FINITE-DIMENSIONAL NICHOLS ALGEBRAS OF SIMPLE YETTER–DRINFELD MODULES (OVER GROUPS) OF PRIME DIMENSION

I. HECKENBERGER, E. MEIR, AND L. VENDRAMIN

ABSTRACT. Over fields of characteristic zero, we determine all absolutely irreducible Yetter–Drinfeld modules over groups that have prime dimension and yield a finite-dimensional Nichols algebra. To achieve our goal, we introduce orders of braided vector spaces and study their degenerations and specializations.

1. INTRODUCTION

Pointed Hopf algebras form a central class of objects in the theory of Hopf algebras since the beginning [49]. Besides the coradical of a pointed Hopf algebra, which is the group ring of a group, the skew-primitive elements and the infinitesimal braiding belong to the most important invariants [16]. The infinitesimal braiding V is a braided vector space that yields another invariant: a connected strictly graded braided Hopf algebra known as the *Nichols algebra* of V. Very prominent examples are the positive part of quantum groups, but the structure theory is also deeply understood for abelian groups and corresponding braided vector spaces of diagonal type. For a general account, we refer to [1] and [33].

Nichols algebras also appear in the highly influential papers of Nichols [46], Woronowicz [51, 52] and Majid [43], Schaubenburg [48], Rosso [47], Kharchenko [40], and Andruskiewitsch and Schneider [17]. Recent interest and applications of Nichols algebras appear in algebraic geometry in the work of Kapranov and Schechtman [38], and in quantum field theory in the paper of Lentner [42]. In number theory, Ellenberg, Tran and Westerland [24] used Nichols algebras to prove an upper bound in the weak Malle conjecture on the distribution of finite extensions of $\mathbb{F}_q(t)$ with specified Galois groups.

The classification of finite-dimensional Nichols algebras of Yetter–Drinfeld modules was achieved in [30] for abelian groups and fields of characteristic zero, and in [34, 35] for non-abelian groups and semi-simple non-simple Yetter–Drinfeld modules over arbitrary fields. The key structure in these classifications is the Weyl groupoid [15, 29]. For most of the Nichols algebras in the classification, a construction from Nichols algebras of diagonal type by folding was described by Lentner [41]. However, the classification problem is wide open for irreducible Yetter–Drinfeld modules, despite of tremendous efforts taken by different authors using different tools [5, 6, 7, 8, 9, 11, 12, 18, 19, 20, 22, 31, 32, 36]. Over non-abelian groups,

2020 *Mathematics Subject Classification.* 16T05, 18M15.
Key words and phrases. Nichols algebra, Affine rack, Alexander rack, braiding.

not even a satisfactory unified explanation of the Hilbert series of the known finite-dimensional examples is available. At the moment, only a few finite-dimensional Nichols algebras are known.

For any group G, let ${}^{\Bbbk G}_{\Bbbk G}\mathcal{YD}$ denote the category of Yetter–Drinfeld modules over the group ring $\Bbbk G$ of G.

Example 1.1. Let G be a non-abelian epimorphic image of the group

$$\langle x_1, x_2, x_3 : x_1x_2 = x_3x_1,\, x_1x_3 = x_2x_1,\, x_2x_3 = x_1x_2\rangle.$$

For all $i \in \{1, 2, 3\}$, let $g_i \in G$ be the image of x_i. Then $g_i \neq g_j$ for all $i \neq j$. Let $\langle g_1\rangle$ be the subgroup of G generated by g_1, and let U be a one-dimensional Yetter–Drinfeld module over $\langle g_1\rangle$ with $\Bbbk\langle g_1\rangle$-coaction $\delta(u) = g_1 \otimes u$ for all $u \in U$ and $\Bbbk\langle g_1\rangle$-action $g_1u = -u$ for all $u \in U$. Then $V = \Bbbk G \otimes_{\Bbbk\langle g_1\rangle} U$ is a Yetter–Drinfeld module over $\Bbbk G$. Let $v_1 = 1 \otimes u$ for some $u \in U$ with $u \neq 0$. Then

$$v_1,\, v_2 = -g_3v_1,\, v_3 = -g_2v_1$$

form a basis of V. The G-degrees of these vectors are g_1, g_2 and g_3, respectively. The action of G on V is given by

$$g_iv_j = -v_{2i-j \bmod 3}, \qquad i, j \in \{1, 2, 3\}.$$

The support of V is the affine rack $\mathrm{Aff}(3, 2)$, see Section 2. Then $\dim \mathcal{B}(V) = 12$. This example appeared first in [45]; see also [27].

The following two examples appeared first in [14].

Example 1.2. Let G be a non-abelian epimorphic image of the group

$$\langle x_1, x_2, x_3, x_4, x_5 : x_ix_jx_i^{-1} = x_{-i+2j \bmod 5}\rangle.$$

For all $i \in \{1, 2, 3, 4, 5\}$, let $g_i \in G$ be the image of x_i. Then $g_i \neq g_j$ for all $i \neq j$. Let $\langle g_1\rangle$ be the subgroup of G generated by g_1, and let U be a one-dimensional Yetter–Drinfeld module over $\langle g_1\rangle$ with $\Bbbk\langle g_1\rangle$-coaction $\delta(u) = g_1 \otimes u$ for all $u \in U$ and $\Bbbk\langle g_1\rangle$-action $g_1u = -u$ for all $u \in U$. Then $V = \Bbbk G \otimes_{\Bbbk\langle g_1\rangle} U$ is a Yetter–Drinfeld module over $\Bbbk G$. Let $v_1 = 1 \otimes u$ for some $u \in U$ with $u \neq 0$. Then the vectors

$$v_1,\, v_2 = -g_5v_1,\, v_3 = -g_4v_1,\, v_4 = -g_3v_1,\, v_5 = -g_2v_1$$

form a basis of V. For each $i \in \{1, 2, 3, 4, 5\}$, $\deg v_i = g_i$. The action of G on V is given by

$$g_iv_j = -v_{-i+2j \bmod 5}, \qquad i, j \in \{1, 2, 3, 4, 5\}.$$

The support of V is the affine rack $\mathrm{Aff}(5, 2)$. Then $\dim \mathcal{B}(V) = 1280$.

Example 1.3. Let G be a non-abelian epimorphic image of the group

$$\langle x_1, x_2, x_3, x_4, x_5 : x_ix_jx_i^{-1} = x_{3(i+j) \bmod 5}\rangle.$$

For all $i \in \{1, 2, 3, 4, 5\}$, let $g_i \in G$ be the image of x_i. Then $g_i \neq g_j$ for all $i \neq j$. Let $\langle g_1\rangle$ be the subgroup of G generated by g_1, and let U be a one-dimensional Yetter–Drinfeld module over $\langle g_1\rangle$ with $\Bbbk\langle g_1\rangle$-coaction $\delta(u) = g_1 \otimes u$ for all $u \in U$ and $\Bbbk\langle g_1\rangle$-action $g_1u = -u$ for all $u \in U$. Then $V = \Bbbk G \otimes_{\Bbbk\langle g_1\rangle} U$ is a Yetter–Drinfeld module over $\Bbbk G$. Let $v_1 = 1 \otimes u$ for some $u \in U$ with $u \neq 0$. Then the vectors

$$v_1,\, v_2 = -x_3v_1,\, v_3 = -x_5v_1,\, v_4 = -x_2v_1,\, v_5 = -x_4v_1$$

form a basis of V. For each $i \in \{1,2,3,4,5\}$, $\deg v_i = g_i$. The action of G on V is given by

$$x_i v_j = -v_{3(i+j) \bmod 5}, \qquad i,j \in \{1,2,3,4,5\}.$$

The support of V is the affine rack $\mathrm{Aff}(5,3)$. Then $\dim \mathcal{B}(V) = 1280$.

Graña found the following two examples.

Example 1.4. Let G be a non-abelian epimorphic image of the group

$$\langle x_1, x_2, \dots, x_7 : x_i x_j x_i^{-1} = x_{5i+3j \bmod 7} \rangle.$$

For all $i \in \{1,2,\dots,7\}$, let $g_i \in G$ be the image of x_i. Then $g_i \neq g_j$ for all $i \neq j$. Let $\langle g_1 \rangle$ be the subgroup of G generated by g_1, and let U be a one-dimensional Yetter–Drinfeld module over $\langle g_1 \rangle$ with $\Bbbk\langle g_1 \rangle$-coaction $\delta(u) = g_1 \otimes u$ for all $u \in U$ and $\Bbbk\langle g_1 \rangle$-action $g_1 u = -u$ for all $u \in U$. Then $V = \Bbbk G \otimes_{\Bbbk\langle g_1 \rangle} U$ is a Yetter–Drinfeld module over $\Bbbk G$. Let $v_1 = 1 \otimes u$ for some $u \in U$ with $u \neq 0$. Then the vectors

$$v_1,\ v_2 = -g_4 v_1,\ v_3 = -g_7 v_1,\ v_4 = -g_3 v_1,\ v_5 = -g_6 v_1,\ v_6 = -g_2 v_1,\ v_7 = -g_5 v_1,$$

form a basis of V. For each $i \in \{1,2,\dots,7\}$, $\deg v_i = g_i$. The action of G on V is given by

$$x_i v_j = -v_{5i+3j \bmod 7}, \qquad i,j \in \{1,2,\dots,7\}.$$

The support of V is the affine rack $\mathrm{Aff}(7,3)$. Then $\dim \mathcal{B}(V) = 326592$.

Example 1.5. Let G be a non-abelian epimorphic image of the group

$$\langle x_1, x_2, \dots, x_7 : x_i x_j x_i^{-1} = x_{3i+5j \bmod 7} \rangle.$$

For all $i \in \{1,2,\dots,7\}$, let $g_i \in G$ be the image of x_i. Then $g_i \neq g_j$ for all $i \neq j$. Let $\langle g_1 \rangle$ be the subgroup of G generated by g_1, and let U be a one-dimensional Yetter–Drinfeld module over $\langle g_1 \rangle$ with $\Bbbk\langle g_1 \rangle$-coaction $\delta(u) = g_1 \otimes u$ for all $u \in U$ and $\Bbbk\langle g_1 \rangle$-action $g_1 u = -u$ for all $u \in U$. Then $V = \Bbbk G \otimes_{\Bbbk\langle g_1 \rangle} U$ is a Yetter–Drinfeld module over $\Bbbk G$. Let $v_1 = 1 \otimes u$ for some $u \in U$ with $u \neq 0$. Then the vectors

$$v_1,\ v_2 = -g_6 v_1,\ v_3 = -g_4 v_1,\ v_4 = -g_2 v_1,\ v_5 = -g_7 v_1,\ v_6 = -g_5 v_1,\ v_7 = -g_3 v_1,$$

form a basis of V. The degrees of these vectors are $x_1, x_2, \dots, x_7$, respectively. The action of G on V is given by

$$x_i v_j = -v_{3i+5j \bmod 7}, \qquad i,j \in \{1,2,\dots,7\}.$$

The support of V is the affine rack $\mathrm{Aff}(7,5)$. Then $\dim \mathcal{B}(V) = 326592$.

Examples 1.2–1.5 in arbitrary characteristic were discussed in [28]. We collected some information on these Nichols algebras in Table 1, where we write

$$(n)_t = 1 + t + \cdots + t^{n-1} \in \mathbb{Z}[t]$$

for all integers $n \geq 0$.

Be warned, that there exists at least one additional finite-dimensional Nichols algebra over $\mathrm{Aff}(3,2)$ in characteristic two; see [31, Appendix A]. Hence Table 1 should not be regarded as a complete list of finite-dimensional Nichols algebras over simple racks with prime cardinality.

With the present paper, we initiate the study of deformations of braided vector spaces to retrieve additional structural information about Nichols algebras of simple Yetter–Drinfeld modules. We introduce and study braided vector space filtrations

TABLE 1. Finite-dimensional Nichols algebras over affine racks (in arbitrary characteristic).

