian group. A finite dimensional Yetter-Drinfeld module V over $\Bbbk\Gamma$ admits a basis x_1, ..., x_θ such that, for some elements $g(1), \dots, g(\theta) \in \Gamma$, $\chi(1), \dots, \chi(\theta) \in \widehat{\Gamma}$, the action and coaction of Γ are given by

$$h.x_j = \chi(j)(h)x_j, \qquad \delta(x_j) = g(j) \otimes x_j, \qquad j = 1, \dots, \theta. \tag{1.5}$$

Since we are interested in finite dimensional braided Hopf algebras R, we can assume that

$$\langle \chi(i), g(i) \rangle \neq 1, \tag{1.6}$$

cf. [AS2, Lemma 4.1]. The braiding c is given with respect to the basis $x_i \otimes x_j$ by

$$c(x_i \otimes x_j) = b_{ij}\, x_j \otimes x_i, \tag{1.7}$$

where $(b_{ij})_{1\le i,j\le\theta} = (\langle \chi(j), g(i) \rangle)_{1\le i,j\le\theta}$.

Definition. We shall say that a braiding given by a matrix $\mathbf{b} = (b_{ij})_{1\le i,j\le\theta}$ whose entries are roots of unity is *of Cartan type* if for all i, j, $b_{ii} \neq 1$ and there exists $a_{ij} \in \mathbb{Z}$ such that

$$b_{ij}b_{ji} = b_{ii}^{a_{ij}}. \tag{1.8}$$

The integers a_{ij} are determined once they are chosen in the following way:

(1.9) If $i = j$ we take $a_{ii} = 2$;
(1.10) if $i \neq j$, we select the unique a_{ij} such that $-\operatorname{ord} b_{ii} < a_{ij} \le 0$.

Then (a_{ij}) is a generalized Cartan matrix [K]. We transfer the terminology from generalized Cartan matrices and Dynkin diagrams to braidings of Cartan type. We shall say that a Yetter-Drinfeld module V is *of Cartan type* (resp., connected, ...) if the matrix (b_{ij}) as above is of Cartan type (resp., connected, ...).

The main known examples of braidings of Cartan type are given by $\mathbf{b} = (q^{i\cdot j})_{i,j\in I}$, where q is a root of unity and $(I, .)$ is a Cartan datum as in [L3, Ch. 1].

Definition. Let $\mathbf{b}$ be a braiding of Cartan type with associated Cartan matrix (a_{ij}) as in (1.9), (1.10). We say that $\mathbf{b}$ is of *FL-type* if there exists positive integers $d_1, \dots, d_\theta$ such that for all i, j,

(1.11) $d_i a_{ij} = d_j a_{ji}$ (hence (a_{ij}) is symmetrizable).
(1.12) There exists $q \in \Bbbk$ such that $b_{ij} = q^{d_i a_{ij}}$.

Furthermore, we shall say that a braiding $\mathbf{b}$ is *locally of FL-type* if any principal 2×2 submatrix of $\mathbf{b}$ gives a braiding of FL-type. Recall that a principal submatrix of (b_{ij}) is a matrix $(b_{ij})_{i,j \in I}$ for some subset $I \subset \{1, \dots, \theta\}$.

Let (b_{ij}) be a braiding of Cartan type. Let $\mathcal{X}$ be the set of connected components of the Dynkin diagram corresponding to it. For each $I \in \mathcal{X}$, we let $\mathfrak{g}_I$ be the Kac-Moody Lie algebra corresponding to the generalized Cartan matrix $(a_{ij})_{i,j \in I}$ and $\mathfrak{n}_I$ be the Lie subalgebra of $\mathfrak{g}_I$ spanned by all its positive roots.

Theorem 1.1. *Let $\mathbf{b} = (b_{ij})$ be a braiding of Cartan type, corresponding to $c : V \otimes V \to V \otimes V$. We also assume that b_{ij} has odd order for all i, j.*

(i). If $\mathbf{b}$ is of finite Cartan type, then $\mathfrak{B}(V)$ is finite dimensional, and if moreover 3 does not divide the order of b_{ii} for all i in a connected component of the Dynkin diagram of type G_2, then

$$\dim \mathfrak{B}(V) = \prod_{I \in \mathcal{X}} N_I^{\dim \mathfrak{n}_I},$$

where $N_I = ord(b_{ii})$ for all $i \in I$ and $I \in \mathcal{X}$.

(ii). Assume that $\mathbf{b}$ is locally of FL-type and that, for all i, the order of b_{ii} is relatively prime to 3 whenever $a_{ij} = -3$ for some j, and is different from 3, 5, 7, 11, 13, 17. If $\mathfrak{B}(V)$ be finite dimensional, then $\mathbf{b}$ is of finite type.

Given a finite dimensional Yetter-Drinfeld module V over Γ, it is easy to decide whether it is of Cartan type and locally of FL-type. Let p be an odd prime number. Assume that $\mathbf{b} = (b_{ij})$ satisfies $b_{ii} \neq 1$ and the order of b_{ij} is either p or 1 for all i and j. Then $\mathbf{b}$ is of Cartan type. If $b_{ij} = b_{ji}$ for all i, j, then it is also not difficult to see that $\mathbf{b}$ is locally of FL-type, see Lemma 4.3, using (1.10) for $p = 3$. We conclude from Theorem 1.1 and the reduction to the symmetric connected case in Section 4.2:

Corollary 1.2. *Let p be an odd prime number, Γ a finite direct sum of copies of $\mathbb{Z}/(p)$ and V a finite dimensional Yetter-Drinfeld module over Γ with braiding $\mathbf{b}$. We assume that $b_{ii} \neq 1$ for all i. Then $\mathbf{b}$ is of Cartan type and*

(i). If $\mathbf{b}$ is of finite type, then $\mathfrak{B}(V)$ is finite dimensional, and $\dim \mathfrak{B}(V) = p^M$, where $M = \sum_{I \in \mathcal{X}} \dim \mathfrak{n}_I$ is the number of positive roots of the root system of $\mathbf{b}$.

(ii). If $\mathfrak{B}(V)$ is finite dimensional and $p > 17$, then $\mathbf{b}$ is of finite type.

We remark however that there are examples of finite dimensional braided Hopf algebras $\mathfrak{B}(V)$ of rank 2 over cyclic groups of even order which are *not* of Cartan type, see [N. pp. 1540 ff.].

We want to apply Theorem 1 to solve step (a) of the general method; we have to determine which braidings $\mathbf{b}$ of finite Cartan type actually appear over Γ. This reduces, for each fixed finite Cartan matrix $(a_{ij}) \in \mathbb{Z}^{\theta\times\theta}$, to find all the sequences $g(1), \dots, g(\theta) \in \Gamma$, $\chi(1), \dots, \chi(\theta) \in \widehat{\Gamma}$ such that

(1.13) $\langle \chi(i), g(i)\rangle \neq 1$, for all i and

(1.14) $\langle \chi(j), g(i)\rangle\langle \chi(i), g(j)\rangle = \langle \chi(i), g(i)\rangle^{a_{ij}}$, for all i, j.

This can be interpreted as a problem of computational number theory: to compute all the solutions of a system of quadratic congruences. See Section 8. In fact, we can show that the number of Yetter-Drinfeld modules V (up to isomorphism) of finite Cartan type over our fixed group Γ is finite.

We illustrate this in the case $\Gamma \simeq \mathbb{Z}/(p)$, where p is a prime number. We assume that p is odd; the case $p = 2$ is covered by [N, Th. 4.2.1].

Before stating the next Theorem, we recall that a graded coalgebra is *coradically graded* if its coradical filtration coincides with the filtration coming from the grading [CM].

Theorem 1.3. *Let $\Gamma \simeq \mathbb{Z}/(p)$, where p is an odd prime number. The following list contains all possible Nichols algebras of finite dimension over Γ and finite dimensional coradically graded Hopf algebras with coradical isomorphic to $k\Gamma$.*

(i). The quantum lines and planes discussed in [AS2]. *By bosonization we get respectively Taft algebras and book Hopf algebras cf.* [AS1].

(ii). There exists a Nichols algebra with Dynkin diagram A_2 if and only if $p = 3$ or $p-1$ is divisible by 3. For $p = 3$, we obtain by bosonization from Nichols algebras of dimension 27 exactly 2 non-isomorphic pointed Hopf algebras of dimension 81 with coradical of dimension 3. For $p \equiv 1 \mod 3$, we obtain by bosonization from Nichols algebras of dimension p^3 exactly $p-1$ non-isomorphic pointed Hopf algebras of dimension p^4 with coradical of dimension p.

(iii). There exists a Nichols algebra with Dynkin diagram B_2 if and only if $p \equiv 1 \mod 4$. For each such prime, we obtain by bosonization from Nichols algebras of dimension p^4 exactly $2(p-1)$ non-isomorphic pointed Hopf algebras of dimension p^5 with coradical of dimension p.

(iv). There exists a Nichols algebra with Dynkin diagram G_2 if and only if $p \equiv 1 \mod 3$. For each such prime, we obtain by bosonization from Nichols algebras of dimension p^6 exactly $2(p-1)$ non-isomorphic pointed Hopf algebras of dimension p^7 with coradical of dimension p.

(v). There exist Nichols algebras with finite Dynkin diagram of rank ≥ 3 if and only if $p = 3$ and the corresponding Dynkin diagram is $A_2 \times A_1$ or $A_2 \times A_2$. We obtain respectively braided Hopf algebras of dimension 3^4 and braided Hopf algebras of dimension 3^6 over $\mathbb{Z}/(3)$; hence, we get exactly 4 Hopf algebras of dimension 3^5 and 2 Hopf algebras of dimension 3^7 with coradical of dimension 3. □

These Hopf algebras are new; but the Hopf algebras of order 81 ($p = 3$, type A_2) were known [N]. An application of Theorem 1.3 is the determination of all possible finite dimensional pointed *coradically graded* Hopf algebras of dimension p^4. See Theorem 7.1.

Theorem 1.3 says in particular that any finite dimensional coradically graded Hopf algebra with coradical of odd prime dimension is generated by skew-primitive and group-like elements.

In general, we conjecture

Conjecture 1.4. *Let A be a finite dimensional pointed Hopf algebra over $\Bbbk$. Then A is generated as an algebra by group-like and skew-primitive elements.*

Finally in the last Section we give some bounds on the number of isomorphism classes of Yetter-Drinfeld modules of finite Cartan type over finite abelian groups of odd order.

The paper is organized as follows: We discuss the necessary facts concerning the twisting operation (resp., Frobenius-Lusztig kernels) in Section 2 (resp., Section 3); we prove Theorem 1.1 in Section 4. Section 5 is devoted to Nichols algebras over $\mathbb{Z}/(p)$ and the existence part of Theorem 1.3. We discuss isomorphisms between different bosonizations in Section 6; this concludes the proof of Theorem 1.3. Section 7 is devoted to pointed Hopf algebras of order p^4. In Section 8, we prove bounds on the dimension of Yetter-Drinfeld modules of finite Cartan type. Our conventions are mostly standard and were already used in [AS2].

Added in January 2000:. Using the results and methods of this paper we meanwhile completely classified finite-dimensional pointed Hopf algebras with coradical $\Bbbk\Gamma$, where Γ is a finite direct sum of copies of $\mathbb{Z}/(p)$ and $p > 17$ is prime, or where Γ is cyclic of prime order > 7 [AS3]. In particular, Conjecture 1.4 is true in this case.

In an earlier version of this paper we conjectured that up to isomorphism there are only finitely many finite-dimensional Nichols algebras over a fixed finite group (of odd order). This conjecture is shown to be true by Graña [Gr2] as a consequence of Theorem 3.1 (2) in the present paper which follows from [L3]. Over abelian groups of even order there are infinitely many finite-dimensional Nichols algebras by [N].

Acknowledgement. We are grateful to Eric Müller for crucial conversations about Frobenius-Lusztig kernels. We also thank Matías Graña for many conversations about Nichols algebras; Jorge and Juan Guccione for enlightening remarks about twisting, and Sorin Dascalescu for interesting conversations.

§2. Twisting.

The idea of twisting was introduced by Drinfeld [Dr2], see also [Dr1], [Dr3]. General facts are discussed in [Mj2], [Mj3]; for applications to quantized enveloping algebras see [Re], for applications to semisimple Hopf algebras see [Nk]. We briefly discuss the general idea referring to the literature for more details and work out accurately the case of our interest.

Let A be a Hopf algebra. Given an invertible $F \in A \otimes A$, we can consider the "twisted" comultiplication Δ_F given by

$$\Delta_F(x) = F\Delta(x)F^{-1}.$$

Under certain conditions on F, A_F (the same algebra A but with comultiplication Δ_F) is again a Hopf algebra. We are interested in the particular case when F belongs indeed to $H \otimes H$, where H is a Hopf subalgebra of A. We further assume that the inclusion $H \hookrightarrow A$ has a Hopf algebra retraction $\pi : A \to H$; so A is the bosonization of R by H where R is a braided Hopf algebra in the category ${}^H_H\mathcal{YD}$ of Yetter-Drinfeld modules over H. Then H_F is a Hopf subalgebra of A_F and π is again a Hopf algebra map. If $H_F \simeq H$ (this happens for instance if H is abelian), then F induces an autoequivalence $V \mapsto V_F$ of the braided category ${}^H_H\mathcal{YD}$ and A_F is in fact the bosonization of R_F by H_F. See [Mj2].

We now assume that $H = \Bbbk\Gamma$ where Γ is a finite abelian group. We fix non-zero elements $y(1), \dots, y(M)$ in Γ such that $\operatorname{ord} y(\ell) = E_\ell$,

$$\Gamma =< y(1) > \oplus \cdots \oplus < y(M) >, \quad \text{and} \quad E_\ell | E_{\ell+1} \text{ for } \ell = 1, \dots, M-1. \tag{2.1}$$

Let q be a root of unity of order E_M. For all i define the integer D_i by $D_i E_i = E_M$. Then $q_i = q^{D_i}$ is a root of unity of order E_i.

Let $\gamma(i) \in \widehat{\Gamma}$ be the unique character such that $\langle \gamma(i), y(j) \rangle = q_i^{\delta_{ij}}$, for $1 \le i, j \le M$. Then $\operatorname{ord} \gamma(\ell) = E_\ell$ and

$$\widehat{\Gamma} =< \gamma(1) > \oplus \cdots \oplus < \gamma(M) > .$$

Given $g \in \Gamma$, $\chi \in \widehat{\Gamma}$ we shall use the notation g_i, χ_j meaning that

$$g = g_1 y(1) + \cdots + g_M y(M), \qquad \chi = \chi_1 \gamma(1) + \cdots + \chi_M \gamma(M). \tag{2.2}$$

We identify H with the Hopf algebra $\Bbbk^{\widehat{\Gamma}}$ of functions on the group $\widehat{\Gamma}$ identifying an element in $\widehat{\Gamma}$ with its evaluation; we denote by $\delta_\tau \in H$ the function given by $\delta_\tau(\zeta) = \delta_{\tau,\zeta}$, $\tau, \zeta \in \widehat{\Gamma}$. Then

$$\delta_\tau = \frac{1}{|\Gamma|} \sum_{g \in \Gamma} \langle \tau, g^{-1} \rangle g.$$

Hence $\zeta(\delta_\tau) = \delta_{\tau,\zeta}$.

We shall describe the datum for twisting F in terms of 2-cocycles, following [Nk], [Mv]. The theory of the cocycles we are interested in goes back to Schur and there is an extensive literature on it; we refer to [BT].

