Annali di Matematica (2011) 190:225–245
DOI 10.1007/s10231-010-0147-0

Finite-dimensional pointed Hopf algebras with alternating groups are trivial

N. Andruskiewitsch · F. Fantino · M. Graña · L. Vendramin

Received: 18 March 2010 / Accepted: 7 May 2010 / Published online: 23 May 2010

Abstract It is shown that Nichols algebras over alternating groups $\mathbb{A}_m$ ($m \geq 5$) are infinite dimensional. This proves that any complex finite dimensional pointed Hopf algebra with group of group-likes isomorphic to $\mathbb{A}_m$ is isomorphic to the group algebra. In a similar fashion, it is shown that the Nichols algebras over the symmetric groups $\mathbb{S}_m$ are all infinite-dimensional, except maybe those related to the transpositions considered in Fomin and Kirillov (Progr Math 172:146–182, 1999), and the class of type $(2, 3)$ in $\mathbb{S}_5$. We also show that any simple rack X arising from a symmetric group, with the exception of a small list, collapse, in the sense that the Nichols algebra $\mathfrak{B}(X, \mathbf{q})$ is infinite dimensional, $\mathbf{q}$ an arbitrary cocycle.

Keywords Pointed Hopf algebras · Nichols algebras · Racks

Mathematics Subject Classification (2000) 16W30 · 17B37

This work was partially supported by ANPCyT-Foncyt, CONICET, Ministerio de Ciencia y Tecnología (Córdoba) and Secyt (UNC).

N. Andruskiewitsch · F. Fantino
Facultad de Matemática, Astronomía y Física, Universidad Nacional de Córdoba. CIEM, CONICET, Medina Allende s/n, Ciudad Universitaria, 5000 Córdoba, Argentina
e-mail: andrus@famaf.unc.edu.ar

F. Fantino
e-mail: fantino@famaf.unc.edu.ar

M. Graña · L. Vendramin
Departamento de Matemática, FCEyN, Universidad de Buenos Aires, Pab. I, Ciudad Universitaria, 1428 Buenos Aires, Argentina
e-mail: matiasg@dm.uba.ar

L. Vendramin (✉)
Instituto de Ciencias, Universidad de Gral. Sarmiento, J.M. Gutierrez 1150, Los Polvorines, 1653 Buenos Aires, Argentina
e-mail: lvendramin@dm.uba.ar

1 Introduction

1.1. In the early 90's, S. Montgomery raised the question of finding a non-trivial finite-dimensional complex pointed Hopf algebra H with non-abelian group G; here "non-trivial" means that H is neither a group algebra, nor is cooked out of a pointed Hopf algebra with abelian group by some kind of extension. This question was addressed by A. Milinski and H.-J. Schneider around 1995, who produced two examples, one with $G = \mathbb{S}_3$, another with $G = \mathbb{S}_4$. The main point was to check that a quadratic algebra $\mathfrak{B}_m$ built from the conjugacy class of transpositions in $\mathbb{S}_m$ is finite-dimensional. They were able to do it for $m = 3, 4$ using Gröbner bases. These results were published later in [27]. Independently, S. Fomin and K. N. Kirillov considered closely related quadratic algebras $\mathcal{E}_m$, also constructed from the transpositions in $\mathbb{S}_m$, and they determined the dimensions of $\mathcal{E}_3$, $\mathcal{E}_4$ and $\mathcal{E}_5$ [14]. With the introduction of the Lifting method, see [9], it became clear that $\mathfrak{B}_m$ and $\mathcal{E}_m$ should be Nichols algebras. This was indeed checked in [27] for $m = 3, 4$ and by the third named author for $m = 5$ [19].

1.2. In this paper, we work over the field $\mathbb{C}$ of complex numbers. If G denotes a finite group, to classify all complex pointed Hopf algebras H with group of group-likes $G(H) \simeq G$ and $\dim H < \infty$, we need to determine the irreducible Yetter-Drinfeld modules over $\mathbb{C}G$ such that the dimension of the corresponding Nichols algebras is finite. In other words, recalling that irreducible Yetter-Drinfeld modules are parameterized by pairs $(\mathcal{O}, \rho)$–$\mathcal{O}$ a conjugacy class of G, $\sigma \in \mathcal{O}$ fixed, ρ an irreducible representation of the centralizer $C_G(\sigma)$—and denoting by $\mathfrak{B}(\mathcal{O}, \rho)$ the associated Nichols algebra, we need to know for which pairs $(\mathcal{O}, \rho)$ is $\dim \mathfrak{B}(\mathcal{O}, \rho) < \infty$. Assume that $G = \mathbb{S}_m$. Then $\mathfrak{B}_m$ and $\mathcal{E}_m$ correspond to $\mathcal{O} = \mathcal{O}_2^m$, the conjugacy class of the transpositions, and ρ the one-dimensional representations of the centralizer $\simeq \mathbb{S}_{m-2} \times \mathbb{S}_2$, $\rho = \epsilon \otimes \operatorname{sgn}$ or $\rho = \operatorname{sgn} \otimes \operatorname{sgn}$ respectively. If $m \geq 6$, it is still open whether:

- $\mathfrak{B}_m$ and $\mathcal{E}_m$ are Nichols algebras,
- the dimensions of $\mathfrak{B}_m$ and $\mathcal{E}_m$ are finite,
- the dimensions of $\mathfrak{B}(\mathcal{O}_2^m, \operatorname{sgn}^j \otimes \operatorname{sgn})$, $j = 1, 2$ are finite.

1.3. Recently, there was some progress on pointed Hopf algebras over $\mathbb{S}_m$:

- The classification of the finite-dimensional Nichols algebras over $\mathbb{S}_3$, respectively, $\mathbb{S}_4$, is concluded in [7].
- The classification of finite-dimensional pointed Hopf algebras with group $\mathbb{S}_3$, respectively, $\mathbb{S}_4$, is concluded in [7], resp. [20].
- Most of the Nichols algebras $\mathfrak{B}(\mathcal{O}, \rho)$ over $\mathbb{S}_m$ have infinite dimension, with the exception of a short list of open possibilities [1,5].

Our first main result adjusts drastically the list given in [5, Th. 1]. See §4.1 for the unexplained notation.

Theorem 1.1 *Let $m \geq 5$. Let $\sigma \in \mathbb{S}_m$ be of type $(1^{n_1}, 2^{n_2}, \dots, m^{n_m})$, let $\mathcal{O}$ be the conjugacy class of σ and let $\rho = (\rho, V) \in \widehat{C_{\mathbb{S}_m}(\sigma)}$. If $\dim \mathfrak{B}(\mathcal{O}, \rho) < \infty$, then the type of σ and ρ are in the following list:*

(i) $(1^{n_1}, 2)$, $\rho_1 = \operatorname{sgn}$ *or* ϵ, $\rho_2 = \operatorname{sgn}$.
(ii) $(2, 3)$ *in* $\mathbb{S}_5$, $\rho_2 = \operatorname{sgn}$, $\rho_3 = \overrightarrow{\chi_0}$.
(iii) (2^3) *in* $\mathbb{S}_6$, $\rho_2 = \overrightarrow{\chi_1} \otimes \epsilon$ *or* $\overrightarrow{\chi_1} \otimes \operatorname{sgn}$.

Actually, the rack $\mathcal{O}_2$ in $\mathbb{S}_6$ is isomorphic to $\mathcal{O}_{2^3}$, since any map in the class of the outer automorphism of $\mathbb{S}_6$ applies (1 2) in (1 2)(3 4)(5 6) [26]. Thus, case (iii) is contained in (i).

The remaining cases can not be treated by consideration of Nichols algebras of subracks, see Remark 4.2.

1.4. The main results in this paper are negative, in the sense that they do not provide any new example of finite-dimensional pointed Hopf algebra. In fact, very few examples of finite-dimensional non-trivial pointed Hopf algebras with non-abelian group are known, see [19]; at the present moment, it is not clear what is the class of non-abelian finite groups that may afford finite-dimensional pointed Hopf algebras. Therefore, it is important to narrow down as many examples as possible in order to have a feeling of what this class might be. Here is our second main result.

Theorem 1.2 *Let $G = \mathbb{A}_m$, $m \geq 5$. If $\mathcal{O}$ is any conjugacy class of G, $\sigma \in \mathcal{O}$ is fixed and $\rho \in \widehat{C_G(\sigma)}$, then* $\dim \mathfrak{B}(\mathcal{O}, \rho) = \infty$.

In order to state the consequences of this result for pointed Hopf algebras, it is convenient to introduce the following terminology.

Definition 1.3 We shall say that a finite group G collapses if for any finite-dimensional pointed Hopf algebra H, with $G(H) \simeq G$, necessarily $H \simeq \mathbb{C}G$.

Let G be a finite group. The category of Yetter-Drinfeld modules over the group algebra $\mathbb{C}G$ is written ${}^{\mathbb{C}G}_{\mathbb{C}G}\mathcal{YD}$. The following result is a well-known consequence of the Lifting Method [9]; we sketch a proof for the sake of the generic reader. See [9] for more details and unexplained notation.

Lemma 1.4 *The following statements are equivalent*:

(1) *If $0 \neq V \in {}^{\mathbb{C}G}_{\mathbb{C}G}\mathcal{YD}$, then* $\dim \mathfrak{B}(V) = \infty$.
(2) *If $V \in {}^{\mathbb{C}G}_{\mathbb{C}G}\mathcal{YD}$ is irreducible, then* $\dim \mathfrak{B}(V) = \infty$.
(3) *G collapses.*

Proof (Sketch). (1) $\Longrightarrow$ (2) is clear; (2) $\Longrightarrow$ (1) because any finite-dimensional $V \in {}^{\mathbb{C}G}_{\mathbb{C}G}\mathcal{YD}$ contains an irreducible submodule. (3) $\Longrightarrow$ (1): If $0 \neq V \in {}^{\mathbb{C}G}_{\mathbb{C}G}\mathcal{YD}$ has $\dim \mathfrak{B}(V) < \infty$, then $H := \mathfrak{B}(V)\#\mathbb{C}G$ is a finite-dimensional pointed Hopf algebra with $G(H) \simeq G$ but $H \not\simeq \mathbb{C}G$.

(1) $\Longrightarrow$ (3): Let H be a pointed Hopf algebra with $G(H) \simeq G$. Let $\operatorname{gr} H$ be the graded Hopf algebra associated to the coradical filtration of H. It is known that $\operatorname{gr} H \simeq R\#\mathbb{C}G$, where $R = \oplus_{n\geq 0} R^n$ is a graded Hopf algebra in the braided category ${}^{\mathbb{C}G}_{\mathbb{C}G}\mathcal{YD}$; that $R^0 = \mathbb{C}$ and $V = R^1$ coincides with the space $P(R)$ of primitive elements in R; and that the Nichols algebra $\mathfrak{B}(V)$ is isomorphic to the subalgebra of R generated by R^1. Let n be the lowest positive integer with $R^n \neq 0$; clearly, $R^n \subset P(R)$. Hence, $R \neq \mathbb{C}$ implies $V = R^1 \neq 0$. Now assume that H is finite-dimensional; then R and a fortiori $\mathfrak{B}(V)$ are finite-dimensional. Hence $V = 0$ by hypothesis, $R = \mathbb{C}$ by the preceding argument, and $H \simeq \operatorname{gr} H \simeq \mathbb{C}G$. □

We conclude from Theorem 1.2:

Theorem 1.5 *If $m \geq 5$, then the alternating group $\mathbb{A}_m$ collapses.*

This result was known for the particular cases $m = 5$ and $m = 7$ [2,13]. We prove it for $m \geq 6$. Since $\mathbb{A}_3$ is abelian, finite dimensional Nichols algebras over it are classified, there are 25 of them; this can be deduced from [8, Th. 1.3], [10, Th. 1.8]. Nichols algebras over $\mathbb{A}_4$ are infinite-dimensional except for four pairs corresponding to the classes of (1 2 3) and (1 3 2) and the non-trivial characters of $\mathbb{Z}/3$ [2, §2.2]. Actually, these four algebras are

connected to each other either by an outer automorphism of $\mathbb{A}_4$ or by the Galois group of $\mathbb{Q}(\zeta_3)|\mathbb{Q}$ (the cyclotomic extension by third roots of unity). Therefore, there is only one pair to study for $\mathbb{A}_4$.

1.5. Our ultimate goal, towards the classification of finite-dimensional pointed Hopf algebras, is to answer the following question.

