

BRAIDED RACKS, HURWITZ ACTIONS AND NICHOLS ALGEBRAS WITH MANY CUBIC RELATIONS

I. HECKENBERGER

Philipps-Universität Marburg
FB Mathematik und Informatik
Hans-Meerwein-Straße
35032 Marburg, Germany
heckenberger@mathematik.uni-marburg.de

A. LOCHMANN

Philipps-Universität Marburg
FB Mathematik und Informatik
Hans-Meerwein-Straße
35032 Marburg, Germany
lochmann@mathematik.uni-marburg.de

L. VENDRAMIN

Depto. de Matemática, FCEyN
Universidad de Buenos Aires
Pab. 1, Ciudad Universitaria (1428)
Buenos Aires, Argentina
lvendramin@dm.uba.ar

Abstract. We classify Nichols algebras of irreducible Yetter–Drinfeld modules over groups such that the underlying rack is braided and the homogeneous component of degree three of the Nichols algebra satisfies a given inequality. This assumption turns out to be equivalent to a factorization assumption on the Hilbert series. Besides the known Nichols algebras we obtain a new example. Our method is based on a combinatorial invariant of the Hurwitz orbits with respect to the action of the braid group on three strands.

Introduction

Since its introduction in 1998 by Andruskiewitsch and Schneider, the Lifting Method [AS98] grew to one of the most powerful and most fruitful methods to study Hopf algebras [AS00], [BDR02], [Did05], [KR09], [ABM10], [Mom10], [ARS10], [AS10], [MPSW], [GG], [Mas]. Although it originates from a purely Hopf algebraic problem, the method quickly showed a strong relationship with other areas of mathematics such as

- quantum groups [Ros98], [AS10],
- noncommutative differential geometry [Wor89], [Sch96], [Maj05], [KS97],
- knot theory [KRT97], [CJK$^+$03], [Gra02],

DOI: 10.1007/s00031-012-9176-7
Keywords: Hopf algebra, Hurwitz action, Nichols algebra, Rack, 3-transposition group.
Received March 24, 2011. Accepted October 17, 2011.

- combinatorics of root systems and Weyl groups [Hec09], [AHS10], [Ang],
- Lyndon words [Kha99], [GH07], [Ang09],
- cohomology of flag varieties [FK99], [Baz06], [KM10],
- projective representations [Ven],
- conformal field theory [Gab03], [ST].

The heart of the Lifting Method is formed by the structure theory of Nichols algebras. Nichols algebras were studied first by Nichols [Nic78]. These are connected graded braided Hopf algebras [And02] generated by primitive elements, and all primitive elements are of degree one. If the braiding is trivial and the base field has characteristic 0, the Nichols algebra is a polynomial ring. The situation becomes much more complicated for non-trivial braidings. A major problem, which is open since the introduction of the Lifting Method, is the classification of finite-dimensional Nichols algebras over groups [And02, Questions 5.53, 5.57]. Under the additional assumption that the base field has characteristic 0 and the group is abelian, this problem was completely solved in [Hec06], [Hec09] using Lie theoretic structures. A generalization of this theory to arbitrary groups is possible [AHS10], [HS10] and opens new research directions [HS]. Nevertheless, the problem of classifying finite-dimensional Nichols algebras of irreducible Yetter–Drinfeld modules over non-abelian groups cannot be attacked with this method. One needs a fundamentally new idea. One approach in this direction is to identify finite groups admitting (almost) only infinite-dimensional Nichols algebras. Here a remarkable progress was achieved for sporadic simple groups and for alternating groups [AFGVb], [AFGV11]. Despite these developments, the structure of important examples of Nichols algebras, for example, those associated with the transpositions of the symmetric groups, remained unknown for more than 10 years [FK99], [MS00], [AFGVb].

So far only a few finite-dimensional Nichols algebras of irreducible Yetter–Drinfeld modules over non-abelian groups are known. These examples have an interesting property in common: the Hilbert series of the Nichols algebras factorize into the product of polynomials of the form $1+t^r+t^{2r}+\cdots+t^{nr}$ with $r,n\geq 1$. A theoretical explanation of this fact is not known. Motivated by this observation, in [GHV] M. Graña and the first and the last authors classified finite-dimensional Nichols algebras over groups with many quadratic relations. This corresponds to a factorization of the Hilbert series, where only $r=1$ appears. After the publication of the paper some other examples appeared which require one to allow $r>1$. In our paper we attack the case $r\leq 2$. We consider in detail the Hurwitz orbits with respect to the action of the braid group $\mathbb{B}_3$ on X^3, where X is the support of the Yetter–Drinfeld module. For such orbits, we obtain an estimate on the kernel of the shuffle map using graph theoretical structures closely related to those in percolation theory [STBT10], [BBJW10]. Such structures are known to be very complicated. Since we are forced to perform very sensitive calculations, we concentrate on braided racks; see Definition 2. We obtain all known examples of finite-dimensional Nichols algebras of irreducible Yetter–Drinfeld modules over non-abelian groups except those over the affine racks with 5 elements (which are not braided), and we also get two new examples. In principal, our method allows us to consider arbitrary racks, but to do so we will need additional improvements of the general theory.

Our approach has the advantage that it works for all groups and it produces quickly all known examples. Surprisingly, during our calculations we never met any examples of Nichols algebras which satisfy our assumption but are not known to be finite-dimensional. Although there exist many indecomposable braided racks, for example, conjugacy classes of 3-transpositions, we do not use difficult classification results such as the classification of 3-transposition groups [Fis71], or [AH73].

The structure of our paper is as follows. In Section 1 we recall the fundamental notions related to racks with particular emphasis on braided racks; see Definition 2. We recall the Hurwitz action of the braid group. The orbits of this action play a fundamental role in our approach. In Proposition 9 we determine the Hurwitz orbits in X^3 for braided racks X. The structure of Hurwitz orbits is in general not known. This is one of the reasons we study braided racks first. In Section 1 we also define and determine the immunity of the Hurwitz orbits. This will be a crucial ingredient for our classification theorem.

In Section 2 we formulate our main theorem concerning Nichols algebras with many cubic relations. With Propositions 14 and 15 we give detailed information on the kernel of the quantum shuffle map restricted to orbits of size 1 and 8. This information will help us to obtain a condition in Proposition 20 allowing us to concentrate on a few braided racks. These racks are classified in Sections 4, 5 and 6. In Section 4 we also mention and use an interesting connection to 3-transposition groups [Fis71], [Asc97]. In Section 7 we collect the information obtained in the previous sections to prove our main theorem. We consider the remaining racks and the corresponding Nichols algebras case by case. Our careful preparations allow us to succeed with the proof without using any technical assumptions.

In two appendices we collect tables with information on the racks and the Nichols algebras found and we display Hurwitz orbits graphically.

Acknowledgement. We are grateful to Gunter Malle for introducing us to 3-transposition groups. Many thanks go to Volkmar Welker for providing us with the references to percolation theory. Finally, we thank the referees for their careful reading and for their suggestions leading to improvements of the paper.

I. H. was supported by the German Research Foundation via a Heisenberg fellowship. L. V. was supported by CONICET and DAAD. L. V. thanks Philipps-Universität Marburg for the support of his visit from December 2010 to April 2011.

1. Braid groups, racks and Hurwitz actions

1.1. Racks

We recall basic notions and facts about racks. For additional information we refer to [AG03]. A *rack* is a pair $(X, \triangleright)$, where X is a non-empty set and $\triangleright : X \times X \to X$ is a map (considered as a binary operation on X) such that

(1) the map $\varphi_i : X \to X$, where $x \mapsto i \triangleright x$, is bijective for all $i \in X$, and
(2) $i \triangleright (j \triangleright k) = (i \triangleright j) \triangleright (i \triangleright k)$ for all $i, j, k \in X$.

For all $n \in \mathbb{N}$ and $i, j \in X$ we write $i \triangleright^n j = \varphi_i^n(j)$.

A rack $(X,\triangleright)$, or simply X, is a *quandle* if $i\triangleright i=i$ for all $i\in X$. A *subrack* of a rack X is a non-empty subset $Y\subseteq X$ such that $(Y,\triangleright)$ is also a rack. The *inner group* of a rack X is the group generated by the permutations φ_i of X, where $i\in X$. We write $\mathrm{Inn}(X)$ for the inner group of X. A rack is said to be *faithful* if the map

$$\varphi : X\to \mathrm{Inn}(X),\qquad i\mapsto \varphi_i, \tag{1}$$

is injective.

Remark 1. Let X be a rack. Then

$$\varphi_{i\triangleright j}=\varphi_i\varphi_j\varphi_i^{-1} \tag{2}$$

for all $i,j\in X$.

We say that a rack X is *indecomposable* if the inner group $\mathrm{Inn}(X)$ acts transitively on X. Also, X is *decomposable* if it is not indecomposable. Any finite rack X is the disjoint union of indecomposable subracks [AG03, Prop. 1.17] called the *components of* X.

Let $(X,\triangleright)$ and $(Y,\triangleright)$ be racks. A map $f:X\to Y$ is a *morphism* of racks if $f(i\triangleright j)=f(i)\triangleright f(j)$ for all $i,j\in X$.

Example 1. A group G is a rack with $x\triangleright y=xyx^{-1}$ for all $x,y\in G$. If a subset $X\subseteq G$ is stable under conjugation by G, then it is a subrack of G. In particular, we list the following examples.

(1) The rack given by the conjugacy class of involutions in $G=\mathbb{D}_p$, the dihedral group with $2p$ elements, has p elements. It is called the *dihedral rack* (of order p) and will be denoted by $\mathbb{D}_p$.
(2) The rack $\mathcal{T}$ is the rack associated to the conjugacy class of $(2\,3\,4)$ in $\mathbb{A}_4$. This is the rack associated with the vertices of the tetrahedron, see [AG03, §1.3.4].
(3) The rack $\mathcal{A}$ is the rack associated to the conjugacy class of $(1\,2)$ in $\mathbb{S}_4$.
(4) The rack $\mathcal{B}$ is the rack associated to the conjugacy class of $(1\,2\,3\,4)$ in $\mathbb{S}_4$.
(5) The rack $\mathcal{C}$ is the rack associated to the conjugacy class of $(1\,2)$ in $\mathbb{S}_5$.

Example 2. The racks $\mathbb{D}_p$ (p a prime number), $\mathcal{T}$, $\mathcal{A}$, $\mathcal{B}$, $\mathcal{C}$ are faithful and indecomposable.

Example 3. Let A be an abelian group and let $X=A$. For any $g\in\mathrm{Aut}(A)$ we have a rack structure on X given by

$$x\triangleright y=(1-g)x+gy$$

for all $x,y\in X$. This rack is called the *affine rack* associated to the pair (A,g) and will be denoted by $\mathrm{Aff}(A,g)$. In particular, let p be a prime number, q a power of p and $\alpha\in\mathbb{F}_q\setminus\{0\}$. We write $\mathrm{Aff}(\mathbb{F}_q,\alpha)$, or simply $\mathrm{Aff}(q,\alpha)$, for the affine rack $\mathrm{Aff}(A,g)$, where $A=\mathbb{F}_q$ and g is the automorphism given by $x\mapsto\alpha x$ for all $x\in\mathbb{F}_q$.

Example 4. A finite affine rack (A, g) is faithful if and only if it is indecomposable; see [AG03, §1.3.8].

Remark 2. Let X be a finite rack and assume that $\mathrm{Inn}(X)$ acts transitively on X. Then for all $i, j \in X$ there exist $r \in \mathbb{N}$ and $k_1, k_2, \dots, k_r \in X$ such that $\varphi_{k_1}^{\pm 1}\varphi_{k_2}^{\pm 1}\cdots\varphi_{k_r}^{\pm 1}(i) = j$. Equation (2) implies that all permutations φ_i, where $i \in X$, have the same cycle structure.

Lemma 1 ([AG03, Lemma 1.14])**.** *Let X be a rack, and let Y be a non-empty proper finite subset of X. The following are equivalent.*

(1) *Y and $X \setminus Y$ are subracks of X.*
(2) *$X \triangleright Y \subseteq Y$.*

By [GHV, Lemma 2.18] it is possible to define the degree of a finite indecomposable rack.

Definition 1. The *degree* of a finite indecomposable rack X is the number $\mathrm{ord}(\varphi_x)$ for some (equivalently, all) $x \in X$.

For any rack X let G_X denote its enveloping group

$$G_X = \langle X\rangle/(xy = (x \triangleright y)x \text{ for all } x, y \in X). \quad (3)$$

For a finite indecomposable rack X of degree n, the *finite enveloping group* of X is defined as $\overline{G_X} = G_X/\langle x^n\rangle$, where $x \in X$. This definition does not depend on the choice of $x \in X$; see [GHV, Lemma 2.18].

1.2. Braided racks

Definition 2. A rack X is *braided* if X is a quandle and for all $x, y \in X$ at least one of the equations $x \triangleright (y \triangleright x) = y$, $x \triangleright y = y$ holds.

Lemma 2. *Let X be a braided rack and let $x, y, z \in X$ such that $x \triangleright y = z$ and $z \neq y$. Then $y \triangleright z = x$ and $z \triangleright x = y$.*

Proof. This follows from Definition 2. □

Lemma 3. *Let X be a braided rack and let $x, y \in X$.*

(1) *If $y \triangleright x = x$ then $x \triangleright y = y$.*
(2) *If $x \triangleright (y \triangleright x) = y$ then $y \triangleright (x \triangleright y) = x$.*

Proof. Assume that $x \triangleright (y \triangleright x) = y$ and $y \triangleright x = x$. Then $y = x \triangleright (y \triangleright x) = x \triangleright x = x$ and hence $x \triangleright y = y$, $y \triangleright (x \triangleright y) = x$. □

Lemma 4. *Let X be a quandle. The following are equivalent.*

(1) *X is braided.*
(2) *$x \triangleright (y \triangleright x) \in \{x, y\}$ for all $x, y \in X$.*

Proof. (1)⇒(2). If $x, y \in X$ with $x \triangleright (y \triangleright x) \neq y$ then $x \triangleright y = y$. Hence $y \triangleright x = x$ by Lemma 3. Thus $x \triangleright (y \triangleright x) = x \triangleright x = x$.

(2)⇒(1). Let $x, y \in X$. Then $x \triangleright (y \triangleright x) \in \{x, y\}$ and $y \triangleright (x \triangleright y) \in \{x, y\}$. We have to show that $x \triangleright (y \triangleright x) = y$ or $x \triangleright y = y$. Assume that $x \triangleright (y \triangleright x) \neq y$. Then $x \triangleright (y \triangleright x) = x$ and hence $y \triangleright x = x$ since X is a quandle. If $y \triangleright (x \triangleright y) = y$ then $x \triangleright y = y$. If $y \triangleright (x \triangleright y) = x$ then $x = (y \triangleright x) \triangleright (y \triangleright y) = x \triangleright y$ and hence $x = y$. Again it follows that $x \triangleright y = y$. □

Lemma 5. *Let X be an indecomposable braided rack. Then X is faithful.*

Proof. Assume first that there exists $x \in X$ such that $z \triangleright x = x$ for all $z \in X$. Since X is indecomposable, Lemma 1 with $Y = \{x\}$ implies that $X = \{x\}$. Then X is faithful.

Let now $x, y \in X$ such that $x \triangleright z = y \triangleright z$ for all $z \in X$. By the previous paragraph we may assume that there exists $z \in X$ such that $z \triangleright x \neq x$. Then $x = z \triangleright (x \triangleright z) = z \triangleright (y \triangleright z) \in \{y, z\}$ and hence $x = y$. Thus X is faithful. □

Let X be a finite indecomposable faithful rack and let $x \in X$. In [GHV, Sect. 2.3] integers k_n for $n \in \mathbb{N}_{\geq 2}$ were defined by

$$k_n = \#\{y \in X \mid \underbrace{x \triangleright (y \triangleright (x \triangleright (y \triangleright \cdots)))}_{n \text{ elements}} = y,$$
$$\underbrace{x \triangleright (y \triangleright (x \triangleright (y \triangleright \cdots)))}_{j \text{ elements}} \neq y \quad \text{for all } j \in \{1, 2, \dots, n-1\}\}.$$

In particular,

$$k_2 = \#\{y \in X \mid x \triangleright y = y, x \neq y\}, \quad k_3 = \#\{y \in X \mid x \triangleright (y \triangleright x) = y, x \triangleright y \neq y\}.$$

Since X is indecomposable, the integers k_n do not depend on the choice of x.

Remark 3. By definition, an indecomposable rack X is braided if and only if X is faithful and $k_n = 0$ for all $n > 3$.

Example 5. The racks $\mathbb{D}_3$, $\mathcal{T}$, $\mathcal{A}$, $\mathcal{B}$, $\mathcal{C}$ are braided; see [GHV, Table 2].

Example 6. Let A be a finite abelian group and $g \in \mathrm{Aut}(A)$. It is well known that the affine rack $\mathrm{Aff}(A, g)$ is faithful if and only if $1 - g$ is injective. Since A is finite, this is equivalent to $x \triangleright y \neq y$ for all $x, y \in X$ with $x \neq y$. Therefore $\mathrm{Aff}(A, g)$ is braided if and only if $1 - g + g^2 = 0$. In particular, the affine racks $\mathrm{Aff}(\mathbb{F}_5, 2)$ and $\mathrm{Aff}(\mathbb{F}_5, 3)$ are not braided, but $\mathrm{Aff}(\mathbb{F}_7, 3)$ and $\mathrm{Aff}(\mathbb{F}_7, 5)$ are braided. If an affine rack $\mathrm{Aff}(\mathbb{F}_q, \alpha)$ is braided, then α has order 2, 3 or 6. If $\mathrm{ord}(\alpha) = 2$, then q is a power of 3. If $\mathrm{ord}(\alpha) = 3$, then q is a power of 2.

