ON NICHOLS ALGEBRAS OVER $\mathbf{SL}(2, \mathbb{F}_q)$ AND $\mathbf{GL}(2, \mathbb{F}_q)$

SEBASTIÁN FREYRE, MATÍAS GRAÑA, AND LEANDRO VENDRAMIN

Abstract. We compute necessary conditions on Yetter-Drinfeld modules over the groups $\mathbf{SL}(2, \mathbb{F}_q)$ and $\mathbf{GL}(2, \mathbb{F}_q)$ to generate finite dimensional Nichols algebras. This is a first step towards a classification of pointed Hopf algebras with a group of group-likes isomorphic to one of these groups.

1. Introduction

Hopf algebras and their variants appear in many contexts; Quantum Groups [Dri], Rational and Logarithmic Conformal Field Theories [PZ, Gab], Quantum Field Theories [Bro] come to mind. This paper is part of the long problem of classifying pointed Hopf algebras. To this end, the best tool known so far is the so called "Lifting procedure" [AS]. The main ingredient of the Lifting procedure are Nichols algebras on Yetter-Drinfeld modules over group algebras. The classification of finite dimensional Nichols algebras over group algebras turns out to be a hard problem: when one restricts the attention to abelian groups, it includes the classification of semisimple Lie algebras [Hec2]; when one considers non-abelian groups, only a few (genuine) examples are known [Gra1] and we possess a very limited amount of general results (see [AG2] for an account).

In last years, two main directions were pursued to classify finite dimensional pointed Hopf algebras over non-abelian groups. One of them is to generate Nichols algebras by means of racks and 2-cocycles [AG2], getting examples that can be present for many groups. The other one is to concentrate on certain (families of) groups and classify which finite dimensional Nichols algebras can appear. In the last vein, let us cite the recently appeared papers: [AZ, AF2, AF1] (where symmetric groups are considered). The present paper can be thought of as an analog of these, but for some finite groups of Lie type: $\mathbf{GL}(2, \mathbb{F}_q)$ and $\mathbf{SL}(2, \mathbb{F}_q)$. As in those papers, using the tools in [Hec2] we are able to rule out most of the Yetter-Drinfeld modules over these groups, as they generate infinite dimensional Nichols algebras.

After applying these techniques, the cases we are left with are difficult and one needs stronger tools to compute them. As an example, we point out that when $q = 5$, the conjugacy classes $\mathcal{C}_i$ $(i = 3, \dots, 6)$ in Table 2 are isomorphic as racks to that of the faces of a dodecahedron, while one of the two classes $\mathcal{C}_8$ is isomorphic to the rack of the faces of an icosahedron (see [Gra1]). The Nichols algebras generated by these racks with a negative 2-cocycle are not yet known.

One of the main results of this paper is the following theorem concerning Nichols algebras over the group $\mathbf{SL}(2, \mathbb{F}_q)$:

2000 *Mathematics Subject Classification.* 16W30.

This work was partially supported by CONICET and ANPCyT (Argentina).

Theorem. *If the Nichols algebra $\mathfrak{B}(\mathcal{C})$ associated to a conjugacy class $\mathcal{C}$ of the group $\mathbf{SL}(2,\mathbb{F}_q)$ is finite dimensional then q is odd and $\mathcal{C}$ is one of the classes $\mathcal{C}_i$ of the table 2 for $i = 2, 5, 6, 7, 8$.*

Necessary conditions over the representations are explicitly given in propositions 3.3, 3.4, 3.5 and 3.9.

In section 4 we analyze Nichols algebras over $\mathbf{GL}(2,\mathbb{F}_q)$ and as a consequence we obtain necessary conditions over the representations to get finite-dimensional Nichols algebras over this group.

2. Preliminaries and conventions

2.1. **Yetter Drinfeld modules over kG.** In what follows G is a finite group and k is an algebraically closed field of characteristic 0. Recall that a kG-comodule V is just a G-graded vector space: $V = \oplus_{g\in G} V_g$, where $V_g = \{v \in V \mid \delta(v) = g \otimes v\}$. A Yetter-Drinfeld module over kG is a left kG-module and a left kG-comodule V satisfying the following compatibility condition

$$\delta(g \cdot v) = ghg^{-1} \otimes g \cdot v, \quad \text{for } v \in V_h$$

We denote by ${}^{kG}_{kG}\mathcal{YD}$ the category of Yetter-Drinfeld modules over kG, the morphisms of which are the maps of modules and comodules. This is a braided category, with braiding given by

$$c_{M,N} : M \otimes N \to N \otimes M, \quad c(m \otimes n) = gn \otimes m, \quad \text{for } m \in M_g. \tag{1}$$

Let $g \in G$. We write $\mathcal{Z}_g$ for the centralizer $\mathcal{Z}_g = \{x \in G \mid xgx^{-1} = g\}$. We write $\mathcal{C}_g$ for the conjugacy class $\mathcal{C}_g = \{xgx^{-1} \mid x \in G\}$. Let $\rho : \mathcal{Z}_g \to \mathrm{GL}(W)$ be a representation. We denote by $V(g,\rho)$ the space $\mathrm{Ind}^G_{\mathcal{Z}_g}\rho$, endowed with the comodule structure $\delta(h \otimes w) = ghg^{-1} \otimes (h \otimes w)$. It is folklore that $V(g,\rho)$ is irreducible iff ρ is, that ${}^{kG}_{kG}\mathcal{YD}$ is semisimple iff kG is, and that in this case the simple modules are given by $V(g,\rho)$, letting g run over representatives of conjugacy classes and ρ on irreducible representations of $\mathcal{Z}_g$. In this work we need only to consider representations of degree 1 since all the centralizers we have to deal with are abelian.

Let $\mathcal{C} = \mathcal{C}_g = \{g_i \mid i \in I\}$ be the conjugacy class of g, with $g_i = x_i g x_i^{-1}$, and let $v_i = x_i \otimes 1 \in V(g,\chi)$, where $\chi = \rho \in \widehat{\mathcal{Z}_g}$ is a character. Let $T \subseteq I$ be a subset such that $g_i g_j = g_j g_i$ for all $i, j \in T$. Let $V_T \subseteq V(g,\chi)$ be the subspace generated by $\{v_i \mid i \in T\}$. Then the braiding restricted to V_T is of *diagonal type*, given by

$$c(v_i \otimes v_j) = \mathbf{q}_{ij} v_j \otimes v_i, \quad \text{where } \mathbf{q}_{ij} = \chi(x_j^{-1} g_i x_j) \in k. \tag{2}$$

Indeed, by (1), if $v_j = x_j \otimes w$, we have

$$\begin{aligned} c(v_i \otimes v_j) &= g_i v_j \otimes v_i = (x_j x_j^{-1} g_i x_j \otimes w) \otimes v_i \\ &= (x_j \otimes x_j^{-1} g_i x_j w) \otimes v_i = (x_j \otimes \mathbf{q}_{ij} w) \otimes v_i, \end{aligned}$$

since $x_j^{-1} g_i x_j \in \mathcal{Z}_g$.

We write $\mathbf{q} = \mathbf{q}_T = (\mathbf{q}_{ij})$. If $T \subseteq I$ and $T' \subseteq \mathcal{C}$, $T' = \{g_i \mid i \in T\}$, then we abuse notation by calling $\mathbf{q}_{T'} = \mathbf{q}_T$ and $V_{T'} = V_T$.

2.2. **Notations.** Throughout the paper, p will stand for a prime number and q for a power of p.

If $\rho = \chi$ is a character of $\mathcal{Z}_g$, we usually write the Nichols algebra generated by the Yetter-Drinfeld module $V(g,\rho)$ by $\mathfrak{B}(\mathcal{C},\chi)$ or just $\mathfrak{B}(\mathcal{C})$ when no confusion can arise.