We recall that $\omega : \widehat{\Gamma} \times \widehat{\Gamma} \to \Bbbk^\times$ is a 2-cocycle if $\omega(\tau, 1) = \omega(1, \tau) = 1$ and

$$\omega(\tau, \zeta)\omega(\tau\zeta, \eta) = \omega(\tau, \zeta\eta)\omega(\zeta, \eta) \text{ for all } \tau, \zeta, \eta \in \widehat{\Gamma}. \tag{2.3}$$

It is not difficult to deduce that

$$\omega(\tau\zeta, \chi)\omega(\chi, \tau\zeta)^{-1}\omega(\zeta, \chi)^{-1}\omega(\chi, \zeta) = \omega(\tau, \chi)\omega(\chi, \tau)^{-1}. \tag{2.4}$$

Lemma 2.1. *Let c_{ij}, $1 \leq i < j \leq M$, be integers such that $0 \leq c_{ij} < E_i$. Let $\omega : \widehat{\Gamma} \times \widehat{\Gamma} \to \Bbbk^\times$ be the map defined by*

$$\omega(\tau, \chi) = \prod_{1 \leq i < j \leq M} q_i^{c_{ij}\tau_j\chi_i} = q^{\sum_{1 \leq i < j \leq M} D_i c_{ij}\tau_j\chi_i}. \tag{2.5}$$

Then ω is a 2-cocycle. Any 2-cocycle can be presented in this way up to a coboundary.

Proof. The first statement follows by a direct computation that we leave to the reader. The second is not needed in the remaining of this paper, but follows from [BT, Th. 4.7, p. 44]. □

Lemma 2.2 [Mv], [Nk]. *Let $\omega : \widehat{\Gamma} \times \widehat{\Gamma} \to \Bbbk^\times$ be a 2-cocycle and let $F \in H \otimes H$ be given by*

$$F = \sum_{\tau, \zeta \in \widehat{\Gamma}} \omega(\tau, \zeta)\delta_\tau \otimes \delta_\zeta.$$

Let A be a Hopf algebra containing H as a Hopf subalgebra. Then A_F, the same algebra A but with the comultiplication Δ_F, is again a Hopf algebra. If $\widetilde{\omega}$ is another 2-cocycle and $\widetilde{F}$ is its corresponding twisting datum, then the Hopf algebras A_F and $A_{\widetilde{F}}$ are isomorphic whenever ω and $\widetilde{\omega}$ differ by a coboundary. □

We recall that a Yetter-Drinfeld module over H is a vector space V provided with structures of left H-module and left H-comodule such that

$$\delta(h.v) = h_{(1)}v_{(-1)}\mathcal{S}h_{(3)} \otimes h_{(2)}.v_{(0)}.$$

This category is semisimple; given $g \in \Gamma$ and $\gamma \in \widehat{\Gamma}$, we denote by V_g^γ the isotypic component of a Yetter-Drinfeld module V corresponding to g, γ. That is, $V_g^\gamma = V_g \cap V^\gamma$, where

$$V_g = \{v \in V : \delta(v) = g \otimes v\}, \qquad V^\gamma = \{v \in V : h.v = \gamma(h)v, \quad \forall h \in \Gamma\}. \tag{2.6}$$

Conversely, a vector space V provided with a direct sum decomposition

$$V = \oplus_{g \in \Gamma, \gamma \in \widehat{\Gamma}} V_g^\gamma$$

is a Yetter-Drinfeld module with structures defined by (2.6). (This is a reformulation of the fact that the double of H is the group algebra of $\Gamma \times \widehat{\Gamma}$).

We now consider a braided Hopf algebra R in the category ${}_H^H\mathcal{YD}$ of Yetter-Drinfeld modules over H and its bosonization $A = R\#H$; then the evident maps $\pi : A \to H$ and $\iota : H \to A$ are Hopf algebra homomorphisms, and $R = \{a \in A : (\mathrm{id} \otimes \pi)\Delta(a) = a \otimes 1\}$. The multiplication in A is determined by the rule $gr = \chi(g)rg$, whenever $r \in R^\chi$, $g \in \Gamma$; hence

$$\delta_\tau r = r\delta_{\tau\chi^{-1}}, \qquad \text{if } r \in R^\chi.$$

We fix $F \in H \otimes H$ as in Lemma 2.2. It follows from the definitions that π and ι are Hopf algebra homomorphisms when replacing A by its twisting A_F. Hence

$$R_F := \{a \in A_F : (\mathrm{id} \otimes \pi)\Delta_F(a) = a \otimes 1\}$$

is a braided Hopf algebra in the category ${}^H_H\mathcal{YD}$.

Lemma 2.3. *(i). The linear map $\psi : R \to R_F$ defined by*

$$\psi(r) = \sum_{\tau \in \widehat{\Gamma}} \omega(\chi, \tau)^{-1} r \# \delta_\tau, \qquad r \in R^\chi,$$

is an isomorphism of Γ-modules. If $r \in R^\chi$ and $s \in R^\tau$ then

$$\psi(rs) = \omega(\chi, \tau)\psi(r)\psi(s). \tag{2.7}$$

If $r \in R^\chi_g$, then $\psi(r) \in (R_F)^\chi_{\psi(\chi,g)}$, where

$$\begin{aligned} \psi(\chi, g) &= \sum_{\tau \in \widehat{\Gamma}} \omega(\tau, \chi)\omega(\chi, \tau)^{-1} \langle \tau, g\rangle \delta_\tau \\ &= \sum_{1 \le j \le M} \left(\sum_{1 \le i < j} \frac{D_i}{D_j} c_{ij}\chi_i + g_j - \sum_{j < h \le M} c_{jh}\chi_h \right) y(j). \end{aligned} \tag{2.8}$$

Here we have used notations (2.2) and (2.5). (The first equality of (2.8) is in $\Bbbk\Gamma$, the second in Γ).

(ii). If R is a graded braided Hopf algebra, then R_F also is and ψ is a graded map. If R is a coradically graded braided Hopf algebra (resp. a Nichols algebra), then R_F also is.

Proof. We first check that ψ is well-defined:

$$\begin{aligned} (\mathrm{id} \otimes \pi)\Delta_F(\psi(r)) =& F(r \otimes 1) \sum_{\tau,\sigma \in \widehat{\Gamma}} \omega(\chi, \sigma\tau)^{-1} \delta_\tau \otimes \delta_\sigma F^{-1} \\ &= \sum_{\mu,\eta \in \widehat{\Gamma}} \omega(\mu, \eta)\delta_\mu \otimes \delta_\eta (r \otimes 1) \sum_{\tau,\sigma \in \widehat{\Gamma}} \omega(\chi, \tau\sigma)^{-1}\omega(\tau, \sigma)^{-1} \delta_\tau \otimes \delta_\sigma \\ &= (r \otimes 1) \sum_{\tau,\sigma \in \widehat{\Gamma}} \omega(\tau\chi, \sigma)\omega(\chi, \tau\sigma)^{-1}\omega(\tau, \sigma)^{-1} \delta_\tau \otimes \delta_\sigma \\ &= (r \otimes 1) \sum_{\tau,\sigma \in \widehat{\Gamma}} \omega(\chi, \tau)^{-1} \delta_\tau \otimes \delta_\sigma \\ &= \psi(r) \otimes 1. \end{aligned}$$

It is easy to see that ψ preserves the action of Γ. It follows that ψ is invertible with inverse $\psi^{-1}(r) = \sum_{\tau\in\widehat{\Gamma}} \omega(\chi,\tau) r\#\delta_\tau$, for $r \in (R_F)^\chi$.

Now we prove (2.7):

$$\begin{aligned}\psi(r)\psi(s) &= \sum_{\sigma,\eta\in\widehat{\Gamma}} \omega(\chi,\sigma)^{-1}\omega(\tau,\eta)^{-1} r\delta_\sigma s\delta_\eta = \sum_{\eta\in\widehat{\Gamma}} \omega(\chi,\tau\eta)^{-1}\omega(\tau,\eta)^{-1} rs\delta_\eta\\ &= \omega(\chi,\tau)^{-1}\sum_{\eta\in\widehat{\Gamma}}\omega(\chi\tau,\eta)^{-1} rs\delta_\eta = \omega(\chi,\tau)^{-1}\psi(rs).\end{aligned}$$

We still assume that $r \in R_g^\chi$. Then the coaction on $\psi(r)$ is given by

$$\begin{aligned}\delta_F(\psi(r)) &= (\pi\otimes \mathrm{id})\Delta_F(\psi(r))\\ &= \left(\sum_{\mu,\eta}\omega(\mu,\eta)\delta_\mu\otimes\delta_\eta\right)(g\otimes r)\,\Delta\left(\sum_\tau \omega(\chi,\tau)^{-1}\delta_\tau\right)F^{-1}\\ &= \sum_{\tau,\zeta}\omega(\tau,\zeta\chi)\omega(\chi,\tau\zeta)^{-1}\omega(\tau,\zeta)^{-1} g\delta_\tau\otimes r\delta_\zeta\\ &= \sum_{\tau,\zeta}\omega(\chi,\tau\zeta)^{-1}\omega(\zeta,\chi)^{-1}\omega(\tau\zeta,\chi) g\delta_\tau\otimes r\delta_\zeta\\ &= \sum_{\tau,\zeta}\omega(\chi,\zeta)^{-1}\omega(\tau,\chi)\omega(\chi,\tau)^{-1} g\delta_\tau\otimes r\delta_\zeta\\ &= \sum_{\tau}\omega(\tau,\chi)\omega(\chi,\tau)^{-1}\langle\tau,g\rangle\delta_\tau\otimes\psi(r),\end{aligned}$$

where we have used repeatedly the cocycle condition and (2.4).

From the coassociativity of Δ_F we conclude that

$$\psi(\chi,g) = \sum_\tau \omega(\tau,\chi)\omega(\chi,\tau)^{-1}\langle\tau,g\rangle\delta_\tau$$

is a group-like element of H, *i.e.* an element of Γ. The last equality in (2.8) follows by evaluating at $\gamma(j)$.

Let us suppose now that $R = \oplus_{n\geq 0} R(n)$ is a *graded* braided Hopf algebra. Then $A = \oplus_{n\geq 0}A(n)$, where $A(n) = R(n)\#H$, is a graded Hopf algebra. Since $F \in H\otimes H = A(0)\otimes A(0)$, we see that A_F is also a graded Hopf algebra with respect to the same grading and π, ι are graded maps. Hence R_F inherits the grading of A and is a graded braided Hopf algebra. It is now evident that ψ is a graded map, R and R_F being both graded subspaces of A.

Let us further suppose that R is coradically graded; then A also is. Since $F \in H\otimes H = A(0)\otimes A(0)$, A_F has the same coradical filtration than A; hence it is also coradically graded. Therefore R_F is coradically graded. See [AS2, Section 2]. In particular, $\psi(P(R)) = P(R_F)$. If in addition R is generated by $P(R)$, *i.e.* is a Nichols algebra, then we conclude from (2.7) that R_F is generated by $P(R_F)$, thus R_F is also a Nichols algebra. $\square$

Let now R be a coradically graded braided Hopf algebra, $x_1, \dots, x_\theta$ a basis of $P(R)$ such that for some $g(1), \dots, g(\theta) \in \Gamma$, $\chi(1), \dots, \chi(\theta) \in \widehat{\Gamma}$ (1.5) holds. Then the braiding (1.7) is given by

$$
\begin{aligned}
(b_{ji})_{1\le i,j\le\theta} &= (\langle \chi(i), g(j)\rangle)_{1\le i,j\le\theta} \\
&= \left(\prod_{1\le h\le M} q_h^{\chi(i)_h g(j)_h} \right)_{1\le i,j\le\theta} = (q^{\alpha_{ij}}), \\
\text{where}\quad \alpha_{ij} &= \sum_{1\le h\le M} D_h \chi(i)_h g(j)_h.
\end{aligned} \tag{2.9}
$$

By Lemma 2.3, R_F is a coradically graded braided Hopf algebra and $\psi(x_1), \dots, \psi(x_\theta)$ is a basis of $P(R_F)$ such that (1.5) holds for $\psi(\chi(1), g(1)), \dots, \psi(\chi(\theta), g(\theta)) \in \Gamma$, $\chi(1), \dots, \chi(\theta) \in \widehat{\Gamma}$. By (2.8), the braiding (1.7) for R_F is given by

$$
\begin{aligned}
(b^F_{ji})_{1\le i,j\le\theta} &= (\langle \chi(i), \psi(\chi(j), g(j))\rangle)_{1\le i,j\le\theta} = (q^{\alpha^F_{ij}}), \\
\text{where}\quad \alpha^F_{ij} &= \sum_{1\le t<h\le M} D_t c_{th} \left(\chi(i)_h \chi(j)_t - \chi(i)_t \chi(j)_h\right) + \alpha_{ij}.
\end{aligned} \tag{2.10}
$$

Remark 2.4. The "symmetrization" of the matrix α_{ij} remains unchanged under twisting:

$$
\begin{aligned}
\alpha^F_{ij} + \alpha^F_{ji} = \sum_{1\le t<h\le M} & D_t c_{th} \left(\chi(i)_h \chi(j)_t - \chi(i)_t \chi(j)_h \right. \\
& \left. + \chi(j)_h \chi(i)_t - \chi(j)_t \chi(i)_h\right) + \alpha_{ij} + \alpha_{ji} = \alpha_{ij} + \alpha_{ji}.
\end{aligned} \tag{2.11}
$$

Hence, if R is of Cartan type, then R_F is of the same Cartan type. Also, $\alpha^F_{ii} = \alpha_{ii}$ and the diagonal elements b_{ii} do not change after twisting.

In particular, if R is a quantum linear space, *i.e.* $\alpha_{ij} + \alpha_{ji} = 0 \mod E_M$ whenever $i \ne j$, then R_F also is a quantum linear space.

§3. Frobenius-Lusztig kernels.

Let $(I, \cdot)$ be a Cartan datum as in [L3, Chapter 1]. Let $a_{ij} = \frac{2 i\cdot j}{i\cdot i}$, $d_i = \frac{i\cdot i}{2}$. Let also $q \ne 1$ be a root of 1 of odd order N. We consider in this Section a vector space V with braiding $\mathbf{b} = (b_{ij})$ where $b_{ij} = q^{i\cdot j}$. We also assume that

(3.1) $N_i > -a_{ij}$, where N_i is the order of b_{ii}, for all i, j.

Now $\mathbf{b}$ is of Cartan type and by (3.1), it is of FL-type and its associated Cartan matrix is (a_{ij}), with the d_i's as above. Conversely, any braiding of FL-type such that b_{ij} has odd order for all i, j arises in this way.

Our aim is to sketch the main ideas of the proof of the following Theorem, which follows from deep results of Lusztig and in addition from the work of Müller [Mü] and Rosso [Ro1].

Theorem 3.1.

(1) *Assume that $(I,\cdot)$ is of finite type. Then $\mathfrak{B}(V)$ is finite-dimensional. Assume moreover that $(I,\cdot)$ is connected and if the corresponding Dynkin diagram has type G_2 that 3 does not divide the order of b_{ii} for all $i \in I$. Then $\mathfrak{B}(V)$ is isomorphic to the positive part of the Frobenius-Lusztig kernel $\mathfrak{u}$, cf.* [L2, 8.2], *and*

$$\dim \mathfrak{B}(V) = N^M,$$

where M is the number of positive roots of the root system of $(I,\cdot)$ and N is the order of b_{ii} for all $i \in I$.

(2) *Assume that $(I,\cdot)$ is not of finite type. Then $\mathfrak{B}(V)$ is infinite dimensional.*

Proof. (1) The finiteness of the dimension of $\mathfrak{B}(V)$ follows from the characterization in [Mü, Section 2] or [Ro1]; in the terminology of Müller, q fits to ${}_kf$ by (3.1) and [Mü, 2.9].

If $(I,\cdot)$ is connected, then there are integers d and $1 \le \tilde{d}_i \le 3$ such that $d_i = d\tilde{d}_i$ for all i. Define $l = q^d$. Then for all i, j, $b_{ij} = q^{d_i a_{ij}} = l^{\tilde{d}_i a_{ij}}$, and b_{ii}, b_{jj} and l have the same order by our assumption about G_2. Hence the dimension formula follows from [L2, 8.3, 8.4].