Question 1 *For any finite group G and for any $V \in {}^{\mathbb{C}G}_{\mathbb{C}G}\mathcal{YD}$, determine if* $\dim \mathfrak{B}(V) < \infty$.

Since the category ${}^{\mathbb{C}G}_{\mathbb{C}G}\mathcal{YD}$ is semisimple, the question splits into two cases:

(i) V irreducible,
(ii) V completely reducible, i.e. direct sum of (at least 2) irreducibles.

Case (i) was addressed in several recent papers for some groups and some conjugacy classes [1–3,5,11,15,16]; case (ii) was considered in [7,24]. Of course, the Nichols algebras of the simple submodules of a completely reducible V such that $\mathfrak{B}(V)$ is finite-dimensional, should be finite-dimensional too. But the interaction between the two cases goes also in the other way. To explain this, we need to recall that Question 1 can be rephrased in terms of racks. Indeed, the Nichols algebra of a Yetter-Drinfeld module depends only on its braiding, which in the case of a group algebra is defined in terms of the conjugation. A rack is a set with a binary operation satisfying the basic properties of the conjugation in a group (see Sect. 2.3 below). Then Question 1 is equivalent to the following one, see [6].

Question 2 *For any finite rack X, for any $n \in \mathbb{N}$, and for any non-principal 2-cocycle* $\mathbf{q}$ *as in page 231, determine if* $\dim \mathfrak{B}(X, \mathbf{q}) < \infty$.

In fact, the consideration of Question 2 is more economical than the consideration of Question 1, since different Yetter-Drinfeld modules over different groups may give rise to the same pair $(X, \mathbf{q})$, X a rack and $\mathbf{q}$ a 2-cocycle. This point of view, advocated in [6,18], is analogous to the similar consideration of braided vector spaces of diagonal type in the classification of finite-dimensional pointed Hopf algebras with abelian group.

The consideration of Question 2 has another advantage. A basic and useful property of Nichols algebras says that, if W is a braided subspace of a braided vector space V, then the Nichols algebra $\mathfrak{B}(W)$ is contained in the Nichols algebra $\mathfrak{B}(V)$. For instance, consider a simple $V = M(\mathcal{O}, \rho) \in {}^{\mathbb{C}G}_{\mathbb{C}G}\mathcal{YD}$—say $\dim \rho = 1$ for simplicity. If X is a proper subrack of $\mathcal{O}$, then $M(\mathcal{O}, \rho)$ has a braided subspace of the form $W = (\mathbb{C}X, c^q)$, which is clearly not a Yetter-Drinfeld submodule but can be realized as a Yetter-Drinfeld module over smaller groups, that could be reducible if X is decomposable. If we know that $\dim \mathfrak{B}(X, q) = \infty$, say because we have enough information on one of these smaller groups, then $\dim \mathfrak{B}(\mathcal{O}, \rho) = \infty$ too.

Both Questions have the common drawback that there is no structure theorem neither for finite groups nor for finite racks. Therefore, and in order to collect evidence about what groups or what racks might afford finite-dimensional Nichols algebras, it is necessary to attack different classes of groups or of racks. Prominent candidates are the finite simple groups and the finite simple racks. Finite simple racks have been classified in [6, Th. 3.9, Th. 3.12] (see also [25]); explicitly, any simple rack is isomorphic to one and only one of the following:

(i) $|X| = p$ a prime, $X \simeq \mathbb{F}_p$ a permutation rack, that is $x \triangleright y = y + 1$.
(ii) $|X| = p^t$, p a prime, $t \in \mathbb{N}$, $X \simeq (\mathbb{F}_{p^t}, T)$ is an affine crossed set where T is the companion matrix of a monic irreducible polynomial of degree t, different from X and $X - 1$.

(iii) $|X|$ is divisible by at least two different primes, and X is twisted homogeneous. That is, there exist a non-abelian simple group L, a positive integer t and $x \in \mathrm{Aut}(L^t)$, where x acts by $x \cdot (l_1, \dots, l_t) = (\theta(l_t), l_1, \dots, l_{t-1})$ for some $\theta \in \mathrm{Aut}(L)$, such that $X = \mathcal{O}_x(n)$ is an orbit of the action $\rightharpoonup_x$ of $N = L^t$ on itself ($n \neq m^{-1}$ if $t = 1$ and x is inner, $x(p) = mpm^{-1}$). Furthermore, L and t are unique, and x only depends on its conjugacy class in $\mathrm{Out}(L^t)$. Here, the action $\rightharpoonup_x$ is given by $p \rightharpoonup_x n = p\, n\, (x \cdot p^{-1})$.

In particular, non-trivial conjugacy classes in finite simple groups, and conjugacy classes in symmetric groups of elements not in the alternating subgroup are simple racks. Therefore, it is natural to begin by families of simple groups.

1.6. To prove Theorems 1.1 and 1.2, we first establish Theorem 4.1, namely that $\dim \mathfrak{B}(X, q) = \infty$ for many conjugacy classes X in $\mathbb{S}_m$ or $\mathbb{A}_m$ and any cocycle q. This relies on a result on Nichols algebras of reducible Yetter-Drinfeld modules [24, Th. 8.6], this paper being a sequel to, and based on the results of, [7]. Indeed, let us say (informally) that a rack collapses if $\dim \mathfrak{B}(X, q) = \infty$ for any cocycle q; see the precise statement of this notion in Def. 2.2. To translate one of the hypothesis of [24, Th.8.6] to rack-theoretical terms, we introduce the notion of rack of type D. We deduce from [24, Th.8.6] our Th. 3.6, that says that any rack of type D collapses. It is easy to see that if $\pi : Z \to X$ is an epimorphism of racks and X is of type D, then so is Z. But any indecomposable rack Z has a simple quotient X; this justifies further why we look at simple racks, starting with non-trivial conjugacy classes in simple groups. This is one of the consequences of the study of Nichols algebras of decomposable Yetter-Drinfeld modules in the analogous study of indecomposable ones. We stress that the computation of a second rack-cohomology group is a difficult task. By [12], it coincides with a first group-cohomology group, but this does not make the problem easier. Two of us have developed a program for calculations with racks, that in particular computes the rack-cohomology groups [21]. The point of view taken in this article allows to disregard sometimes these considerations.

Actually, we give in Th. 4.1 a list of conjugacy classes in $\mathbb{S}_m$ or $\mathbb{A}_m$ which are of type D; hence, if X belongs to this list and $\pi : Z \to X$ is an epimorphism of racks, then the Nichols algebra $\mathfrak{B}(Z, q)$ has infinite-dimension for an arbitrary cocycle q.

To consider the cases left open in Th. 4.1 we use techniques of abelian subracks from our previous papers—see Lemma 4.4.

The paper is organized as follows. After Sect. 2 with Preliminaries, we present our applications of [24, Th. 8.6] in Sect. 3. In Sect. 4 we prove Th. 4.1 and then complete the proofs of Ths. 1.1 and 1.2.

1.7 Glossary

We have found useful to introduce several notations concerning racks and groups in relation with the finite-dimensional Hopf algebras and Nichols algebras. We collect here these new terms.

- A finite group G collapses[1] if for any finite-dimensional pointed Hopf algebra H, with $G(H) \simeq G$, necessarily $H \simeq \mathbb{C}G$. Equivalently, for any $0 \neq V \in {}^{\mathbb{C}G}_{\mathbb{C}G}\mathcal{YD}$, $\dim \mathfrak{B}(V) = \infty$. See Def. 1.3, p. 227.
- A finite rack X collapses if for any finite faithful cocycle $\mathbf{q}$, the Nichols algebra $\mathfrak{B}(X, \mathbf{q})$ is infinite dimensional. See Def. 2.2, p. 232.
- A finite rack X is of type B if it satisfies condition (B) in Lemma 2.3, p. 232.

[1] This was referred to as of type B in [15].

- A finite rack X is of type D if it contains a decomposable subrack $Y = R \coprod S$ such that $r \triangleright (s \triangleright (r \triangleright s)) \neq s$, for some $r \in R, s \in S$.[2] See Def. 3.5, p. 234.
- A finite group G is of type D if all its non-trivial conjugacy classes are of type D. See [4].

2 Preliminaries

2.1 Notation

Let G be a group, $\sigma \in G$. We write $|G|$, respectively, $|\sigma|$, for the order of G, respectively, σ; $\mathcal{O}_\sigma = \mathcal{O}_\sigma^G$ for the conjugacy class of σ in G, with a superscript G if emphasis is needed. Also, $\widehat{G}$ is the set of isomorphism classes of irreducible representations of G. If X is a set, $\mathbb{C}X$ is the vector space with a basis $(e_x)_{x\in X}$.

A braided vector space is a pair (V, c), where V is a vector space and $c \in \mathbf{GL}(V \otimes V)$ is a solution of the braid equation: $(c \otimes \mathrm{id})(\mathrm{id} \otimes c)(c \otimes \mathrm{id}) = (\mathrm{id} \otimes c)(c \otimes \mathrm{id})(\mathrm{id} \otimes c)$. If (V, c) is a braided vector space, then $\mathfrak{B}(V)$ denotes its Nichols algebra. See [9, p. 22].

2.2 Yetter-Drinfeld modules

Let G be a group. A Yetter-Drinfeld module over the group algebra $\mathbb{C}G$ is a G-module M provided with a G-grading $M = \oplus_{g\in G} M_g$ such that $h \cdot M_g = M_{ghg^{-1}}$ for all $g, h \in G$. The category ${}^{\mathbb{C}G}_{\mathbb{C}G}\mathcal{YD}$ of Yetter-Drinfeld modules over the group algebra $\mathbb{C}G$ is a braided category; in particular any $M \in {}^{\mathbb{C}G}_{\mathbb{C}G}\mathcal{YD}$ is a braided vector space with $c \in \mathbf{GL}(M \otimes M)$ given by

$$c(m \otimes n) = g \cdot n \otimes m, \quad \text{for } m \in M_g \ (g \in G), \ n \in M. \tag{1}$$

The support of $M \in {}^{\mathbb{C}G}_{\mathbb{C}G}\mathcal{YD}$ is $\operatorname{supp} M = \{g \in G : M_g \neq 0\}$.

Assume that G is finite. Then the category ${}^{\mathbb{C}G}_{\mathbb{C}G}\mathcal{YD}$ is semisimple and its irreducible objects are parameterized by pairs $(\mathcal{O}, \rho)$, where $\mathcal{O}$ is a conjugacy class of $G, \sigma \in \mathcal{O}$ fixed, ρ an irreducible representation of the centralizer $C_G(\sigma)$ of σ. If $M(\mathcal{O}, \rho)$ denotes the irreducible Yetter-Drinfeld module corresponding to a pair $(\mathcal{O}, \rho)$ and V is the vector space affording the representation ρ, then $M(\mathcal{O}, \rho)$ is the induced module $\operatorname{Ind}_{C_G(\sigma)}^G \rho$ with the grading given by the identification $\operatorname{Ind}_{C_G(\sigma)}^G \rho = \mathbb{C}G \otimes_{C_G(\sigma)} V \simeq \mathbb{C}\mathcal{O} \otimes_{\mathbb{C}} V$. If $\sigma \in G$ and $\rho \in \widehat{C_G(\sigma)}$, then $\rho(\sigma)$ is a scalar denoted $q_{\sigma\sigma}$. The Nichols algebra of $M(\mathcal{O}, \rho)$ is denoted $\mathfrak{B}(\mathcal{O}, \rho)$.

Notice that $M(\mathcal{O}, \rho)$ can be defined and is a Yetter-Drinfeld module for any representation ρ of $C_G(\sigma)$.

2.3 Racks

We briefly recall the definition and main properties of racks; see [6] for details, more information and bibliographical references.

A rack is a pair $(X, \triangleright)$ where X is a non-empty set and $\triangleright : X \times X \to X$ is an operation such that

$$\text{the map } \varphi_x = x \triangleright \_ \text{ is invertible for any } x \in X, \quad \text{and} \tag{2}$$

$$x \triangleright (y \triangleright z) = (x \triangleright y) \triangleright (x \triangleright z) \text{ for all } x, y, z \in X. \tag{3}$$

[2] Here D stands for decomposable, and B for the class that produces nothing.