$\dim V$	$\operatorname{supp} V$	$\dim \mathcal{B}(V)$	Hilbert series	Comments
3	$\mathrm{Aff}(3,2)$	12	$(2)_t^2(3)_t$	Example 1.1
5	$\mathrm{Aff}(5,2)$	1280	$(4)_t^4(5)_t$	Example 1.2
5	$\mathrm{Aff}(5,3)$	1280	$(4)_t^4(5)_t$	Example 1.3
7	$\mathrm{Aff}(7,3)$	326592	$(6)_t^6(7)_t$	Example 1.4
7	$\mathrm{Aff}(7,5)$	326592	$(6)_t^6(7)_t$	Example 1.5

and orders of braided vector spaces. Note that filtrations of Yetter–Drinfeld modules are already commonly used, see e.g. [3]. For simple Yetter–Drinfeld modules however those filtrations are trivial, whereas our definition is much less restrictive. This fact is one of the main reasons that our approach leads to new results.

Deformation techniques are common in several parts of mathematics. Even in the representation theory of generalized quantum groups, (Poisson) orders have been used successfully by Angiono, Andruskiewitsch and Yakimov in [4]. In our context, orders of braided vector spaces and special properties in suitable singular points are studied to obtain information on the size of the Nichols algebra in characteristic 0. This is a new approach, as orders have not yet been applied systematically in the structure theory of Nichols algebras of braided vector spaces. We demonstrate the method's power by solving the long-standing problem of classifying finite-dimensional Nichols algebras of irreducible Yetter–Drinfeld modules of prime dimension over non-abelian groups. We confirm that there exist no finite-dimensional Nichols algebras in this class except the known examples: Over fields of characteristic 0, the Nichols algebras of Examples 1.1–1.5 are the only examples appearing when the (absolutely irreducible) braided vector space has prime dimension.

Theorem 1.6. *Assume that* $\operatorname{char}(\Bbbk) = 0$. *Let* V *be an absolutely irreducible Yetter–Drinfeld module over a group* G *such that the support* $\{x \in G : V_x \neq 0\}$ *of* V *generates* G. *Assume that* $\dim V$ *is a prime number. Then* $\mathcal{B}(V)$ *is finite-dimensional if and only if* $\dim V \in \{3,5,7\}$ *and* V *is isomorphic to one of the Yetter–Drinfeld modules of Examples 1.1, 1.2, 1.3, 1.4, 1.5.*

We remark that in Theorem 1.6 the assumption on the group being generated by the support of V is not too restrictive. Indeed, for the study of $\mathcal{B}(V)$ one can always replace G by its subgroup generated by the support of V.

In [45], Milinski and Schneider studied Nichols algebras of Yetter–Drinfeld modules over Coxeter groups. Later, in [13], Andruskiewitsch and Graña explicitly considered the case of Nichols algebras over dihedral groups of size $2p$, where p is a prime number. In the non-abelian case, this boils down to study Nichols algebras of braided vector spaces of dihedral type, that is, finite-dimensional vector spaces V_p, where $p \geq 3$ is a prime number and the braiding of V_p is of the form

$$c\colon V_p \otimes V_p \to V_p \otimes V_p, \quad c(v_i \otimes v_j) = \lambda v_{2i-j \bmod p} \otimes v_i,$$

for some basis $v_0, v_1, \dots, v_{p-1}$ and some non-zero scalar λ.

The case where $(p,\lambda) = (3,-1)$ is that of Example 1.1.

The question of determining the finite-dimensional Nichols algebras whose support is a simple rack was raised in [11, page 228] and discussed in several papers, including [10, 12, 26] and [2, §4.4]. Theorem 1.6 answers this question for simple racks with a prime cardinal.

The paper is organized as follows. In Section 2 we discuss affine racks and absolutely irreducible Yetter–Drinfeld modules of prime dimension. Section 3 concerns orders of braided vector spaces. In Section 4 we discuss the passage from characteristic zero to positive characteristic. The proof of Theorem 1.6 appears in Section 5. In an appendix, we discuss the applicability of our methods to similar problems like that of Nichols algebras over symmetric groups or classes of non-abelian finite groups (see Corollary 7.3).

The strategy of the proof. The proof of Theorem 1.6 consists of three major steps. First, we study Nichols algebras of Yetter–Drinfeld orders and, in particular, their specializations at well-chosen primes. Second, we relate these specializations to Nichols algebras of diagonal type using filtrations of braided vector spaces. Finally, we use the classification of rank two Nichols algebras of diagonal type in positive characteristic obtained in [50]. To deal with the cases not treated by this method, we develop a second technique based on Yetter–Drinfeld orders which relies on the classification of finite-dimensional Nichols algebras of semisimple Yetter–Drinfeld modules in positive characteristic in [35].

2. Preliminaries

In this section, we review some basic notions about racks and quandles. We refer to [14] for more details. A *rack* is a set X together with a binary operation $(x,y)\mapsto x\triangleright y$ on X such that every map $\varphi_x\colon X\to X$, $y\mapsto x\triangleright y$, is bijective, and $x\triangleright(y\triangleright z)=(x\triangleright y)\triangleright(x\triangleright z)$ holds for all $x,y,z\in X$. A rack is said to be *indecomposable* if the group generated by $\{\varphi_x : x\in X\}$ acts transitively on X.

A rack is a *quandle* if $x\triangleright x=x$ for all $x\in X$.

In this work, we deal with a particular family of racks. An *affine (or Alexander) rack* is a triple $(A,g,\triangleright)$, where A is an abelian group, $g\in\operatorname{Aut}(A)$ and $(a,b)\mapsto a\triangleright b$ is the binary operation on A given by $a\triangleright b=(\mathrm{id}-g)(a)+g(b)$ for all $a,b\in A$. In this case, we denote this rack by $\operatorname{Aff}(A,g)$.

An affine rack $\operatorname{Aff}(A,g)$ is *indecomposable* if and only if $\mathrm{id}-g$ is surjective.

In this work, the following family of affine racks will be crucial. Let p be a prime number and $\mathbb{Z}/p\mathbb{Z}$ be the ring of integers modulo p. For $\alpha\in\mathbb{Z}/p\mathbb{Z}\setminus\{0,1\}$, $\operatorname{Aff}(p,\alpha)$ denotes the affine rack $\operatorname{Aff}(\mathbb{Z}/p\mathbb{Z},g)$, where

$$g\colon\mathbb{Z}/p\mathbb{Z}\to\mathbb{Z}/p\mathbb{Z},\quad g(x)=\alpha x.$$

Then $\operatorname{Aff}(p,\alpha)$ is an affine indecomposable rack.

The following lemmas give some information on the structure of groups generated by a conjugacy class. We will need this when studying Yetter–Drinfeld modules over such groups. For any element g of a group G, we write $\langle g\rangle$ for the subgroup generated by g.

Lemma 2.1. *Let G be a group generated by a finite conjugacy class X, let m be the order of the conjugation action of any $x\in X$ on X, let $<$ be a total order of X, and let z be the maximal element of $(X,<)$. Then for all $n\ge 0$, every element of $X^n\subseteq G$ is of the form $x_1^{n_1}x_2^{n_2}\cdots x_k^{n_k}z^l$ with $k,l\ge 0$, $n_1+n_2+\cdots+n_k+l=n$, $x_1<x_2<\cdots<x_k<z$, and $1\le n_i\le m-1$ for all $1\le i\le k$.*

See Dietzmann's theorem in [37, Theorem 5.10] and Lemmas 2.18 and 2.19 in [28] for related claims.

Proof. The claim is trivial for $n \le 1$. Let $n \in \mathbb{N}$ with $n \ge 2$. Then in any $x_1x_2\cdots x_n \in X^n$, a factor $x_ix_{i+1} \in X^2$ with $1 \le i \le k-1$ and $x_{i+1} < x_i$ can be replaced by the lexicographically smaller factor $x_{i+1}(x_{i+1}^{-1}x_ix_{i+1}) \in X^2$. We now prove that $x^m = z^m$ for all $x \in X$. Then using that z^m is in the center of G, we can achieve that the exponents of the factors $x_i \neq z$ are at most $m-1$.

Note that $x^my = yx^m = (yxy^{-1})^my$ for all $x, y \in X$, Hence $x^m = (yxy^{-1})^m$ for all $x, y \in X$. It follows that $x^m = (gxg^{-1})^m$ for all $x \in X$ and $g \in G$, since G is generated by X. Moreover, X is a conjugacy class of G, and hence $x^m = z^m$ for all $x \in X$. This completes the proof of the lemma. □

Our main objects of interest are Yetter–Drinfeld modules of prime dimension over non-abelian groups.

Lemma 2.2. *Let G be a group generated by a finite conjugacy class X. Then the derived subgroup $[G,G]$ of G is finite and is generated by the elements xy^{-1} with $x, y \in X$. Moreover, for all $z \in X$,*

$$G = [G,G]\langle z\rangle \quad \textit{and} \quad C_G(z) = \big([G,G] \cap C_G(z)\big)\langle z\rangle.$$

Proof. Since G is generated by the conjugacy class X, the group $[G,G]$ is generated by the elements $uyu^{-1}y^{-1}$ with $u, y \in X$, and since $uyu^{-1} \in X$, by the elements xy^{-1} with $x, y \in X$.

Since $(xy^{-1})^{-1} = yx^{-1}$ and $y^{-1}x = (y^{-1}xy)y^{-1}$ for all $x, y \in X$,

$$[G,G] = \{x_1x_2\cdots x_n(y_1y_2\cdots y_n)^{-1} : n \ge 0, x_1, x_2, \dots, x_n, y_1, y_2, \dots, y_n \in X\}.$$

Let $z \in X$. Since

$$x = xz^{-1}z \in [G,G]z \quad \text{and} \quad x^{-1} = x^{-1}zz^{-1} \in [G,G]z^{-1}$$

for all $x \in X$, it follows that $G = [G,G]\langle z\rangle$. Hence $C_G(z) = \big([G,G] \cap C_G(z)\big)\langle z\rangle$.

It remains to prove that $[G,G]$ is finite. Let $<$ be a total order of X with maximal element z. By Lemma 2.1, in this description, we may assume that the monomials $x_1x_2\cdots x_n$ and $y_1y_2\cdots y_n$ are ordered and do not contain factors of the form x^m, $x \in X \setminus \{z\}$, where m is the order of the conjugation action of any $x \in X$ on X. Thus, $[G,G]$ is the set of all elements $\bar{x}z^l\bar{y}^{-1}$, where $\bar{x}, \bar{y}$ are ordered monomials in the letters $X \setminus \{z\}$ without factors x^m, $x \in X \setminus \{z\}$, and $l = |y| - |x|$. This set is finite. □

Lemma 2.3. *Let G be a group and let X be a conjugacy class of G. Assume that X generates G, and that there is a rack isomorphism $\varphi : \mathrm{Aff}(p, \alpha) \to X$ for some prime p and some $\alpha \in \mathbb{Z}/p\mathbb{Z} \setminus \{0,1\}$. For all $i \in \mathbb{Z}/p\mathbb{Z}$ let $g_i = \varphi(i)$, and let $\gamma = g_0g_1^{-1}$.*

(1) *The following relations hold in G:*

$$g_xg_y^{-1} = g_{x+z}g_{y+z}^{-1},$$
$$g_0g_k^{-1} = \gamma^k,$$
$$g_x\gamma = \gamma^\alpha g_x$$

for all $x, y, z \in \mathbb{Z}/p\mathbb{Z}$ and $k \ge 0$.

(2) *The derived subgroup of G is cyclic of order p and is generated by γ.*

Proof. We write $\triangleright$ for the rack action of X.