We sketch now the proof of Part (2). We keep the notation from [L3]. It is in principle not always true that the positive part $\mathfrak{u}^+$ of the Frobenius-Lusztig kernel is isomorphic to $\mathfrak{B}(V)$. We have however an epimorphism $\mathfrak{u}^+ \to \mathfrak{B}(V)$.

Since $(I,\cdot)$ is not of finite type, its Weyl group is not finite. Hence, for any $M > 0$ there exists an element $w \in W$ of length M, say with reduced expression $w = s_{i_1} \dots s_{i_M}$. We shall show that $\mathfrak{B}(V)$ contains 2^M linearly independent elements; this concludes the proof of (2).

We work first in the transcendental case. We use now specifically the notation from [L3, 38.2.2]. The sequence $\mathbf{h} = (i_1, \dots, i_M)$ is admissible because of [L3, Proposition 40.2.1 (a)]. It is clear that the element $x = 1$ is adapted to $(\mathbf{h}, 0)$. Let c, c' be as [L3, Proposition 38.2.3] and suppose that their entries are either 0 or 1. Then $L(\mathbf{h}, c, 0, 1)$ is orthogonal (resp, not orthogonal) to $L(\mathbf{h}, c', 0, 1)$ if c is different (resp., equal) to c'. But we can pass from the transcendental case to our case (q a root of unity) thanks to the results in [Mü, Section 2], notably Lemma 2.2, Proposition 2.3 and Theorem 2.11 (a). $\square$

§4. Proof of Theorem 1.1.

4.1 Sketch of the proof.

Let us first outline the proof of Theorem 1.1. Let V be a Yetter-Drinfeld module over our fixed group Γ as in (1.5) and let $R = \mathfrak{B}(V)$. We begin by passing from a general braiding (1.7) to a symmetric one. It is natural to try to apply a Drinfeld twist to the Hopf algebra $\Bbbk\Gamma\# R$ (compare with [Ro2]). Unfortunately this is not always possible. It fails already for quantum linear planes over cyclic groups, since no twist is possible in the cyclic group case. However, we can overcome this difficulty because the algebra and coalgebra structures of R do not depend on Γ but only on the braiding (1.7). That is, let Υ be another finite abelian group and let $h(1), \dots,$ $h(\theta) \in \Upsilon$, $\eta(1), \dots, \eta(\theta) \in \widehat{\Upsilon}$ be sequences satisfying

$$\langle \eta(i), h(j)\rangle = \langle \chi(i), g(j)\rangle, \quad \forall i, j.$$

Let T be the Nichols algebra over Υ such that $T(1) = V$ with Yetter-Drinfeld module structure given by (1.5) but with $h(i)$'s and $\eta(j)$'s instead of $g(i)$'s and $\chi(j)$'s. Then T is isomorphic to R both as an algebra and coalgebra. This follows at once from the description of T and R in terms of "quantum antisymmetrizers"; see for instance [Sbg], [Ro2], [AG]. So we change the group, twist and assume that the braiding (1.7) is symmetric.

We then discuss briefly the relations between the notions of Cartan type, FL-type and locally of FL-type. We state the last one in arithmetical terms and describe several instances where it holds. One of them is the following:

Let $\mathbf{b} = (b_{ij})$ be a connected braiding of Cartan type whose entries have odd order. We say that $\mathbf{b}$ satisfies the *relative primeness condition* if a_{ij} is 0 or relatively prime to the order of b_{ii} for all i, j.

We prove then that a braiding of symmetrizable Cartan type satisfying the relative primeness condition is of FL-type. By the results evoked in Section 3, this is enough for part (i) of Theorem 1.1.

For the converse part (ii) of Theorem 1.1, we prove that if $\mathfrak{B}(V)$ is finite dimensional and $\mathbf{b}$ is locally of FL-type then it is symmetrizable. By the results of Section 3 again, this concludes the proof of the theorem.

4.2 Reduction to the symmetric connected case.

Let $(b_{ij})_{1\le i,j\le\theta}$ be a matrix with entries in $\Bbbk^\times$. Let V be a vector space with a basis $x_1, \dots, x_\theta$ and let $c : V\otimes V \to V \otimes V$ be the linear map given by

$$c(x_i \otimes x_j) = b_{ij} x_j \otimes x_i, \quad 1 \le i, j \le \theta. \tag{4.1}$$

It is easy to verify that c satisfies the Braid relation:

$$(c\otimes \mathrm{id})(\mathrm{id}\otimes c)(c\otimes \mathrm{id}) = (\mathrm{id}\otimes c)(c\otimes \mathrm{id})(\mathrm{id}\otimes c).$$

Therefore, it induces representations of the Braid group $\mathbb{B}_n$ on $V^{\otimes n}$ for any $n \ge 2$ and this in turn allows to define "braided antisymmetrizers" which are linear maps $\mathfrak{S}_n : V^{\otimes n} \to V^{\otimes n}$. Let $R = \oplus_{n\ge 0} V^{\otimes n}/\ker \mathfrak{S}_n$; it is a graded algebra. See for instance [Sbg], [AG]. Using the methods of [Mj3, Th. 10.2.1] it is possible to prove that R is a braided Hopf algebra. In our case this will follow from Lemma 4.1 below.

If Γ is an abelian group, $g(1), \dots, g(\theta) \in \Gamma$, $\chi(1), \dots, \chi(\theta) \in \widehat{\Gamma}$ are sequences such that $b_{ij} = \langle \chi(j), g(i)\rangle$ and we consider V as a Yetter-Drinfeld module over Γ via (1.5), then c is the "commutativity isomorphism" in the braided category ${}_{\Gamma}^{\Gamma}\mathcal{YD}$. Moreover, R has a braided Hopf algebra structure and is in fact the Nichols algebra associated to V.

Lemma 4.1. *Let (b_{ij}) be a braiding of Cartan type and let us assume that b_{ij} is a root of 1 of odd order for any i,j. Then there exists a finite abelian group Γ, sequences $g(1), \dots, g(\theta) \in \Gamma$, $\chi(1), \dots, \chi(\theta) \in \widehat{\Gamma}$ and $F \in \Bbbk\Gamma \otimes \Bbbk\Gamma$ given by a 2-cocycle of $\widehat{\Gamma}$ as in Lemma 2.2 such that*

(i) *for $1 \leq i, j \leq \theta$, we have*

$$b_{ij} = \langle \chi(j), g(i) \rangle; \tag{4.2}$$

(ii) *the braiding (1.7) corresponding to the Nichols algebra R_F is symmetric and of Cartan type, with the same associated Cartan matrix and diagonal elements.*

Here R is the Nichols algebra associated to the Yetter-Drinfeld module V with basis $x_1, \dots, x_\theta$ and structure defined by (1.5).

Proof. (i): We define $\Gamma := < y(1) > \oplus \dots \oplus < y(\theta) >$, where we impose that the order E_j of yj is the least common multiple of the orders of $b_{i\ell}$, for all i, and for $\ell \leq j$. Then $E_j | E_{j+1}$: (2.1) holds. Let $q \in k$ be a root of 1 of order E_θ. Let $D_i = \dfrac{E_\theta}{E_i}$, $1 \leq i \leq \theta$ and let $q_i = q^{D_i}$. Then q_i is a root of 1 of order E_i. Let $\gamma(i) \in \widehat{\Gamma}$ be the unique character such that $\langle \gamma(i), y(j) \rangle = q_i^{\delta_{ij}}$, for $1 \leq i, j \leq N$. Then $\operatorname{ord} \gamma(\ell) = E_\ell$ and $\widehat{\Gamma} = < \gamma(1) > \oplus \dots \oplus < \gamma(M) >$. We choose $\chi(j) = \gamma(j)$ for all j and define $g(i)$ by (4.2); it makes sense because the order of $\langle \chi(j), g(i) \rangle$ divides E_j for all i, j.

(ii): Let α_{ij} be given by (2.9). We are looking for integers c_{ij} such that, if F is associated to the cocycle ω given by (2.5), then the matrix α^F_{ij} is symmetric. Assume that $i < j$. By (2.10) and our preceding choices, we have

$$\begin{aligned} \alpha_{ij} &= D_i g(j)_i, \\ \alpha^F_{ij} &= -D_i c_{ij} + \alpha_{ij}, \\ \alpha^F_{ji} &= D_i c_{ij} + \alpha_{ji}; \end{aligned}$$

hence $\alpha^F_{ij} \equiv \alpha^F_{ji} \mod E_\theta$ if and only if

$$2 D_i c_{ij} \equiv \alpha_{ij} - \alpha_{ji} \equiv D_i g(j)_i - D_j g(i)_j \mod E_\theta. \tag{4.3}$$

We solve (4.3). The factor 2 can be ignored because E_θ is odd. That is, it is enough to solve

$$D_i \widetilde{c}_{ij} \equiv D_i g(j)_i - D_j g(i)_j \mod E_\theta. \tag{4.4}$$

Now, since $g(i) = \sum_t g(i)_t y(t)$ in Γ, we have

$$b_{ij} = \langle \chi(j), g(i) \rangle = q_j^{g(i)_j} = q^{D_j g(i)_j}.$$

As the braiding (b_{ij}) is of Cartan type, we see that

$$q^{D_i g(j)_i + D_j g(i)_j} = b_{ij} b_{ji} = b_{ii}^{a_{ij}} = q^{D_i a_{ij}}$$

and therefore

$$D_j g(i)_j \equiv D_i a_{ij} - D_i g(j)_i \mod E_\theta.$$

Thus $\widetilde{c}_{ij} = 2g(j)_i - a_{ij}$ is a solution of (4.4). The last statement follows from Remark 2.4 $\square$

In the rest of this section, we shall consider matrices $\mathbf{b} = (b_{ij})_{1\le i,j\le \theta}$ of Cartan type, such that b_{ij} is a root of 1 of odd order and $b_{ij} = b_{ij}$ for all i, j. By Lemma 4.1, we can consider its associated Nichols algebra R; the comultiplication is an algebra map where the product in $R \otimes R$ is determined by

$$(x_r \otimes x_i)(x_j \otimes x_s) = b_{ij} x_r x_j \otimes x_i x_s.$$

If $I \subset \{1, \dots, \theta\}$ then we denote by $R(I)$ the Nichols algebra corresponding to the braiding $(b_{ij})_{i,j \in I}$. Clearly, there is an injective map of braided Hopf algebras $R(I) \to R$.

Lemma 4.2. *(i). If $b_{ij} = 1$ then $x_i x_j = x_j x_i$.*

(ii). Assume there is $I \subset \{1, \dots, \theta\}$ such that $b_{ij} = 1$ for all $i \in I$, $j \in J := \{1, \dots, \theta\} - I$. Then $R \simeq R(I) \otimes R(J)$.

Proof. By a direct computation, we see that $x_i x_j - x_j x_i$ is primitive; but the primitive elements are concentrated in degree one, so it should be 0. This proves (i). Let $S = R(I) \otimes R(J)$; it is a graded algebra and coalgebra with respect to the grading $S(h) = \oplus_\ell R(I)(\ell) \otimes R(J)(h-\ell)$ and the usual tensor product multiplication and comultiplication. Then S is a strictly graded coalgebra, *i.e.* (1.1), (1.2), (1.3) hold, *cf.* [Sw, p. 240]. On the other hand, S is a Yetter-Drinfeld module and it is easy to conclude from the hypothesis and (i) that it is a braided Hopf algebra. Clearly, S is generated as algebra by $S(1) \simeq V$, *i.e.* it satisfies (1.4). Thus S is a Nichols algebra, hence isomorphic to R because their spaces of primitive elements coincide. $\square$

We consider the following equivalence relation on $\{1, \dots, \theta\}$: $i \sim j$ if there exists a sequence of elements $i = h_0, \dots, h_P = j$ in $\{1, \dots, \theta\}$ such that $h_\ell \neq h_{\ell+1}$ and $b_{h_\ell h_{\ell+1}} \neq 1$. Note that $P = 0$ is allowed and gives $i \sim i$. A class of this relation is called a connected component. This is equivalent to the notion of connected Dynkin diagram or indecomposable matrix as in [K, 1.7.1]. The preceding Lemma 4.2 shows that the Nichols algebra R is the tensor product of the Nichols algebras corresponding to its connected components. Therefore, to prove Theorem 1.1 it is enough to assume that $\mathbf{b}$ is *connected.*

4.3 Conditions for FL-type.

Lemma 4.3. *Let $\mathbf{b} = (b_{ij})_{1\le i,j\le\theta}$ be a braiding of Cartan type such that b_{ij} is a root of 1 of odd order and $b_{ij} = b_{ji}$ for all i, j.*

If $\mathbf{b}$ is symmetrizable and satisfies the relative primeness condition (a_{ij} is 0 or relatively prime to the order of b_{ii} for all i, j) then it is of FL-type.

Proof. We can easily reduce to the case when $\mathbf{b}$ is connected.

We claim first that the order of b_{kk} is the same for all k. Indeed, let us fix $i \neq j$ such that $a_{ij} \neq 0$ (if no such pair i, j exists, then by connectedness $\theta = 1$ and there is nothing to prove). Then $b_{ii}^{a_{ij}} = b_{jj}^{a_{ji}}$ and $\operatorname{ord} b_{ii} = \operatorname{ord} b_{jj}$ by the relative primeness condition. The claim follows by connectedness. We call $N = \operatorname{ord} b_{ii}$.

Let d_k be integers as in (1.11). We can assume that they are relatively prime, that is, $(d_1, \dots, d_\theta) = 1$. Then it is easy to see that N and d_k are relatively prime for all k. Indeed, if t divides N and d_i then t divides d_j, since t divides $d_i a_{ij} = d_j a_{ji}$ and $(N, a_{ji}) = 1$. Again, the claim follows by connectedness.

In particular, there is a unique root of unity q of order N such that $b_{ii} = q^{2d_i}$. We claim finally that this q satisfies (1.12). Indeed, $b_{ii}^{a_{ij}} = q^{2d_i a_{ij}} = q^{2d_j a_{ji}}$ and $b_{ii}^{a_{ij}} = b_{ij}^2 = b_{jj}^{a_{ji}}$. Thus, $b_{ij} = q^{d_i a_{ij}}$ (since N is odd) and $b_{jj} = q^{2d_j}$ (since $(N, a_{ji}) = 1$). Once more, the claim follows by connectedness. □

We now investigate conditions for FL-type in rank 2. Let $\mathbf{b} = (b_{ij})_{1\le i,j\le 2}$ be a braiding of connected Cartan type whose entries have odd order, such that $b_{12} = b_{21}$. Then it is automatically symmetrizable since the rank is 2. "Connected" means that $a_{12} \neq 0$. Let d_1, d_2 be relatively prime integers such that $d_1 a_{12} = d_2 a_{21}$. We denote by N_i the order of b_{ii}.

Lemma 4.4. *The following are equivalent:*

(i) $\mathbf{b}$ *is of FL-type.*
(ii) *There exists $u \in \Bbbk$ of odd order such that $u^{2d_i} = b_{ii}$, $i = 1, 2$.*
(iii) *There exists $v \in \Bbbk$ such that $v^{d_i} = b_{ii}$, $i = 1, 2$.*

Proof. (iii) $\Longrightarrow$ (ii): Note that the order of v divides $d_1 N_1$ and $d_2 N_2$. Since the N_i's are odd and d_1, d_2 are relatively prime, the order of v is odd. Hence v has a square root u of odd order.

(ii) $\Longrightarrow$ (i): We have $b_{12}^2 = b_{11}^{a_{12}} = u^{2d_1 a_{12}}$. Hence $b_{12} = u^{d_1 a_{12}}$ since both have odd order.

(i) $\Longrightarrow$ (iii): If q satisfies (1.12), take $v = q^2$. □

We want to give a criterion for the condition (iii) in the preceding Lemma. Let e_i , $i = 1, 2$ be non-zero integers such that

$$e_1 d_1 N_1 = e_2 d_2 N_2 =: r;$$

for instance we could take r the lowest common multiple of $d_1 N_1$ and $d_2 N_2$. Observe that there exists $s \in \mathbb{Z}$ such that $r = d_1 d_2 s$.

