Journal of Lie Theory
Volume **24** (2014) 351–372
© 2014 Heldermann Verlag

Finite Dimensional Nichols Algebras over Finite Cyclic Groups

Weicai Wu, Shouchuan Zhang, and Yao-Zhong Zhang*

Communicated by K. Schmüdgen

Abstract. All finite dimensional Nichols algebras of diagonal type of connected finite dimensional Yetter-Drinfeld modules over a finite cyclic group $\mathbb{Z}_n$ are found. It is proved that the Nichols algebra of a connected Yetter-Drinfeld module V over $\mathbb{Z}_n$ with $\dim V > 3$ is infinite dimensional.
Mathematics Subject Classification 2000: 16W30, 11A07.
Key Words and Phrases: Arithmetic root system, Hopf algebra, cyclic group.

1. Introduction

This paper concerns the classification of finite dimensional pointed Hopf algebras with finite cyclic groups. Recently Heckenberger established a one-to-one correspondence between arithmetic root systems and Nichols algebras of diagonal type having a finite set of (restricted) Poincare-Birkhoff-Witt generators [He04b] and between twisted equivalence classes of arithmetic root systems and generalized Dynkin diagrams [He06a]. In this latter work, arithmetic root systems were also classified in full generality.

The theory of Nichols algebras is dominated by the classification of finite dimensional pointed Hopf algebras (see e.g. [AS98, AS00]). Nichols algebras appear in the construction of quantized Kac-Moody algebras and their $\mathbb{Z}_2$-graded (see [KT91, KS97]) and $\mathbb{Z}_3$-graded versions [Ya03]. They are natural quantum groups and are connected to the bicovariant differential calculus initiated by Woronowicz [Wo89]. Bicovariant differential calculi on quantum groups have been studied by Klimyk and Schmüdgen in their book [KS97] (see especially Part IV of this book).

Nichols algebras play a central role in the theory of (pointed) Hopf algebras. Any braided vector space has a canonical Nichols algebra. The easiest braidings are those of diagonal type, that is, the vector space V has a basis $x_1, \cdots, x_r$ such that the braiding $c \in \mathrm{Aut}(V \otimes V)$ is given by $c(x_i \otimes x_j) = q_{ij} x_j \otimes x_i$ for some nonzero numbers q_{ij} , for all $i, j \in \{1, 2, \cdots, r\}$. The braided vector spaces of diagonal type with finite-dimensional Nichols algebra were essentially classified by Heckenberger.

* Y.-Zh. Zhang was supported by the Australian Research Council.

ISSN 0949–5932 / $2.50 © Heldermann Verlag

In this paper we study diagonal braidings and their Nichols algebras coming from Yetter–Drinfeld modules over finite cyclic groups. This is a substantial restriction, and it turns out. We classify finite dimensional Nichols algebras with diagonal type of connected finite dimensional Yetter–Drinfeld (YD) modules over finite cyclic group $\mathbb{Z}_n$. We first determine which braided vector space V is a $\mathbb{Z}_n$-YD module by means of equation systems in $\mathbb{Z}_n$. Using the classification of arithmetic root systems, we find all finite dimensional Nichols algebras with diagonal type of connected finite dimensional $\mathbb{Z}_n$-YD modules.

This paper is organized as follows. In sections 1 and 2 we find all finite dimensional Nichols algebras with diagonal type of connected 2-dimensional and 3-dimensional $\mathbb{Z}_n$-YD modules, respectively. In section 3 we prove that Nichols algebra of connected $\mathbb{Z}_n$-YD module V with $\dim V > 3$ is infinite dimensional.

Throughout, k is a field of characteristic zero, which contains a primitive nth root of unity. Let G be a finite abelian group. Let

$$\widehat{G} := \{\chi \mid \chi \text{ is a homomorphism from } G \text{ to } k^*\}$$

and $R_n := \{\omega \in k \mid \omega \text{ is a primitive } n\text{th root of unit}\}$. If $G = (g)$ is a cyclic group with order n and $V \in^{kG}_{kG} \mathcal{YD}$ with basis $v_1, v_2, \cdots, v_r$, then there exist $\chi_i \in \widehat{G}, g_i \in G$, such that $\delta(v_i) = g_i \otimes v_i$ and $h \cdot v_i = \chi_i(h)v_i$ for any $h \in G$, $1 \le i \le r$. Let $\chi \in \widehat{G}$ such that $\chi(g) \in R_n$. Thus $\chi_i = \chi^{n_i}$ and $g_i = g^{m_i}$ for $1 \le i \le r$.

If V is a vector space with a basis $x_1, x_2, \cdots, x_r$ and $q_{ij} \in k^*$ for $1 \le i, j \le r$ such that map $c : \begin{cases} V \otimes V & \to \quad V \otimes V \\ x_i \otimes x_j & \mapsto \quad q_{ij} x_j \otimes x_i \end{cases}$, then (V, c) is called a braided vector space of diagonal type. Denote by $(q_{ij})_{r\times r}$ the braiding matrix of (V, c) under the basis $x_1, x_2, \cdots, x_r$. Then (V, c) is also written as $(V, (q_{ij})_{r\times r})$. Let $1, 2, \cdots, r$ be vertexes of a diagram. There is a line between vertexes i and j if $q_{ij}q_{ji} \neq 1$. Label vertex i by q_{ii} and line between i and j by $q_{ij}q_{ji}$. This diagram is called generalized Dynkin diagram (written as GDD in short) of matrix $(q_{ij})_{r\times r}$ or V. V is said to be connected if the generalized Dynkin diagram is connected. Let $e_1 := (1, 0, \cdots, 0), e_2 := (0, 1, \cdots, 0), \cdots, e_r := (0, 0, \cdots, 1)$ be a basis of $\mathbb{Z}_r$. Let $E_0 := \{e_1, e_2, \cdots, e_r\}$ and $\chi_0(e_i, e_j) := q_{ij}$. Then V is a $\mathbb{Z}_r$ graded vector space if one defines deg $x_i = e_i$. Let

$$\Delta^+(\mathfrak{B}(V)) := \{\deg u \mid u \text{ is a generator of (restricted) PBW basis }\}$$

and $\Delta(\mathfrak{B}(V)) := \Delta^+(\mathfrak{B}(V)) \cup -\Delta^+(\mathfrak{B}(V))$.

2. Rank 2 Nichols algebras of diagonal type

In this section we find all finite dimensional Nichols algebras with diagonal type of connected 2-dimensional $\mathbb{Z}_n$-YD modules.

Lemma 2.1. (i) *(See [ZZC04, Lemma 2.3] or appendix) Every kG-YD module is a braided vector space of diagonal type.*

*(*ii *) V is a G-YD module of diagonal type and braiding matrix $(q_{ij})_{n\times n}$ if and only if there exist $\chi_j \in \widehat{G}$, $g_i \in G$ such that $\chi_j(g_i) = q_{ij}$ for $1 \le i, j \le n$.*

(iii) *If* $\omega \in R_n$*, then* V *is a* $\mathbb{Z}_n$-YD *module of diagonal type and braiding matrix* $(q_{ij})_{n\times n}$ *if and only if there exist* $m_i, n_j \in \mathbb{Z}$ *such that* $q_{ij} = \omega^{m_i n_j}$ *for* $1 \le i, j \le n$*.*

(iv) *If* $\xi \in R_n$ *and* $q \in R_m$ *with* $m \mid n$*, then there exists* $s \in \mathbb{Z}$ *such that* $q = \xi^{\frac{ns}{m}}$ *with* $(s, m) = 1$.

(v) *If* $q \in R_m$ *with* $m \mid n$*, then there exists* $\omega \in R_n$ *such that* $q = \omega^{\frac{n}{m}}$*.*

Proof. (ii) It follows from [ZZC04, Pro. 2.4].

(iii) Let $G = (g)$ be a cyclic group with $\mid G \mid= n$ and $\chi \in \widehat{G}$ such that $\chi(g) = \omega$, then $\widehat{G} = \{\chi^m \mid 1 \le m \le n\}$ and $G = \{g^m \mid 1 \le m \le n\}$. If V is a G-YD module with diagonal type and braiding matrix $(q_{ij})_{n\times n}$, then there exist $\chi_j \in \widehat{G}$ and $g_i \in G$ such that $\chi_j(g_i) = q_{ij}$ for $1 \le i, j \le n$. Furthermore, there exist m_i, n_i such that $\chi_i = \chi^{n_i}$ and $g_i = g^{m_i}$ for for $1 \le i, j \le n$. Conversely, it is clear.

(iv) There exist $1 \le t \le n$ such that $\xi^t = q$ with $m = \frac{n}{(t,n)}$. Consequently, $(t, n) = \frac{n}{m}$. There exists $s \in \mathbb{Z}$ such that $t = \frac{n}{m}s$. Let $(s, m) = d$, $m = m'd$ and $s = s'd$. Thus $t = \frac{n}{m'}s'$. $\mathrm{ord}(\xi^t) \le m'$ since $n \mid tm'$, which implies that $m = m'$ and $(s, m) = 1$.

(v) Set $\tau := \prod\{p \mid p$ is prime with $p \mid n$ and $p \nmid s$ $\}$. It is clear $m \mid \tau$ and $(\tau + s, n) = 1$. Set $\mu = \tau + s$ and $\omega := \xi^{\mu}$. Thus, $\omega^{\frac{n}{m}} = \xi^{\frac{sn}{m}} = q$. ■

Lemma 2.2. *Let* $n = km$*,* $(s, m) = 1$*,* $t_1, t_2, t_3 \in \mathbb{Z}$*.*

(i)

$$\begin{cases} x_1y_1 & \equiv t_1sk \pmod n \\ x_2y_2 & \equiv t_2sk \pmod n \\ x_1y_2 + x_2y_1 & \equiv t_3sk \pmod n \end{cases} \tag{2.1}$$

has a solution in $\mathbb{Z}$ *if and only if*

$$\begin{cases} \frac{x_1y_1}{ks} & \equiv t_1 \pmod m \\ \frac{x_2y_2}{ks} & \equiv t_2 \pmod m \\ \frac{x_1y_2+x_2y_1}{ks} & \equiv t_3 \pmod m \end{cases} \tag{2.2}$$

has a solution in $\mathbb{Z}$ *.*

(ii) *If* d *is a solution of*

$$t_1x^2 - t_3x + t_2 \equiv 0 \pmod m, \tag{2.3}$$

then $x_1 = 1, y_1 = t_1sk, x_2 = d, y_2 = (t_3 - dt_1)sk$ *is a solution of (2.1) .*

(iii) *If* d *is a solution of*

$$t_2x^2 - t_3x + t_1 \equiv 0 \pmod m, \tag{2.4}$$

then $x_2 = 1, y_2 = t_2sk, x_1 = d, y_1 = (t_3 - dt_2)sk$ *a solution of (2.1).*

Proof. It is clear. ■

Lemma 2.3. *Let $n = km$ and $(s,m) = 1,\ t_1, t_2, t_3 \in \mathbb{Z}$. If (2.1) has a solution, then*

$$x^2 - t_3 x + t_1 t_2 \equiv 0 \pmod{m} \tag{2.5}$$

has a solution.