(1) Since φ is a rack isomorphism, we obtain that

$$g_i \triangleright g_j = g_{(1-\alpha)i+\alpha j} = g_{j+(1-\alpha)(i-j)},$$
$$g_i^{-1} \triangleright g_j = g_{j+(1-\alpha^{-1})(i-j)}$$

for all $i, j \in \mathbb{Z}/p\mathbb{Z}$. Therefore, for all $i, j \in \mathbb{Z}/p\mathbb{Z}$ the relations

$$g_i g_j^{-1} = g_{i\triangleright j}^{-1} g_i = g_{i+(1-\alpha^{-1})((i\triangleright j)-i)} g_{i\triangleright j}^{-1} = g_{i+(1-\alpha)(i-j)} g_{j+(1-\alpha)(i-j)}^{-1}$$

hold in G. Since the difference of $i + (1-\alpha)(i-j)$ and $j + (1-\alpha)(i-j)$ is $i-j$, it follows that

$$g_i g_j^{-1} = g_{i+k(\alpha-1)(i-j)} g_{j+k(\alpha-1)(i-j)}^{-1}$$

for all $k \in \mathbb{Z}$. Since $\alpha \neq 1$, we conclude that $g_x g_y^{-1} = g_{x+z} g_{y+z}^{-1}$ for all $x, y, z \in \mathbb{Z}/p\mathbb{Z}$. As a direct consequence,

$$(g_0 g_1^{-1})^k = g_0 g_1^{-1} g_1 g_2^{-1} \cdots g_{k-1} g_k^{-1} = g_0 g_k^{-1}$$

for all $k \geq 0$. Moreover, for all $x \in \mathbb{Z}/p\mathbb{Z}$ we obtain that

$$g_x \gamma = g_x g_0 g_1^{-1} = g_{x\triangleright 0} g_{x\triangleright 1}^{-1} g_x = g_{(1-\alpha)x} g_{(1-\alpha)x+\alpha}^{-1} g_x = g_0 g_\alpha^{-1} g_x = \gamma^\alpha g_x.$$

(2) By Lemma 2.2, the derived subgroup of G is generated by the elements $g_x g_y^{-1}$ with $x, y \in X$. Thus $[G,G]$ is generated by γ because of (1). Since $\gamma^p = 1$ and since $g_0 \neq g_1$ in G, the order of γ in G is p. □

Theorem 2.4 (Etingof–Guralnick–Soloviev)**.** *Any indecomposable quandle with a prime number of elements is isomorphic to* $\mathrm{Aff}(p,\alpha)$ *for some prime number* p *and* $\alpha \in \mathbb{Z}/p\mathbb{Z} \setminus \{0,1\}$.

Proof. It follows from [25, Theorems 2.5 and 3.1]. □

Recall that a Yetter–Drinfeld module V over a group G is absolutely irreducible if and only if its support is a conjugacy class of G and for some (equivalently, any) $x \in G$ with $V_x \neq 0$ the $\Bbbk C_G(x)$-module V_g is absolutely irreducible.

Corollary 2.5. *Let* $\Bbbk$ *be a field,* G *be a group, and* V *be an absolutely irreducible Yetter–Drinfeld module over* $\Bbbk G$ *of dimension* p *for some prime* p*. Let*

$$X = \{x \in G : V_x \neq 0\},$$

and assume that G *is generated by* X*. Then* $X \cong \mathrm{Aff}(p,\alpha)$ *for some* $\alpha \in \mathbb{Z}/p\mathbb{Z}$, $\dim V_x = 1$ *for all* $x \in X$*, and there is a scalar* $\lambda \in \Bbbk^\times$ *and a family* $(v_x)_{x\in X}$ *of vectors* $v_x \in V_x$*, such that*

$$x v_y = \lambda v_{x\triangleright y}$$

for all $x, y \in X$.

Proof. Let X be the support of V. Since V is irreducible, X is a conjugacy class of G. Since $\dim V = p$, we obtain that $|X| \in \{1, p\}$. By assumption, X generates G. Since V is absolutely irreducible and $\dim(V) = p > 1$, the group G can not be abelian and hence $|X| = p$. Thus X is an indecomposable quandle of size p, and it follows from Theorem 2.4 that there is a rack isomorphism

$$\varphi : \mathrm{Aff}(p,\alpha) \to X$$

for some $\alpha \in \mathbb{Z}/p\mathbb{Z} \setminus \{0,1\}$. For all $i \in \mathbb{Z}/p\mathbb{Z}$ let $g_i = \varphi(i) \in X$, and let $\gamma = g_0 g_1^{-1}$. Since $|X| = \dim V$, it follows that $\dim V_x = 1$ for all $x \in X$. Let $w_0 \in V_{g_0}$ be a non-zero element, $v_{\varphi(0)} = w_0$, and let $\lambda \in \Bbbk$ with $g_0 w_0 = \lambda w_0$. For all $1 \le i \le p-1$ let

$$w_i = \gamma^{i\beta} w_0, \quad v_{\varphi(i)} = w_i,$$

where $\beta \in \mathbb{Z}/p\mathbb{Z}$ with $\beta(\alpha - 1) = 1$. (Note that the claim of the corollary is on the family $(v_x)_{x\in X}$. We use the vectors w_i in order to simplify the notation.)

By Lemma 2.3(1),

$$g_i w_j = g_i \gamma^{j\beta} w_0 = \gamma^{j\alpha\beta} g_i g_0^{-1} \lambda w_0 = \gamma^{j\alpha\beta} g_0 g_{p-i}^{-1} \lambda w_0 = \gamma^{j\alpha\beta} \gamma^{p-i} \lambda w_0.$$

Now note that $p - i = (p - i)(\alpha - 1)\beta$, and hence

$$g_i w_j = \lambda \gamma^{(j\alpha + i(1-\alpha))\beta} w_0 = \lambda w_{i \triangleright j}.$$

This proves the corollary. □

The following lemma will be needed later for technical reasons.

Lemma 2.6. *Let G be a group generated by a conjugacy class x^G of an element $x \in G$. Let m be the order of the conjugation action of x on x^G. Then for all $r \in \mathbb{N}$ with $\gcd(r, m) = 1$, $(x^r)^G$ is a conjugacy class of G of size $|x^G|$.*

Proof. Let $a, b \in \mathbb{Z}$ with $ar + bm = 1$. Then

$$(gx^r g^{-1})^a = gx^{ar} g^{-1} = gx^{1-bm} g^{-1} = gxg^{-1} x^{bm}$$

for all $g \in G$, since x^m is central in G. Hence the map $(x^r)^G \to x^G$, $y \mapsto y^a x^{-bm}$, is bijective. □

Lastly, for our analysis, the following proposition will be crucial.

Proposition 2.7. *Let $\Bbbk$ be a field. Let G be a group and V and W be absolutely irreducible Yetter–Drinfeld modules over $\Bbbk G$. Assume that the supports of V and W do not commute and their union generates G. If $\dim \mathcal{B}(V \oplus W) < \infty$, then*

$$\{\dim V, \dim W\} = \{\{1, 3\}, \{1, 4\}, \{2\}, \{2, 3\}, \{2, 4\}\}.$$

Proof. This is a consequence of [35, Theorem 2.1] by inspection of [35, Table 1]. □

At this point it is interesting to mention that Proposition 2.7 is the main tool in [7, 8, 9, 22] to study Nichols algebras over simple groups.

3. Orders of braided vector spaces and Nichols algebras

Assume that $\mathrm{char}(\Bbbk) = 0$ and let H be a Hopf algebra over $\Bbbk$ with bijective antipode. To study Nichols algebras of Yetter–Drinfeld modules over H, we will use orders of the underlying braided vector spaces.

Definition 3.1. Let V be a finite-dimensional Yetter–Drinfeld module over H and let R be a subring of $\Bbbk$. An *R-order of* the braided vector space V is a finitely generated projective R-submodule V_R of V such that

(1) the canonical map $\Bbbk \otimes_R V_R \to V$, $\lambda \otimes v \mapsto \lambda v$, is bijective, and
(2) $c(V_R^{\otimes 2}) \subseteq V_R^{\otimes 2}$ and $c^{-1}(V_R^{\otimes 2}) \subseteq V_R^{\otimes 2}$.

Example 3.2. Let R be a subring of $\Bbbk$, which is a Dedekind domain, e.g., the ring of integers $\mathbb{Z}[q]$ of a cyclotomic field. Then finitely generated R-submodules of vector spaces over $\Bbbk$ are torsion-free and hence projective. In our applications, in particular in the proof of Theorem 3.7 and of Theorem 1.6, the R-orders will be of this form.

Example 3.3. Let R be a subring of $\Bbbk$ and let V be a Yetter–Drinfeld module over H. Assume that $\dim(H) < \infty$ and let X be a Hopf order of H. This means that X is an R-order of H as a $\Bbbk$-vector space and that X is closed under multiplication, comultiplication, unit, counit, and the antipode (see [23] for precise definitions). The dual Hopf algebra H^* admits a dual Hopf order $X^\star$. By definition,

$$X^\star = \{f \in H^* : f(X) \subseteq R\}.$$

Recall that Yetter–Drinfeld modules can be considered as modules over the Drinfeld double $D(H)$ of H. As a coalgebra, $D(H) = (H^{op})^* \otimes H$, and as an algebra the multiplication is given by the rule

$$(f \otimes a)(g \otimes b) = g_{(1)}(S^{-1}(a_{(3)}))g_3(a_{(1)})fg_{(2)} \otimes a_{(2)}b;$$

see [39, §IX.4.1] for more details. In particular, by using the formulas for the multiplication and comultiplication, it is straightforward to show that the image of $X^\star \otimes_R X$ inside $D(H)$ provides a Hopf order of $D(H)$ that we will write as $D(X)$. The R-matrix is then given by $M = \sum_i e^i \otimes e_i \in D(H)$, where $\{e_i\}$ is a basis of H and $\{e_i\}$ denotes the dual basis of H^*. This element is necessarily contained in $D(X)$ as well. Indeed, $D(X)$ can be characterized as the set of all elements in $H^* \otimes H$ such that their pairing with any element in $X \otimes_R X^\star$ is in R, and it holds that $M(x \otimes f) = f(x)$.

Let now $v_1, \dots, v_n$ be a basis of V. Then

$$\left\{ \sum_{i=1}^n t_i v_i : t_i \in D(X) \right\} \subseteq V$$

is an example of an R-order of V as a braided vector space.

Recall from [33, Definition 7.1.13] that for any $V \in {}^H_H\mathcal{YD}$, the Nichols algebra of V is

$$\mathcal{B}(V) = T(V)/I_V,$$

where $T(V)$ is the tensor algebra of V and

$$I_V = \bigoplus_{n=2}^{\infty} \ker(\Delta_{1^n} : T^n(V) \to T^n(V)) \subseteq T(V),$$

and for each $n \geq 2$, Δ_{1^n} is the n-th symmetrizer morphism. It is well-known that I_V is an ideal and coideal of $T(V)$. The Nichols algebra $\mathcal{B}(V)$ is an $\mathbb{N}_0$-graded algebra and coalgebra with homogeneous components

$$\mathcal{B}^n(V) = T^n(V)/\ker(\Delta_{1^n})$$

for all $n \geq 0$.

Now assume that V is finite-dimensional. Let R be a subring of $\Bbbk$ and let V_R be an R-order of the braided vector space V. Then for all $n \in \mathbb{N}_0$,

$$V_R^{\otimes n} := V_R \otimes_R V_R \otimes_R \cdots \otimes_R V_R$$

is a finitely generated projective module. Moreover, the inclusion $V_R \to V$ induces injections $V_R^{\otimes n} \to V^{\otimes n}$, and isomorphisms

$$\Bbbk \otimes_R V_R^{\otimes n} \xrightarrow{\cong} V^{\otimes n}.$$

Hence

$$\mathcal{B}(V_R)=\bigoplus_{n=0}^{\infty}\big(V_R^{\otimes n}+\ker(\Delta_{1^n})\big)/\ker(\Delta_{1^n})\cong\bigoplus_{n=0}^{\infty}V_R^{\otimes n}/\big(V_R^{\otimes n}\cap\ker(\Delta_{1^n})\big)$$

is a graded braided Hopf algebra over R. As an algebra, it is generated in degree one. We call it the *Nichols algebra of* V_R. We would like to stress that this Hopf algebra is one of the basic points of the paper.