Let now $\xi \in \Bbbk$ be a primitive r-th root of 1 and choose integers k_1, k_2 such that

$$b_{ii} = \xi^{e_i d_i k_i};$$

this is possible because $\xi^{e_i d_i}$ has order N_i.

Lemma 4.5. *Condition (iii) in Lemma 4.4 is equivalent to*

(4.5) $e_1 k_1 \equiv e_2 k_2 \mod s$.

Proof. We claim first that (iii) is equivalent to the following statement:

(iv) There exists $t_i \in \mathbb{Z}$, $i = 1, 2$ such that

$$e_i d_i k_i \equiv e_i d_i t_i \mod r, \quad i = 1, 2 \tag{4.6}$$

$$e_1 t_1 \equiv e_2 t_2 \mod r. \tag{4.7}$$

Indeed, if (iii) holds then $q^{d_i N_i} = 1$; as ξ^{e_i} has order $d_i N_i$, there exists $t_i \in \mathbb{Z}$ such that $q = \xi^{e_i t_i}$. Then (4.6), (4.7) follow now without difficulty. Conversely, if (iv) holds, take $q = \xi^{e_1 t_1} = \xi^{e_2 t_2}$, by (4.7). Then (iii) is true by (4.6). The claim is proved.

Now (4.6) is equivalent to $k_i \equiv t_i \mod N_i$, $i = 1, 2$.

Assume (iv). Then there exist $x_i \in \mathbb{Z}$ such that $t_i = k_i + N_i x_i$, $i = 1, 2$. Now r (and *a fortiori* s) divides

$$e_1 t_1 - e_2 t_2 = e_1 k_1 - e_2 k_2 + e_1 N_1 x_1 - e_2 N_2 x_2;$$

but $e_1 N_1 = d_2 s$ and $e_2 N_2 = d_1 s$. So (4.5) holds.

If (4.5) holds, let $y \in \mathbb{Z}$ such that $e_1 k_1 - e_2 k_2 = -ys$. As d_1 and d_2 are relatively prime, there exists x_1, x_2 such that $y = d_2 x_1 - d_1 x_2$. If now we take $t_i = k_i + N_i x_i$, $i = 1, 2$, then (4.6) holds by definition; and

$$e_1 t_1 - e_2 t_2 = e_1 k_1 - e_2 k_2 + e_1 N_1 x_1 - e_2 N_2 x_2 = e_1 k_1 - e_2 k_2 + d_2 s x_1 - d_1 s x_2 = 0.$$

So, (4.7) follows. □

Lemma 4.5 describes an easy algorithm to decide whether a given $\mathbf{b}$ is locally of FL-type. As an example we note:

Corollary 4.6. *There are braidings of symmetrizable Cartan type which are not of FL-type.*

Proof. Let p be an odd prime number and take $N_1 = N_2 = p^2$, $a_{12} = a_{12} = -p$. Let k_1, k_2 be two elements not divisible by p such that

$$k_1 \not\equiv k_2 \mod p^2, \qquad k_1 \equiv k_2 \mod p.$$

Let q be a root of unity of order p^2 and let $b_{ii} = q^{k_i}$, $i = 1, 2$, $b_{12} = b_{21}$ the unique root of unity of odd order such that $b_{12}^2 = b_{11}^p$. Then $b_{12}^2 = b_{22}^p$, but $s = p^2$ and $e_1 = e_2 = 1$, so (4.5) does not hold. □

Example 4.7. *There are braidings of Cartan type which are locally of FL-type but not symmetrizable.*

Proof. Take $\mathbf{b} = (q^{d_i a_{ij}})$, where q is a root of 1 of order 5, $d_1 = 1$, $d_2 = 2$, $d_3 = 3$ and

$$(a_{ij}) = \begin{pmatrix} 2 & -3 & -3 \\ -4 & 2 & -3 \\ -1 & -2 & 2 \end{pmatrix}.$$

Then $\mathbf{b}$ is of Cartan type since $d_i a_{ij} = d_j a_{ji} \mod 5$ for all i, j. By Lemma 4.3, $\mathbf{b}$ is locally of FL-type. But (a_{ij}) is not symmetrizable. □

Lemma 4.8. *Let* $\mathbf{b}$ *be a braiding of Cartan type and rank 2 and assume* $b_{12} = b_{21}$. *If* $a_{12} = -1$ *and* a_{21} *is odd, then* $\mathbf{b}$ *is of FL-type.*

Proof. Let $n = -a_{21}$. Let $\widetilde{q}$ be a root of 1 such that $\widetilde{q}^n = b_{12}^{-1}$; then $b_{22}^n = b_{11} = b_{12}^{-2} = \widetilde{q}^{2n}$. Hence there exists an n-th root of 1 ω such that $b_{22} = \omega^2 \widetilde{q}^2$ since n is odd. We choose then $q = \omega\widetilde{q}$. $\square$

4.4 Proof of Theorem 1.1.

By Lemma 4.1 we can assume that $\mathbf{b}$ is symmetric, that is $b_{ij} = b_{ji}$ for all i, j. By Lemma 4.2 we can assume that $\mathbf{b}$ is connected.

Part (i). By Lemma 4.3 (if the type is different from G_2) or Lemma 4.8 (if the type is G_2), the braiding $\mathbf{b}$ is of FL-type. We now apply Theorem 3.1.

Part (ii). For any fixed pair i, j in $\{1, \dots, \theta\}$, the braiding of rank 2 corresponding to the submatrix supported by i, j is of FL-type and $\mathfrak{B}(V)$ is finite dimensional. By Theorem 3.1, we conclude that $a_{ij}a_{ji} = 0, 1, 2$ or 3. Since 3 is relatively prime to the orders of the b_{ii} whenever $a_{ij} = -3$ for some j by hypothesis, we can apply Lemma 4.3 and conclude again from Theorem 3.1 that $\mathbf{b}$ is of finite type whenever it is symmetrizable.

So, it only remains to show that: $\mathbf{b}$ is necessarily symmetrizable.

It is known that a matrix which is either simply-laced or has no cycles is symmetrizable, cf. [K, ex. 2.1]. We are reduced to prove that no cycle with a double or triple arrow can arise. We proceed by induction on θ.

Assume first that $\mathbf{b}$ is a cycle with a triple arrow. If $\theta \geq 4$, then we remove a suitable vertex and get a subdiagram with no cycles which is not of finite type. This is a contradiction.

So, assume $\theta = 3$. Then there are several possibilities of cycles with (at least) one triple arrow. We can discard two of them which are symmetrizable. We discard the rest because of the restrictions on the orders of b_{ii}. Let us proceed with the details. Consider a Cartan matrix

$$(a_{ij}) = \begin{pmatrix} 2 & -3 & -b \\ -1 & 2 & -c \\ -d & -e & 2 \end{pmatrix}.$$

Here b, c, d, e are positive integers such that $bd, ce = 1, 2$ or 3. This means that

$$b_{11}^3 = b_{22}, \quad b_{22}^c = b_{33}^e, \quad b_{11}^b = b_{33}^d.$$

Hence,

$$b_{11}^b = b_{33}^d, \quad b_{11}^{3c} = b_{33}^e.$$

We know that $b = 1$ or $d = 1$. Assume $b = 1$. Then $b_{33}^{3cd-e} = 1$. We have several subcases according to the values of c, d, e.

(i) If $e = 3$, then $c = 1$ and $b_{33}^{3(d-1)} = 1$. There are three possibilities:

If $d = 1$ the matrix is symmetrizable and we can apply Theorem 3.1. If $d = 2$, $b_{33}^3 = 1$. If $d = 3$, $b_{33}^6 = 1$. As we assume that the orders are odd, we should have $b_{33}^3 = 1$. These two possibilites are not possible by our choice following the rule (1.10).

(ii) If $e = 2$, then $c = 1$ and $b_{33}^{3d-2} = 1$. There are three possibilities:

If $d = 1$ $b_{33} = 1$, a possibility that we excluded. If $d = 2$, $b_{33}^4 = 1$, but we assume that the orders are odd. If $d = 3$, $b_{33}^7 = 1$. For this reason we exclude the order 7.

(iii) If $e = 1$, then $b_{33}^{3cd-1} = 1$. There are various possibilities:

As $cd = 1, 2, 3, 4, 6, 9$, $3cd - 1$ could take the values $2, 5, 8, 11, 17, 26$. Since we assume that the orders are odd, we have to exclude the orders 5, 11, 13, 17.

Let us now assume that $d = 1$. Then $b_{11}^{3c-be} = 1$.

(iv) If $c = 3$, then $e = 1$ and $b_{11}^{9-b} = 1$. There are three possibilities:

If $b = 1$, $b_{11}^8 = 1$; but the orders are odd. If $b = 2$, $b_{11}^7 = 1$. This is a new instance where 7 should be excluded. If $b = 3$, $b_{11}^6 = 1$. As we assume that the orders are odd, we should have $b_{11}^3 = 1$. This contradicts the rule (1.10).

(v) If $c = 2$, then $e = 1$ and $b_{11}^{6-b} = 1$. There are three possibilities:

If $b = 1$, $b_{11} = 5$. This is a new instance where 5 should be excluded. If $b = 2$, $b_{11}^4 = 1$, but we assume that the orders are odd. If $b = 3$, $b_{11}^3 = 1$. This contradicts the rule (1.10).

(vi) If $c = 1$, then $b_{11}^{3-be} = 1 = b_{33}^{3-be}$. There are various possibilities:

As $be = 1, 2, 3, 4, 6, 9$, $3 - be$ could take the values $2, 1, 0, -1, -3, -6$. The values $2, 1, -1$ are excluded by hypothesis; the values $-3, -6$ are excluded by the rule (1.10). The value 0 arises only when $\mathbf{b}$ is symmetrizable, but then we can apply Theorem 3.1.

We next assume that $\mathbf{b}$ is a cycle with no triple arrow but at least a double one. If $\theta \geq 6$, again we have a contradiction by removing a suitable vertex. If $\theta = 5$, we remove systematically different vertices. Since the resulting subdiagrams are symmetrizable and hence of finite type, we see that $\mathbf{b}$ has only one double arrow. We can easily get a contradiction.

Now we assume $\theta = 4$, with a Cartan matrix

$$(a_{ij}) = \begin{pmatrix} 2 & -2 & 0 & -b \\ -1 & 2 & -c & 0 \\ 0 & -d & 2 & -e \\ -f & 0 & -g & 2 \end{pmatrix}.$$

Here b, c, d, e, f, g are positive integers such that $bf, cd, eg = 1, 2$. By removing the third, respectively the fourth, vertex, we conclude that $bf = cd = 1$. There are three possibilities: $(e, g) = (1, 1), (1, 2)$ or $(2, 1)$. The first is not possible by a similar argument as for $\theta = 5$. The second corresponds to a symmetrizable matrix and the third is the first instance forcing to exclude the order 3.

We finally assume that $\theta = 3$. We have a 3-cycle with no triple arrow but at least a double one. Arguing as in the case of triple arrows, we eliminate all the possibilities except two; for those we exclude the orders 3 and 7. For instance,

$$(a_{ij}) = \begin{pmatrix} 2 & -2 & -1 \\ -1 & 2 & -2 \\ -2 & -1 & 2 \end{pmatrix},$$

then

$$b_{11}^2 = b_{22}, \quad b_{22}^2 = b_{33}, \quad b_{11} = b_{33}^2.$$

Hence $b_{11} = b_{11}^8$, which is not possible because the order of b_{11} is not 7.

Remark. We observe that the preceding proof of Theorem 1.1 Part (2) only needs the hypothesis "locally of FL-type" to conclude that

(4.8) A finite dimensional Nichols algebra $\mathfrak{B}(V)$ of rank 2 is necessarily of finite type.

If Γ is any finite abelian group such that (4.8) holds for $\mathfrak{B}(V)$ in ${}_\Gamma^\Gamma\mathcal{YD}$ then the conclusion of Theorem 1.1 Part (2) is valid for all $\mathfrak{B}(V)$ in ${}_\Gamma^\Gamma\mathcal{YD}$.

For further use, we list the Cartan matrices, up to numbering, causing trouble for small values of p:

(4.9) For $p = 3$, the matrix

$$(a_{ij}) = \begin{pmatrix} 2 & -2 & -1 \\ -1 & 2 & -1 \\ -2 & -1 & 2 \end{pmatrix}.$$

(4.10) For $p = 3$, the matrix

$$(a_{ij}) = \begin{pmatrix} 2 & -2 & 0 & -1 \\ -1 & 2 & -1 & 0 \\ 0 & -1 & 2 & -2 \\ -1 & 0 & -1 & 2 \end{pmatrix}.$$

(4.11) For $p = 5$, the matrix

$$(a_{ij}) = \begin{pmatrix} 2 & -3 & -1 \\ -1 & 2 & -1 \\ -2 & -1 & 2 \end{pmatrix}.$$

(4.12) For $p = 5$, the matrix

$$(a_{ij}) = \begin{pmatrix} 2 & -3 & -1 \\ -1 & 2 & -2 \\ -1 & -1 & 2 \end{pmatrix}.$$

(4.13) For $p = 7$, the matrix

$$(a_{ij}) = \begin{pmatrix} 2 & -3 & -1 \\ -1 & 2 & -1 \\ -3 & -2 & 2 \end{pmatrix}.$$

(4.14) For $p = 7$, the matrix

$$(a_{ij}) = \begin{pmatrix} 2 & -2 & -1 \\ -1 & 2 & -2 \\ -2 & -1 & 2 \end{pmatrix}.$$

(4.15) For $p = 11$, the matrix

$$(a_{ij}) = \begin{pmatrix} 2 & -3 & -1 \\ -1 & 2 & -2 \\ -2 & -1 & 2 \end{pmatrix}.$$

(4.16) For $p = 13$, the matrix

$$(a_{ij}) = \begin{pmatrix} 2 & -3 & -1 \\ -1 & 2 & -3 \\ -3 & -1 & 2 \end{pmatrix}.$$

(4.17) For $p = 17$, the matrix

$$(a_{ij}) = \begin{pmatrix} 2 & -3 & -1 \\ -1 & 2 & -2 \\ -3 & -1 & 2 \end{pmatrix}.$$

§5. Nichols algebras over $\mathbb{Z}/(p)$.

In this section, Γ will denote $\mathbb{Z}/(p)$, p an odd prime. We first discuss Nichols algebras of rank 2. If V is a Yetter-Drinfeld module of dimension 2 satisfying (1.6), then there exists a generator u of Γ, $q \in k^\times$ of order p and integers b, d such that

$$g(1) = u, \quad g(2) = u^b, \quad \langle\chi(1), u\rangle = q, \quad \langle\chi(2), u\rangle = q^d. \tag{5.1}$$

So $b_{11} = q, \quad b_{22} = q^{bd}$.

Dynkin diagram of type A_2. We should have

$$\langle\chi(1), g(2)\rangle\langle\chi(2), g(1)\rangle = b_{11}^{-1} = b_{22}^{-1}.$$

This means $b + d \equiv -1 \equiv -bd \mod p$. It follows readily that $b^2 + b + 1 \equiv 0 \mod p$. Hence $p = 3$ and $b \equiv 1 \mod p$, or $b \not\equiv 1 \mod p$ is a cubic root of 1. In the last case, b exists if and only if $p - 1$ is divisible by 3. The corresponding matrices are not symmetric if $p \neq 3$.

Dynkin diagram of type B_2. We should have

$$\langle\chi(1), g(2)\rangle\langle\chi(2), g(1)\rangle = b_{11}^{-1} = b_{22}^{-2}.$$

This means $b + d \equiv -1 \equiv -2bd \mod p$. Thus $2b^2 + 2b + 1 \equiv 0 \mod p$ and looking at the discriminant of this equation we see that it has a solution if and only if -1 is a square, *i.e.* exactly when $p \equiv 1 \mod 4$. The corresponding matrices are not symmetric.