If $n \in \mathbb{N}$, we write $\mathcal{R}_n \subset k$ for the set of primitive n-th roots of unity in k. The order of an element h in a group will be denoted by $|h|$.

We recall from [Hec2] the Dynkin diagram notation for braidings of diagonal type. If $\{v_1, \cdots, v_\ell\}$ is a basis of the braided vector space V and

$$c(v_i \otimes v_j) = \mathbf{q}_{ij} v_j \otimes v_i,$$

then the Dynkin diagram of c has one vertex for each $i = 1, \cdots, \ell$, and vertices i and j are joined by an edge iff $\mathbf{q}_{ij}\mathbf{q}_{ji} \neq 1$. Moreover, vertices and edges have labels as follows: the vertex i has as label the number $\mathbf{q}_{ii}$, while the edge between i and j (if any) has as label the number $\mathbf{q}_{ij}\mathbf{q}_{ji}$.

2.3. **Needed lemmas.**

Lemma 2.1. *Let W be a two-dimensional space with a braiding of diagonal type. Assume that the Dynkin diagram of W is given by* $\overset{\zeta}{\circ}\!\!-\!\!\overset{\mu}{}\!\!-\!\!\overset{\zeta}{\circ}$ *and suppose that* $\dim \mathfrak{B}(W) < \infty$. *Then the Dynkin diagram is among the following ones:*

Dynkin diagram	*fixed parameter*
$\overset{\alpha}{\circ}\quad\overset{\alpha}{\circ}$	$\alpha \in k^\times$
$\overset{\alpha}{\circ}\!\!-\!\!\overset{\alpha^{-1}}{}\!\!-\!\!\overset{\alpha}{\circ}$	$\alpha \neq 1$
$\overset{-1}{\circ}\!\!-\!\!\overset{\alpha}{}\!\!-\!\!\overset{-1}{\circ}$	$\alpha \neq \pm 1$
$\overset{-\alpha^{-2}}{\circ}\!\!-\!\!\overset{-\alpha^{3}}{}\!\!-\!\!\overset{-\alpha^{-2}}{\circ}$	$\alpha \in \mathcal{R}_{12}$
$\overset{-\alpha^{-2}}{\circ}\!\!-\!\!\overset{\alpha}{}\!\!-\!\!\overset{-\alpha^{-2}}{\circ}$	$\alpha \in \mathcal{R}_{12}$

Proof. This follows at once by inspection on [Hec1, Table 1] □

The following corollary appears in different forms in [AZ, AF2, AF1]. We prove it here for the reader's convenience.

Corollary 2.2.

(1) *Assume there exists $x \in G$ such that $xgx^{-1} = g^n \neq g$. Let $T = \{g, g^n\}$ and write $\frac{1}{n} = n^{-1} \pmod{|g|}$. Then $\mathbf{q} = \begin{pmatrix} \alpha & \alpha^{\frac{1}{n}} \\ \alpha^n & \alpha \end{pmatrix}$, $\alpha = \chi(g)$. If $\dim \mathfrak{B}(\mathcal{C},\rho) < \infty$ then $\alpha = -1$ or $\alpha \in \mathcal{R}_3$. If moreover $g^{n^2} \neq g$, then $\alpha = -1$.*

(2) *As a particular case, if $g^n = g^{-1}$ and $\dim \mathfrak{B}(\mathcal{C},\rho) < \infty$ then g has even order and $\mathbf{q} = \begin{pmatrix} -1 & -1 \\ -1 & -1 \end{pmatrix}$.*

Proof. We consider first the case $g^{n^2} = g$. After using Lemma 2.1 we obtain that $\alpha^{n+\frac{1}{n}} = 1$ or $\alpha^{n+\frac{1}{n}+1} = 1$. If $|\alpha|$ divides n^2+1 then, since $|\alpha|$ divides n^2-1, $\alpha = -1$ ($\alpha = 1$ would imply $\dim \mathfrak{B}(\mathcal{C},\rho) = \infty$). If $|\alpha| \mid n^2+n+1$ then $|\alpha|$ divides $n+2$ and then $\alpha \in \mathcal{R}_3$. Now we consider the case $g^{n^2} \neq g$, i.e. g, g^n and g^{n^2} are different and they belong to $\mathcal{Z}_g \cap \mathcal{C}_g$. Then, if $T = \{g, g^n, g^{n^2}\}$ we have

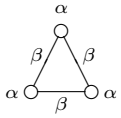
$$\mathbf{q}_T = \begin{pmatrix} \alpha & \alpha^{\frac{1}{n}} & \alpha^{\frac{1}{n^2}} \\ \alpha^n & \alpha & \alpha^{\frac{1}{n}} \\ \alpha^{n^2} & \alpha^n & \alpha \end{pmatrix}.$$

By inspection on [Hec1, Table 2], the only possibilities for $\mathbf{q}_T$ to produce a finite dimensional Nichols algebra are either

- $\alpha = -1$, or
- $\alpha^{\frac{1}{n}+n} = 1$ and $\alpha^{\frac{1}{n^2}+n^2} = 1$ (but then $\alpha = -1$), or
- $\alpha^{\frac{1}{n}+n} = 1$ and $\alpha^{\frac{1}{n^2}+n^2+1} = 1$ (but then $\alpha = 1$), or
- $\alpha^{\frac{1}{n^2}+n^2} = 1$ and $\alpha^{\frac{1}{n}+n+1} = 1$ (but then $\alpha = 1$).

This completes the proof. □

Lemma 2.3. (1) *Let W be a three-dimensional space with a braiding of diagonal type. Assume that the Dynkin diagram of W is*



and suppose that $\dim \mathfrak{B}(W) < \infty$. Then $\alpha = -1$ and $\beta \in \mathcal{R}_3$.

(2) *Suppose that the Dynkin diagram contains a cycle of length ≥ 4. Then $\dim \mathfrak{B}(W) = \infty$.*

Proof. The first part follows by inspection on [Hec1, Table 2], while the second is [Hec2, Lemma 20]. □

3. Nichols algebras over $\mathbf{SL}(2,\mathbb{F}_q)$

In this section, $E = \mathbb{F}_{q^2}$ will be the quadratic extension of $\mathbb{F}_q$ and $\overline{x}$ will be the Galois conjugate of $x \in E$. Recall that the order of $\mathbf{SL}(2,\mathbb{F}_q)$ is $(q-1)q(q+1)$. The conjugacy classes of $\mathbf{SL}(2,\mathbb{F}_q)$ ar given in Tables 1 and 2 (see [FH, §5.2] for q odd and [ZN] for q even).

3.1. **The case q even.** There are $q+1$ conjugacy classes divided in 4 types:

Table 1: Conjugacy classes in $\mathbf{SL}(2,\mathbb{F}_q)$, q even.

Type	Representative	Size	Number	Centralizer
$\mathcal{C}_1$	$I = c_1 = \begin{pmatrix} 1 & \\ & 1 \end{pmatrix}$	1	1	$\mathbf{SL}(2,\mathbb{F}_q)$
$\mathcal{C}_2$	$c_2 = \begin{pmatrix} 1 & 1 \\ & 1 \end{pmatrix}$	q^2-1	1	$\mathbb{F}_q$
$\mathcal{C}_3$	$c_3(x) = \begin{pmatrix} x & \\ & x^{-1} \end{pmatrix}$ $(x \neq 1)$	$q(q+1)$	$\frac{(q-2)}{2}$	$\mathbb{F}_q^\times$
$\mathcal{C}_4$	$c_4(x) = \begin{pmatrix} & 1 \\ 1 & x+\overline{x} \end{pmatrix}$ $(x \in E \setminus \mathbb{F}_q)$	$(q-1)q$	$\frac{q}{2}$	cyclic

We first consider the case $q = 2$. We have $\mathbf{SL}(2,\mathbb{F}_q) \simeq \mathbb{S}_3$. Nichols algebras generated by irreducible Yetter-Drinfeld modules over $\mathbb{S}_3$ were studied in [AG1]. They are infinite dimensional except for $\mathfrak{B}(\tau, \mathrm{sgn})$, which is 12-dimensional (here τ is a transposition and sgn is the non-trivial character of its centralizer).