A morphism of racks is a map of the underlying sets $f : X \to Y$ such that $f(x \triangleright y) = f(x) \triangleright f(y)$ for all $x, y \in X$. Note that for any rack X, the map $\varphi : X \to \mathbb{S}_X$ given by $x \mapsto \varphi_x$ as defined above, is a morphism of racks. Really, there is an hierarchy

$$\{\text{racks}\} \supset \{\text{quandles}\} \supset \{\text{crossed sets}\},$$

where a quandle is a rack X such that $x \triangleright x = x$ for all $x \in X$; and a crossed set is a quandle X such that $x \triangleright y = y$ implies $y \triangleright x = x$, for any $x, y \in X$. The permutation rack mentioned in page 228, class (i) of the classification, is not a quandle. We are only interested in conjugacy classes and their subracks, which are all crossed sets.

Here are some examples and basic notions of racks.

- A group G is a rack (actually, a crossed set) with $x \triangleright y = xyx^{-1}$, $x, y \in G$. Furthermore, if $X \subset G$ is stable under conjugation by G, that is a union of conjugacy classes, then it is a subrack of G; e. g., the support of any $M \in {}^{\mathbb{C}G}_{\mathbb{C}G}\mathcal{YD}$ is a subrack of G.
- If A is an abelian group and $T \in \mathrm{Aut}(A)$, then A becomes a rack with $x \triangleright y = (1 - T)x + Ty$. It will be denoted by (A, T) and called an affine rack.
- A rack X is decomposable iff there exist disjoint subracks $X_1, X_2 \subset X$ such that $X_i \triangleright X_j = X_j$ for any $1 \leq i, j \leq 2$ and $X = X_1 \coprod X_2$. Otherwise, X is indecomposable.
- A decomposition of a rack X is a family $(X_i)_{i \in I}$ of pairwise disjoint subracks of X such that $X = \coprod_{i \in I} X_i$ and $X \triangleright X_i = X_i$ for all $i \in I$.
- A rack X is said to be simple iff $\mathrm{card}\, X > 1$ and for any surjective morphism of racks $\pi : X \to Y$, either π is a bijection or $\mathrm{card}\, Y = 1$.

2.4 Cocycles

Let X be a rack, $n \in \mathbb{N}$. A map $q : X \times X \to \mathbf{GL}(n, \mathbb{C})$ is a principal 2-cocycle of degree n if

$$q_{x, y \triangleright z} q_{y,z} = q_{x \triangleright y, x \triangleright z} q_{x,z},$$

for all $x, y, z \in X$. Here is an equivalent formulation: let $V = \mathbb{C}X \otimes \mathbb{C}^n$ and consider the linear isomorphism $c^q : V \otimes V \to V \otimes V$,

$$c^q(e_x v \otimes e_y w) = e_{x \triangleright y} q_{x,y}(w) \otimes e_x v,$$

$x, y \in X$, $v, w \in \mathbb{C}^n$. Then q is a 2-cocycle iff c^q is a solution of the braid equation. If this is the case, then the Nichols algebra of (V, c^q) is denoted $\mathfrak{B}(X, q)$.

More generally, let $(X_i)_{i \in I}$ be a decomposition of a rack X and let $\mathbf{n} = (n_i)_{i \in I}$ be a family of natural numbers. Then a non-principal 2-cocycle of degree $\mathbf{n}$, associated to the decomposition $(X_i)_{i \in I}$, is a family $\mathbf{q} = (q_i)_{i \in I}$ of maps $q_i : X \times X_i \to \mathbf{GL}(n_i, \mathbb{C})$ such that

$$q_i(x, y \triangleright z) q_i(y, z) = q_i(x \triangleright y, x \triangleright z) q_i(x, z), \tag{4}$$

for all $x, y \in X$, $z \in X_i$, $i \in I$. Again, this notion is related to braided vector spaces. Given a family $\mathbf{q}$, let $V = \oplus_{i \in I} \mathbb{C}X_i \otimes \mathbb{C}^{n_i}$ and consider the linear isomorphism $c^{\mathbf{q}} : V \otimes V \to V \otimes V$,

$$c^{\mathbf{q}}(e_x v \otimes e_y w) = e_{x \triangleright y} q_i(x, y)(w) \otimes e_x v,$$

$x \in X_j$, $y \in X_i$, $v \in \mathbb{C}^{n_j}$, $w \in \mathbb{C}^{n_i}$. Then $\mathbf{q}$ is a 2-cocycle iff $c^{\mathbf{q}}$ is a solution of the braid equation. If this is the case, then the Nichols algebra of $(V, c^{\mathbf{q}})$ is denoted $\mathfrak{B}(X, \mathbf{q})$.

Let X be a rack, $\mathbf{q}$ a non-principal 2-cocycle and V as above. Define a map $g : X \to \mathbf{GL}(V)$ by

$$g_x(e_y w) = e_{x \triangleright y} q_i(x, y)(w), \quad x \in X, y \in X_i, i \in I. \tag{5}$$

Note that $g : X \to \mathbf{GL}(V)$ is a morphism of racks.

The next result shows why Nichols algebras associated to racks and cocycles are important for the classification of pointed Hopf algebras. It says that Questions 1 and 2 in the Introduction are indeed equivalent.

Theorem 2.1 [6, Th. 4.14]

(i) *Let X be a finite rack, $(X_i)_{i\in I}$ a decomposition of X, $\mathbf{n} \in \mathbb{N}^I$ and $\mathbf{q}$ a 2-cocycle as above. If $G \subset \mathbf{GL}(V)$ is the subgroup generated by $(g_x)_{x\in X}$, then $V \in {}^{\mathbb{C}G}_{\mathbb{C}G}\mathcal{YD}$. If the image of q_i generates a finite subgroup of $\mathbf{GL}(n_i, \mathbb{C})$ for all $i \in I$, then G is finite.*

(ii) *Conversely, if G is a finite group and $V \in {}^{\mathbb{C}G}_{\mathbb{C}G}\mathcal{YD}$, then there exist a rack X, a decomposition $X = \coprod_{i\in I} X_i$, $\mathbf{n} \in \mathbb{N}^I$ and non-principal 2-cocycle $\mathbf{q}$ such that V is given as above and the braiding $c \in \mathrm{Aut}(V \otimes V)$ in the category ${}^{\mathbb{C}G}_{\mathbb{C}G}\mathcal{YD}$ coincides with $c^{\mathbf{q}}$.*

If X is indecomposable, then there is only one possible decomposition and only principal 2-cocycles arise. Conversely, the proof of [6, Th. 4.14] shows that if $V \in {}^{\mathbb{C}G}_{\mathbb{C}G}\mathcal{YD}$ as in part (ii) is irreducible, then the cocycle $\mathbf{q}$ is actually principal.

For an easy way of reference, we shall say that a cocycle $\mathbf{q}$ is finite if the image of q_i generates a finite subgroup of $\mathbf{GL}(n_i, \mathbb{C})$ for all $i \in I$.

Parallel to the approach to the classification of finite-dimensional pointed Hopf algebras group-by-group, we envisage the approach to the classification of finite-dimensional Nichols algebras rack-by-rack. It is then natural to introduce the following terminology.

Let X be a finite rack and $\mathbf{q}$ a 2-cocycle. First, we shall say that $(X, \mathbf{q})$ is faithful if the morphism of racks $g : X \to \mathbf{GL}(V)$ defined in (5) is injective; if X is clear from the context, we shall also say that $\mathbf{q}$ is faithful. Recall that a rack X is faithful if $\varphi : X \to \mathbb{S}_X$ is injective [6, Def. 1.11]; clearly, if X is faithful, then $(X, \mathbf{q})$ is faithful for any $\mathbf{q}$.

Definition 2.2 We shall say that a finite rack X collapses if for any finite faithful cocycle $\mathbf{q}$ (associated to any decomposition of X and of any degree $\mathbf{n}$), $\dim \mathfrak{B}(X, \mathbf{q}) = \infty$.

Here is a useful reformulation of the preceding definition.

Lemma 2.3 *Let X be a finite rack. Assume that*

(B) *For any finite group G and any $M \in {}^{\mathbb{C}G}_{\mathbb{C}G}\mathcal{YD}$ such that X is isomorphic to a subrack of $\mathrm{supp}\, M$, $\dim \mathfrak{B}(M) = \infty$.*

Then X collapses. The converse is true if X is faithful.

Proof Assume (B). Let $\mathbf{q}$ be a finite faithful cocycle. By Th. 2.1 (i), the braided vector space $(V, c^{\mathbf{q}})$ arises from a Yetter-Drinfeld module over a finite group Γ; since $\mathbf{q}$ is faithful, X can be identified with $\mathrm{supp}\, V$.

Now assume that X is faithful and collapses. Let G, M as in (B). The rack Y constructed in Th. 2.1 (ii) is $Y = \coprod_{i\in I} \mathcal{O}_i$, where $M = \oplus_{i\in I} M_i$ is a decomposition in irreducible submodules and $\mathcal{O}_i = \mathrm{supp}\, M_i$. In general, $\mathrm{supp}\, M \neq Y$, but there is an injective morphism of racks $\mathrm{supp}\, M \hookrightarrow Y$, which induces an injective morphism of racks $X \hookrightarrow Y$. Since X is faithful, the restriction of the cocycle $\mathbf{q}$ on Y to X is a cocycle on X whence it is faithful. Finally observe that $\mathfrak{B}(X, \mathbf{q}_{|X})$ can be embedded in $\mathfrak{B}(M)$. □

3 Techniques

From now on, we shall consider any group G as a rack with the operation given by conjugation.

3.1 The technique of a suitable subgroup

If W is a braided subspace of a braided vector space V, then $\mathfrak{B}(W) \hookrightarrow \mathfrak{B}(V)$ [9, Cor. 2.3]. Let G be a group, $M \in {}^{\mathbb{C}G}_{\mathbb{C}G}\mathcal{YD}$. Here are two ways of getting braided subspaces of M:

- If Y is a subrack of $\operatorname{supp} M$, then $M_Y := \oplus_{y \in Y} M_y$ is a braided subspace of M.
- Let H be a subgroup of G and let $\sigma \in H$. If ρ is a representation of $C_G(\sigma)$, then $M(\mathcal{O}_\sigma^H, \rho|_{C_H(\sigma)})$ is a braided subspace of $M(\mathcal{O}_\sigma^G, \rho)$.

These ways are actually closely related by the following result.

Lemma 3.1 *If Y is a subrack of* $\operatorname{supp} M$ *and K is the subgroup of G generated by Y, then M_Y is an object in ${}^{\mathbb{C}K}_{\mathbb{C}K}\mathcal{YD}$.*

Proof By construction, M_Y is K-graded. Furthermore, if $k \in K$ and $y \in Y$, then $k \cdot M_y = M_{k \triangleright y} \subset M_Y$ since Y is closed under conjugation by K. □

Assume now that G is a finite group, and let σ, ρ and H be as above. Then $\rho|_{C_H(\sigma)} = \tau_1 \oplus \cdots \oplus \tau_s$ where $\tau_j \in \widehat{C_H(\sigma)}$, $1 \leq j \leq s$. Therefore, we have the following criterium.

Lemma 3.2 *Keep the notation above.*

(i) *If* $\dim \mathfrak{B}(\mathcal{O}_\sigma^H, \lambda) = \infty$ *for all* $\lambda \in \widehat{C_H(\sigma)}$, *then* $\dim \mathfrak{B}(\mathcal{O}_\sigma^G, \rho) = \infty$ *for all* $\rho \in \widehat{C_G(\sigma)}$.
(ii) *Let* $\sigma_1, \sigma_2 \in \mathcal{O}^G \cap H$. *Let* $\mathcal{O}_i = \mathcal{O}_{\sigma_i}^H$ *and assume that* $\mathcal{O}_1 \neq \mathcal{O}_2$. *If* $\dim \mathfrak{B}(M(\mathcal{O}_1, \lambda_1) \oplus M(\mathcal{O}_2, \lambda_2)) = \infty$ *for all pairs* $\lambda_1 \in \widehat{C_H(\sigma_1)}$, $\lambda_2 \in \widehat{C_H(\sigma_2)}$, *then* $\dim \mathfrak{B}(\mathcal{O}^G, \rho) = \infty$ *for all* $\rho \in \widehat{C_G(\sigma)}$.

3.2 The splitting technique

We begin by stating the following result of Heckenberger and Schneider, whose proof uses the main Theorem of [7].