Dynkin diagram of type G_2. By (1.10), we have $p > 3$. We should have

$$\langle\chi(1), g(2)\rangle\langle\chi(2), g(1)\rangle = b_{11}^{-1} = b_{22}^{-3}.$$

This means $b + d \equiv -1 \equiv -3bd \mod p$. Thus $3b^2 + 3b + 1 \equiv 0 \mod p$ and looking at the discriminant of this equation we see that it has a solution if and only if -3 is a square $\mod p$. By the quadratic reciprocity law, this happens exactly when $p \equiv 1 \mod 3$. The matrices are not symmetric.

We now conclude the proof of the existence part of Theorem 1.3.

Proposition 5.1. *There is no Nichols algebra of rank ≥ 3 over $\mathbb{Z}/(p)$ with finite Cartan matrix except when $p = 3$ and the corresponding Dynkin diagram is $A_2 \times A_1$ or $A_2 \times A_2$.*

Proof. We first consider Dynkin diagrams of rank 3. We have the following cases:

$$\begin{array}{llll} (a)\, A_2 \times A_1, & (b)\, B_2 \times A_1, & (c)\, G_2 \times A_1, & \\ (d)\, A_3, & (e)\, B_3, & (f)\, C_3, & (g)\, A_1 \times A_1 \times A_1. \end{array}$$

The case (g) does not arise, as shown in [AS2, Section 4]. Therefore we can fix a numeration of the vertices of the Dynkin diagram such that the vertices 1 and 2 (resp., 1 and 3) are connected (resp., not connected). We also assume that there is only one arrow between 1 and 2 in cases (e) an (f). That is,

$$\begin{array}{lll} (a)\ \underset{1}{\circ} - \underset{2}{\circ} \quad \underset{3}{\circ}, & (b)\ \underset{1}{\circ} \Rightarrow \underset{2}{\circ} \quad \underset{3}{\circ}, & (c)\ \underset{1}{\circ} \Rrightarrow \underset{2}{\circ} \quad \underset{3}{\circ}, \\ (d)\ \underset{1}{\circ} - \underset{2}{\circ} - \underset{3}{\circ}, & (e)\ \underset{1}{\circ} - \underset{2}{\circ} \Rightarrow \underset{3}{\circ}, & (f)\ \underset{1}{\circ} - \underset{2}{\circ} \Leftarrow \underset{3}{\circ}. \end{array}$$

If V is a Yetter-Drinfeld module of dimension 3 satisfying (1.6) and of Cartan type (a), (b), ... or (f), then there exist a generator u of Γ, $q \in k^{\times}$ of order p and integers b, d, e, f (none of them divisible by p) such that

$$\begin{array}{ccc} g(1) = u, & g(2) = u^b, & g(3) = u^e, \\ \langle\chi(1), u\rangle = q, & \langle\chi(2), u\rangle = q^d, & \langle\chi(3), u\rangle = q^f. \end{array}$$

So $b_{11} = q$, $b_{22} = q^{bd}$, $b_{33} = q^{ef}$. Also, $\langle\chi(1), g(3)\rangle\langle\chi(3), g(1)\rangle = 1$ means

$$e + f \equiv 0 \mod p. \tag{5.2}$$

Now, considering the subdiagram supported by the vertices 1 and 2, we conclude from the arguments above for the rank 2 case that

(5.3) In cases (a), (d), (e) and (f), $b^2 + b + 1 \equiv 0 \mod p$, $bd \equiv 1 \mod p$ and $p = 3$ or $p \equiv 1 \mod 3$.
(5.4) In case (b), $2b^2 + 2b + 1 \equiv 0 \mod p$, $2bd \equiv 1 \mod p$ and $p \equiv 1 \mod 4$.
(5.5) In case (c), $3b^2 + 3b + 1 \equiv 0 \mod p$, $3bd \equiv 1 \mod p$ and $p \equiv 1 \mod 3$.

On the other hand, in cases (a), (b) and (c) we have $\langle\chi(2), g(3)\rangle\langle\chi(3), g(2)\rangle = 1$, *i.e.*

$$ed + bf \equiv 0 \mod p. \tag{5.6}$$

Now, combining (5.6) with (5.2) we conclude that $b \equiv d \mod p$. Hence:

In case (a), $b^2 \equiv 1 \mod p$. But also $b^3 \equiv 1 \mod p$, so $b \equiv 1 \mod p$ and $p = 3$.

In case (b), $2b^2 \equiv 1 \mod p$ and thus $b \equiv -1 \mod p$ and $1 \equiv 0 \mod p$, a contradiction.

In case (c), $3b^2 \equiv 1 \mod p$. Plugging this into the first equation of (5.5) we easily get a contradiction.

Now we turn to the remaining cases. In case (d), we have

$$\langle\chi(2), g(3)\rangle\langle\chi(3), g(2)\rangle = b_{22}^{-1} = b_{33}^{-1};$$

using (5.2), this implies

$$f(b-d) \equiv -1 \equiv f^2 \mod p.$$

Thus $b - d \equiv f \mod p$ and $(b-d)^2 \equiv b^2 + b - 2 \equiv -1 \mod p$; this last equation contradicts the first of (5.3). In case (e), we have $\langle\chi(2), g(3)\rangle\langle\chi(3), g(2)\rangle = b_{22}^{-1} = b_{33}^{-2}$; using (5.2), this implies

$$f(b-d) \equiv -1 \equiv 2f^2 \mod p.$$

Thus $b - d \equiv 2f \mod p$ and $(b-d)^2 \equiv b^2 + b - 2 \equiv 4f^2 \equiv -2 \mod p$; this last equation contradicts the first of (5.3). In case (f), we have $\langle\chi(2), g(3)\rangle\langle\chi(3), g(2)\rangle = b_{22}^{-2} = b_{33}^{-1}$; using (5.2), this implies

$$f(b-d) \equiv -2 \equiv f^2 \mod p.$$

Thus $b - d \equiv f \mod p$ and $(b-d)^2 \equiv b^2 + b - 2 \equiv f^2 \equiv -2 \mod p$; this last equation contradicts the first of (5.3).

We have shown that the only possibility in rank 3 is case (a) with $p = 3$. Then, if V is a Yetter-Drinfeld module of Cartan type satisfying (1.6) with finite Cartan matrix and rank ≥ 3, then $p = 3$, the corresponding Dynkin diagram should have at most 2 connected components– *cf.* case (g)– and each component is of type A_1 or A_2. On the other hand, let u be a generator of $\mathbb{Z}/(3)$ and q a root of 1 of order 3. It is easy to see that the sequences

$$\begin{gathered} g(1) = u = g(2), \quad g(3) = u^e = g(4), \\ \langle\chi(1), u\rangle = q = \langle\chi(2), u\rangle, \quad \langle\chi(3), u\rangle = q^{-e} = \langle\chi(4), u\rangle \end{gathered} \tag{5.7}$$

define a Yetter-Drinfeld module of rank 4 over $\mathbb{Z}/(3)$, which is of Cartan type and has Dynkin diagram $A_2 \times A_2$. $\square$

Lemma 5.2. *Let $\mathfrak{B}(V)$ be a finite dimensional Nichols algebra over $\mathbb{Z}/(p)$. Then V is of finite Cartan type.*

Proof. We know that the Lemma is true whenever p is different from 3, 5, 7, 11, 13, 17. Assume that p is one of these small primes. By the proof of Theorem 1.1 (ii), it would be enough to show that no Cartan matrix as in (4.9), ... , (4.17) is possible over $\mathbb{Z}/(p)$. Note that the relative primeness condition is satisfied for $p = 3$ since no subdiagram of type G_2 is possible over $\mathbb{Z}/(3)$. All these matrices have a subdiagram of rank 2 of type B_2 or G_2. This eliminates all the primes except for 13. We show then that no matrix like (4.16) exists over $\mathbb{Z}/(13)$. Suppose in the contrary that it exists. Then there exists a generator u of Γ, $q \in k^\times$ of order p and integers b, c, d, e (none of them divisible by 13) such that $g(1) = u$, $g(2) = u^b$, $g(3) = u^c$, $\langle\chi(1), u\rangle = q$, $\langle\chi(2), u\rangle = q^d$, $\langle\chi(3), u\rangle = q^e$; and the following equations hold

$$b + d \equiv -3 \equiv -bd \mod 13, \tag{5.8}$$

$$c + e \equiv -1 \equiv -3ec \mod 13, \tag{5.9}$$

$$be + dc \equiv -ec \equiv -3bd \mod 13. \tag{5.10}$$

Now (5.8) implies $(b, d) = (2, 8)$ or $(8, 2)$; and (5.9) implies $(c, e) = (5, 7)$ or $(7, 5)$. We have four possibilities for $be + dc$ but none of them gives $-9 \mod 13$; that is, (5.10) does not hold. □

Lemma 5.3. *Let R be a finite dimensional braided Hopf algebra in ${}^{\Gamma}_{\Gamma}\mathcal{YD}$, $\Gamma = \mathbb{Z}/(p)$. Then $\dim P(R) \leq 2$ for $p > 3$; and $\dim P(R) \leq 4$ for $p = 3$.*

Proof. Consider first the coradical filtration of R and the subalgebra S of the corresponding graded coalgebra generated by $P(R)$. Then S is a Nichols algebra and the claim follows from Proposition 5.1 and Lemma 5.2. □

Proposition 5.4. *Let R be a finite dimensional braided Hopf algebra in ${}^{\Gamma}_{\Gamma}\mathcal{YD}$, $\Gamma = \mathbb{Z}/(p)$. Assume that (1.1), (1.2) and (1.3) hold. Then R is a Nichols algebra.*

Proof. Let $S = R^*$; it is a braided Hopf algebra in ${}^{\Gamma}_{\Gamma}\mathcal{YD}$ and satisfies (1.1), (1.2) and (1.4); that is, S is graded, $S_0 = \Bbbk 1$ and is generated in degree 1. We want to show that (1.3) holds for S; hence (1.4) holds for R. See Lemma 5.5 below.

We know that $V := S(1) \subseteq P(S)$ and $\mathfrak{B}(V)$ is an epimorphic image of S as braided Hopf algebras. We want to prove $V = P(S)$, that is $S = \mathfrak{B}(V)$. If $\dim V = 1$, we are done by [AS2, Th. 3.2]. If $\dim V \geq 2$ and $p > 3$, or $\dim V \geq 4$ and $p = 3$, then we are done by Lemma 5.3 applied to S. Thus the remaining cases are $\dim V = 2$ or 3 and $p = 3$.

We assume first that V is 2-dimensional with basis x_1, x_2. Then there exists a generator u of $\mathbb{Z}/(3)$, $q \in k^\times$ of order 3 and integers b, d such that

$$g(1) = u, \quad g(2) = u^b, \quad \langle\chi(1), u\rangle = q, \quad \langle\chi(2), u\rangle = q^d. \tag{5.1}$$

So $b_{11} = q, \quad b_{22} = q^{bd}, \quad b_{12} = q^d, \quad b_{21} = q^b$.

Let $z := \mathrm{ad}_c(x_1)(x_2) = x_1x_2 - b_{12}x_2x_1$ be the braided commutator. There are two cases: a quantum plane or A_2.

In the first case we have to show $z = 0$ and $x_1^3 = 0, x_2^3 = 0$.

But z is primitive in this case and

$$\delta(z) = u^{1+b} \otimes z, \qquad u.z = q^{1+d}z.$$

Now $u^{1+b}.z = q^{(1+b)(1+d)}z$. Since $b = -d$, the exponent $(1+b)(1+d) = 1 - b^2$ is 0 mod 3. This is a contradiction by [AS2, Lemma 3.1] unless $z = 0$.

Since the third powers of the primitive elements x_1, x_2 are primitive by the quantum binomial formula and have trivial coaction, we see that $x_1^3 = 0$ and $x_2^3 = 0$ again by [AS2, Lemma 3.1].

In the second case we have to show the Serre relations

$$s_1 := (\mathrm{ad}_c(x_1))^2(x_2) = 0, s_2 := (\mathrm{ad}_c(x_2))^2(x_1) = 0$$

and also the root vector relations $x_1^3 = 0, x_2^3 = 0$ and $z^3 = 0$, since it is not difficult to see that these are the defining relations of $\mathfrak{B}(V)$ when the type is A_2 (cf. [AS4, part 3 of the proof of Theorem 3.6]). In this situation, $b = d = 1$. But for $i = 1, 2$, $\delta(s_i) = u^{2+1} \otimes s_i$. Again, this is a contradiction unless $s_i = 0$, since the elements s_i are primitive (cf. Lemma A.1).

By the same argument as before, $x_1^3 = 0, x_2^3 = 0$. Then it is easy to see that also the third root vector z is primitive. Hence again we conclude $z^3 = 0$.

We assume finally that $\dim S(1)$ is 3. In this case, $S(1)$ is the direct sum $V_1 \oplus V_2$, where say V_1 is of type A_2 and V_2 is of type A_1, cf. Proposition 5.1. Applying the considerations for case 2, we see that S is the twisted tensor product of $\mathfrak{B}(V_1)$ and $\mathfrak{B}(V_2)$. It follows that S is $\mathfrak{B}(V)$, as claimed. $\square$

Then next Lemma is implicit in [AG, Example 3.2.8]. It was also observed by the referee of [AS2]. We first recall the basic notions over arbitrary Hopf algebras H with bijective antipode S (see for example [AG, Section 2]). If $V \in^H_H \mathcal{YD}$ is finite-dimensional, the dual $V^* = \mathrm{Hom}(V, \Bbbk)$ is in ${}^H_H\mathcal{YD}$ with the usual structure. Let $f \in V^*$. Then $(h \cdot f)(v) = f(S(v))$ for all $h \in H, v \in V$, defines the action of H; the coaction $\delta(f) = f_{(-1)} \otimes f_{(0)}$ is given by the equation $f_{(-1)}f_{(0)}(v) = S^{-1}(v_{-1})f(v_0)$ for all $v \in V$, where $\delta(v) = v_{-1} \otimes v_0$ denotes the coaction of v.

Let $R = \oplus_{n\geq 0}R(n)$ be a finite-dimensional graded Hopf algebra in ${}^H_H\mathcal{YD}$. The dual $S = R^* = \oplus_{n\geq 0}R(n)^*$ is in ${}^H_H\mathcal{YD}$ as just explained. To define S as a braided Hopf algebra we introduce for any finite-dimensional $V, W \in^H_H \mathcal{YD}$ the isomorphism

$$\Phi : W^* \otimes V^* \to (V \otimes W)^*$$

with $\Phi(\varphi \otimes \psi)(v \otimes w) = \psi(v)\varphi(w)$ for all $\varphi \in W^*, \psi \in V^*, v \in V, w \in W$.

Then S is a graded Hopf algebra in ${}^H_H\mathcal{YD}$ with multiplication $\Delta^*\Phi$ and comultiplication $\Phi^{-1}\mu^*$, where Δ and μ denote the comultiplication and multiplication of R. (This is R^{*bop} in the notation of [AG, Section 2] and other versions of the braided dual would also work). If R is not finite-dimensional but has finite-dimensional homogeneous components, then in the same way the graded dual $S = R^* = \oplus_{n\geq 0}R(n)^*$ is a graded Hopf algebra in ${}^H_H\mathcal{YD}$.

Lemma 5.5. *Let H be a Hopf algebra with bijective antipode and $R = \oplus_{n\geq 0} R(n)$ a graded Hopf algebra in ${}^H_H\mathcal{YD}$ with finite-dimensional homogeneous components $R(n), n \geq 0$, and $R(0) = \Bbbk 1$. Let $S = \oplus_{n\geq 0} R(n)^*$ be the graded dual of R. S is a graded Hopf algebra in ${}^H_H\mathcal{YD}$ with $S(0) = \Bbbk 1$. Then $R(1) = P(R)$ if and only if S is generated as an algebra by $S(1)$.*

Proof. Let $\Delta^k : R \to R^{\otimes(k+1)} = R \otimes \cdots \otimes R$ ($k+1$ times), $k \geq 0$, be the iterated comultiplication defined by $\Delta^0 = \mathrm{id}, \Delta^1 = \Delta, \Delta^k = (\mathrm{id} \otimes \Delta)\Delta^{k-1}, k \geq 2$. Let $\pi : R \to R(1)$ be the projection. It is easy to see that the Lemma follows from the equivalence of the following statements:

(1) R(1) = P(R).