Proof. If (2.1) has a solution: $x_1 = m_1, y_1 = n_1, x_2 = m_2, y_2 = n_2$, then

$$\begin{cases} \frac{s^{-1}m_1n_1}{k} & \equiv t_1 \pmod{m} \\ \frac{s^{-1}m_2n_2}{k} & \equiv t_2 \pmod{m} \\ \frac{s^{-1}m_1n_2}{k} + \frac{s^{-1}m_2n_1}{k} & \equiv t_3 \pmod{m} \end{cases} \quad \text{and}$$

$$\begin{cases} \frac{s^{-1}m_1n_2}{k}\frac{s^{-1}m_2n_1}{k} & \equiv t_1t_2 \pmod{m} \\ \frac{s^{-1}m_1n_2}{k} + \frac{s^{-1}m_2n_1}{k} & \equiv t_3 \pmod{m} \end{cases}$$

have solutions. Thus there exist $u, v \in \mathbb{Z}$, such that

$$\begin{cases} \frac{s^{-1}m_1n_2}{k}\frac{s^{-1}m_2n_1}{k} & = t_1t_2 + um \\ \frac{s^{-1}m_1n_2}{k} + \frac{s^{-1}m_2n_1}{k} & = t_3 + vm \end{cases},$$

which implies that rational number $\frac{s^{-1}m_1n_2}{k}$ is a solution of integer coefficient equation $x^2 - (t_3 + vm)x + t_1t_2 + um = 0$. Consequently, $\frac{s^{-1}m_1n_2}{k} \in \mathbb{Z}$. Therefore, $\frac{s^{-1}m_1n_2}{k}$ is a solution of $x^2 - t_3x + t_1t_2 \equiv 0 \pmod{m}$. ■

Lemma 2.4. *Let $n = km$ and $(s,m) = 1,\ t_1, t_2, t_3 \in \mathbb{Z}$.*

(i) *If m is odd and $(t_1, m) = 1$, then (2.3) has a solution if and only if (2.5) has a solution.*

(ii) *If t_1 is odd and $(t_1, m) = 1$, then (2.3) has a solution if and only if (2.5) has a solution.*

(iii) *If t_2 is odd and $(t_2, m) = 1$, then (2.4) has a solution if and only if (2.5) has a solution.*

(iv) *If $(t_1, m) = 1$, then (2.1) has a solution if and only if (2.3) has a solution.*

Proof. (i) (2.3) and (2.5) are equivalent to $(2t_1x - t_3)^2 \equiv t_3^2 - 4t_1t_2 \pmod{m}$ and $(2x - t_3)^2 \equiv t_3^2 - 4t_1t_2 \pmod{m}$, respectively. Consequently, (2.3) has a solution if and only if (**??** has a solution

(ii) Considering Part (i) we only need prove this for even m. If $2 \nmid t_3$ and $2 \nmid t_2$, then both (2.3) and (2.5) have not any solutions. If $2 \nmid t_3$ and $2 \mid t_2$, then both (2.3) and (2.5) have solutions. If $2 \mid t_3$, then $(t_1x - \frac{t_3}{2})^2 \equiv (\frac{t_3}{2})^2 - t_1t_2 \pmod{2^{\alpha_1}}$ has a solution if and only if $(x - \frac{t_3}{2})^2 \equiv (\frac{t_3}{2})^2 - t_1t_2 \pmod{2^{\alpha_1}}$ has a solution. Consequently, (2.3) has a solution if and only if (2.5) has a solution.

(iii) It is similar to (ii).

(iv) If (2.1) has a solution, then (2.5) has a solution by Lemma 2.3, which implies that (2.3) has a solution by Part (ii). Conversely, it follows from Lemma 2.2. ■

Remark 2.5. Lemma 2.3 and 2.4 hold when $s = 1$.

Lemma 2.6. *If $(V, (q_{ij})_{r\times r})$ is a* YD- *module over $\mathbb{Z}_n$ and $(V', (q'_{ij})_{r\times r})$ has degree $s_i(E_0)$ with respect to V (defined in [He05b, Definition 2]), then $(V', (q'_{ij})_{r\times r})$ is also a* YD- *module over $\mathbb{Z}_n$.*

Proof. By Lemma 2.1, there exist $m_j, n_l \in \mathbb{N}$ such that $q_{jl} = \omega^{m_j n_l}$ for $1 \le j, l \le r$, By [He05b, Definition 2],

$$\begin{aligned} q'_{jl} &= q_{jl} q_{il}^{m_{ij}} q_{ji}^{m_{il}} q_{ii}^{m_{ij}m_{il}} \\ &= \omega^{m_j n_l} \omega^{m_i n_l m_{ij}} \omega^{m_j n_i m_{il}} \omega^{m_i n_i m_{ij} m_{il}} \\ &= \omega^{(m_j + m_{ij} m_i)(n_l + m_{il} n_i)}. \end{aligned}$$

Set $m'_j := m_j + m_{ij} m_i, n'_l := n_l + m_{il} n_i$. One has $q'_{jl} = \omega^{m'_j n'_l}$ for $1 \le j, l \le r$. Therefore, V' is a $\mathbb{Z}_n$-YD module. ■

Thus, if $(V, (q_{ij})_{r\times r})$ and $(V', (q'_{ij})_{r\times r})$ are Weyl equivalent, then $(V, (q_{ij})_{r\times r})$ is a $\mathbb{Z}_n$- YD module if and only if $(V', (q'_{ij})_{r\times r})$ a $\mathbb{Z}_n$- YD module.

Theorem 2.7. *Let $n = km$ $(m > 1)$ and $m = 2^{\alpha_1} 3^{\alpha_2} p_3^{\alpha_3} \cdots p_r^{\alpha_r}$ be the prime decomposition of m, $r \in \mathbb{N}$; $\alpha_3, \alpha_4, \cdots, \alpha_r > 0$, when $r > 2$. If $(V, (q_{ij})_{2\times 2})$ is a braided vector space, then V is a connected $\mathbb{Z}_n$-YD module such that $\dim \mathfrak{B}(V) < \infty$ if and only if one of the following conditions holds:*

T2(1). $1 - q_{11}q_{12}q_{21} = 1 - q_{12}q_{21}q_{22} = 0$, $q_{12}q_{21} \in R_m$, $\alpha_1 = 0$; $\alpha_2 = 0, 1$; $(\frac{-3}{p_i}) = 1$ *for* $2 < i \le r$. *Here symbol* $(\frac{-3}{p_i})$ *is defined in Appendix (A.1).*

T2(2)$_1$. $1 + q_{11} = 1 - q_{12}q_{21}q_{22} = 0$, $q_{12}q_{21} \in R_m$, $\alpha_1 = 0$; $\alpha_1 > 1$.

T2(2)$_2$. $1 + q_{22} = 1 - q_{12}q_{21}q_{11} = 0$, $q_{12}q_{21} \in R_m$, $\alpha_1 = 0$; $\alpha_1 > 1$.

T2(3). $1 + q_{11} = 1 + q_{22} = 0$, $q_{12}q_{21} \in R_m$, $\alpha_1 = 0$; $\alpha_1 > 1$.

T3(1)$_1$. $q_{12}q_{21} = q_{11}^{-2}$, $q_{22} = q_{11}^2$, $q_{11} \in R_m$, $m > 2$; $\alpha_1 = 0, 1$; $\alpha_2 = 0$; $p_i \equiv 1 \pmod 4$, *for* $2 < i \le r$.

T3(1)$_2$. $q_{12}q_{21} = q_{11}^{-2}$, $q_{22} = -1$, $q_{11} \in R_m$, $m > 2$, $\alpha_1 \ne 2, 3$.

T3(2)$_1$. $\omega \in R_n$, $s = 1, 2$; $q_{11} = \omega^{\frac{ns}{3}}$, $q_{22} = \omega^{\frac{n}{m}}$, $q_{12}q_{21}q_{22} = 1$, $m > 3$; $3 \nmid m$ *or* $\frac{ms}{3} \not\equiv 2 \pmod 3$.

T3(2)$_2$. $q_{12}q_{21}q_{22} = 1$, $q_{11} \in R_3$, $q_{22} \in R_2$, $m = 6$;

T3(3). $q_{11} \in R_3$, $q_{12}q_{21} = -q_{11}$, $q_{22} = -1$; $m = 6$.

T4(1). $q_0 = q_{12}q_{21}q_{11} \in R_{12}$, $q_{11} = q_0^4$, $q_{22} = -q_0^2$, $m = 12$.

T4(2). $q_{12}q_{21} \in R_{12}$, $q_{11} = q_{22} = -(q_{12}q_{21})^2$, $m = 12$.

T5(1). $q_{12}q_{21} \in R_{12}$, $q_{11} = -(q_{12}q_{21})^2$, $q_{22} = -1$, $m = 12$.

T5(2). $q_0 = q_{12}q_{21}q_{11} \in R_{12}$, $q_{11} = q_0^4$, $q_{22} = -1$, $m = 12$.

T6. $q_{11} \in R_{18}$, $q_{12}q_{21} = q_{11}^{-2}$, $q_{22} = -q_{11}^3$, $m = 18$.

T7(1). $q_{11} \in R_{12}$, $q_{12}q_{21} = q_{11}^{-3}$, $q_{22} = -1$; $m = 12$.

T7(2). $q_{12}q_{21} \in R_{12}$, $q_{11} = (q_{12}q_{21})^{-3}$, $q_{22} = -1$; $m = 12$.

T8(1). $q_{12}q_{21} = q_{11}^{-3}$, $q_{22} = q_{11}^3$, $q_{11} \in R_m$, $m > 3$, $\alpha_1 = 0$; $\alpha_2 = 0, 1$; $(\frac{-3}{p_i}) = 1$ *for* $2 < i \le r$.

T8(2). $_1$ $(q_{12}q_{21})^4 = -1$, $q_{22} = -1$, $q_{12}q_{21} = -q_{11}$; $m = 8$.