We now consider the case $q > 2$.

Proposition 3.1. *Let $q = 2^n$ for $n \geq 2$. For each $i = 1, \dots, 4$ and for any representation χ of the centralizer of c_i, we have* $\dim \mathfrak{B}(\mathcal{C}_i, \chi) = \infty$.

Proof. We consider each class separately. The class $\mathcal{C}_1$ gives the trivial braiding. For $\mathcal{C}_2$, we take, for $a \in \mathbb{F}_q^\times$, $x_a = \begin{pmatrix} a & \\ & a^{-1} \end{pmatrix}$. Then $g_a = x_a c_2 x_a^{-1} = \begin{pmatrix} 1 & a^2 \\ & 1 \end{pmatrix}$. The centralizer of c_2 is the abelian group $\mathbb{F}_q$ embedded in $\mathbf{SL}(2,\mathbb{F}_q)$ as $\begin{pmatrix} 1 & \mathbb{F}_q \\ & 1 \end{pmatrix}$. If $\chi : \mathbb{F}_q \to \mathbb{C}$ is a character of the centralizer, we get $\mathbf{q}_{ab} = \chi(x_b^{-1} g_a x_b) = \chi(g_{ab^{-1}})$, whence $\mathbf{q}_{ab}\mathbf{q}_{ba} = \chi \begin{pmatrix} 1 & a^2b^{-2} + a^{-2}b^2 \\ & 1 \end{pmatrix}$ (we write $\mathbf{q}_{uv}$ for $\mathbf{q}_{g_u g_v}$). Since $q = 2^n$, χ takes values on ± 1. If $\mathbf{q}_{aa} = 1$, then $\dim \mathfrak{B}(\mathcal{C}_2, \chi) = \infty$, so we may assume $\mathbf{q}_{aa} = -1$.

If there exists $a \in \mathbb{F}_q \setminus \{0, 1\}$ such that $\chi \begin{pmatrix} 1 & a^2 + a^{-2} \\ & 1 \end{pmatrix} = -1$, then we get

$$\mathbf{q}_{1,a}\mathbf{q}_{a,1} = \mathbf{q}_{a,a^2}\mathbf{q}_{a^2,a} = \cdots = \mathbf{q}_{a^m,1}\mathbf{q}_{1,a^m} = -1,$$

where $a^{m+1} = 1$. This implies that the space V_T contains a cycle of length $m \geq 3$ with edges labelled by -1, whence $\mathfrak{B}(\mathcal{C}_2, \chi)$ is infinite dimensional by Lemma 2.3. Assume then that $\chi \begin{pmatrix} 1 & a^2 + a^{-2} \\ & 1 \end{pmatrix} = 1$ for all $a \neq 0, 1$. But then, for all x in the subgroup generated by the elements of the form $a^2 + a^{-2}$ ($a \neq 0, 1$), we get $\chi \begin{pmatrix} 1 & x \\ & 1 \end{pmatrix} = 1$. Take now any $a \in \mathbb{F}_q \setminus \{0, 1\}$, and let r be the order of $a^2 + a^{-2}$. Since r is odd, $1 = (a^2 + a^{-2})^r$ is in the subgroup generated by elements $a^{2i} + a^{-2i}$ for $0 < i \leq r$, but this contradicts the fact that $\mathbf{q}_{aa} = \chi \begin{pmatrix} 1 & 1 \\ & 1 \end{pmatrix} = -1$.

For the class $\mathcal{C}_3$, the centralizer of $c_3(x)$ is the cyclic group $\mathbb{F}_q^\times$. It is easy to see that $c_3(x)$ and $c_3(x^{-1}) = c_3(x)^{-1}$ are conjugate, whence they both have the same odd order. Then by Corollary 2.2 (2), $\dim \mathfrak{B}(\mathcal{C}_3) = \infty$.

Finally, for the class $\mathcal{C}_4$, we have that the centralizer of $c_4(x)$ is a subgroup of the cyclic group $E^\times$, hence it is cyclic. Again, it is easy to see that both $c_4(x)$ and $c_4(x)^{-1} = \begin{pmatrix} x + \overline{x} & 1 \\ 1 & \end{pmatrix}$ are conjugate and they have odd order. Then, by Corollary 2.2 (2), $\dim \mathfrak{B}(\mathcal{C}_4) = \infty$. □

3.2. **The case q odd.** There are $q + 4$ conjugacy classes divided in 8 types, displayed in Table 2.

We first consider the case $q = 3$. The conjugacy class $\mathcal{C}_1$ in Table 2 gives infinite dimensional Nichols algebras. Class $\mathcal{C}_2$ gives either exterior algebras or infinite-dimensional algebras. Classes $\mathcal{C}_3$, $\mathcal{C}_4$, $\mathcal{C}_5$ and $\mathcal{C}_6$ give the rack of order 4 associated to the vertices of a tetrahedron (see [Gra2]). Class $\mathcal{C}_7$ is not present in this case, and class $\mathcal{C}_8$ gives an infinite dimensional Nichols algebra of diagonal type, after changing the basis in a similar way as in [Gra2, Remark 5.2.1].

Table 2: Conjugacy classes in $\mathbf{SL}(2,\mathbb{F}_q)$, q odd.

Type	Representative	Size	Number	Centralizer
$\mathcal{C}_1$	$c_1 = \begin{pmatrix} 1 & \\ & 1 \end{pmatrix}$	1	1	$\mathbf{SL}(2,\mathbb{F}_q)$
$\mathcal{C}_2$	$c_2 = \begin{pmatrix} -1 & \\ & -1 \end{pmatrix}$	1	1	$\mathbf{SL}(2,\mathbb{F}_q)$
$\mathcal{C}_3$	$c_3 = \begin{pmatrix} 1 & 1 \\ & 1 \end{pmatrix}$	$\frac{q^2-1}{2}$	1	$\mathbb{Z}_2 \times \mathbb{F}_q$
$\mathcal{C}_4$	$c_4 = \begin{pmatrix} 1 & x \\ & 1 \end{pmatrix}$ $(\sqrt{x} \notin \mathbb{F}_q)$	$\frac{q^2-1}{2}$	1	$\mathbb{Z}_2 \times \mathbb{F}_q$
$\mathcal{C}_5$	$c_5 = \begin{pmatrix} -1 & 1 \\ & -1 \end{pmatrix}$	$\frac{q^2-1}{2}$	1	$\mathbb{Z}_2 \times \mathbb{F}_q$
$\mathcal{C}_6$	$c_6 = \begin{pmatrix} -1 & x \\ & -1 \end{pmatrix}$ $(\sqrt{x} \notin \mathbb{F}_q)$	$\frac{q^2-1}{2}$	1	$\mathbb{Z}_2 \times \mathbb{F}_q$
$\mathcal{C}_7$	$c_7(x) = \begin{pmatrix} x & \\ & x^{-1} \end{pmatrix}$ $(x \neq \pm 1)$	$q(q+1)$	$\frac{(q-3)}{2}$	$\mathbb{F}_q^\times$
$\mathcal{C}_8$	$c_8(x) = \begin{pmatrix} & -1 \\ 1 & x+\overline{x} \end{pmatrix}$ $(x \in E \setminus \mathbb{F}_q)$	$(q-1)q$	$\frac{q-1}{2}$	cyclic

We now consider the case $q > 3$.