Theorem 3.3 [24, Th. 8.6 (1)] *Let G be a finite group, $M(\mathcal{O}, \rho)$, $M(\mathcal{O}', \rho')$ irreducible objects in ${}^{\mathbb{C}G}_{\mathbb{C}G}\mathcal{YD}$ such that* $\dim \mathfrak{B}(M(\mathcal{O}, \rho) \oplus M(\mathcal{O}', \rho')) < \infty$. *Then for all $r \in \mathcal{O}$, $s \in \mathcal{O}'$, $(rs)^2 = (sr)^2$.*

We use the previous Theorem as in the following Proposition.

Proposition 3.4 *Let G be a finite group and $\mathcal{O}$ a conjugacy class in G. Assume that there exist σ_1, σ_2 in $\mathcal{O}$ such that $(\sigma_1\sigma_2)^2 \neq (\sigma_2\sigma_1)^2$. If there exists a subgroup H such that σ_1 and σ_2 are not conjugate in H, then $\mathfrak{B}(\mathcal{O}, \rho) = \infty$.*

Proof It follows by Theorem 3.3 and Lemma 3.2 (ii). □

We now aim to state a rack-theoretical version of Prop. 3.4. Let G be a group, $r, s \in G$. Then $(rs)^2 = (sr)^2 \iff r \triangleright (s \triangleright (r \triangleright s)) = s$. We next introduce a notion that is central in our considerations.

Definition 3.5 Let $(X, \triangleright)$ be a rack. We say that X is of type D if there exists a decomposable subrack $Y = R \coprod S$ of X such that

$$r \triangleright (s \triangleright (r \triangleright s)) \neq s, \quad \text{for some } r \in R, s \in S. \tag{6}$$

Here D stands for 'a rack with a *decomposable* subrack satisfying (6)'.

Theorem 3.6 *If X is a finite rack of type D, then X collapses.*

Proof We shall prove that X is, more generally, of type B as in Lemma 2.3. Let $Y \subseteq X$, $Y = R \coprod S$ a decomposition as in Definition 3.5. Let G be a finite group, $M \in {}^{\mathbb{C}G}_{\mathbb{C}G}\mathcal{YD}$ such that X is isomorphic to a subrack of $\operatorname{supp} M$. We identify X to this subrack, and then we can take M_R and M_S, which are non trivial objects in ${}^{\mathbb{C}K}_{\mathbb{C}K}\mathcal{YD}$, K the subgroup of G generated by Y. We may assume that M_R and M_S are irreducible; otherwise, we replace them by irreducible submodules. Now, $\dim \mathfrak{B}(M_R \oplus M_S) = \infty$ by Th. 3.3, and then $\dim \mathfrak{B}(M) = \infty$. □

Being of type D is an ubiquitous notion:

(i) If $Y \subseteq X$ is a subrack of type D, then X is of type D.
(ii) If Z is a finite rack and admits a rack epimorphism $\pi : Z \to X$, where X is of type D, then Z is of type D. For, $\pi^{-1}(Y) = \pi^{-1}(R) \coprod \pi^{-1}(S)$ is a decomposable subrack of Z satisfying (6).

Let now X be any finite rack. If some indecomposable component [6, Prop. 1.17] is of type D, then X is of type D. Assume then that X is indecomposable; then it admits a projection of racks $\pi : X \to Y$ with Y simple. Thus, it is of primary interest to solve the following problem.

Question 3 *Determine all simple racks of type D.*

In this paper we consider simple racks arising as conjugacy classes of the alternating or symmetric groups. In subsequent papers, we shall investigate other simple racks; our paper [4] is devoted to conjugacy classes in sporadic groups.

Here are some useful observations to detect conjugacy classes of type D.

Lemma 3.7 (a). *If X is of type D and Z is a quandle, then $X \times Z$ is of type D.*
(b). *Let K be a subgroup of a finite group G, $\tau \in K$ and $\kappa \in C_G(K)$. We consider the map $\mathcal{R}_\kappa : K \to G$, $g \mapsto \widetilde{g} := g\kappa$. Then the conjugacy class $\mathcal{O}$ of τ computed in K can be identified with a subrack of the conjugacy class $\widetilde{\mathcal{O}}$ of $\widetilde{\tau}$ in G. Therefore, if $\mathcal{O}$ is of type D, then $\widetilde{\mathcal{O}}$ is of type D.*

Proof (a). If $r, s \in X$ and $z \in Z$, then $(r, z) \triangleright (s, z) = (r \triangleright s, z)$ because Z is a quandle. The rest is straightforward. (b) follows because the map $\mathcal{R}_\kappa$ is a morphism of racks. □

We need the following definition to state our next result.

Definition 3.8 Let G be a finite group, $\mathcal{O}$ a conjugacy class in G, $\sigma \in \mathcal{O}$. Classically, $\sigma \in G$ and $\mathcal{O}$ are real if $\sigma^{-1} \in \mathcal{O}$. If σ is conjugated to $\sigma^j \neq \sigma$ for some $j \in \mathbb{N}$, then we say that σ and $\mathcal{O}$ are quasi-real of type j. Clearly, any real σ, which is not an involution, is quasi-real of type $|\sigma| - 1$.

Proposition 3.9 *Let G be a finite group and $g = \tau\kappa \in G$, where τ and $\kappa \neq e$ commute. Let $K = C_G(\kappa) \ni \tau$; then $\kappa \in C_G(K)$. Hence, the conjugacy class $\mathcal{O}$ of τ in K can be identified with a subrack of the conjugacy class $\widetilde{\mathcal{O}}$ of g in G via the morphism $\mathcal{R}_\kappa$ as in the preceding example. Assume that*

- $\widetilde{\mathcal{O}}$ *and* $\mathcal{O}$ *are quasi-real of type* j,
- *the orders* N *of* τ *and* M *of* κ *are coprime,*
- M *does not divide* $j-1$,
- *there exist* $r_0, s_0 \in \mathcal{O}$ *such that* $r_0 \triangleright (s_0 \triangleright (r_0 \triangleright s_0)) \neq s_0$.

Then $\widetilde{\mathcal{O}}$ *is of type D.*

Proof Observe first that $(\kappa^j x) \triangleright (\kappa^h y) = \kappa^h (x \triangleright y)$ for any $x, y \in K$, $j, h \in \mathbb{Z}$. Let $R = \mathcal{R}_\kappa(\mathcal{O})$, $S = \mathcal{R}_{\kappa^j}(\mathcal{O})$; R and S are subracks of $\widetilde{\mathcal{O}}$ by Lemma 3.7. For,

$$S = \mathcal{R}_{\kappa^j}(\mathcal{O}) \overset{\mathcal{O} \text{ quasi-real}}{=} \mathcal{R}_{\kappa^j}(\mathcal{O}^K_{\tau^j}) = \mathcal{O}^K_{\tau^j \kappa^j} \subseteq \mathcal{O}^G_{\tau^j \kappa^j} \overset{\widetilde{\mathcal{O}} \text{ quasi-real}}{=} \widetilde{\mathcal{O}}.$$

We next claim that R and S are disjoint. Indeed, if $z = \kappa x = \kappa^j y$, where $x, y \in \mathcal{O}$, then the order of $\kappa^{j-1} = xy^{-1}$ divides both N and M (note that x and y commute); hence $\kappa^{j-1} = e$, a contradiction. Now $r = \kappa r_0 \in R$, $s = \kappa^j s_0 \in S$ satisfy (6). □

Remark 3.10 Theorem 3.6 generalizes [3, Cor. 4.12]. Indeed, if $\mathfrak{O}$ is the octahedral rack and $\mathfrak{O}^{(2)}$ is a disjoint union of two copies of $\mathfrak{O}$, see [3], then $\mathfrak{O}^{(2)}$ is of type D. For the other techniques in [3], see Example 3.18.

3.3 Some constructions of racks

We now present a general construction that might be of independent interest. Let X be a rack, with operation $x \triangleright y = \varphi_x(y)$, and let j an integer. Let $X^{[j]}$ be a disjoint copy of X, with a fixed bijection $X \to X^{[j]}$, $x \mapsto x^{[j]}$, $x \in X$. We define a multiplication $\triangleright$ in $X^{[j]}$ by

$$x^{[j]} \triangleright y^{[j]} = (\varphi_x^j(y))^{[j]}, \quad x, y \in X. \tag{7}$$

Notice that $X^{[j][k]} \simeq X^{[jk]}$, for $j, k \in \mathbb{Z}\backslash\{0\}$.

Lemma 3.11 (i) $X^{[j]}$ *is a rack, called the* j*-th power of* X.

(ii) *The disjoint union* $X^{[1,j]}$ *of* X *and* $X^{[j]}$ *with multiplication such that* X *and* $X^{[j]}$ *are subracks, and*

$$x \triangleright y^{[j]} = (x \triangleright y)^{[j]}, \quad x^{[j]} \triangleright y = \varphi_x^j(y), \quad x, y \in X, \tag{8}$$

is a rack.

$X^{[1,j]}$ is a particular case of an amalgamated sum of racks. The rack $X^{[-1]}$ will be called the inverse rack of X and will be denoted X'; the corresponding bijection is denoted $x \mapsto x'$. Note $X'' \simeq X$. The rack $X^{[1,1]}$ will be denoted $X^{(2)}$ in accordance with [3].

Proof We first show (i) for $j = -1$. The self-distributivity (3) holds iff $\varphi_x \varphi_y = \varphi_{x \triangleright y} \varphi_x$ for all $x, y \in X$, iff $\varphi^{-1}_{\varphi_x^{-1}(u)} \varphi_x^{-1} = \varphi_x^{-1} \varphi_u^{-1}$ for all $x, u \in X$ (setting $u = x \triangleright y$); this is in turn equivalent to the self-distributivity for X'. We next show (i) for $j \in \mathbb{N}$. We check inductively that $\varphi_x \varphi_y^j = \varphi^j_{x \triangleright y} \varphi_x$, $\varphi_x^j \varphi_y = \varphi_{\varphi_x^j(y)} \varphi_x^j$. Hence $\varphi_x^j \varphi_y^j = \varphi^j_{\varphi_x^j(y)} \varphi_x^j$, and we have self-distributivity for $X^{[j]}$. Combining these two cases, we see that self-distributivity holds for $X^{[j]}$, for any $j \in \mathbb{Z}\backslash\{0\}$. The proof of (ii) is straightforward. □

Example 3.12 Let $j \in \mathbb{Z}\backslash\{0\}$. Assume that X is a subrack of G such that the map $\eta_j : X \to G$, $x \mapsto x^j$, is injective. Then the image X^j of η_j is also a subrack, isomorphic to the rack $X^{[j]}$. If $X \cap X^j = \emptyset$, then the disjoint union $X \cup X^j$ is a subrack of G isomorphic to $X^{[1,j]}$.

3.4 Affine double racks

Let (A, T) be a finite affine rack, see page 231. We realize it as a conjugacy class in the following way. Let $d = |T|$. Consider the semidirect product $G = A \rtimes \langle T \rangle$. The conjugation in G gives

$$(v, T^h) \triangleright (w, T^j) = (T^h(w) + (\mathrm{id} - T^j)(v), T^j). \tag{9}$$

Let $\mathsf{Q}^j_{A,T} := \{(w, T^j) : w \in A\}$, $j \in \mathbb{Z}/d$, a subrack of G isomorphic to the affine rack (A, T^j). Let $\mathsf{Q}^{[1,j]}_{A,T}$ be the disjoint union $\mathsf{Q}^1_{A,T} \cup \mathsf{Q}^j_{A,T}$, $j \in \mathbb{Z}/d$; this is a rack with multiplication (9); it is called an affine double rack. If $j \neq 1$, it can be identified with a subrack of G.

Remark 3.13 If $(j)_T = \sum_{i=0}^{j-1} T^i$ is an isomorphism, then $\mathsf{Q}^j_{A,T} \simeq (\mathsf{Q}^1_{A,T})^{[j]}$. Indeed, the map $(\mathsf{Q}^1_{A,T})^{[j]} \to \mathsf{Q}^j_{A,T}$, $(v, T) \mapsto (v, T)^j = ((j)_T v, T^j)$, is a rack isomorphism. Hence, $\mathsf{Q}^{[1,j]}_{A,T}$ is isomorphic to $(\mathsf{Q}^1_{A,T})^{[1,j]}$, cf. Lemma 3.11.

Let $A^T = \ker(\mathrm{id} - T)$ be the subgroup of points fixed by T.