T8(2). $_2$ $(q_{12}q_{21})^4 = -1$, $q_{22} = -1$, $q_{11} = (q_{12}q_{21})^{-2}$; $m = 8$.
T8(3). $(q_{12}q_{21})^4 = -1$, $q_{11} = (q_{12}q_{21})^2$, $q_{22} = (q_{12}q_{21})^{-1}$; $m = 8$.
T9. $q_{12}q_{21} \in R_9$, $q_{11} = (q_{12}q_{21})^{-3}$, $q_{22} = -1$; $m = 18$.
T10. $q_{12}q_{21} \in R_{24}$, $q_{11} = (q_{12}q_{21})^{-6}$, $q_{22} = (q_{12}q_{21})^{-8}$; $m = 24$.
T11(1). $q_{11} \in R_5$, $q_{12}q_{21} = q_{11}^{-3}$, $q_{22} = -1$; $m = 10$.
T11(2). $q_{11} \in R_{20}$, $q_{12}q_{21} = q_{11}^{-3}$, $q_{22} = -1$; $m = 20$.
T12. $q_{11} \in R_{30}$, $q_{12}q_{21} = q_{11}^{-3}$, $q_{22} = -q_{11}^5$; $m = 30$.
T13. $q_{12}q_{21} \in R_{24}$, $q_{11} = (q_{12}q_{21})^6$, $q_{22} = (q_{12}q_{21})^{-1}$; $m = 24$.
T14. $q_{11} \in R_{18}$, $q_{12}q_{21} = q_{11}^{-4}$, $q_{22} = -1$; $m = 18$.
T15. $q_{12}q_{21} \in R_{30}$, $q_{11} = -(q_{12}q_{21})^{-3}$, $q_{22} = (q_{12}q_{21})^{-1}$; $m = 30$.
T16(1). $q_{11} \in R_{10}$, $q_{12}q_{21} = q_{11}^{-4}$, $q_{22} = -1$; $m = 10$.
T16(2). $q_{12}q_{21} \in R_{20}$, $q_{11} = (q_{12}q_{21})^{-4}$, $q_{22} = -1$; $m = 20$.
T17. $q_{12}q_{21} \in R_{24}$, $q_{11} = -(q_{12}q_{21})^4$, $q_{22} = -1$; $m = 24$.
T18. $q_{12}q_{21} \in R_{30}$, $q_{11} = -(q_{12}q_{21})^5$, $q_{22} = -1$; $m = 30$.
T20. $q_{12}q_{21} \in R_{30}$, $q_{11} = (q_{12}q_{21})^{-6}$, $q_{22} = -1$; $m = 30$.
T21. $q_{11} \in R_{24}$, $q_{12}q_{21} = q_{11}^{-5}$, $q_{22} = -1$; $m = 24$.

Proof. By [He04a, Th. 4], it is enough to check if there exist $\mathbb{Z}_n$-YD satisfying T2-T22.

T2(1) If

$$\begin{cases} x_1y_1 & \equiv \frac{sn}{m} \pmod n \\ x_2y_2 & \equiv \frac{sn}{m} \pmod n \\ x_1y_2 + x_2y_1 & \equiv -\frac{sn}{m} \pmod n \end{cases} \tag{2.6}$$

has a solution, where $(s, m) = 1$, then $x^2 + x + 1 \equiv 0 \pmod m$ has a solution, which implies $\alpha_1 = 0$ and $(2x+1)^2 \equiv -3 \pmod{p_i^{\alpha_i}}$ has a solution for $2 < i \le r$. It is clear that $(2x+1)^2 \equiv -3 \pmod 3$ has a solution and $(2x+1)^2 \equiv -3 \pmod{3^2}$ has not any solution. thus $\alpha_2 = 0, 1$; $(\frac{-3}{p_i}) = 1$ for $2 < i \le r$. Conversely, (2.1) has a solution by Lemma 2.2 since (2.3) has a solution when $\alpha_1 = 0$; $\alpha_2 = 0, 1$; $(\frac{-3}{p_i}) = 1$ for $2 < i \le r$.

T2(2)$_1$ (i) $2 \mid m$. If

$$\begin{cases} x_1y_1 & \equiv \frac{sn}{m} \pmod n \\ x_2y_2 & \equiv \frac{sn}{2} \pmod n \\ x_1y_2 + x_2y_1 & \equiv -\frac{sn}{m} \pmod n \end{cases} \tag{2.7}$$

has a solution, where $(s, m) = 1$, then $x^2 + x + \frac{m}{2} \equiv 0 \pmod m$ has a solution, which implies $\alpha_1 > 1$ and $(2x+1)^2 \equiv 1 \pmod{p_i^{\alpha_i}}$ by Lemma A.2 (i) for $1 < i \le r$.

(ii) $2 \nmid m$ and $2 \mid n$. Since $mx^2 + 2sx + 2s \equiv 0 \pmod{2m}$ has always a solution,

$$\begin{cases} x_1y_1 & \equiv 2sk_1 \pmod n \\ x_2y_2 & \equiv mk_1 \pmod n \\ x_1y_2 + x_2y_1 & \equiv -2sk_1 \pmod n \end{cases}$$

has a solution by Lemma 2.2 (ii), where $(s, m) = 1$ and $n = 2mk_1$.

T2 $(2)_2$ It is similar to T2 $(2)_1$.

T2 (3) (i) $2 \mid m$. Considering Lemma 2.2(i) one obtains that

$$\begin{cases} x_1y_1 & \equiv \frac{n}{2} \pmod{n} \\ x_2y_2 & \equiv \frac{n}{2} \pmod{n} \\ x_1y_2 + x_2y_1 & \equiv \frac{sn}{m} \pmod{n} \end{cases}$$

has not any solution, where $(s,m) = 1$, since $x^2 - x + \frac{m^2}{4} \equiv 0 \pmod{m}$ has not any solutions when $\alpha_1 = 1$ by Lemma A.2(i). It is clear that $\frac{m}{2}x^2 - x + \frac{m}{2} \equiv 0 \pmod{2^{\alpha_1}}$ has a solution $2^{\alpha_1 - 1}$ when $\alpha_1 > 1$.

(ii) $2 \nmid m$ and $2 \mid n$. One obtains that

$$\begin{cases} x_1y_1 & \equiv mk_1 \pmod{n} \\ x_2y_2 & \equiv mk_1 \pmod{n} \\ x_1y_2 + x_2y_1 & \equiv 2sk_1 \pmod{n} \end{cases}$$

has a solution, where $(s,m) = 1$ and $n = 2mk_1$, since $mx^2 - 2sx + m \equiv 0 \pmod{2m}$ has always a solution.

T3 $(1)_1$ By Lemma 2.2(i) and

$$\begin{cases} x_1y_1 & \equiv \frac{sn}{m} \pmod{n} \\ x_2y_2 & \equiv \frac{2sn}{m} \pmod{n} \\ x_1y_2 + x_2y_1 & \equiv \frac{-2sn}{m} \pmod{n} \end{cases}$$

where $(s,m) = 1$, one obtains

$$x^2 + 2x + 2 \equiv 0 \pmod{m}$$

and

$$(x+1)^2 \equiv -1 \pmod{m}$$

which implies $\alpha_1 = 0, 1; \alpha_2 = 0$; $(\frac{-1}{p_i}) = 1$ for $2 < i \leq r$.

T3 $(1)_2$ (i) $2 \mid m$. By Lemma 2.2(i) and

$$\begin{cases} x_1y_1 & \equiv \frac{sn}{m} \pmod{n} \\ x_2y_2 & \equiv \frac{n}{2} \pmod{n} \\ x_1y_2 + x_2y_1 & \equiv \frac{-2sn}{m} \pmod{n} \end{cases}$$

where $(s,m) = 1$, one obtains

$$x^2 + 2x + \frac{m}{2} \equiv 0 \pmod{m}$$

and

$$(x+1)^2 \equiv 1 - \frac{m}{2} \pmod{m}.$$

By Lemma A.3(ii),

$$(x+1)^2 \equiv 1 - \frac{m}{2} \pmod{2^2}$$

and

$$(x+1)^2 \equiv 1 - \frac{m}{2} \pmod{2^3}$$

has not any solutions.

$$(x+1)^2 \equiv 1 - \frac{m}{2} \pmod{2^{\alpha_1}}$$

has a solution when $\alpha_1 > 3$.

(ii) $2 \nmid m$. $n = 2mk_1$. By Lemma 2.2(i) and

$$\begin{cases} x_1y_1 & \equiv & 2sk_1 \pmod n \\ x_2y_2 & \equiv & mk_1 \pmod n \\ x_1y_2 + x_2y_1 & \equiv & -4sk_1 \pmod n \end{cases}$$

where $(s,m) = 1$, one obtains

$$mx^2 + 4sx + 2s \equiv 0 \pmod{2m}$$

has a solution.

T3 $(2)_1$ (i) $3 \mid m$. By Lemma 2.1, one has

$$\begin{cases} x_1y_1 & \equiv & \frac{sn}{3} \pmod n \\ x_2y_2 & \equiv & \frac{n}{m} \pmod n \\ x_1y_2 + x_2y_1 & \equiv & -\frac{n}{m} \pmod n \end{cases}. \tag{2.8}$$

Let $m = 3m'$. $x^2 + x + \frac{sm}{3} \equiv 0 \pmod m$. $(2x+1)^2 \equiv 1 - 4m's \pmod{p_i^{\alpha_i}}$ has a solution for $2 < i \leq r$. Consequently, $1 - 4m's \not\equiv 2 \pmod 3$ since $m's \not\equiv 2 \pmod 3$. This implies $(2x+1)^2 \equiv 1 - 4m's \pmod 3$ has a solution.

(ii) $3 \nmid m$. $n = mk$ and $k = 3k_1$. If

$$\begin{cases} x_1y_1 & \equiv & \frac{s_1n}{3} \pmod n \\ x_2y_2 & \equiv & \frac{sn}{m} \pmod n \\ x_1y_2 + x_2y_1 & \equiv & -\frac{sn}{m} \pmod n \end{cases} \tag{2.9}$$

has a solution, where $s_1 = 1$ or 2, $(s,m) = 1$. then $ms_1x^2 + 3sx + 3s \equiv 0 \pmod{3m}$ has a solution, which implies that (2.9) has a solution by Lemma 2.2.

T3$(2)_2$ (2.3) has a solution $d = 3$ with $m = 6$, $t_1 = 2$, $t_2 = 3$, $t_3 = -3$.

T3(3) (2.3) has a solution $d = 1$ with $m = 6$, $t_1 = 2$, $t_2 = 3$, $t_3 = 5$.

T4(1) (2.3) has a solution $d = 4$ with $m = 12$, $t_1 = 4$, $t_2 = 8$, $t_3 = 9$.

T4(2) (2.3) has a solution $d = 4$ with $m = 12$, $t_1 = 8$, $t_2 = 8$, $t_3 = 1$.

T5(1) (2.3) has a solution $d = 2$ with $m = 12$, $t_1 = 8$, $t_2 = 6$, $t_3 = 1$.

T5(2) (2.3) has a solution $d = 6$ with $m = 12$, $t_1 = 4$, $t_2 = 6$, $t_3 = 9$.

T6 (2.3) has a solution $d = 12$ with $m = 18$, $t_1 = 1$, $t_2 = 12$, $t_3 = 16$.

T7(1) (2.3) has a solution $d = 3$ with $m = 12$, $t_1 = 1$, $t_2 = 6$, $t_3 = -3$.

T7(2) (2.3) has a solution $d = 3$ with $m = 12$, $t_1 = -3$, $t_2 = 6$, $t_3 = 1$.

