



Contents lists available at ScienceDirect

Journal of Algebra

www.elsevier.com/locate/jalgebra



On Hopf algebras of dimension $4p$

Yi-Lin Cheng, Siu-Hung Ng^{*,1}

Department of Mathematics, Iowa State University, Ames, IA 50011, USA

ARTICLE INFO

Article history:

Received 6 May 2010

Available online 15 October 2010

Communicated by Nicolás Andruskiewitsch

Dedicated to Professor Miriam Cohen on the occasion of her retirement

Keywords:

Frobenius algebra

Hopf algebras

Braided Hopf algebras

Yetter–Drinfeld modules

ABSTRACT

In this paper, we prove that a non-semisimple Hopf algebra H of dimension $4p$ with p an odd prime over an algebraically closed field of characteristic zero is pointed provided H contains more than two group-like elements. In particular, we prove that non-semisimple Hopf algebras of dimensions 20, 28 and 44 are pointed or their duals are pointed, and this completes the classification of Hopf algebras in these dimensions.

© 2010 Elsevier Inc. All rights reserved.

Introduction

Let \mathbb{k} be an algebraically closed field of characteristic zero. Kaplansky conjectured in [Kap] that there are only finitely many isomorphism classes of finite-dimensional Hopf algebras over \mathbb{k} for any given dimension. His conjecture was disproved by counterexamples of dimension p^4 with p an odd prime (cf. [AS1,BDG,Gel2]). However, there are only finitely many isomorphism classes of dimension 16 [GV]. The smallest known dimension for which infinitely many non-isomorphic Hopf algebras exist is 32 [EG1].

The dimension 30 has been recently classified in [FukD]. For the dimensions less than 32, only 20, 24, 27 and 28 have not been completely classified, and they are products of at least three primes. All other Hopf algebras of dimension less than 32 are known to have finitely many isomorphism classes (cf. [Bea] for more details). This paper concerns mainly non-semisimple Hopf algebras of dimension $4p$, and we complete the classification for dimensions 20, 28 and 44 in Theorem II.

For a pair of distinct primes p and q , semisimple Hopf algebras of dimension $pq^2 < 100$ are classified (cf. [Nat1,Nat2,Nat4]). By the recent result of [ENO], these semisimple Hopf algebras are of Frobenius type. For $q = 2$, it follows from [Nat2, Theorem 0.1] that there are exactly two isomorphism

* Corresponding author.

E-mail addresses: elynn@iastate.edu (Y.-L. Cheng), rng@iastate.edu (S.-H. Ng).

¹ The second author was partially supported by NSA grant H98230-08-1-0078 and NSF grant DMS10-01566.

classes $\mathcal{A}_0, \mathcal{A}_1$ of non-trivial semisimple Hopf algebras over \mathbb{k} of dimension $4p$. These semisimple Hopf algebras \mathcal{A}_i were constructed in [Gel1] and they are self-dual.

Non-semisimple pointed Hopf algebras of dimension pq^2 were classified in [AN, Lemma A.1]. The classification can be described in terms of the Taft algebras and the Hopf algebra $\mathcal{A}(\tau, \mu)$ which is defined as follows: for a primitive q -th root of unity $\tau \in \mathbb{k}$, and $\mu \in \{0, 1\}$, $\mathcal{A}(\tau, \mu)$ is the \mathbb{k} -algebra generated by the elements a and y with the relations

$$a^{pq} = 1, \quad y^q = \mu(1 - a^q), \quad ay = \tau ya.$$

The comultiplication Δ on $\mathcal{A}(\tau, \mu)$ is defined by

$$\Delta(a) = a \otimes a, \quad \Delta(y) = y \otimes 1 + a \otimes y.$$

There are exactly $4(q-1)$ isomorphism classes of non-semisimple pointed Hopf algebras H of dimension pq^2 , and they are given by $\mathcal{A}(\tau, 0)$, $\mathcal{A}(\tau, 0)^*$, $\mathcal{A}(\tau, 1)$, and $T_q \otimes \mathbb{k}[\mathbb{Z}_p]$ where τ is a primitive q -th root of unity, and T_q is a Taft algebra of dimension q^2 . The set of group-like elements of any of these Hopf algebras forms a cyclic group of order pq .

It was proved in [Rad1] that $\mathcal{A}(\tau, 1)^*$ is not a pointed Hopf algebra. Therefore,

$$\mathcal{A}(\tau, 0), \quad \mathcal{A}(\tau, 0)^*, \quad \mathcal{A}(\tau, 1), \quad \mathcal{A}(\tau, 1)^* \quad \text{and} \quad T_q \otimes \mathbb{k}[\mathbb{Z}_p] \quad (\dagger)$$

account for $5(q-1)$ isomorphism classes of non-semisimple Hopf algebras of dimension pq^2 .

The classification of general non-semisimple Hopf algebras of dimension pq^2 remains open. The problem requires a thorough understanding of Hopf algebras of dimension pq which is also open in general (cf. [EG2, Ng2, Ng4]). However, the classification of Hopf algebras of dimension p , p^2 , $2p$ (cf. [Zhu, Ng1, Ng3]) suggests a possibility for dimension $2q^2$ or $4p$. It has been recently proved in [HN] that a non-semisimple Hopf algebra of dimension $2q^2$ is isomorphic to exactly one in the list (\dagger) with $p = 2$.

By the same rationale, one would expect the $4p$ case can be solved by adjusting the technique used in the $2p^2$ case. In fact, we prove the following theorem which completes the classification of non-semisimple Hopf algebras of dimension $4p$ with more than two group-like elements.

Theorem I. *Let H be a non-semisimple Hopf algebra over \mathbb{k} of dimension $4p$ where p is an odd prime. Then H is pointed if, and only if, $|G(H)| > 2$.*

It remains unclear whether there exists a non-semisimple Hopf algebra H of dimension $4p$ with fewer than three group-like elements such that neither H nor H^* is pointed.

A $4p$ -dimensional Hopf algebra which is neither pointed nor dual pointed could be constructed from a p -dimensional braided Hopf algebra R in the Yetter–Drinfeld category ${}^{H_4}_{H_4}\mathcal{YD}$ by Radford biproduct or bosonization $R \times H_4$, where H_4 denotes the Sweedler algebra. We prove in Proposition 3.2 that H is such a biproduct if, and only if, both H and H^* admit a non-trivial skew primitive element.

For any odd prime $p \leq 11$, we show in Lemma 5.1 by counting arguments that every non-semisimple Hopf algebra of dimension $4p$ admits a non-trivial skew primitive element. Together with the investigation of p -dimensional braided Hopf algebras in ${}^{H_4}_{H_4}\mathcal{YD}$ in Sections 3 and 4, we prove our main theorem in this paper:

Theorem II. *If H is a non-semisimple Hopf algebra of dimension $4p$, where $p \leq 11$ is an odd prime, then H or H^* is pointed. In particular, for each of these dimensions, there are exactly 5 isomorphism classes which are given by the list (\dagger) .*

The non-semisimple case of dimension 12 was classified by Natale in [Nat3], and the semisimple case was completed by Fukuda in [Fuk].

Theorem II and the main result of [HN] justify the following conjecture.

Conjecture. Let p, q be distinct primes. For any non-semisimple Hopf algebra H over \mathbb{k} of dimension pq^2 , H or H^* is pointed.

This paper is organized as follows: Section 1 collects some notation and preliminary results for the later sections. In Section 2, we specialize to study non-semisimple Hopf algebras of dimension $4p$, and prove Theorem I. In Section 3, we turn our focus to p -dimensional braided Hopf algebras R in the Yetter–Drinfeld category ${}^{H_4}\mathcal{YD}$. We show that these algebras are always semisimple, and we provide a necessary condition in Theorem 3.8 for a non-commutative R . This condition implies R is commutative for $\dim R = 3, 7, 11$. For $\dim R = 5$, the commutativity of R is shown in Section 4. Finally, we prove the technical Lemma 5.1, and complete the proof of Theorem II in Section 5.

1. Notation and preliminaries

Let H be a finite-dimensional Hopf algebra over \mathbb{k} with comultiplication Δ , counit ϵ and antipode S . A *left integral* of H is an element $\lambda \in H$ such that $h\lambda = \epsilon(h)\lambda$, and a *right integral* of H can be defined similarly. The subspace of left (or right) integrals of H is always 1-dimensional (cf. [Mon]).

The dual H^* of H admits a natural Hopf algebra structure and the comultiplication Δ induces two natural actions of H^* , \rightharpoonup and \leftharpoonup , on H given by

$$f \rightharpoonup h = h_1 f(h_2), \quad \text{and} \quad h \leftharpoonup f = f(h_1)h_2 \quad \text{for } h \in H, f \in H^*,$$

where $\Delta(h) = h_1 \otimes h_2$ is the Sweedler notation for comultiplication with the summation suppressed. One can easily see that an element $\lambda \in H^*$ is a right integral if, and only if,

$$h \leftharpoonup \lambda = \lambda(h)1_H \quad \text{for all } h \in H. \quad (1.1)$$

A non-zero element $g \in H$ is said to be *group-like* if $\Delta(g) = g \otimes g$. The set of all group-like elements of H , denoted by $G(H)$, forms a group under the multiplication of H , and is linearly independent over \mathbb{k} . The *distinguished group-like* elements $a \in G(H)$ and $\alpha \in G(H^*)$ are respectively defined by the conditions:

$$\lambda h = \alpha(h)\lambda, \quad \lambda \rightharpoonup h = \lambda(h)a \quad \text{for all } h \in H,$$

where $\lambda \in H^*$ is a non-zero right integral, and $\lambda \in H$ is a non-zero left integral. The fourth power of the antipode can be expressed in terms of the distinguished group-like elements $a \in H$ and $\alpha \in H^*$ by the celebrated Radford formula [Rad2]:

$$S^4(h) = a(\alpha \rightharpoonup h \leftharpoonup \alpha^{-1})a^{-1} \quad \text{for } h \in H. \quad (1.2)$$

The antipode conceives important information of the underlying Hopf algebra. The following theorem by Larson and Radford (cf. [LR, LR, Rad4]) manifests how the antipode relates to the semisimplicity of a Hopf algebra.

Theorem 1.1. Let H be a finite-dimensional Hopf algebra over the field \mathbb{k} with antipode S . Then the following statements are equivalent:

- (i) H is not semisimple;
- (ii) H^* is not semisimple;
- (iii) $S^2 \neq \text{id}_H$;
- (iv) $\text{Tr}(S^2) = 0$;
- (v) $\text{Tr}(S^2 \circ r(b)) = 0$ for all $b \in H$,

where $r(b)$ denotes the linear operator on H defined by $r(b)(x) = xb$.

This well-known result will be used repeatedly without further explanation in the sequel.

Recall that for an H -module V , the left dual V^\vee is the left H -module with the underlying space $V^* = \text{Hom}_{\mathbb{k}}(V, \mathbb{k})$ and the H -action given by

$$(hf)(x) = f(S(h)x) \quad \text{for } x \in V, f \in V^*, h \in H.$$

The right dual ${}^\vee V$ of V is defined similarly but the H -action is given by

$$(hf)(x) = f(S^{-1}(h)x).$$

The collection $H\text{-}\mathbf{mod}_{\text{fin}}$ of all the H -modules of finite dimension over \mathbb{k} forms a rigid monoidal category.