Proposition 6. *Let X be a braided indecomposable rack. Then X has degree* 1*,* 2*,* 3*,* 4 *or* 6*.*

Proof. Let $x, y \in X$ such that $x \triangleright y \neq y$. Assume that $x \triangleright^n y = y$ with $n > 4$ minimal. We will prove that $n = 6$. We have

$$(x \triangleright y) \triangleright (x \triangleright^2 y) = x \triangleright (y \triangleright (x \triangleright y)) = x \triangleright x = x.$$

By applying φ_y we obtain that

$$x \triangleright (y \triangleright (x \triangleright^2 y)) = (y \triangleright (x \triangleright y)) \triangleright (y \triangleright (x \triangleright^2 y)) = y \triangleright x = x \triangleright^{n-1} y.$$

Then $y \triangleright (x \triangleright^2 y) = x \triangleright^{n-2} y$. By applying $\varphi_{x \triangleright^2 y}$ to the equation $x \triangleright (x \triangleright^3 y) = x \triangleright^4 y$ we obtain that $(x \triangleright^2 y) \triangleright (x \triangleright^4 y) = y$, since

$$\begin{aligned}(x \triangleright^2 y) \triangleright (x \triangleright (x \triangleright^3 y)) &= ((x \triangleright^2 y) \triangleright x) \triangleright ((x \triangleright^2 y) \triangleright (x \triangleright^3 y)) \\ &= (x \triangleright y) \triangleright (x \triangleright^2 (y \triangleright (x \triangleright y))) = (x \triangleright y) \triangleright x = y.\end{aligned}$$

Since $x \triangleright^4 y \neq y$, we conclude that $(x \triangleright^2 y) \triangleright (x \triangleright^4 y) \neq x \triangleright^4 y$. Then

$$((x \triangleright^2 y) \triangleright (x \triangleright^4 y)) \triangleright (x \triangleright^2 y) = x \triangleright^4 y,$$

because X is braided. Therefore $x \triangleright^4 y = y \triangleright (x \triangleright^2 y) = x \triangleright^{n-2} y$ and hence the claim holds. □

Proposition 7. *There exist infinitely many finite braided indecomposable racks of degree* 6 *which are generated by two elements.*

Proof. The affine racks $X = \mathrm{Aff}(\mathbb{F}_q, \alpha)$ are braided if and only if $1 - \alpha + \alpha^2 = 0$. Take any prime number $p > 3$. If there exists $\alpha \in \mathbb{F}_p$ such that $1 - \alpha + \alpha^2 = 0$, then $X = \mathrm{Aff}(\mathbb{F}_q, \alpha)$ is braided. Otherwise, take the quadratic extension of $\mathbb{F}_p$ by α, where $1 - \alpha + \alpha^2 = 0$. These racks are indecomposable, since $\alpha \neq 1$. Moreover, $1 - \alpha + \alpha^2 = 0$ implies that $\alpha^6 = 1$. Since $p > 3$, $\alpha^2 \neq 1$ and $\alpha^3 \neq 1$. We claim that these affine racks are always generated by two elements. If there exists $\alpha \in \mathbb{F}_p$ such that $1 - \alpha + \alpha^2 = 0$, the claim follows from [AFGVa, Prop. 4.2]. Otherwise take the quadratic extension of $\mathbb{F}_p$ by α. Then

$$(u + \alpha v) \triangleright (x + \alpha y) = (u + v - y) + \alpha(x + y - u) \tag{4}$$

for all $u, v, x, y \in \mathbb{F}_p$. In particular, $u \triangleright^3 0 = 2u$ for all $u \in \mathbb{F}_p$ and hence $\mathbb{F}_p$ is included in S, the subrack generated by 0 and 1. Since $0 \triangleright 1 = \alpha$ and $(\alpha v) \triangleright^3 0 = \alpha(2v)$ for all $v \in \mathbb{F}_p$, we conclude similarly that $\alpha\mathbb{F}_p$ is also included in S. Therefore the claim follows from equation (4) by taking $(u, v) = (0, k)$ for $k \in \mathbb{F}_p$ and $(x, y) = (l, 0)$ for $l \in \mathbb{F}_p$. □

1.3. Hurwitz actions

For any $n \in \mathbb{N}$ let

$$\begin{aligned} \mathbb{B}_n = \langle \sigma_1, \dots, \sigma_{n-1} \rangle / (\sigma_i\sigma_j = \sigma_j\sigma_i \;\text{ if } |i - j| \geq 2, \\ \sigma_i\sigma_j\sigma_i = \sigma_j\sigma_i\sigma_j \;\text{ if } |i - j| = 1) \end{aligned} \tag{5}$$

denote the braid group on n strands. According to [Bri88], the action of $\mathbb{B}_n$ on the set $X^n = X \times \cdots \times X$ (n-times), where X is a conjugacy class of a group, was studied implicitly in [Hur91].

Let X be a rack and let $n \in \mathbb{N}$. There is a unique action of the braid group $\mathbb{B}_n$ on X^n such that

$$\sigma_i(x_1, \dots, x_n) = (x_1, \dots, x_{i-1}, x_i \triangleright x_{i+1}, x_i, x_{i+2}, \dots, x_n) \tag{6}$$

for all $x_1, \dots, x_n \in X$, $i \in \{1, 2, \dots, n-1\}$. This action of $\mathbb{B}_n$ on X^n is called the *Hurwitz action* on X^n. For any $(x_1, x_2, \dots, x_n) \in X^n$ we write $\mathcal{O}(x_1, x_2, \dots, x_n)$ for its *Hurwitz orbit*, the orbit under the Hurwitz action. The rack X acts on itself via the map $\triangleright$. This extends to a canonical action of the enveloping group G_X on X. More generally, G_X acts on X^n diagonally:

$$g \triangleright (x_1, \dots, x_n) = (g \triangleright x_1, \dots, g \triangleright x_n) \quad \text{for all } g \in G_X,\ x_1, \dots, x_n \in X. \tag{7}$$

The diagonal action of G_X and the action of $\mathbb{B}_n$ on X^n commute. Two Hurwitz orbits $\mathcal{O}_1, \mathcal{O}_2 \subseteq X^n$ are called *conjugate* if there exists $g \in G_X$ such that the map $X^n \to X^n$, $\bar{x} \mapsto g \triangleright \bar{x}$, induces a bijection $\mathcal{O}_1 \to \mathcal{O}_2$. Two Hurwitz orbits $\mathcal{O}_1, \mathcal{O}_2 \subseteq X^n$ are called *isomorphic* if there exists a bijection $\varphi : \mathcal{O}_1 \to \mathcal{O}_2$ such that $\varphi(\sigma(\bar{x})) = \sigma(\varphi(\bar{x}))$ for all $\sigma \in \mathbb{B}_n$, $\bar{x} \in \mathcal{O}_1$. Clearly, conjugate Hurwitz orbits are isomorphic.

Remark 4. The braided action studied in [GHV] is the same as the Hurwitz action on X^2.

Remark 5. Let X be a rack, $n \in \mathbb{N}$ and $x_1, \dots, x_n, y_1, \dots, y_n \in X$. By the definition of the enveloping group G_X, if $(y_1, y_2, \dots, y_n) \in \mathcal{O}(x_1, x_2, \dots, x_n)$ then $y_1 y_2 \cdots y_n = x_1 x_2 \cdots x_n$ in G_X.

In this work we focus on orbits of the Hurwitz action of $\mathbb{B}_3$. For a given rack X and for all $j \in \mathbb{N}$ let

$$l_j^{(3)} = \#\{\mathcal{O}(x, y, z) \mid x, y, z \in X,\ \#\mathcal{O}(x, y, z) = j\}.$$

It should always be clear from the context which rack X is.

In Proposition 9 below we determine the Hurwitz orbits $\mathcal{O} \subseteq X^3$ of a braided rack X up to isomorphism. The non-trivial orbits are illustrated in Figures 8–14 in Appendix B. In these figures, circles stand for triples in $\mathcal{O}$, black arrows indicate the action of σ_1 and dotted arrows indicate the action of σ_2; see Figure 1.

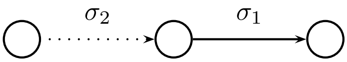

Figure 1: The notation for Hurwitz orbits

For the proof of Proposition 9 the following theorem going back to Coxeter is useful.

Theorem 8. *Let $n, p \in \mathbb{N}$. The group $\mathbb{B}_n/(\sigma_1^p)$ is finite if and only if $(1/n) + (1/p) > 1/2$. In particular,*

$$\mathbb{B}_3/\langle\sigma_1^p\rangle \simeq \begin{cases} \mathbb{S}_3 & \text{if } p = 2, \\ \mathrm{SL}(2,3) & \text{if } p = 3, \\ \mathrm{SL}(2,3) \rtimes \mathbb{Z}_4 & \text{if } p = 4, \\ \mathrm{SL}(2,5) \times \mathbb{Z}_5 & \text{if } p = 5. \end{cases}$$

Proof. See [Cox59] for the first claim. For the second claim see [MK99]. The group $\mathbb{B}_n/(\sigma_1)$ can also be identified with the help of GAP [GAP06]. □

Proposition 9. *Let $d \in \mathbb{N}$ and X a braided rack of size d. Then the possible sizes for a Hurwitz orbit $\mathcal{O} \subseteq X^3$ are 1, 3, 6, 8, 9, 12, 16, and 24. Two such Hurwitz orbits are isomorphic if and only if they have the same size. If X is indecomposable, then*

$$l_1^{(3)} = d, \qquad l_3^{(3)} = dk_2, \qquad l_6^{(3)} = \frac{dt}{6}, \qquad l_9^{(3)} = \frac{d(k_2(k_2-1)-t)}{3},$$
$$l_8^{(3)} = \frac{dk_3}{2}, \qquad l_{12}^{(3)} = \frac{dm}{12}, \qquad l_{16}^{(3)} = \frac{d}{4}(k_2k_3 - k_2^2 + k_2 + t),$$

where

$$m = \#\{x \in X \mid 1 \triangleright x \neq x,\ 1 \triangleright^3 x = x\}, \tag{8}$$
$$t = \#\{(1, x, y) \mid 1 \triangleright x = x,\ 1 \triangleright y = y,\ x \triangleright y = y,\ x \neq 1,\ y \neq 1,\ x \neq y\} \tag{9}$$

and 1 is a fixed element of X.

Remark 6. Let X and m be as in the Proposition. Then $3|m$ since $1 \in X$ acts on $\{x \in X \mid 1 \triangleright x \neq x, 1 \triangleright^3 x = x\}$ and all orbits of this action have size 3 by assumption.

Proof. Let $\mathcal{O} \subseteq X^3$ be a Hurwitz orbit. We distinguish two cases and several subcases.

Case A. Assume that $a_1 \triangleright (a_2 \triangleright a_1) = a_2$ for all $(a_1, a_2, a_3) \in \mathcal{O}$. Then

$$\sigma_1^3(a_1, a_2, a_3) = (a_1, a_2, a_3) \quad \text{for all} \quad (a_1, a_2, a_3) \in \mathcal{O}.$$

In particular, $\mathbb{B}_3/(\sigma_1^3)$ acts on $\mathcal{O}$ via the Hurwitz action. The group $\mathbb{B}_3/(\sigma_1^3)$ is finite by Theorem 8. Moreover, the order of $\mathbb{B}_3/(\sigma_1^3)$ is 24. Thus $\#\mathcal{O}$ divides 24. Let $(a, b, c) \in \mathcal{O}$. The elements of $\mathcal{O}$ (counted possibly several times) are

$$\begin{aligned}
A &= (a, b, c), & B &= (a \triangleright b, a \triangleright c, a),\\
C &= (a \triangleright b, a, c), & D &= ((a \triangleright b) \triangleright c, a \triangleright (b \triangleright c), a \triangleright b),\\
E &= (b, a \triangleright b, c), & F &= (a \triangleright b, c, a \triangleright c),\\
G &= (b, (a \triangleright b) \triangleright c, a \triangleright b), & H &= ((a \triangleright b) \triangleright c, a \triangleright b, a \triangleright c),\\
I &= (a \triangleright (b \triangleright c), b, a \triangleright b), & J &= (b, c, (a \triangleright b) \triangleright c),\\
K &= (c, (a \triangleright b) \triangleright c, a \triangleright c), & L &= (a \triangleright (b \triangleright c), a \triangleright b, a),\\
M &= (c, b \triangleright c, (a \triangleright b) \triangleright c), & N &= (a \triangleright (b \triangleright c), a, b),\\
O &= (b \triangleright c, b, (a \triangleright b) \triangleright c), & P &= (c, a \triangleright c, b \triangleright c),\\
Q &= (b \triangleright c, a \triangleright (b \triangleright c), b), & R &= (a, c, b \triangleright c),\\
S &= (a, b \triangleright c, b), & T &= (b \triangleright c, (a \triangleright b) \triangleright c, a \triangleright (b \triangleright c)),\\
U &= (a \triangleright c, a, b \triangleright c), & V &= (a \triangleright c, b \triangleright c, a \triangleright (b \triangleright c)),\\
W &= ((a \triangleright b) \triangleright c, a \triangleright c, a \triangleright (b \triangleright c)), & X &= (a \triangleright c, a \triangleright (b \triangleright c), a);
\end{aligned}$$

see also Figure 14 in Appendix B.

Case A.1. There exists $(a, b, c) \in \mathcal{O}$ with $a = b = c$. Then $\mathcal{O} = \{(a, a, a)\}$. There are $l_1^{(3)} = d$ such orbits.

Case A.2. There is $(a, b, c) \in \mathcal{O}$ with $\#\{a, b, c\} = 2$. By applying σ_1^{-1} and/or σ_2^{-1} if needed, we may assume that $a = b$. In this case, $\mathcal{O}$ is the Hurwitz orbit of size 8 depicted in Figure 10 in Appendix B, with

$$\begin{aligned}
A &= (c, a \triangleright c, a \triangleright c), & B &= (a, c, a \triangleright c), & C &= (a, a, c),\\
D &= (a \triangleright c, a, a \triangleright c), & & & E &= (a, a \triangleright c, a),\\
F &= (a \triangleright c, a \triangleright c, a \triangleright^2 c), & G &= (a \triangleright c, a \triangleright^2 c, a), & H &= (a \triangleright^2 c, a, a).
\end{aligned}$$

Note that $a \triangleright^2 c$ neither commutes with a nor with $a \triangleright c$ and it differs from both. There are dk_3 triples $(a_1, a_1, a_3) \in X^3$ with $a_1 \triangleright a_3 \neq a_3$. Since C and F are the only triples in $\mathcal{O}$ of this type, we conclude that $l_8^{(3)} = (1/2)\, d\, k_3$.

Case A.3. Assume that $\#\{a_1, a_2, a_3\} = 3$ for all $(a_1, a_2, a_3) \in \mathcal{O}$. Then $a \triangleright b \notin \{a, b, c\}$ and $b \triangleright c \notin \{a, b, c\}$. If the triple $A = (a, b, c)$ differs from all other triples in the above list, then $\#\mathcal{O} = 24$. Otherwise

$$a = (a \triangleright b) \triangleright c, \qquad b = a \triangleright c, \qquad c = a \triangleright (b \triangleright c), \tag{10}$$

in which case $A = W$ and then the graph in Figure 14 in Appendix B collapses to the graph in Figure 12, corresponding to an orbit of size 12. The second and third equations in (10) imply that $b \triangleright c = a \triangleright b$, and hence from (10) one obtains that $c = a \triangleright (a \triangleright b) = a \triangleright^3 c$. In turn, it follows that (10) is equivalent to

$$b = a \triangleright c, \qquad c = a \triangleright^3 c. \tag{11}$$

The triples corresponding to the vertices in Figure 12 are

$$\begin{aligned}
&A = (a, a \triangleright c, c), && B = (a, c, c \triangleright a), && \\
& && C = (a \triangleright c, a, c \triangleright a), && D = (a \triangleright c, c \triangleright a, c), \\
&E = (a, c \triangleright a, a \triangleright c), && F = (c, a \triangleright c, c \triangleright a), && G = (a \triangleright c, c, a), \\
& && H = (c, a, a \triangleright c), && I = (c, c \triangleright a, a), \\
& && J = (c \triangleright a, c, a \triangleright c), && K = (c \triangleright a, a \triangleright c, a), \\
& && L = (c \triangleright a, a, c). &&
\end{aligned}$$

The number of 12-orbits is just the number of triples $(a_1, a_1 \triangleright a_3, a_3)$ with $a_1 \triangleright a_3 \neq a_3$, $a_1 \triangleright^3 a_3 = a_3$ (which is dm) divided by the number of occurrences of such triples in the 12-orbit (which is 12), that is, $l_{12}^{(3)} = (1/12)\, dm$.

Case B. There is $(a, b, c) \in \mathcal{O}$ such that two of a, b, c are different but commuting. We are left with four subcases:

(1) Two of a, b, c are equal, the third one commutes with both.
(2) a, b, c are pairwise different and commuting.
(3) a, b, c are pairwise different; there are precisely two commuting pairs among (a, b), (a, c), (b, c).
(4) a, b, c are pairwise different; there is precisely one commuting pair.

Case B.1. We have an orbit of size 3; see Figure 8 in Appendix B. The number of triples of the form (a_1, a_1, a_3) with $a_1 \neq a_3$ and $a_1 \triangleright a_3 = a_3$ is $l_3^{(3)} = d\, k_2$.

Case B.2. Here $\mathcal{O}$ is an orbit of size 6, see Figure 9 in Appendix B. The braid group acts on the triples in $\mathcal{O}$ just as the permutation group $\mathbb{S}_3$ does. All 6 triples of $\mathcal{O}$ are of this type and there are dt such triples. Hence $l_6^{(3)} = (1/6)\, d\, t$.