Remark 3.14 Assume that $A^T = 0$. Then $\mathsf{Q}_{A,T} = \mathsf{Q}^1_{A,T}$ is indecomposable and it does not contain any abelian subrack with more than one element.

For, assume that $\mathsf{Q}_{A,T} = R \coprod S$ is a decomposition, with $(0, T) \in R$. But then $R \ni (v, T) \triangleright (0, T) = ((\mathrm{id} - T)(v), T)$ for any $v \in A$; since $\mathrm{id} - T$ is bijective, $\mathsf{Q}_{A,T} = R$. The second claim follows at once from (9).

Lemma 3.15 *Let $j \in \mathbb{Z}/d$. The rack $\mathsf{Q}^{[1,j]}_{A,T}$ is of type D, provided that*

$$(\mathrm{id} + T^{j+1})(\mathrm{id} - T) \neq 0. \tag{10}$$

Proof Let $R = \mathsf{Q}^1_{A,T}$, $S = \mathsf{Q}^j_{A,T}$, $r = (0, T) \in R$. Then $\mathsf{Q}^{[1,j]}_{A,T} = R \coprod S$. We check (6). Pick $v \notin \ker(\mathrm{id} + T^{j+1})(\mathrm{id} - T)$ and $s = (v, T^j) \in S$. Then

$$r \triangleright (s \triangleright (r \triangleright s)) = ((T - T^{j+1} + T^{j+2})(v), T^j) \neq s,$$

since $(\mathrm{id} - T + T^{j+1} - T^{j+2})(v) \neq 0$. □

3.5 Applications of affine double racks

If X a rack that contains a subrack isomorphic to $\mathsf{Q}^{[1,j]}_{A,T}$, for some affine rack satisfying (10), then X is of type D (therefore it collapses). We now present a way to check this hypothesis. Recall the notion of quasi-real element of a finite group, see Definition 3.8.

Proposition 3.16 *Let G be a finite group, $\mathcal{O} \subset G$ a conjugacy class which is quasi-real of type $j \in \mathbb{N}$. Let (A, T) be an affine rack, and let $\psi : A \to \mathcal{O}$ be a monomorphism of racks. If $\mathrm{id} - T^j$ is an isomorphism and $\mathrm{id} + T^{j+1} \neq 0$, then $\mathcal{O}$ is of type D.*

Proof Since $\mathrm{id} - T^j = (\mathrm{id} - T)(j)_T$, both Remarks 3.13 and 3.14 apply. If $Y = \psi(\mathsf{Q}_{A,T})$, then $Y \cap Y^j = \emptyset$. If not, pick $y \in Y \cap Y^j$, $y = x^j$ for some $x \in Y$. Then $x = x^j$, because Y does not contain any abelian subrack with more than one element. But this contradicts the definition of quasi-real. Hence $\mathcal{O}$ contains a subrack isomorphic to $\mathsf{Q}^1_{A,T} \cup \mathsf{Q}^j_{A,T}$ by Example 3.12, which is isomorphic to $\mathsf{Q}^{[1,j]}_{A,T}$ by Remark 3.13. Now the statement follows from Lemma 3.15. □

Assume for the rest of this Subsection that (A, T) *is a simple affine rack*; that is, $A = \mathbb{F}_p^t$, p a prime, and $T \in \mathbf{GL}(t, \mathbb{F}_p) - \{\mathrm{id}\}$ of order d, acting irreducibly.

In this context, Lemma 3.15 specializes as follows.

Lemma 3.17 *If* $j \in \mathbb{Z}/d$, *then* $\mathsf{Q}_{A,T}^{[1,j]}$ *is of type D, provided that*

$$j \neq \begin{cases} \frac{d}{2} - 1, & \text{if } p \text{ is odd,} \\ d - 1, & \text{if } p = 2. \end{cases} \tag{11}$$

Proof Since $T \neq \mathrm{id}$ is irreducible, $(\mathrm{id} + T^{j+1})(\mathrm{id} - T) = 0$ implies $T^{j+1} = -\mathrm{id}$. If $p = 2$, then $j + 1 = d$; if $p > 2$, then $j + 1$ is the unique element of order 2 in $\mathbb{Z}/d$, thus d is even and $j = \frac{d}{2} - 1$. In other words, (11) implies (10); hence Lemma 3.15 applies. □

Example 3.18 Let G be a finite group, $\mathcal{O} \subset G$ a conjugacy class which is quasi-real of type $j \in \mathbb{N}$. Let (A, T) be an affine simple rack with $|T| = d$, and let $\psi : A \to \mathcal{O}$ be a monomorphism of racks. If $j \neq \frac{d}{2} - 1$ when p is odd, or if $j \neq d - 1$ when $p = 2$, then $\mathcal{O}$ is of type D. Notice that the first case in (11) always holds if d is odd or 2.

If $A = \mathbb{Z}/p$, p a prime, and T has order 2, then $\mathsf{Q}_{A,T}^1$ is called a dihedral rack and denoted $\mathcal{D}_p$ in accordance with [3, Def. 2.2]; thus $\mathsf{Q}_{A,T}^{[1,1]}$ is denoted $\mathcal{D}_p^{(2)}$. Therefore, the splitting technique includes (without having to resort to look for cocycles) the case of quasi-real orbits containing a dihedral subrack [3, Cor. 2.9].

4 Simple racks from $\mathbb{S}_m$ and $\mathbb{A}_m$

4.1 Notations on symmetric groups

Let $\sigma \in \mathbb{S}_m$. We say that $\sigma \in \mathbb{S}_m$ is of type $(1^{n_1}, 2^{n_2}, \dots, m^{n_m})$ if the decomposition of σ as product of disjoint cycles contains n_j cycles of length j, for every j, $1 \leq j \leq m$. Let $A_j = A_{1,j} \cdots A_{n_j,j}$ be the product of the $n_j \geq 0$ disjoint j-cycles $A_{1,j}, \dots, A_{n_j,j}$ of σ. Then

$$\sigma = A_1 \cdots A_m; \tag{12}$$

we shall omit A_j when $n_j = 0$. The even and the odd parts of σ are

$$\sigma_e := \prod_{j \text{ even}} A_j, \quad \sigma_o := \prod_{1<j \text{ odd}} A_j. \tag{13}$$

Thus, $\sigma = A_1 \sigma_e \sigma_o = \sigma_e \sigma_o$; we define σ_o in this way for simplicity of some statements and proofs. We say also that σ has type $(1^{n_1}, 2^{n_2}, \dots, \sigma_o)$, for brevity, to point out the number of even cycles or fixed points, with arbitrary cycles of odd lengths. For instance, the type of σ is $(2, 4^2, \sigma_o)$ means that σ fixes no point, has exactly one cycle of length 2, exactly two cycles of length 4 and any other cycle has odd length.

We now recall the notation on representations of the centralizer needed in the statement of Theorem 1.1. See [5, Sect. 2.2] for more details. First, the centralizer $\mathbb{S}_m^\sigma = C_{\mathbb{S}_m}(\sigma) = T_1 \times \cdots \times T_m$, where

$$T_j = \langle A_{1,j}, \dots, A_{n_j,j} \rangle \rtimes \langle B_{1,j}, \dots, B_{n_j-1,j} \rangle \simeq (\mathbb{Z}/j)^{n_j} \rtimes \mathbb{S}_{n_j}, \tag{14}$$

$1 \leq j \leq m$. We describe the irreducible representations of the centralizers. If $\rho = (\rho, V) \in \widehat{C_{\mathbb{S}_m}(\sigma)}$, then $\rho = \rho_1 \otimes \cdots \otimes \rho_m$, where $\rho_j \in \widehat{T_j}$ has the form

$$\rho_j = \operatorname{Ind}_{(\mathbb{Z}/j)^{n_j} \rtimes \mathbb{S}_{n_j}^{\chi_j}}^{(\mathbb{Z}/j)^{n_j} \rtimes \mathbb{S}_{n_j}} (\chi_j \otimes \mu_j), \tag{15}$$

with $\chi_j \in \widehat{(\mathbb{Z}/j)^{n_j}}$ and $\mu_j \in \widehat{\mathbb{S}_{n_j}^{\chi_j}}$—see [28, Sect. 8.6]. Here $\mathbb{S}_{n_j}^{\chi_j}$ is the isotropy subgroup of χ_j under the induced action of $\mathbb{S}_{n_j}$ on $\widehat{(\mathbb{Z}/j)^{n_j}}$. Actually, χ_j is of the form $\chi_{(t_{1,j},\dots,t_{n_j,j})}$, where $0 \leq t_{1,j}, \dots, t_{n_j,j} \leq j-1$ are such that

$$\chi_{(t_{1,j},\dots,t_{n_j,j})}(A_{l,j}) = \omega_j^{t_{l,j}}, \quad 1 \leq l \leq n_j, \tag{16}$$

with $\omega_j := e^{\frac{2\pi i}{j}}$, where i denotes the imaginary unit. Assume that $\deg(\rho) = 1$; that is, $\deg(\rho_j) = 1$, for all j. Then $\mathbb{S}_{n_j}^{\chi_j} = \mathbb{S}_{n_j}$, $\mu_j = \epsilon$ or sgn $\in \widehat{\mathbb{S}_{n_j}}$, for all j. Hence, we have that $t_j := t_{1,j} = \cdots = t_{n_j,j}$, for every j, and $\rho_j = \chi_j \otimes \mu_j$. In that case, we will denote $\chi_j = \chi_{(t_j,\dots,t_j)}$ by $\overrightarrow{\chi_{t_j}}$.

4.2 The collapse of simple racks from $\mathbb{S}_m$ or $\mathbb{A}_m$

Let $m \geq 5$. In this Subsection, we show that many simple racks arising as conjugacy classes in $\mathbb{S}_m$ or $\mathbb{A}_m$ collapse. We fix $\sigma \in \mathbb{S}_m$ be of type $(1^{n_1}, 2^{n_2}, \dots, m^{n_m})$ and let

$$\mathcal{O} = \begin{cases} (a) & \text{the conjugacy class of } \sigma \text{ in } \mathbb{S}_m, \quad \text{if } \sigma \notin \mathbb{A}_m, \\ (b) & \text{the conjugacy class of } \sigma \text{ in } \mathbb{A}_m, \quad \text{if } \sigma \in \mathbb{A}_m. \end{cases}$$

Thus $\mathcal{O}$ is a simple rack. If σ is in $\mathbb{A}_m$, then either $\mathcal{O}_\sigma^{\mathbb{S}_m}$ splits as a disjoint union of two orbits in $\mathbb{A}_m$, or else $\mathcal{O}_\sigma^{\mathbb{S}_m} = \mathcal{O}_\sigma^{\mathbb{A}_m}$. This last possibility arises when either $n_i > 0$ for some i even, or else $n_i > 1$ for some i odd. In any case, if $\mathcal{O}_\sigma^{\mathbb{A}_m}$ is of type D, then so is $\mathcal{O}_\sigma^{\mathbb{S}_m}$.

Theorem 4.1 *If the type of σ is NOT in the list below, then $\mathcal{O}$ is of type D, hence it collapses.*

(a) $(2, 3)$; (2^3); $(1^n, 2)$.
(b) (3^2); $(2^2, 3)$; $(1^n, 3)$; (2^4); $(1^2, 2^2)$; $(1, 2^2)$; $(1, p)$, (p) *with p prime.*

Proof We proceed in several steps.

Step 1 (Reduction by juxtaposition) *Let $m = p + q$, $\mu \in \mathbb{S}_p$, $\tau \in \mathbb{S}_q$ and $\sigma = \mu \perp \tau \in \mathbb{S}_m$ the juxtaposition. If $\mathcal{O}_\mu^p$ is of type D, then $\mathcal{O}_\sigma^m$ also is. In the same vein, if $\mu \in \mathbb{A}_p$ and its conjugacy class in $\mathbb{A}_p$ is of type D, and $\tau \in \mathbb{A}_q$, then the conjugacy class of $\sigma = \mu \perp \tau \in \mathbb{A}_m$ is of type D.*

This is so because the inclusion $\mathbb{S}_p \times \mathbb{S}_q \hookrightarrow \mathbb{S}_m$ induces an inclusion of racks $\mathcal{O}_\mu^p \times \mathcal{O}_\tau^q \hookrightarrow \mathcal{O}_\sigma^m$. With this inclusion, the result follows from Lemma 3.7.