T8 (1) By

$$\begin{cases} x_1y_1 & \equiv \frac{sn}{m} \pmod n \\ x_2y_2 & \equiv \frac{3sn}{m} \pmod n \\ x_1y_2 + x_2y_1 & \equiv \frac{-3sn}{m} \pmod n \end{cases}$$

where $(s, m) = 1$, one obtains

$$x^2 + 3x + 3 \equiv 0 \pmod m. \tag{2.10}$$

By Lemma A.2, $x^2+3x+3 \equiv 0 \pmod 2$ does not have any solutions, which implies $\alpha_1 = 0$; $(2x+3)^2 \equiv -3 \pmod{p^{\alpha_i}}$ for $2 < i \le r$, which implies $(\frac{-3}{p_i}) = 1$ for $2 < i \le r$; $(2x+3)^2 \equiv -3 \pmod 3$ has a solution and $(2x+3)^2 \equiv -3 \pmod{3^2}$ does not have any solutions, which implies $\alpha_2 = 0, 1$.

T8(2)$_1$ (2.3) has a solution $d = 4$ with $m = 8$, $t_1 = 5$, $t_2 = 4$, $t_3 = 1$.

T8(2)$_2$ (2.3) has a solution $d = 4$ with $m = 8$, $t_1 = -2$, $t_2 = 4$, $t_3 = 1$.

T8(3) (2.3) has a solution $d = 1$ with $m = 8$, $t_1 = 2$, $t_2 = -1$, $t_3 = 1$.

T9 (2.4) has a solution $d = 6$ with $m = 18$, $t_1 = -6$, $t_2 = 9$, $t_3 = 2$.

T10 (2.3) has a solution $d = 16$ with $m = 24$, $t_1 = -6$, $t_2 = -8$, $t_3 = 1$.

T11(1) (2.4) has a solution $d = 8$ with $m = 10$, $t_1 = 2$, $t_2 = 5$, $t_3 = -6$.

T11 (2) (2.3) has a solution $d = 7$ with $m = 20$, $t_1 = 1$, $t_2 = 10$, $t_3 = -3$.

T12 (2.3) has a solution $d = 10$ with $m = 30$, $t_1 = 1$, $t_2 = 20$, $t_3 = -3$.

T13 (2.3) has a solution $d = 5$ with $m = 24$, $t_1 = 6$, $t_2 = -1$, $t_3 = 1$.

T14 (2.3) has a solution $d = 9$ with $m = 18$, $t_1 = 1$, $t_2 = 9$, $t_3 = -4$.

T15 (2.3) has a solution $d = 11$ with $m = 30$, $t_1 = 12$, $t_2 = -1$, $t_3 = 1$.

T16 (1) (2.3) has a solution $d = 5$ with $m = 10$, $t_1 = 1$, $t_2 = 5$, $t_3 = -4$.

T16 (2) (2.3) has a solution $d = 10$ with $m = 20$, $t_1 = -4$, $t_2 = 10$, $t_3 = 1$.

T17 (2.3) has a solution $d = 4$ with $m = 24$, $t_1 = 16$, $t_2 = 12$, $t_3 = 1$.

T18 (2.3) has a solution $d = 5$ with $m = 30$, $t_1 = 20$, $t_2 = 15$, $t_3 = 1$.

T19 (2.5) becomes $x^2 + 3x + 7 \equiv 0 \pmod{14}$, which does not have any solution by Lemma A.2(i).

T20 (2.3) has a solution $d = 15$ with $m = 30$, $t_1 = -6$, $t_2 = 15$, $t_3 = 1$.

T21 (2.3) has a solution $d = 7$ with $m = 24$, $t_1 = 1$, $t_2 = 12$, $t_3 = -5$.

T22 (2.5) becomes $x^2 + 5x + 7 \equiv 0 \pmod{14}$, which does not have any solutions by Lemma A.2(i). ■

Proposition 2.8. *If $(V, (q_{ij})_{2\times 2})$ is a braided vector space and q_{ij} is a root of unit for $i, j = 1, 2$, then $\dim \mathfrak{B}(V) < \infty$ if and only if $\Delta(\mathfrak{B}(V))$ is finite.*

Proof. It is clear that $\Delta(\mathfrak{B}(V))$ is finite if $\dim \mathfrak{B}(V) < \infty$ by [He06b]. Conversely, if $\Delta(\mathfrak{B}(V))$ is finite, then the generalized Dynkin diagram of V is in [He05c, Table 1]. It follows $\dim \mathfrak{B}(V) < \infty$ from [He04a, Th. 4]. ■

3. Rank 3 Nichols algebras of diagonal type

In this section we present all finite dimensional Nichols algebras with diagonal type of connected 3-dimensional $\mathbb{Z}_n$-YD modules.

Let $|u|$ denote length of word u.

Lemma 3.1. *(*i) *If* $|u|=|v|$, *then* $u<v$ *if and only if* $uw<vw$.

*(*ii) *If* $u=vw$ *is the Shirshow decomposition of Lyndon word* u *and* $[u]$ *is hard, then both* $[v]$ *and* $[w]$ *are hard too.*

Proof. (i) It is clear.

(ii) If $[w]$ is not hard, then there exist words $w_i>w$ and $k_i\in k$ such that $w=\sum_{i=1}^m k_iw_i$ by [Kh99, Cor. 3.2.4]. Consequently, $u=vw=\sum_{i=1}^m k_ivw_i$ and $[u]$ is not a hard word by [Kh99, Cor. 3.2.4]. This is a contradiction. If $[v]$ is not hard, then there exist words $v_i>v$ and $k_i\in k$ such that $v=\sum_{i=1}^m k_iv_i$ by [Kh99, Cor. 3.2.4]. Consequently, $u=vw=\sum_{i=1}^m k_iv_iw$ and $v_iw>vw$ by Part (i), which implies that $[u]$ is not a hard word by [Kh99, Cor. 3.2.4]. ■

Let χ_u and g_u denote $\chi_{i_1}*\chi_{i_2}*\cdots*\chi_{i_r}$ and $g_{i_1}g_{i_2}\cdots g_{i_r}$, respectively, for any homogeneous element $u\in\mathfrak{B}(V)$ with $deg(u)=g_{i_1}g_{i_2}\cdots g_{i_r}$, where $(\chi_{i_1}*\chi_{i_2}*\cdots\chi_{i_r})(g)=\chi_{i_1}(g)\chi_{i_2}(g)\cdots\chi_{i_r}(g)$. Define

$$[u,v]=vu-p_{v,u}uv \qquad (3.1)$$

and $[u,v]_c=[v,u]$, where $p_{u,v}=\chi_v(g_u)$. By [ZZ04], $(\mathfrak{B}(V),[\ ]_c)$ is a braided m-Lie algebra and we have the braided Jacobi identity as follows:

$$[[u,v],w]=[u,[v,w]]+p_{vw}^{-1}[[u,w],v]+(p_{wv}-p_{vw}^{-1})v\cdot[u,w]. \qquad (3.2)$$

Recall duality $\mathfrak{B}(V^*)$ of Nichols algebra $\mathfrak{B}(V)$ in [He05, Section 1.3] and [He06b]. Let y_1,y_2,y_3 be a dual basis of x_1,x_2,x_3. $\delta(y_i)=g_i^{-1}\otimes y_i$, $g_i\cdot y_j=q_{ij}^{-1}y_j$ and $\Delta(y_i)=g_i^{-1}\otimes y_i+y_i\otimes 1$. There exists a bilinear map $<,>$ from $(\mathfrak{B}(V^*)\#kG)\times\mathfrak{B}(V)$ to $\mathfrak{B}(V)$ such that $<y_i,uv>=<y_i,u>v+g_i^{-1}.u<y_i,v>$ and $<y_i,<y_j,u>>=<y_iy_j,u>$ for any $u,v\in\mathfrak{B}(V)$ and $i=1,2,3$. Furthermore, for any $u\in\oplus_{i=1}^\infty\mathfrak{B}(V)_{(i)}$, one has that $u=0$ if and only if $<y_i,u>=0$ for $i=1,2,3$. We often use this to show many relations.

Let $1,2,3$ denote x_1,x_2,x_3 in short, respectively.

Lemma 3.2. *Let* $q_{11}=-1$, $q_{23}q_{32}=1$. *Then*

(i) *1)* $<y_k,[j,i]>=0,\forall\ k\neq j$.

2) $[[1,3],2]=q_{32}^{-1}[[1,2],3]$, $<y_i,[[1,3],2]>=0$, *for* $i=2,3$.

3) $[2,3]=0$ *and* $32=q_{32}23$.

4) $[1,[1,2]]=[1,[1,3]]=0$.

(ii) $<y_1,[[1,3],2]>=(q_{12}^{-1}-q_{21})(q_{13}^{-1}-q_{31})23$.

(iii) $<y_1,[[1,2],[1,3]]>=-q_{12}^{-1}q_{13}^{-1}(1-q_{12}q_{21}q_{31}q_{13})[2,[1,3]]$
$=q_{13}^{-1}(1-q_{12}q_{21}q_{31}q_{13})(q_{32}231-q_{12}^{-1}312+q_{12}^{-1}q_{31}q_{32}123-q_{31}q_{32}213)$.

(iv) $<y_1,[[[1,2],[1,3]],2]>=-q_{12}^{-1}q_{13}^{-1}(1-q_{12}q_{21}q_{31}q_{13})\left(q_{12}^{-1}2[2[1,3]]\right.$
$\left.-q_{21}^2q_{22}q_{23}[2[1,3]]2\right)$.

(v) *Furthermore, if* $(q_{22}+1)(q_{22}q_{12}q_{21}-1)=(q_{33}+1)(q_{33}q_{13}q_{31}-1)=0$, *then*

1) $[[1,2],2]=[[1,3],3]=0$.

2) $[[1,2],[[1,3],2]]=[[[1,2],[1,3]],2]$.