Remark 3.2. Conjugation by $\begin{pmatrix} x & \\ & 1 \end{pmatrix} \in \mathbf{GL}(2,\mathbb{F}_q)$ gives an automorphism of $\mathbf{SL}(2,\mathbb{F}_q)$ which switches $\mathcal{C}_3$ with $\mathcal{C}_4$, and $\mathcal{C}_5$ with $\mathcal{C}_6$. Hence, when classifying the irreducible Yetter-Drinfeld modules which produce finite dimensional Nichols algebras over $\mathcal{C}_3$, one automatically also classifies those over $\mathcal{C}_4$. Ditto for $\mathcal{C}_5$ and $\mathcal{C}_6$.

Furthermore, if one is only interested in the conjugacy classes *as racks*, it turns out that $\mathcal{C}_i$ $(i = 3, \dots, 6)$ are all isomorphic. Indeed, consider the projection $\mathbf{SL}(2,\mathbb{F}_q) \to \mathbf{PSL}(2,\mathbb{F}_q)$; it is injective when restricted to these classes. Further, it maps $\mathcal{C}_3$ and $\mathcal{C}_5$ to the same conjugacy class in $\mathbf{PSL}(2,\mathbb{F}_q)$ when -1 is a square in $\mathbb{F}_q$, and it maps $\mathcal{C}_3$ and $\mathcal{C}_6$ to the same conjugacy class when -1 is not a square in $\mathbb{F}_q$.

Proposition 3.3. $\dim \mathfrak{B}(\mathcal{C}_1) = \infty$. *If* $\dim \mathfrak{B}(\mathcal{C}_2) < \infty$, *then* $\mathfrak{B}(C_2)$ *is the exterior algebra.*

Proof. The first statement is clear since in this case the braiding is the usual flip $x \otimes y \mapsto y \otimes x$, and therefore the Nichols algebra is the symmetric algebra. In the second case, if $\chi(c_2) = 1$ we get again an infinite dimensional Nichols algebra. Thus, we must have $\chi(c_2) = -1$, and the braiding is given by $x \otimes y \mapsto -y \otimes x$, wich yields an exterior algebra. □

Proposition 3.4. *If* $\dim \mathfrak{B}(\mathcal{C}_7) < \infty$, *then* $\mathbf{q}_T = \begin{pmatrix} -1 & -1 \\ -1 & -1 \end{pmatrix}$ *and* x *has even order, where* $T = \{c_7(x), c_7(x^{-1})\}$ *(notice that* $c_7(x^{-1})$ *and* $c_7(x)$ *are conjugate).*

Proof. It follows from Corollary 2.2 (2). □

Proposition 3.5. *Let $x \in E \setminus \mathbb{F}_q$. Then $c_8(x)$ and $c_8(x)^{-1}$ are conjugate, and we take $T = \{c_8(x), c_8(x)^{-1}\}$. If $\dim \mathfrak{B}(\mathcal{C}_8) < \infty$, then $\mathbf{q}_T = \begin{pmatrix} -1 & -1 \\ -1 & -1 \end{pmatrix}$ (in particular, $c_8(x)$ has even order).*

Proof. The proof follows from Corollary 2.2 (2), once we see that $c_8(x)$ and $c_8(x)^{-1}$ are conjugate. To this end, we consider the quadratic form

$$\phi(u,v) = u^2 + uv(x+\overline{x}) + v^2$$

over $\mathbb{F}_q$. It is easy to see that this form has rank 2. Then, by [Ser, Proposition 4 (1.7)], it represents all elements of $\mathbb{F}_q^\times$ and in particular it represents -1. Thus, there exist $a, c \in \mathbb{F}_q$ such that $a^2 + ac(x+\overline{x}) + c^2 = -1$. This implies that $\begin{pmatrix} a & c + a(x+\overline{x}) \\ c & -a \end{pmatrix} \in \mathbf{SL}(2,\mathbb{F}_q)$. Furthermore,

$$\begin{pmatrix} a & c + a(x+\overline{x}) \\ c & -a \end{pmatrix} \begin{pmatrix} & -1 \\ 1 & x+\overline{x} \end{pmatrix} \begin{pmatrix} a & c + a(x+\overline{x}) \\ c & -a \end{pmatrix}^{-1} = \begin{pmatrix} x+\overline{x} & 1 \\ -1 & \end{pmatrix}$$

finishing the proof. □

Proposition 3.6. $\dim \mathfrak{B}(\mathcal{C}_3) = \infty$. *The same holds for $\mathfrak{B}(\mathcal{C}_4)$.*

Proof (case $q \neq 3^{2n+1}$). Let $\alpha = \chi(c_3)$ ($\chi \in \widehat{\mathbb{Z}_2 \times \mathbb{F}_q}$). First of all note that $|c_3| = p$. Thus, if $\dim \mathfrak{B}(\mathcal{C}_3) < \infty$, we may suppose that $|\alpha| = p$ (if $\alpha = 1$ then $\mathfrak{B}(\mathcal{C}_3)$ is infinite dimensional). Let us consider the case $q \equiv 1 \pmod 4$. In this case there exists an element $a \in \mathbb{F}_q$ such that $a^2 = -1$. Then

$$\begin{pmatrix} a & \\ & a^{-1} \end{pmatrix} \begin{pmatrix} 1 & 1 \\ & 1 \end{pmatrix} \begin{pmatrix} a^{-1} & \\ & a \end{pmatrix} = \begin{pmatrix} 1 & -1 \\ & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ & 1 \end{pmatrix}^{-1}.$$

Now the Proposition follows from Corollary 2.2 (2), since c_3 must have an even order.

If $q \equiv 3 \pmod 4$ we have (since $p \neq 3$),

$$c_3 \neq c_3^4 = \begin{pmatrix} 1 & 4 \\ & 1 \end{pmatrix} = \begin{pmatrix} 2 & \\ & 2^{-1} \end{pmatrix} \begin{pmatrix} 1 & 1 \\ & 1 \end{pmatrix} \begin{pmatrix} 2^{-1} & \\ & 2 \end{pmatrix}$$

and then, by Corollary 2.2 (1), we get $\dim \mathfrak{B}(\mathcal{C}_3) = \infty$.

The statement about $\mathcal{C}_4$ follows from Remark 3.2. □

We consider now the case $q = 3^{2n+1}$. For this, we need Lemma 3.7 and Corollary 3.8 below, which we could not find in the literature. Let φ denote the Euler function, $\varphi(n) = \#\{m \in \mathbb{N} \mid m < n \text{ and } m \text{ is coprime to } n\}$.

Lemma 3.7. *If $n \in \mathbb{N}$ is such that $3 \nmid n$ and $4 \nmid n$, then $\varphi(n) > (\frac{n}{2})^{\frac{3}{4}}$.*

Proof. If n is even, $n = 2p_1^{r_1} p_2^{r_2} \cdots p_N^{r_N}$, where $5 \leq p_1 < p_2 < \cdots < p_N$ are prime numbers. Then

$$\frac{\varphi(n)^2}{n} = \frac{1}{2} \prod_i \frac{(p_i - 1)^2 p_i^{2r_i - 2}}{p_i^{r_i}} = \frac{1}{2} \prod_i (p_i - 1)^2 p_i^{r_i - 2}.$$

Since $(p_i - 1)^2 > p_i^{3/2} \geq p_i^{2 - \frac{r_i}{2}}$ for $r_i \geq 1$, we have

$$\frac{\varphi(n)^2}{n} > \frac{1}{2} \prod p_i^{\frac{r_i}{2}} = \frac{\sqrt{n}}{2\sqrt{2}}.$$

If n is odd, $\varphi(n) = \varphi(2n) > n^{\frac{3}{4}} > (\frac{n}{2})^{\frac{3}{4}}$. □

Corollary 3.8. $\frac{\varphi(3^p-1)}{p} > 3^{\frac{p-1}{2}}$ *for all odd prime number* p.