Case B.3. By applying σ_1 and/or σ_2 if needed, we may assume that $a \triangleright b = b$, $a \triangleright c = c$. Then $a \triangleright (b \triangleright c) = b \triangleright c$ and $b \triangleright c \notin \{a, b, c\}$. Then $\#\mathcal{O} = 9$; see Figure 11 in Appendix B:

$$\begin{aligned}
A &= (b, c, a), & B &= (b \triangleright c, b, a), & C &= (c, b \triangleright c, a), \\
D &= (b, a, c), & E &= (b \triangleright c, a, b), & F &= (c, a, b \triangleright c), \\
G &= (a, b, c), & H &= (a, b \triangleright c, b), & I &= (a, c, b \triangleright c).
\end{aligned}$$

The total number of triples $(a_1, a_2, a_3) \in X^3$ with

$$a_1 \triangleright a_2 = a_2, \quad a_1 \triangleright a_3 = a_3, \quad a_1 \neq a_2, \quad a_1 \neq a_3, \quad a_2 \neq a_3$$

is $dk_2(k_2 - 1)$. From this we subtract the number of triples in which a_2 and a_3 commute (there are dt such triples) and divide by the number of occurrences of such triples in the 9-orbit (which is 3). Hence $l_9^{(3)} = (1/3)\, d\,(k_2(k_2 - 1) - t)$.

Case B.4. As argued in Case B.3, we may assume that $a \triangleright b = b$. Then $a \triangleright (b \triangleright c) \neq b \triangleright c$ and $(a \triangleright c) \triangleright (b \triangleright c) = b \triangleright c$. Therefore, the orbit $\mathcal{O}$ has at most size 16, with the following triples:

$$
\begin{aligned}
A &= (a, c, b \triangleright c), & B &= (a \triangleright c, a, b \triangleright c),\\
C &= (a \triangleright c, a \triangleright (b \triangleright c), a), & D &= (a, b \triangleright c, b),\\
E &= (c, a \triangleright c, b \triangleright c), & F &= (a \triangleright c, b \triangleright c, a \triangleright (b \triangleright c)),\\
G &= (b, a \triangleright c, a), & H &= (a, b, c),\\
I &= (a \triangleright (b \triangleright c), b, a), & J &= (b, a, c),\\
K &= (c, b \triangleright c, a \triangleright c), & L &= (b \triangleright c, a \triangleright c, a \triangleright (b \triangleright c)),\\
M &= (a \triangleright (b \triangleright c), a, b), & N &= (b, c, a \triangleright c),\\
O &= (b \triangleright c, b, a \triangleright c), & P &= (b \triangleright c, a \triangleright (b \triangleright c), b)
\end{aligned}
$$

(see also Figure 13 in Appendix B). Further, $\#\{a, b, c, a \triangleright c, b \triangleright c\} = 5$ and $a \triangleright (b \triangleright c) \notin \{a, b, a \triangleright c, b \triangleright c\}$. Looking at the first and last components of the above triples it follows that $\#\mathcal{O} = 16$. In particular, $\mathcal{O}$ did not appear in Cases B1–B3.

The total number of triples (a_1, a_2, a_3) of pairwise different elements, such that only a_1 and a_2 commute, can be calculated as follows: the total number of triples (a_1, a_2, a_3) with pairwise different a_1, a_2, a_3, such that a_1 and a_2 commute, but a_1 and a_3 do not commute, is dk_2k_3. Among these we have the $d(k_2(k_2 - 1) - t)$ triples with $a_2 \triangleright a_3 = a_3$ (see also Case B.3). With this, the total number of triples, such that only a_1 and a_2 commute, is

$$d\,k_2\,k_3 - d\,(k_2\,(k_2 - 1) - t) = d\big(k_2\,k_3 - k_2^2 + k_2 + t\big).$$

Finally, there are four triples in $\mathcal{O}(a, b, c)$ of the form (a_1, a_2, a_3) with $a_1 \triangleright a_2 = a_2$: F, H, J and L. Hence

$$l_{16}^{(3)} = \frac{1}{4}\, d\,\big(k_2\,k_3 - k_2^2 + k_2 + t\big).$$

This completes the proof of the proposition. □

1.4. The immunity of a Hurwitz orbit

Let X be a rack. In the next section we will need a combinatorial invariant of a Hurwitz orbit $\mathcal{O} \subseteq X^3$ which is defined as follows.

Definition 3. Let $\mathcal{O} \subseteq X^3$ be a Hurwitz orbit. A *quarantine of* $\mathcal{O}$ is a non-empty subset $Q \subseteq \mathcal{O}$ such that if two of

$$(x, y, z), \quad (x, y \triangleright z, y), \quad (x \triangleright (y \triangleright z), x, y)$$

are in Q, then the third one is in Q. Graphically this means the following (see Figures 1, 2): if two vertices along a path consisting of a dotted arrow followed by a black arrow are in Q, then the third vertex is in Q.

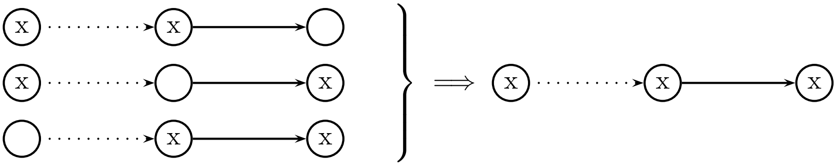

Figure 2: The rule defining a quarantine

A subset $P \subseteq \mathcal{O}$ is called a *plague* if the smallest quarantine of $\mathcal{O}$ containing P is $\mathcal{O}$. Let P be a plague of the smallest possible size. The *immunity of* $\mathcal{O}$ is the number $\mathrm{imm}_{\mathcal{O}} = \#P/\#\mathcal{O} \in \mathbb{Q} \cap (0,1]$.

Proposition 10. *Let X be a braided rack and $\mathcal{O} \subseteq X^3$ a Hurwitz orbit.*

- *If* $\#\mathcal{O} = 1$ *then* $\mathrm{imm}_{\mathcal{O}} = 1$.
- *If* $\#\mathcal{O} \in \{3, 6, 9, 12\}$ *then* $\mathrm{imm}_{\mathcal{O}} = 1/3$.
- *If* $\#\mathcal{O} = 8$ *then* $\mathrm{imm}_{\mathcal{O}} = 3/8$.
- *If* $\#\mathcal{O} = 16$ *then* $\mathrm{imm}_{\mathcal{O}} = 5/16$.
- *If* $\#\mathcal{O} = 24$ *then* $\mathrm{imm}_{\mathcal{O}} = 7/24$.

Proof. By Proposition 9, any Hurwitz orbit $\mathcal{O} \subseteq X^3$ is up to isomorphism uniquely determined by its size, which is one of 1, 3, 6, 8, 9, 12, 16 or 24. The case $\#\mathcal{O} = 1$ is trivial. We use a labeling of the triples of the orbit as on Figures 8–14 in the Appendix. If $\#\mathcal{O} = 3$, then $P = \{A\}$ is a plague. If $\#\mathcal{O} = 6$, then $P = \{A, B\}$ is a plague and no subset of $\mathcal{O}$ of cardinality 1 is a plague.

Assume that $\#\mathcal{O} = 8$. The set $\{A, D, H\}$ is a plague of $\mathcal{O}$. On the other hand, since $\{A, B, D, E, F, G\}$ and $\{B, C, D, E, G, H\}$ are quarantines, for any plague P of $\mathcal{O}$ we have $P \cap \{C, H\} \neq \varnothing$ and $P \cap \{A, F\} \neq \varnothing$. Since none of $\{A, C\}$, $\{A, H\}$, $\{C, F\}$, $\{F, H\}$ is a plague, we obtain that $\mathrm{imm}_{\mathcal{O}} = 3/8$.

Assume that $\#\mathcal{O} = 9$. The set $\{A, B, C\}$ is a plague of $\mathcal{O}$. On the other hand, B is an element of the quarantines $\{B, C, E, G, H\}$, $\{A, B, D, G, I\}$ and $\{B, F\}$, and hence there is no plague P with $B \in P$, $\#P = 2$. Similarly, H is an element of the quarantines $\{B, C, E, G, H\}$, $\{A, C, F, H, I\}$, $\{D, H\}$, and hence there is no plague P with $H \in P$, $\#P = 2$. Finally, $\{B, C, E, G, H\}$, $\{A, E\}$, $\{D, E\}$, $\{E, F\}$, $\{E, I\}$ are quarantines containing E, and hence there is no plague P with $E \in P$, $\#P = 2$. By symmetry, there is no plague P of $\mathcal{O}$ with $\#P = 2$. We conclude that $\mathrm{imm}_{\mathcal{O}} = 1/3$.

The proof for the other orbits is similar but more tedious. However, the crucial inequality $\mathrm{imm}_{\mathcal{O}} \leq \dots$ is easily checked: If $\#\mathcal{O} = 12$, then $\{A, B, D, E\}$ is a plague. If $\#\mathcal{O} = 16$, then $\{A, B, C, E, H\}$ is a plague. If $\#\mathcal{O} = 24$, then $\{A, B, C, D, E, K, N\}$ is a plague. $\square$

2. Nichols algebras over groups

For the general theory of Nichols algebras we refer to [AS02]. Details on the relationship between racks and Nichols algebras can be found in [AG03, §6].

Let $\Bbbk$ be a field. Yetter–Drinfeld modules over a group G are $\Bbbk G$-modules with a left coaction $\delta : V \to \Bbbk G \otimes V$ satisfying the Yetter–Drinfeld condition. Any

Yetter–Drinfeld module V over G decomposes as $V = \bigoplus_{g \in G} V_g$, where $V_g = \{v \in V \mid \delta(v) = g \otimes v\}$ for all $g \in G$. The set

$$\operatorname{supp} V = \{g \in G \mid V_g \neq 0\} \tag{12}$$

is called the *support of* V. By the Yetter–Drinfeld condition, $\operatorname{supp} V$ is invariant under the adjoint action of G.

For any group G, any $g \in G$ and any representation (ρ, W) of the centralizer $C_G(g)$ of g the $\Bbbk G$-module

$$M(g, \rho) = \Bbbk G \otimes_{\Bbbk C_G(g)} W \tag{13}$$

is a Yetter–Drinfeld module, where W is regarded as a $\Bbbk C_G(g)$-module via $\rho \in \operatorname{End}_{\Bbbk}(W)$ and $\delta(h \otimes w) = hgh^{-1} \otimes (h \otimes w)$ for all $h \in G$, $w \in W$. Let g^G be the conjugacy class of g in G. Then $M(g, \rho) = \bigoplus_{x \in g^G} M(g, \rho)_x$, where $M(g, \rho)_{hgh^{-1}} = \Bbbk h \otimes W$ for all $h \in G$.

The category ${}^{\Bbbk G}_{\Bbbk G}\mathcal{YD}$ of Yetter–Drinfeld modules over a group G is a braided monoidal category. Unless otherwise specified, all tensor products are taken over the fixed field $\Bbbk$. The braiding is denoted by c. If the braiding appears together with the tensor product, we also use leg notation: for all $k \in \mathbb{N}$, $i \in \{1, 2, \dots, k-1\}$ and all Yetter–Drinfeld modules $V_{(1)}, \dots, V_{(k)}$ let

$$c_{i,i+1} : V_{(1)} \otimes \cdots \otimes V_{(k)} \to V_{(1)} \otimes \cdots \otimes V_{(i-1)} \otimes V_{(i+1)} \otimes V_{(i)} \otimes V_{(i+2)} \otimes \cdots \otimes V_{(k)},$$
$$c_{i,i+1} = \operatorname{id}^{i-1} \otimes c \otimes \operatorname{id}^{k-i-1}.$$

Nichols algebras are $\mathbb{N}_0$-graded braided Hopf algebras. For any Yetter–Drinfeld module V over a group G the Nichols algebra of V is denoted by $\mathfrak{B}(V)$. Then

$$\mathfrak{B}(V) = \bigoplus_{n \in \mathbb{N}_0} \mathfrak{B}_n(V)$$

is its decomposition into the direct sum of the homogeneous components, where $\mathfrak{B}_0(V) = \Bbbk$, $\mathfrak{B}_1(V) = V$, and $\mathfrak{B}_n(V)$ is a Yetter–Drinfeld submodule of $\mathfrak{B}(V)$ for all $n \in \mathbb{N}_0$. The *Hilbert series of* $\mathfrak{B}(V)$ is the formal power series $\mathcal{H}_{\mathfrak{B}(V)}(t) \in \mathbb{Z}[\![t]\!]$ defined by

$$\mathcal{H}_{\mathfrak{B}(V)}(t) = \sum_{i=0}^{\infty} (\dim \mathfrak{B}_n(V)) t^n. \tag{14}$$

We use the notation

$$(n)_{t^r} = \sum_{i=0}^{n-1} t^{ri}, \qquad (\infty)_{t^r} = \sum_{i=0}^{\infty} t^{ri} \tag{15}$$

for all $r, n \in \mathbb{N}_{\geq 1}$ in connection with the Hilbert series of Nichols algebras.

2.1. Nichols algebras with many cubic relations

The main result of our paper is the following theorem. In (3) the map $1+c_{12}+c_{12}c_{23}\in \mathrm{End}_{\Bbbk}(V^{\otimes 3})$ will appear which is defined using leg notation.

Theorem 11. *Let G be a non-abelian group, $g\in G$ and ρ a finite-dimensional absolutely irreducible representation of $C_G(g)$. Assume that the conjugacy class X of g is a finite braided rack and generates the group G. Let $V=M(g,\rho)$. The following are equivalent.*

(1) *The Hilbert series $\mathcal{H}_{\mathfrak{B}(V)}(t)$ of $\mathfrak{B}(V)$ is a product of factors from*

$$\{(n)_t,(n)_{t^2}\mid n\in\mathbb{N}_{\geq 2}\cup\{\infty\}\}.$$

(2) $\dim\mathfrak{B}_3(V)\leq \dim V\big(\dim\mathfrak{B}_2(V)-(1/3)((\dim V)^2-1)\big)$.
(3) $\dim\ker(1+c_{12}+c_{12}c_{23})\geq (1/3)\dim V((\dim V)^2-1)$.
(4) *The Yetter–Drinfeld module V appears in Tables 4 and 5.*

Remark 7. In the setting of Theorem 11, the rack X is indecomposable since G is generated by X and X is a conjugacy class of G.

Definition 4. Let V be a Yetter–Drinfeld module over a group algebra. We say that the Nichols algebra $\mathfrak{B}(V)$ *has many cubic relations* if the inequality in Theorem 11(3) is satisfied.

The difficult part of Theorem 11 is the implication (3)⇒(4). Its proof will occupy the remaining part of the paper. The other implications are elementary.

Proof. (1)⇒(2). Consider $\mathcal{H}_{\mathfrak{B}(V)}(t)$ in $\mathbb{Z}[\![t]\!]/(t^4)$. Then (1) implies that $\mathcal{H}_{\mathfrak{B}(V)}(t)$ is a product of polynomials $1+t$, $1+t+t^2$, $1+t+t^2+t^3$ and $1+t^2$. By replacing the factors $1+t+t^2$ by $1+t+t^2+t^3$ we may raise the coefficient of t^3 in $\mathcal{H}_{\mathfrak{B}(V)}(t)$ without changing the coefficients of 1, t, and t^2. Now replace the factors $1+t+t^2+t^3$ by $(1+t)(1+t^2)$. Thus there exist $n,a,b\in\mathbb{N}_0$ such that

$$\mathcal{H}_{\mathfrak{B}(V)}(t)=(1+t)^a(1+t^2)^b-nt^3+\text{ terms of degree}\geq 4. \tag{16}$$

Since $\mathfrak{B}_1(V)=V$, we conclude that $a=\dim V$. The coefficient of t^2 in $\mathcal{H}_{\mathfrak{B}(V)}(t)$ is $a(a-1)/2+b$ and the coefficient of t^3 is

$$\frac{a(a-1)(a-2)}{6}+ab-n=a\left(\frac{a(a-1)}{2}+b\right)-\frac{a(a^2-1)}{3}-n.$$

This implies the claim.

(2)⇒(3). Let $S_3=(1+c_{23})(1+c_{12}+c_{12}c_{23})\in\mathrm{End}_{\Bbbk}(V^{\otimes 3})$ denote the third quantum symmetrizer. By definition of $\mathfrak{B}_3(V)$ and by (2),

$$\begin{aligned}\dim\ker S_3&=(\dim V)^3-\dim\mathfrak{B}_3(V)\\&\geq\dim V\left(\dim\ker(1+c)+\frac{1}{3}((\dim V)^2-1)\right).\end{aligned}$$

On the other hand, by linear algebra we obtain that

$$\begin{aligned}(\dim V)\dim\ker(1+c)+\dim\ker(1+c_{12}+c_{12}c_{23})&\\ &=\dim\ker(1+c_{23})+\dim\ker(1+c_{12}+c_{12}c_{23})\\ &\geq \dim\ker(1+c_{23})(1+c_{12}+c_{12}c_{23})\\ &=\dim\ker S_3.\end{aligned}$$

The combination of these two inequalities yields the claim.

(4)⇒(1) The Hilbert series of $\mathfrak{B}(V)$ can be found in Table 4. For the old examples, $\mathcal{H}_{\mathfrak{B}(V)}(t)$ was already known. For the new examples, we calculate $\mathcal{H}_{\mathfrak{B}(V)}(t)$ in Propositions 32 and 36. □

Remark 8. The inequality

$$\dim\ker S_3 \leq (\dim V)\dim\ker(1+c)+\dim\ker(1+c_{12}+c_{12}c_{23})$$

used in the proof of (2)⇒(3) is in fact an equality for arbitrary braidings of finite-dimensional vector spaces, but we don't need this fact here.