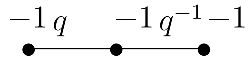
(vi) *Furthermore, if* $q_{22}=q_{33}=-1$, *then* $<y_1,[[1,3],[[1,3],2]]>$

$= \{-(q_{12}^{-1} - q_{21})(q_{13}^{-1} - q_{31})q_{31} + q_{11}^{-1}q_{13}^{-1}q_{12}^{-1}(q_{13}^{-1} - q_{31})$
$+q_{11}q_{13}q_{31}q_{33}q_{21}(q_{13}^{-1} - q_{31})q_{31}\}2313 + \{-q_{11}^{-1}q_{13}^{-1}q_{12}^{-1}q_{21}q_{23}(q_{13}^{-1} - q_{31})$
$-q_{11}q_{13}q_{31}q_{33}q_{21}q_{23}(q_{13}^{-1} - q_{31})q_{21}q_{31} - q_{31}q_{33}q_{21}q_{23}(q_{12}^{-1} - q_{21})(q_{13}^{-1} - q_{31})\}3123.$

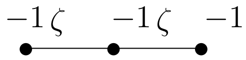
(vii) *Furthermore, if* $q_{22} = q_{33} = -1$, *then* $< y_1, [[[1,2],[1,3]],[1,3]] >$
$= q_{13}^{-2}q_{12}^{-1}(1 - q_{12}q_{21}q_{31}q_{13} - q_{12}q_{21}q_{31}q_{13}q_{33} + q_{12}q_{21}q_{31}^2q_{13}^2q_{33})[1,3]^2 2$
$+q_{12}q_{32}^2q_{13}^{-1}q_{31}(1 - q_{31}q_{13} - q_{31}q_{13}q_{33} + q_{12}q_{21}q_{31}^2q_{13}^2q_{33})2[1,3]^2$
$+q_{32}q_{13}^{-2}(-1 + q_{31}q_{13}q_{33} + q_{12}q_{21}q_{31}^2q_{13}^2 - q_{12}q_{21}q_{31}^3q_{13}^3q_{33})[1,3]2[1,3].$

(viii) *Furthermore, if* $q_{22} = q_{33} = -1$, *then* $< y_1, [[1,2],[[1,2],[1,3]]] >$
$= \{(q_{12}^{-1} - q_{21}) - (1 - q_{12}q_{21}q_{31}q_{13})q_{21}q_{22}\}q_{12}^{-1}q_{13}^{-1}[1,3][1,2]2$
$+q_{13}^{-1}q_{32}(1 - q_{12}q_{21}q_{31}q_{13} - q_{12}q_{21}q_{22}q_{31}q_{13} + q_{12}^2q_{21}^2q_{22}q_{31}q_{13})2[1,3][1,2]$
$+q_{13}^{-1}q_{32}q_{31}\{(q_{12}^{-1} - q_{21}) - (1 - q_{12}q_{21}q_{31}q_{13})q_{21}q_{22}\}[1,2][1,3]2$
$+q_{13}^{-1}q_{21}q_{22}q_{32}^2q_{12}q_{31}(1 - q_{12}q_{21}q_{31}q_{13} - q_{12}q_{21}q_{22}q_{31}q_{13} + q_{12}^2q_{21}^2q_{22}q_{31}q_{13})[1,2]2[1,3].$

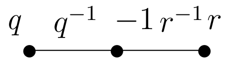
According to [He05c, Table 2], the first node, second node and third node of every generalized Dynkin diagram denote q_{33}, q_{11}, q_{22}, respectively. Let $\mathbb{B}_V$ be the set of all hard super-letters in $\mathfrak{B}(V)$ (i.e. the generators of PBW basis. Hard super-letters were defined in [Kh99, Def. 6]) .

Theorem 3.3. (i) *If* 

, $q \in R_m, m > 2$, *then* $\mathbb{B}_V = \{[x_1],[x_2],[x_3],[x_1,x_2],[x_1,x_3],[[x_1,x_3],x_2]\}$ *and* $\dim \mathfrak{B}(V) = 2^4 m^2$.

(ii) *If* 

, $\zeta \in R_3$,
then $\mathbb{B}_V = \{[x_1],[x_2],[x_3],[x_1,x_2],[x_1,x_3],[[x_1,x_3],x_2],[[x_1,x_2],[x_1,x_3]],$
$[[x_1,x_2],[[x_1,x_3],x_2]],[[x_1,x_3],[[x_1,x_3],x_2]],[[[x_1,x_2],[[x_1,x_3],x_2]],[x_1,x_3]]\}$
and $\dim \mathfrak{B}(V) = 2^7 3^4$.

(iii) *If* 

, $q \in R_m, r \in R_{m'}, q \neq r, rq \neq 1; m, m' > 1$,
then $\mathbb{B}_V = \{[x_1],[x_2],[x_3],[x_1,x_2],[x_1,x_3],[[x_1,x_3],x_2],[[x_1,x_2],[x_1,x_3]]\}$ *and*
$\dim \mathfrak{B}(V) = 2^4 \frac{m^2 m'^2}{(m,m')}$.

Proof. Assume that $[u]$ is a hard super-letter or zero and $u = vw$ is the Shirshow decomposition of u when $[u] \neq 0$. Applying Lemma 3.2 we can show $[u] \in \mathbb{B}_V$ step by step for the length $\mid u \mid$ of u. ■

Lemma 3.4. *Let* $n = km$ *and* $(s,m) = 1$. $t_1, t_2, t_3 \in \mathbb{Z}$. *If* $t_1 \equiv 1 \pmod n$, *then the following conditions are equivalent.*

(i)

$$\begin{cases} x_1y_1 & \equiv t_1sk \pmod n \\ x_2y_2 & \equiv t_2sk \pmod n \\ x_3y_3 & \equiv t_3sk \pmod n \\ x_1y_2 + x_2y_1 & \equiv t_4sk \pmod n \\ x_1y_3 + x_3y_1 & \equiv t_5sk \pmod n \\ x_3y_2 + x_2y_3 & \equiv t_6sk \pmod n \end{cases} \tag{3.3}$$

has a solution

(ii)

$$\begin{cases} t_1(x_2)^2 - t_4x_2 + t_2 & \equiv 0 & (mod\ m) \\ t_1(x_3)^2 - t_5x_3 + t_3 & \equiv 0 & (mod\ m) \\ x_1 & \equiv 1 & (mod\ n) \\ y_1 & \equiv t_1ks & (mod\ n) \\ y_2 & \equiv (t_4 - x_2t_1)ks & (mod\ n) \\ y_3 & \equiv (t_5 - x_3t_1)ks & (mod\ n) \\ x_1y_1 & \equiv t_1sk & (mod\ n) \\ x_2y_2 & \equiv t_2sk & (mod\ n) \\ x_3y_3 & \equiv t_3sk & (mod\ n) \\ x_1y_2 + x_2y_1 & \equiv t_4sk & (mod\ n) \\ x_1y_3 + x_3y_1 & \equiv t_5sk & (mod\ n) \\ x_3y_2 + x_2y_3 & \equiv t_6sk & (mod\ n) \end{cases} \tag{3.4}$$

has a solution.

(iii)

$$\begin{cases} t_1(x_2)^2 - t_4x_2 + t_2 & \equiv 0 & (mod\ m) \\ t_1(x_3)^2 - t_5x_3 + t_3 & \equiv 0 & (mod\ m) \\ x_1 & \equiv 1 & (mod\ n) \\ y_1 & \equiv t_1ks & (mod\ n) \\ y_2 & \equiv (t_4 - x_2t_1)ks & (mod\ n) \\ y_3 & \equiv (t_5 - x_3t_1)ks & (mod\ n) \\ 2t_1x_2x_3 - t_4x_3 - t_5x_2 & \equiv -t_6 & (mod\ m) \end{cases} \tag{3.5}$$

has a solution.

Lemma 3.5. *Let $n = km$ and $(s, m) = 1$; $t_1, t_2, t_3 \in \mathbb{Z}$. If $(m, t_1) = 1$, then*

$$\begin{cases} x_1y_1 & \equiv t_1sk & (mod\ n) \\ x_2y_2 & \equiv t_2sk & (mod\ n) \\ x_3y_3 & \equiv t_3sk & (mod\ n) \\ x_1y_2 + x_2y_1 & \equiv t_4sk & (mod\ n) \\ x_1y_3 + x_3y_1 & \equiv t_5sk & (mod\ n) \\ x_3y_2 + x_2y_3 & \equiv t_6sk & (mod\ n) \end{cases} \tag{3.6}$$

has a solution if and only if

$$\begin{cases} t_1(x_2)^2 - t_4x_2 + t_2 & \equiv 0 & (mod\ m) \\ t_1(x_3)^2 - t_5x_3 + t_3 & \equiv 0 & (mod\ m) \\ x_1 & \equiv 1 & (mod\ m) \\ y_1 & \equiv t_1 & (mod\ m) \\ y_2 & \equiv (t_4 - x_2t_1) & (mod\ m) \\ y_3 & \equiv (t_5 - x_3t_1) & (mod\ m) \\ x_1y_2 + x_2y_1 & \equiv t_4 & (mod\ m) \\ x_1y_3 + x_3y_1 & \equiv t_5 & (mod\ m) \\ x_3y_2 + x_2y_3 & \equiv t_6 & (mod\ m) \end{cases} \tag{3.7}$$

has a solution.

Lemma 3.6. *Let f denote the lowest common multiple of m and m' with $(s,m)=1=(s',m')$ and $m,m'>1$. Then*

$$\begin{cases} x_1y_1 & \equiv \frac{n}{2} \quad (mod\ n) \\ x_2y_2 & \equiv \frac{sn}{m} \quad (mod\ n) \\ x_3y_3 & \equiv \frac{s'n}{m'} \quad (mod\ n) \\ x_1y_2+x_2y_1 & \equiv -\frac{sn}{m} \quad (mod\ n) \\ x_1y_3+x_3y_1 & \equiv -\frac{s'n}{m'} \quad (mod\ n) \\ x_3y_2+x_2y_3 & \equiv 0 \quad (mod\ n) \end{cases} \tag{3.8}$$

has a solution if and only if $\alpha_i=\alpha_i'$ when $\alpha_i\alpha_i'\neq 0$ for $1\leq i\leq t$, and

$$-s\equiv m''s' \quad (mod\ m') \tag{3.9}$$

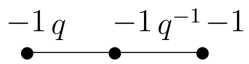
when $m=m''m'$ and $(m',m'')=1$;

$$-s'\equiv m''s \quad (mod\ m) \tag{3.10}$$

when $m'=m''m$ and $(m,m'')=1$. Here $m = 2^{\alpha_1}3^{\alpha_2}p_3^{\alpha_3}\cdots p_t^{\alpha_t}$, $m' = 2^{\alpha_1'}3^{\alpha_2'}p_3^{\alpha_3'}\cdots p_t^{\alpha_t'}$ be the prime decomposition, respectively.

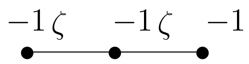
Theorem 3.7. *If $(V,(q_{ij})_{3\times 3})$ is a braided vector space, then V is a connected $\mathbb{Z}_n$-YD module such that $\dim\mathfrak{B}(V)<\infty$ if and only if one of the following conditions holds:*

(i) *The generalized Dynkin diagram of V is Weyl equivalent to*



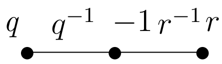
, $q\in R_m, m>2$.

(ii) *The generalized Dynkin diagram of V is Weyl equivalent to*



, $\zeta\in R_3$.