Proof. If $p = 3$, 5 or 7, it follows immediately. Otherwise, by the Lemma,

$$\frac{\varphi(3^p-1)}{p} > \frac{(3^p-1)^{3/4}}{2^{3/4}p} > \frac{3^{3p/4}}{2p} > 3^{\frac{p-1}{2}}.$$

□

We finish now with the proof of Proposition 3.6.

End of proof of Proposition 3.6 (case $q = 3^{2n+1}$). Assume first that $r = 2n+1$ is a prime number. For $z \in \mathbb{F}_q$, we denote $f_z = f_z(X) \in \mathbb{F}_3[X]$ the minimal polynomial of z. We consider the sets

$$\mathcal{I} = \left\{ f_{x^2} \in \mathbb{F}_3[X] \mid x^2 \in \mathbb{F}_{3^r} \setminus \mathbb{F}_3,\ |x^2| = \frac{3^r-1}{2} \right\}, \text{ and}$$
$$\mathcal{S} = \left\{ X^r + a_{r-1}X^{r-1} + \cdots + a_1X - 1 \in \mathbb{F}_3[X] \mid \forall i = 1,\dots,r,\ a_{r-i} + a_i = 0 \right\}.$$

Note that $\#\mathcal{I} = \frac{\varphi(\frac{3^r-1}{2})}{r} = \frac{\varphi(3^r-1)}{r}$ (because all minimal polynomials of elements in $\mathbb{F}_{3^r} \setminus \mathbb{F}_3$ have degree r, since r is a prime number). We have that $\#\mathcal{S} = 3^{\frac{r-1}{2}} < \#\mathcal{I}$ by Corollary 3.8. Then there exists $f \in \mathcal{I} \setminus \mathcal{S}$, and we chose such an f. Since $f(0) = (-1)^r \cdot \operatorname{norm}(x^2) = -1$, in order for f not to be in $\mathcal{S}$, there exists an i such that $a_{r-i} + a_i \neq 0$.

Consider now $x \in \mathbb{F}_{3^r}^\times$ of order $\frac{3^r-1}{2}$, and let $\mathbf{X} = \{x, x^3, \dots, x^{3^{r-1}}\}$ be the orbit of x by the action of the Galois group of the extension $\mathbb{F}_{3^r}/\mathbb{F}_3$. Then $\prod_{y\in\mathbf{X}} y = 1$ (because x is a square). Also, if $\emptyset \neq \mathbf{S} \subseteq \mathbf{X}$ and $\prod_{y\in\mathbf{S}} y \in \mathbb{F}_3^\times$, then $\mathbf{S} = \mathbf{X}$. Indeed, $\prod_{y\in\mathbf{X}} y = x^{\sum_{i=0}^{r-1} 3^i} = x^{\frac{3^r-1}{2}} = 1$. Now, if $z = \prod_{y\in\mathbf{S}} y$, and $\mathbf{S} \neq \mathbf{X}$, then $z = x^s$ for some $s < \frac{3^r-1}{2}$. Note that x is a square and $s < |x|$, which implies that $x^s \neq \pm 1$. Let

$$A = \{a^2 + a^{-2} \mid a \in \mathbb{F}_{3^r}^\times \setminus (\mathcal{R}_1 \cup \mathcal{R}_2 \cup \mathcal{R}_3 \cup \mathcal{R}_4 \cup \mathcal{R}_6)\} = \{a^2 + a^{-2} \mid a \in \mathbb{F}_{3^r} \setminus \mathbb{F}_3\}.$$

Now,

$$a_i = \sum_{\substack{\mathbf{Y}\subset\mathbf{X}\\ \#\mathbf{Y}=r-i}} \prod_{y\in\mathbf{Y}} y, \qquad a_{r-i} = \sum_{\substack{\mathbf{Y}\subset\mathbf{X}\\ \#\mathbf{Y}=i}} \prod_{y\in\mathbf{Y}} y = \sum_{\#\mathbf{Y}=r-i} \prod_{y\in\mathbf{Y}} \frac{1}{y}.$$

Thus, $a_{r-i} + a_i \in (A)$, the subgroup generated by A. Then, $1 \in (A)$.

Let now χ be a character of the centralizer of c_3. If $\chi\begin{pmatrix} 1 & t \\ & 1 \end{pmatrix} \neq 1$ for some $t \in A$, then we get a Dynkin diagram with a cycle of length ≥ 4, which is of infinite type. Otherwise, since $1 \in (A)$, we get $\mathbf{q}_{11} = 1$, which also yields an infinite dimensional Nichols algebra by Lemma 2.3.

If $r = 2n+1$ is not a prime number, one can repeat the same argument with r', a prime factor of r, taking $\mathbb{F}_{3^{r'}}$ as a subfield of $\mathbb{F}_{3^r}$. □

Proposition 3.9. *If $p \neq 3$ and $\dim \mathfrak{B}(\mathcal{C}_5) < \infty$, then $\chi = \operatorname{sgn} \times \varepsilon$, where* sgn *is the non-trivial representation of $\mathbb{Z}_2$ and ε is the trivial representation of $\mathbb{F}_q$. The same statement goes for $\mathfrak{B}(\mathcal{C}_6)$.*

Proof. As before, for $a \in \mathbb{F}_q^\times$, let

$$x_a = \begin{pmatrix} a & \\ & a^{-1} \end{pmatrix}, \quad g_a = x_a c_5 x_a^{-1} = \begin{pmatrix} -1 & a^2 \\ & -1 \end{pmatrix}.$$

Then $\mathbf{q}_{ab} = \chi \begin{pmatrix} -1 & a^2b^{-2} \\ & -1 \end{pmatrix}$, and $\mathbf{q}_{a1}\mathbf{q}_{1a} = \chi \begin{pmatrix} 1 & -(a^2+a^{-2}) \\ & 1 \end{pmatrix}$. For $t \in \mathbb{F}_q$, let $n_t = \begin{pmatrix} 1 & t \\ & 1 \end{pmatrix}$. Let

$$A = \{-(a^2+a^{-2}) \mid a \in \mathbb{F}_q^\times \setminus \mathcal{R}_1 \cup \mathcal{R}_2 \cup \mathcal{R}_3 \cup \mathcal{R}_4 \cup \mathcal{R}_6\}.$$

If there exists $t \in A$ with $\chi(n_t) \neq 1$, then $\dim \mathfrak{B}(\mathcal{C}_5) = \infty$ by Lemma 2.3, as in the proof of Proposition 3.1. Thus, we may suppose that $\chi(n_t) = 1$ for all $t \in A$. Now, notice that $\#A \geq \frac{q-9}{4}$. When $q \notin \{5, 25, 7, 11, 13\}$, we get $\#A > \frac{q}{p}$. In this case, A generates (as an abelian group) the whole $\mathbb{F}_q$, which implies the statement. If $q = 11$ or $q = 13$ an easy computation shows that A generates $\mathbb{F}_q$, whence we are done.

Let $q = 25$, $\mathbb{F}_q = \mathbb{F}_5[s]/(s^2-2)$. Let first $a = 1+s$, then $|a| = 12$ (hence $a \notin \mathcal{R}_1 \cup \mathcal{R}_2 \cup \mathcal{R}_3 \cup \mathcal{R}_4 \cup \mathcal{R}_6$), and $-(a^2+a^{-2}) = -((3+2s)+(3+3s)) = 4$. Now, take $a = 1+2s$, then $|a| = 24$ and $-(a^2+a^{-2}) = 2s$. Therefore, A generates $\mathbb{F}_q$, and we are done.