Let G be a group, V a Yetter–Drinfeld module over $\Bbbk G$ and $X=\operatorname{supp}V$. For any Hurwitz orbit $\mathcal{O}\subseteq X^3$ let

$$V_{\mathcal{O}}^{\otimes 3}=\bigoplus_{(x,y,z)\in\mathcal{O}} V_x\otimes V_y\otimes V_z.$$

Since $V=\bigoplus_{g\in X}V_g$, we conclude that $V^{\otimes 3}=\bigoplus_{\mathcal{O}}V_{\mathcal{O}}^{\otimes 3}$, where $\mathcal{O}$ is running over all Hurwitz orbits. Further, each of $V_{\mathcal{O}}^{\otimes 3}$ is invariant under $1+c_{12}+c_{12}c_{23}$. Thus

$$\dim\ker(1+c_{12}+c_{12}c_{23})=\sum_{\mathcal{O}}\dim\ker(1+c_{12}+c_{12}c_{23})|_{V_{\mathcal{O}}^{\otimes 3}}. \tag{17}$$

The next proposition is one of our main tools to find a good estimate of the dimension of $\ker(1+c_{12}+c_{12}x_{23})$.

Proposition 12. *Let G be a group, V a non-zero finite-dimensional Yetter–Drinfeld module over $\Bbbk G$, $X=\operatorname{supp}V$ and $\mathcal{O}\subseteq X^3$ a Hurwitz orbit. Then*

$$\dim\ker(1+c_{12}+c_{12}c_{23})|_{V_{\mathcal{O}}^{\otimes 3}}\leq \operatorname{imm}_{\mathcal{O}}\dim V_{\mathcal{O}}^{\otimes 3}.$$

Proof. Let $\tau\in\ker(1+c_{12}+c_{12}c_{23})|_{V_{\mathcal{O}}^{\otimes 3}}$. Then for all $(x,y,z)\in\mathcal{O}$ there exist uniquely determined elements $\tau_{(x,y,z)}\in V_x\otimes V_y\otimes V_z$ such that $\tau=\sum_{\bar{x}\in\mathcal{O}}\tau_{\bar{x}}$. Since $\tau\in\ker(1+c_{12}+c_{12}c_{23})$, it follows that

$$\tau_{(x\triangleright(y\triangleright z),x,y)}+c_{12}\tau_{(x,y\triangleright z,y)}+c_{12}c_{23}(\tau_{(x,y,z)})=0$$

for all $(x,y,z)\in\mathcal{O}$. If two summands of such an expression vanish, then so does the third, since c_{12} and c_{23} are bijective. Now let $P\subseteq\mathcal{O}$ be a plague. If $\tau_{(x,y,z)}=0$ for all $(x,y,z)\in P$, then $\tau=0$ by the choice of P. Hence the rank of $1+c_{12}+c_{12}c_{23}|_{V_{\mathcal{O}}^{\otimes 3}}$ is bounded from below by $\dim V_{\mathcal{O}}^{\otimes 3}-\#P(\dim V_x)^3$, where $x\in X$, that is,

$$\dim\ker(1+c_{12}+c_{12}c_{23})|_{V_{\mathcal{O}}^{\otimes 3}}\leq\#P(\dim V_x)^3=\frac{\#P}{\#\mathcal{O}}\dim V_{\mathcal{O}}^{\otimes 3}=\operatorname{imm}_{\mathcal{O}}\dim V_{\mathcal{O}}^{\otimes 3}.$$

This proves the claim. □

Definition 5. Let G be a group, V a non-zero finite-dimensional Yetter–Drinfeld module over $\Bbbk G$, $X = \operatorname{supp} V$ and $\mathcal{O} \subseteq X^3$ a Hurwitz orbit. The pair $(V, \mathcal{O})$ is said to be *optimal with respect to* $1 + c_{12} + c_{12}c_{23} \in \operatorname{End}_\Bbbk(V_\mathcal{O}^{\otimes 3})$ if

$$\dim \ker(1 + c_{12} + c_{12}c_{23})|_{V_\mathcal{O}^{\otimes 3}} = \operatorname{imm}_\mathcal{O} \dim V_\mathcal{O}^{\otimes 3}.$$

2.2. Hurwitz orbits with one element

For the study of Nichols algebras over groups with many cubic relations, the Hurwitz orbits of size 1 and 8 will play a distinguished role. We start with a lemma to warm up and with the analysis of the 1-orbits.

Lemma 13. *Let G be a group, V a non-zero Yetter–Drinfeld module over $\Bbbk G$, and $X = \operatorname{supp} V$. Let $q \in \Bbbk \setminus \{0\}$, $x \in X$, and $\mathcal{O} = \mathcal{O}(x, x) \subseteq X^2$. Assume that $e = \dim V_x < \infty$ and that $xv = qv$ for all $v \in V_x$. Then* $\dim \ker(1 + c)$ *is the following:*

$$\begin{aligned} e(e+1)/2 &\quad \text{if } q = -1,\\ e(e-1)/2 &\quad \text{if } q = 1,\ \operatorname{char} \Bbbk \neq 2,\\ 0 &\quad \text{otherwise.} \end{aligned}$$

Proof. Let $v_1, v_2, \dots, v_e$ be a basis of V_x. For all $i, j \in \{1, \dots, e\}$ let $W_{ij} = \Bbbk(v_i \otimes v_j)$. Decompose $V_x \otimes V_x$ as

$$V_x \otimes V_x = \Big(\bigoplus_i W_{ii}\Big) \oplus \bigoplus_{i<j} (W_{ij} \oplus W_{ji}).$$

Then

$$(1 + c)|_{W_{ii}} = (1 + q)\mathrm{id}_{W_{ii}}$$

for all $i \in \{1, \dots, e\}$, and the matrix of $1+c$ with respect to the basis $(v_i \otimes v_j, v_j \otimes v_i)$ of $W_{ij} \bigoplus W_{ji}$ for $i \neq j$ is

$$\begin{pmatrix} 1 & q \\ q & 1 \end{pmatrix}.$$

This matrix has rank 1 if $q^2 = 1$ and rank 2 if $q^2 \neq 1$. Now the claim of the lemma follows by counting. □

Proposition 14. *Let G be a group, V a non-zero Yetter–Drinfeld module over $\Bbbk G$, and $X = \operatorname{supp} V$. Let $q \in \Bbbk \setminus \{0\}$, $x \in X$, and $\mathcal{O} = \mathcal{O}(x, x, x) \subseteq X^3$. Assume that $e = \dim V_x < \infty$ and that $xv = qv$ for all $v \in V_x$. Then* $\dim \ker(1+c_{12}+c_{12}c_{23})|_{V_\mathcal{O}^{\otimes 3}}$ *is the following:*

$$\begin{aligned} e(e^2+2)/3 &\quad \text{if } \operatorname{char} \Bbbk = 3,\ q = 1,\\ e(e^2-1)/3 &\quad \text{if } q = -1 \text{ or } \operatorname{char} \Bbbk \neq 3,\ q = 1,\\ e(e+1)(e+2)/6 &\quad \text{if } \operatorname{char} \Bbbk \neq 3,\ 1 + q + q^2 = 0,\\ e(e-1)(e-2)/6 &\quad \text{if } \operatorname{char} \Bbbk \neq 2, 3,\ 1 - q + q^2 = 0,\\ 0 &\quad \text{otherwise.} \end{aligned}$$

In particular, $\dim \ker(1 + c_{12} + c_{12}c_{23})|_{V_\mathcal{O}^{\otimes 3}} \leq e(e^2 + 2)/3$.

Proof. Let $v_1, v_2, \dots, v_e$ be a basis of V_x. For all $i,j,k \in \{1,\dots,e\}$ let $W_{ijk} = \Bbbk(v_i \otimes v_j \otimes v_k)$. Decompose $V_x \otimes V_x \otimes V_x$ as

$$V_x \otimes V_x \otimes V_x = \Big(\bigoplus_i W_{iii}\Big) \oplus \bigoplus_{i\neq j}(W_{iij} \oplus W_{iji} \oplus W_{jii}) \oplus \Big(\bigoplus_{i\neq j\neq k, i\neq k} W_{ijk}\Big).$$

Then

$$(1+c_{12}+c_{12}c_{23})(w_1 \otimes w_2 \otimes w_3) = w_1 \otimes w_2 \otimes w_3 + q w_2 \otimes w_1 \otimes w_3 + q^2 w_3 \otimes w_1 \otimes w_2$$

for all $w_1 \in V_i$, $w_2 \in V_j$ and $w_3 \in V_k$. In particular, if $1+q+q^2=0$, then $\dim\ker(1+c_{12}+c_{12}c_{23})|_{\bigoplus_i W_{iii}}$ is e, otherwise it is zero.

Assume that $e \geq 2$. Let $i,j \in \{1,\dots,e\}$ with $i \neq j$ and let $\lambda_1,\lambda_2,\lambda_3 \in \Bbbk$. Then

$$\begin{aligned}(1+c_{12}+c_{12}c_{23})&(\lambda_1 v_i \otimes v_i \otimes v_j + \lambda_2 v_i \otimes v_j \otimes v_i + \lambda_3 v_j \otimes v_i \otimes v_i)\\ &= (\lambda_1+\lambda_1 q+\lambda_2 q^2) v_i \otimes v_i \otimes v_j\\ &\quad + (\lambda_2+\lambda_3 q+\lambda_3 q^2) v_i \otimes v_j \otimes v_i + (\lambda_3+\lambda_2 q+\lambda_1 q^2) v_j \otimes v_i \otimes v_i.\end{aligned}$$

This expression is zero if and only if

$$0 = (1+q)\lambda_1 + q^2\lambda_2 = \lambda_2 + (q+q^2)\lambda_3 = q^2\lambda_1 + q\lambda_2 + \lambda_3.$$

Note that

$$\det\begin{pmatrix}1+q & q^2 & 0\\ 0 & 1 & q+q^2\\ q^2 & q & 1\end{pmatrix} = (1+q)^2(1-q)^2(1+q+q^2)$$

and the rank of this matrix is at least 2. Therefore if $(1+q)(1-q)(1+q+q^2)=0$, then the dimension of $\ker(1+c_{12}+c_{12}c_{23})$ restricted to $\bigoplus_{i\neq j}(W_{iij} \bigoplus W_{iji} \bigoplus W_{jii})$ is $e(e-1)$; otherwise it is zero.

Assume that $e \geq 3$. Let $i_1,i_2,i_3 \in \{1,\dots,e\}$ be pairwise different elements and for all $\sigma \in \mathbb{S}_3$ let $\lambda_\sigma \in \Bbbk$. Similarly to the previous calculation,

$$\sum_{\sigma\in\mathbb{S}_3} \lambda_\sigma v_{i_{\sigma(1)}} \otimes v_{i_{\sigma(2)}} \otimes v_{i_{\sigma(3)}} \in \ker(1+c_{12}+c_{12}c_{23})$$

if and only if $(\lambda_\sigma)_{\sigma\in\mathbb{S}_3} \in \ker A$, where

$$A = \begin{pmatrix}1 & 0 & q & q^2 & 0 & 0\\ 0 & 1 & 0 & 0 & q & q^2\\ q & q^2 & 1 & 0 & 0 & 0\\ 0 & 0 & 0 & 1 & q^2 & q\\ q^2 & q & 0 & 0 & 1 & 0\\ 0 & 0 & q^2 & q & 0 & 1\end{pmatrix}.$$

We obtain the following facts:

- $\det A = (q+1)^4(q-1)^4(q^2+q+1)(q^2-q+1)$,
- $\operatorname{rank} A = 4$ if and only if $q \in \{-1,1\}$,
- $\operatorname{rank} A = 5$ if and only if $(q^2+q+1)(q^2-q+1)=0$, $q^2 \neq 1$.

The claim of the proposition follows by summing up $\dim\ker(1+c_{12}+c_{12}c_{23})$ for different values of q. □

2.3. Hurwitz orbits with eight elements

The other important Hurwitz orbits for the proof of Theorem 11 are the orbits with 8 elements.

Proposition 15. *Let G be a group, V a non-zero Yetter–Drinfeld module over $\Bbbk G$, and $X = \operatorname{supp} V$. Let $x, y \in X$, $\mathcal{O} = \mathcal{O}(x,x,y) \subseteq X^3$, and $q \in \Bbbk \setminus \{0\}$. Assume that $x \triangleright (y \triangleright x) = y$, $x \neq y$, $e = \dim V_x < \infty$ and $xv = qv$ for all $v \in V_x$. Then $\dim V_{\mathcal{O}}^{\otimes 3} = 8e^3$.*

(1) *If $q = -1$ then $\dim \ker(1 + c_{12} + c_{12}c_{23})|_{V_{\mathcal{O}}^{\otimes 3}} \leq e^2(5e+1)/2$.*
(2) *If $q \neq -1$ then $\dim \ker(1 + c_{12} + c_{12}c_{23})|_{V_{\mathcal{O}}^{\otimes 3}} \leq e^2(5e-1)/2$.*

Proof. Let $z = x \triangleright y$ and $w = x \triangleright z$. Then $w \notin \{x, z\}$, $z \triangleright x = y$, $w \triangleright x = z$, $y \triangleright z = x$, $z \triangleright w = x$, and

$$\mathcal{O} = \{(x,x,y),(x,z,x),(w,x,x),(z,w,x),(z,z,w),(z,x,z),(y,z,z),(x,y,z)\}.$$

Since $x \triangleright (y \triangleright x) = y$, it follows that $\dim V_x = \dim V_y$ and $\dim V_{\mathcal{O}}^{\otimes 3} = 8e^3$. Any element $\tau \in V_{\mathcal{O}}^{\otimes 3}$ has the form

$$\tau = \tau_{xxy} + \tau_{xzx} + \tau_{wxx} + \tau_{zwx} + \tau_{zzw} + \tau_{zxz} + \tau_{yzz} + \tau_{xyz},$$

where $\tau_{ijk} \in V_i \otimes V_j \otimes V_k$ for all $i, j, k \in X$. Suppose that $\tau \in \ker(1 + c_{12} + c_{12}c_{23})|_{V_{\mathcal{O}}^{\otimes 3}}$. Applying $1 + c_{12} + c_{12}c_{13}$ to τ and considering summands of different degrees we obtain the following equations:

$$\begin{aligned}
&\tau_{xxy} + c_{12}(\tau_{xxy}) + c_{12}c_{23}(\tau_{xyz}) = 0, && \tau_{xzx} + c_{12}(\tau_{zwx}) + c_{12}c_{23}(\tau_{zxz}) = 0,\\
&\tau_{wxx} + c_{12}(\tau_{xzx}) + c_{12}c_{23}(\tau_{xxy}) = 0, && \tau_{zwx} + c_{12}(\tau_{wxx}) + c_{12}c_{23}(\tau_{wxx}) = 0,\\
&\tau_{zzw} + c_{12}(\tau_{zzw}) + c_{12}c_{23}(\tau_{zwx}) = 0, && \tau_{zxz} + c_{12}(\tau_{xyz}) + c_{12}c_{23}(\tau_{xzx}) = 0,\\
&\tau_{yzz} + c_{12}(\tau_{zxz}) + c_{12}c_{23}(\tau_{zzw}) = 0, && \tau_{xyz} + c_{12}(\tau_{yzz}) + c_{12}c_{23}(\tau_{yzz}) = 0.
\end{aligned}$$

This system of equations is equivalent to

$$\tau_{zwx} = -(c_{12}c_{23})^{-1}(1 + c_{12})(\tau_{zzw}), \tag{18}$$
$$\tau_{yzz} = -c_{12}(\tau_{zxz}) - c_{12}c_{23}(\tau_{zzw}), \tag{19}$$
$$\begin{aligned}\tau_{xyz} &= -c_{12}(\tau_{yzz}) - c_{12}c_{23}(\tau_{yzz})\\ &= c_{12}(1 + c_{23})c_{12}(\tau_{zxz}) + c_{12}(1 + c_{23})c_{12}c_{23}(\tau_{zzw}),\end{aligned} \tag{20}$$
$$\begin{aligned}\tau_{xzx} &= -(c_{12}c_{23})^{-1}(\tau_{zxz} + c_{12}(\tau_{xyz}))\\ &= -c_{23}^{-1}\left((c_{12}^{-1} + c_{12}^2 + c_{12}c_{23}c_{12})(\tau_{zxz}) + c_{12}(1 + c_{23})c_{12}c_{23}(\tau_{zzw})\right),\end{aligned} \tag{21}$$
$$\tau_{wxx} = -c_{12}(\tau_{xzx}) - c_{12}c_{23}(\tau_{xxy}), \tag{22}$$
$$0 = \tau_{xxy} + c_{12}(\tau_{xxy}) + c_{12}c_{23}(\tau_{xyz}), \tag{23}$$
$$0 = \tau_{xzx} + c_{12}(\tau_{zwx}) + c_{12}c_{23}(\tau_{zxz}), \tag{24}$$
$$0 = \tau_{zwx} + c_{12}(\tau_{wxx}) + c_{12}c_{23}(\tau_{wxx}). \tag{25}$$

Using equation (20), equation (23) is equivalent to

$$(1 + c_{12})(\tau_{xxy}) - c_{12}c_{23}c_{12}(1 + c_{23})(\tau_{yzz}) = 0. \tag{26}$$

Since $xv = qv$ for all $v \in V_x$, Lemma 13 yields that $\dim \ker(1+c)|_{V_x \otimes V_x} = e(e+1)/2$ if $q = -1$ and $\dim \ker(1+c)|_{V_x \otimes V_x} \leq e(e-1)/2$ if $q \neq -1$. This implies the claim.
□

Proposition 16. *Let $G, V, X, x, y, \mathcal{O}, q, e$ be as in Proposition 15. Let $v_x \in V_x \setminus \{0\}$, $v_y \in V_y \setminus \{0\}$. The following are equivalent.*

(1) *The pair $(V, \mathcal{O})$ is optimal with respect to $1 + c_{12} + c_{12}c_{23}$.*
(2) *$e = \dim V_x = 1$, $q = -1$ and $(1 + c^3)(v_x \otimes v_y) = 0$.*

Proof. We use the same notation as in the proof of Proposition 15. Since $\mathrm{imm}_{\mathcal{O}} = 3/8$, (1) holds if and only if equations (23)–(25) are satisfied for all tensors $\tau_{xxy} \in V_x \otimes V_x \otimes V_y$, $\tau_{zxz} \in V_z \otimes V_x \otimes V_z$ and $\tau_{zzw} \in V_z \otimes V_z \otimes V_w$, where τ_{zwx}, τ_{yzz}, τ_{xyz}, τ_{xzx}, τ_{wxx} are as in (18)–(22). By equation (19), equation (26) holds for all τ_{xxy}, τ_{zxz} and τ_{zzw} if and only if

$$(1 + c)(V_x \otimes V_x) = 0, \tag{27}$$

that is, $\dim V_x = 1$ and $q = -1$.