For any $U, V, W \in H\text{-}\mathbf{mod}_{\text{fin}}$, we have the following natural isomorphisms:

$$\text{Hom}_H(V^\vee \otimes U, W) \cong \text{Hom}_H(U, V \otimes W) \cong \text{Hom}_H(U \otimes {}^\vee W, V). \quad (1.3)$$

For an algebra automorphism σ on H , denote by ${}_\sigma V$ the H -module with the underlying space V and the σ -twisted action given by $h \cdot v = \sigma(h)v$ for $h \in H, v \in V$. The natural isomorphism $j: {}_{S^2}V \rightarrow V^{\vee\vee}$ of vector spaces is an H -module map. In particular, we have

$${}_{S^2}V \stackrel{j}{\cong} V^{\vee\vee} \quad \text{for } V \in H\text{-}\mathbf{mod}_{\text{fin}}. \quad (1.4)$$

Similarly, one also has the H -module isomorphism ${}_{S^{-2}}V \stackrel{j}{\cong} {}^\vee\vee V$.

Let $P(V)$ and $I(V)$ respectively denote the projective cover and the injective hull of $V \in H\text{-}\mathbf{mod}_{\text{fin}}$, and $\text{Irr}(H)$ a complete set of non-isomorphic simple H -modules. For $\beta \in G(H^*)$, we define \mathbb{k}_β as the 1-dimensional H -module which affords the irreducible character β . We will simply write \mathbb{k} for the trivial 1-dimensional H -module \mathbb{k}_ϵ . If $\alpha \in H^*$ is the distinguished group-like element and $V \in \text{Irr}(H)$, then it follows from [Ng4, Lemma 1.1] that

$$\mathbb{k}_{\alpha^{-1}} \otimes {}^\vee\vee V \cong \text{Soc}(P(V)) \quad \text{and} \quad V \cong \text{Soc}(P(\mathbb{k}_\alpha \otimes V^{\vee\vee})).$$

Since H is a Frobenius algebra, we have

$$I(\mathbb{k}_{\alpha^{-1}} \otimes {}^\vee\vee V) \cong P(V). \quad (1.5)$$

For $M, V \in H\text{-}\mathbf{mod}_{\text{fin}}$, we define $[M : V] := \dim \text{Hom}_H(P(V), M)$. If V is simple, $[M : V]$ is equal to the multiplicity of V appearing as a composition factor of M . By [Ben, Lemma 1.7.7], we have

$$[M : V] = \dim \text{Hom}_H(M, I(V)). \quad (1.6)$$

Lemma 1.2. *Let V, W be simple H -modules. Then*

$$[P(V) : W] = [P(W) : \mathbb{k}_{\alpha^{-1}} \otimes {}^\vee\vee V].$$

In addition, if $\dim V \neq \dim W$ and $[P(V) : W] > 0$, then

$$\begin{aligned} \dim P(W) &\geq 2 \dim W + [P(V) : W] \dim V \quad \text{and} \\ \dim P(V) &\geq 2 \dim V + [P(V) : W] \dim W. \end{aligned}$$

Proof. By (1.5) and (1.6), we have

$$\begin{aligned}[P(V) : W] &= \dim \operatorname{Hom}_H(P(W), P(V)) \\ &= \dim \operatorname{Hom}_H(P(W), I(\mathbb{k}_{\alpha^{-1}} \otimes {}^{\vee\vee} V)) = [P(W) : \mathbb{k}_{\alpha^{-1}} \otimes {}^{\vee\vee} V].\end{aligned}$$

If $[P(V) : W] > 0$ and $\dim V \neq \dim W$, then $[P(W) : \mathbb{k}_{\alpha^{-1}} \otimes {}^{\vee\vee} V] > 0$. Thus, besides the socle and the head, $P(W)$ has the composition factor $\mathbb{k}_{\alpha^{-1}} \otimes {}^{\vee\vee} V$ with multiplicity $[P(V) : W]$. Therefore,

$$\dim P(W) \geq 2 \dim W + [P(V) : W] \dim V.$$

The second inequality can be obtained by the same argument. \square

Lemma 1.3. *Let H be a finite-dimensional non-semisimple Hopf algebra with Jacobson radical J . For any simple H -modules V, W , we have*

$$[JP(V)/J^2P(V) : W] = \dim \operatorname{Ext}(V, W) = [\operatorname{Soc}(I(W)/W) : V].$$

In addition, if H^ has no non-trivial skew primitive element, then each simple H -submodule of $JP(\mathbb{k})/J^2P(\mathbb{k})$ or $\operatorname{Soc}(I(\mathbb{k})/\mathbb{k})$ is not 1-dimensional.*

Proof. Let us abbreviate $P(V)$ as P , and consider the natural exact sequence

$$0 \rightarrow JP \rightarrow P \rightarrow V \rightarrow 0.$$

For any simple H -module W , we have the associated long exact sequence

$$0 \rightarrow \operatorname{Hom}_H(V, W) \rightarrow \operatorname{Hom}_H(P, W) \rightarrow \operatorname{Hom}_H(JP, W) \rightarrow \operatorname{Ext}(V, W) \rightarrow \operatorname{Ext}(P, W).$$

Since $\operatorname{Ext}(P, W) = 0$ and $\operatorname{Hom}_H(V, W) \rightarrow \operatorname{Hom}_H(P, W)$ is an isomorphism, we find

$$\operatorname{Hom}_H(JP/J^2P, W) \cong \operatorname{Hom}_H(JP, W) \xrightarrow{\cong} \operatorname{Ext}(V, W).$$

Therefore, $[JP/J^2P : W] = \dim \operatorname{Ext}(V, W)$. The second equality can be obtained similarly by considering the exact sequence

$$0 \rightarrow W \rightarrow I(W) \rightarrow I(W)/W \rightarrow 0.$$

If H^* does not have any non-trivial skew primitive element, then, by [EG2, Lemma 2.3], $\operatorname{Ext}(V, W) = 0$ for any 1-dimensional H -modules V, W . Therefore,

$$[JP(\mathbb{k})/J^2P(\mathbb{k}) : W] = [\operatorname{Soc}(I(\mathbb{k})/\mathbb{k}) : W] = 0$$

for all 1-dimensional H -modules W . \square

The dimensions of projective modules over a finite-dimensional Hopf algebra are of particular importance to the remainder of this paper. The following fact on linear algebra is quite useful to study these dimensions.

Lemma 1.4. (See [Ng3, Lemma 1.4].) *Let V be a finite-dimensional vector space over the field \mathbb{k} , p a prime, and T a linear automorphism on V such that $\operatorname{Tr}(T) = 0$. If $T^{p^n} = \operatorname{id}_V$ for some positive integer n , then p divides the dimension of V .*

We close this section with the following corollary which is an application of the preceding lemma.

Corollary 1.5. *Let H be a non-semisimple Hopf algebra over \mathbb{k} with antipode S . If $\text{ord}(S^2) = p^n$ for some prime p , then every indecomposable projective H -module P such that $P \cong P^{\vee\vee}$ as H -modules has dimension divisible by p .*

Proof. Let P be an indecomposable projective H -module such that $P \cong P^{\vee\vee}$. In view of (1.4), $P \cong {}_{S^2}P$. By [HN, Lemma A.2], there exists an H -module isomorphism $\varphi : P \rightarrow {}_{S^2}P$ such that $\varphi^{p^n} = \text{id}$. It follows from [Ng4, Lemma 1.3] that $\text{Tr}(\varphi) = 0$. Therefore, Lemma 1.4 implies that p divides $\dim P$. \square

Sweedler's 4-dimensional Hopf algebra H_4 is of particular interest in this paper. The Hopf algebra H_4 is identical to the Taft algebra T_2 , which is generated as a \mathbb{k} -algebra by x, g subject to the relations

$$g^2 = 1, \quad x^2 = 0 \quad \text{and} \quad gx = -xg. \quad (1.7)$$

The comultiplication Δ_{H_4} , the counit ϵ_{H_4} , and the antipode S_{H_4} are given by

$$\begin{aligned} \Delta_{H_4}(x) &= x \otimes g + 1 \otimes x, & \epsilon_{H_4}(x) &= 0, & S_{H_4}(x) &= -xg, \\ \Delta_{H_4}(g) &= g \otimes g, & \epsilon_{H_4}(g) &= 1, & S_{H_4}(g) &= g. \end{aligned}$$

This notation will be used frequently in Sections 3 and 4.

Remark 1.6. The Hopf algebra H_4 is self-dual, and it is the unique non-semisimple Hopf algebra over \mathbb{k} of dimension 4 up to isomorphism.

2. Non-semisimple Hopf algebras with dimension $4p$

In this section, we will focus on non-semisimple Hopf algebras H of dimension $4p$, where p is an odd prime, and we prove Theorem I. In particular, this completes the classification of non-semisimple Hopf algebras H of dimension $4p$ with $|G(H)|$ or $|G(H^*)| > 2$ by applying the result of Andruskiewitsch and Natale [AN, Lemma A.1]. It will be shown in Section 5 that this condition on the group-like elements holds for $p \leq 11$.

Throughout the remainder of this paper, we assume p is an odd prime, and H is a non-semisimple Hopf algebra of dimension $4p$. We begin with

Lemma 2.1.

- (i) *If H contains a Hopf subalgebra K of dimension $2p$, then H is pointed and K is isomorphic to a cyclic group algebra.*
- (ii) *If H contains a Hopf ideal I of dimension $2p$, then H^* is pointed and H/I is isomorphic to a cyclic group algebra.*

Proof. (i) By [Ng3], K is semisimple and so $S_K^2 = \text{id}_K$. Therefore, there are at least $2p$ eigenvalues of S^2 , including multiplicities, which are 1. Since H is not semisimple, $\text{Tr}(S^2) = 0$ and this forces the remaining $2p$ eigenvalues of S^2 to be all -1 . Thus, $S^4 = \text{id}_H$ and the order of S^2 is 2. By [AS2, Proposition 5.1], K is equal to the coradical of H . It follows from [AN, Lemmas A.1 and A.2] that H is pointed, $K = \mathbb{k}[G(H)]$ and $G(H)$ is a cyclic group of order $2p$.

(ii) If I is a Hopf ideal of dimension $2p$, then H/I is a Hopf algebra of dimension $2p$ and H^* admits a Hopf subalgebra isomorphic to $(H/I)^*$. By (i), H^* is pointed and H/I is isomorphic to a cyclic group algebra. \square

We precede our discussion with the following remark.

Remark 2.2. Let K be a commutative semisimple Hopf subalgebra of H . By Nichols–Zoeller Theorem, H is a right free K -module of rank $\dim H / \dim K$. If E is the set of orthogonal primitive idempotents of K , then $H = \bigoplus_{e \in E} He$ is a decomposition of left H -module and $\dim He = \dim H / \dim K$ for all $e \in E$.

Lemma 2.3. *If $p \mid |G(H)|$, then H is pointed.*

Proof. Let $g \in G(H)$ such that $\text{ord}(g) = p$. First we show that the composition factors of $P(\mathbb{k})$ are 1-dimensional.