We deal now with the cases $q \in \{5, 7\}$. Let $q = 5$ and $a = 2 \in \mathbb{F}_q^\times$. With g_1, g_a, we get a Dynkin diagram as in Lemma 2.1, with $\zeta = \chi \begin{pmatrix} -1 & 1 \\ & -1 \end{pmatrix}$, and $\mu = \chi \begin{pmatrix} 1 & 2 \\ & 1 \end{pmatrix}$. Since this implies that $|\zeta|$ divides 10 and $\mu = \zeta^8$, by the Lemma we get that $\mathfrak{B}(\mathcal{C}_5)$ is infinite dimensional unless either

- $\zeta \neq 1$ and $\zeta\mu = 1$, or
- $\zeta \neq 1$ and $\mu = 1$, or
- $\zeta = -1$.

The first case is impossible, while in the second and third case we arrive to the statement.

Let $q = 7$. Let $a = 3$, $\alpha = \chi \begin{pmatrix} -1 & 1 \\ & -1 \end{pmatrix}$ and $\beta = \chi \begin{pmatrix} 1 & 1 \\ & 1 \end{pmatrix}$. Then if $\beta \neq 1$, we have a Dynkin diagram as in Lemma 2.3, which yields an infinite dimensional Nichols algebra (notice that $\beta \notin \mathcal{R}_3$). If $\beta = 1$, as $\alpha^6 = \beta$ and $|\alpha|$ divides 14, this implies $\alpha = -1$, which is the statement again.

Remark 3.2 gives the statement about $\mathcal{C}_6$. □

Remark 3.10. If $p = 3$ one can prove, using the same techniques as in Proposition 3.6 (case $q = 3^{2n+1}$), that $\chi = \mathrm{sgn} \times \varepsilon$ when restricted to each subfield $\mathbb{F}_{3^r}$ where r is an odd prime.

4. Nichols algebras over $\mathbf{GL}(2,\mathbb{F}_q)$

We proceed in this section with the groups $\mathbf{GL}(2,\mathbb{F}_q)$. Recall that the order of $\mathbf{GL}(2,\mathbb{F}_q)$ is $(q-1)^2q(q+1)$. Again, E will be the quadratic extension of $\mathbb{F}_q$ and $\overline{x}$ will be the Galois conjugate of $x \in E$. Since $\mathbf{GL}(2,\mathbb{F}_2) \simeq \mathbb{S}_3$, we consider only the case $q > 2$.

There are $q^2 - 1$ conjugacy classes divided in 4 types:

Table 3: Conjugacy classes in $\mathbf{GL}(2,\mathbb{F}_q)$.

Type	Representative	Size	Number	Centralizer
$\mathcal{C}_1$	$c_1(x) = \begin{pmatrix} x & \\ & x \end{pmatrix}$	1	$q-1$	$\mathbf{GL}(2,\mathbb{F}_q)$
$\mathcal{C}_2$	$c_2(x) = \begin{pmatrix} x & 1 \\ & x \end{pmatrix}$	q^2-1	$q-1$	$\mathbb{F}_q^\times \times \mathbb{F}_q$
$\mathcal{C}_3$	$c_3(x,y) = \begin{pmatrix} x & \\ & y \end{pmatrix}$ $(x \neq y)$	$q(q+1)$	$\frac{(q-1)(q-2)}{2}$	$\mathbb{F}_q^\times \times \mathbb{F}_q^\times$
$\mathcal{C}_4$	$c_4(x) = \begin{pmatrix} & -x\overline{x} \\ 1 & x+\overline{x} \end{pmatrix}$ $(x \in E \setminus \mathbb{F}_q)$	$(q-1)q$	$\frac{q(q-1)}{2}$	cyclic

For the next proposition we need to recall the character table of the non-abelian group $\mathbf{GL}(2,\mathbb{F}_q)$ from [FH, §5.2]. We know that there are q^2-1 irreducible representations. The relevant information for our purposes is contained in the following table:

Table 4: Representations of $\mathbf{GL}(2,\mathbb{F}_q)$ in scalar matrices

Representation	Dimension	Number	$c_1(x) = \begin{pmatrix} x & \\ & x \end{pmatrix}$
U_α $(\alpha \in \widehat{\mathbb{F}_q^\times})$	1	$q-1$	$\alpha(x)^2$
V_α $(\alpha \in \widehat{\mathbb{F}_q^\times})$	q	$q-1$	$\alpha(x)^2$
$W_{\alpha,\beta}$ $(\alpha,\beta \in \widehat{\mathbb{F}_q^\times}$ y $\alpha \neq \beta)$	$q+1$	$\frac{1}{2}(q-1)(q-2)$	$\alpha(x)\beta(x)$
X_γ $(\alpha \in \widehat{E_q^\times})$	$q-1$	$\frac{1}{2}q(q-1)$	$\gamma(x)$

Proposition 4.1. *If* $\dim \mathfrak{B}(\mathcal{C}_1,\chi) < \infty$ *then:*

(1) $-1 = \alpha(x)^2$, *where* $\alpha \in \widehat{\mathbb{F}_q^\times}$; *or*
(2) $-1 = \alpha(x)\beta(x)$, *where* $\alpha,\beta \in \widehat{\mathbb{F}_q^\times}$; *or*
(3) $-1 = \alpha(x)$, *where* $\alpha \in \widehat{E^\times}$; *or*

Proof. If follows from [Gra2, Lemma 3.1]. □

Proposition 4.2. *If* $\dim \mathfrak{B}(\mathcal{C}_3) < \infty$ *then* $\mathbf{q}_T = \begin{pmatrix} \alpha & \beta \\ \beta & \alpha \end{pmatrix}$ *where* $\alpha = \chi(c_3(x,y))$, $\beta = \chi(c_3(y,x))$, *and* $T = \{c_3(x,y), c_3(y,x)\}$. *Furthermore, one of the following conditions is satisfied:*

- $\beta^2 = 1$ *and* $\alpha \neq 1$
- $\beta^2 \neq 1$ *and* $\alpha\beta^2 = 1$
- $\beta^2 \neq 1$ *and* $\alpha\beta^2 \neq 1$ *and* $\alpha = -1$
- $\beta^2 \in \mathcal{R}_{12}$ *and* $\alpha = -\beta^4 \in \mathcal{R}_3$

Proof. Notice that $c_3(x,y)$ and $c_3(y,x)$ are conjugated in $\mathbf{GL}(2,\mathbb{F}_q)$ by the involution $\begin{pmatrix} & 1 \\ 1 & \end{pmatrix}$. The result now follows from Lemma 2.1. □

Proposition 4.3. *Let* $T = \left\{c_4(x), \begin{pmatrix} x+\overline{x} & x\overline{x} \\ -1 & \end{pmatrix}\right\}$. *If* $\dim \mathfrak{B}(\mathcal{C}_4) < \infty$ *then* $\mathbf{q}_T$ *is either* $\begin{pmatrix} -1 & -1 \\ -1 & -1 \end{pmatrix}$ *or* $\begin{pmatrix} \omega & \omega \\ \omega & \omega \end{pmatrix}$, *where* $\omega \in \mathcal{R}_3$.