(2) For all $n \geq 2$, $\phi_n := \pi^{\otimes n}\Delta^{n-1} : R \to R(1)^{\otimes n}$ is injective on $R(n)$.

Assume (2). Then the only primitive elements are in degree one. This proves (1), since in general $R(1) \subset P(R)$ by the assumption $R(0) = \Bbbk 1$.

Assume (1) and let $x \in R(n), n \geq 2$, with $\phi_n(x) = 0$. Write $\Delta(x) = \sum_{i=0}^n y_i$, where $y_i \in R(i) \otimes R(n-i)$, $0 \leq i \leq n$. By coassociativity, for all $1 \leq i \leq n-1$, $\phi_n = (\phi_i \otimes \phi_{n-i})\Delta$. For all $0 \leq j \leq n, i \neq j$, $\Delta^{i-1}(R(j))$ has no non-zero component in $R(1)^{\otimes i}$. Hence

$$\phi_n(x) = (\phi_i \otimes \phi_{n-i})(y_i), \text{ for all } 1 \leq i \leq n-1.$$

Thus we see by induction that $y_i = 0$ for all $1 \leq i \leq n-1$. Hence x must be primitive. By (1), we conclude $x \in R(1)$ and then $x = 0$, since $n \geq 2$. □

Finally we mention two easy counterexamples to Conjecture 1.4 when the Hopf algebra is not finite-dimensional or the characteristic is not 0:

(5.11). Let F be a field of positive characteristic p. Let S be the (usual) Hopf algebra $F[x]/\langle x^{p^2}\rangle$ with $x \in P(S)$. Then $x^p \in P(S)$. Hence $R = S^*$ satisfies (1.1), (1.2) and (1.3) but not (1.4).

(5.12). Let $S = \Bbbk[X] = \oplus_{n\geq 0} S(n)$ be a polynomial algebra in one variable. We consider S as a braided Hopf algebra in ${}^H_H\mathcal{YD}$, where $H = \Bbbk\Gamma$, Γ an infinite cyclic group with generator g, with action, coaction and comultiplication given by

$$\delta(X^n) = g^n \otimes X^n, \quad g.X = qX, \quad \Delta(X) = X \otimes 1 + 1 \otimes X.$$

Here $q \in \Bbbk$ is a root of 1 of order N. That is, S is a so-called quantum line. Then S satisfies (1.1), (1.2) and (1.4) but not (1.3) since X^N is also primitive. Hence the graded dual $R = S^d = \oplus_{n\geq 0} S(n)^*$ is a braided Hopf algebra satisfying (1.1), (1.2) and (1.3) but not (1.4). Let us present explicitly R. It is a vector space with basis y_n, $n \geq 0$; the structure is given by $y_0 = 1$,

$$y_n y_m = \begin{bmatrix} m+n \\ n \end{bmatrix}_q y_{n+m}, \quad \Delta(y_n) = \sum_{0\leq i\leq n} y_i \otimes y_{n-i},$$
$$\delta(y_n) = g^{-n} \otimes y_n, \quad g.y_n = q^{-n} y_n.$$

We do not know any finite dimensional counterexample in characteristic zero. Note that in both examples above a Frobenius homomorphism is given implicitly. In characteristic zero, Lusztig said that "there are no powers of the quantum Frobenius map" [L4, 8.5, p. 58]; this could be related to our lack of examples.

§6. Isomorphisms between bosonizations.

We begin with a general Lemma whose proof is straightforward. We shall denote the comultiplication of R by $\Delta_R(r) = \sum r^{(1)} \otimes r^{(2)}$; we omit most of the time the summation sign.

Lemma 6.1. *Let H be a Hopf algebra, $\psi : H \to H$ an automorphism of Hopf algebras, V, W Yetter-Drinfeld modules over H.*

(1) *Let V^ψ be the same space underlying V but with action and coaction*

$$h._\psi v = \psi(h).v, \quad \delta^\psi(v) = \left(\psi^{-1} \otimes \mathrm{id}\right) \delta(v), \quad h \in H, v \in V. \tag{6.1}$$

Then V^ψ is also a Yetter-Drinfeld module over H. If $T : V \to W$ is a morphism in ${}_H^H\mathcal{Y}D$, then $T : V^\psi \to W^\psi$ also is. Moreover, the braiding $c : V^\psi \otimes W^\psi \to W^\psi \otimes V^\psi$ coincides with the braiding $c : V \otimes W \to W \otimes V$.

(2) *If R is an algebra (resp., a coalgebra, a Hopf algebra) in ${}_H^H\mathcal{Y}D$ then R^ψ also is, with the same structural maps.*

(3) *Let R be a Hopf algebra in ${}_H^H\mathcal{YD}$. Then the map $\Psi : R^\psi \# H \to R\# H$ given by $\Psi(r\#h) = r\#\psi(h)$ is an isomorphism of Hopf algebras.*

Proof. The proof of (1) is a direct computation that we leave to the reader. The statement (2) follows from (1). Let us check (3). If $r, s \in R$ and $h, g \in H$ then

$$\Psi\left((r\#h)(s\#g)\right) = \Psi\left(r h_{(1)} ._\psi s\# h_{(2)} g\right) = r\psi(h_{(1)}).s\#\psi(h_{(2)}g);$$
$$\Psi(r\#h)\Psi(s\#g) = (r\#\psi(h))(s\#\psi(g)) = r\psi(h)_{(1)}.s\#\psi(h)_{(2)}\psi(g).$$

That is, Ψ is an algebra map. On the other hand,

$$\Delta\Psi(r\#h) = \Delta(r\#\psi(h)) = r^{(1)}\#(r^{(2)})_{(-1)}\psi(h)_{(1)} \otimes (r^{(2)})_{(0)}\#\psi(h)_{(2)};$$
$$\begin{aligned}(\Psi\otimes\Psi)\Delta(r\#h) &= (\Psi\otimes\Psi)\left(r^{(1)}\#\psi^{-1}\left((r^{(2)})_{(-1)}\right) h_{(1)} \otimes (r^{(2)})_{(0)}\#h_{(2)}\right)\\ &= r^{(1)}\#(r^{(2)})_{(-1)}\psi(h_{(1)}) \otimes (r^{(2)})_{(0)}\#\psi(h_{(2)}).\end{aligned}$$

Thus Ψ is a bialgebra map and *a fortiori* a Hopf algebra map. □

Let H be a cosemisimple Hopf algebra. Let $A = \oplus_{n\geq 0} A(n)$ be a coradically graded Hopf algebra with coradical $A_0 = A(0)$ isomorphic to H. Let $\iota : A(0) \to A$ denote the inclusion. Let $\pi : A \to A(0)$ be the unique graded projection with image $A(0)$ and let $R = \{a \in A : (\mathrm{id}\otimes\pi)\Delta(a) = a \otimes 1\}$. Let B be another Hopf algebra with coradical B_0 isomorphic to H.

Lemma 6.2. *Let $\Psi : A \to B$ be an isomorphism of Hopf algebras. Let $B(n) := \Psi(A(n))$; then B is also coradically graded with respect to the grading $B = \oplus_{n\geq 0} B(n)$. Let $\psi : H \to H$ denote the isomorphism induced by the restriction of Ψ, with respect to fixed identifications $A_0 \simeq H$, $B_0 \simeq H$. Let $\jmath$, ζ, S denote the same objects as ι, π, R but with respect to the grading in B. Then*

$\Psi(R) = S$ and the restriction $\phi : R \to S$ of Ψ is a morphism $R \to S^{\psi}$ of braided Hopf algebras in ${}^H_H\mathcal{YD}$. Moreover, the following diagram commutes

$$\begin{array}{ccc} A & \xrightarrow{\Psi} & B \\ \simeq\big\downarrow & & \simeq\big\downarrow \\ R\#H & \xrightarrow{\phi\otimes\psi} & S\#H \end{array}$$

where the vertical isomorphisms are the inverses of the bosonization maps.

Note that $R\#H \xrightarrow{\phi\otimes\psi} S\#H$ factorizes as the composition of two Hopf algebra maps: $R\#H \xrightarrow{\phi\otimes\mathrm{id}} S^{\psi}\#H \xrightarrow{\mathrm{id}\otimes\psi} S\#H$.

Proof. It is clear that $B = \oplus_{n\geq 0} B(n)$ is a grading of Hopf algebras. Since Ψ preserves the terms of the coradical filtration, we have

$$B_m = \Psi(A_m) = \Psi\left(\oplus_{0\leq n\leq m} A(n)\right) = \oplus_{0\leq n\leq m} B(n);$$

that is, B is coradically graded. It follows at once that

$$\jmath\Psi = \Psi\iota, \quad \Psi\pi = \zeta\Psi. \tag{6.2}$$

Hence $\Psi(R) = S$. We check that ϕ is a morphism from R to S^{ψ}. It preserves the multiplication because is the restriction of the algebra map Ψ. It preserves the comultiplication because Ψ is a coalgebra map and by (6.2). It preserves the action and the coaction:

$$\begin{aligned} \phi(h.r) &= \Psi\left(h_{(1)} r\, \mathcal{S}(h_{(2)})\right) = \psi\left(h_{(1)}\right)\phi(r)\psi\left(\mathcal{S}(h_{(2)})\right) \\ &= (\psi(h))_{(1)}\phi(r)\,\mathcal{S}\left((\psi(h))_{(2)}\right) = \psi(h).\phi(r) = h._{\psi}\phi(r); \\ \delta^{\psi}\phi(r) &= (\psi^{-1}\otimes\mathrm{id})(\zeta\otimes\mathrm{id})(\Psi\otimes\Psi)\Delta(r) = (\psi^{-1}\zeta\Psi\otimes\Psi)\Delta(r) \\ &= (\pi\otimes\Psi)\Delta(r) = (\mathrm{id}\otimes\phi)\delta(r). \end{aligned}$$

Here again we used (6.2). The last statement follows because Ψ is an algebra map. $\square$

Let now $H = k\Gamma$, where Γ is a finite abelian group. Let $g(1), \dots, g(\theta) \in \Gamma$, $\chi(1), \dots, \chi(\theta) \in \widehat{\Gamma}$ and let V be the Yetter-Drinfeld module with structure given by (1.5). Let also $h(1), \dots, h(\theta) \in \Gamma$, $\eta(1), \dots, \eta(\theta) \in \widehat{\Gamma}$ and let analogously W be the Yetter-Drinfeld module with structure given by (1.5) with $g(i)$'s, resp. $\chi(j)$'s, replaced by $h(i)$'s, resp. $\eta(j)$'s. Let R, S be the corresponding Nichols algebras and $A = R\#H$, $B = S\#H$.

Proposition 6.3. *Assume that R and S are finite dimensional. The Hopf algebras A and B are isomorphic if and only if there exist $\varphi \in \mathrm{Aut}(\Gamma)$ and $\sigma \in \mathbb{S}_{\theta}$ such that*

$$g(j) = \varphi^{-1}\left(h(\sigma j)\right), \qquad \chi(j) = \eta(\sigma j)\varphi, \qquad 1 \leq j \leq \theta. \tag{6.3}$$

Proof. Assume that $\Psi : A \to B$ is an isomorphism of Hopf algebras. We claim that $\Psi(A(n)) = B(n)$ for all $n \geq 0$. This is clear for $n = 0$ since Ψ preserves the coradical filtration. For $n = 1$ we argue as in [AS2, Lemma 5.4]. Indeed, let us consider the adjoint action of Γ on A. The decomposition $A_1 = A(0) \oplus A(1)$ is a decomposition of Γ-modules. By [AS2, Lemma 3.1] $A(0)$ is the isotypical component of trivial type of the Γ-module A_1 (here we use that A is finite dimensional). Hence $A(1)$ is the sum of all the other isotypical components. This implies that $\Psi(A(1)) = B(1)$, since Ψ intertwines the respective adjoint actions of Γ. It is not difficult to see that A is generated by A_1 as an algebra, by definition of Nichols algebra and [AS2, Lemma 2.4 (iii)]. Hence $\Psi(A(n)) = B(n)$ for all $n \geq 0$. We can apply now (the second half of) Lemma 6.2. The automorphism $\psi \in \operatorname{Aut}(H)$ is determined by $\varphi \in \operatorname{Aut}(\Gamma)$. We also know that $R \simeq S^\psi$ as braided Hopf algebras; but this is equivalent to $V \simeq W^\psi$ in ${}^H_H\mathcal{YD}$. This is possible if and only if (6.3) holds. If (6.3) holds, we do not need to assume that R and S are finite dimensional. By what we have just said, $R \simeq S^\psi$. Hence $R\#H \simeq S^\psi\#H$. By Lemma 6.1, we infer that $A \simeq B$. $\square$

We now finish the proof of Theorem 1.3. We shall apply Proposition 6.3 with $\Gamma = \mathbb{Z}/(p)$. Let us first assume $\theta = 2$. Let $g(1), g(2) \in \Gamma$ and $\chi(1), \chi(2) \in \widehat{\Gamma}$ define a Nichols algebra of finite Cartan type. Let $u \in \Gamma - 1$, $q \in k^\times$ of order p and integers b, d such that the $g(i)$'s and $\chi(j)$'s are given by (5.1). Note that d is determined by b. We denote by $R(q, b)$ the Nichols algebra corresponding to the $g(i)$'s and $\chi(j)$'s. Let now $h(1), h(2) \in \Gamma$, $\eta(1), \eta(2) \in \widehat{\Gamma})$ define another Nichols algebra of finite Cartan type. Let also $v \in \Gamma - 1$, $\widetilde{q} \in k^\times$ of order p, integers s, t and

$$h(1) = v, \quad h(2) = v^s, \quad \langle \eta(1), v\rangle = \widetilde{q}, \quad \langle \eta(2), v\rangle = \widetilde{q}^t.$$

We can assume, by Proposition 6.3, that $u = v$. Then the Nichols algebra corresponding to the $h(i)$'s and $\eta(j)$'s is $R(\widetilde{q}, s)$.

Lemma 6.4. *The Hopf algebras $A = R(q, b)\#k\Gamma$ and $B = R(\widetilde{q}, s)\#k\Gamma$ are isomorphic if and only if*

(i) *$q = \widetilde{q}$ and $b \equiv s \mod p$ when the type is B_2 or G_2,*
(ii) *$q = \widetilde{q}$ and $b \equiv s$ or $\equiv -1 - s \mod p$ when the type is A_2 .*

Proof. We assume that A and B are isomorphic; it is clear that they are of the same type. Let φ, σ be as in Proposition 6.3, *i.e.* (6.3) holds. If $\sigma = \mathrm{id}$, then $\varphi(u) = u$ and hence $q = \widetilde{q}$, $b = s$. If $\sigma \neq \mathrm{id}$, then $\varphi(u) = u^s$, $\varphi(u^b) = u$,

$$q = \langle \chi(1), u\rangle = \langle \eta(2), u^s\rangle = \widetilde{q}^{st}, \qquad q^d = \langle \chi(2), u\rangle = \langle \eta(1), u^s\rangle = \widetilde{q}^s.$$

These equalities imply $bs \equiv 1 \mod p$, $dt \equiv 1 \mod p$. Hence $st \equiv (bd)^{-1} \mod p$. We know that $(bd)^{-1} \equiv (st)^{-1} \equiv 1, 2$ or $3 \mod p$ if the type is respectively A_2, B_2 or G_2. This leads immediately to a contradiction unless the type is A_2. But in this last case, $s \equiv d \mod p$ and $t \equiv b \mod p$. Hence $q = \widetilde{q}$ and $b \equiv -1 - s \mod p$. $\square$

We now pass to the cases $\theta = 3$ and $\theta = 4$. We denote by $R_4(q,e)$, resp. $R_3(q,e)$, the Nichols algebra corresponding to the sequence in (5.7), resp. the sequence of the first three terms in (5.7). Here q is a third root of 1 and $e = 1$ or 2. By Proposition 6.3, arguing as for $\theta = 2$, we are reduced to prove:

Lemma 6.5. *Let $q, \widetilde{q}$ be third roots of 1 and $e, \widetilde{e} = 1$ or 2.*

(i). The Hopf algebras $R_4(q,e)\#k\mathbb{Z}/(3)$ and $R_4(\widetilde{q},\widetilde{e})\#k\mathbb{Z}/(3)$ are isomorphic if and only if $e = \widetilde{e}$.