Assume now that equation (27) holds. Then $(1 + c)(V_u \otimes V_u) = 0$ for all $u \in X$. Hence (18)–(25) are equivalent to

$$\tau_{zwx} = 0, \quad \tau_{xyz} = 0, \tag{28}$$

$$\tau_{yzz} = -c_{12}(\tau_{zxz}) - c_{12}c_{23}(\tau_{zzw}), \tag{29}$$

$$\tau_{xzx} = -(c_{12}c_{23})^{-1}(\tau_{zxz}), \tag{30}$$

$$\tau_{wxx} = c_{12}(c_{12}c_{23})^{-1}(\tau_{zxz}) - c_{12}c_{23}(\tau_{xxy}), \tag{31}$$

$$0 = -(c_{12}c_{23})^{-1}(\tau_{zxz}) + c_{12}c_{23}(\tau_{zxz}). \tag{32}$$

Clearly, equation (32) is equivalent to

$$\tau_{zxz} = (c_{12}c_{23})^2(\tau_{zxz}) = c_{12}^2c_{23}c_{12}(\tau_{zxz}). \tag{33}$$

Since $c_{12}(\tau_{zxz}) \in V_y \otimes V_z \otimes V_z$, we conclude that $c_{23}c_{12}(\tau_{zxz}) = -\tau_{zxz}$ and hence equation (33) is equivalent to

$$c_{12}^{-1}(1 + c_{12}^3)\tau_{zxz} = 0.$$

Since $\dim V_x = 1$, this implies the equivalence claimed in the Proposition. □

Proposition 17. *Let G be a group, V a non-zero Yetter–Drinfeld module over $\Bbbk G$, and $X = \operatorname{supp} V$. Let $x, y \in X$, $\mathcal{O} = \mathcal{O}(x, x, y) \subseteq X^3$, $v_x \in V_x \setminus \{0\}$, $v_y \in V_y \setminus \{0\}$ and $q \in \Bbbk \setminus \{0, -1\}$. Assume that $x \triangleright (y \triangleright x) = y$, $x \neq y$, $\dim V_x = 1$ and $xv = qv$ for all $v \in V_x$. Then $\dim \ker(1 + c_{12} + c_{12}c_{23})|_{V_{\mathcal{O}}^{\otimes 3}} \leq 2$ and if equality holds then $(1 + c^3)(v_x \otimes v_y) = 0$.*

Proof. We use the same notation as in the proof of Proposition 15. Let $\tau \in \ker(1 + c_{12} + c_{12}c_{23})|_{V_{\mathcal{O}}^{\otimes 3}}$ as in the proof of Proposition 15. Since $\dim V_x = 1$ and $q \neq -1$, we conclude that

$$\tau_{xxy} = c_{12}c_{23}c_{12}(\tau_{yzz}) = -c_{12}c_{23}c_{12}^2(\tau_{zxz}) - c_{12}c_{23}c_{12}^2c_{23}(\tau_{zzw}),$$

where the first equation follows from (20) and (23) and the second from (19). Hence $\dim \ker(1 + c_{12} + c_{12}c_{23})|_{V_{\mathcal{O}}^{\otimes 3}} \leq 2$. Equation (24) implies that

$$0 = -c_{23}^{-1}c_{12}^{-1}(1 + c_{12}^3)(\tau_{zxz}) - c_{23}^{-1}c_{12}^{-1}(1 + c_{12}^3)c_{23}(1 + c_{12})(\tau_{zzw}). \tag{34}$$

Thus, if $\dim \ker(1 + c_{12} + c_{12}c_{23})|_{V_{\mathcal{O}}^{\otimes 3}} = 2$, then equation (34) holds for all τ_{zxz} and τ_{zzw}. This implies the claim. □

3. The inequality in the main theorem for braided racks

Let G be a group, $x \in G$, X the conjugacy class of x in G, and let $d \in \mathbb{N}$. Assume that X is a finite indecomposable braided rack of size d. Let V be a finite-dimensional Yetter–Drinfeld module over G with $\operatorname{supp} V = X$ and let $e = \dim V_x$. Let $q \in \Bbbk\setminus\{0\}$ and assume that $xv = qv$ for all $v \in V_x$. We collect properties which hold if $\mathfrak{B}(V)$ has many cubic relations. The number m was defined in equation (8).

Proposition 18. *Let $d_1, d_8 \in \mathbb{N}_0$. Assume that* $\dim\ker(1+c_{12}+c_{12}c_{23})|_{V_\mathcal{O}^{\otimes 3}} \le d_1$ *for all Hurwitz 1-orbits $\mathcal{O} \subseteq X^3$ and* $\dim\ker(1+c_{12}+c_{12}c_{23})|_{V_\mathcal{O}^{\otimes 3}} \le d_8$ *for all Hurwitz 8-orbits $\mathcal{O} \subseteq X^3$. If $\mathfrak{B}(V)$ has many cubic relations, then*

$$12k_3d_8 + 24d_1 - k_3^2 - 30k_3 + m - 8d^2(e^3-1) + 8(e-1) \ge 0. \tag{35}$$

Proof. Assume that $\mathfrak{B}(V)$ has many cubic relations. Proposition 12 implies that

$$\sum_{\mathcal{O}\mid\#\mathcal{O}\notin\{1,8\}} \operatorname{imm}_\mathcal{O} \dim V_\mathcal{O}^{\otimes 3} + \sum_{\mathcal{O}\mid\#\mathcal{O}\in\{1,8\}} \dim\ker(1+c_{12}+c_{12}c_{23})|_{V_\mathcal{O}^{\otimes 3}} \ge \frac{de((de)^2-1)}{3}.$$

Since the only Hurwitz orbits have sizes 1, 3, 6, 8, 9, 12, 16 and 24, we further obtain that

$$l_1^{(3)} + 3l_3^{(3)} + 6l_6^{(3)} + 8l_8^{(3)} + 9l_9^{(3)} + 12l_{12}^{(3)} + 16l_{16}^{(3)} + 24l_{24}^{(3)} = d^3. \tag{36}$$

Since X is braided, we also know that $k_2 = d - k_3 - 1$. Using Proposition 9 and the numbers $\operatorname{imm}_\mathcal{O}$ from Proposition 10, we conclude that the inequality in (35) holds. □

Lemma 19.

(1) *Let $d_1 = e(e^2-1)/3$ and $d_8 = e^2(5e+1)/2$. Then the inequality in* (35) *is equivalent to $ek_3^2 - em - 6k_3 \le 0$.*
(2) *Let $d_1 = e(e^2+2)/3$ and $d_8 = e^2(5e-1)/2$. Then the inequality in* (35) *is equivalent to $e^2k_3^2 - e^2m + 6ek_3 - 24 \le 0$.*

Proof. This follows by direct calculation. □

Proposition 20. *Assume that $\mathfrak{B}(V)$ has many cubic relations. Then $k_3 \le 6$. Further, if $e \ge 2$ then $k_3 \le 3$.*

Proof. Assume first that $q = -1$. Then we can set

$$d_1 = \frac{e(e^2-1)}{3}, \qquad d_8 = \frac{e^2(5e+1)}{2}$$

in Proposition 18 because of Propositions 14, 15. Thus, if $\mathfrak{B}(V)$ has many cubic relations, then Proposition 18 implies that the inequality in Lemma 19(1) holds. Hence

$$(ek_3-6)(k_3-1) + e(k_3-m) \le 6.$$

Since $e \ge 1$, $m \le k_3$ and $3|m$ by Remark 6, the latter inequality does not hold for $k_3 \ge 7$. Similarly, it does not hold if $k_3 \ge 4$, $e \ge 2$.

Assume now that $q \ne -1$. Then, as above, one obtains that the inequality in Lemma 19(2) holds. Since $m \le k_3$, it follows that $e^2k_3(k_3-1) + 6ek_3 - 24 \le 0$. Since $e \ge 1$, this does not happen for $k_3 > 3$. □

4. Braided racks of degree 2 and 3-transposition groups

4.1. 3-transposition groups

A set D of involutions in a group G is called a *set of* 3*-transpositions* if D is a union of conjugacy classes of G, G is generated by D and for each $x, y \in D$ the product xy has order 1, 2 or 3. In this case we say that the pair (G, D) is a 3*-transposition group.* For more information related to 3-transposition groups see [Asc97].

Example 7. Symmetric groups are 3-transposition groups, where the 3-transpositions are the transpositions.

Example 8. Let (G, D) be a 3-transposition group and $\pi : G \to H$ an epimorphism of groups. Then $(H, \pi(D))$ is a 3-transposition group.

All 3-transposition groups generated by at most four elements are classified in [HS95]. Let $F(k, d)$ be the largest 3-transposition group (G, D), where D has size d and G can be generated by k (and not less than k) elements in D.

Let (G, D) be a 3-transposition group and let $Y \subseteq D$ be a subset generating D as a rack. Let $\mathcal{G}(Y)$ be the graph with vertex set Y such that $x, y \in Y$ are adjacent in $\mathcal{G}(Y)$ if and only if $\operatorname{ord}(xy) = 3$.

Remark 9. The graph $\mathcal{G}(Y)$ is the complementary graph of the commuting graph of Y defined in [Asc97, Ch. 2].

One says that two 3-transposition groups (G_1, D_1) and (G_2, D_2) *have the same central type* if $G_1/Z(G_1) \simeq G_2/Z(G_2)$ as 3-transposition groups.

Theorem 21. *Let (G, D) be a 3-transposition group which is generated by a subset Y of D such that $\#Y \leq 3$ and $\mathcal{G}(Y)$ is connected. Then G has the same central type as one of the groups $F(1, 1) \simeq \mathbb{Z}_2$, $F(2, 3) \simeq \mathbb{S}_3$, $F(3, 6) \simeq \mathbb{S}_4$, $F(3, 9) \simeq \mathrm{SU}(3, 2)'$.*

Proof. This has been proved independently by several people; see, for example, [HS95, Theorem 1.1]. □

4.2. Graphs and racks of degree two

Lemma 22. *Let (G, D) be a 3-transposition group. Assume that D is an indecomposable rack. Let $Y \subseteq D$ be a minimal subset generating D as a rack. Then $\mathcal{G}(Y)$ is connected.*

Proof. Assume that $\mathcal{G}(Y)$ is not connected. Let $Y = Y_1 \sqcup Y_2$ be a decomposition into non-empty disjoint subsets such that $y_1 \triangleright y_2 = y_2$ for all $y_1 \in Y_1$, $y_2 \in Y_2$. Then $D = \langle Y \rangle = \langle Y_1 \rangle \cup \langle Y_2 \rangle$ is a decomposition of the rack D into the union of two subracks and by the minimality of Y we may assume that $Y_1 \cap \langle Y_2 \rangle = \varnothing$, $Y_2 \cap \langle Y_1 \rangle = \varnothing$. Then $\langle Y_1 \rangle \cap \langle Y_2 \rangle = \varnothing$, a contradiction to the indecomposability of D and to Lemma 1. □

4.3. Examples

Using the classification of 3-transposition groups generated by at most three elements given in Theorem 21, it is not difficult to produce examples of braided racks of degree two.

Example 9. The 3-transposition group $F(1, 1) \simeq \mathbb{Z}_2$ gives the braided rack of one element.

Example 10. Figure 3 gives the 3-transposition group $F(2,3) \simeq \mathbb{S}_3$. The conjugacy class of involutions of $\mathbb{S}_3$ gives a braided rack isomorphic to $\mathbb{D}_3$. In this case $k_3 = 2$ (see Table 1 at the end of this section) and $\overline{G}_X \simeq \mathbb{S}_3$.

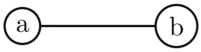

Figure 3: Diagram of type (ab)

Example 11. Figure 4 gives the 3-transposition group $F(3,6) \simeq \mathbb{S}_4$. The conjugacy class of transpositions of $\mathbb{S}_4$ gives a braided rack isomorphic to $\mathcal{A}$. In this case $k_3 = 4$ (see Table 1) and $\overline{G}_X \simeq \mathbb{S}_4$.

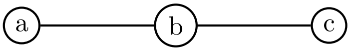

Figure 4: Diagram of type (abc)

Example 12. Figure 5 gives the 3-transposition group $F(3,9)$. A presentation for this group is given in [HS95]. The generators are a, b and c. The defining relations are

$$a^2 = b^2 = c^2 = (a^b c)^3 = 1,$$
$$aba = bab, \quad aca = cac, \quad bcb = cbc.$$

The group $F(3,9)$ has order 54 and it is isomorphic to $\mathrm{SU}(3,2)'$. The elements a, b, c belong to the same conjugacy class X. The conjugacy class X is a braided rack of 9 elements. As a rack, X is isomorphic to the affine rack $\mathrm{Aff}(\mathbb{F}_9, 2)$. Further, $k_3 = 8$.

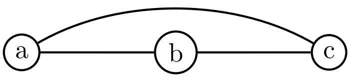

Figure 5: The diagram $(abca)$

Example 13. Figure 6 gives the 3-transposition group $F(4,10) \simeq \mathbb{S}_5$. The conjugacy class of transpositions of $\mathbb{S}_5$ gives a braided rack isomorphic to $\mathcal{C}$. In this case $k_3 = 6$ (see Table 1) and $\overline{G}_X \simeq \mathbb{S}_5$.

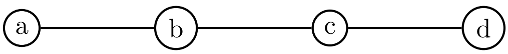

Figure 6: Diagram of type $(abcd)$

Example 14. Figure 7 gives the 3-transposition group $F(4,12)$. Following [HS95], the group $F(4,12)$ is defined by generators a, b, c, d and relations

$$a^2 = b^2 = c^2 = d^2,$$
$$aba = bab, \quad ada = dad, \quad aca = cac,$$
$$cb = bc, \quad cd = dc, \quad bd = db.$$

The group $F(4,12)$ has order 192. The elements a, b, c, d belong to the same conjugacy class X. The conjugacy class X is a braided rack of size 12 and $k_3 = 8$.

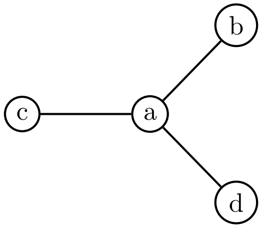

Figure 7: Diagram of type (cab, ad)

Let $\mathcal{GC}$ denote the category of pairs (G, D), where G is a group with trivial center, D is a conjugacy class of G generating G, and a morphism between pairs (G, D) and (H, E) is a group homomorphism $f : G \to H$ such that $f(D) = E$.

Proposition 23 ([AG03, Prop. 3.2])**.** *There is an equivalence of categories between the category of faithful indecomposable racks with surjective morphisms and the category $\mathcal{GC}$.*

Corollary 24. *There is an equivalence of categories between the category of braided indecomposable racks of degree two with surjective morphisms and the category of 3-transposition groups in $\mathcal{GC}$.*

Proof. Let Γ denote the equivalence in Proposition 23. Then a rack X has degree two if and only if D consists of involutions, where $\Gamma(X) = (G, D)$. Further, X is braided if and only if $\mathrm{ord}(xy) \in \{1, 2, 3\}$ for all $x, y \in D$. $\square$

Lemma 25. *Let X, X' be finite indecomposable braided racks such that $X \subsetneq X'$. Then $k_3(X) < k_3(X')$.*

Proof. Since X' is indecomposable, there exist $x \in X$, $y \in X' \setminus X$ such that $x \triangleright y \neq y$. Then $k_3(X') = \#\{z \in X' \mid x \triangleright z \neq z\} > \#\{z \in X \mid x \triangleright z \neq z\} = k_3(X)$. $\square$

Proposition 26. *Let X be a finite braided indecomposable rack of degree two with $k_3 \leq 6$. Then X is isomorphic to one of the racks $\mathbb{D}_3$, $\mathcal{A}$ and $\mathcal{C}$.*

Proof. First assume that the rack X is generated by at most three elements. By Theorem 21 and Corollary 24 we only have to check Examples 10, 11 and 12. In this case $X \simeq \mathbb{D}_3$ or $X \simeq \mathcal{A}$. Assume now that X is generated by a subset

$Y \subseteq X$ with $\#Y = 4$. By Lemma 22, the graph $\mathcal{G}(Y)$ is connected. If $\mathcal{G}(Y)$ contains a triangle, then $k_3(X) > 8$ by Lemma 25 and Example 12. If $\mathcal{G}(Y)$ is as in Example 14 then $k_3(X) > 6$. Hence $X \simeq \mathcal{C}$ by Example 13. Finally, if X is generated by more than four elements, then $k_3(X) > 6$ by Lemma 25. □

Table 1: Some braided racks of degree two

Rack	Diagram	Size	k_3	Reference
$\mathbb{D}_3$	(ab)	3	2	Example 10
$\mathcal{A}$	(abc)	6	4	Example 11
$\mathrm{Aff}(9,2)$	$(abca)$	9	8	Example 12
$\mathcal{C}$	$(abcd)$	10	6	Example 13

5. Braided racks of degree four

Proposition 27. *Let X be a finite braided indecomposable rack of degree 4 such that $k_3 \leq 6$. Then X is isomorphic to $\mathcal{B}$.*

Proof. Let $1, 2, \dots, \#X$ denote the elements of X. Since k_3 is the number of moved points of the permutation φ_1, the type of φ_1 is $(2,4)$ or (4).

Type $(2,4)$. Without loss of generality we may assume that

$$\varphi_1 = (2\,3)(4\,5\,6\,7).$$

Lemma 2 implies that $\varphi_2 = (1\,3)\pi_2$, where π_2 is a 4-cycle that commutes with $(1\,3)$. Similarly, $\varphi_3 = (1\,2)\pi_3$, where π_3 is a 4-cycle that commutes with $(1\,2)$. We prove that $2 \triangleright 4 \notin \{4,5,6,7,8\}$, which is a contradiction.