Proof. Note that the centralizer of $c_4(x)$ is the cyclic group

$$\left\{\begin{pmatrix} a & -cx\overline{x} \\ c & a + c(x+\overline{x}) \end{pmatrix} : a, c \in \mathbb{F}_q^\times\right\},$$

and this group is isomorphic to $E^\times$ by $a + cx \mapsto \begin{pmatrix} a & -cx\overline{x} \\ c & a + c(x+\overline{x}) \end{pmatrix}$. Take the involution $\begin{pmatrix} 1 & x+\overline{x} \\ & -1 \end{pmatrix}$ to get

$$\begin{pmatrix} x+\overline{x} & x\overline{x} \\ -1 & \end{pmatrix} = \begin{pmatrix} 1 & x+\overline{x} \\ & -1 \end{pmatrix}\begin{pmatrix} & -x\overline{x} \\ 1 & x+\overline{x} \end{pmatrix}\begin{pmatrix} 1 & x+\overline{x} \\ & -1 \end{pmatrix} \in \mathcal{C}_{c_4(x)}.$$

Since $E^\times$ is cyclic, there exists $n \in \mathbb{N}$ such that $c_4(x)^n = \begin{pmatrix} x+\overline{x} & x\overline{x} \\ -1 & \end{pmatrix}$. We get the result by using Corollary 2.2(1). □

Proposition 4.4. *If* $p = 2$ *then* $\mathfrak{B}(\mathcal{C}_2)$ *is infinite dimensional. If* $p \neq 2$, $q \neq 9$ *and* $\dim \mathfrak{B}(\mathcal{C}_2) < \infty$ *then* $\chi\begin{pmatrix} x^i & a \\ & x^i \end{pmatrix} = (-1)^i$.

Proof. Similarly to the proof of Proposition 3.9, we take $x_a = \begin{pmatrix} a & \\ & 1 \end{pmatrix}$ and we get $g_a = \begin{pmatrix} x & a \\ & x \end{pmatrix}$. Then $\mathbf{q}_{ab} = \chi(g_{ab^{-1}})$, $\mathbf{q}_{a1}\mathbf{q}_{1a} = \chi\begin{pmatrix} x^2 & x(a+a^{-1}) \\ & x^2 \end{pmatrix}$. As before, if $\mathbf{q}_{1a}\mathbf{q}_{a1} \neq 1$ for some $a \in \mathbb{F}_q^\times \setminus (\mathcal{R}_1 \cup \mathcal{R}_2 \cup \mathcal{R}_3)$, then we get a Dynkin diagram of infinite type, since

$$\mathbf{q}_{1,a}\mathbf{q}_{a,1} = \mathbf{q}_{a,a^2}\mathbf{q}_{a^2,a} = \cdots = \mathbf{q}_{a^m,1}\mathbf{q}_{1,a^m}, \qquad |a| = m+1.$$

Assume then that $\forall a \in \mathbb{F}_q^\times \setminus (\mathcal{R}_1 \cup \mathcal{R}_2 \cup \mathcal{R}_3)$, $\mathbf{q}_{1a}\mathbf{q}_{a1} = 1$. We define $\chi_1 \in \widehat{\mathbb{F}_q^\times}$ and $\chi_2 \in \widehat{\mathbb{F}_q}$ by $\chi\begin{pmatrix} \tau & \sigma \\ & \tau \end{pmatrix} = \chi_1(\tau)\chi_2(\tau^{-1}\sigma)$. Let

$$A = \left\{x^{-1}\left(a + a^{-1}\right) \mid a \in \mathbb{F}_q^\times \setminus (\mathcal{R}_1 \cup \mathcal{R}_2 \cup \mathcal{R}_3)\right\}.$$

Thus we assume $\chi_1(x^2)\chi_2(b) = 1$ for all $b \in A$. Since the orders of $\mathbb{F}_q^\times$ and $\mathbb{F}_q$ are coprime, we get $\chi_2(b) = 1$ for all $b \in A$. Note that, since $\#(\mathcal{R}_1 \cup \mathcal{R}_2 \cup \mathcal{R}_3) \leq 4$, $\#A \geq \frac{q-5}{2}$. If $\#A > \frac{q}{p} = p^{n-1}$ then A is not contained in any $\mathbb{F}_p$-hyperplane of $\mathbb{F}_q$, and thus it generates $\mathbb{F}_q$ as an abelian group. Therefore, $\chi_2 = 1$ if $p^{n-1}(p-2) > 5$. Furthermore, we get $\chi_1(x^2) = 1$, from where we conclude with the statement.

We study now the cases $q = 2^n (n \in \mathbb{N})$ and $q \in \{3, 5, 7\}$. Let $q = 2^{2n}$. We write $\mathbb{F}_4 \subseteq \mathbb{F}_q$, $\mathbb{F}_4 = \mathbb{F}_2[s]/(s^2+s+1)$. We get $s + s^{-1} = 1$, $|s| = 3$. Let then $\beta := \mathbf{q}_{1s}\mathbf{q}_{s1} = \chi\begin{pmatrix} x^2 & x \\ & x^2 \end{pmatrix}$, $\alpha := \chi(c_2) = \chi\begin{pmatrix} x & 1 \\ & x \end{pmatrix}$. Notice that $\alpha^{2|x|} = 1$ and $\beta = \alpha^{|x|+2}$. Then either $\beta = 1$ (which implies $\alpha = 1$ since $|x|$ is odd), or, by using Lemma 2.3, $\alpha = -1$, but then $\beta = -1$. In any case, we get an infinite-dimensional Nichols algebra.

The case $q = 2^{2n+1}$. Since $2^{2n+1} \equiv 2 \pmod 3$, then $\mathcal{R}_3 = \{1\}$. Therefore, $\#A = \frac{2^n-2}{2} = 2^{n-1} - 1$. It is easy to see that $1 \notin A$ and $0 \notin A$. Let (A) be the subgroup generated by A. We will prove that $1 \in (A)$, which will imply $(A) = \mathbb{F}_q$, and we shall be done. Let r be a prime number such that $r \mid 2n+1$. If $\xi \in \mathbb{F}_{2^r} \setminus \mathbb{F}_2$, we denote by f_ξ its minimal polynomial. On the one hand there exist exactly $\frac{2^r-2}{r}$ irreducible polynomials in $\mathbb{F}_2[X]$ of degree r. On the other hand,

$$f_\xi = X^r + a_{r-1}X^{r-1} + \cdots + a_1X + 1 = \Pi_{i=1}^r(X - \xi_i).$$

As done in the proof of Proposition 3.6 (case $q = 3^{2n+1}$), one can prove that $a_{r-k} + a_k \in (A) \cap \mathbb{F}_2$. It suffices then to prove that there exists k such that $a_{r-k} + a_k = 1$. If $a_{r-k} + a_k = 0$ for all k, then $f_\xi \in \mathcal{S}$, where

$$\mathcal{S} = \{X^r + b_{r-1}X^{r-1} + \cdots + b_1X + 1 \mid b_{r-k} = b_k \ \forall k\}.$$

Thence, we have $\mathcal{I} = \{f \in \mathbb{F}_2[X] \mid f \text{ irreducible}\} \subseteq \mathcal{S}$, which is a contradiction because $\#\mathcal{S} = 2^{\frac{r-1}{2}} < \frac{2^r-2}{r}$ for any $r > 3$. If $r = 3$, $f = (X+1)^3 \in \mathcal{S} \setminus \mathcal{I}$, and since $\#\mathcal{S} = \#\mathcal{I}$, we also get $\mathcal{I} \setminus \mathcal{S} \neq \emptyset$. Then $\#(A) \geq 2^{r-1} + 1$ and then $(A) = \mathbb{F}_{2^r}$.

The case $q = 3$. If $x = 1$, we use Corollary 2.2 (2) to see that $\dim \mathfrak{B}(\mathcal{C}_2) = \infty$ for any representation (notice that $|c_2(x)| = 3$). If $x = -1$, $c_2(x)$ generates its centralizer and again by Corollary 2.2 (2) we get $\chi(c_2(x)) = -1$.