Let $\{e_1, \dots, e_p\}$ be the complete set of orthogonal primitive idempotents of $\mathbb{k}[g]$. By the preceding remark, $H = \bigoplus_i He_i$ is a decomposition of left H -modules, and $\dim He_i = 4$. By the Krull–Schmidt Theorem, $\dim P(V) \leq 4$ for all $V \in \text{Irr}(H)$. Since H is not semisimple, \mathbb{k} is not projective. Therefore, $2 \leq \dim P(\mathbb{k}) \leq 4$.

If $\dim P(\mathbb{k}) = 2, 3$, then all its composition factors are 1-dimensional. Suppose $\dim P(\mathbb{k}) = 4$ and it has a composition factor V of dimension greater than 1. Then $\dim V = 2$, $[P(\mathbb{k}) : V] = 1$ and V is not projective. By Lemma 1.2,

$$\dim P(V) \geq 2 \dim V + 1 > 4, \quad \text{a contradiction!}$$

Since $P(\mathbb{k})$ is not simple and all its composition factors are 1-dimensional, it follows from Lemma 1.3 that H^* admits a non-trivial skew primitive element. Now, we apply [AN, Proposition 1.8] to conclude that H^* contains a non-semisimple pointed Hopf subalgebra K of dimension $M^2 N$ with $M > 1$. By Nichols–Zoeller Theorem, $M^2 N \mid 4p$ and this implies $M = 2$ and $N = 1$ or p .

If $N = p$, then $K = H^*$. By the classification [AN, Lemma A.1] of pointed Hopf algebras of dimension $4p$, either K^* is pointed or $|G(K^*)| = 2$. Since $p \mid |G(H)|$, K^* is pointed and so is H .

If $N = 1$, then K is isomorphic to the Sweedler algebra H_4 . By dualizing the inclusion map $K \rightarrow H^*$, we find a Hopf algebra surjection $\pi : H \rightarrow H_4$. Moreover, the coinvariant $R = H^{\text{co}\pi} = \{r \in H \mid r_1 \otimes \pi(r_2) = r \otimes 1\}$ is a (left) normal left coideal subalgebra of dimension p (cf. [Mon, 3.4.2 (2)]). Since $\pi(g)$ is a group-like element of H_4 , $\pi(g) = 1$ and hence $R = \mathbb{k}[g]$. In particular, R is a normal Hopf subalgebra of H by [Tak, 4.5 (a)]. Therefore, we have the exact sequence of Hopf algebras:

$$1 \rightarrow \mathbb{k}[g] \rightarrow H \rightarrow H_4 \rightarrow 1.$$

One can dualize the sequence and apply [HN, Proposition 1.6] to conclude that H contains a semisimple Hopf subalgebra of dimension $2p$. Then, by Lemma 2.1, H is pointed. \square

Corollary 2.4. *Let S be the antipode of H . Then $S^{16} = \text{id}_H$. Moreover, for $V \in \text{Irr}(H)$ such that $V \cong V^{\vee\vee}$, $\dim P(V)$ is even. In particular, $\dim P(\mathbb{k})$ is an even integer.*

Proof. Let $\alpha \in H^*$ and $a \in H$ be the distinguished group-like elements. If p divides $\text{ord}(\alpha) \text{ord}(a)$, then $p \mid |G(H)|$ or $p \mid |G(H^*)|$. It follows from Lemma 2.3 that H or H^* is pointed. By [AN, Lemma A.1], $S^4 = \text{id}_H$. On the other hand, if $p \nmid \text{ord}(\alpha) \text{ord}(a)$, then $\text{ord}(\alpha)$ and $\text{ord}(a)$ are factors of 4. Thus, the statement follows from Radford's formula (1.2) of S^4 .

If $V \in \text{Irr}(H)$ is isomorphic to $V^{\vee\vee}$, then $P(V) \cong P(V)^{\vee\vee}$, and the second statement follows immediately from Corollary 1.5. \square

Lemma 2.5. *The order of $G(H)$ is not divisible by 4 and $S^8 = \text{id}$.*

Proof. Suppose $4 \mid |G(H)|$. Then $|G(H)| = 4$ otherwise $|G(H)| = 4p$ which implies H is semisimple. The Hopf subalgebra $K = \mathbb{k}[G(H)]$ is commutative and semisimple. Let $\{e_1, e_2, e_3, e_4\}$ be the set of orthogonal primitive idempotents of K . In view of Remark 2.2,

$$\dim He_i = p.$$

Note that S^2 stabilizes He_i and $\text{Tr}(S^2|_{He_i}) = 0$. It follows from Lemma 1.4 and Corollary 2.4 that $\dim He_i$ is even, a contradiction. Therefore, $4 \nmid |G(H)|$.

If H or H^* is pointed, then the classification of [AN, Lemma A.1] implies $S^4 = \text{id}$. If neither H nor H^* is pointed, then Lemma 2.3 forces $p \nmid |G(H)||G(H^*)|$. Thus, $\text{lcm}(|G(H)|, |G(H^*)|) \leq 2$ and the second part of the statement follows immediately from Radford's formula of S^4 . \square

Now we can prove Theorem I.

Proof of Theorem I. If $|G(H)| > 2$, then it follows from Lemma 2.5 that $p \mid |G(H)|$. The result then follows immediately from Lemma 2.3. Conversely, if H is a pointed Hopf algebra of $4p$, then $G(H)$ is a cyclic group of order $2p$ by [AN, Lemma A.1]. This completes the proof of Theorem I. \square

We close this section with an observation on 2-dimensional simple H -modules.

Lemma 2.6. *Every 2-dimensional simple H -module is not self-dual.*

Proof. Suppose V is a simple H -module of dimension 2 such that $V \cong V^\vee$. Then H^* is not pointed otherwise all simple H -modules are of dimension 1. Moreover, we have $\text{ann } V = \text{ann } V^\vee = S(\text{ann } V)$. Therefore, S induces an isomorphism \bar{S} on $H/\text{ann } V$. Since V is simple, $H/\text{ann } V$ is a simple algebra of dimension 4. Let $\pi : H \rightarrow H/\text{ann } V$ be the natural surjection. Then $\pi^* : (H/\text{ann } V)^* \rightarrow H^*$ is an injective coalgebra map which satisfies the commutative diagram:

$$\begin{array}{ccc} (H/\text{ann } V)^* & \xrightarrow{\pi^*} & H^* \\ \bar{S}^* \downarrow & & \downarrow S^* \\ (H/\text{ann } V)^* & \xrightarrow{\pi^*} & H^*. \end{array}$$

In particular, $C = \pi^*((H/\text{ann } V)^*)$ is a simple subcoalgebra of H^* stabilized by S^* .

Let K be the subalgebra of H^* generated by C . Then K is a Hopf subalgebra of H^* and hence $\dim K = 4, p, 2p$ or $4p$. Since K contains the simple subcoalgebra C , $\dim K \neq 4, p$. If $\dim K = 2p$, then K is a cyclic group algebra by Lemma 2.1 but this is absurd. So we have $\dim K = 4p$, and hence $H^* = K$. By [Nat3], there exists an exact sequence of Hopf algebras

$$1 \rightarrow \mathbb{k}^G \rightarrow H^* \rightarrow B \rightarrow 1,$$

where B^* is a non-semisimple pointed Hopf algebra and G is a finite group. Note that $\dim B$ can only be 4 or $4p$ since Hopf algebras of dimension 2, $2p$, p are semisimple. If $\dim B = 4$, then G is a cyclic group of order p and it follows from Remark 1.6 that $B \cong H_4$. Since $\mathbb{k}^G \cong \mathbb{k}[G]$ as Hopf algebras, $G(H^*)$ contains a subgroup of order p . It follows from Lemma 2.3 that H^* is pointed but this is absurd. This forces $\dim B = 4p$ and hence $H^* = B$. In particular, H is pointed. By [AN, Lemma A.1], $H \cong \mathcal{A}(\tau, 1)$. It follows from [Rad1] that every 2-dimensional simple H -module is not self-dual, a contradiction. \square

3. p -Dimensional Hopf algebras in a Yetter–Drinfeld category

Let p be an odd prime. The Radford biproduct or bosonization $R \times H_4$ of a p -dimensional braided Hopf algebra R in the Yetter–Drinfeld category ${}^{H_4}\mathcal{YD}$ is a non-semisimple Hopf algebra of dimension $4p$. In addition, if 1_R is the unique group-like element of R , then $G(R \times H_4)$ is of order 2, and hence, by Theorem I, $R \times H_4$ is not pointed. However, it remains unclear whether such a braided Hopf algebra exists.

In this section, we mainly study p -dimensional braided Hopf algebras in ${}^{H_4}\mathcal{YD}$, and we show in Theorem 3.1 that they must be semisimple as a \mathbb{k} -algebra. Moreover, the bosonization $R \times H_4$ is

pointed if, and only if, R is commutative. If R is not commutative, we show in Theorem 3.8 that $|G(R^*)| \equiv 1 \pmod{4}$. This theorem implies that all the 7- or 11-dimensional braided Hopf algebras in ${}^{H_4}\mathcal{YD}$ are trivial Hopf algebras.

Recall that a Yetter–Drinfeld module over a Hopf algebra B is a \mathbb{k} -vector space V equipped with a left B -module action \triangleright and a left B -comodule action $\rho_V : V \rightarrow B \otimes V$ which satisfy the compatibility condition:

$$\rho_V(b \triangleright v) = b_1 v_{-1} S_B(b_3) \otimes b_2 \triangleright v_0$$

for $b \in B$ and $v \in V$, where $\rho_V(v) = v_{-1} \otimes v_0$ is the Sweedler notation with the summation suppressed again. The Yetter–Drinfeld category ${}^B_B\mathcal{YD}$, which consists of the Yetter–Drinfeld modules over B as objects, is a braided monoidal category. One can define a Hopf algebra in such category (cf. [Mon] or [And]), and it is often called a *braided Hopf algebra* in ${}^B_B\mathcal{YD}$. The Radford biproduct or bosonization $R \times B$ constructed from a braided Hopf algebra R in ${}^B_B\mathcal{YD}$ is an ordinary Hopf algebra [Rad3]. If both R and B are finite-dimensional, then R^* is naturally a braided Hopf algebra in ${}^{B^*}_{B^*}\mathcal{YD}$ and we have an isomorphism

$$(R \times B)^* \cong R^* \times B^* \quad (3.1)$$

as Hopf algebras.

The underlying space of $R \times B$ is $R \otimes B$. For simplicity, we use the identifications $r = r \otimes 1_B$ and $b = 1_R \otimes b$ in $R \times B$ for $r \in R$ and $b \in B$. Under this convention, the multiplication, the comultiplication, the counit and the antipode of $R \times B$ are given by

$$\begin{aligned} (ra)(sb) &:= r(a_1 \triangleright s)a_2b, & \Delta(rb) &:= r^{(1)}(r^{(2)})_{-1}b_1 \otimes (r^{(2)})_0b_2, \\ \epsilon(rb) &:= \epsilon_R(r)\epsilon_B(b), & \text{and } S(rb) &= (S_B(b_2) \triangleright S_R(r))S_B(b_1) \end{aligned}$$

for $r, s \in R$, $a, b \in B$ where $\Delta_R(r) = r^{(1)} \otimes r^{(2)}$ denotes the Sweedler notation for the comultiplication Δ_R of R .