(ii). The Hopf algebras $R_3(q,e)\#k\mathbb{Z}/(3)$ and $R_3(\widetilde{q},\widetilde{e})\#k\mathbb{Z}/(3)$ are isomorphic if and only if $e = \widetilde{e}$ and $q = \widetilde{q}$.

Proof. All the elements $g(i)$ are equal for $e = 1$ but $g(1) \neq g(3)$ for $e = 2$. Hence, by Proposion 6.3, $e = \widetilde{e}$ if the Hopf algebras are isomorphic. By Proposition 6.3 again, $\phi = \mathrm{id}$ resp. $\phi(u) = u^2$ and $\sigma(1) = 3, \sigma(2) = 4, \sigma(3) = 1, \sigma(4) = 2$ define an isomorphism $R_4(q,1)\#k\mathbb{Z}/(3) \cong R_4(q^{-1},1)\#k\mathbb{Z}/(3)$ resp. $R_4(q,2)\#k\mathbb{Z}/(3) \cong R_4(q^{-1},2)\#k\mathbb{Z}/(3)$. This proves (i). In case (ii) it follows from Proposition 6.3 that an isomorphism is only possible if $q = \widetilde{q}$. □

§7. Pointed Hopf algebras of order p^4.

Let p be an odd prime number. We now characterize coradically graded pointed Hopf algebras of order p^4.

Theorem 7.1. *Let G be a coradically graded pointed Hopf algebras of order p^4 with coradical $\Bbbk\Gamma$. Then $G \simeq R\#\Bbbk\Gamma$, where*

(7.2) *R is a quantum line if Γ has order p^3;*

(7.3) *R is a quantum line or plane if Γ has order p^2;*

(7.4) *$R = \mathfrak{B}(V)$, where V has Dynkin diagram A_2 if Γ has order p, where $p = 3$ or $p - 1$ is divisible by 3.*

Proof. The case (7.2) follows from Proposition 7.5 below; we can not apply directly [AS2] since there are non-abelian groups of order p^3. The case (7.3) follows directly from [AS2, Lemma 5.6]. If Γ has order p, then we see from Theorem 1.3 that only the case (ii), that is (7.4), is possible. □

Proposition 7.5. *Let Γ be a finite (non-necessarily abelian) group. Let R be a braided Hopf algebra in ${}^{\Gamma}_{\Gamma}\mathcal{YD}$ of prime order p, where p is the smallest prime dividing the order of Γ. Assume that $R_0 = \Bbbk 1$. Then R is a quantum line.*

Proof. As $P(R)$ is a Yetter-Drinfeld submodule of R and it is non-zero by hypothesis, there exists $1 \neq g \in \Gamma$ such that $P(R)_g \neq 0$. But the Yetter-Drinfeld condition shows that $P(R)_g$ is stable under the action of g. Hence, there exists $y \in P(R)$, $y \neq 0$, such that

$$g.y = qy, \quad \delta(y) = g \otimes y.$$

Let N be the order of q. By [AS2, Lemma 3.1] N is not 1. Now N divides the order of Γ, hence $N \geq p$. Since the dimension of $k[y]$ is N by the quantum binomial formula (cf. [AS2, Lemma 3.3]), we conclude that $N = p$. □

Remark. Proposition 7.5 allows the classification of finite dimensional pointed Hopf algebras of dimension p^n whose coradical has index p. This last result was independiently given in [D] by a different method.

§8. A bound on the dimension.

Let Γ be again our fixed finite abelian group of odd order. Theorem 1.1 gives a method to obtain finite dimensional Nichols algebras over Γ: pick a finite Cartan matrix (a_{ij}) and a Yetter-Drinfeld module V over Γ of Cartan type with associated matrix (a_{ij}); then $\mathfrak{B}(V)$ is finite dimensional and we know in fact its dimension. We want now to describe explicitly a way to construct Yetter-Drinfeld modules over Γ of Cartan type with associated matrix (a_{ij}).

We fix elements $y_1, \dots, y_M$ of Γ such that $\operatorname{ord} y_\ell = E_\ell$, $\Gamma = \langle y(1)\rangle \oplus \dots \oplus \langle y(M)\rangle$, E_ℓ divides $E_{\ell+1}$ and set $E = E_M$. Then $\Gamma = \oplus_{1\le \ell\le M} \mathbb{Z}/(E)y(\ell)$ is a direct sum of cyclic $\mathbb{Z}/(E)$-modules $\mathbb{Z}/(E)y(\ell)$ of order E_ℓ. Let q be a primitive E-th root of 1 in $\Bbbk$.

A Yetter-Drinfeld module V over Γ of Cartan type $(a_{ij})_{1\le i,j\le\theta}$ is given (up to permutation) by sequences $g(1), \dots, g(\theta) \in \Gamma$, $\chi(1), \dots, \chi(\theta) \in \widehat{\Gamma}$ such that the elements $b_{ji} = \langle \chi(i), g(j)\rangle$ which we write as $b_{ji} = q^{z_{ij}}$, $z_{ij} \in \mathbb{Z}/(E)$, satisfy

(8.1) $z_{ij} + z_{ji} = z_{ii}a_{ij}$, for all i, j;
(8.2) $z_{ii} \ne 0$, for all i.

Clearly, (8.1) is equivalent to $z_{ij} + z_{ji} = z_{ii}a_{ij}$ and $z_{ij} = z_{ji}$, for all $i < j$.

Suppose we have solved the system of linear equations (8.1) over $\mathbb{Z}/(E)$ such that (8.2) holds. To realize (b_{ij}) over Γ we have to find elements $x_{i\ell}$, $w_{\ell j} \in \mathbb{Z}/(E)$, $1 \le i, j \le \theta$, $1 \le \ell \le M$, with $E_\ell x_{i\ell} = 0$, such that $b_{ji} = \langle \chi(i), g(j)\rangle$ for all i, j, where

$$\langle \chi(i), y(\ell)\rangle = q^{x_{i\ell}}$$
$$g(j) = \sum_{1\le \ell\le M} w_{\ell j} y(\ell),$$

$1 \le i, j \le \theta$, $1 \le \ell \le M$. We have then to solve the following system of quadratic equations over $\mathbb{Z}/(E)$ in the $2\theta M$ unknowns $x_{i\ell}$, $w_{\ell j}$:

$$\sum_{1\le \ell\le M} x_{i\ell} w_{\ell j} = z_{ij}, \qquad \text{for all } i, j. \tag{8.3}$$

The analysis of this system, and in particular the existence of solutions, involves arithmetic tools, namely the quadratic reciprocity law.

Let F be the free $\mathbb{Z}/(E)$-module with basis $e(1), \dots, e(\theta)$. Define $\mathbb{Z}/(E)$-linear maps $x : \Gamma \to F$, $w : F \to \Gamma$ and $z : \Gamma \to \Gamma$ by $x(y(\ell)) = \sum_{1\le i\le\theta} x_{i\ell} e(i)$, $w(e(j)) = \sum_{1\le \ell\le M} w_{\ell j} y(\ell)$ and $z(e(j)) = \sum_{1\le i\le\theta} z_{ij} e(i)$ for all ℓ, j. Then (8.3) is equivalent to

$$xy = z. \tag{8.4}$$

Thus we see that giving $g(1), \dots, g(\theta) \in \Gamma$, $\chi(1), \dots, \chi(\theta) \in \widehat{\Gamma}$ with $b_{ji} = \langle \chi(i), g(j)\rangle$ for all i, j is equivalent to factorizing z over Γ. Such a factorization exists if and only if the row space of (z_{ij}) is an epimorphic image of a subgroup of Γ, or equivalently of Γ (since by duality, any subgroup of Γ is an epimorphic image of Γ). In particular, if $(\mathbb{Z}/(E))^\theta$ itself is an an epimorphic image of Γ, then for any solution (z_{ij}) of (8.1), (8.2) there is a Yetter-Drinfeld module over Γ with braiding $b_{ji} = q^{z_{ij}}$ of Cartan type $(a_{ij})_{1\le i,j\le\theta}$.

Proposition 8.1. *If Γ is a finite abelian group of odd order and V is a Yetter-Drinfeld module over Γ of finite Cartan type, then*

$$\dim V \leq 2(\operatorname{ord}\Gamma)^2. \tag{8.5}$$

Proof. We describe V as above. By (8.4), the image of z is contained in the image of x; hence $\operatorname{ord}(\operatorname{Im} z) \leq \operatorname{ord}\Gamma$. We now apply the duality functor $M \mapsto M^* := \operatorname{Hom}_{\mathbb{Z}/(E)}(M, \mathbb{Z}/(E))$ to (8.4) and conclude that also $\operatorname{ord}(\operatorname{Im} z^*) \leq \operatorname{ord}\Gamma$ since $\Gamma^* \simeq \Gamma$. Thus we obtain from (8.1) that the row space of $(z_{ij}) +^t (z_{ij}) = (z_{ii}a_{ij})$ has at most $\operatorname{ord}(\operatorname{Im} z)\operatorname{ord}(\operatorname{Im} z^*) \leq (\operatorname{ord}\Gamma)^2$ elements.

We compute now a lower bound for the number of elements in the row space of $(z_{ii}a_{ij})$ over $\mathbb{Z}/(E)$. We can assume that (a_{ij}) is a diagonal of blocks corresponding to matrices of connected finite Cartan type. It is easy to check the following (rather weak) claim about the row space of a connected finite Cartan matrix C modulo $\mathbb{Z}/(E)$, not of type A_2: Let α, β be non-zero elements in $\mathbb{Z}/(E)$ and a, b two different rows in C. Then $\alpha a \neq 0$, $\beta b \neq 0$ and $\alpha a \neq \beta b$.

(If C is of type A_2, $a = (2, -1)$ and $b = (-1, 2)$ then $\alpha a = \beta b$ whenever $\alpha = \beta$ and $3\alpha = 0$).

Let s be the number of connected components of (a_{ij}) of type A_2. Then $\theta = 2s+t$ for some $t \geq 0$ and the row space of $(z_{ii}a_{ij})$ has at least $s + t$ elements. Therefore

$$\theta = 2s + t \leq 2(s + t) \leq 2(\operatorname{ord}\Gamma)^2. \qquad \square$$

Corollary 8.2. *Let Γ be a fixed finite abelian group of odd order. Then there are (up to isomorphisms) only finitely many Yetter-Drinfeld modules over Γ of finite Cartan type.*

Proof. This follows from Proposition 8.1 since there are only finitely many Yetter-Drinfeld modules over Γ of a given dimension (up to isomorphisms). $\square$

It is easy to improve the bound in (8.5) under additional assumptions. If the Cartan matrix of V is invertible over $\mathbb{Z}/(E)$, then

$$f_1 \dots f_\theta \leq (\operatorname{ord}\Gamma)^2,$$

where $1 \neq f_i := \operatorname{ord}(\mathbb{Z}/(E)z_{ii})$ is a divisor of E. This follows from the proof of Proposition 8.1. Let f the least divisor of E greater than one; then $f^\theta \leq (\operatorname{ord}\Gamma)^2$, so

$$\theta \leq 2\log_f(\operatorname{ord}\Gamma).$$

In particular we get a better bound for quantum linear spaces (all connected components are of type A_1). On the other hand, if Γ is a product of r cyclic groups (not in the canonical form above, so r could be much greater than M) then there exists at least a quantum linear space over Γ of dimension $2r$, see [AS2, Lemma 4.1].

Finally, we consider the special case when $\Gamma \simeq (\mathbb{Z}/(p))^r$, p an odd prime. We have shown that there is always a Yetter-Drinfeld module over Γ of any given finite Cartan type of rank θ if $\theta \leq r$. In general we have the following bound.

Proposition 8.3. *Let $p > 3$ be a prime, $r \geq 1$ a natural number, $\Gamma \simeq (\mathbb{Z}/(p))^r$ and V a Yetter-Drinfeld module over Γ of finite Cartan type. Then*

$$\dim V \leq 2r\frac{p-1}{p-2}. \tag{8.6}$$

Proof. We work as in the proof of Proposition 9.1, but with $E = p$ and over the field $\mathbb{Z}/(p)$. From (8.1) and (8.4) we obtain an upper bound for the rank over $\mathbb{Z}/(p)$:

$$\operatorname{rk}(z_{ii}a_{ij}) \leq 2\operatorname{rk}(z_{ij}) \leq 2r.$$

If (a_{ij}) is invertible mod p we conclude that

$$\theta \leq 2r.$$

The determinants of the connected Cartan matrices of finite type are $\ell + 1$ for A_ℓ and $1, 2, 3$ or 4 for the other types. Let C_i, $1 \leq i \leq s$, be the connected components of (a_{ij}) of type A_{ℓ_i} such that $p|(\ell_i + 1)$; hence $\ell_i \geq p - 1$. Write $\theta = \sum_{1 \leq i \leq s} \ell_i + r$ for some $r \leq 0$. Then $\theta \geq s(p-1)$ and

$$\theta - s \geq \theta - \frac{\theta}{p-1} = \frac{p-2}{p-1}\theta. \tag{8.7}$$

We now replace in (a_{ij}) each diagonal block C_i by the smaller block of type $A_{\ell_i - 1}$. The new Cartan matrix is invertible mod p of rank $\theta - s$ since p does not divide $\ell_i + 1$. Hence we know

$$\theta - s \leq 2r. \tag{8.8}$$

Now (8.6) follows from (8.7) and (8.8). $\square$

Note that Proposition 8.3 gives an alternative proof of Proposition 5.1 for $p > 3$.

Appendix. Primitive elements from quantum Serre relations.

Gaussian binomial coefficients.