Remark 3.4. *In the literature, authors use different approaches to introduce orders. Alternatively to our definition, we could start with an integral domain R, a Hopf order H_R over R, and a Yetter–Drinfeld module V_R over H_R which is finitely generated projective as an R-module. Then $\mathcal{B}(V_R)$ could be introduced as the quotient of the tensor algebra of V_R by the kernel of $\oplus_n\Delta_{1^n}$. Note however, that our definition of an R-order of V does not require the existence of an R-order of H.*

Let now $\mathfrak{m}$ be a maximal ideal of R. Then $R/\mathfrak{m}$ is a field, and for each finitely generated projective R-module M, $R/\mathfrak{m}\otimes_R M$ is a vector space over $R/\mathfrak{m}$ of dimension $\dim_{\Bbbk}(\Bbbk\otimes_R M)$. (This follows e.g. from Theorem 1 of [21, V.2]; see also the remark on page 111.) Let $c=c_{V,V}$ be the braiding of V. By Definition 3.1,

$$\mathrm{id}\otimes c\in\mathrm{End}_{R/\mathfrak{m}}(R/\mathfrak{m}\otimes_R V_R^{\otimes 2}).$$

It follows that

$$V_{R,\mathfrak{m}}:=R/\mathfrak{m}\otimes_R V_R$$

is a braided vector space and $R/\mathfrak{m}\otimes_R\mathcal{B}(V_R)$ is an $\mathbb{N}_0$-graded braided Hopf algebra with degree one part $V_{R,\mathfrak{m}}$. As an algebra, $R/\mathfrak{m}\otimes_R\mathcal{B}(V_R)$ is generated by $V_{R,\mathfrak{m}}$. Hence $R/\mathfrak{m}\otimes_R\mathcal{B}(V_R)$ is a pre-Nichols algebra of $V_{R,\mathfrak{m}}$. In other words, we have a canonical surjection

$$R/\mathfrak{m}\otimes_R\mathcal{B}(V_R)\to\mathcal{B}(V_{R,\mathfrak{m}}).$$

The analysis in this section is based on the observation that the above surjection might not be injective, which means that it is possible that $R/\mathfrak{m}\otimes_R\mathcal{B}(V_R)$ will not be a Nichols algebra. This has consequences for the structure of $\mathcal{B}(V)$.

We keep our notation and assumptions regarding $\Bbbk$, H, V and R. The following lemma is immediately clear from the preceding discussion.

Lemma 3.5. *Let V_R be an R-order of V and let $\mathfrak{m}$ be a maximal ideal of R. Then $c_{V,V}$ induces a braided vector space structure on $V_{R,\mathfrak{m}}$, and $R/\mathfrak{m}\otimes_R\mathcal{B}(V_R)$ is a pre-Nichols algebra of $V_{R,\mathfrak{m}}$. If $\mathcal{B}(V)$ is finite-dimensional, then $R/\mathfrak{m}\otimes_R\mathcal{B}(V_R)$ and $\mathcal{B}(V_{R,\mathfrak{m}})$ are finite-dimensional.*

We recall Takeuchi's notion of categorical subspaces, see for example [33, Definition 6.1.5]. A *categorical subspace* of a braided vector space (W,c) is a subspace U of W such that

$$c(U\otimes W)=W\otimes U \text{ and } c(W\otimes U)=U\otimes W.$$

Next we formulate a very useful criterion to identify infinite-dimensional Nichols algebras. Another one we will discuss in Section 4.2.

Lemma 3.6. *Let V_R be an R-order of V and let $\mathfrak{m}$ be a maximal ideal of R. Let $W\subseteq\bigoplus_{n\geq 2}R/\mathfrak{m}\otimes_R\mathcal{B}^n(V_R)$ be a categorical subspace consisting of primitive elements. Assume that the Nichols algebra of $V_{R,\mathfrak{m}}\oplus W$ is infinite-dimensional. Then $\mathcal{B}(V)$ is infinite-dimensional.*

Proof. Let $\mathcal{F}$ be the increasing algebra filtration by $\mathbb{N}_0$ of $R/\mathfrak{m} \otimes_R \mathcal{B}(V_R)$ such that $V_{R,\mathfrak{m}}$ and W are in degree one. Then $\mathcal{F}$ is a Hopf algebra filtration. To prove that $\mathcal{F}$ is a coalgebra filtration it is needed that W is a categorical subspace. The graded Hopf algebra associated to $\mathcal{F}$ is a pre-Nichols algebra of $V_{R,\mathfrak{m}} \oplus W$ by construction. Since its canonical quotient Nichols algebra is infinite-dimensional by assumption, it follows that $R/\mathfrak{m} \otimes_R \mathcal{B}(V_R)$ is infinite-dimensional, and hence $\mathcal{B}(V)$ is infinite-dimensional by Lemma 3.5. □

Theorem 3.7. *Assume that* $\mathrm{char}(\Bbbk) = 0$. *Let* V *be an absolutely irreducible Yetter–Drinfeld module over a group* G *such that* $\dim V_x \leq 1$ *for all* $x \in G$. *Assume that the support* $X = \{x \in G : V_x \neq 0\}$ *of* V *generates* G *and has at least three elements. Let* m *be the order of the conjugation action of any* $x \in X$ *on* X. *Let* $\lambda \in \Bbbk \setminus \{0\}$ *be such that*

$$xv = \lambda v \qquad \text{for all } x \in X \text{ and } v \in V_x,$$

and that

1. λ *is a root of* 1,
2. *the order* N *of* λ *is divisible by at least two distinct prime factors, and*
3. *either* $\gcd(m, N) = 1$ *or there is a (unique) prime number* p *such that* $\gcd(m, N) = p^k$ *for some* $k \geq 1$.

Then $\dim \mathcal{B}(V) = \infty$.

Proof. Let $z \in X$ and let $0 \neq v_z \in V_z$. Let R be the smallest subring of $\Bbbk$ such that

$$gv_z \in Rv_z \quad \text{for all } g \in C_G(z). \tag{3.1}$$

Note that $C_G(z) = \big([G,G] \cap C_G(z)\big)\langle z\rangle$. Since $[G,G]$ is finite by Lemma 2.2 and $zv_z = \lambda v_z$, where λ is a root of 1, we conclude that R is an extension of $\mathbb{Z}$ by a root of 1, and $\lambda \in R$.

Now we define an R-order of V. For all $y \in X$ let $h_y \in G$ be such that $h_y v_z \in V_y$, where $h_z = 1$. Let V_R be the (free) R-submodule of V generated by $h_y v_z$ for all $y \in X$. Then Equation (3.1) implies that V_R is an R-order of V.

If $\gcd(m, N) = 1$, let p be a prime divisor of N. Note that otherwise p is by assumption the unique common prime divisor of m and N.

Let $l \geq 1$ and $r \geq 2$ be such that $N = p^l r$ and $\gcd(p, r) = 1$. Let

$$W_R = \sum_{y \in X} R(h_y v_z)^r \subseteq \mathcal{B}(V_R). \tag{3.2}$$

Note that W_R is an RG-subcomodule and an RG-submodule, since the action of G on V_R permutes the R-submodules $Rh_y v_z$ with $y \in X$. Moreover,

$$\Delta((h_y v_z)^r) = \sum_{i=0}^{r} \binom{r}{i}_\lambda (h_y v_z)^i \otimes (h_y v_z)^{r-i} \tag{3.3}$$

for all $y \in X$, where the scalars $\binom{r}{i}_\lambda$ are Gaussian binomial coefficients (see e.g. [33, Section 1.9]).

Let $\mathfrak{m}$ be a maximal ideal of R containing p. Then $W_{R,\mathfrak{m}} = R/\mathfrak{m} \otimes_R W_R$ is a Yetter–Drinfeld submodule over $(R/\mathfrak{m})G$ of $R/\mathfrak{m} \otimes_R \mathcal{B}(V_R)$. Since the order of λ in $R/\mathfrak{m}$ is r, Equation (3.3) implies that $W_{R,\mathfrak{m}}$ consists of primitive elements.

Next we prove that $W_{R,\mathfrak{m}}$ is absolutely irreducible as a Yetter–Drinfeld module over $(R/\mathfrak{m})G$ and determine its dimension. Equation (3.2) implies that the support of $W_{R,\mathfrak{m}}$ is $\{x^r : x \in X\}$. Since $\gcd(r, m) = 1$, Lemma 2.6 implies that the support of $W_{R,\mathfrak{m}}$ consists of $|X|$ elements. Then $\dim(W_{R,\mathfrak{m}})_{z^r} = 1$, and $W_{R,\mathfrak{m}}$ is absolutely irreducible. Note that $|X| \geq 3$. Therefore $\dim \mathcal{B}(V_{R,\mathfrak{m}} \oplus W_{R,\mathfrak{m}}) = \infty$ by Proposition 2.7 and hence $\dim \mathcal{B}(V) = \infty$ by Lemma 3.6. □

4. Nichols algebras in positive characteristic

4.1. **Nichols algebras of diagonal type.** Let $\mathcal{D} = \mathcal{D}(G, (g_i)_{i\in\{1,2\}}, (\chi_i)_{i\in\{1,2\}})$ be a Yetter–Drinfeld datum in the sense of [33, Definition 8.2.2]. Let

$$(q_{ij})_{i,j\in\{1,2\}} = (\chi_j(g_i))_{i,j\in\{1,2\}}$$

be the braiding matrix of $\mathcal{D}$. Let $V \in {}^{\Bbbk G}_{\Bbbk G}\mathcal{YD}$ be a Yetter–Drinfeld module defined by $\mathcal{D}$ with basis x_1, x_2, see [33, Section 8.3]. Thus

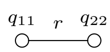
$$\delta(x_i) = g_i \otimes x_i, \quad gx_i = \chi_i(g)x_i$$

for all $i \in \{1,2\}$ and $g \in G$. Then V is a braided vector space of diagonal type with braiding $c = c_{V,V}$ and

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

for all $i,j \in \{1,2\}$.

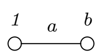
The generalized Dynkin diagram of the braiding matrix $(q_{ij})_{i,j\in\{1,2\}}$ is the labeled graph



with $r = q_{12}q_{21}$, where the edge and the label $q_{12}q_{21}$ are omitted if $q_{12}q_{21} = 1$.

The following result is a particular case of the classification of rank two Nichols algebras of diagonal type in positive characteristic:

Proposition 4.1. *Assume that* $\operatorname{char}(\Bbbk) = p > 0$. *Let* V *be a two-dimensional braided vector space of diagonal type with generalized Dynkin diagram*



where $a \in \{2,3,\dots,p-1\}$ *and* $0 \neq b \in \Bbbk$. *Then* $\dim \mathcal{B}(V) < \infty$ *if and only if*

$$(p,a,b) \in \{(3,2,-1),(5,2,-1),(5,3,-1),(7,3,-1),(7,5,-1)\}.$$

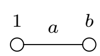
Proof. See [50, Theorem 5.1 and Remark 5.3]. □

For all $m \geq 0$, let $\beta_m = (\operatorname{ad} x_1)^m(x_2)$ in $\mathcal{B}(V)$. By [33, Proposition 4.3.12],

$$\Delta(\beta_m) = \beta_m \otimes 1 + \sum_{k=0}^{m} \binom{m}{k}_{q_{11}} \left(\prod_{l=m-k}^{m-1} (1 - q_{11}^l q_{12}q_{21}) \right) x_1^k g_1^{m-k} g_2 \otimes \beta_{m-k}$$

in $\mathcal{B}(V)\#\Bbbk G$ for all $m \geq 0$.

Assume now that $q_{11} = q_{12} = 1$ and let $a = q_{21}$ and $b = q_{22}$. Thus the generalized Dynkin diagram of V is



Moreover,

$$\Delta(\beta_m) = \beta_m \otimes 1 + \sum_{k=0}^{m} \binom{m}{k}(1-a)^k x_1^k g_1^{m-k} g_2 \otimes \beta_{m-k}$$

in $\mathcal{B}(V)\#\Bbbk G$ for all $m \geq 0$.