We mainly focus on p -dimensional braided Hopf algebras in ${}^{H_4}_{H_4}\mathcal{YD}$ in this section, and they are always semisimple and cosemisimple.

Theorem 3.1. *For any p -dimensional braided Hopf algebra R in ${}^{H_4}_{H_4}\mathcal{YD}$, R and R^* are semisimple algebras.*

Proof. Let S be the antipode of $R \times H_4$. Then R is stable under S^2 . By [AS2, Theorem 7.3], it suffices to show that $\text{Tr}(S^2|_R) \neq 0$. Suppose $\text{Tr}(S^2|_R) = 0$. By Corollary 2.4, $\text{ord}(S^2|_R)$ is a positive power of 2. In view of Lemma 1.4, $\dim R$ is even which is a contradiction. \square

For a Hopf algebra H of dimension $4p$ such that H and H^* are not pointed, one would like to know when it can be isomorphic to a bosonization of the form $R \times H_4$. The following proposition provides a sufficient condition.

Proposition 3.2. *Let H be a $4p$ -dimensional Hopf algebra such that neither H nor H^* is pointed. Then $H \cong R \times H_4$ for some braided Hopf algebra R in ${}^{H_4}_{H_4}\mathcal{YD}$ if, and only if, both H and H^* admit a non-trivial skew primitive element.*

Proof. Since $R \times H_4$ and $(R \times H_4)^*$ contain a Hopf subalgebra isomorphic to H_4 , both of them contain a non-trivial skew primitive element. Conversely, we assume both H and H^* admit a non-trivial skew primitive element. It follows from Theorem 1 that $|G(H)| = |G(H^*)| = 2$. By [AN, Proposition 1.8], there exists a non-semisimple Hopf subalgebra K of H such that $\dim K = mn^2$ with $n > 1$ and $|G(K)| = mn$.

Since $|G(H)| = 2$, $n = 2$ and $m = 1$. Therefore, K is isomorphic to the Sweedler algebra H_4 (cf. Remark 1.6). By the same reason, H^* also contains a Hopf subalgebra isomorphic to H_4 . Since $H_4 \cong H_4^*$, there exists a Hopf algebra surjection $\pi : H \rightarrow H_4$. It is well known that $R := H^{\text{co}\pi}$ and $K' := K^{\text{co}\pi}$ are left coideal subalgebras of H . Moreover, $K' \subset R$ and R is a Hopf module in ${}^H_K \mathcal{M}$. Note that $\pi(K)$ is a Hopf subalgebra of H_4 , and $\dim K' = 1, 2$ or 4 . More precisely, $K' \cong \mathbb{k}[X]/[X^2]$ or H_4 as \mathbb{k} -algebras, and they are Frobenius algebras. By [Mas], R is a free module over K' . This forces $\dim K' = 1$ as $\dim R = p$. Thus, $\pi(K) = H_4$ or $\pi|_K : K \rightarrow H_4$ is a Hopf algebra isomorphism. It follows from [Rad3] that R is a braided Hopf algebra in ${}^{H_4}_{H_4} \mathcal{YD}$, and $H \cong R \times H_4$ as Hopf algebras. \square

To proceed with our discussion, we further establish some basic facts on semisimple braided Hopf algebras in a Yetter–Drinfeld category. The readers are referred to [FMS] for more details.

Let us assume that both B and R are finite-dimensional. By [FMS, Remark 5.9], R is a Frobenius algebra with the Frobenius map λ_R given by a right integral of R^* , i.e. $\lambda_R(r^{(1)})r^{(2)} = \lambda_R(r)1_R$ for all $r \in R$. Moreover, λ_R determines an element $\chi \in G(B^*)$ by the equation

$$\lambda_R(b \triangleright r) = \chi(b)\lambda_R(r) \quad \text{for all } b \in B, r \in R. \quad (3.2)$$

The algebra R also admits a right integral $\Lambda_R \in R$ such that $\lambda_R(\Lambda_R) = 1$. This implies that

$$b \triangleright \Lambda_R = \chi(b)\Lambda_R \quad \text{for all } b \in B. \quad (3.3)$$

If R is semisimple, it has been proved in [FMS, p. 4885] that $\epsilon_R(\Lambda_R) \neq 0$ and $\chi = \epsilon_B$. This implies

$$\lambda_R(b \triangleright r) = \epsilon_B(b)\lambda_R(r) \quad \text{and} \quad b \triangleright \Lambda_R = \epsilon_B(b)\Lambda_R \quad (3.4)$$

for $b \in B$. We also need the following lemma for semisimple braided Hopf algebras.

Lemma 3.3. *Let B be a finite-dimensional Hopf algebra over \mathbb{k} , and R a braided Hopf algebra in the Yetter–Drinfeld category ${}^B_B \mathcal{YD}$ such that R is a semisimple \mathbb{k} -algebra. Suppose Λ_R is a right integral of R and λ_R is a right integral of R^* . Then*

$$\rho_R(\Lambda_R) = 1_B \otimes \Lambda_R, \quad S_R(\Lambda_R) = \Lambda_R \quad \text{and} \quad r_{-1}\lambda_R(r_0) = 1_B\lambda_R(r) \quad (3.5)$$

for $r \in R$.

Proof. From [Doi, 1.6], there exists a group-like element $z \in B$ such that

$$\rho_R(\Lambda_R) = S_B(z) \otimes \Lambda_R \quad \text{and} \quad \lambda_R(r)z = S_B^{-1}(r_{-1})\lambda_R(r_0)$$

for $r \in R$. Since $\epsilon_R(\Lambda_R) \neq 0$ and ϵ_R is a B -comodule map, i.e. $\epsilon_R(\Lambda_R)1_B = S_B(z)\epsilon_R(\Lambda_R)$, we find $S_B(z) = 1_B$. Hence, the first and the last equalities follow immediately.

Note that S_R is a bijection which satisfies $S_R(rs) = S_R(r_{-1} \triangleright s)S_R(r_0)$ for all $r, s \in R$. In particular, we have

$$\epsilon_R(s)S_R(\Lambda_R) = S_R(\Lambda_R s) = S_R(s)S_R(\Lambda_R).$$

Since $\epsilon_R \circ S_R = \epsilon_R$, $S_R(\Lambda_R)$ is also a left integral. The semisimplicity of R implies $S_R(\Lambda_R) = \gamma \Lambda_R$ for some $\gamma \in \mathbb{k}$. Since $\epsilon_R(\Lambda_R) \neq 0$, we find $\gamma = 1$. \square

Now, we return to our specific case where B is the Sweedler algebra H_4 . The elements $x, g \in H_4$ defined in the end of Section 1 will be used in the reminder of Section 3 and Section 4.

Let us first consider H_4 -module algebras which are semisimple as \mathbb{k} -algebras.

Lemma 3.4. Let A be a finite-dimensional left (resp. right) H_4 -module algebra. If A is a semisimple algebra and e is a central idempotent of A such that $I = Ae$ is closed under the action of g , then I is a H_4 -submodule of A , and

$$g \triangleright e = e \quad \text{and} \quad x \triangleright e = 0.$$

In particular, I is also a H_4 -module algebra.

Proof. If e is not a primitive idempotent, write $e = e_1 + \cdots + e_k$ as a sum of orthogonal primitive central idempotents of A . Then $e_i e = e_i = e e_i \in I$ for $1 \leq i \leq k$. Note that g acts on A as an algebra automorphism. Since I is an ideal closed under g -action, $g \triangleright e_i \in I$ is a primitive central idempotent of A , and the action of g permutes the idempotents e_1, \dots, e_k . Thus, we have $g \triangleright e = e$. Note that

$$x \triangleright e = x \triangleright e^2 = (x \triangleright e)(g \triangleright e) + e(x \triangleright e) = 2e(x \triangleright e) \in I. \quad (3.6)$$

The equality also implies that $x \triangleright e = 2x \triangleright e$. Since \mathbb{k} is of characteristic zero, $x \triangleright e = 0$. Now, for any $r \in R$, we find $x \triangleright (re) = (x \triangleright r)e \in I$. Therefore, I is closed under the H_4 -action. \square

Lemma 3.5. Let R be a finite-dimensional braided Hopf algebra in ${}^{H_4}\mathcal{YD}$. If R is a semisimple algebra and I is a 1-dimensional ideal of R , then $x \triangleright I = 0$.

Proof. Since R is semisimple, there exists a primitive central idempotent e_1 of R such that $I = Re_1$. If $g \triangleright e_1 = e_1$, then $x \triangleright e_1 = 0$ by Lemma 3.4. Now, we assume $g \triangleright e_1 = e_2 \neq e_1$. Then e_2 is also a primitive central idempotent of R and $e_1 e_2 = 0$. The ideal $\hat{I} = Re_1 + Re_2 = R(e_1 + e_2)$ is closed under the action of g . By Lemma 3.4, $x \triangleright e_i = \alpha_{i1}e_1 + \alpha_{i2}e_2$ for some $\alpha_{ij} \in \mathbb{k}$ and $i, j \in \{1, 2\}$, and $x \triangleright (e_1 + e_2) = 0$. These equations imply $\alpha_{11} = -\alpha_{21}$ and $\alpha_{12} = -\alpha_{22}$. By the equation $gx \triangleright e_1 = -x \triangleright e_2$, we find $\alpha_{12} = -\alpha_{21}$ and $\alpha_{11} = -\alpha_{22}$. Thus, we have $x \triangleright e_1 = \alpha(e_1 + e_2)$ and $x \triangleright e_2 = -\alpha(e_1 + e_2)$, where $\alpha = \alpha_{11}$. Applying (3.4) with $b = g$ and $r = e_1$, we obtain $\lambda_R(e_1) = \lambda_R(e_2)$. Since $\ker \lambda_R$ cannot have any non-zero ideal of R , $\lambda_R(e_1) \neq 0$. Applying (3.4) again with $b = x$ and $r = e_1$, we find $2\alpha\lambda(e_1) = 0$ which implies $\alpha = 0$. Therefore, $x \triangleright \hat{I} = 0$. \square

Proposition 3.6. Let R be a p -dimensional Hopf algebra in ${}^{H_4}\mathcal{YD}$. The following statements are equivalent:

- (i) R is commutative;
- (ii) R is cocommutative;
- (iii) $R \times H_4$ is pointed;
- (iv) $(R \times H_4)^*$ is pointed;
- (v) R admits a g -invariant 1-dimensional ideal I which is not spanned by any non-zero integral of R ;
- (vi) The action of x on R is trivial.

If one of the equivalent statements holds, then the H_4 -action and the H_4 -coaction of R are trivial. In particular, R is an ordinary Hopf algebra.

Proof. Let H be the biproduct $R \times H_4$. By (3.1), $H^* \cong R^* \times H_4^*$. Note that R and R^* are semisimple algebras by Theorem 3.1.

(i) \Rightarrow (iv) and (vi). Since R is a commutative semisimple algebra, R is a direct sum of 1-dimensional ideals. By Lemma 3.5, $x \triangleright R = 0$. Then Hx is a Hopf ideal of H and $\dim Hx = 2p$. Therefore, H^* is pointed by Lemma 2.1.