In the polynomial algebra $\mathbb{Z}[\mathbf{q}]$, we consider the Gaussian, or $\mathbf{q}$-binomial, coefficients

$$\binom{n}{i}_{\mathbf{q}} = \frac{(n)!_{\mathbf{q}}}{(n-i)!_{\mathbf{q}}(i)!_{\mathbf{q}}},$$

where $(n)!_{\mathbf{q}} = (n)_{\mathbf{q}} \dots (2)_{\mathbf{q}}(1)_{\mathbf{q}}$, and $(n)_{\mathbf{q}} = 1 + \mathbf{q} + \dots + \mathbf{q}^{n-1}$, for $n \in \mathbb{N}$, $0 \leq i \leq n$. We have the identity

$$\mathbf{q}^h\binom{n}{h}_{\mathbf{q}} + \binom{n}{h-1}_{\mathbf{q}} = \binom{n}{h}_{\mathbf{q}} + \mathbf{q}^{n+1-h}\binom{n}{h-1}_{\mathbf{q}} = \binom{n+1}{h}_{\mathbf{q}}, 1 \leq h \leq n; \tag{A.1}$$

This implies that $\binom{n}{i}_{\mathbf{q}} \in \mathbb{Z}[\mathbf{q}]$. If A is an associative algebra over k and $q \in k$, then $\binom{n}{i}_q$ denotes the specialization of $\binom{n}{i}_{\mathbf{q}}$ in q. If $x, y \in A$ are two elements that

q-commute, i.e. $xy = qyx$, then the quantum binomial formula holds for every $n \in \mathbb{N}$:

$$(x+y)^n = \sum_{i=0}^{n} \binom{n}{i}_q y^i x^{n-i}. \tag{A.2}$$

Let us also record

$$(r)_{\mathbf{q}} + \mathbf{q}^r (s)_{\mathbf{q}} = (r+s)_{\mathbf{q}}. \tag{A.3}$$

There is another version of "$\mathbf{q}$-binomial coefficients": in the Laurent polynomial algebra $\mathbb{Z}[\mathbf{q}, \mathbf{q}^{-1}]$, we consider

$$\begin{bmatrix} n \\ i \end{bmatrix}_{\mathbf{q}} = \frac{[n]!_{\mathbf{q}}}{[n-i]!_{\mathbf{q}}[i]!_{\mathbf{q}}}, \quad \text{where } [n]!_{\mathbf{q}} = [n]_{\mathbf{q}} \dots [2]_{\mathbf{q}}[1]_{\mathbf{q}}, \quad \text{and } [n]_{\mathbf{q}} = \frac{\mathbf{q}^n - \mathbf{q}^{-n}}{\mathbf{q} - \mathbf{q}^{-1}}.$$

Clearly,

$$(n)_{\mathbf{q}^2} = \mathbf{q}^{n-1}[n]_{\mathbf{q}},$$

and hence

$$\binom{n}{i}_{\mathbf{q}^2} = \mathbf{q}^{i(n-i)} \begin{bmatrix} n \\ i \end{bmatrix}_{\mathbf{q}}.$$

In particular, for $n \geq 1$, the following equality- see [L3, 1.3.4 (a)]-

$$\sum_{i=0}^{n} (-1)^i \mathbf{q}^{i(1-n)} \begin{bmatrix} n \\ i \end{bmatrix}_{\mathbf{q}} = 0 \tag{A.4}$$

translates into

$$\sum_{i=0}^{n} (-1)^i \mathbf{q}^{(i^2+i)/2-ni} \binom{n}{i}_{\mathbf{q}} = 0. \tag{A.5}$$

This last equality is also equivalent, by a change of the summation index, to

$$\sum_{h=0}^{n} (-1)^h \mathbf{q}^{(h^2-h)/2} \binom{n}{h}_{\mathbf{q}} = 0. \tag{A.6}$$

Primitive elements.

Let S be a braided Hopf algebra over our an abelian group Γ. Let $x, y \in P(S)$ such that

$$\delta(x) = g \otimes x, \quad h.x = \chi(h)x \quad , \delta(y) = t \otimes y, \quad h.y = \eta(h)y \quad \forall h \in \Gamma,$$

for some $g, t \in \Gamma$, $\chi, \eta \in \widehat{\Gamma}$. We assume that the orders of $\chi(g)$, $\eta(t)$ are positive.

Definition. The *braided adjoint representation* is the linear map $\mathrm{ad}_c : S \to \operatorname{End} S$ given by

$$\mathrm{ad}_c(u)(v) = \mu(u \otimes v - c(u \otimes v));$$

here μ is the multiplication map of S and c is the commutativity constraint.

The following property holds:

$$\mathrm{ad}_c(u)(vw) = \mathrm{ad}_c(u)(v)w + (u_{(-1)}.v)\,\mathrm{ad}_c(u_{(0)})(w). \tag{A.7}$$

In our situation, we define inductively $z_1 = \mathrm{ad}_c(x)(y) = xy - \eta(g)yx$; $z_{j+1} = \mathrm{ad}_c(x)(z_j)$. For instance,

$$\begin{aligned} z_2 &= x^2y - \eta(g)\,(1+\chi(g))\,xyx + \eta(g)^2\chi(g)yx^2, \\ z_3 &= x^3y - \eta(g)(3)_{\chi(g)}x^2yx + \eta(g)^2\chi(g)(3)_{\chi(g)}xyx^2 - \eta(g)^3\chi(g)^3yx^3 \end{aligned}$$

and in general

$$z_N = \sum_{i=0}^{N}(-1)^i\binom{N}{i}_{\chi(g)}\chi(g)^{i(i-1)/2}\eta(g)^i\,x^{N-i}yx^i. \tag{A.8}$$

The proof of (A.8) is by induction using (A.7).

The following Lemma is probably well-known. For completeness, we give a direct proof.

Lemma A.1. *Let $r \geq 1$ be a natural number. Assume that*

$$\eta(g)\chi(t)\chi(g)^{r-1} = 1 \tag{A.9}$$

and $r - 1 < \operatorname{ord}(\chi(g))$. Then $(\mathrm{ad}_c\, x)^r y$ is primitive.

Proof. Let $z = \sum_{i=0}^{r}\alpha_i x^i y x^{r-i}$, where $\alpha_i \in k$. Then by the quantum binomial formula,

$$\begin{aligned} \Delta(z) &= \sum_{i=0}^{r}\sum_{\ell=0}^{i}\sum_{h=0}^{r-i}\alpha_i\binom{i}{\ell}_{\chi(g)}\binom{r-i}{h}_{\chi(g)}\Big[\eta(g)^{i-\ell}\chi(g)^{h(i-\ell)}x^\ell y x^h \otimes x^{r-\ell-h} \\ &\quad + \chi(t)^h\chi(g)^{h(i-\ell)}x^{\ell+h} \otimes x^{i-\ell}yx^{r-i-h}\Big] \\ &= z\otimes 1 + 1 \otimes z \\ &\quad + \sum_{\substack{\ell\geq 0, h\geq 0\\ \ell+h<r}}\left(\sum_{\ell\leq i\leq r-h}\alpha_i\binom{i}{\ell}_{\chi(g)}\binom{r-i}{h}_{\chi(g)}\eta(g)^{i-\ell}\chi(g)^{h(i-\ell)}\right)x^\ell yx^h\otimes x^{r-\ell-h} \\ &\quad + \sum_{\substack{u\geq 0, v\geq 0\\ u+v<r}}\left(\sum_{u\leq i\leq r-v}\alpha_i\binom{i}{u}_{\chi(g)}\binom{r-i}{v}_{\chi(g)}\chi(t)^{r-i-v}\chi(g)^{u(r-i-v)}\right)x^{r-u-v}\otimes x^u yx^v. \end{aligned}$$

∎

Hence, if $\alpha_0, \dots, \alpha_r$ is a solution of the system of equations

(A.10a)
$$\sum_{\ell \le i \le r-h} \alpha_i \binom{i}{\ell}_{\chi(g)} \binom{r-i}{h}_{\chi(g)} \eta(g)^{i-\ell} \chi(g)^{h(i-\ell)} = 0,$$

(A.10b)
$$\sum_{u \le i \le r-v} \alpha_i \binom{i}{u}_{\chi(g)} \binom{r-i}{v}_{\chi(g)} \chi(t)^{r-i-v} \chi(g)^{u(r-i-v)} = 0,$$

where $l \ge 0, h \ge 0, l+h < r$ and $u \ge 0, v \ge 0, u+v < r$, then z is primitive.

Now assume that $z = (\operatorname{ad}_c x)^r y$, that is

$$z = \sum_{0 \le i \le r} (-1)^{r-i} \binom{r}{i}_{\chi(g)} \chi(g)^{(r-i)(r-i-1)/2} \eta(g)^{r-i} x^i y x^{r-i}.$$

To see that z is primitive, we divide z by $(-1)^r \chi(g)^{(r^2-r)/2} \eta(g)^r$ and reduce to check that

$$\alpha_i := (-1)^i \binom{r}{i}_{\chi(g)} \chi(g)^{(i^2+i)/2 - ri} \eta(g)^{-i}$$

satisfies the system of equations (A.10). We proceed with (A.10a). If $l = 0$ and $h = 0$, then (A.10a) follows from (A.5). If $\ell \ge 0$, $h \ge 0$ and $1 \le \ell + h < r$, then

$$\begin{aligned} &\sum_{\ell \le i \le r-h} (-1)^i \binom{r}{i}_{\chi(g)} \binom{i}{\ell}_{\chi(g)} \binom{r-i}{h}_{\chi(g)} \eta(g)^{i-\ell-i} \chi(g)^{(i^2+i)/2 - ri + h(i-\ell)} \\ &\quad = \frac{(r)! \eta(g)^{-\ell} \chi(g)^{-h\ell}}{(\ell)!(h)!(r-\ell-h)!} \sum_{\ell \le i \le r-h} (-1)^i \frac{(r-\ell-h)!}{(i-\ell)!(r-i-h)!} \chi(g)^{(i^2+i)/2 + i(h-r)}. \end{aligned}$$

Here the denominators are q-factorials with $q = \chi(g)$, and they are non-zero since $1 \le \ell + h < r$ and $r - 1 < \operatorname{ord}(q)$. Dividing by the appropiate factor and changing the summation index, we get

$$(-1)^\ell \chi(g)^{(\ell^2+\ell)/2} \sum_{0 \le i \le r-h-\ell} \binom{r-h-\ell}{i}_{\chi(g)} \chi(g)^{(i^2+i)/2 + i(h+\ell-r)} = 0,$$

by (A.5).

Now we pass to (A.10b). If $u = 0$ and $v = 0$, then (A.10b) follows from (A.6) and (A.9). For $u \ge 0$, $v \ge 0$, and $1 \le u + v < r$, we compute:

$$\begin{aligned} &\sum_{u \le i \le r-v} (-1)^i \binom{r}{i}_{\chi(g)} \binom{i}{u}_{\chi(g)} \binom{r-i}{v}_{\chi(g)} \eta(g)^{-i} \chi(t)^{r-i-v} \chi(g)^{(i^2+i)/2 - ri + u(r-i-v)} \\ &= \frac{(r)! \chi(t)^{r-v} \chi(g)^{u(r-v)}}{(u)!(v)!(r-u-v)!} \sum_{u \le i \le r-v} (-1)^i \frac{(r-u-v)!}{(i-u)!(r-i-v)!} \chi(g)^{(i^2+i)/2 - ri - ui + i(r-1)}, \end{aligned}$$

where we have used (A.9). The denominators are non-zero by the same reason as before. After dividing by the appropiate factor and changing the summation index we obtain

$$(-1)^u \chi(g)^{(u^2+u)/2} \sum_{0\le i\le r-v-u} (-1)^i \binom{r-u-v}{i}_{\chi(g)} \chi(g)^{(i^2-i)/2} = 0,$$

by (A.6). □

References

[AJS] H. H. Andersen, J. Jantzen and W. Soergel, *Representations of quantum groups at a p-th root of unity and of semisimple groups in characteristic p: Independence of p*, Astérisque **220** (1994).

[AG] N. Andruskiewitsch and M. Graña, *Braided Hopf algebras over non-abelian finite groups*, Bol. Acad. Nac. Ciencias Córdoba, Argentina **63** (1999), 45–78.

[AS1] N. Andruskiewitsch and H.-J. Schneider, *Hopf Algebras of order p^2 and braided Hopf algebras of order p*, J. Algebra **199** (1998), 430–454.

[AS2] ———, *Lifting of Quantum Linear Spaces and Pointed Hopf Algebras of order p^3*, J. Algebra **209** (1998), 659–691.

[AS3] ———, *Finite Quantum Groups over Abelian Groups of Prime Exponent*, preprint.

[BD] Y. Bespalov and B. Drabant, *Hopf (bi-)modules and crossed modules in monoidal categories*, J. Pure Appl. Algebra **123** (1998), 105–129.

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

[BT] F. R. Beyl and J. Tappe, *Group extensions, representations, and the Schur multiplicator*, Lecture Notes in Maths. 958, Springer-Verlag, 1982.

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

[CDR] S. Caenepeel, S. Dascalescu and S. Raianu, *Classifying Pointed Hopf algebras of dimension* 16, Comm. Algebra (to appear).

[CM] W. Chin and I. Musson, *The coradical filtration for quantized universal enveloping algebras*, J. London Math. Soc. **53** no. 2 (1996), 50–67.

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

[D] S. Dascalescu, *Pointed Hopf algebras of dimension p^n with large coradical*, Comm. Algebra **27** (1999), 4821–4826.

[dCP] C. de Concini and C. Procesi, *Quantum Groups*, D-modules, Representation theory and Quantum Groups, Lecture Notes in Maths. 1565, Springer-Verlag, 1993, pp. 31–140.

[Dr1] V. G. Drinfeld, *On constant, quasi-classical solutions of the Quantum Yang-Baxter equation*, Soviet Math. Dokl. **28** (1983), 667–671.

[Dr2] ———, *Quasi-Hopf algebras*, Leningrad Math. J. **1** no. 6 (1990), 1419–1457.

[Dr3] ———, *On quasitriangular quasi-Hopf algebras and a group closely related to* $Gal(\bar{\mathbf{Q}}, \mathbf{Q})$, Leningrad Math. J. **2** (1991), 829–860.

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

[Gr1] M. Graña, *Pointed Hopf algebras of dimension* 32, Comm. Algebra (to appear).

[Gr2] M. Graña, *On Nichols algebras of low dimension*, Contemp. Math. (to appear).

[K] V. Kac, *Infinite dimensional Lie algebras*, Third edition, Cambridge Univ. Press, 1995.

[L1] G. Lusztig, *Finite dimensional Hopf algebras arising from quantized universal enveloping algebras*, J. of Amer. Math. Soc. **3** no. 1 pages 257–296.

[L2] ———, *Quantum groups at roots of 1*, Geom. Dedicata **35** (1990), 89–114.

[L3] ———, *Introduction to quantum groups*, Birkhäuser, 1993.

[L4] ———, *Introduction to quantized enveloping algebras*, New developments in Lie Theory and their applications (Tirao and Wallach, eds.), Prog. in Maths. 105, Birkhäuser, 1991, pp. 49–67.

[Mj1] S. Majid, *Crossed products by braided groups and bosonization*, J. Algebra **163** (1994), 165–190.

[Mj2] ———, *Quasi $*$-structures on q-Poincaré algebras*, Preprint **DAMTP** (1995), 1–56.

[Mj3] ———, *Foundations of quantum group theory*, Cambridge University Press, 1995.

[Mo1] S. Montgomery, *Hopf algebras and their actions on rings* CBMS Vol. 82 , AMS, 1993.

[Mo2] ———, *Classifying semisimple Hopf algebras*, Contemporary Mathematics **229** (1998), 265–279.

[Mv] M. Movshev, *Twisting in group algebras of finite groups*, Funct. Anal. Appl. **27** (1994), 240–244.

[Mü] E. Müller, *Some topics on Frobenius-Lusztig kernels, I*, J. Algebra **206** (1998), 624–658.

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

[Nk] D. Nikshych, *K_0-rings and twisting of finite dimensional semisimple Hopf algebras*, Commun. Alg. **26** (1998), 321–342; *Corrigendum*, Commun. Alg. **26** (1998), 2019.

[Ra] D. Radford, *Hopf algebras with projection*, J. Algebra **92** (1985), 322–347.

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

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

[Ro2] ———, *Groupes quantiques et algebres de battage quantiques*, C. R. A. S. (Paris) **320** (1995), 145–148.

[Ro3] ———, *Quantum groups and quantum shuffles*, Inventiones Math. **133** (1998), 399–416.

[Rz] J. Rozanski, *Braided antisymmetrizer as bialgebras homomorphism*, Rep. Math. Phys. **38** (1996), 273–277.

[Sbg] P. Schauenburg, *A Characterization of the Borel-like subalgebras of Quantum Enveloping algebras*, Commun. Alg. **24** (1996), 2811–2823.

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

[Sw] Sweedler, M., *Hopf algebras*, Benjamin, New York, 1969.

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

N. Andruskiewitsch: FAMAF. UNC. (5000) C. Universitaria. Córdoba. Argentina

E-mail: andrus@mate.uncor.edu

H.-J. Schneider: Mathematisches Institut der Universität München. Theressienstr. 39. (80333) München. Germany

E-mail: hanssch@rz.mathematik.uni-muenchen.de