This statement can be be rewritten as follows: Let $\mu \in \mathbb{S}_p$, with $p \leq m$ and μ is of type $(1^{h_1}, 2^{h_2}, \dots, p^{h_p})$ with $h_j \leq n_j$, $1 \leq j \leq p$, and let

$$\mathcal{O}' = \begin{cases} \text{the conjugacy class of } \mu \text{ in } \mathbb{S}_p, \quad \text{if } \mu \notin \mathbb{A}_p, \\ \text{the conjugacy class of } \mu \text{ in } \mathbb{A}_p, \quad \text{if } \mu \in \mathbb{A}_p. \end{cases}$$

If $\mathcal{O}'$ is of type D, then $\mathcal{O}$ is of type D.

Step 2 *If the type of σ is (m) with $m \geq 6$ not prime, then $\mathcal{O}$ is of type D.*

Let $\sigma = (1\ 2\ 3\ 4 \cdots m)$. We study different cases.

(i) $m \geq 6$ *is even.*

If $m = 6$, take $\tau = (1\ 2\ 5\ 6\ 3\ 4)$. It is straightforward to check that σ and τ are not conjugate in $H = \langle \sigma, \tau \rangle$ and that $(\sigma\tau)^2 \neq (\tau\sigma)^2$.

If $m > 6$, take $\tau = (1\ 3) \triangleright \sigma = (3\ 2\ 1\ 4 \cdots m)$. Then $\tau\sigma\tau\sigma(1) = 1$ and $\sigma\tau\sigma\tau(1) = 7$. Therefore, $(\sigma\tau)^2 \neq (\tau\sigma)^2$. Let $H = \langle \sigma, \tau \rangle$ be the subgroup of $\mathbb{S}_m$ generated by σ and τ.

Note that $H = \langle \sigma, \tau \rangle = \langle \sigma, \tau\sigma^{-1} \rangle = \langle (1\ 2 \cdots n), (1\ 3)(2\ 4) \rangle$. It is easy to see that the elements in H can be written as products $(\mu_1 \times \mu_2)\sigma^i$, where $\mu_1 \in \mathbb{S}_{\{1,3,5,\ldots,m-1\}}$, $\mu_2 \in \mathbb{S}_{\{2,4,6,\ldots,m\}}$ and the signs $\operatorname{sgn}(\mu_1) = \operatorname{sgn}(\mu_2)$. Now, if $x \in \mathbb{S}_m$ is such that $x \triangleright \sigma = \tau$, then $x = (1\ 3)\sigma^i$ for some i, which does not belong to H. Hence, σ and τ belong to different conjugacy classes in H.

(ii) $m \geq 5$ *odd and divisible by a non-trivial square number.* Let $m = h^2k$, with $h \geq 3$. For $1 \leq i \leq hk$, let $r_i = (i\ (hk+i)\ (2hk+i) \cdots ((h-1)hk+i))$, and consider $\tau = r_1 \triangleright \sigma$. Then σ and τ are conjugate in $\mathbb{A}_m$, but they are not conjugate in $H = \langle \sigma, \tau \rangle$. To see this, notice that $\sigma r_1^{-1} \sigma^{-1} = r_2^{-1}$, and then, as in the proof of case (i),

$$H = \langle \sigma, \tau\sigma^{-1} \rangle = \langle \sigma, r_1 r_2^{-1} \rangle$$

Then $H \subseteq G := \langle \sigma, r_1, \ldots, r_{hk} \rangle$. Actually, since $\sigma^{hk} = r_1 r_2 \cdots r_{hk}$, G is an extension

$$1 \to \langle r_1, \ldots, r_{hk} \rangle \simeq (\mathbb{Z}/m)^{hk} \to G \to \mathbb{Z}/hk \to 1.$$

Any element in G can be written uniquely as a product $r_1^{i_1} \cdots r_{hk}^{i_{hk}} \sigma^j$, where $0 \leq j < hk$. We can consider then the homomorphism $\alpha : G \to \mathbb{Z}/h$, given by $\alpha(r_1^{i_1} \cdots r_{hk}^{i_{hk}} \sigma^j) = \omega^{i_1 + i_2 + \cdots + i_{hk}}$, where ω is a generator of $\mathbb{Z}/h$. This homomorphism is well defined, since $\alpha(\sigma^{hk}) = \alpha(r_1 r_2 \cdots r_{hk}) = \omega^{hk} = 1$. On the other hand, the centralizer of σ in $\mathbb{A}_m$ is the subgroup generated by σ. Thus, for σ and τ to be conjugate in H, there should exist an integer j such that $r_1\sigma^j \in H$. But it is clear that H is in the kernel of α, while $\alpha(r_1\sigma^j) = \omega$.

(iii) $m \geq 9$ *odd and divisible by at least two primes.*

Express $\sigma = \tau\kappa$, where $\tau \neq e$ and $\kappa \neq e$ are powers of σ, the orders N of τ and M of κ are coprime and $N > 3$ is prime. Note that $m = NM$ and the type of κ is (M^N), hence $K = C_{\mathbb{A}_m}(\kappa) \simeq (\mathbb{Z}/M)^N \rtimes \mathbb{A}_N$. Let $\widetilde{\mathcal{O}} = \mathcal{O}_\sigma^{\mathbb{A}_m}$ and $\mathcal{O} = \mathcal{O}_\tau^K$. It is known that $\widetilde{\mathcal{O}}$ is quasi-real of type 4.

We will prove that:

- $\mathcal{O}$ is quasi-real of type 4,
- there exist $r_0, s_0 \in \mathcal{O}$ such that $r_0 \triangleright (s_0 \triangleright (r_0 \triangleright s_0)) \neq s_0$.

For the first item, we write $\tau = (v, \alpha) \in (\mathbb{Z}/M)^N \rtimes \mathbb{A}_N$. Since $|\tau| = N$, $(\alpha)_N(v) = 0$, where $(\alpha)_N := \mathrm{id} + \alpha + \alpha^2 + \cdots + \alpha^{N-1}$, and $|\alpha| = N$, i. e. a N-cycle in $\mathbb{A}_N$, because N is prime. Let $\beta \in \mathbb{A}_N$ such that $\beta \triangleright \alpha = \alpha^4$. We will show that there exists $u \in (\mathbb{Z}/M)^N$ such that $(u, \beta) \triangleright (v, \alpha) = (v, \alpha)^4$. The last amounts to $(\alpha)_4 v - \beta v = (\mathrm{id} - \alpha^4)u$ for some $u \in (\mathbb{Z}/M)^N$. Notice that $\operatorname{Im}(\mathrm{id} - \alpha^4) = \ker((\alpha^4)_N) = \ker((\alpha)_N)$. Thus $(\alpha)_4 v - \beta v \in \operatorname{Im}(\mathrm{id} - \alpha^4)$ if and only if $(\alpha)_N \beta v = 0$. But the last follows from $(\alpha)_N \beta = \beta(\alpha)_N$.

For the second item, let $r_0 := \tau = (v, \alpha)$. Observe that $s_0 := (v + (\mathrm{id} - \alpha)(u), \alpha) \in \mathcal{O}$ for any $u \in (\mathbb{Z}/M)^N$. Now

$$\begin{aligned}
((v,\alpha)(v + (\mathrm{id} - \alpha)(u), \alpha))^2 &= \left((\mathrm{id} + \alpha)(v) + (\alpha - \alpha^2)(u), \alpha^2\right)^2 \\
&= \left((\mathrm{id} + \alpha^2)(\mathrm{id} + \alpha)(v) + (\mathrm{id} + \alpha^2)(\alpha - \alpha^2)(u), \alpha^4\right) \\
((v + (\mathrm{id} - \alpha)(u), \alpha)(v, \alpha))^2 &= \left((\mathrm{id} + \alpha)(v) + (\mathrm{id} - \alpha)(u), \alpha^2\right)^2 \\
&= \left((\mathrm{id} + \alpha^2)(\mathrm{id} + \alpha)(v) + (\mathrm{id} + \alpha^2)(\mathrm{id} - \alpha)(u), \alpha^4\right).
\end{aligned}$$

Then $(r_0s_0)^2 = (s_0r_0)^2$ iff $(\mathrm{id}+\alpha^2)(\mathrm{id}-\alpha)^2(u) = 0$. Now the order of α is the odd prime N, hence there exists some u such that[3] $(\mathrm{id}+\alpha^2)(\mathrm{id}-\alpha)^2(u) \neq 0$; thus $(r_0s_0)^2 \neq (s_0r_0)^2$, that is $r_0 \triangleright (s_0 \triangleright (r_0 \triangleright s_0)) \neq s_0$.

Assume that $M > 3$. Now, $\widetilde{\mathcal{O}}$ is of type D by Proposition 3.9.

Assume that $M = 3$. We will see that there exists j such that $j \equiv 2 \mod 3$ and $\sigma^j \in \widetilde{\mathcal{O}}$. Let k be relative prime to m and $\lambda_k : \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ the map $i \mod m \mapsto ki \mod m$. We can think λ_k as a permutation of $\mathbb{S}_m$ in the obvious way. Then

$$\lambda_k \triangleright \sigma = \sigma^k. \tag{17}$$

Indeed, for all i, $1 \leq i \leq m$, we have

$$\begin{aligned}(\lambda_k \triangleright \sigma)(i) &= \lambda_k \sigma \lambda_k^{-1}(i) = \lambda_k \sigma(k^{-1}i \mod m) = \lambda_k(k^{-1}i + 1 \mod m)\\ &= k(k^{-1}i + 1) \mod m = i + k \mod m = \sigma^k(i).\end{aligned}$$

Claim 1 *The following are equivalent*:

$$\text{(a) } \sigma^k \in \widetilde{\mathcal{O}}, \quad \text{(b) } \operatorname{sgn}(\lambda_k) = 1, \quad \text{(c) } J(k, m) = 1,$$

where $J(k, m)$ means the Jacobi symbol of $k \mod m$.

Proof By (17) (a) is equivalent to $\lambda_k = \alpha\sigma^i$, for some $\alpha \in \mathbb{A}_m$ and $i \in \{0, \dots, m-1\}$. This condition amounts to $\lambda_k \in \mathbb{A}_m$, which means that (b) holds. [29, Th. 1] says that (b) is equivalent to (c). This last equivalence is Zolotarev's Lemma when $m > 2$ is prime – see [30]. □

Let $k \in \mathbb{Z}$ such that k is not a quadratic residue modulo N; it is well-known that there are $\frac{N-1}{2}$ of such k's with $1 \leq k \leq N-1$. By Chinese Remainder Theorem there exists j, with $0 \leq j < m$, such that $j \equiv 2 \mod 3$ and $j \equiv k \mod N$.Thus $J(j, 3) = -1 = J(j, N)$, and $J(j, m) = J(j, 3)J(j, N) = 1$. Hence, $j \equiv 2 \mod 3$ and $\sigma^j \in \widetilde{\mathcal{O}}$ as desired.

Now, $\tau^j = ((\alpha)_j v, \alpha^j) \notin \mathcal{O}$ because $\alpha^j \notin \mathcal{O}_\alpha^{\mathbb{A}_N}$. So, if we identify α with the N-cycle $(1\,2\,\cdots\,N)$ in $\mathbb{A}_N$ and $\widetilde{\alpha} := (1\,3) \triangleright \alpha$, then α^j and $\widetilde{\alpha}$ are conjugate in $\mathbb{A}_N$ and $(\alpha\widetilde{\alpha})^2 \neq (\widetilde{\alpha}\alpha)^2$. Set $r_0 = \tau, s_0 = (v, \widetilde{\alpha})$, $R = \mathcal{O} \cdot \kappa$, $S = \mathcal{O}^K_{\tau^j} \cdot \kappa^j = \mathcal{O}^K_{\tau^j} \cdot \kappa^{-1}$. Then $s_0 \in \mathcal{O}^K_{\tau^j}$, $(r_0s_0)^2 \neq (s_0r_0)^2$, $R \bigsqcup S$ is an indecomposable subrack of $\widetilde{\mathcal{O}}$ and $(rs)^2 \neq (sr)^2$, with $r = r_0\kappa = \sigma$ and $s = s_0\kappa^{-1}$. Therefore, $\widetilde{\mathcal{O}}$ is of type D.