(iii) *The generalized Dynkin diagram of V is Weyl equivalent to*



; *$\alpha_i=\alpha_i'$ when $\alpha_i\alpha_i'\neq 0$ for $1\leq i\leq t$; $-s\equiv m''s' \quad (mod\ m')$ when $m=m''m'$ and $(m'',m')=1$; $-s\equiv m''s' \quad (mod\ m)$ when $m'=m''m$ and $(m,m'')=1$; Here $q\in R_m, r\in R_{m'}, \omega\in R_n$, $m>1, m'>1; q\neq r, q\neq r^{-1}$; $(s,m)=1$; $(s',m')=1$; $q=\omega^{\frac{ns}{m}}$, $r=\omega^{\frac{ns'}{m'}}$; $m=2^{\alpha_1}3^{\alpha_2}p_3^{\alpha_3}\cdots p_t^{\alpha_t}$, $m'=2^{\alpha_1'}3^{\alpha_2'}p_3^{\alpha_3'}\cdots p_t^{\alpha_t'}$ be the prime decomposition, respectively.*

Proof. *The necessity.* By [He05c, Th. 12], we only need to consider the generalized Dynkin diagrams in [He05c, Table 2]. The Dynkin diagrams above are in Row 8, 9, 15 of [He05c, Table 2]. So we need to exclude the Dynkin diagrams in all other Rows of [He05c, Table 2]. This follows from the application of Lemma

2.1 and Lemma 3.4. For instance, Row 1 of [He05c, Table 2]. By Lemma 2.1,

$$\begin{cases} x_1y_1 & \equiv \ sk \pmod n \\ x_2y_2 & \equiv \ sk \pmod n \\ x_3y_3 & \equiv \ sk \pmod n \\ x_1y_2+x_2y_1 & \equiv \ -sk \pmod n \\ x_1y_3+x_3y_1 & \equiv \ -sk \pmod n \\ x_3y_2+x_2y_3 & \equiv \ 0 \pmod n \end{cases}$$

has a solution. Thus by Lemma 3.4

$$\begin{cases} x_1 & \equiv \ 1 & \pmod n \\ y_1 & \equiv \ ks & \pmod n \\ y_2 & \equiv \ (-1-x_2)ks & \pmod n \\ y_3 & \equiv \ (-1-x_3)ks & \pmod n \\ (x_2)^2+x_2+1 & \equiv \ 0 & \pmod m \\ (x_3)^2+x_3+1 & \equiv \ 0 & \pmod m \\ 2x_2x_3+x_2+x_3 & \equiv \ 0 & \pmod m \end{cases}$$

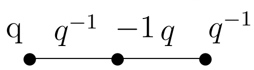
has a solution, which implies that $2 \nmid m$ and

$$\begin{cases} (2x_2+1)^2 & \equiv \ -3 & \pmod m \\ (2x_3+1)^2 & \equiv \ -3 & \pmod m \\ (2x_2+1)(2x_3+1) & \equiv \ 1 & \pmod m \end{cases}$$

has a solution. One gets $9 \equiv 1 \pmod m$, which is a contradiction. So the diagram in Row 1 of [He05c, Table 2] is excluded. By similar procedure, we can exclude the generalized Dynkin diagrams in all other Rows except those in Rows 8, 9, 15 of [He05c, Table 2] .

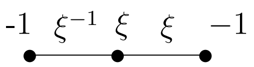
The sufficiency. It follows from Lemma 3.3 that $\dim \mathfrak{B}(V) < \infty$ when the generalized Dynkin diagrams are in Row 8, 9, 15 of [He05c, Table 2]. By [He05c, Th. 12], we need to decide if Row 8, Row 9 and Row 15 in [He05c, Table 2] are kG- YD modules.

(i) Row 8 [He05c, Table 2]. There exists a DDG



, $q \in R_m$, in Row 8 [He05c, Table 2]. It follows from Lemma 3.6 when one sets $s = -s'$.

(ii) Row 15 [He05c, Table 2]. There exists a DDG



, $\xi \in R_3$, in Row 15 [He05c, Table 2].

$$\begin{cases} x_1y_1 & \equiv \ 2sk \pmod{6k} \\ x_2y_2 & \equiv \ 3sk \pmod{6k} \\ x_3y_3 & \equiv \ 3sk \pmod{6k} \\ x_1y_2+x_2y_1 & \equiv \ 2sk \pmod{6k} \\ x_3y_1+x_1y_3 & \equiv \ -2sk \pmod{6k} \\ x_2y_3+x_3y_2 & \equiv \ 0 \pmod{6k} \end{cases}$$

has a solution: $x_2 = 1, y_2 = 3ks,\ x_1 = 4, y_1 = 2sk,\ x_3 = 5, y_3 = 3ks$.

(iii) Row 9 [He05c, Table 2]. It follows from Lemma 3.6. ■

4. Nichols algebras of diagonal type with rank > 3

In this section we prove that finite dimensional Nichols algebra over $\mathbb{Z}_2$ is a quantum linear space and Nichols algebra of connected $\mathbb{Z}_n$-YD module V with $\dim V > 3$ is infinite dimensional.

Theorem 4.1. *If V is a connected $k\mathbb{Z}_n$-Yetter-Drinfeld module with diagonal type and rank > 3, then $\dim \mathfrak{B}(V) = \infty$ and $\Delta(\mathfrak{B}(V))$ is infinite.*

Proof. It is enough to show this is the case for $\dim V = 4$.

Except Row 18, Row 20, Row 21, Row 22, all GDDs in [He06a, Table B] contain GDDs in [He05c, Table 2]. By Theorem 3.7, these four cases are not GDDs of any kG-YD modules.

(i) Row 18. $n = mk$, $m = 6$, $(s, m) = 1$. By Lemma 2.1,

$$\begin{cases} x_1y_1 & \equiv -2sk \pmod n \\ x_2y_2 & \equiv -2sk \pmod n \\ x_3y_3 & \equiv 2sk \pmod n \\ x_1y_2 + x_2y_1 & \equiv 2sk \pmod n \\ x_1y_3 + x_3y_1 & \equiv 0 \pmod n \\ x_3y_2 + x_2y_3 & \equiv 2sk \pmod n \end{cases}$$

has a solution. Let $s_1 = 2s$. Obviously, $(s_1, 3) = 1$. Thus

$$\begin{cases} x_1y_1 & \equiv -s_1k \pmod{3k} \\ x_2y_2 & \equiv -s_1k \pmod{3k} \\ x_3y_3 & \equiv s_1k \pmod{3k} \\ x_1y_2 + x_2y_1 & \equiv s_1k \pmod{3k} \\ x_1y_3 + x_3y_1 & \equiv 0 \pmod{3k} \\ x_3y_2 + x_2y_3 & \equiv s_1k \pmod{3k} \end{cases}$$

has a solution. Thus by Lemma 3.4

$$\begin{cases} x_3 & \equiv 1 & \pmod{3k} \\ y_3 & \equiv s_1k & \pmod{3k} \\ y_1 & \equiv -x_1s_1k & \pmod{3k} \\ y_2 & \equiv (1 - x_2)s_1k & \pmod{3k} \\ (x_1)^2 - 1 & \equiv 0 & \pmod 3 \\ (x_2)^2 - x_2 - 1 & \equiv 0 & \pmod 3 \\ -2x_1x_2 + x_1 & \equiv 1 & \pmod 3 \end{cases}$$

has a solution, which implies that

$$\begin{cases} (2x_2 - 1)^2 & \equiv 5 \pmod 3 \\ (x_1)^2 & \equiv 1 \pmod 3 \\ x_1(-2x_2 + 1) & \equiv 1 \pmod 3. \end{cases}$$

One gets $5 \equiv 1 \pmod 3$, which is a contradiction.

(ii) Row 20. $n = mk$, $m = 6$, $(s, m) = 1$. Consider the last GDD in Row 21. By Lemma 2.1,

$$\begin{cases} x_1y_1 & \equiv 2sk \pmod n \\ x_2y_2 & \equiv 2sk \pmod n \\ x_3y_3 & \equiv -2sk \pmod n \\ x_1y_2 + x_2y_1 & \equiv -2sk \pmod n \\ x_1y_3 + x_3y_1 & \equiv 0 \pmod n \\ x_3y_2 + x_2y_3 & \equiv 2sk \pmod n \end{cases}$$

has a solution. Let $s_1 = 2s$. Obviously, $(s_1, 3) = 1$. Thus

$$\begin{cases} x_1y_1 & \equiv s_1k \pmod{3k} \\ x_2y_2 & \equiv s_1k \pmod{3k} \\ x_3y_3 & \equiv -s_1k \pmod{3k} \\ x_1y_2 + x_2y_1 & \equiv -s_1k \pmod{3k} \\ x_1y_3 + x_3y_1 & \equiv 0 \pmod{3k} \\ x_3y_2 + x_2y_3 & \equiv s_1k \pmod{3k} \end{cases}$$

has a solution. Thus by Lemma 3.4

$$\begin{cases} x_1 & \equiv 1 & \pmod{3k} \\ y_1 & \equiv s_1k & \pmod{3k} \\ y_2 & \equiv (-1 - x_2)s_1k & \pmod{3k} \\ y_3 & \equiv (-x_3)s_1k & \pmod{3k} \\ (x_2)^2 + x_2 + 1 & \equiv 0 & \pmod 3 \\ (x_3)^2 - 1 & \equiv 0 & \pmod 3 \\ 2x_2x_3 + x_3 & \equiv -1 & \pmod 3 \end{cases}$$

has a solution, which implies that

$$\begin{cases} (2x_2 + 1)^2 & \equiv -3 & \pmod 3 \\ (x_3)^2 & \equiv 1 & \pmod 3 \\ x_3(2x_2 + 1) & \equiv -1 & \pmod 3). \end{cases}$$

One gets $-3 \equiv 1 \pmod 3$, which is a contradiction.

(iii) Row 21. $n = mk$, $m = 6$, $(s, m) = 1$. Consider the last GDD in Row 21. By Lemma 2.1,

$$\begin{cases} x_1y_1 & \equiv 2sk \pmod n \\ x_2y_2 & \equiv 2sk \pmod n \\ x_3y_3 & \equiv 2sk \pmod n \\ x_1y_2 + x_2y_1 & \equiv -2sk \pmod n \\ x_1y_3 + x_3y_1 & \equiv 0 \pmod n \\ x_3y_2 + x_2y_3 & \equiv -2sk \pmod n \end{cases}$$

has a solution. Let $s_1 = 2s$. Obviously, $(s_1, 3) = 1$. Thus

$$\begin{cases} x_1y_1 & \equiv s_1k \pmod{3k} \\ x_2y_2 & \equiv s_1k \pmod{3k} \\ x_3y_3 & \equiv s_1k \pmod{3k} \\ x_1y_2 + x_2y_1 & \equiv -s_1k \pmod{3k} \\ x_1y_3 + x_3y_1 & \equiv 0 \pmod{3k} \\ x_3y_2 + x_2y_3 & \equiv -s_1k \pmod{3k} \end{cases}$$

has a solution. Thus by Lemma 3.4

$$\begin{cases} x_1 & \equiv & 1 & \pmod{3k} \\ y_1 & \equiv & s_1 k & \pmod{3k} \\ y_2 & \equiv & (-1-x_2)s_1 k & \pmod{3k} \\ y_3 & \equiv & (-x_3)s_1 k & \pmod{3k} \\ (x_2)^2 + x_2 + 1 & \equiv & 0 & \pmod{3} \\ (x_3)^2 + 1 & \equiv & 0 & \pmod{3} \\ 2x_2x_3 + x_3 & \equiv & 1 & \pmod{3} \end{cases}$$

has a solution, which implies that

$$\begin{cases} (2x_2+1)^2 & \equiv & -3 & \pmod{3} \\ (x_3)^2 + 1 & \equiv & 0 & \pmod{3} \\ x_3(2x_2+1) & \equiv & 1 & \pmod{3} \end{cases}.$$

One gets $0 \equiv 1 \pmod{3}$, which is a contradiction.