Assume that $2 \triangleright 4 = 4$. Then $1 \triangleright (2 \triangleright 5) = \varphi_2\varphi_1(2 \triangleright 4) = \varphi_2\varphi_1(4) = 2 \triangleright 5$. Let $8 = 2 \triangleright 5$ be this new element that commutes with 1. Then $8 = \varphi_1^2(2 \triangleright 5) = 2 \triangleright 7$, which is a contradiction.

Assume that $2 \triangleright 4 = 5$. Then $4 \triangleright 5 = 1$ and $4 \triangleright 5 = 2$ by Lemma 2, which is a contradiction.

Assume that $2 \triangleright 4 = 6$. Then $2 \triangleright 6 = \varphi_1^2(2 \triangleright 4) = \varphi_1^2(6) = 4$, which contradicts the type of φ_2.

Assume that $2 \triangleright 4 = 7$. Then $2 \triangleright 6 = \varphi_1^2(2 \triangleright 4) = \varphi_1^2(7) = 5$. We obtain that $\varphi_2 = (1\,3)(4\,7\,6\,5)$ and $\varphi_3 = (1\,2)(5\,4\,7\,6)$. Then $2 \triangleright 7 = 6$ implies that $6 \triangleright 2 = 7$ and $3 \triangleright 7 = 6$ implies that $6 \triangleright 3 = 7$, a contradiction.

Assume that $2 \triangleright 4 = 8$. Then $8 = \varphi_1^2(8) = \varphi_1^2(2 \triangleright 4) = 2 \triangleright 6$, which is a contradiction.

Type (4). Without loss of generality we may assume that

$$\varphi_1 = (2\,3\,4\,5).$$

Then $1 \triangleright 5 = 2$, $5 \triangleright 2 = 1$, and hence 5 and 2 do not commute. Let $x = 2 \triangleright 5$. Then Lemma 2 implies that $\varphi_2 = (3\,1\,5\,x)$, $\varphi_3 = (4\,1\,2\,\varphi_1(x))$, $\varphi_4 = (5\,1\,3\,\varphi_1^2(x))$ and $\varphi_5 = (2\,1\,4\,\varphi_1^3(x))$.

Assume that $2 \triangleright 5 = 4$. Then $3 \triangleright 2 = \varphi_1(2 \triangleright 5) = \varphi_1(4) = 5$ and hence $2 \triangleright 5 = 3$, a contradiction. Therefore $2 \triangleright 5 = 6$ and hence $\varphi_2 = (3\,1\,5\,6)$, $\varphi_3 = (4\,1\,2\,6)$, $\varphi_4 = (5\,1\,3\,6)$, $\varphi_5 = (2\,1\,4\,6)$ and $\varphi_6 = (2\,5\,4\,3)$. Therefore $X \simeq \mathcal{B}$, the rack associated to the conjugacy class of 4-cycles in $\mathbb{S}_4$. $\square$

6. Braided racks of degree three or six

Proposition 28. *Let X be a finite braided indecomposable rack of degree 3 such that $k_3 \leq 6$. Then X is isomorphic to the rack $\mathcal{T}$.*

Proof. Let $1, 2, \dots, \#X$ denote the elements of X. Since k_3 is the number of moved points of the permutation φ_1, the type of φ_1 is (3) or $(3, 3)$.

Type (3). Without loss of generality we may assume that

$$\varphi_1 = (2\,3\,4).$$

Lemma 2 implies that $\varphi_2 = (3\,1\,4)$, $\varphi_3 = (4\,1\,2)$ and $\varphi_4 = (1\,3\,2)$. Then $X \simeq \mathcal{T}$.

Type $(3, 3)$. Without loss of generality we may assume that

$$\varphi_1 = (2\,3\,4)(5\,6\,7).$$

Lemma 2 implies that φ_2 contains the 3-cycle $(3\,1\,4)$, φ_5 contains the 3-cycle $(6\,1\,7)$ and φ_7 contains the 3-cycle $(1\,6\,5)$.

If φ_2 contains the 2-cycle $(5\,6\,7)$ or $(5\,7\,6)$ then $2 \triangleright 5 \in \{6, 7\}$. However, $2 \triangleright 5 = 6$ and Lemma 2 imply that $1 = 5 \triangleright 6 = 2$, a contradiction. Similarly, $2 \triangleright 5 = 7$ and Lemma 2 imply that $6 = 5 \triangleright 7 = 2$, a contradiction.

Without loss of generality we may assume that $2 \triangleright 5 = 5$. Apply the permutation $\varphi_2\varphi_1$ to $2 \triangleright 5 = 5$ to obtain $1 \triangleright (2 \triangleright 6) = 2 \triangleright 6$. We may assume that $8 = 2 \triangleright 6$ and that $2 \triangleright 8 \in \{7, 9\}$.

Assume that $2 \triangleright 8 = 9$. Applying $\varphi_2\varphi_1$ we obtain that $1 \triangleright (2 \triangleright 8) = 2 \triangleright 9$, that is, $9 = 2 \triangleright 9$. This is a contradiction to $2 \triangleright 8 = 9$.

We have proved that $2 \triangleright 8 = 7$ and hence $\varphi_2 = (3\,1\,4)(6\,8\,7)$. Since $2 \triangleright 7 = 6$, Lemma 2 implies that $5 = 7 \triangleright 6 = 2$, a contradiction. $\square$

Proposition 29. *Let X be a finite braided indecomposable rack of degree 6 such that $k_3 \leq 6$. Then X is isomorphic to one of the racks* $\mathrm{Aff}(7, 3)$, $\mathrm{Aff}(7, 5)$.

Proof. Let $1, 2, \dots, \#X$ denote the elements of X. Since k_3 is the number of moved points of the permutation φ_1, the type of φ_1 is $(2, 3)$ or (6).

Type $(2, 3)$. Without loss of generality we may assume that

$$\varphi_1 = (2\,3)(4\,5\,6).$$

Lemma 2 implies that φ_2 contains the transposition $(1\,3)$ and φ_4 contains the 3-cycle $(1\,6\,5)$.

First we show that $2 \triangleright 4 = 4$. Indeed, the possible values for $2 \triangleright 4$ are 4, 5, 6 and 7. The case $2 \triangleright 4 = 7$ is excluded by the formula $\varphi_1^2(2 \triangleright 4) = 2 \triangleright 6$. The case $2 \triangleright 4 = 5$ contradicts Lemma 2 since $1 \triangleright 4 = 5$. If $2 \triangleright 4 = 6$, then Lemma 2 implies that $2 = 4 \triangleright 6 = 5$, a contradiction.

Since $2 \triangleright 4 = 4$, we obtain that $2 \triangleright 5 = \varphi_1^4(2 \triangleright 4) = \varphi_1^4(4) = 5$ and $2 \triangleright 6 = \varphi_1^2(2 \triangleright 4) = \varphi_1^2(4) = 6$. Since the permutation φ_2 is of type $(2,3)$, we may assume that $\varphi_2 = (1\,3)(7\,8\,9)$. Then $8 = 1 \triangleright 8 = \varphi_2\varphi_1(2 \triangleright 7) = \varphi_2\varphi_1(8) = 2 \triangleright 8$, which is a contradiction.

Type (6). Without loss of generality we may assume that

$$\varphi_1 = (2\,3\,4\,5\,6\,7).$$

Lemma 2 implies that $\varphi_2 = (3\,1\,7\,\cdots)$, $\varphi_3 = (4\,1\,2\,\cdots)$, $\varphi_4 = (5\,1\,3\,\cdots)$, $\varphi_5 = (6\,1\,4\,\cdots)$, $\varphi_6 = (7\,1\,5\,\cdots)$ and $\varphi_7 = (2\,1\,6\,\cdots)$. Since

$$7 = 2 \triangleright 1 = 2 \triangleright (3 \triangleright 4) = (2 \triangleright 3) \triangleright (2 \triangleright 4) = 1 \triangleright (2 \triangleright 4),$$

it follows that $2 \triangleright 4 = 6$. Moreover, $2 \triangleright 5 \neq 5$. Indeed, otherwise,

$$7 = 2 \triangleright 1 = 2 \triangleright (4 \triangleright 5) = (2 \triangleright 4) \triangleright (2 \triangleright 5) = 6 \triangleright 5 \neq 7,$$

a contradiction. Therefore $\varphi_2 \in \{(3\,1\,7\,4\,6\,5), (3\,1\,7\,5\,4\,6)\}$. By conjugation with φ_1 one obtains all permutations φ_i with $i \in \{3,4,5,6,7\}$. Since X is indecomposable, we conclude that $\#X = 7$.

Assume that $\varphi_2 = (3\,1\,7\,4\,6\,5)$. Then $\varphi_3 = (4\,1\,2\,5\,7\,6)$, $\varphi_4 = (5\,1\,3\,6\,2\,7)$, $\varphi_5 = (6\,1\,4\,7\,3\,2)$, $\varphi_6 = (7\,1\,5\,2\,4\,3)$ and $\varphi_7 = (2\,1\,6\,3\,5\,4)$. This rack is isomorphic to the affine rack $\mathrm{Aff}(7,5)$. On the other hand, if $\varphi_2 = (3\,1\,7\,5\,4\,6)$, then $\varphi_3 = (4\,1\,2\,6\,5\,7)$, $\varphi_4 = (5\,1\,3\,7\,6\,2)$, $\varphi_5 = (6\,1\,4\,2\,7\,3)$, $\varphi_6 = (7\,1\,5\,3\,2\,4)$ and $\varphi_7 = (2\,1\,6\,4\,3\,5)$. This rack is isomorphic to the affine rack $\mathrm{Aff}(7,3)$. □

7. The proof of Theorem 11

In this section we prove Theorem 11(3)⇒(4). If $\#X = 1$, then G is cyclic. Hence $\#X > 1$. Since X is indecomposable, Proposition 6 implies that the degree of X is 2, 3, 4, or 6. Further, $k_3 \leq 6$ by Proposition 20 and $k_3 \leq 3$ if the degree of ρ is at least 2. By Propositions 26, 27, 28 and 29 we only have to take care about the racks $X = \mathbb{D}_3$, $\mathcal{T}$, $\mathcal{A}$, $\mathcal{B}$, $\mathcal{C}$, $\mathrm{Aff}(7,3)$ and $\mathrm{Aff}(7,5)$. Each of these racks is considered in a separate subsection. Since G is generated by X, there is an epimorphism $G_X \to G$. Thus we may assume that $G = G_X$. The elements of X and their image in G_X will be denoted by $1, 2, \dots, \#X$ and $x_1, x_2, \dots, x_{\#X}$, respectively. Since any braided rack is faithful, the elements $x_1, \dots x_{\#X}$ are pairwise distinct.

During the proof some known and some new finite-dimensional Nichols algebras will appear. The Hilbert series of these algebras are collected in Table 4. The formulas for the known examples are taken from [GHV, Table 1].

7.1. The rack $\mathbb{D}_3$

Let $X = \{1,2,3\} = \mathbb{D}_3$. The size of X is $d = 3$. The rack structure of X is uniquely determined by $\varphi_1 = (2\,3)$.

Lemma 30 ([GHV, Lemma 5.2]). *The centralizer of x_1 in G_X is the cyclic group generated by x_1.*

Proposition 31. *Let ρ be an absolutely irreducible representation of $C_{G_X}(x_1)$ and let $V = M(x_1, \rho)$. Then $\mathfrak{B}(V)$ has many cubic relations if and only if $\rho(x_1) = -1$ or $\operatorname{char} \Bbbk = 2$, $\rho(x_1)^2 + \rho(x_1) + 1 = 0$.*

Remark 10. The Nichols algebra $\mathfrak{B}(V)$ in the case $\rho(x_1) = -1$ appeared first in [MS00]. Some data about $\mathfrak{B}(V)$ can be found in Table 4. The Nichols algebra $\mathfrak{B}(V)$ in the case $\operatorname{char} \Bbbk = 2$, $\rho(x_1)^2 + \rho(x_1) + 1 = 0$ is an unpublished example found by H.-J. Schneider and the first author. More details can be found in Proposition 32.

Proof. Assume first that $\rho(x_1) = -1$ or $\operatorname{char} \Bbbk = 2$, $\rho(x_1)^2 + \rho(x_1) + 1 = 0$. Then $\mathcal{H}_{\mathfrak{B}(V)}(t)$ is a product of polynomials $(n)_t$ and $(n)_{t^2}$ for some $n \in \mathbb{N}$; see Table 4. We conclude that $\mathfrak{B}(V)$ has many cubic relations by Theorem 11(4)⇒(3).

Assume that $\mathfrak{B}(V)$ has many cubic relations and $\rho(x_1) \neq -1$. By Lemma 30, the group $C_{G_X}(x_1)$ is abelian. Hence the degree of ρ is $e = 1$. Further, Proposition 15 implies that $\dim \ker(1 + c_{12} + c_{12}c_{23})|_{V_{\mathcal{O}}^{\otimes 3}} \leq 2$ for all orbits $\mathcal{O}$ of size 8, since $\rho(x_1) \neq -1$. If $\dim \ker(1 + c_{12} + c_{12}c_{23})|_{V_{\mathcal{O}}^{\otimes 3}} \leq 1$ for all orbits $\mathcal{O}$ of size 8, then Proposition 18 yields a contradiction, since $d = 3$, $m = 0$, $k_3 = 2$ and $d_1 \leq 1$. Since the three Hurwitz orbits of size 8 are conjugate, we conclude that $\dim \ker(1+c_{12}+c_{12}c_{23})|_{V_{\mathcal{O}}^{\otimes 3}} = 2$ for all orbits $\mathcal{O}$ of size 8. Proposition 17 implies that $(1+c_{12}^3)(v \otimes x_3 v) = 0$ for all $v \in V_{x_1}$. Then

$$
\begin{aligned}
0 = (1 + c_{12}^3)(v \otimes x_3 v) &= v \otimes x_3 v + x_2 x_1 x_3 v \otimes x_3 v \\
&= (v + x_2^2 x_1 v) \otimes x_3 v = 2v \otimes x_3 v
\end{aligned}
$$

since $x_1^2 = x_2^2$. Therefore $\operatorname{char} \Bbbk = 2$. If $\rho(x_1)^2 + \rho(x_1) + 1 \neq 0$, then Proposition 14 gives that $\dim \ker(1 + c_{12} + c_{12}c_{23})|_{V_{\mathcal{O}}^{\otimes 3}} = 0$ for all orbits $\mathcal{O}$ of size 1. Then Proposition 18 yields a contradiction. □

Now we discuss one of the Nichols algebras mentioned above. Assume that $\operatorname{char} \Bbbk = 2$ and that $\Bbbk$ contains an element $q \in \Bbbk$ with $q^2 + q + 1 = 0$. Recall that $X = \mathbb{D}_3$. Let ρ be the absolutely irreducible representation of $C_{G_X}(x_1)$ with $\rho(x_1) = q$. Let $V = M(x_1, \rho)$, $a \in V_{x_1} \setminus \{0\}$, $b = q^{-1} x_3 a$ and $c = q^{-1} x_1 b$. The action of G_X on V is then determined by Table 2.

Table 2: The action of G_X on V, where $X = \mathbb{D}_3$

	a	b	c
x_1	qa	qc	qb
x_2	qc	qb	qa
x_3	qb	qa	qc

Proposition 32. *The Nichols algebra $\mathfrak{B}(V)$ can be presented by generators a, b, c with defining relations*

$$ab + q^2 bc + qca = 0, \tag{37}$$

$$ac + q^2 cb + qba = 0, \tag{38}$$

$$a^3 = b^3 = c^3 = 0, \tag{39}$$

$$(a^2b^2)^3 + b(a^2b^2)^2 a^2 b + b^2 (a^2b^2)^2 a^2 + ab^2 (a^2b^2)^2 a = 0. \tag{40}$$

The Hilbert series of $\mathfrak{B}(V)$ *is*

$$\mathcal{H}_{\mathfrak{B}(V)}(t) = (3)_t(4)_t(6)_t(6)_{t^2}.$$

The dimension of $\mathfrak{B}(V)$ *is* 432. *The top degree of* $\mathfrak{B}(V)$ *is* 20. *An integral of* $\mathfrak{B}(V)$ *is given by*

$$a^2ba^2b(a^2b^2)^3c^2.$$

Proof. The relations in (37)–(40) “generate” a Hopf ideal of the tensor algebra $T(V)$. Using the theory of Gröbner bases [CK, GAP06], it can be seen that the quotient algebra has the stated dimensions in each degree. Using [AG03, Theorem 6.4, part (2)], it is sufficient to see that $a^2ba^2b(a^2b^2)^3c^2$ does not vanish in $\mathfrak{B}(V)$ in order to prove the claim. Direct calculation gives that

$$\partial_b\partial_b\partial_a\partial_a\partial_c\partial_c\partial_a\partial_a\partial_c\partial_c\partial_b\partial_b\partial_c\partial_b\partial_c\partial_b\partial_c\partial_b\partial_c\partial_c$$

applied to $a^2ba^2b(a^2b^2)^3c^2$ gives a non-zero number. This completes the proof. □

7.2. The rack $\mathcal{T}$

Let $X = \{1,2,3,4\} = \mathcal{T}$ and $d = 4$. Using that X is braided, the rack structure of X is uniquely determined by $\varphi_1 = (2\ 3\ 4)$. Note that $x_1 \triangleright x_2 = x_3$ in contrast to the convention $x_2 \triangleright x_1 = x_3$ in [GHV, §5.2]. Hence our group G_X is the opposite of the group G_X in [GHV, §5.2].