The case $q = 5$. Note that $|c_2(x)| = 5|x|$. If $x = 1$ then $\mathfrak{B}(\mathcal{C}_2)$ is infinite dimensional by Corollary 2.2 (2). Assume now that $x = 2$ or $x = 3$. We take $a = 2$ and then $a + a^{-1} = 0$. Let

$$\alpha = \chi(g) = \mathbf{q}_{11} = \mathbf{q}_{22} = \mathbf{q}_{33} = \mathbf{q}_{44},$$
$$\beta = \mathbf{q}_{12}\mathbf{q}_{21} = \mathbf{q}_{24}\mathbf{q}_{42} = \mathbf{q}_{34}\mathbf{q}_{43} = \mathbf{q}_{31}\mathbf{q}_{13} = \chi\begin{pmatrix} 4 & \\ & 4 \end{pmatrix} = \pm 1 \text{ and}$$
$$\gamma = \mathbf{q}_{23}\mathbf{q}_{32} = \mathbf{q}_{14}\mathbf{q}_{41} = \chi\begin{pmatrix} 4 & 1 \\ & 4 \end{pmatrix}.$$

If $\beta = -1$ we get a length-four cycle, thence $\beta = 1$. Note that $\alpha^{10} = 1$ and then $|\alpha| = 2, 5, 10$. But $\alpha^{-2} = \gamma$. If $\gamma = 1$ then $\alpha = -1$ and the representation is completely determined as in the statement. If $\gamma \neq 1$ we have a Dynkin diagram as in Lemma 2.1 with $\zeta = \alpha$ and $\mu = \alpha^{-2}$, which is of infinite type. If $x = 4$, take again $a = 2$. We have that $\mathbf{q}_{12}\mathbf{q}_{21} = \cdots = \beta = \chi\begin{pmatrix} 1 & \\ & 1 \end{pmatrix} = 1$ and that $\gamma = \mathbf{q}_{23}\mathbf{q}_{32} = \mathbf{q}_{14}\mathbf{q}_{41} = \chi\begin{pmatrix} 1 & 2 \\ & 1 \end{pmatrix}$. Again, $\alpha^{-2} = \gamma$, and we get the statement as for $x = 2, 3$.

The case $q = 7$. Note that $|c_2(x)| = 7|x|$. The case $x = 1$ follows as before from Corollary 2.2 (2). The cases $x = 3$ and $x = 5$ follow by taking $a = 3$. In fact, let $\alpha = \mathbf{q}_{11} = \chi(c_2(x))$ and $\beta = \mathbf{q}_{13}\mathbf{q}_{31} = \chi\begin{pmatrix} 2 & 3 \\ & 2 \end{pmatrix}$. If $\beta \neq 1$, we get a Dynkin diagram with a cycle of length 6. Then $\beta = 1$, but $\beta = \alpha^8$ and since $|\alpha|$ divides 42, we must have $\alpha = \pm 1$. If $\alpha = 1$ we again have an infinite dimensional Nichols algebra, whence $\alpha = -1$. But $c_2(x)$ generates the centralizer, and we get the statement. The cases $x = 2$ and $x = 4$ are easier: we take as before $a = 3$, $\alpha = \mathbf{q}_{11}$, $\beta = \mathbf{q}_{13}\mathbf{q}_{31}$. Then we get that $\alpha^8 = \beta = \pm 1$ but $|\alpha|$ divides 21. If $x = 6$

again we use $a = 3$, $\alpha = \mathbf{q}_{11} = \chi(c_2(x))$, $\beta = \mathbf{q}_{13}\mathbf{q}_{31} = \chi\begin{pmatrix} 1 & -1 \\ & 1 \end{pmatrix}$. As before, we must have $\alpha^{36} = \beta = 1$ but $|\alpha|$ divides 14, which implies the result. □

Acknowledgement. We benefited from discussions with N. Andruskiewitsch, F. Fantino, C. Sánchez and A. Pacetti, to whom we thank. We used GAP [GAP] to do some of the computations.

References

[AF1] Nicolás Andruskiewitsch and Fernando Fantino. On pointed Hopf algebras associated with alternating and dihedral groups. math.QA/0702559, 2007, To appear in *Rev. Unión Mat. Argent.* 48(1).

[AF2] Nicolás Andruskiewitsch and Fernando Fantino. On pointed Hopf algebras associated with unmixed conjugacy classes in $\mathbb{S}_m$. *J. Math. Phys.*, 48(3):033502, 26, 2007.

[AG1] Nicolás Andruskiewitsch and Matías Graña. Braided Hopf algebras over non-abelian finite groups. *Bol. Acad. Nac. Cienc. (Córdoba)*, 63:45–78, 1999. Colloquium on Operator Algebras and Quantum Groups (Spanish) (Vaquerías, 1997).

[AG2] Nicolás Andruskiewitsch and Matías Graña. From racks to pointed Hopf algebras. *Adv. Math.*, 178(2):177–243, 2003.

[AS] Nicolás Andruskiewitsch and Hans-Jürgen Schneider. Pointed Hopf algebras. In *New directions in Hopf algebras*, volume 43 of *Math. Sci. Res. Inst. Publ.*, pages 1–68. Cambridge Univ. Press, Cambridge, 2002.

[AZ] Nicolás Andruskiewitsch and Shouchuan Zhang. On pointed Hopf algebras associated to some conjugacy classes in $\mathbb{S}_n$. *Proc. Amer. Math. Soc.*, 135(9):2723–2731 (electronic), 2007.

[Bro] Christian Brouder. Quantum field theory meets Hopf algebra, 2006. hep-th/0611153.

[Dri] V. G. Drinfel′d. Quantum groups. In *Proceedings of the International Congress of Mathematicians, Vol. 1, 2 (Berkeley, Calif., 1986)*, pages 798–820, Providence, RI, 1987. Amer. Math. Soc.

[FH] William Fulton and Joe Harris. *Representation theory*, volume 129 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1991. A first course, Readings in Mathematics.

[Gab] Matthias R. Gaberdiel. An algebraic approach to logarithmic conformal field theory. *Internat. J. Modern Phys. A*, 18(25):4593–4638, 2003.

[GAP] The GAP Group. Gap – Groups, Algorithms, and Programming, version 4.4.9, `http://www.gap-system.org`, 2006.

[Gra1] Matías Graña. Nichols algebras of nonabelian group type. Web page at `http://mate.dm.uba.ar/~matiasg/zoo.html`.

[Gra2] Matías Graña. On Nichols algebras of low dimension. In *New trends in Hopf algebra theory (La Falda, 1999)*, volume 267 of *Contemp. Math.*, pages 111–134. Amer. Math. Soc., Providence, RI, 2000.

[Hec1] István Heckenberger. Classification of arithmetic root systems of rank 3. *Actas of XVI Colloquium Latinoamericano de Álgebra*, 2005.

[Hec2] István Heckenberger. Classification of arithmetic root systems, 2006.

[PZ] Valentina Petkova and Jean-Bernard Zuber. Conformal field theories, graphs and quantum algebras. In *MathPhys odyssey, 2001*, volume 23 of *Prog. Math. Phys.*, pages 415–435. Birkhäuser Boston, Boston, MA, 2002.

[Ser] Jean Pierre Serre. *A course in arithmetic*. Springer-Verlag, New York, 1973. Translated from the French, Graduate Texts in Mathematics, No. 7.

[ZN] A. V. Zelevinskiĭ and G. S. Narkunskaja. Representations of the group SL(2, F_q), where $q = 2^n$. *Funkcional. Anal. i Priložen.*, 8(3):75–76, 1974.

E-mail address: `(sfreyre|matiasg|lvendramin)@dm.uba.ar`

Departamento de Matemática - FCEyN, Universidad de Buenos Aires, Pab I - Ciudad Universitaria, (1428) Buenos Aires - Argentina