(ii) \Rightarrow (iii). Since R is cocommutative, R^* is a commutative braided Hopf algebra in ${}^{H_4^*}\mathcal{YD}$. Since $H_4^* \cong H_4$, the isomorphism in (3.1) and the preceding paragraph imply $R \times H_4$ is pointed.

(iii) \Rightarrow (i) and (ii). If H is pointed, then $G(H)$ is a cyclic group of order $2p$. Since $|G(H)| > 2$, it follows from [Rad3, 2.11] that there exists a non-trivial group-like element $r \in G(R)$ such that

$\rho_R(r) = 1_{H_4} \otimes r$. Then r is a group-like element of H , $\text{ord}(r) = p$ and $R = \mathbb{k}[r]$. In particular, R is an ordinary Hopf algebra and the H_4 -coaction on R is trivial.

(iv) \Rightarrow (i), (ii), (v) and (vi). By (3.1), $R^* \times H_4^*$ is pointed. Using the same argument as in the preceding paragraph, R^* is isomorphic to the ordinary Hopf algebra $\mathbb{k}[\mathbb{Z}_p]$, and the H_4^* -coaction on R^* is trivial. Therefore, the H_4 -action on R is trivial. In particular, g acts as identity on R , and x acts trivially.

(v) \Rightarrow (iv). Let χ be the character of R associated with the 1-dimensional ideal I . Then $\chi \in G(R^*)$ and $\chi \neq \epsilon_R$. Since I is g -invariant, $x \triangleright I = 0$ by Lemma 3.5. Thus, $\rho_{R^*}(\chi) = \epsilon_{H_4} \otimes \chi$. In view of [Rad3, 2.11], $R^* \times H_4^*$ has at least 3 group-like elements. By Theorem 1, $(R \times H_4)^*$ is pointed.

(vi) \Rightarrow (i). Since x acts on R trivially, $I = Hx$ is a $2p$ -dimensional Hopf ideal in H . By Lemma 2.1, H/I is isomorphic to a cyclic group algebra of dimension $2p$. Since R is isomorphic to the subalgebra $R + I$ of H/I , R is commutative. \square

We continue to study the possible non-commutative p -dimensional braided Hopf algebras R in ${}^{H_4}_{H_4}\mathcal{YD}$. Since R is a semisimple \mathbb{k} -algebra, one can always decompose R into a direct product of simple ideals. Since the group-like element $g \in G(H_4)$ acts as a \mathbb{k} -algebra automorphism on R , the action of g permutes the simple ideals of R . In particular, $A_I = I + (g \triangleright I)$ is g -stable for any simple ideal I of R . In view of Lemma 3.4, A_I is stable under the action H_4 and is a H_4 -module algebra. The ideal A_I is called a H_4 -simple ideal of R in the sequel.

A semisimple braided Hopf algebra R in ${}^{H_4}_{H_4}\mathcal{YD}$ can be decomposed into a direct product of H_4 -simple ideals. Namely,

$$R = A_1 \oplus \cdots \oplus A_l \quad (3.7)$$

where $A_i = I + (g \triangleright I)$ for some simple ideal I of R . Therefore,

$$R \times H_4 = A_1 H_4 \oplus \cdots \oplus A_l H_4 \quad (3.8)$$

is an ideal decomposition of the biproduct $R \times H_4$.

Let A be a H_4 -simple ideal of the semisimple braided Hopf algebra R in ${}^{H_4}_{H_4}\mathcal{YD}$. Then A does not admit any proper H_4 -invariant ideal of R . Let $e_0 = (1_{H_4} + g)/2$ and $e_1 = (1_{H_4} - g)/2$. Then e_0, e_1 are idempotents of H_4 and $\{e_0, e_1, xe_0, xe_1\}$ forms a \mathbb{k} -basis for H_4 . Moreover, it forms an R -basis for $R \times H_4$.

Suppose

$$E = r_1 e_0 + r_2 e_1 + r_3 x e_0 + r_4 x e_1 \quad (3.9)$$

is a central idempotent of AH_4 for some $r_1, r_2, r_3, r_4 \in A$. Since $gE = Eg$, we find

$$g \triangleright r_1 = r_1, \quad g \triangleright r_2 = r_2, \quad g \triangleright r_3 = -r_3, \quad g \triangleright r_4 = -r_4. \quad (3.10)$$

Similarly, by the equality $xE = Ex$, we find

$$x \triangleright r_1 = x \triangleright r_2 = 0 \quad \text{and} \quad x \triangleright r_3 = x \triangleright r_4 = r_1 - r_2. \quad (3.11)$$

Note that

$$Ee_0 = r_1 e_0 + r_3 x e_0, \quad Ee_1 = r_2 e_1 + r_4 x e_1$$

are idempotents. This implies

$$r_1^2 = r_1, \quad r_2^2 = r_2, \quad r_3 = r_1 r_3 + r_3 r_2, \quad r_4 = r_2 r_4 + r_4 r_1. \quad (3.12)$$

For $r \in A$, the commutativity $rE = Er$ implies

$$[r_1, r] = -r_3(x \triangleright r), \quad [r_2, r] = r_4(x \triangleright r), \quad [r_3, r] = [r_4, r] = 0 \quad (3.13)$$

whenever $g \triangleright r = r$, and

$$rr_1 = r_2r + r_4(x \triangleright r), \quad rr_2 = r_1r - r_3(x \triangleright r), \quad rr_3 = r_4r, \quad rr_4 = r_3r \quad (3.14)$$

whenever $g \triangleright r = -r$. In particular, we have

$$[r_i, r_j] = 0 \quad \text{for } i \in \{1, 2\}, j \in \{3, 4\}, \quad \text{and} \quad [r_3 + r_4, r] = 0 \quad \text{for all } r \in A. \quad (3.15)$$

In view of (3.12),

$$r_3 = r_3(r_1 + r_2) = (r_1 + r_2)r_3 \quad \text{and} \quad r_4 = r_4(r_1 + r_2) = (r_1 + r_2)r_4. \quad (3.16)$$

Lemma 3.7. *Let I be a simple ideal of R of dimension n^2 .*

- (i) *If A_I is a simple ideal of R or the action of x on A_I is trivial, then $A_I H_4$ is an indecomposable ideal of $R \times H_4$.*
- (ii) *If $A_I = I \oplus (g \triangleright I)$, then every simple quotient algebra of $A_I H_4$ has dimension $4n^2$. Moreover, $A_I H_4$ is either a direct sum of two simple ideals of dimension $4n^2$ or a primary algebra, i.e. $\frac{A_I H_4}{\text{Rad}(A_I H_4)}$ is a simple algebra of dimension $4n^2$.*
- (iii) *If $A_I = I \oplus (g \triangleright I)$ and the action of x on A_I is trivial, then $A_I H_4$ is a primary algebra and $\frac{A_I H_4}{\text{Rad}(A_I H_4)}$ is a simple algebra of dimension $4n^2$.*

In particular, $A_I H_4$ is either an indecomposable ideal or a direct sum of two simple ideals of dimension $4n^2$.

Proof. (i) Suppose E , given by (3.9), is a non-zero central idempotent of $A_I H_4$. If A_I is simple, then (3.15) implies that $r_3 + r_4 = \gamma 1_{A_I}$ for some scalar $\gamma \in \mathbb{k}$. By Lemma 3.4, $x \triangleright (r_3 + r_4) = 0$. Hence, by (3.11), $r_1 = r_2$. If the action of x on A_I is trivial, then we also have $r_1 = r_2$ by (3.11). It follows from (3.12) that r_1 is a non-zero idempotent, otherwise $E = 0$. Thus, $r_i = 2r_1 r_i$ for $i = 3, 4$. This implies that $r_3 = r_4 = 0$ and $E = r_1$. In particular, r_1 is a non-zero central idempotent of A_I . Since A_I is H_4 -simple and r_1 is g -invariant by (3.10), r_1 must be the identity of A_I . Thus, there is no non-trivial central idempotent in $A_I \times H_4$.

(ii) For the first statement, it is equivalent to show that every simple $A_I H_4$ -module V has dimension $2n$. By restriction, V is an A_I -module and so $V \cong m_1 V_1 + m_2 V_2$ as A_I -modules where V_1, V_2 are the simple modules of I and $g \triangleright I$ respectively. We claim that $m_1 = m_2 = 1$. Let $z_1, \dots, z_{m_1} \in V$ such that $I z_i$ is a simple I -module and $I V = I z_1 \oplus \dots \oplus I z_{m_1}$. Then $g I V = g I z_1 \oplus \dots \oplus g I z_{m_1}$ is a decomposition of vector subspaces and $g I z_i = (g \triangleright I) g z_i$ is $g \triangleright I$ -module. Therefore, $m_1 \leq m_2$. Similarly, one can show that $m_2 \leq m_1$, and hence $m_1 = m_2 = m$. Therefore, $\dim V = 2mn$, and so $\frac{A_I H_4}{\text{Rad}(A_I H_4)}$ contains a simple ideal of dimension $4m^2 n^2$. This forces $m = 1$ and $\dim V = 2n$.

If $A_I H_4$ is not a primary algebra, then there is more than one simple module over $A_I H_4$. Thus, we have the inequality

$$8n^2 = \dim A_I H_4 \geq \dim \left(\frac{A_I H_4}{\text{Rad}(A_I H_4)} \right) \geq 8n^2.$$

Therefore, $\text{Rad}(A_I H_4) = 0$ and $A_I H_4$ is a direct sum of two simple ideals of dimension $4n^2$.

(iii) If the action of x on A_I is trivial, then $A_I H_4 x$ is a nilpotent ideal of $A_I H_4$. In particular, $A_I H_4$ is not semisimple. In view of (ii), $A_I H_4$ is a primary algebra. \square

Theorem 3.8. *Let p be an odd prime and R a non-commutative p -dimensional braided Hopf algebra in ${}^{H_4}\mathcal{YD}$. Then $|G(R^*)|$ and $|G(R)|$ are integers congruent to 1 modulo 4.*

Proof. By Proposition 3.6, R^* is also non-commutative. It suffices to show that $|G(R^*)| \equiv 1 \pmod{4}$. Since g acts on R as an algebra automorphism, g permutes the simple ideals of R . In particular, g permutes the set \mathfrak{D} of 1-dimensional ideals of R and g fixes the ideal spanned by a non-zero integral Λ_R of R . If g fixes another 1-dimensional ideal which is not spanned by Λ_R , then it follows from Proposition 3.6 that R is commutative. Therefore, g fixes exactly one element of \mathfrak{D} and hence $|\mathfrak{D}|$ is an odd number.