Lemma 33 ([GHV, Lemma 5.5])**.** *The centralizer of* x_1 *in* G_X *is abelian and is generated by* x_1 *and* x_2x_4*. Further, the relation* $(x_2x_4)^2 = x_1^4$ *holds in* G_X*.*

Lemma 34. *Let* $x, y, x', y' \in X$ *with* $x \neq y$ *and* $x' \neq y'$*. Then* $\mathcal{O}(x,x,y)$ *and* $\mathcal{O}(x',x',y')$ *are conjugate.*

Proof. By applying φ_1 we conclude that $\mathcal{O}(1,1,2)$ is conjugate to $\mathcal{O}(1,1,z)$ for all $z \in X \setminus \{1\}$. Since X is indecomposable, the claim follows. □

Proposition 35. *Let* ρ *be an absolutely irreducible representation of* $C_{G_X}(x_1)$ *and let* $V = M(x_1, \rho)$*. Then* $\mathfrak{B}(V)$ *has many cubic relations if and only if*

(1) $\rho(x_1) = -1$ *and* $\rho(x_2x_4) = 1$*, or*
(2) $\rho(x_1)^2 + \rho(x_1) + 1 = 0$ *and* $\rho(x_2x_4) = -\rho(x_1)^{-1}$*.*

Remark 11. The Nichols algebra $\mathfrak{B}(V)$ with ρ as in (1) appeared first in [AG03, Thm. 6.15]. For arbitrary fields the example was discussed in [GHV, Prop. 5.6]. Recall that $\mathfrak{B}(V)$ depends essentially on char $\Bbbk$.

The Nichols algebra $\mathfrak{B}(V)$ with ρ as in (2) is new. It will be discussed in Proposition 36.

Proof. Assume first that (1) or (2) hold. Then $\mathcal{H}_{\mathfrak{B}(V)}(t)$ is a product of polynomials $(n)_t$ and $(n)_{t^2}$ for some $n \in \mathbb{N}$; see Table 4. We conclude that $\mathfrak{B}(V)$ has many cubic relations by Theorem 11(4)⇒(3).

Assume that $\mathfrak{B}(V)$ has many cubic relations. By Lemma 33, the group $C_{G_X}(x_1)$ is abelian. Hence the degree of ρ is $e = 1$. Since $m = k_3 = 3$, Proposition 18 implies that $36d_8 + 24d_1 \geq 96$, where $d_1 \in \{0, 1\}$ and $d_8 \in \{0, 1, 2, 3\}$ by Proposition 15. Hence $d_8 = 3$, $d_1 \in \{0, 1\}$ or $d_8 = 2$, $d_1 = 1$.

Assume first that $\rho(x_1) = -1$. Then we can choose $d_1 = 0$ by Proposition 14. Since then $d_8 = 3$, there is at least one 8-orbit with immunity $3/8$. By Lemma 34, all Hurwitz orbits of size 8 are conjugate. Hence for each 8-orbit the pair $(V, \mathcal{O})$ is optimal with respect to $1 + c_{12} + c_{12}c_{23}$. Thus Proposition 16 implies that

$$\begin{aligned}0 = (1 + c_{12}^3)(v \otimes x_3 v) &= v \otimes x_3 v + x_2 x_1 x_3 v \otimes x_3 v \\ &= (v + x_2 x_4 x_1 v) \otimes x_3 v = (1 + \rho(x_2 x_4)\rho(x_1)) v \otimes x_3 v\end{aligned} \tag{41}$$

for all $v \in V_{x_1}$. Since $\rho(x_1) = -1$, it follows that $\rho(x_2 x_4) = 1$, that is, (1) holds.

Assume now that $\rho(x_1) \neq -1$. Then, by Proposition 16, the pair $(V, \mathcal{O})$ is not optimal with respect to $1 + c_{12} + c_{12}c_{23}$ for any 8-orbit $\mathcal{O}$. Hence $d_8 = 2$ and $d_1 = 1$. Proposition 14 and $d_1 = 1$ imply that $\rho(x_1)^2 + \rho(x_1) + 1 = 0$. By Lemma 34, all Hurwitz orbits of size 8 are conjugate. Hence $\dim \ker(1 + c_{12} + c_{12}c_{23})|_{V_{\mathcal{O}}^{\otimes 3}} = 2$ for all orbits $\mathcal{O}$ of size 8. Proposition 17 implies that (41) holds for all $v \in V_{x_1}$, that is, $\rho(x_2 x_4) = -\rho(x_1)^{-1}$. This proves the claim. □

Now we discuss the Nichols algebra corresponding to ρ in Proposition 35(2). Assume that $\Bbbk$ contains an element $q \in \Bbbk$ with $q^2 + q + 1 = 0$. Recall that $X = \mathcal{T}$. Let ρ be the absolutely irreducible representation of $C_{G_X}(x_1)$ with $\rho(x_1) = -1$, $\rho(x_4 x_2) = 1$. Let $V = M(x_1, \rho)$, $a \in V_{x_1} \setminus \{0\}$, $b = q^{-1} x_3 a \in V_{x_2}$, $c = q^{-1} x_4 a \in V_{x_3}$, $d = q^{-1} x_2 a \in V_{x_4}$. The action of G_X on V is then determined by Table 3.

Table 3: The action of G_X on V, where $X = \mathcal{T}$.

	a	b	c	d
x_1	qa	qc	qd	qb
x_2	qd	qb	$-qa$	$-qc$
x_3	qb	$-qd$	qc	$-qa$
x_4	qc	$-qa$	$-qb$	qd

Proposition 36. *The Nichols algebra $\mathfrak{B}(V)$ can be presented by generators a, b, c, d with defining relations*

$$a^3 = b^3 = c^3 = d^3 = 0, \tag{42}$$

$$-q^2 ab - qbc + ca = -q^2 ac - qcd + da = 0, \tag{43}$$

$$qad - q^2 ba + db = qbd + q^2 cb + dc = 0, \tag{44}$$

$$\begin{gathered}a^2bcb^2 + abcb^2a + bcb^2a^2 + cb^2a^2b + b^2a^2bc + ba^2bcb, \\ +bcba^2c + cbabac + cb^2aca = 0.\end{gathered} \tag{45}$$

The Hilbert series of $\mathfrak{B}(V)$ is

$$\mathcal{H}_{\mathfrak{B}(V)}(t) = (6)_t^4 (2)_{t^2}^2.$$

The dimension of $\mathfrak{B}(V)$ is 5184. The top degree of $\mathfrak{B}(V)$ is 24. An integral of $\mathfrak{B}(V)$ is given by

$$a^2ba^2ba^2b^2a^2cb^2a^2cb^2a^2d^2.$$

Proof. The relations in (42)–(45) “generate” a Hopf ideal of the tensor algebra $T(V)$. Using the theory of Gröbner bases [CK, GAP06], it can be seen that the quotient algebra has the stated dimensions in each degree. Using [AG03, Theorem 6.4 part (2)], it is sufficient to see that $a^2ba^2ba^2b^2a^2cb^2a^2cb^2a^2d^2$ does not vanish in $\mathfrak{B}(V)$ in order to prove the claim. Direct calculation gives that

$$\partial_c\partial_c\partial_d\partial_c\partial_c\partial_d\partial_c\partial_c\partial_d\partial_d\partial_c\partial_c\partial_b\partial_b\partial_d\partial_d\partial_b\partial_a\partial_d\partial_d\partial_a\partial_a\partial_b\partial_b$$

applied to $a^2ba^2ba^2b^2a^2cb^2a^2cb^2a^2d^2$ gives $-q^2$. This completes the proof. □

7.3. The rack $\mathcal{A}$

Let $X = \{1,2,3,4,5,6\} = \mathcal{A}$ and $d = \#X = 6$. Using that X is braided, the rack structure of X is uniquely determined by $\varphi_1 = (2\ 3)(5\ 6)$, $\varphi_2 = (1\ 3)(4\ 5)$.

Lemma 37 ([GHV, Lemma 5.8])**.** *The centralizer of x_1 in G_X is the abelian group generated by x_1 and x_4. These generators satisfy $x_1^2 = x_4^2$.*

Proposition 38. *Let ρ be an absolutely irreducible representation of $C_{G_X}(x_1)$ and let $V = M(x_1,\rho)$. Then $\mathfrak{B}(V)$ has many cubic relations if and only if $\rho(x_1) = -1$ and $\rho(x_4) \in \{-1,1\}$.*

Remark 12. The Nichols algebras $\mathfrak{B}(V)$ with $\rho(x_4) = -1$ and $\rho(x_4) = 1$ appeared first in [MS00, Example 6.4] and [FK99, Def. 2.1], respectively. These two Nichols algebras are twist equivalent; see [Ven]. Their Hilbert series are given in Table 4.

Proof. If $\rho(x_1) = -1$, then $\rho(x_4)^2 = \rho(x_1)^2 = 1$ and hence $\rho(x_4) \in \{-1,1\}$. Then $\mathfrak{B}(V)$ has many cubic relations by Theorem 11(4)⇒(3) and Table 4.

Assume that $\mathfrak{B}(V)$ has many cubic relations. By Lemma 37, the group $C_{G_X}(x_1)$ is abelian. Hence the degree of ρ is $e = 1$. Since $d = 6$, $k_3 = 4$ and $m = 0$, Proposition 18 implies that

$$24d_1 + 48d_8 \geq 136. \tag{46}$$

If $q \neq -1$, then we may set $d_8 < 3$ by Proposition 15. This is a contradiction to (46). Hence $\rho(x_1) = -1$ and the claim of the proposition follows. □

7.4. The rack $\mathcal{B}$

Let $X = \{1,2,\dots,6\} = \mathcal{B}$ and $d = \#X = 6$. Using that X is braided, the rack structure of X is uniquely determined by $\varphi_1 = (2\ 3\ 4\ 5)$, $\varphi_2 = (1\ 5\ 6\ 3)$.

Lemma 39. *[GHV, Lemma 5.10] The centralizer of x_1 in G_X is the abelian group generated by x_1 and x_6. These generators satisfy $x_1^4 = x_6^4$.*

Lemma 40. *Let $x,y,x',y' \in X$ with $x \triangleright y \neq y$ and $x' \triangleright y' \neq y'$. Then $\mathcal{O}(x,x,y)$ and $\mathcal{O}(x',x',y')$ are conjugate.*

Proof. By applying φ_1 we conclude that $\mathcal{O}(1,1,2)$ is conjugate to $\mathcal{O}(1,1,z)$ for all $z \in \{2,3,4,5\} = \{z' \in X \mid 1 \triangleright z' \neq z'\}$. Since X is indecomposable, the claim follows. □

Proposition 41. *Let ρ be an absolutely irreducible representation of $C_{G_X}(x_1)$ and let $V = M(x_1,\rho)$. Then $\mathfrak{B}(V)$ has many cubic relations if and only if $\rho(x_1) = \rho(x_6) = -1$.*

Remark 13. The Nichols algebras of Prop. 41 appeared first in [AG03, Thm. 6.12] over the complex numbers and in [GHV, Prop. 5.11] over arbitrary fields. The Hilbert series of $\mathfrak{B}(V)$ is given in Table 4.

Proof. If $\rho(x_1) = \rho(x_6) = -1$, then $\mathfrak{B}(V)$ has many cubic relations by Theorem 11(4)⇒(3) and Table 4.

Assume that $\mathfrak{B}(V)$ has many cubic relations. By Lemma 39, the group $C_{G_X}(x_1)$ is abelian. Hence the degree of ρ is $e = 1$. Let d_1, d_8 be as in Proposition 18. Since $d = 6$, $k_3 = 4$ and $m = 0$, Proposition 18 implies that (46) holds. If $q \neq -1$, then we may assume that $d_8 < 3$ by Proposition 15. This is a contradiction to (46). Hence $\rho(x_1) = -1$. Assume that $\rho(x_6) \neq -1$. Then

$$(1 + c_{12}^3)(v_1 \otimes v_2) \neq 0$$

for $v_1 \in V_{x_1} \setminus \{0\}$ and $v_2 = x_3 v_1 \in V_{x_2}$. Indeed, we obtain that

$$\begin{aligned}(1 + c_{12}^3)(v_1 \otimes v_2) &= v_1 \otimes x_3 v_1 + x_2 x_1 x_3 v_1 \otimes x_3 v_1 \\ &= (v_1 + x_6 x_1^2 v_1) \otimes x_3 v_1 = (v_1 + x_6 v_1) \otimes x_3 v_1.\end{aligned}$$

Since all Hurwitz orbits of size 8 are conjugate by Lemma 40, we again may assume that $d_8 < 3$ by Proposition 15. This yields a contradiction to (46). □

7.5. The rack $\mathcal{C}$

In order to avoid confusion, let $X = \{x_1, x_2, \dots, x_{10}\} = \mathcal{C}$. The size of X is $d = 10$. The rack X can be seen as the rack of transpositions in $\mathbb{S}_5$. We identify the elements of X with transpositions as follows: $x_1 = (1\,2)$, $x_2 = (2\,3)$, $x_3 = (1\,3)$, $x_4 = (2\,4)$, $x_5 = (1\,4)$, $x_6 = (2\,5)$, $x_7 = (1\,5)$, $x_8 = (3\,4)$, $x_9 = (3\,5)$, $x_{10} = (4\,5)$.

Lemma 42 ([GHV, Lemma 5.8])**.** *The centralizer of x_1 in G_X is the non-abelian subgroup generated by x_1, x_8, x_9. These generators satisfy $x_1^2 = x_8^2 = x_9^2$, $x_2 x_8 = x_8 x_2$, $x_2 x_9 = x_9 x_2$, $x_8 x_9 x_8 = x_9 x_8 x_9$.*

Proposition 43. *Let ρ be an absolutely irreducible representation of $C_{G_X}(x_1)$ and let $V = M(x_1, \rho)$. Then $\mathfrak{B}(V)$ has many cubic relations if and only if $\rho(x_1) = -1$ and $\rho(x_8) = \rho(x_9) = \pm 1$.*

Remark 14. The Nichols algebras of Proposition 43 appeared first in [FK99] for $\rho(x_8) = 1$ and in [Gra] for $\rho(x_8) = -1$. These two Nichols algebras are twist equivalent; see [Ven]. Their Hilbert series are given in Table 4 (see Appendix A).

Proof. If $\rho(x_1) = -1$ and $\rho(x_8) = \rho(x_9) = \pm 1$, then $\mathfrak{B}(V)$ has many cubic relations by Theorem 11(4)⇒(3) and Table 4.

Assume that $\mathfrak{B}(V)$ has many cubic relations. Since $k_3 = 6$, the argument at the beginning of Section 7 yields that $e = 1$. Let d_1, d_8 be as in Proposition 18. Since $d = 10$, $k_3 = 6$ and $m = 0$, Proposition 18 implies that

$$24 d_1 + 72 d_8 \geq 216. \tag{47}$$

If $q \neq -1$, then we may assume that $d_8 < 3$ by Proposition 15. This is a contradiction to (47). Hence $\rho(x_1) = -1$. Since $x_1^2 = x_8^2 = x_9^2$ and $x_8 x_9 x_8 = x_9 x_8 x_9$ by Lemma 42, we conclude that $\rho(x_8) = \rho(x_9) = \pm 1$. □

7.6. The racks Aff(7, 3) and Aff(7, 5)

Let $X = \mathrm{Aff}(7,3)$ or $X = \mathrm{Aff}(7,5)$ with $X = \{1,2,\dots,7\}$ and let $d = \#X = 7$.

Proposition 44. *Let ρ be an absolutely irreducible representation of $C_{G_X}(x_1)$ and let $V = M(x_1,\rho)$. Then $\mathfrak{B}(V)$ has many cubic relations if and only if $\rho(x_1) = -1$.*

Remark 15. The Nichols algebras with many cubic relations in Proposition 44 appeared first in [Gra] over $\mathbb{C}$ and over arbitrary fields in [GHV, Prop. 5.15]. The Hilbert series of $\mathfrak{B}(V)$ is given in Table 4.

Proof. If $\rho(x_1) = -1$ and $\rho(x_8) = \rho(x_9) = \pm 1$, then $\mathfrak{B}(V)$ has many cubic relations by Theorem 11(4)⇒(3) and Table 4.

Assume that $\mathfrak{B}(V)$ has many cubic relations. By [GHV, Lemma 5.14], the group $C_{G_X}(x_1)$ is cyclic and it is generated by x_1. Hence the degree of ρ is $e = 1$. Let d_1, d_8 be as in Proposition 18. Since $d = 7$, $k_3 = 6$ and $m = 0$, Proposition 18 implies that (47) holds. If $q \neq -1$, then we may assume that $d_8 < 3$ by Proposition 15. This is a contradiction to (47). Hence $\rho(x_1) = -1$. □

Appendix A. Braided racks and Nichols algebras

Tables 4, 5 and 6 contain data of finite-dimensional Nichols algebras over groups which have a non-trivial indecomposable braided rack as support.