(iv) Row 22. $n = mk$, $m = 4$, $(s, m) = 1$. By Lemma 2.1,

$$\begin{cases} x_3y_3 & \equiv & sk & \pmod{n} \\ x_4y_4 & \equiv & 3sk & \pmod{n} \\ x_4y_3 + x_3y_4 & \equiv & sk & \pmod{n} \end{cases}$$

has a solution. By Lemma 2.3 (i),

$$x^2 - x + 3 \equiv 0 \pmod{4}$$

has a solution, which contradicts to Lemma A.2(i). ∎

Corollary 4.2. (i) *If V is a connected finite dimensional* YD *module over $\mathbb{Z}_n$ with* $\dim \mathfrak{B}(V) < \infty$, *then* $\dim V < 4$.

(ii) *If V is a finite dimensional* YD *module over $\mathbb{Z}_n$ with* $\dim \mathfrak{B}(V) < \infty$, *then dimension of every connected component of V is lesser than 4.*

Proof. (i) It follows from Theorem 4.1.

(ii) It follows from Part (i) and [AS00, Lemma 4.2]. ∎

Corollary 4.3. *If V is a finite dimensional* YD *module over $\mathbb{Z}_n$ with braided matrix (q_{ij}) and* $\operatorname{ord}(q_{ii}) \neq 1$, *then the following conditions are equivalent:*

(i) $\dim \mathfrak{B}(V) < \infty$.

(ii) $\Delta(\mathfrak{B}(V))$ *is finite.*

(iii) $(\Delta(\mathfrak{B}(V)), \chi_0, E_0)$ *is an arithmetic root system.*

The concept of quantum linear spaces was introduced in [AS98, P673]. In this case, $q_{ij}q_{ji} = 1$ for $i \neq j$.

Corollary 4.4. *Every finite dimensional Nichols algebra over $\mathbb{Z}_2$ is a quantum linear space.*

Corollary 4.5. *Assume that $(V,(q_{ij})_{2\times 2})$ is a braided vector space.*

(I) *If p is a prime number, then V is a connected $\mathbb{Z}_p$-YD module such that $\dim \mathfrak{B}(V) < \infty$ if and only if one of the following conditions holds:*

T2(1) $1-q_{11}q_{12}q_{21} = 1-q_{12}q_{21}q_{22} = 0$, $q_{12}q_{21} \in R_p$; $p=3$ *or* $p>3$ *and* $(\frac{-3}{p})=1$.

T2(2)$_1$ $1+q_{11} = 1-q_{12}q_{21}q_{22} = 0$, $q_{12}q_{21} \in R_p$; $p>2$.

T2(2)$_2$ $1+q_{22} = 1-q_{12}q_{21}q_{11} = 0$, $q_{12}q_{21} \in R_p$, $p>2$.

T2(3) $1+q_{11} = 1+q_{22} = 0$, $q_{12}q_{21} \in R_p$, $p>2$.

T3(1)$_1$ $q_{12}q_{21} = q_{11}^{-2}$, $q_{22} = q_{11}^2$, $q_{11} \in R_p$; $p>3$ *and* $p \equiv 1 \pmod 4$.

T3(1)$_2$ $q_{12}q_{21} = q_{11}^{-2}$, $q_{22} = -1$, $q_{11} \in R_p$; $p>2$.

T8(1) $q_{12}q_{21} = q_{11}^{-3}$, $q_{22} = q_{11}^3$, $q_{11} \in R_p$, $p>3$ *and* $(\frac{-3}{p})=1$.

(II) *Let p be a prime number, $n=p^\beta$ and $m=p^\alpha$ with $0<\alpha\le\beta$ and $\beta>1$. Then V is a connected $\mathbb{Z}_n$-YD module such that $\dim\mathfrak{B}(V)<\infty$ if and only if one of the following conditions holds:*

T2(1) $1-q_{11}q_{12}q_{21} = 1-q_{12}q_{21}q_{22} = 0$, $q_{12}q_{21} \in R_m$; $p=3, \alpha=1$; $p>3$ *and* $(\frac{-3}{p})=1$.

T2(2)$_1$ $1+q_{11} = 1-q_{12}q_{21}q_{22} = 0$, $q_{12}q_{21} \in R_m$; $p=2, \alpha>1$; $p>2$.

T2(2)$_2$ $1+q_{22} = 1-q_{12}q_{21}q_{11} = 0$, $q_{12}q_{21} \in R_m$; $p=2, \alpha>1$; $p>2$.

T2(3) $1+q_{11} = 1+q_{22} = 0$, $q_{12}q_{21} \in R_m$; $p=2, \alpha>1$; $p>2$.

T3(1)$_1$ $q_{12}q_{21} = q_{11}^{-2}$, $q_{22} = q_{11}^2$, $q_{11} \in R_m$, $m>2$; $p>3$ *and* $p \equiv 1 \pmod 4$.

T3(1)$_2$ $q_{12}q_{21} = q_{11}^{-2}$, $q_{22} = -1$, $q_{11} \in R_m$, $m>2$; $p=2$, $\alpha>3$; $p>2$.

T3(2)$_1$ $\omega \in R_n$, $s=1,2$; $q_{11} = \omega^{\frac{ns}{3}}$, $q_{22} = \omega^{\frac{n}{m}}$, $q_{12}q_{21}q_{22} = 1$, $m>3$; $p=3$ *and* $\alpha>1$.

T8(1) $q_{12}q_{21} = q_{11}^{-3}$, $q_{22} = q_{11}^3$, $q_{11} \in R_m$, $m>3$; $p>3$ *and* $(\frac{-3}{p})=1$.

T8(2)$_1$ $(q_{12}q_{21})^4 = -1$, $q_{22} = -1$, $q_{12}q_{21} = -q_{11}$; $m=8$; $\alpha=3$.

T8(2)$_2$ $(q_{12}q_{21})^4 = -1$, $q_{22} = -1$, $q_{11} = (q_{12}q_{21})^{-2}$; $m=8$, $\alpha=3$.

T8(3) $(q_{12}q_{21})^4 = -1$, $q_{11} = (q_{12}q_{21})^2$, $q_{22} = (q_{12}q_{21})^{-1}$; $m=8$, $\alpha=3$.

Proof. It follows from Theorem 2.7. ■

Corollary 4.6. *Assume that $(V,(q_{ij})_{3\times 3})$ is a braided vector space.*

(I) *If p is a prime number, then V is a connected $\mathbb{Z}_p$-YD module such that $\dim\mathfrak{B}(V)<\infty$ if and only if one of the following conditions holds:*

(i) *The generalized Dynkin diagram of V is Weyl equivalent to*

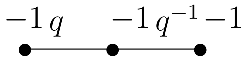
$\overset{-1}{\bullet}\overset{q}{\text{—}}\overset{-1}{\bullet}\overset{q^{-1}}{\text{—}}\overset{-1}{\bullet}$, $q \in R_p; p>2$.

(ii) *The generalized Dynkin diagram of V is Weyl equivalent to*

$\overset{q}{\bullet}\overset{q^{-1}}{\text{—}}\overset{-1}{\bullet}\overset{r^{-1}}{\text{—}}\overset{r}{\bullet}$; $-s \equiv s' \pmod p$. *Here $q,r,\omega \in R_p$, $q \ne r, q \ne r^{-1}$; $(s,p)=1$; $(s',p)=1$; $q=\omega^s$, $r=\omega^{s'}$.*

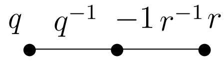
(II) *Let p be a prime number, $n=p^\beta$ and $m=p^\alpha$ with $0<\alpha\le\beta$ and $\beta>1$. Then V is a connected $\mathbb{Z}_n$-YD module such that $\dim\mathfrak{B}(V)<\infty$ if and only if one of the following conditions holds:*

(i) *The generalized Dynkin diagram of V is Weyl equivalent to*



, $q \in R_m; m > 2$; $p = 2$ *and* $\alpha > 1$ *or* $p > 2$.

(ii) *The generalized Dynkin diagram of V is Weyl equivalent to*



; $-s \equiv s' \pmod m$; $m' = m > 1$; $p = 2$ *and* $\alpha > 1$ *or* $p > 2$. *Here* $q \in R_m, r \in R_{m'}, \omega \in R_n$, $q \neq r, q \neq r^{-1}$; $(s, m) = 1$; $(s', m') = 1$; $q = \omega^{\frac{ns}{m}}$, $r = \omega^{\frac{ns'}{m'}}$.

Proof. It follows from Theorem 3.7. ■

A. Appendix

In this section, we recall some results on solutions of equation systems in $\mathbb{Z}_n$ [Hu67] and braided vector spaces.

A.1. Equation systems in $\mathbb{Z}_n$.

If prime $p \nmid a$ and $x^2 \equiv a \pmod p$ has a solution, then a is called a quadratic residue of module p. Set

$$(\frac{a}{p}) := \begin{cases} 1 & \text{when } a \text{ is a quadratic residue of module } p \\ -1 & \text{when } a \text{ is a quadratic non-residue of module } p \end{cases} . \tag{A.1}$$

This is called Legendre sign.

Lemma A.1. *Let $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$ and $f'(x) := n a_n x^{n-1} + (n-1)a_{n-1}x^{n-2} + \cdots + a_1$.*

(i) *If $f(x) \equiv 0 \pmod p$ and $f'(x) \equiv 0 \pmod p$ has not any common solution with prime number p, then $f(x) \equiv 0 \pmod{p^k}$ has a solution if and only if $f(x) \equiv 0 \pmod p$ has a solution.*

(ii) *$ax + b \equiv 0 \pmod m$ has a solution if and only if $(a, m) \mid b$.*

Lemma A.2. *Let*

$$f(x) := ax^2 + bx + c \equiv 0 \pmod{p^k}, \tag{A.2}$$

with prime p, $p \nmid (a, b, c)$ and $k \in \mathbb{N}$.