Now, we assume that $|\mathfrak{D}| \equiv 3 \pmod{4}$. Let I be a 1-dimensional ideal of R such that $\Lambda_R \notin I$. Then $A = I \oplus (g \triangleright I)$ is a 2-dimensional H_4 -simple ideal. In view of Lemma 3.5, the action of x on A is trivial. It follows from Lemma 3.7(iii) that AH_4 is an indecomposable ideal of $R \times H_4$ and $\dim AH_4 = 8$. By Lemma 3.7, for any simple ideal J of R with $\dim J > 1$, each indecomposable ideal summand of $(J + (g \triangleright J))H_4$ has dimension at least 16. Therefore, $\widehat{\mathfrak{D}} = \{A_I H_4 \mid I \in \mathfrak{D}, I \neq \mathbb{k}\Lambda_R\}$ are all the 8-dimensional indecomposable ideal summands of $R \times H_4$. Moreover, each of these indecomposable summands is primary and its simple quotient is 4-dimensional. The antipode S of $R \times H_4$ permutes the ideals in $\widehat{\mathfrak{D}}$. Since $|\widehat{\mathfrak{D}}|$ is an odd number and $\text{ord}(S)$ is a power of 2 by Lemma 2.5, one of these 8-dimensional ideals is stable under S . Therefore, the associated 2-dimensional simple $(R \times H_4)$ -module is self-dual. However, this contradicts Lemma 2.6. Therefore $|\mathfrak{D}| \equiv 1 \pmod{4}$.

Since $|G(R^*)| = |\mathfrak{D}|$, the result follows. \square

Corollary 3.9. *Braided Hopf algebras of dimension 3, 7 or 11 in ${}^{H_4}\mathcal{YD}$ are trivial Yetter–Drinfeld modules, and they are group algebras.*

Proof. Note that these braided Hopf algebras R are semisimple by Theorem 3.1. Thus, R is obviously commutative when $\dim R = 3$. Suppose there exists a braided Hopf algebra R in ${}^{H_4}\mathcal{YD}$ of dimension 7 or 11 which is not a commutative algebra. The number of 1-dimensional characters of R is either congruent to 3 modulo 4 or equal to 2, but this contradicts Theorem 3.8. Therefore, R must be commutative, and the result follows immediately from Proposition 3.6. \square

4. Braided Hopf algebras of dimension 5 in ${}^{H_4}\mathcal{YD}$

Theorem 3.8 cannot be applied to decide the commutativity of a braided Hopf algebra of dimension congruent to 1 modulo 4. In this section, we use the result of Chen and Zhang [CZ] on the classification of 4-dimensional matrix algebra in $D(H_4)\text{-mod}$ to deal with the 5-dimensional case, and we prove

Lemma 4.1. *Braided Hopf algebras of dimension 5 in ${}^{H_4}\mathcal{YD}$ are commutative.*

The proof of Lemma 4.1 will be elaborated in the remainder of this section. We will continue to use the convention for the Sweedler algebra H_4 introduced in the end of Section 1.

Remark 4.2. The classification of 4-dimensional matrix algebras in ${}^{H_4}\mathcal{YD}$ follows immediately from [CZ, Theorem 4.10]. In general, for any finite-dimensional Hopf algebra B , the categories $\mathcal{C} = D(B)\text{-mod}$ and $\mathcal{D} = {}^B_B\mathcal{YD}$ are isomorphic as monoidal categories under the strict monoidal functor $\mathcal{F} : \mathcal{C} \rightarrow \mathcal{D}$ defined as follows: for $M \in \mathcal{C}$, the B -module structure of $\mathcal{F}(M)$ is the B -restriction of M , and the left B -comodule structure $\rho : M \rightarrow B \otimes M$ of $\mathcal{F}(M)$ given by

$$\rho(v) = \sum_i S_B(b_i) \otimes b^i v \quad (4.1)$$

for $v \in M$, where $\{b_i\}_i$ is a basis for B and $\{b^i\}_i$ is its dual basis. For any morphism $f : M \rightarrow N$ in \mathcal{C} , the assignment $\mathcal{F}(f) := f$ is a morphism from $\mathcal{F}(M)$ to $\mathcal{F}(N)$ in \mathcal{D} . Since $M = \mathcal{F}(M)$ as vector spaces, $\dim M = \dim \mathcal{F}(M)$ for all $M \in \mathcal{C}$.

This isomorphism of monoidal categories implies that A is an algebra in \mathcal{C} if, and only, if $\mathcal{F}(A)$ is an algebra in \mathcal{D} . In this case, $A = \mathcal{F}(A)$ as \mathbb{k} -algebras. Moreover, A and B are isomorphic algebras in \mathcal{C} if, and only if, $\mathcal{F}(A)$ and $\mathcal{F}(B)$ are isomorphic algebras in \mathcal{D} .

Assume R is a 5-dimensional non-commutative braided Hopf algebra in ${}^{H_4}\mathcal{YD}$ with left H_4 -action \triangleright and left H_4 -coaction ρ_R . By Theorem 3.1, R is a semisimple \mathbb{k} -algebra, and so R has a unique ideal decomposition $R = A \oplus I$ where A is a 4-dimensional ideal isomorphic to a matrix algebra and I is a 1-dimensional ideal generated by the normalized integral $e = \Lambda_R / \epsilon_R(\Lambda_R)$. Hence, $\epsilon_R(A) = 0$ and e is a central idempotent of R . It follows from (3.4) and Lemma 3.3 that $t \triangleright e = \epsilon_{H_4}(t)e$ for $t \in H_4$, and $\rho_R(e) = 1_{H_4} \otimes e$. Since the action of g is an algebra automorphism of R , $g \triangleright A = A$ and hence g fixes the central idempotent ι of A . By Lemma 3.4, A is closed under the H_4 -action of R and $x \triangleright \iota = 0$. Thus, A is also a H_4 -module algebra.

The left H_4 -comodule algebra structure of R induces a right H_4^* -module algebra on R . Since $H_4^* \cong H_4$ as Hopf algebras, by the preceding arguments, A is also a right H_4^* -submodule of R and hence a H_4 -subcomodule of R . Thus, A is a 4-dimensional matrix algebra in the category ${}^{H_4}\mathcal{YD}$. Since R is not commutative and x acts trivially on I , the x -action on A cannot be trivial by Proposition 3.6.

In view of Remark 4.2, we apply the classification of 4-dimensional matrix algebra in ${}^{H_4}\mathcal{YD}$ follows from [CZ, Theorem 4.10]. Since the x -action on A is trivial and \mathbb{k} is algebraically closed, the Yetter–Drinfeld H_4 -algebra A can only be isomorphic to the corresponding classes (c), (h), (i), (k), (m) or (n) of [CZ, Theorem 4.10]. There exist $u, v \in A$ such that $\{\iota, u, v, uv\}$ forms a basis for A and satisfy the relations

$$u^2 = \alpha\iota, \quad v^2 = \beta\iota, \quad uv + vu = \gamma\iota \quad \text{for some } \alpha, \beta, \gamma \in \mathbb{k}, \quad (4.2)$$

and the H_4 -action \triangleright is given by

$$x \triangleright u = 0, \quad x \triangleright v = \iota, \quad g \triangleright u = -u, \quad g \triangleright v = -v. \quad (4.3)$$

The H_4 -comodule structures on A can only be one of the following three cases:

- (A) $\rho_R(u) = 1_{H_4} \otimes u + 2x \otimes uv, \quad \rho_R(v) = g \otimes v - 2\beta xg \otimes \iota \quad \text{and} \quad \gamma = 0;$
 - (B) $\rho_R(u) = g \otimes u, \quad \rho_R(v) = \eta xg \otimes \iota + g \otimes v \quad \text{where } \eta \in \mathbb{k};$
 - (C) $\rho_R(u) = xg \otimes \iota + g \otimes u, \quad \rho_R(v) = g \otimes v.$
- (4.4)

By (4.3), A can be decomposed into a direct sum $A = P_0 \oplus P_1$ of H_4 -submodules, where P_0 is spanned by uv, u and P_1 by v, ι . The H_4 -modules P_0 and P_1 are two principal modules of H_4 , i.e. $H_4 \cong P_0 \oplus P_1$. Therefore, $R = P_0 \oplus P_1 \oplus I$ is a direct sum of indecomposable H_4 -submodules of R . Note that

$$\text{Hom}_{H_4}(P_i, P_j) \cong \text{Hom}_{H_4}(P_0, I) \cong \text{Hom}_{H_4}(I, P_1) \cong \text{Hom}_{H_4}(I, I) \cong \mathbb{k}$$

as \mathbb{k} -linear spaces for all $i, j = 0, 1$. Since the antipode of R is a left H_4 -module map, we have

$$\begin{aligned} S_R(\iota) &= \zeta_1 \iota \\ S_R(u) &= \zeta_2 u \\ S_R(v) &= \zeta_3 u + \zeta_1 v \\ S_R(uv) &= \zeta_4 \iota + \zeta_2 uv + \zeta_5 e \\ S_R(e) &= \zeta_6 \iota + \zeta_7 e \end{aligned}$$

for some $\zeta_1, \dots, \zeta_7 \in \mathbb{k}$. Since $S_R(1_R) = 1_R$ and $\epsilon_R \circ S_R = \epsilon_R$, it follows immediately from Lemma 3.3 that

$$\zeta_5 = \zeta_6 = 0, \quad \text{and} \quad \zeta_1 = \zeta_7 = 1.$$

Let λ_R be a right integral of R^* such that $\lambda_R(e) = 1$. Since R^* is also a semisimple \mathbb{k} -algebra, λ_R is a two-sided integral. In view of (3.4) and (4.3), $\lambda_R(\iota) = \lambda_R(u) = \lambda_R(v) = 0$. Since $\ker \lambda_R$ cannot contain any non-zero ideal of R , $\lambda_R(uv) \neq 0$. It follows from (3.5) of Lemma 3.3 that case (A) of (4.4) is impossible.

One can renormalize u or v to further assume $\lambda_R(uv) = 1$. Then it follows from (4.2) that $\lambda_R(vu) = -1$. With respect to the Frobenius map λ_R , $\{\iota, u, v, uv, e\}$ and $\{uv, -v, u, \iota, e\}$ form a pair of the dual bases for R , i.e.

$$r = \iota \lambda_R(uv r) - u \lambda_R(v r) + v \lambda_R(u r) + uv \lambda_R(\iota r) + e \lambda_R(e r) \quad \text{for } r \in R.$$

By [FMS],

$$\begin{aligned} & \iota \otimes uv - u \otimes v + v \otimes u + uv \otimes \iota + e \otimes e \\ &= S_R^{-1}((e^{(2)})_0) \otimes \epsilon_{H_4}((e^{(2)})_{-1}) S_{H_4}^{-1}((e^{(2)})_{-2}) \triangleright e^{(1)} \\ &= S_R^{-1}((e^{(2)})_0) \otimes S_{H_4}^{-1}((e^{(2)})_{-1}) \triangleright e^{(1)}. \end{aligned} \quad (4.5)$$

Hence

$$\begin{aligned} & S_R(\iota) \otimes uv - S_R(u) \otimes v + S_R(v) \otimes u + S_R(uv) \otimes \iota + S_R(e) \otimes e \\ &= (e^{(2)})_0 \otimes S_{H_4}^{-1}((e^{(2)})_{-1}) \triangleright e^{(1)}. \end{aligned} \quad (4.6)$$

Applying $\lambda_R \otimes \text{id}$ to the equation, we then have

$$\begin{aligned} \zeta_2 \iota + e &= \lambda_R((e^{(2)})_0) S_{H_4}^{-1}((e^{(2)})_{-1}) \triangleright e^{(1)} \\ &= \lambda_R(e^{(2)}) S_{H_4}^{-1}(1_{H_4}) \triangleright e^{(1)} = \lambda_R(e^{(2)}) e^{(1)} = 1_R \lambda_R(e) = 1_R. \end{aligned} \quad (4.7)$$