Let $\mathcal{A} = \mathcal{B}(\Bbbk x_1)\#\Bbbk G$ and let $K = (\mathcal{B}(V)\#\Bbbk G)^{\mathrm{co}\,\mathcal{A}}$, see [33, Section 13.2]. Let

$$W = (\mathrm{ad}\,\mathcal{A})(\Bbbk x_2) \subseteq \mathcal{B}(V). \tag{4.1}$$

Then $W \in {}^{\mathcal{A}}_{\mathcal{A}}\mathcal{YD}$ by [33, Proposition 13.2.4], and consists of primitive elements of the Hopf algebra $K \in {}^{\mathcal{A}}_{\mathcal{A}}\mathcal{YD}$. The vector space W is spanned by the elements β_m with $m \geq 0$. The braiding of W is given by

$$c(\beta_m \otimes \beta_n) = b \sum_{k=0}^{m} \binom{m}{k} (1-a)^k a^n \beta_{n+k} \otimes \beta_{m-k}. \tag{4.2}$$

By [33, Theorem 13.2.8], $K \cong \mathcal{B}(W)$ as braided Hopf algebras in ${}^{\mathcal{A}}_{\mathcal{A}}\mathcal{YD}$. Moreover,

$$\mathcal{B}(V)\#\Bbbk G \cong K\#\mathcal{A} \quad \text{and} \quad \mathcal{B}(V) \cong K\#\Bbbk[x_1]$$

via bosonization.

Let now p be a prime number and assume that $\mathrm{char}(\Bbbk) = p$. Then $x_1^p = 0$ in $\mathcal{B}(V)$ (since $q_{11} = 1$) and β_p is $g_1^p g_2$-primitive in $\mathcal{B}(V)\#\Bbbk G$ and hence $\beta_p = 0$ in $\mathcal{B}(V)$. In particular, $\dim K < \infty$ if and only if $\dim \mathcal{B}(V) < \infty$. Therefore, by Proposition 4.1, the following holds.

Lemma 4.2. *Let W, K, p, a, b as above. Assume that $\mathrm{char}(\Bbbk) = p$. Then the Nichols algebra $\mathcal{B}(W) \cong K$ is finite-dimensional if and only if*

$$(p, a, b) \in \{(3, -1, -1), (5, 2, -1), (5, 3, -1), (7, 3, -1), (7, 5, -1)\}.$$

4.2. **Deformation of the braided vector space.**

Definition 4.3. Let (V, c) be a braided vector space. A *decreasing filtration of V* is a family $(\mathcal{F}^i V)_{i \geq 0}$ of subspaces $\mathcal{F}^i V \subseteq V$ such that

1. $V = \mathcal{F}^0 V \supseteq \mathcal{F}^k V \supseteq \mathcal{F}^l V$ for all $0 \leq k \leq l$,
2. $\bigcap_{i \geq 0} \mathcal{F}^i V = \{0\}$, and
3. $c(\mathcal{F}^i V \otimes \mathcal{F}^j V) \subseteq \bigoplus_{k+l \geq i+j} \mathcal{F}^k V \otimes \mathcal{F}^l V$ for all $i, j \geq 0$.

Definition 4.4. Let (V, c) be a braided vector space with a decreasing filtration $(\mathcal{F}^i V)_{i \geq 0}$. The pair $(V^{\mathrm{gr}}, c^{\mathrm{gr}})$ with

$$V^{\mathrm{gr}} = \bigoplus_{i \geq 0} \mathcal{F}^i V / \mathcal{F}^{i+1} V,$$

$$c^{\mathrm{gr}} : V^{\mathrm{gr}} \otimes V^{\mathrm{gr}} \to V^{\mathrm{gr}} \otimes V^{\mathrm{gr}}, \qquad x \otimes y \mapsto c(x \otimes y) + \sum_{k+l > i+j} \mathcal{F}^k V \otimes \mathcal{F}^l V$$

$$\text{for all } x \in \mathcal{F}^i V,\ y \in \mathcal{F}^j V,\ i, j \geq 0,$$

is called the *associated graded braided vector space*. We also say that (V, c) *degenerates to* $(V^{\mathrm{gr}}, c^{\mathrm{gr}})$.

Remark 4.5. *In [44], the terminology "specializes" instead of "degenerates" is used.*

Remark 4.6. *Let V be an object in a braided monoidal category, where V is in particular a vector space. In Definition 4.4, we do not require that the filtration consists of objects in the same category. In particular, the degeneration is possibly not an object of the category where V comes from.*

The notion introduced in Definition 4.4 is justified by the following lemma. The proof of this lemma is fairly elementary and is omitted.

Lemma 4.7. *Let (V,c) be a braided vector space and $(\mathcal{F}^iV)_{i\geq 0}$ be a decreasing filtration of V. Then $(V^{\mathrm{gr}}, c^{\mathrm{gr}})$ is a braided vector space, and*

$$c^{\mathrm{gr}}(\mathcal{F}^iV/\mathcal{F}^{i+1}V \otimes \mathcal{F}^jV/\mathcal{F}^{j+1}V) \subseteq \bigoplus_{k+l=i+j} \mathcal{F}^kV/\mathcal{F}^{k+1}V \otimes \mathcal{F}^lV/\mathcal{F}^{l+1}V.$$

For our analysis, the following observation will be crucial.

Proposition 4.8. *Let (V,c) be a braided vector space with a decreasing filtration $(\mathcal{F}^iV)_{i\geq 0}$. Then $\operatorname{gr}\mathcal{B}(V)$ is a pre-Nichols algebra of V^{gr}. In particular, if $\mathcal{B}(V)$ is finite-dimensional, then $\mathcal{B}(V^{\mathrm{gr}})$ is finite-dimensional.*

For Yetter–Drinfeld modules, there is an elementary construction of decreasing filtrations using decreasing Hopf algebra filtrations of finite length.

For any Hopf algebra H with comultiplication Δ, counit ϵ and antipode S, we say that a family $(H_i)_{i\geq 0}$ of subspaces of H is a *decreasing Hopf algebra filtration* if the following conditions hold:

(1) $H_0 = H$, and $H_i \supseteq H_j$ for all $0 \leq i \leq j$.
(2) $H_iH_j \subseteq H_{i+j}$ for all $i,j \geq 0$.
(3) $\Delta(H_i) \subseteq \sum_{j=0}^{i} H_j \otimes H_{i-j}$ for all $i \geq 0$.
(4) $\varepsilon(H_i) = 0$ and $S(H_i) \subseteq H_i$ for all $i \geq 1$.

We say that this filtration has *finite length*, if $H_n = \{0\}$ for some $n \geq 1$.

Proposition 4.9. *Let H be a Hopf algebra with bijective antipode and $(H_i)_{0\leq i\leq n}$ be a decreasing Hopf algebra filtration of H with $H_n = \{0\}$. Let $V \in {}^H_H\mathcal{YD}$, and for all $i \geq 0$ let $\mathcal{F}^iV = H_iV$. Then*

$$\delta(\mathcal{F}^iV) \subseteq \sum_{k\geq 0} H_k \otimes \mathcal{F}^{i-k}V$$

for all $i \geq 0$, and $(\mathcal{F}^iV)_{i\geq 0}$ is a decreasing filtration of the braided vector space V.

Proof. It is clear that $\mathcal{F}^0V = V$ and $\mathcal{F}^{i+1}V = H_{i+1}V \subseteq H_iV = \mathcal{F}^iV$ for all $i \geq 0$. Moreover, $\mathcal{F}^nV = H_nV = \{0\}$.

We now prove the claim about $\delta(\mathcal{F}^iV)$ for all $i \geq 0$. Let $i \geq 0$, $v \in V$ and $h \in H_i$. Then

$$\begin{aligned}\delta(hv) &= h_{(1)}v_{(-1)}S(h_{(3)}) \otimes h_{(2)}v_{(0)} \\ &\in \sum_{j+k+l=i} H_jH_0S(H_l) \otimes H_kV \subseteq \sum_{k\geq 0} H_{i-k} \otimes H_kV\end{aligned}$$

since $(H_i)_{0\leq i\leq n}$ is a decreasing Hopf algebra filtration of H and since $\mathcal{F}^iV = H_iV$.

Finally, for all $i,j \geq 0$ we obtain that

$$c(\mathcal{F}^iV \otimes \mathcal{F}^jV) \subseteq \sum_{k\geq 0} H_k\mathcal{F}^jV \otimes \mathcal{F}^{i-k}V = \sum_{k\geq 0} \mathcal{F}^{j+k}V \otimes \mathcal{F}^{i-k}V,$$

and hence $(\mathcal{F}^iV)_{i\geq 0}$ is a decreasing filtration of V. □

Corollary 4.10. *Let H be a Hopf algebra with bijective antipode, and let $J \subseteq H$ be a nilpotent Hopf ideal and $H_i = J^i$ for all $i \geq 0$. Let $V \in {}^H_H\mathcal{YD}$.*

(1) *The family $(J^i)_{i\geq 0}$ is a decreasing Hopf algebra filtration of H of finite length.*
(2) *The family $(J^iV)_{i\geq 0}$ is a decreasing filtration of the braided vector space V.*

(3) *Let*

$$H^{\mathrm{gr}} = \bigoplus_{i\geq 0} H_i/H_{i+1}.$$

Then H^{gr} is an $\mathbb{N}_0$-graded Hopf algebra.

(4) *The H-action and the H-coaction on V induce an H^{gr}-action and an H^{gr}-coaction on*

$$V^{\mathrm{gr}} = \bigoplus_{i\geq 0} J^iV/J^{i+1}V.$$

With them, V^{gr} is an $\mathbb{N}_0$-graded Yetter–Drinfeld module over H^{gr}.

Proof. (1) The defining properties of a decreasing Hopf algebra filtration follow from the fact that J is a Hopf ideal of H. The finite length property follows from the nilpotency of J.

(2) Apply Proposition 4.9 with $H_i = J^i$ for all $i \geq 0$.

(3) This is mainly due to (1). The claim can be proven by standard arguments.

(4) The H-action and H-coaction on $V \in {}^H_H\mathcal{YD}$ are filtered morphisms. This implies the claim. □

Remark 4.11. *The family $(J^i)_{i\geq 0}$ is also known as the J-adic topology of H, and the corresponding family $(J^iV)_{i\geq 0}$ as the J-adic topology of V.*

Proposition 4.12. *Let $\Bbbk$ be a field of characteristic $p > 0$. Let G be a group and V be an absolutely irreducible Yetter–Drinfeld module over $\Bbbk G$ of dimension p. Assume that*

$$X = \{x \in G : V_x \neq 0\}$$

generates G. Let $\varphi : \mathrm{Aff}(p,\alpha) \to X$ be a rack isomorphism with $\alpha \in \mathbb{Z}/p\mathbb{Z} \setminus \{0,1\}$. Let $g_0 = \varphi(0)$, $\gamma = \varphi(0)\varphi(1)^{-1}$, $0 \neq v_0 \in V_{g_0}$, and $\lambda \in \Bbbk$ be such that $g_0v_0 = \lambda v_0$.

(1) *The ideal $J \subseteq \Bbbk G$ generated by $\gamma - 1$ is a nilpotent Hopf ideal of $\Bbbk G$.*

(2) *The J-adic filtration $(J^i)_{i\geq 0}$ of $\Bbbk G$ defines a filtration $(J^iV)_{i\geq 0}$ of the braided vector space V.*

(3) *For each $0 \leq j \leq p-1$, $V^{\mathrm{gr}}(j)$ is spanned linearly by $(\gamma-1)^jv_0$. The structure maps of the Yetter–Drinfeld module V^{gr} are determined by*

$$g_0(\gamma-1)^jv_0 = \lambda\alpha^j(\gamma-1)^jv_0,$$

$$\delta((\gamma-1)^jv_0) = \sum_{i=0}^{j}\binom{j}{i}(1-\alpha)^i(\gamma-1)^ig_0 \otimes (\gamma-1)^{j-i}v_0$$

for all $0 \leq j \leq p-1$.

Proof. The isomorphism φ exists by Corollary 2.5. For all $i \in \mathbb{Z}/p\mathbb{Z}$ let $g_i = \varphi(i)$.

(1) It is clear that J is a Hopf ideal. By Lemma 2.3(1),

$$g_i(\gamma-1) = (\gamma^\alpha - 1)g_i \in (\gamma-1)\Bbbk G, \tag{4.3}$$

and hence $G(\gamma-1) \subseteq (\gamma-1)\Bbbk G$. Similarly, $(\gamma-1)G \subseteq \Bbbk G(\gamma-1)$, and hence

$$J = \Bbbk G(\gamma-1) = (\gamma-1)\Bbbk G. \tag{4.4}$$

Moreover, $(\gamma-1)^p = \gamma^p - 1 = 0$. Therefore J is nilpotent.