Step 3 *The class of type (n, p) in $\mathbb{A}_{n+p}$ is of type D if both n and p are odd, $n \geq 3$ and $p \geq 5$.*

We take $\sigma_1 = (1\,2\cdots n)(n+1\;\, n+2\cdots n+p)$, $\sigma_2 = (1\;2)(n+1\;\, n+3) \triangleright \sigma_1$. Then consider the subgroup $H = \langle \sigma_1, \sigma_2 \rangle \subseteq \mathbb{A}_n \times \mathbb{A}_p$. Let $\pi : \mathbb{A}_n \times \mathbb{A}_p \to \mathbb{S}_p$ be the projection to the second component, and notice that $\pi(\sigma_1), \pi(\sigma_2)$ belong to different conjugacy classes in $\mathbb{A}_p$. Then, $(\sigma_1\sigma_2)^2 \neq (\sigma_2\sigma_1)^2$ and they are not conjugate in H, since both statements hold in $\pi(H)$.

Step 4 *If the type of σ is $(1^2, j)$ with $j > 5$ odd, then $\mathcal{O}$ is of type D.*

The class $\mathcal{O}_j^{\mathbb{S}_j}$ splits as a union $\mathcal{O}_1 \bigsqcup \mathcal{O}_2$ of 2 classes in $\mathbb{A}_j$; if $R = \mathcal{O}_1 \times \{(j+1)(j+2)\}$, $S = \mathcal{O}_2 \times \{(j+1)(j+2)\}$, then $Y = R \bigsqcup S$ is a subrack of $\mathcal{O}$ and satisfies (6) since it generates the subgroup $\mathbb{A}_j$.

[3] Here one may simply work in a vector space over some quotient field of $\mathbb{Z}/M$.

Table 1 Some classes of type D from the literature

Type	Subrack	Reference
$(1, 2, \sigma_o), \sigma_o \neq \mathrm{id}$	$\mathfrak{D}_3^{(2)}$	[3, Ex. 3.9]
$(2^3, \sigma_o), \sigma_o \neq \mathrm{id}$	$\mathfrak{D}_3^{(2)}$	[3, Ex. 3.12]
$(4, \sigma_o), \sigma_o \neq \mathrm{id}$	$\mathfrak{O}^{(2)}$	[5, Prop. 3.7]
(4^2)	$\mathfrak{O}^{(2)}$	[5, Proof of Prop. 3.5]

Step 5 *If the type of σ is as in Table 1, then $\mathcal{O}$ is of type D.*

This follows from previous works as explained in Table 1.

Step 6 *If the type of σ is $(2, j)$, where $j > 3$ is odd, then $\mathcal{O}$ is of type D.*

Choose $\sigma = (1\,2)(3\,4\,5\,6\cdots j+2)$. Set $\sigma_1 = \sigma, h = (3\,5)$ and $\sigma_2 = h \triangleright \sigma$. Then, $\sigma_2 = (1\,2)(5\,4\,3\,6\cdots j+2)$. We claim

(a) $(\sigma_1\sigma_2)^2 \neq (\sigma_2\sigma_1)^2$.
(b) $H := \langle \sigma_1, \sigma_2 \rangle \simeq \mathbb{Z}/2 \times \mathbb{A}_j$.
(c) The conjugacy classes of σ_1 and σ_2 in H are distinct.

(a) follows since $(\sigma_2\sigma_1)^2(3) = 3$, whereas $(\sigma_1\sigma_2)^2(3) = 4$ if $j = 5$ and $(\sigma_1\sigma_2)^2(3) = 9$ if $j \geq 7$. (b) follows because the j-cycles $(3\,4\,5\,6\cdots j+2)$ and $(5\,4\,3\,6\cdots j+2)$ generate $\mathbb{A}_I$, $I = \{3, 4, 5, \ldots, j+2\}$. (c) follows since the conjugacy class of one cycle of odd length splits into two classes in $\mathbb{A}_I$.

Step 7 *If the type of σ is $(2, 3^2)$, then $\mathcal{O}$ is of type D.*

The set formed by $\sigma_1 = (1\,2\,3)(4\,5\,6)(7\,8)$, $\sigma_2 = (1\,6\,3)(2\,4\,5)(7\,8)$, $\sigma_3 = (1\,6\,4)(2\,3\,5)(7\,8)$ and $\sigma_4 = (1\,2\,4)(3\,5\,6)(7\,8)$, is the affine rack associated to the tetrahedron, i.e. $\mathsf{Q}^1_{\mathbb{F}_2^2,T}$ with $|T| = 3$. The Step follows from Ex. 3.18.

Step 8 *If the type of σ is $(1, 4)$, then $\mathcal{O}$ is of type D.*

The group $H = \mathbb{F}_5 \rtimes \mathbb{F}_5^\times \simeq \mathbb{F}_5 \rtimes \mathbb{Z}/4$ acts on $\mathbb{F}_5$ by translations and dilations; if we identify $\{1, \ldots, 5\}$ with $\mathbb{F}_5$, then the translation by 1 is the 5-cycle $(1\,2\,3\,4\,5)$, the dilation by 2 is σ and H is isomorphic to a subgroup of $\mathbb{S}_5$. Thus $\mathcal{O}$ contains a subrack isomorphic to $\mathsf{Q}^1_{\mathbb{F}_5,T}$ with $|T| = 4$. The Step follows from Ex. 3.18.

Step 9 *If the type of σ is $(2, 4)$, then $\mathcal{O}$ is of type D.*

Let H be the subgroup of $\mathbb{A}_6$ generated by $(1\,3\,6)$, $(2\,4\,5)$ and σ. Since $(1\,3\,6)$ and $(2\,4\,5)$ span a subgroup isomorphic to $\mathbb{F}_3^2$, $\sigma \triangleright (1\,3\,6) = (2\,4\,5)$ and $\sigma \triangleright (2\,4\,5) = (1\,6\,3)$, we conclude that H is isomorphic to $\mathbb{F}_3^2 \rtimes \langle T \rangle$, where $T^2 = -\mathrm{id}$. Thus $\mathcal{O}$ contains a subrack isomorphic to $\mathsf{Q}^1_{\mathbb{F}_3^2,T}$ with $|T| = 4$. The Step follows from Ex. 3.18.

Step 10 *If the type of σ is as in Table 2, then $\mathcal{O}$ is of type D.*

We list σ_1, σ_2 and $H = \langle \sigma_1, \sigma_2 \rangle$ in Table 2; a straightforward computation shows that $(\sigma_1\sigma_2)^2 \neq (\sigma_2\sigma_1)^2$ and that the conjugacy classes of σ_1 and σ_2 in H are distinct.

Table 2 Some classes of type D in $\mathbb{A}_m$ or $\mathbb{S}_m$

$\mathcal{O}$	σ_1	σ_2	$H = \langle \sigma_1, \sigma_2 \rangle$
$(1^3, 2^2)$	(4 5)(6 7)	(1 2)(3 7)	$\mathbb{D}_6$
$(1, 3^2)$	(2 3 4)(5 6 7)	(1 2 5)(3 4 6)	$\mathbb{Z}/7 \rtimes \mathbb{Z}/3$
(3^3)	(1 2 3)(4 5 6)(7 8 9)	(1 2 4)(3 5 6)(7 9 8)	$\mathbb{A}_4 \times \mathbb{Z}/3$
(2^5)	(1 2)(3 4)(5 6)(7 8)(9 10)	(1 3)(2 4)(5 7)(6 9)(8 10)	$\mathbb{D}_6$
$(1, 2^3)$	(2 3)(4 5)(6 7)	(1 6)(2 4)(3 5)	$\mathbb{D}_6$

Final Step. Assume now that $\mathcal{O}$ is not of type D; we apply systematically Step 1. By Step 2, $n_j = 0$ if $j \geq 6$ is not prime.

Assume that $n_4 \neq 0$; then σ is of type $(1^{n_1}, 2^{n_2}, 4)$ by Step 5. But $n_1 = 0$ by Step 8 and $n_2 = 0$ by Step 9; a contradiction since $m = \sum_j j\, n_j \geq 5$. Hence, $n_4 = 0$.

Assume that $n_3 \neq 0$; then σ is of type $(1^{n_1}, 2^{n_2}, 3^{n_3})$ by Step 3, and either $n_1 = 0$ or else $n_2 = 0$ by Step 5. In fact, if both $n_1 > 0$ and $n_2 > 0$, then $\mathcal{O}$ is of type D by the first line in Table 1. If $n_1 = 0$, then $n_3 = 1$ by Step 7 and $n_2 \leq 2$ by Step 5; in other words, only types $(2, 3)$ and $(2^2, 3)$ remain. If $n_2 = 0$, then type (3^2) remains, by Step 10. Also, if $n_1 \neq 0$ and $n_2 = 0$, then type $(1^{n_1}, 3)$ remains, by Step 10.

Assume next that $n_3 = 0$; then σ is of type $(1^{n_1}, 2^{n_2}, j^{n_j})$ by Step 3, with $j \geq 5$ prime and $n_j = 0$ or 1. Furthermore, $n_2 \leq 4$ by Step 10.

If $n_j = 0$ and $n_1 \neq 0$, then $n_2 \leq 2$ by Step 10; but $n_2 = 2$ implies $n_1 \leq 2$ by Step 10. In other words, only types (2^3), (2^4), $(1, 2^2)$, $(1^2, 2^2)$ and $(1^n, 2)$ remain.

If $n_j = 1$, then either $n_1 = 0$ or else $n_2 = 0$ by Step 5. The possibility $n_2 \neq 0$ is excluded by Step 6. Thus $n_2 = 0$, hence $n_1 \leq 1$ by Step 4; thus, only types (j) and $(1, j)$, with $j \geq 5$ prime, remain. □

Remark 4.2 The remaining conjugacy classes do not have enough bad subracks to arrive to similar conclusions, except (p) and $(1, p)$ where we do not have enough information yet, as said. We list the proper subracks generated by two elements in these classes:

(a) The proper subracks of the class of type $(1^{m-2}, 2)$ in $\mathbb{S}_m$ are all of the form $\mathcal{O}_2^{m_1} \coprod \mathcal{O}_2^{m_2} \coprod \cdots \coprod \mathcal{O}_2^{m_s}$; $\mathcal{O}_2^{m_i}$ commutes with $\mathcal{O}_2^{m_j}$ if $i \neq j$.
(b) The proper subracks generated by two elements of the class of type $(1^n, 3)$ are either abelian, or isomorphic to the racks of the vertices of a tetrahedron, or a cube, or a dodecahedron. The same for the class of type (3^2).
(c) The proper subracks of the class of type $(2, 3)$ are abelian with either one or two elements.
(d) The proper subracks of the class of type $(1, 2^2)$ are abelian racks and dihedral racks with 3 and 5 elements.
(e) The proper subracks generated by two elements of the class of type $(1^2, 2^2)$ are abelian racks and dihedral racks with 3, 4 and 5 elements.
(f) The proper subracks generated by two elements of the class of type (2^4) are abelian racks and dihedral racks with 3 and 4 elements.
(g) The proper subracks generated by two elements of the class of type $(2^2, 3)$ are either abelian racks or indecomposable with 20 elements.

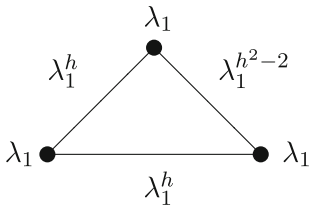

Fig. 1 Generalized Dynkin diagram of the braided vector space given in Lemma 4.3

We were not able to find out in general whether or not the classes $(1, p), (p)$ with p prime, are of type D. For instance, the classes (5), (7), (11) are not of type D, while the classes (13), (17) and (31) are of type D.

Also, the classes (1, 5), (1, 11) are not of type D, while the class (1, 7) is of type D. More generally, if $p = 2^h - 1$ is a Mersenne prime, then $(1, p)$ is of type D. For, set $q = 2^h$; then, the group $H = \mathbb{F}_q \rtimes \mathbb{F}_q^\times \simeq \mathbb{F}_q \rtimes \mathbb{Z}/p$ acts on $\mathbb{F}_q$ by translations and dilations; if we identify $\{1, \dots, q\}$ with $\mathbb{F}_q$, then H is isomorphic to a subgroup of $\mathbb{S}_q$.

4.3 An abelian subrack with 3 elements

To deal with the remaining cases, we apply techniques of abelian subracks. We begin by recording a result that is needed in Lemma 4.4.