Therefore, $\zeta_2 = 1$. Applying the equality

$$S_R^{-1}((e^{(2)})_0) S_{H_4}^{-1}((e^{(2)})_{-1}) \triangleright e^{(1)} = \epsilon_R(e) 1_R$$

(cf. [Doi, 1.6]) to (4.5), we find $\gamma \iota + e = 1_R$ and hence $\gamma = 1$. However, this implies S_R cannot be an anti-algebra homomorphism in the braided sense, i.e.

$$S_R(rs) = (r_{-1} \triangleright S_R(s)) S_R(r_0). \quad (4.8)$$

Suppose S_R satisfies the condition (4.8). In both cases (B) and (C), we find

$$\begin{aligned} (u_{-1} \triangleright S_R(u)) S_R(u_0) &= -\alpha \iota, \quad S_R(u^2) = \alpha \iota, \\ (v_{-1} \triangleright S_R(u)) S_R(v_0) &= -\zeta_3 \alpha \iota - uv, \quad S_R(vu) = (1 - \zeta_4) \iota - uv. \end{aligned}$$

These equalities imply $\alpha = 0$ and $\zeta_4 = 1$. Thus, $S_R(uv) = uv + \iota$. Since

$$(u_{-1} \triangleright S_R(v))S_R(u_0) = \begin{cases} uv - \iota & \text{for case (B) and} \\ uv - 2\iota & \text{for case (C),} \end{cases}$$

both cases (B) and (C) do not satisfy (4.8). Therefore, there does not exist any non-commutative semisimple braided Hopf algebra of dimension 5 in ${}^{H_4}\mathcal{YD}$. This completes the proof of Lemma 4.1.

5. Non-semisimple Hopf algebras of dimension 20, 28 and 44

Let H be a non-semisimple Hopf algebra over \mathbb{k} of dimension $4p$ where p is an odd prime. By Proposition 3.2, if H and H^* are not pointed and they both admit a non-trivial skew primitive element, then H is a biproduct of the form $R \times H_4$. In this section, we prove the following technical lemma:

Lemma 5.1. *If H is a non-semisimple Hopf algebra over \mathbb{k} of dimension $4p$ where $p = 3, 5, 7, 11$, then both H and H^* have a non-trivial skew primitive element.*

As a consequence, we can complete the proof of Theorem II.

Proof of Theorem II. Suppose H and H^* are not pointed. By Lemma 5.1 and Proposition 3.2, $H \cong R \times H_4$ for some braided Hopf algebra R in ${}^{H_4}\mathcal{YD}$ and $\dim R = 3, 5, 7$ or 11 . Applying Corollary 3.9 and Lemma 4.1, R is a commutative algebra. By Proposition 3.6, $R \times H_4$ is a pointed Hopf algebra, a contradiction. \square

The remainder of the section is devoted to prove Lemma 5.1, and we need to establish a few lemmas for the proof. Throughout this section, we assume H is a non-semisimple Hopf algebra over \mathbb{k} of dimension $4p$, and let

$$\text{Irr}_1(H) = \{U \in \text{Irr}(H) \mid \dim U \text{ is odd}\}.$$

Lemma 5.2. *Let V be a simple H -module with $\dim V > 1$. Suppose V is a composition factor of $P(\mathbb{k})$. Then*

- (i) $\dim P(V) \geq 2 \dim V + 1$, $\dim P(\mathbb{k}) \geq \dim V + 2$, and $\dim P(\mathbb{k})$ is even.
- (ii) If $V \cong V^{\vee\vee}$, then $\dim P(V) \geq 2 \dim V + 2$ and

$$\sum_{W \in \text{Irr}_1(H)} [P(V) : W]$$

is a positive even integer.

Proof. (i) follows immediately from Lemma 1.2 and Corollary 2.4.

(ii) If $V \cong V^{\vee\vee}$, $\dim P(V)$ is even, and hence the inequality follows. Moreover, the number of odd dimensional simple constituent of $P(V)$ including multiplicities must be even, or $\sum_{W \in \text{Irr}_1(H)} [P(V) : W]$ is even. By Lemma 1.2, $[P(\mathbb{k}) : V] = [P(V) : \mathbb{k}_{\alpha^{-1}}] \geq 1$ where α is the distinguished group-like element of H^* . Therefore, $\sum_{W \in \text{Irr}_1(H)} [P(V) : W] > 0$. \square

The cyclic group \mathfrak{D} generated by the antipode S acts on $\text{Irr}(H)$ by duality, i.e. $S \cdot U \cong U^\vee$ for $U \in \text{Irr}(H)$. The orbit \mathfrak{D}_U of $U \in \text{Irr}(H)$ is given by

$$\mathfrak{D}_U = \{U, U^\vee, U^{\vee\vee}, U^{\vee\vee\vee}, \dots\}$$

up to isomorphism. It follows from Lemma 2.5 that $|\mathfrak{D}_U| = 1, 2, 4$ or 8 for all simple H -modules U . By (1.5),

$$P(U)^{\vee\vee\vee} \otimes_{\mathbb{k}_\alpha} \cong P(U^\vee)$$

for $U \in \text{Irr}(H)$. Thus,

$$\dim P(W) = \dim P(U) \quad \text{for all } W \in \mathfrak{D}_U. \quad (5.1)$$

Therefore, one has the equation

$$\dim H = \sum_{U \in \text{Irr}(H)} \dim U \cdot \dim P(U) = \sum_{U \in \mathcal{R}} |\mathfrak{D}_U| \cdot \dim U \cdot \dim P(U) \quad (5.2)$$

where \mathcal{R} is a complete set of representatives of \mathfrak{D} -orbits.

Lemma 5.3. *For any simple H -module U such that $\dim U > 1$ and $|\mathfrak{D}_U| = 1$,*

$$\dim U \cdot \dim P(U) \geq 16.$$

Proof. If $|\mathfrak{D}_U| = 1$, then $U \cong U^\vee$. In view of Lemma 2.6, $\dim U \geq 3$. Since $U \cong U^{\vee\vee}$, $\dim P(U)$ is even by Corollary 2.4. Thus, $\dim P(U) > \dim U$ for $\dim U$ odd. In particular, U is not projective and hence $\dim P(U) \geq 2 \dim U$. Therefore,

$$\dim U \cdot \dim P(U) \geq \dim U \cdot 2 \dim U \geq 18$$

for any odd dimensional U . If $\dim U$ is even, then $\dim U \geq 4$ and so

$$\dim U \cdot \dim P(U) \geq (\dim U)^2 \geq 16. \quad \square$$

Following [EG2], we always have

$$\dim U \cdot \dim P(U) \geq \dim P(\mathbb{k}) \quad (5.3)$$

for all $U \in \text{Irr}(H)$. This inequality together with (5.2) imply

$$|\text{Irr}(H)| \leq \dim H / \dim P(\mathbb{k}). \quad (5.4)$$

Lemma 5.4. *Suppose H^* does not have any non-trivial skew primitive element. Then there exist $U, W \in \text{Irr}(H)$ such that $\dim U, \dim W \geq 2$ and $\mathfrak{D}_U \neq \mathfrak{D}_W$.*

Proof. Since H^* does not have any non-trivial skew primitive element, H^* is not pointed. In view of Lemma 1.3, $P(\mathbb{k})$ admits a simple subquotient V of dimension greater than one. By Theorem I, $|G(H^*)| \leq 2$.

Assume the lemma is false. Then \mathfrak{D}_V is a complete set of non-isomorphic simple H -modules with dimension greater than 1. For simplicity, we let

$$D_0 = \dim P(\mathbb{k}), \quad D = \dim P(V), \quad d = \dim V \quad \text{and} \quad m = |\mathfrak{D}_V|.$$

By Lemma 5.2, $D_0 \geq 4$ and $D \geq 5$. Eq. (5.2) becomes

$$4p = |G(H^*)| D_0 + mdD. \quad (5.5)$$

The H -module $V^\vee \otimes P(V)$ is projective, and $\dim \operatorname{Hom}_H(V^\vee \otimes P(V), \mathbb{k}_\beta)$ is equal to the multiplicity of $P(\mathbb{k}_\beta)$ in an indecomposable decomposition of $V^\vee \otimes P(V)$ for $\beta \in G(H)$. By (1.3),

$$\dim \operatorname{Hom}_H(V^\vee \otimes P(V), \mathbb{k}_\beta) = [V \otimes \mathbb{k}_\beta : V] = \begin{cases} 1 & \text{if } V \cong V \otimes \mathbb{k}_\beta, \\ 0 & \text{otherwise.} \end{cases}$$

Therefore, by (5.1) and a decomposition of $V^\vee \otimes P(V)$ into indecomposable H -modules, we find

$$dD = \dim(V^\vee \otimes P(V)) = n_0 D_0 + n_1 D \quad (5.6)$$

where n_0, n_1 are integers satisfying $1 \leq n_0 \leq |G(H^*)|$ and $0 \leq n_1 < d$. Eqs. (5.5) and (5.6) imply

$$(d - n_1)D = n_0 D_0 \quad \text{and} \quad 4p = (md + k(d - n_1))D, \quad (5.7)$$

where $k = \frac{|G(H^*)|}{n_0} \in \mathbb{Z}_+$. Since $m, k \geq 1$ and $d \geq 2$, $md + k(d - n_1) \geq 3$. Eq. (5.7) implies $D = p$ and $md + k(d - n_1) = 4$. In particular, D is odd and so $V \not\cong V^{\vee\vee}$. Thus $m \geq 4$, and hence $md + k(d - n_1) > 8$, a contradiction. \square

Now, we can prove our key lemma in this section.

Proof of Lemma 5.1. By duality, it suffices to show that H^* has a non-trivial skew primitive element. Suppose H^* has only trivial skew primitive elements. Then H^* is not pointed, and hence, by Theorem 1, $|G(H^*)| \leq 2$. In view of [EG2, Lemma 2.3], $P(\mathbb{k})$ has a composition factor V with $\dim V \geq 2$. By Lemma 5.4, there exists a simple H -module W such that $\dim W \geq 2$ and $\mathfrak{D}_W \neq \mathfrak{D}_V$.

(i) $|\mathfrak{D}_V| \leq 2$ and $\dim P(V) \geq 2 \dim V + 2$. Note that

$$\dim W \dim P(W) \geq \dim P(\mathbb{k}) \geq 4.$$

By (5.2) and Lemma 5.2,

$$44 \geq \dim P(\mathbb{k}) + |\mathfrak{D}_V| \dim V \dim P(V) + \dim W \dim P(W) \geq 4 + |\mathfrak{D}_V| \cdot 2 \cdot 5 + 4.$$

This implies $|\mathfrak{D}_V| < 4$ and hence $|\mathfrak{D}_V| \leq 2$. In particular, $V \cong V^{\vee\vee}$. Thus, the desired inequality follows from Lemma 5.2(ii).

(ii) $\dim V = 2$ and $\dim P(V) \geq 6$. In view of (i), the inequality follows from the first equality.