(2) follows from Corollary 4.10.

(3) Let $0 \leq j \leq p-1$. By definition, $(\gamma-1)^jv_0 \in J^jV$. Moreover, since $V = \Bbbk Gv_0$, Equation (4.4) implies that $J^jV = \Bbbk G(\gamma-1)^jv_0$.

By Equation (4.3),

$$g_0(\gamma-1)+J^2=(\gamma^\alpha-1)g_0+J^2=(\gamma-1)\sum_{i=0}^{\alpha-1}\gamma^i g_0+J^2=\alpha(\gamma-1)g_0+J^2.$$

Since $g_0v_0=\lambda v_0$, it follows by induction on j that

$$g_0(\gamma-1)^j v_0+J^{j+1}V=\alpha^j\lambda(\gamma-1)^j v_0+J^{j+1}V.$$

For all $1\leq i\leq p-1$,

$$g_i=g_ig_0^{-1}g_0=g_0g_{p-i}^{-1}g_0=\gamma^{p-i}g_0.$$

Hence

$$\begin{aligned}g_i(\gamma-1)^j v_0&=\gamma^{p-i}g_0(\gamma-1)^j v_0\\&\in \Bbbk\gamma^{p-i}(\gamma-1)^j v_0+J^{j+1}V\subseteq \Bbbk(\gamma-1)^j v_0+J^{j+1}V.\end{aligned}$$

Therefore

$$J^jV=\Bbbk(\gamma-1)^j v_0+J^{j+1}V.$$

The proof of the formula for $\delta((\gamma-1)^j v_0)$ follows similarly by induction on j. □

Theorem 4.13. *Let p be a prime number and assume that* $\operatorname{char}(\Bbbk)=p$. *Let V be an absolutely irreducible Yetter–Drinfeld module over a group G such that $\dim V=p$ and the support of V generates G. Then $\mathcal{B}(V)$ is finite-dimensional if and only if $p\in\{3,5,7\}$ and V is isomorphic to one of the Yetter–Drinfeld modules of Examples 1.1, 1.2, 1.3, 1.4, 1.5.*

Proof. Let X be the support of V. By Corollary 2.5, $X\cong\operatorname{Aff}(p,\alpha)$ for some $\alpha\in\mathbb{Z}/p\mathbb{Z}\setminus\{0,1\}$, $\dim V_x=1$ for all $x\in X$, and there exist a scalar $\lambda\in\Bbbk^\times$ and a basis $(v_x)_{x\in X}$ of V such that

$$xv_y=\lambda v_{x\triangleright y},\quad \delta(v_y)=y\otimes v_y$$

for all $x,y\in X$.

Assume first that

$$(p,\alpha,\lambda)\in\{(3,2,-1),(5,2,-1),(5,3,-1),(7,3,-1),(7,5,-1)\}.$$

Then $\mathcal{B}(V)$ is one of the Nichols algebras of Examples 1.1, 1.2, 1.3, 1.4, 1.5 and therefore it is finite-dimensional.

Assume now that

$$(p,\alpha,\lambda)\notin\{(3,2,-1),(5,2,-1),(5,3,-1),(7,3,-1),(7,5,-1)\}.$$

By assumption, $\operatorname{char}(\Bbbk)=p$. Let $(J^jV)_{j\geq 0}$ be the J-adic filtration of V in Proposition 4.12 and let V^{gr} be the associated graded Yetter–Drinfeld module. Then by functoriality, the filtration induces a filtration of $\mathcal{B}(V)$. By Proposition 4.8, $\operatorname{gr}\mathcal{B}(V)$ is a pre-Nichols algebra of $\mathcal{B}(V^{\mathrm{gr}})$. It suffices to prove that $\dim\mathcal{B}(V^{\mathrm{gr}})=\infty$.

By Proposition 4.12(3), there exist $g_0\in X$ and $0\neq v_0\in V_{g_0}$ such that the elements $y_j=(\gamma-1)^j v_0$ with $0\leq j\leq p-1$ form a basis of V^{gr}. Moreover, the

Yetter–Drinfeld structure of V^{gr} in Proposition 4.12(3) implies that

$$\begin{aligned} c^{\mathrm{gr}}(y_m \otimes y_n) &= (y_m)_{(-1)} y_n \otimes (y_m)_{(0)} \\ &= \sum_{i=0}^{m} \binom{m}{i} (1-\alpha)^i (\gamma - 1)^i g_0 y_n \otimes y_{m-i} \\ &= \sum_{i=0}^{m} \binom{m}{i} (1-\alpha)^i \lambda \alpha^n y_{n+i} \otimes y_{m-i} \end{aligned}$$

for all $0 \leq m, n \leq p-1$. Let W be the braided vector space in Equation (4.1) corresponding to the parameters $a = \alpha$ and $b = \lambda$. By (4.2) and the above formula for c^{gr}, the linear map

$$V^{\mathrm{gr}} \to W, \quad y_m \mapsto \beta_m,$$

is an isomorphism of braided vector spaces. Thus $\dim \mathcal{B}(V^{\mathrm{gr}}) = \infty$ by Lemma 4.2, and the proof is completed. □

5. Proof of Theorem 1.6

Let X denote the support of V. By Corollary 2.5, $X \cong \mathrm{Aff}(p, \alpha)$ for $p = \dim(V)$ and some $\alpha \in \mathbb{Z}/p\mathbb{Z} \setminus \{0, 1\}$, $\dim V_x = 1$ for all $x \in X$, and there is a scalar $\lambda \in \Bbbk^\times$ and a family $(v_x)_{x \in X}$ of vectors $v_x \in V_x$, such that

$$x v_y = \lambda v_{x \triangleright y}$$

for all $x, y \in X$.

If λ is not a root of 1, or $\lambda = 1$, then for all $x \in X$, $\mathcal{B}(V_x)$ is infinite-dimensional (see e.g. [33, Example 1.9.6]), and hence $\mathcal{B}(V)$ is infinite-dimensional.

Assume that λ is a root of 1 and $\lambda \neq 1$. Let $R = \mathbb{Z}[\lambda] \subseteq \Bbbk$. Let V_R be the (free) R-submodule of V generated by the vectors v_x with $x \in X$. Then V_R is an R-order of the braided vector space V. Let $\mathfrak{m}$ be a maximal ideal of R containing p. Then $\mathrm{char}(R/\mathfrak{m}) = p$.

Assume first that $\lambda \neq -1$ in $R/\mathfrak{m}$ or

$$(p, \alpha) \notin \{(3,2), (5,2), (5,3), (7,3), (7,5)\}.$$

Then $\mathcal{B}(V_{R,\mathfrak{m}})$ is infinite-dimensional by Theorem 4.13. Hence $\mathcal{B}(V)$ is infinite-dimensional by Lemma 3.5.

Assume now that $\lambda = -1$ in $R/\mathfrak{m}$ and

$$(p, \alpha) \in \{(3,2), (5,2), (5,3), (7,3), (7,5)\}.$$

If $\lambda = -1$ in R, then $\lambda = -1$ in $\Bbbk$ and hence V is one of the Examples 1.1–1.5. In this case, $\mathcal{B}(V)$ is finite-dimensional. Otherwise, assume that $\lambda \neq -1$ in R. Then the order of λ in $\Bbbk$ is $2p^k$ for some $k \geq 1$. Moreover, since $|\alpha|$ is the order of the conjugation action, $\gcd(|\alpha|, p) = 1$. In particular, $\gcd(2p^k, |\alpha|) \in \{1, 2\}$. Then $\mathcal{B}(V)$ is infinite-dimensional by Theorem 3.7, and the proof of the theorem is completed.

Remark 5.1. *Theorem 1.6 is not valid if V is assumed to be irreducible but not absolutely irreducible. Indeed, let $\Bbbk = \mathbb{R}$ and let $V = V_g$ be a 2-dimensional Yetter–Drinfeld module over $G = \mathbb{Z}$, where g is a generator of the group $\mathbb{Z}$. Assume that $g^2 + g + 1$ acts by 0 on V. Then $\mathbb{C} \otimes_{\mathbb{R}} V$ is a braided vector space of diagonal type, and* $\dim \mathcal{B}(V) = 9$.

6. An example

In this section, we work out explicitly our results in the case of 3-dimensional Yetter–Drinfeld modules.

Let $\Bbbk$ be a field of characteristic zero. Let

$$G = \langle s_1, s_2 : s_1^2 = s_2^2,\ s_1s_2s_1 = s_2s_1s_2 \rangle.$$

Then G is a central extension of the symmetric group $\mathbb{S}_3$. Let X be the conjugacy class of s_1 in G, that is, $X = \{s_1, s_2, s_1s_2s_1^{-1}\}$. Let $\lambda \in \Bbbk^\times$ be a root of 1, and let V be the Yetter–Drinfeld module over $\Bbbk G$ with basis $\{v_x : x \in X\}$ and

$$xv_y = \lambda v_{xyx^{-1}}, \quad x, y \in X.$$

If $\lambda = -1$, then $\mathcal{B}(V)$ is finite-dimensional, see Example 1.1.

Note that $X = \operatorname{supp} V$ and that the map

$$\varphi\colon \operatorname{Aff}(3, -1) \to X, \quad 0 \mapsto s_1,\ 1 \mapsto s_2,\ 2 \mapsto s_1s_2s_1^{-1},$$

is a rack isomorphism. By Lemma 2.3, $\gamma = \varphi(0)\varphi(1)^{-1}$ generates the derived subgroup of G, and has order 3.

For the following, let $R = \mathbb{Z}[\lambda]$ and let V_R be the R-submodule of V generated by $\{v_x : x \in X\}$. Take a maximal ideal $\mathfrak{m}$ of R containing 3, and define

$$V_{R,\mathfrak{m}} = R/\mathfrak{m} \otimes_R V_R.$$

Theorem 3.7 implies that if the order of λ is divisible by at least two prime factors (in particular, if the order of λ is $2 \cdot 3^r$ for some $r \geq 1$), then $\dim \mathcal{B}(V) = \infty$. The proof of Theorem 3.7 follows the following steps:

(1) identify a 3-dimensional Yetter–Drinfeld module W of primitive elements in an associated graded Hopf algebra of $R/\mathfrak{m} \otimes_R \mathcal{B}(V_R)$, spanned by powers of the generators of $V_{R,\mathfrak{m}}$;
(2) use the classification of Nichols algebras of semisimple Yetter–Drinfeld modules to observe that $\mathcal{B}(V_{R,\mathfrak{m}} \oplus W)$ is infinite-dimensional;
(3) use Lemma 3.5 to conclude that $\mathcal{B}(V)$ is infinite-dimensional.

Assume now that the order of λ in R is different from $2 \cdot 3^r$ for all $r \geq 0$, that is, $\lambda 1 \otimes_R R/\mathfrak{m} \neq -1$. Then $\mathcal{B}(V_{R,\mathfrak{m}})$ is infinite-dimensional by Theorem 4.13. (For the proof of this theorem one uses the filtration of V induced by the powers of the radical of the derived subgroup of G and the classification of Nichols algebras of diagonal type in prime characteristic.) Consequently, $\mathcal{B}(V)$ is infinite-dimensional by Lemma 3.5.

7. Appendix: On filtrations of braided vector spaces

In this appendix, we determine some consequences of the existence of filtrations of certain braided vector spaces. We prepare the claims with a lemma.