Lemma 4.3 *Let G be a finite group and $\mathcal{O}$ be the conjugacy class of σ_1 in G. Let $\sigma_2 \neq \sigma_3 \in \mathcal{O} - \{\sigma_1\}$; let $g_1 = e, g_2, g_3 \in G$ such that $\sigma_i = g_i \sigma_1 g_i^{-1}$, for all i. Assume that*

- *$\sigma_1^h = \sigma_2\sigma_3$ for an odd integer h,*
- *g_3g_2 and g_2g_3 belong to $C_G(\sigma_1)$, and*
- *$\sigma_i\sigma_j = \sigma_j\sigma_i$, $1 \leq i, j \leq 3$.*

Then $\dim \mathfrak{B}(\mathcal{O}, \rho) = \infty$, for any $\rho \in \widehat{C_G(\sigma_1)}$.

Proof Since $\sigma_i\sigma_j = \sigma_j\sigma_i$, there exist $w \in V\backslash\{0\}$ and $\lambda_i \in \mathbb{C}$ such that $\rho(\sigma_i)(w) = \lambda_i w$ for $i = 1, 2, 3$. For any $1 \leq i, j \leq 3$, we call $\gamma_{ij} = g_j^{-1}\sigma_i g_j$. It is easy to see that $\gamma_{ij} \in C_G(\sigma_1)$ and that

$$\gamma = (\gamma_{ij}) = \begin{pmatrix} \sigma_1 & \sigma_3 & \sigma_2 \\ \sigma_2 & \sigma_1 & \sigma_2^h\sigma_1^{-1} \\ \sigma_3 & \sigma_3^h\sigma_1^{-1} & \sigma_1 \end{pmatrix}.$$

Then, $W = \operatorname{span}\{g_1w, g_2w, g_3w\}$ is a braided vector subspace of $M(\mathcal{O}, \rho)$ of abelian type with Dynkin diagram given by Fig. 1. Assume that $\dim \mathfrak{B}(\mathcal{O}, \rho)$ is finite. Then $\lambda_1 \neq 1$; also $\lambda_1^h \neq 1$, for otherwise g_2w, g_3w span a braided vector subspace of Cartan type with Dynkin diagram $A_1^{(1)}$. Thus, we should have $\lambda_1 = -1$ and h even, by [22, Table 2], but this is a contradiction to the hypothesis that h is odd. □

Lemma 4.4 (i) *Let $r \geq 1$ be odd and let $G = \mathbb{A}_4 \times \mathbb{Z}/r$, where $\mathbb{Z}/r$ is the cyclic group of order r, generated by τ. Let $\mathcal{O}$ be the conjugacy class of $\sigma = ((1\ 2)(3\ 4), \tau)$ in G. Then, $\dim \mathfrak{B}(\mathcal{O}, \rho) = \infty$ for every $\rho \in \widehat{C_G(\sigma)}$.*

(ii) *Let $m \geq 5$ and let $\sigma \in \mathbb{A}_m$ be of type $(1^{n_1}, 2^{n_2}, \sigma_o)$, $\mathcal{O}$ the conjugacy class of σ in $\mathbb{A}_m$ and $\rho = (\rho, V) \in \widehat{C_{\mathbb{A}_m}(\sigma)}$. Then $\dim \mathfrak{B}(\mathcal{O}, \rho) = \infty$.*

Proof For the first part, apply Lemma 4.3 with $\sigma_1 = ((1\ 2)(3\ 4), \tau)$, $\sigma_2 = ((1\ 3)(2\ 4), \tau)$, $\sigma_3 = ((1\ 4)(2\ 3), \tau)$, $g_1 = e$, $g_2 = ((1\ 3\ 2), 1)$, $g_3 = g_2^{-1}$ and $h = r + 2$.

We prove now the second part. Notice that the result follows from [2, Th. 2.3] if $n_2 = 0$. Otherwise, $n_2 = 2k$ is even and positive. Let r be the order of σ_o. We claim $\mathbb{A}_4 \times \mathbb{Z}/r$ embeds into $\mathbb{A}_m$ in such a way that the class of $((1\ 2)(3\ 4), \tau) \in \mathbb{A}_4 \times \mathbb{Z}/r$ is mapped into the class of type $(1^{n_1}, 2^{n_2}, \sigma_o)$ in $\mathbb{A}_m$. For this, just take σ to be of type σ_o, acting on indices $\{n_1 + 2n_2 + 1, \dots, m\}$, and $\alpha : \mathbb{Z}/r \to \mathbb{A}_m$, $\alpha(\tau) = \sigma$. Let $\delta : \mathbb{A}_4 \to (\mathbb{A}_4)^k$ be the diagonal map, and consider $(\mathbb{A}_4)^k$ as a subgroup of $\mathbb{A}_m$ acting on indices $\{n_1 + 1, \dots, n_1 + 2n_2\}$. Then, $\delta \times \alpha : \mathbb{A}_4 \times \mathbb{Z}/4 \to (\mathbb{A}_4)^k \times \mathbb{A}_{m-n_1-2n_2} \subseteq \mathbb{A}_m$, is the claimed map. □

Remark 4.5 The case $r = 1$ of this Lemma is known (see for example [2, Prop. 2.4]) and it is used to kill the conjugacy class of involutions in $\mathbb{A}_4$.

4.4 Proof of Theorem 1.1

Let $\sigma \in \mathbb{A}_m$; if $\mathcal{O}_\sigma^{\mathbb{A}_m}$ is of type D, then $\mathcal{O}_\sigma^{\mathbb{S}_m}$ is of type D. Then Th. 1.1 follows from Th. 4.1 and previous results:

(i) (p) in $\mathbb{S}_p$, $(1, p)$ in $\mathbb{S}_{1+p}$ (with p odd prime), $(1^n, 3)$ in $\mathbb{S}_{n+3}$, (3^2) in $\mathbb{S}_6$: discarded by [11, Th. 1].
(ii) $(1, 2^2)$ in $\mathbb{S}_5$, $(1^2, 2^2)$ in $\mathbb{S}_6$, $(2^2, 3)$ in $\mathbb{S}_7$: discarded by [11, Th. 1].
(iii) (2^4) in $\mathbb{S}_8$: discarded by [1, Th. 1 (B) (i)].
(iv) The restrictions on the representations of the remaining classes have been explained in [5].

4.5 Proof of Theorem 1.2

It follows from Theorem 4.1 and the following considerations:

(i) (p) in $\mathbb{A}_p$, $(1, p)$ in $\mathbb{A}_{1+p}$ (with p odd prime), $(1^n, 3)$ in $\mathbb{A}_{n+3}$, (3^2) in $\mathbb{A}_6$: discarded by [2, Th. 2.3].
(ii) $(2^2, 3)$ in $\mathbb{A}_7$, (2^4) in $\mathbb{A}_8$, $(1^2, 2^2)$ in $\mathbb{A}_6$, $(1, 2^2)$ in $\mathbb{A}_5$: discarded by Lemma 4.4 (ii).

Acknowledgments We have used [17] to perform some computations. Part of the work of F. F. was done during a visit to the Universidad de Almería (supported by Dpto. Álgebra y Análisis Matemático, Univ. de Almería and the CONICET); he is grateful to J. Cuadra by his hospitality. Part of the work of N. A. was done during a visit to the University of Munich (the travel was supported by the Mathematisches Institut); he is grateful to H.-J. Schneider and S. Natale by their hospitality.

References

1. Andruskiewitsch, N., Fantino, F.: On pointed Hopf algebras associated with unmixed conjugacy classes in $\mathbb{S}_m$. J. Math. Phys. **48**, 033502-1–033502-26 (2007)
2. Andruskiewitsch, N., Fantino, F.: On pointed Hopf algebras associated with alternating and dihedral groups. Rev. Unión Mat. Argent **48-3**, 57–71 (2007)
3. Andruskiewitsch, N., Fantino, F.: New techniques for pointed Hopf algebras. Contemp. Math. **491**, 323–348 (2009)
4. Andruskiewitsch, N., Fantino, F., Graña M., Vendramin L.: Pointed Hopf algebras over the sporadic simple groups. preprint arXiv:1001.1108v1
5. Andruskiewitsch, N., Fantino, F., Zhang, S.: On pointed Hopf algebras associated with the symmetric groups. Manuscr. Math. **128**, 359–371 (2009)
6. Andruskiewitsch, N., Graña, M.: From racks to pointed Hopf algebras. Adv. Math. **178**, 177–243 (2003)
7. Andruskiewitsch, N., Heckenberger, I., Schneider, H.-J.: The Nichols algebra of a semisimple Yetter-Drinfeld module. preprint arXiv:0803.2430v1

8. Andruskiewitsch, N., Schneider, H.-J.: Finite quantum groups and Cartan matrices. Adv. Math. **54**, 1–45 (2000)
9. Andruskiewitsch, N., Schneider, H.-J.: Pointed Hopf Algebras. In: New directions in Hopf algebras, pp. 1–68. Math. Sci. Res. Inst. Publ. vol. 43. Cambridge Univ. Press, Cambridge (2002)
10. Andruskiewitsch, N., Schneider, H.-J.: Finite quantum groups over abelian groups of prime exponent. Ann. Sci. Ec. Norm. Super. **35**, 1–26 (2002)
11. Andruskiewitsch, N., Zhang, S.: On pointed Hopf algebras associated to some conjugacy classes in $\mathbb{S}_n$. Proc. Am. Math. Soc. **135**, 2723–2731 (2007)
12. Etingof, P., Graña, M.: On rack cohomology. J. Pure Appl. Alg. **177**, 49–59 (2003)
13. Fantino, F.: Álgebras de Hopf punteadas sobre grupos no abelianos. Tesis de doctorado, Universidad de Córdoba (2008). http://www.mate.uncor.edu/~fantino/
14. Fomin, S., Kirillov, K.N.: Quadratic algebras, Dunkl elements, and Schubert calculus. Progr. Math. **172**, 146–182 (1999)
15. Freyre, S., Graña, M., Vendramin, L.: On Nichols algebras over $\mathbf{GL}(2, \mathbb{F}_q)$ and $\mathbf{SL}(2, \mathbb{F}_q)$. J. Math. Phys. 48:123513-1–123513-11 (2007)
16. Freyre, S., Graña, M., Vendramin, L.: On Nichols algebras over $\mathbf{PSL}(2, q)$ and $\mathbf{PGL}(2, q)$. J. Algebra Appl. **9**, 195–208 (2010)
17. The GAP Group, GAP—Groups, Algorithms, and Programming, Version 4.4.12 (2008). http://www.gap-system.org
18. Graña, M.: Finite dimensional Nichols algebras of non-diagonal group type, zoo of examples available at http://mate.dm.uba.ar/~matiasg/zoo.html
19. Graña, M.: On Nichols algebras of low dimension. Contemp. Math. **267**, 111–134 (2000)
20. García, G.A.: García Iglesias, A. Finite dimensional pointed Hopf algebras over $\mathbb{S}_4$, Israel J. Math. (to appear), preprint arXiv:0904.2558
21. Graña M., Vendramin L.: RiG, A GAP package for racks and Nichols Algebras, available at http://mate.dm.uba.ar/~lvendram
22. Heckenberger, I.: Classification of arithmetic root systems of rank 3, Actas del "XVI Coloquio Latino-americano de Álgebra" Colonia, Uruguay, pp. 227–252. Biblio. Rev. Iber. Matemática (2005)
23. Heckenberger, I.: Classification of arithmetic root systems. Adv. Math. **220**, 59–124 (2009)
24. Heckenberger, I., Schneider, H.-J. Root systems and Weyl groupoids for semisimple Nichols algebras, Proc. London Math. Soc. doi:10.1112/plms/pdq001
25. Joyce, D.: Simple quandles. J. Algebra **79**(2), 307–318 (1982)
26. Janusz, G., Rotman, J.: Outer Automorphisms of $\mathbb{S}_6$. Am. Math. Monthly **89**(6), 407–410 (1982)
27. Milinski, A., Schneider, H.-J.: Pointed Indecomposable Hopf Algebras over Coxeter Groups. Contemp. Math. **267**, 215–236 (2000)
28. Jean-Pierre, S.: Linear representations of finite groups. Springer, Berlin (1977)
29. Szyjewski, M.: Zolotarev's proof of Gauss reciprocity and Jacobi symbols, preprint http://www.math.us.edu.pl/~szyjewski/Preprints/Zolotarew.pdf
30. Zolotarev, G.: Nouvelle démonstration de la loi de réciprocité de Legendre. Nouv. Ann. Math. **2**(11), 354–362 (1872)