Assume $\dim V \geq 3$. By (i) and Lemma 5.2, $\dim P(V) \geq 8$ and $\dim P(\mathbb{k}) \geq 6$. It follows from (5.3) that

$$\dim W \dim P(W) \geq 6. \quad (5.8)$$

We claim that $\dim W \dim P(W) \geq 8$. This inequality obviously holds for $\dim W > 2$. For $\dim W = 2$, the inequality (5.8) implies $\dim P(W) > \dim W$ and hence $\dim P(W) \geq 2 \dim W$. Therefore, $\dim W \dim P(W) \geq 8$.

Now, we apply (5.2) to obtain

$$44 \geq \dim P(\mathbb{k}) + \dim V \dim P(V) + |\mathfrak{D}_W| \dim W \dim P(W) \geq 6 + 3 \cdot 8 + |\mathfrak{D}_W| 8.$$

The inequality forces $|\mathfrak{D}_W| = 1$, and hence, by Lemma 5.3, $\dim W \dim P(W) \geq 16$. However, this implies

$$44 \geq \dim H \geq \dim P(\mathbb{k}) + \dim V \dim P(V) + \dim W \dim P(W) \geq 6 + 24 + 16$$

which is absurd.

(iii) $|\mathfrak{D}_V| = 2$ by Lemma 2.6, (i) and (ii).

(iv) All composition factors of $P(V)$ are of dimension 1 or 2. Suppose there exists a composition factor U of $P(V)$ such that $\dim U \geq 3$. Then, by Lemma 1.2 and Corollary 2.4,

$$\dim P(V), \dim P(U) \geq 8.$$

However,

$$\begin{aligned} \dim H &\geq \dim P(\mathbb{k}) + |\mathfrak{D}_V| \dim V \dim P(V) + \dim U \dim P(U) \\ &\geq 4 + 2 \cdot 2 \cdot 8 + 3 \cdot 8 > 44. \end{aligned}$$

Therefore, all the composition factors of $P(V)$ are of dimension 1 or 2.

(v) Let $M = \bigoplus_{\beta \in G(H^*)} P(\mathbb{k}_\beta)$. By Lemma 1.2,

$$[M : V] = \sum_{\beta \in G(H^*)} [P(\mathbb{k}_\beta) : V] = \sum_{\beta \in G(H^*)} [P(V) : \mathbb{k}_\beta].$$

By (iv) and Lemma 5.2(ii), $[M : V] \geq 2$.

Since M is self-dual, $[M : V^\vee] = [M : V]$. Thus, we have

$$\dim M \geq 2|G(H^*)| + 2[M : V] \dim V \geq 2|G(H^*)| + 8.$$

If $|G(H^*)| = 2$, then $\dim P(\mathbb{k}) = \dim M/2 \geq 6$ and so $\dim W \dim P(W) \geq 6$. Since $\dim P(V) \geq 6$, we find

$$\dim H \geq \dim M + 2 \dim V \dim P(V) + |\mathfrak{D}_W| 6 \geq 12 + 2 \cdot 2 \cdot 6 + |\mathfrak{D}_W| 6.$$

This again forces $|\mathfrak{D}_W| = 1$. It follows from Lemma 5.3 that $\dim W \dim P(W) \geq 16$. However,

$$\dim M + 2 \dim V \dim P(V) + \dim W \dim P(W) > 44.$$

Therefore, $|G(H^*)| = 1$. In this case, $\dim P(\mathbb{k}) = \dim M \geq 10$ and so $\dim W \dim P(W) \geq 10$. By (5.4), $|\text{Irr}(H)| \leq 4$. Therefore, $|\mathfrak{D}_W| = 1$ and so $\dim W \dim P(W) \geq 16$. This implies

$$\dim H \geq \dim P(\mathbb{k}) + 2 \dim V \dim P(V) + \dim W \dim P(W) \geq 50,$$

a contradiction. This completes the proof of the lemma. \square

Acknowledgments

The authors would like to thank Zhongzhu Lin for his suggestion on the proof of Lemma 1.3, and Michael Hilgeman for his comments on the first draft of this paper.

References

- [AN] Nicolás Andruskiewitsch, Sonia Natale, Counting arguments for Hopf algebras of low dimension, *Tsukuba J. Math.* 25 (1) (2001) 187–201, MR 2002d:16046.
- [And] Nicolás Andruskiewitsch, About finite dimensional Hopf algebras, in: *Quantum Symmetries in Theoretical Physics and Mathematics*, Bariloche, 2000, in: *Contemp. Math.*, vol. 294, Amer. Math. Soc., Providence, RI, 2002, pp. 1–57, MR 1907185 (2003f:16059).
- [AS1] N. Andruskiewitsch, H.-J. Schneider, Lifting of quantum linear spaces and pointed Hopf algebras of order p^3 , *J. Algebra* 209 (2) (1998) 658–691, MR 1659895 (99k:16075).

- [AS2] Nicolás Andruskiewitsch, Hans-Jürgen Schneider, Hopf algebras of order p^2 and braided Hopf algebras of order p , *J. Algebra* 199 (2) (1998) 430–454, MR 99c:16033.
- [BDG] M. Beattie, S. Dăscălescu, L. Grünenfelder, On the number of types of finite-dimensional Hopf algebras, *Invent. Math.* 136 (1) (1999) 1–7, MR 1681117 (2000a:16068).
- [Bea] Margaret Beattie, A survey of Hopf algebras of low dimension, *Acta Appl. Math.* 108 (1) (2009) 19–31, MR 2540955.
- [Ben] David J. Benson, *Representations and Cohomology*, Cambridge Stud. Adv. Math., vol. 30, Cambridge University Press, Cambridge, 1991.
- [CZ] Hui-Xiang Chen, Zhang Yinhao, Four-dimensional Yetter–Drinfeld module algebras over H_4 , *J. Algebra* 296 (2) (2006) 582–634, MR 2201057 (2006i:16054).
- [Doi] Yukio Doi, The trace formula for braided Hopf algebras, *Comm. Algebra* 28 (4) (2000) 1881–1895, MR 2001i:16066.
- [EG1] Pavel Etingof, Shlomo Gelaki, On families of triangular Hopf algebras, *Int. Math. Res. Not.* 14 (2002) 757–768, MR 2002m:16036.
- [EG2] Pavel Etingof, Shlomo Gelaki, On Hopf algebras of dimension pq , *J. Algebra* 277 (2) (2004) 668–674, MR 2067625 (2005d:16061).
- [ENO] P. Etingof, D. Nikshych, V. Ostrik, Weakly group-theoretical and solvable fusion categories, preprint.
- [FMS] D. Fischman, S. Montgomery, H.-J. Schneider, Frobenius extensions of subalgebras of Hopf algebras, *Trans. Amer. Math. Soc.* 349 (12) (1997) 4857–4895, MR 1401518 (98c:16049).
- [Fuk] Nobuyuki Fukuda, Semisimple Hopf algebras of dimension 12, *Tsukuba J. Math.* 21 (1) (1997) 43–54, MR 1467220 (98h:16060).
- [FukD] Daijiro Fukuda, Hopf algebras of dimension 30, *J. Algebra Appl.* 9 (1) (2010) 11–15, MR 2642810.
- [Gel1] Shlomo Gelaki, Quantum groups of dimension pq^2 , *Israel J. Math.* 102 (1997) 227–267, MR 1489107 (98j:16023).
- [Gel2] Shlomo Gelaki, Pointed Hopf algebras and Kaplansky’s 10th conjecture, *J. Algebra* 209 (2) (1998) 635–657, MR 1659891 (99j:16024).
- [GV] G.A. García, C. Vay, Hopf algebras of dimension 16, *Algebr. Represent. Theory*, doi:10.1007/s10468-009-9128-7.
- [HN] M. Hilgmann, Siu-Hung Ng, Hopf algebras of dimension $2p^2$, *J. Lond. Math. Soc.* 80 (2) (2009) 295–310.
- [Kap] Irving Kaplansky, *Bialgebras*, Lecture Notes in Math., Department of Mathematics, University of Chicago, Chicago, IL, 1975.
- [LR] Richard G. Larson, David E. Radford, Semisimple cosemisimple Hopf algebras, *Amer. J. Math.* 109 (1) (1987) 187–195, MR 89a:16011.
- [LR] Richard G. Larson, David E. Radford, Finite-dimensional cosemisimple Hopf algebras in characteristic 0 are semisimple, *J. Algebra* 117 (2) (1988) 267–289, MR 89k:16016.
- [Mas] Akira Masuoka, Freeness of Hopf algebras over coideal subalgebras, *Comm. Algebra* 20 (5) (1992) 1353–1373, MR 1157912 (93d:16051).
- [Mon] Susan Montgomery, *Hopf Algebras and Their Actions on Rings*, CBMS Reg. Conf. Ser. Math., vol. 82, Published for the Conference Board of the Mathematical Sciences, Washington, DC, 1993.
- [Nat1] Sonia Natale, On semisimple Hopf algebras of dimension pq^2 , *J. Algebra* 221 (1) (1999) 242–278, MR 1722912 (2000k:16050).
- [Nat2] Sonia Natale, On semisimple Hopf algebras of dimension pq^2 , II, *Algebr. Represent. Theory* 4 (3) (2001) 277–291, MR 1852000 (2002i:16055).
- [Nat3] Sonia Natale, Hopf algebras of dimension 12, *Algebr. Represent. Theory* 5 (5) (2002) 445–455, MR 1935855 (2003i:16055).
- [Nat4] Sonia Natale, On semisimple Hopf algebras of dimension pq^f , *Algebr. Represent. Theory* 7 (2) (2004) 173–188, MR 2063008 (2005c:16057).
- [Ng1] Siu-Hung Ng, Non-semisimple Hopf algebras of dimension p^2 , *J. Algebra* 255 (1) (2002) 182–197.
- [Ng2] Siu-Hung Ng, Hopf algebras of dimension pq , *J. Algebra* 276 (1) (2004) 399–406, MR 2054403 (2005d:16066).
- [Ng3] Siu-Hung Ng, Hopf algebras of dimension $2p$, *Proc. Amer. Math. Soc.* 133 (8) (2005) 2237–2242 (electronic), MR 2138865 (2006a:16055).
- [Ng4] Siu-Hung Ng, Hopf algebras of dimension pq , II, *J. Algebra* 319 (7) (2008) 2772–2788, MR 2397407 (2009h:16052).
- [Rad1] David E. Radford, On a coradical of a finite-dimensional Hopf algebra, *Proc. Amer. Math. Soc.* 53 (1) (1975) 9–15, MR 0396652 (53 #514).
- [Rad2] David E. Radford, The order of the antipode of a finite dimensional Hopf algebra is finite, *Amer. J. Math.* 98 (2) (1976) 333–355, MR 53 #10852.
- [Rad3] David E. Radford, The structure of Hopf algebras with a projection, *J. Algebra* 92 (2) (1985) 322–347, MR 86k:16004.
- [Rad4] David E. Radford, The trace function and Hopf algebras, *J. Algebra* 163 (3) (1994) 583–622, MR 95e:16039.
- [Tak] Mitsuhiro Takeuchi, Quotient spaces for Hopf algebras, *Comm. Algebra* 22 (7) (1994) 2503–2523, MR 1271619 (95h:16055).
- [Zhu] Yongchang Zhu, Hopf algebras of prime dimension, *Int. Math. Res. Not.* 1 (1994) 53–59, MR 1255253 (94j:16072).