Lemma 7.1. *Let V be a finite-dimensional vector space together with a direct sum decomposition $V = V(1) \oplus V(2) \oplus \cdots \oplus V(l)$ and a flag*

$$V = \mathcal{F}^0V \supseteq \mathcal{F}^1V \supseteq \cdots \supseteq \mathcal{F}^mV = \{0\}$$

of subspaces with $l, m \geq 1$. Let $n = \dim V$, and for all $1 \leq i \leq n$ let

$$f(i) = \max\{k \geq 0 : i \leq \dim \mathcal{F}^kV\}.$$

Then there exist bases $(x_i)_{1\leq i\leq n}$ and $(b_i)_{1\leq i\leq n}$ of V, and an upper triangular matrix $S = (s_{ij}) \in \Bbbk^{n\times n}$ with diagonal entries 1, satisfying all of the following properties:

(1) *For each* $1 \le i \le n$ *there exists* $1 \le g(i) \le l$ *such that* $x_i \in V(g(i))$.
(2) *For each* $0 \le k \le m-1$, *the vectors* b_i *with* $1 \le i \le \dim \mathcal{F}^k V$ *form a basis of* $\mathcal{F}^k V$.
(3) *For all* $1 \le i \le n$,

$$b_i = x_i + \sum_{j>i} s_{ij} x_j = x_i + \sum_{\substack{j: f(j)<f(i)\\ g(j)\ne g(i)}} s_{ij} x_j.$$

Proof. The claim and the proof are a variation of the LU decomposition of an invertible square matrix.

Let $\mathcal{X} = (x_i)_{1\le i\le n}$ and $\mathcal{B} = (b_i)_{1\le i\le n}$ be bases of V satisfying (1) and (2), respectively. Let $S = (s_{ij}) \in \Bbbk^{n\times n}$ be such that $b_i = \sum_{j=1}^n s_{ij} x_j$ for all $1 \le i \le n$. Clearly, S is invertible. We are going to modify $\mathcal{X}$ and $\mathcal{B}$ step by step such that properties (1) and (2) of the lemma are preserved and S approaches the desired form in (3).

Step 1. We may assume that S is an upper triangular matrix with 1's on the diagonal, and $s_{ij} \ne 0$ with $i<j$ implies that $f(j) < f(i)$. Indeed, the first $\dim \mathcal{F}^{m-1} V$ rows of S are linearly independent. Thus there exist $\dim \mathcal{F}^{m-1} V$ columns of S such that the corresponding square submatrix has full rank. By permuting the basis vectors of $\mathcal{X}$, we may assume that these are the first $\dim \mathcal{F}^{m-1} V$ columns. After applying appropriate row transformations of S (change of vectors b_i in $\mathcal{B}$ with $f(i) = m-1$) we may assume that $s_{ij} = \delta_{ij}$ (Kronecker's delta) for all $1 \le i, j \le \dim \mathcal{F}^{m-1} V$.

With the remaining rows of S we proceed by induction. Regarding vectors $b_i \in \mathcal{B}$ with $f(i) = t$ for some t, we first add to them appropriate vectors in $\mathcal{F}^{t+1} V$ in order to achieve that $s_{ij} = 0$ for all j with $f(j) > f(i)$. Then we choose $\dim \mathcal{F}^t V - \dim \mathcal{F}^{t+1} V$ vectors from $\mathcal{X}$ such that the corresponding square submatrix of S (with rows i such that $f(i) = t$) has full rank, and permute them to the columns j with $f(j) = t$. After suitable row transformations in S (change of vectors b_i in $\mathcal{B}$ with $f(i) = t$) we may assume that $s_{ij} = \delta_{ij}$ (Kronecker's delta) for all $1 \le i, j \le \dim \mathcal{F}^t V$ with $f(j) \ge f(i)$. We then proceed similarly with the rows i with $f(i) = t-1$.

Step 2. We may assume additionally that $s_{ij} = 0$ whenever $1 \le i < j \le n$, $f(j) < f(i)$, and $g(j) = g(i)$. Indeed, let i_0 be the smallest integer such that there exists j with $f(j) < f(i_0)$ and $g(j) = g(i_0)$. Then replace x_{i_0} by

$$x_{i_0} + \sum_{\substack{j: f(j)<f(i_0)\\ g(j)=g(i_0)}} s_{i_0 j} x_j.$$

After this transformation, the matrix S does not change in rows $> i_0$, and the basis vectors b_i with $i \le i_0$ will satisfy the required property in (3). Thus, by induction on the rows of S, we may complete the construction of $\mathcal{X}$ and $\mathcal{B}$ with the claimed properties. □

Proposition 7.2. *Let G be a group and $V \in {}^{\Bbbk G}_{\Bbbk G}\mathcal{YD}$. Assume that $\dim V < \infty$, V is irreducible, and G is generated by the support of V. Let $(\mathcal{F}^i V)_{i\ge 0}$ be a decreasing filtration of the braided vector space V with $\mathcal{F}^1 V \ne \{0\}$. Then $h\mathcal{F}^i V \subseteq \mathcal{F}^i V$ for all $h \in G$ and $i \ge 0$. Moreover, there exists a normal subgroup $N \ne \{1\}$ of G such that $N \subseteq [G,G]$ and*

$$(g-1)\mathcal{F}^i V \subseteq \mathcal{F}^{i+1} V$$

for all $g \in N$ and $i \geq 0$.

Proof. Let $n = \dim V$ and let $\mathcal{X} = (x_i)_{1 \leq i \leq n}$ and $\mathcal{B} = (b_i)_{1 \leq i \leq n}$ be bases of V as in Lemma 7.1 with respect to the direct sum decomposition of V as a $\Bbbk G$-comodule and the flag of subspaces corresponding to the filtration $(\mathcal{F}^k V)_{k \geq 0}$. For all $1 \leq i \leq n$ let

$$f(i) = \max\{k \geq 0 : i \leq \dim \mathcal{F}^k V\}$$

as in Lemma 7.1. Then for each $k \geq 0$, the vectors

$$(b_i)_{f(i) \geq k}$$

form a basis of $\mathcal{F}^k V$. For all $1 \leq i \leq n$ let $g_i \in G$ such that $x_i \in V_{g_i}$. Let $S = (s_{ij})_{1 \leq i,j \leq n}$ be the upper triangular matrix from Lemma 7.1. We note that

(S1) $s_{ij} = 0$ for all i, j with $i \neq j$ and $f(i) = f(j)$, and
(S2) $s_{ij} = 0$ for all i, j with $i < j$ and $g(i) = g(j)$.

Let now $(t_{ij})_{1 \leq j \leq n}$ be the upper triangular matrix with 1's on the diagonal such that

$$x_i = b_i + \sum_{j > i} t_{ij} b_j$$

for all $1 \leq i \leq n$. Then

$$s_{ij} + t_{ij} + \sum_{i<k<j} s_{ik} t_{kj} = 0 \tag{7.1}$$

for all i, j with $i < j$. Moreover, (S1) implies that

(T1) $t_{ij} = 0$ for all i, j with $i < j$ and $f(i) = f(j)$.

One obtains for all $1 \leq i, j \leq n$ that

$$\begin{aligned} c(b_i \otimes b_j) &= c\Big(\big(x_i + \sum_{k>i} s_{ik} x_k\big) \otimes b_j\Big) \\ &= g_i b_j \otimes \Big(b_i + \sum_{k>i} t_{ik} b_k\Big) + \sum_{k>i} s_{ik} g_k b_j \otimes \Big(b_k + \sum_{l>k} t_{kl} b_l\Big) \\ &= g_i b_j \otimes b_i + \sum_{k>i} t_{ik} g_i b_j \otimes b_k + \sum_{k>i} s_{ik} g_k b_j \otimes b_k + \sum_{k>l>i} s_{il} t_{lk} g_l b_j \otimes b_k. \end{aligned}$$

We can slightly reformulate the last term by inserting and subtracting additional terms. We obtain that

$$\begin{aligned} c(b_i \otimes b_j) = g_i b_j \otimes b_i &+ \sum_{k>i} (t_{ik} + s_{ik}) g_i b_j \otimes b_k + \sum_{k>i} s_{ik} (g_k b_j - g_i b_j) \otimes b_k \\ &+ \sum_{k>l>i} s_{il} t_{lk} (g_l b_j - g_i b_j) \otimes b_k + \sum_{k>l>i} s_{il} t_{lk} g_i b_j \otimes b_k. \end{aligned}$$

Then Equation (7.1) gives the formula

$$\begin{aligned} c(b_i \otimes b_j) = g_i b_j \otimes b_i &+ \sum_{k>i} s_{ik} (g_k b_j - g_i b_j) \otimes b_k \\ &+ \sum_{k>l>i} s_{il} t_{lk} (g_l b_j - g_i b_j) \otimes b_k. \end{aligned} \tag{7.2}$$

Recall that for all $m \geq 0$, the vectors $(b_\alpha)_{f(\alpha) \geq m}$ form a basis of $\mathcal{F}^m V$. Hence for all $m \geq 0$, the vectors $b_\alpha \otimes b_\beta$ with $f(\alpha) + f(\beta) \geq m$ form a basis of the vector space $\sum_{k+l \geq m} \mathcal{F}^k V \otimes \mathcal{F}^l V$.

Now take $1 \le i, j \le n$. Then $b_i \otimes b_j \in \mathcal{F}^{f(i)}V \otimes \mathcal{F}^{f(j)}V$. Let $m = f(i) + f(j)$. Since $(\mathcal{F}^k V)_{k\ge 0}$ is a decreasing filtration of the braided vector space V, we conclude that $c(b_i \otimes b_j)$ is a linear combination of the tensors $b_\alpha \otimes b_\beta$ with $f(\alpha) + f(\beta) \ge m$. Then Equation (7.2) and (S1) imply that $g_i b_j \in \mathcal{F}^{f(j)}V$, and since G is generated by the elements g_k with $1 \le k \le n$, we conclude that

(C1) for all $k \ge 0$, $\mathcal{F}^k V$ is a $\Bbbk G$-submodule of V.

It also follows from the previous paragraph that

(S3) there exist $i < j$ with $s_{ij} \ne 0$.

Ideed, if $s_{ij} = 0$ for all $i < j$, then $b_i \in V_{g_i}$ for all $1 \le i \le n$. In particular, $\mathcal{F}^i V$ is a $\Bbbk G$-subcomodule for all i, and hence a Yetter–Drinfeld submodule because of (C1). However, this contradicts the irreducibility of V and the fact that $\mathcal{F}^1 V \ne \{0\}$.

Now let $d = \min\{f(i) - f(j) : i < j, s_{ij} \ne 0\}$. Then, by (T1) and Equation (7.1), it follows that

(T2) $t_{ij} = 0$ for all $i < j$ with $f(i) - f(j) < d$.

Now the assumptions on c and Equation (7.2) imply that

$$s_{ik}(g_k b_j - g_i b_j) \in \mathcal{F}^{f(j)+d} \quad \text{for all } i < k \text{ with } f(i) - f(k) = d.$$

Using (S2) and (S3), it follows that

(C2) there exist $i < j$ such that $s_{ij} \ne 0$, $g_i \ne g_j$, and $g_i^{-1} g_j v - v \in \mathcal{F}^{l+1}V$ for all $l \ge 0$ and $v \in \mathcal{F}^l V$.

Since $g_i^{-1} g_j \in [G, G]$ for all $1 \le i < j \le n$, (C2) implies that the normal subgroup N of G generated by $g_i^{-1} g_j$ in (C2) satisfies the properties required in the proposition. This completes the proof. □

Corollary 7.3. *Let G be a finite group generated by a conjugacy class X. Assume that the derived subgroup $[G, G]$ is simple non-abelian. Let $V \in {}^{\Bbbk G}_{\Bbbk G}\mathcal{YD}$ be irreducible with support X. Then V does not admit a non-trivial decreasing filtration.*

Proof. Assume that V admits a non-trivial decreasing filtration. By Proposition 7.2, there exists a non-trivial normal subgroup N of G such that $N \subseteq [G, G]$ and

$$(g - 1)\mathcal{F}^i V \subseteq \mathcal{F}^{i+1} V \tag{7.3}$$

for all $g \in N$ and $i \ge 0$. Then $N = [G, G]$ since $[G, G]$ is simple. Since $[G, G]$ is non-abelian, there exists $1 \ne g \in [G, G]$ of order m which is coprime to char($\Bbbk$). In particular, char($\Bbbk$) $= p > 0$. Then $(g - 1)^{p^k} = g^{p^k} - 1$ for all $k \ge 1$, and $g^{p^k} = g$ for k the order of p in $U(\mathbb{Z}/m\mathbb{Z})$. Thus Equation (7.3) implies that $(g - 1)v = 0$ for all $v \in V$. The set of all $h \in [G, G]$ acting trivially on V is a normal subgroup of G and has then to coincide with $[G, G]$. Thus the action of G on V factors through the abelian group $G/[G, G]$, and hence $|X| = 1$, a contradiction to the assumptions on G. □

We conclude the paper with some questions.