(i) *If $2 \nmid a$, $2 \nmid b$, then $2 \mid c$ if and only if (A.2) has a solution when $p = 2$.*

(ii) *If $2 \nmid a$ and $2 \mid b$, then (A.2) is equivalent to $(ax + \frac{b}{2})^2 \equiv \frac{b^2}{4} - ac \pmod{2^k}$ when $p = 2$.*

(iii) *If $p > 2$, $p \mid a$, $p \nmid b$, then (A.2) always has a solution.*

(iv) *If $p > 2$, $p \nmid a$, then (A.2) is equivalent to $(2ax + b)^2 \equiv b^2 - 4ac \pmod{p^k}$. Furthermore (A.2) has a solution if and only if $(2ax + b)^2 \equiv b^2 - 4ac \pmod p$ has a solution.*

Lemma A.3. *Let*

$$x^2 \equiv a \pmod{p^k} \tag{A.3}$$

where prime $p \nmid a$, $k \in \mathbb{N}$.

(i) *If* $p > 2$, *then the number of solution of (A.3) is* $1 + (\frac{a}{p})$.

(ii) *If* $p = 2$, *then*

(1) (A.3) has a solution when $k = 1$.

(2) (A.3) has two solutions when $k = 2$ *and* $a \equiv 1 \pmod 4$.

(3) (A.3) has not any solutions when $k = 2$ *and* $a \not\equiv 1 \pmod 4$.

(4) (A.3) has four solutions when $k > 2$ *and* $a \equiv 1 \pmod 8$.

(5) (A.3) has not any solutions when $k > 2$ *and* $a \not\equiv 1 \pmod 8$.

Lemma A.4. *Let* $m = m_1 m_2 \cdots m_r$, *where* $m_1, m_2, \cdots, m_r$ *are pairwise relatives prime. then* $f(x) \equiv 0 \pmod m$ *has a solution if and only if every equation below has a solution :*

$$\begin{array}{lcll} f(x) & \equiv & 0 & (mod\ m_1) \\ f(x) & \equiv & 0 & (mod\ m_2) \\ \cdots & \cdots & \cdots & \\ f(x) & \equiv & 0 & (mod\ m_r) \end{array}.$$

A.2. Braided vector space.

If $\sigma \in \mathbb{S}_r$ and $q_{\sigma(i),\sigma(j)} = q'_{ij}$ for any $1 \le i, j \le r$, then the two matrixes $\begin{pmatrix} q_{11} & q_{12} & \cdots & q_{1r} \\ q_{21} & q_{22} & \cdots & q_{2r} \\ \cdots & \cdots & \cdots & \cdots \\ q_{r1} & q_{r2} & \cdots & q_{rr} \end{pmatrix}$ and $\begin{pmatrix} q'_{11} & q'_{12} & \cdots & q'_{1r} \\ q'_{21} & q'_{22} & \cdots & q'_{2r} \\ \cdots & \cdots & \cdots & \cdots \\ q'_{r1} & q'_{r2} & \cdots & q'_{rr} \end{pmatrix}$ are called to be permutation similarity. In this case, GDDs of the two matrixes are called to be isomorphic.

If (q_{ij}) and (q'_{ij}) are permutation similarity, then the two braided vector spaces $(V, (q_{ij}))$ and $(V, (q'_{ij}))$ are the same since $x_{\sigma(1)}, x_{\sigma(2)}, \cdots, x_{\sigma(r)}$ is also a basis of V with $C(x_{\sigma(i)} \otimes x_{\sigma(j)}) = q_{\sigma(i)\sigma(j)} x_{\sigma(j)} \otimes x_{\sigma(i)} = q'_{ij} x_{\sigma(j)} \otimes x_{\sigma(i)}$.

Recall [ZZC04]. $(G, \overrightarrow{g}, \overrightarrow{\chi}, J)$ is called an *element system with characters* (simply, ESC) if G is a group, J is a set, $\overrightarrow{g} = \{g_i\}_{i \in J} \in Z(G)^J$ and $\overrightarrow{\chi} = \{\chi_i\}_{i \in J} \in \widehat{G}^J$ with $g_i \in Z(G)$ and $\chi_i \in \widehat{G}$. ESC$(G, \overrightarrow{g}, \overrightarrow{\chi}, J)$ and ESC$(G', \overrightarrow{g}', \overrightarrow{\chi}', J')$ are said to be isomorphic if there exist a group isomorphism $\phi : G \to G'$ and a bijective map $\sigma : J \to J'$ such that $\phi(g_i) = g'_{\sigma(i)}$ and $\chi'_{\sigma(i)}\phi = \chi_i$ for any $i \in J$.

Let $(G, g_i, \chi_i; i \in J)$ be an ESC. Let V be a k-vector space with $\dim(V) = |J|$. Let $\{x_i \mid i \in J\}$ be a basis of V over k. Define a left kG-action and a left kG-coaction on V by

$$g \cdot x_i = \chi_i(g) x_i,\ \delta^-(x_i) = g_i \otimes x_i,\ i \in J,\ g \in G.$$

Then it is easy to see that V is a pointed YD kG-module and kx_i is a one dimensional YD kG-submodule of V for any $i \in J$. Denote by $V(G, g_i, \chi_i; i \in J)$ the pointed YD kG-module V. Obviously, $C(x_i \otimes x_j) = \chi_j(g_i) x_j \otimes x_i$ for any $i, j \in J$, is the braiding. (See [ZZC04, Lemma 2.3 and Lemma 2.4]) Every kG-YD module is isomorphic to $V(G, g_i, \chi_i; i \in J)$, which is a braided vector space with diagonal type and braided matrix $(q_{ij}) = (\chi_j(g_i))$ when $J = \{1, 2, \cdots, r\}$.

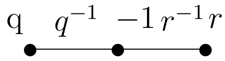
Lemma A.5. *If There is a Hopf algebra isomorphism $\phi : kG \to kG'$ such that $V(G, g_i, \chi_i;\ i \in J) \cong {}^{\phi^{-1}}_{\phi}V'(G'g'_i, \chi'_i;\ i \in J')$ as* YD *kG-modules with $J = J' = \{1, 2, \cdots, r\}$ and $G = G'$, then $(q_{ij})_{r\times r}$ and $(q'_{ij})_{r\times r}$ are permutation similarity, where $q_{ij} = \chi_j(g_i)$ and $q'_{ij} = \chi'_j(g'_i)$ for* $1, 2, \cdots, r$.

Proof. By [ZZC04, Th. 4], $\mathrm{ESC}(G, g_i, \chi_i; i \in J) \cong \mathrm{ESC}(G', g'_i, \chi'_i; i \in J')$ with $J = J' = \{1, 2, \cdots, r\}$. Consequently, there exists a bijective map $\sigma : J \to J'$ such that $\phi(g_i) = g'_{\sigma(i)}$ and $\chi'_{\sigma(i)}\phi(g_j) = \chi_i(g_j)$ for any $i, j \in J$. That is, $q'_{\sigma(j),\sigma(i)} = q_{ji}$ for any $i, j \in J$. ■

Corollary A.6. *Assume $q_{11} = -1$ and $(q_{22} + 1)(q_{22}q_{12}q_{21} - 1) = 0$. If V is connected with rank 2, then the generators of PBW basis $\mathbb{B}_V = \{x_1, x_2, [x_1, x_2]\}$.*

Proof. It follows By Lemma 3.2. ■

Remark A.7. In this paper, the first node, second node and third node of every generalized Dynkin diagram denote q_{33}, q_{11}, q_{22}, respectively. For example,



, $q \in R_m, r \in R_{m'}, q \neq r; m, m' > 1$

denotes $q_{11} = -1, q_{22} = r, q_{33} = q,\ q_{12}q_{21} = r^{-1},\ q_{13}q_{31} = q^{-1}$.

Acknowledgement. We would like to thank Prof. N. Andruskiewitsch for pointing out an error in the previous version, which has led to the current substantially modified version.

References

[AS98] Andruskiewitsch, N., and H. J. Schneider, *Lifting of quantum linear spaces and pointed Hopf algebras of order p^3*, J. Alg. **209** (1998), 645–691.

[AS00] —, *Finite quantum groups and Cartan matrices*, Adv. Math. **154** (2000), 1–45.

[An02] Andruskiewitsch, N., *About finite dimensional Hopf algebras*, Contemp. Math **294** (2002), 1–57.

[He05] Heckenberger, I., "Nichols algebras of diagonal type and arithmetic root systems," Habilitation Thesis, 2005.

[He06b] —, *The Weyl-Brandt groupoid of a Nichols algebra of diagonal type*, Invent. Math. **164** (2006), 175–188.

[He06a] —, *Classification of arithmetic root systems*, Adv. Math. **220** (2009), 59-124.

[He04a] —, *Finite dimensional rank 2 Nichols algebras of diagonal type I: Examples*, Preprint, `arXiv:math/0402350`.

[He04b] —, *Rank 2 Nichols algebras with finite arithmetic root system*, Preprint, arXiv:math/0412458.

[He05b] —, *Weyl equivalence for rank 2 Nichols algebras of diagonal type*, Ann. Univ. Ferrara–Sez. VII–Sc. Mat. **51** (2005), 281–289.

[He05c] —, *Classification of arithmetic root systems of rank 3*, Preprint, arXiv:math/0509145.

[Hu67] Hua, L., "Introduction to Number Theory," Science China Press, China, 1967.

[Kh99] Kharchenko, V. K., *A Quantum analog of the Poincaré-Birkhoff-Witt Theorem*, Algebra and Logic **38** (1999), 259–276.

[KT91] Khoroshkin, S. M., and V. N. Tolstoy, *Universal R-matrix for quantized (super)algebras*, Comm. Math. Phys. **141** (1991), 599–617.

[KS97] Klimyk, A., and K. Schmüdgen, "Quantum groups and their representations," Springer-Verlag, Heidelberg, 1997.

[MS00] Milinski, A., and H. J. Schneider, *Pointed indecomposable Hopf algebras over Coxeter groups*, Contemp. Math. **267** (2000), 215–236.

[Ro98] Rosso, M. *Quantum groups and quantum shuffles*, Invent. Math. **133** (1998), 299–416.

[Wo89] Woronowicz, S. L., *Differential calculus on compact matrix pseudogroups (quantum groups)*, Comm. Math. Phys. **122** (1989), 125–170.

[Ya03] Yamane, H., *Representations of a Z/3Z-quantum group*, Publ. RIMS, Kyoto Univ. **43** (2007), 75–93.

[ZZC04] Zhang, S., Y.-Zh. Zhang, and H.-X. Chen, *Classification of PM quiver Hopf algebras*, J. Algebra Appl. **6** (2007), 919–950.

[ZZ04] Zhang, S. C., Y.-Zh. Zhang, *Braided m-Lie algebras*. Lett. Math. Phys. **70** (2004), 155–167.

Weicai Wu
Department of Mathematics
Hunan University
Changsha 410082, P. R. China
weicaiwu@hnu.edu.cn

Shouchuan Zhang
Department of Mathematics
Hunan University
Changsha 410082, P.R. China
sczhang@hnu.edu.cn

Yao-Zhong Zhang
School of Mathematics and Physics
The University of Queensland
Brisbane 4072, Australia
yzz@maths.uq.edu.au

Received August 1, 2013
and in final form September 11, 2013