Table 4: Finite-dimensional Nichols algebras

Rack	Rank	Dimension	Hilbert series	Remark
$\mathbb{D}_3$	3	12	$(2)_t^2(3)_t$	§7.1
$\mathbb{D}_3$	3	432	$(3)_t(4)_t(6)_t(6)_{t^2}$	Prop. 32, char $\Bbbk = 2$
$\mathcal{T}$	4	36	$(2)_t^2(3)_t^2$	§7.2, char $\Bbbk = 2$
$\mathcal{T}$	4	72	$(2)_t^2(3)_t(6)_t$	§7.2, char $\Bbbk \neq 2$
$\mathcal{T}$	4	5184	$(6)_t^4(2)_{t^2}^2$	Prop. 36
$\mathcal{A}$	6	576	$(2)_t^2(3)_t^2(4)_t^2$	§7.3
$\mathcal{B}$	6	576	$(2)_t^2(3)_t^2(4)_t^2$	§7.4
$\mathrm{Aff}(7,3)$	7	326592	$(6)_t^6(7)_t$	§7.6
$\mathrm{Aff}(7,5)$	7	326592	$(6)_t^6(7)_t$	§7.6
$\mathcal{C}$	10	8294400	$(4)_t^4(5)_t^2(6)_t^4$	§7.5

Table 5: Centralizers and characters

Rack	Generators of $C_{G_X}(x_1)$	Linear character ρ on $C_{G_X}(x_1)$
$\mathbb{D}_3$	x_1	$\rho(x_1) = -1$
$\mathbb{D}_3$	x_1	char $\Bbbk = 2$, $\rho(x_1)^2 + \rho(x_1) + 1 = 0$
$\mathcal{T}$	$x_1,\ x_4x_2$	$\rho(x_1) = -1,\ \rho(x_4x_2) = 1$
$\mathcal{T}$	$x_1,\ x_4x_2$	$\rho(x_1)^2 + \rho(x_1) + 1 = 0,\ \rho(x_4x_2x_1) = -1$
$\mathcal{A}$	$x_1,\ x_4$	$\rho(x_1) = -1,\ \rho(x_4) = \pm 1$
$\mathcal{B}$	$x_1,\ x_6$	$\rho(x_1) = \rho(x_6) = -1$
$\mathrm{Aff}(7,3)$	x_1	$\rho(x_1) = -1$
$\mathrm{Aff}(7,5)$	x_1	$\rho(x_1) = -1$
$\mathcal{C}$	$x_1,\ x_8,\ x_9$	$\rho(x_1) = -1,\ \rho(x_8) = \rho(x_9) = \pm 1$

Table 6: Indecomposable braided racks occuring with Nichols algebras with many cubic relations.

Rack	deg	size	k_3	m	Reference
$\mathbb{D}_3$	2	3	2	0	Example 10
$\mathcal{T}$	3	4	3	3	Prop. 28
$\mathcal{A}$	2	6	4	0	Example 11
$\mathcal{B}$	4	6	4	0	Prop. 27
$\mathcal{C}$	2	10	6	0	Example 13
$\mathrm{Aff}(7,3)$	6	7	6	0	Prop. 29
$\mathrm{Aff}(7,5)$	6	7	6	0	Prop. 29

Appendix B. Hurwitz orbits of braided racks

With Figures 8–14 we present the isomorphism classes of nontrivial Hurwitz orbits of braided racks. There are nontrivial Hurwitz orbits of size 3, 6, 8, 9, 12, 16 and 24.

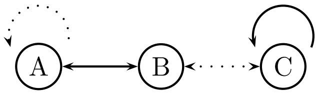

Figure 8: The Hurwitz orbit of size 3

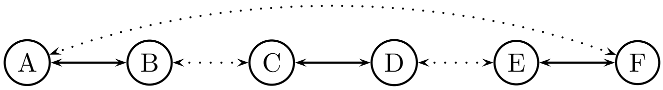

Figure 9: The Hurwitz orbit of size 6

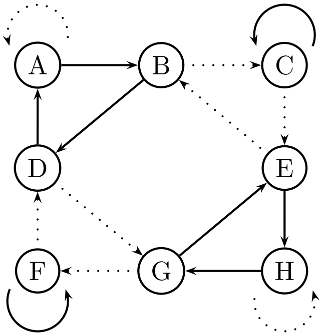

Figure 10: The Hurwitz orbit of size 8

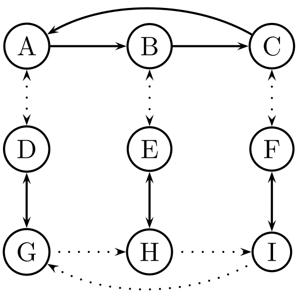

Figure 11: The Hurwitz orbit of size 9

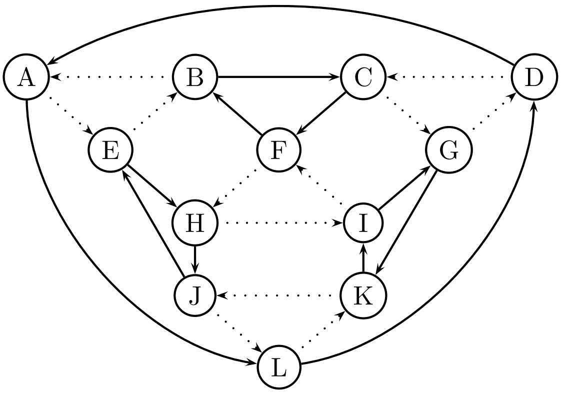

Figure 12: The Hurwitz orbit of size 12

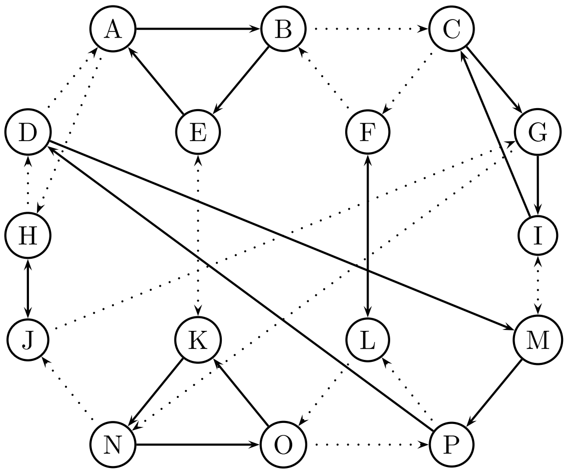

Figure 13: The Hurwitz orbit of size 16

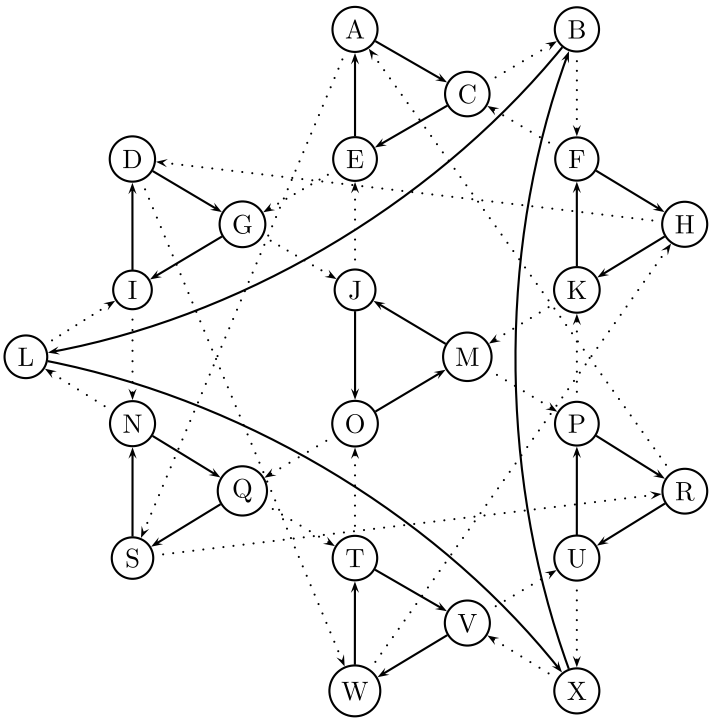

Figure 14: The Hurwitz orbit of size 24

References

[ABM10] A. Ardizzoni, M. Beattie, C. Menini, *Cocycle deformations for Hopf algebras with a coalgebra projection*, J. Algebra **324** (2010), no. 4, 673–705.

[AFGVa] N. Andruskiewitsch, F. Fantino, G. A. Garcia, L. Vendramin, *On Nichols algebras associated to simple racks*, Contemp. Math. **537** (2011) 31–56.

[AFGVb] N. Andruskiewitsch, F. Fantino, M. Graña, L. Vendramin, *Finite-dimensional pointed Hopf algebras with alternating groups are trivial*, Ann. Mat. Pura Appl. (4) **190** (2011), no. 2, 225–245.

[AFGV11] N. Andruskiewitsch, F. Fantino, M. Graña, L. Vendramin, *Pointed Hopf algebras over the sporadic simple groups*, J. Algebra **325** (2011), no. 1, 305–320.

[AG03] N. Andruskiewitsch, M. Graña, *From racks to pointed Hopf algebras*, Adv. Math. **178** (2003), no. 2, 177–243.

[AH73] M. Aschbacher, M. Hall, Jr., *Groups generated by a class of elements of order* 3, J. Algebra **24** (1973), 591–612.

[AHS10] N. Andruskiewitsch, I. Heckenberger, H.-J. Schneider, *The Nichols algebra of a semisimple Yetter–Drinfeld module*, Amer. J. Math. **132** (2010), no. 6, 1493–1547.

[And02] N. Andruskiewitsch, *About finite dimensional Hopf algebras*, in: *Quantum Symmetries in Theoretical Physics and Mathematics* (Bariloche, 2000), Contemp. Math., Vol. 294, Amer. Math. Soc., Providence, RI, 2002, pp. 1–57.

[Ang] I. Angiono, *A presentation by generators and relations of Nichols algebras of diagonal type and convex orders on root systems*, preprint: `arXiv:1008.4144`.

[Ang09] I. Angiono, *Nichols algebras with standard braiding*, Algebra Number Theory **3** (2009), no. 1, 35–106.

[ARS10] N. Andruskiewitsch, D. Radford, H.-J. Schneider, *Complete reducibility theorems for modules over pointed Hopf algebras*, J. Algebra **324** (2010), no. 11, 2932–2970.

[AS98] N. Andruskiewitsch, H.-J. Schneider, *Lifting of quantum linear spaces and pointed Hopf algebras of order* p^3, J. Algebra **209** (1998), no. 2, 658–691.

[AS00] N. Andruskiewitsch, H.-J. Schneider, *Finite quantum groups and Cartan matrices*, Adv. Math. **154** (2000), no. 1, 1–45.

[AS02] N. Andruskiewitsch, H.-J. Schneider, *Pointed Hopf algebras*, in: *New Directions in Hopf Algebras*, Math. Sci. Res. Inst. Publ., Vol. 43, Cambridge Univ. Press, Cambridge, 2002, pp. 1–68.

[AS10] N. Andruskiewitsch, H.-J. Schneider, *On the classification of finite-dimensional pointed Hopf algebras*, Ann. of Math. (2) **171** (2010), no. 1, 375–417.

[Asc97] M. Aschbacher, 3-*Transposition Groups*, Cambridge Tracts in Mathematics, Vol. 124, Cambridge University Press, Cambridge, 1997.

[Baz06] Y. Bazlov, *Nichols–Woronowicz algebra model for Schubert calculus on Coxeter groups*, J. Algebra **297** (2006), no. 2, 372–399.

[BBJW10] P. Balister, B. Bollobás, J. R. Johnson, M. Walters, *Random majority percolation*, Random Structures Algorithms **36** (2010), no. 3, 315–340.

[BDR02] M. Beattie, S. Dăscălescu, Ş. Raianu, *Lifting of Nichols algebras of type* B_2, Israel J. Math. **132** (2002), 1–28. With an appendix by the authors and I. Rutherford.

[Bri88] E. Brieskorn, *Automorphic sets and braids and singularities*, in: *Braids* (Santa Cruz, CA, 1986), Contemp. Math., Vol. 78, Amer. Math. Soc., Providence, RI, 1988, pp. 45–115.

[CJK+03] J. S. Carter, D. Jelsovsky, S. Kamada, L. Langford, M. Saito, *Quandle cohomology and state-sum invariants of knotted curves and surfaces*, Trans. Amer. Math. Soc. **355** (2003), no. 10, 3947–3989.

[CK] A. M. Cohen, J.W. Knopper, *GBNP, A GAP Package for Gröbner Bases of Noncommutative Polynomials*, available at `http://dam02.win.tue.nl/products/gbnp/`.

[Cox59] H. Coxeter, *Factor groups of the braid group*, Proc. of the Fourth Can. Math. Congress, Banff 1957, University of Toronto Press, 1959, pp. 95–122.

[Did05] D. Didt, *Pointed Hopf algebras and quasi-isomorphisms*, Algebr. Represent. Theory **8** (2005), no. 3, 347–362. MR 2176141 (2006g:16084)

[Fis71] B. Fischer, *Finite groups generated by 3-transpositions.* I, Invent. Math. **13** (1971), 232–246.

[FK99] S. Fomin, A. N. Kirillov, *Quadratic algebras, Dunkl elements, and Schubert calculus*, in: *Advances in Geometry*, Progr. Math., Vol. 172, Birkhäuser Boston, Boston, MA, 1999, pp. 147–182.

[Gab03] M. R. Gaberdiel, *An algebraic approach to logarithmic conformal field theory*, in: *Proceedings of the School and Workshop on Logarithmic Conformal Field Theory and its Applications* (Tehran, 2001), Vol. 18, 2003, pp. 4593–4638.

[GAP06] *The GAP Group*, 2006, GAP — Groups, Algorithms, and Programming, Version 4.4.12, available at `http://www.gap-system.org`.

[GG] G. A. García, A. García Iglesias, *Finite dimensional pointed Hopf algebras over* S_4, Israel J. Math. **183** (2011), 417–444.

[GH07] M. Graña, I. Heckenberger, *On a factorization of graded Hopf algebras using Lyndon words*, J. Algebra **314** (2007), no. 1, 324–343.

[GHV] M. Graña, I. Heckenberger, L. Vendramin, *Nichols algebras of group type with many quadratic relations*, Adv. Math. **227** (2011), no. 5, 1956–1989.

[Gra] M. Graña, *Nichols algebras of nonabelian group type, zoo of examples*, available at `http://mate.dm.uba.ar/~matiasg/zoo.html`.

[Gra02] M. Graña, *Quandle knot invariants are quantum knot invariants*, J. Knot Theory Ramifications **11** (2002), no. 5, 673–681.

[Hec06] I. Heckenberger, *The Weyl groupoid of a Nichols algebra of diagonal type*, Invent. Math. **164** (2006), no. 1, 175–188.

[Hec09] I. Heckenberger, *Classification of arithmetic root systems*, Adv. Math. **220** (2009), no. 1, 59–124.

[HS] I. Heckenberger, H.-J. Schneider, *Right coideal subalgebras of Nichols algebras and the Duflo order on the Weyl groupoid*, preprint: `arXiv:0909.0293`.

[HS10] I. Heckenberger, H.-J. Schneider, *Root systems and Weyl groupoids for Nichols algebras*, Proc. Lond. Math. Soc. (3) **101** (2010), no. 3, 623–654.

[HS95] J. I. Hall, L. H. Soicher, *Presentations of some* 3*-transposition groups*, Comm. Algebra **23** (1995), no. 7, 2517–2559.

[Hur91] A. Hurwitz, *Ueber Riemann'sche Flächen mit gegebenen Verzweigungspunkten*, Math. Ann. **39** (1891), no. 1, 1–60.

[Kha99] V. K. Kharchenko, *A quantum analogue of the Poincaré–Birkhoff–Witt theorem*, Algebra and Logic **38** (1999), no. 4, 259–276.

[KM10] A. N. Kirillov, T. Maeno, *Nichols–Woronowicz model of coinvariant algebra of complex reflection groups*, J. Pure Appl. Algebra **214** (2010), no. 4, 402–409.

[KR09] L. Krop, D. E. Radford, *Representations of pointed Hopf algebras and their Drinfel'd quantum doubles*, J. Algebra **321** (2009), no. 9, 2567–2603.

[KRT97] C. Kassel, M. Rosso, V. Turaev, *Quantum groups and knot invariants*, in: *Panoramas et Synthèses* [*Panoramas and Syntheses*], Vol. 5, Société Mathématique de France, Paris, 1997.

[KS97] A. Klimyk, K. Schmüdgen, *Quantum Groups and Their Representations*, Texts and Monographs in Physics, Springer-Verlag, Berlin, 1997.

[Maj05] S. Majid, *Noncommutative differentials and Yang-Mills on permutation groups S_n*, in: *Hopf Algebras in Noncommutative Geometry and Physics*, Lecture Notes in Pure and Appl. Math., Vol. 239, Dekker, New York, 2005, pp. 189–213.

[Mas] A. Masuoka, *Hopf ideals of the generalized quantum double associated to skew-paired Nichols algebras*, preprint: `arXiv:0911.2282`.

[MK99] K. Murasugi, B. I. Kurpita, *A Study of Braids*, Mathematics and its Applications, Vol. 484, Kluwer Academic Publishers, Dordrecht, 1999.

[Mom10] M. Mombelli, *Module categories over pointed Hopf algebras*, Math. Z. **266** (2010), no. 2, 319–344.

[MPSW] M. Mastnak, J. Pevtsova, P. Schauenburg, S. Witherspoon, *Cohomology of finite dimensional pointed Hopf algebras*, Proc. Lond. Math. Soc. (3) **100** (2010), no. 2, 377–404.

[MS00] A. Milinski, H.-J. Schneider, *Pointed indecomposable Hopf algebras over Coxeter groups*, in: *New Trends in Hopf algebra Theory* (La Falda, 1999), Contemp. Math., Vol. 267, Amer. Math. Soc., Providence, RI, 2000, pp. 215–236.

[Nic78] W. D. Nichols, *Bialgebras of type one*, Comm. Algebra **6** (1978), no. 15, 1521–1552.

[Ros98] M. Rosso, *Quantum groups and quantum shuffles*, Invent. Math. **133** (1998), no. 2, 399–416.

[Sch96] P. Schauenburg, *A characterization of the Borel-like subalgebras of quantum enveloping algebras*, Comm. Algebra **24** (1996), no. 9, 2811–2823.

[ST] A. Semikhatov, I. Tipunin, *The Nichols algebra of screenings*, preprint: `arXiv:1101.5810`.

[STBT10] F. Sausset, C. Toninelli, G. Biroli, G. Tarjus, *Bootstrap percolation and kinetically constrained models on hyperbolic lattices*, J. Stat. Phys. **138** (2010), nos. 1–3, 411–430.

[Ven] L. Vendramin, *Nichols algebras associated to the transpositions of the symmetric group are twist-equivalent*, accepted for publication in Proc. Amer. Math. Soc.

[Wor89] S. L. Woronowicz, *Differential calculus on compact matrix pseudogroups (quantum groups)*, Comm. Math. Phys. **122** (1989), no. 1, 125–170.