Following a question of Andruskiewitsch, we remark that with our techniques the Gelfand–Kirillov dimension of the Nichols algebras in Theorem 1.6 can not yet be determined. The main reason for this is that, at the moment, no sufficiently strong results are available on the Gelfand–Kirillov dimension of Nichols algebras of diagonal type in positive characteristic.

Question 7.4. *Is it possible to determine the precise Hilbert series and the Gelfand–Kirillov dimension of the Nichols algebra of a Yetter–Drinfeld module as in Corollary 2.5?*

A basis for the Nichols algebra of Example 1.1 can be obtained by a straightforward calculation using the Diamond Lemma. However, computer calculations are needed to obtain bases for the algebras of the other examples mentioned in the introduction.

Question 7.5. *Is it possible to construct without computer calculations a basis for each of the Nichols algebras in Examples 1.2–1.5?*

Acknowledgements. This work was partially supported by the project OZR3762 of Vrije Universiteit Brussel. EM would like to thank Ben Martin for fruitful discussions about geometric invariant theory in positive characteristic.

References

[1] N. Andruskiewitsch. On finite-dimensional Hopf algebras. In *Proceedings of the International Congress of Mathematicians—Seoul 2014. Vol. II*, pages 117–141. Kyung Moon Sa, Seoul, 2014.

[2] N. Andruskiewitsch. An introduction to Nichols algebras. In *Quantization, geometry and noncommutative structures in mathematics and physics*, Math. Phys. Stud., pages 135–195. Springer, Cham, 2017.

[3] N. Andruskiewitsch, I. Angiono, and I. Heckenberger. On finite GK-dimensional Nichols algebras over abelian groups. *Mem. Amer. Math. Soc.*, 271(1329):ix+125, 2021.

[4] N. Andruskiewitsch, I. Angiono, and M. Yakimov. Poisson orders on large quantum groups. `arXiv:2008.11025`, 2023.

[5] N. Andruskiewitsch, G. Carnovale, and G. A. García. Finite-dimensional pointed Hopf algebras over finite simple groups of Lie type I. Non-semisimple classes in $\mathbf{PSL}_n(q)$. *J. Algebra*, 442:36–65, 2015.

[6] N. Andruskiewitsch, G. Carnovale, and G. A. García. Finite-dimensional pointed Hopf algebras over finite simple groups of Lie type II: unipotent classes in symplectic groups. *Commun. Contemp. Math.*, 18(4):1550053, 35, 2016.

[7] N. Andruskiewitsch, G. Carnovale, and G. A. García. Finite-dimensional pointed Hopf algebras over finite simple groups of Lie type III. Semisimple classes in $\mathbf{PSL}_n(q)$. *Rev. Mat. Iberoam.*, 33(3):995–1024, 2017.

[8] N. Andruskiewitsch, G. Carnovale, and G. A. García. Finite-dimensional pointed Hopf algebras over finite simple groups of Lie type IV. Unipotent classes in Chevalley and Steinberg groups. *Algebr. Represent. Theory*, 23(3):621–655, 2020.

[9] N. Andruskiewitsch, G. Carnovale, and G. A. García. Finite-dimensional pointed Hopf algebras over finite simple groups of Lie type V. Mixed classes in Chevalley and Steinberg groups. *Manuscripta Math.*, 166(3-4):605–647, 2021.

[10] N. Andruskiewitsch, F. Fantino, G. A. García, and L. Vendramin. On Nichols algebras associated to simple racks. In *Groups, algebras and applications*, volume 537 of *Contemp. Math.*, pages 31–56. Amer. Math. Soc., Providence, RI, 2011.

[11] N. Andruskiewitsch, F. Fantino, M. Graña, and L. Vendramin. Finite-dimensional pointed Hopf algebras with alternating groups are trivial. *Ann. Mat. Pura Appl. (4)*, 190(2):225–245, 2011.

[12] N. Andruskiewitsch, F. Fantino, M. Graña, and L. Vendramin. Pointed Hopf algebras over the sporadic simple groups. *J. Algebra*, 325:305–320, 2011.

[13] N. Andruskiewitsch and M. Graña. Braided Hopf algebras over non-abelian finite groups. volume 63, pages 45–78. 1999. Colloquium on Operator Algebras and Quantum Groups (Spanish) (Vaquerías, 1997).

[14] N. Andruskiewitsch and M. Graña. From racks to pointed Hopf algebras. *Adv. Math.*, 178(2):177–243, 2003.

[15] N. Andruskiewitsch, I. Heckenberger, and H.-J. Schneider. The Nichols algebra of a semisimple Yetter-Drinfeld module. *Amer. J. Math.*, 132(6):1493–1547, 2010.

[16] N. Andruskiewitsch and H.-J. Schneider. Lifting of quantum linear spaces and pointed Hopf algebras of order p^3. *J. Algebra*, 209(2):658–691, 1998.
[17] N. Andruskiewitsch and H.-J. Schneider. Pointed Hopf algebras. In *New directions in Hopf algebras*, volume 43 of *Math. Sci. Res. Inst. Publ.*, pages 1–68. Cambridge Univ. Press, Cambridge, 2002.
[18] Y. Bazlov. Nichols-Woronowicz algebra model for Schubert calculus on Coxeter groups. *J. Algebra*, 297(2):372–399, 2006.
[19] A. Berenstein and D. Kazhdan. Hecke-Hopf algebras. *Adv. Math.*, 353:312–395, 2019.
[20] J. Blasiak, R. I. Liu, and K. Mészáros. Subalgebras of the Fomin-Kirillov algebra. *J. Algebraic Combin.*, 44(3):785–829, 2016.
[21] N. Bourbaki. *Commutative algebra. Chapters 1–7*. Elements of Mathematics (Berlin). Springer-Verlag, Berlin, 1998. Translated from the French, Reprint of the 1989 English translation.
[22] G. Carnovale and M. Costantini. Finite-dimensional pointed Hopf algebras over finite simple groups of Lie type VI. Suzuki and Ree groups. *J. Pure Appl. Algebra*, 225(4):Paper No. 106568, 19, 2021.
[23] J. Cuadra and E. Meir. On the existence of orders in semisimple Hopf algebras. *Trans. Amer. Math. Soc.*, 368(4):2547–2562, 2016.
[24] J. S. Ellenberg, T. Tran, and C. Westerland. Fox-neuwirth-fuks cells, quantum shuffle algebras, and malle's conjecture for function fields. `arXiv:1701.0454`, 2023.
[25] P. Etingof, A. Soloviev, and R. Guralnick. Indecomposable set-theoretical solutions to the quantum Yang-Baxter equation on a set with a prime number of elements. *J. Algebra*, 242(2):709–719, 2001.
[26] F. Fantino and L. Vendramin. On twisted conjugacy classes of type D in sporadic simple groups. In *Hopf algebras and tensor categories*, volume 585 of *Contemp. Math.*, pages 247–259. Amer. Math. Soc., Providence, RI, 2013.
[27] S. Fomin and A. N. Kirillov. Quadratic algebras, Dunkl elements, and Schubert calculus. In *Advances in geometry*, volume 172 of *Progr. Math.*, pages 147–182. Birkhäuser Boston, Boston, MA, 1999.
[28] M. Graña, I. Heckenberger, and L. Vendramin. Nichols algebras of group type with many quadratic relations. *Adv. Math.*, 227(5):1956–1989, 2011.
[29] I. Heckenberger. The Weyl groupoid of a Nichols algebra of diagonal type. *Invent. Math.*, 164(1):175–188, 2006.
[30] I. Heckenberger. Classification of arithmetic root systems. *Adv. Math.*, 220(1):59–124, 2009.
[31] I. Heckenberger, A. Lochmann, and L. Vendramin. Braided racks, Hurwitz actions and Nichols algebras with many cubic relations. *Transform. Groups*, 17(1):157–194, 2012.
[32] I. Heckenberger, A. Lochmann, and L. Vendramin. Nichols algebras with many cubic relations. *Trans. Amer. Math. Soc.*, 367(9):6315–6356, 2015.
[33] I. Heckenberger and H.-J. Schneider. *Hopf algebras and root systems*, volume 247 of *Mathematical Surveys and Monographs*. American Mathematical Society, Providence, RI, [2020] ©2020.
[34] I. Heckenberger and L. Vendramin. A classification of Nichols algebras of semisimple Yetter-Drinfeld modules over non-abelian groups. *J. Eur. Math. Soc. (JEMS)*, 19(2):299–356, 2017.
[35] I. Heckenberger and L. Vendramin. The classification of Nichols algebras over groups with finite root system of rank two. *J. Eur. Math. Soc. (JEMS)*, 19(7):1977–2017, 2017.
[36] I. Heckenberger and L. Vendramin. PBW deformations of a Fomin-Kirillov algebra and other examples. *Algebr. Represent. Theory*, 22(6):1513–1532, 2019.
[37] I. M. Isaacs. *Finite group theory*, volume 92 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 2008.
[38] M. Kapranov and V. Schechtman. Shuffle algebras and perverse sheaves. *Pure Appl. Math. Q.*, 16(3):573–657, 2020.
[39] C. Kassel. *Quantum groups*, volume 155 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1995.
[40] V. K. Kharchenko. A quantum analogue of the Poincaré-Birkhoff-Witt theorem. *Algebra Log.*, 38(4):476–507, 509, 1999.
[41] S. Lentner. New large-rank Nichols algebras over nonabelian groups with commutator subgroup $\mathbb{Z}_2$. *J. Algebra*, 419:1–33, 2014.

[42] S. D. Lentner. Quantum groups and Nichols algebras acting on conformal field theories. *Adv. Math.*, 378:Paper No. 107517, 71, 2021.
[43] S. Majid and E. Raineri. Electromagnetism and gauge theory on the permutation group S_3. *J. Geom. Phys.*, 44(2-3):129–155, 2002.
[44] E. Meir. Geometric perspective on Nichols algebras. *J. Algebra*, 601:390–422, 2022.
[45] A. Milinski and H.-J. Schneider. Pointed indecomposable Hopf algebras over Coxeter groups. In *New trends in Hopf algebra theory (La Falda, 1999)*, volume 267 of *Contemp. Math.*, pages 215–236. Amer. Math. Soc., Providence, RI, 2000.
[46] W. D. Nichols. Bialgebras of type one. *Comm. Algebra*, 6(15):1521–1552, 1978.
[47] M. Rosso. Quantum groups and quantum shuffles. *Invent. Math.*, 133(2):399–416, 1998.
[48] P. Schauenburg. A characterization of the Borel-like subalgebras of quantum enveloping algebras. *Comm. Algebra*, 24(9):2811–2823, 1996.
[49] M. E. Sweedler. *Hopf algebras*. Mathematics Lecture Note Series. W. A. Benjamin, Inc., New York, 1969.
[50] J. Wang and I. Heckenberger. Rank 2 Nichols algebras of diagonal type over fields of positive characteristic. *SIGMA Symmetry Integrability Geom. Methods Appl.*, 11:Paper 011, 24, 2015.
[51] S. L. Woronowicz. Compact matrix pseudogroups. *Comm. Math. Phys.*, 111(4):613–665, 1987.
[52] S. L. Woronowicz. Differential calculus on compact matrix pseudogroups (quantum groups). *Comm. Math. Phys.*, 122(1):125–170, 1989.

(I. Heckenberger) Philipps-Universität Marburg, FB Mathematik und Informatik, Hans-Meerwein-Strasse, 35032 Marburg, Germany.
Email address: heckenberger@mathematik.uni-marburg.de

(E. Meir) Institute of Mathematics, University of Aberdeen, Fraser Noble Building, Aberdeen AB24 3UE, UK
Email address: meirehud@gmail.com

(L. Vendramin) Department of Mathematics and Data Science, Vrije Universiteit Brussel, Pleinlaan 2, 1050 Brussel
Email address: Leandro.Vendramin@vub.be