Louisiana State University

LSU Digital Commons

Faculty Publications

Department of Mathematics

1-1-2009

Hopf algebras of dimension $2p^2$

Michael Hilgemann

Iowa State University

Siu Hung Ng

Iowa State University

Follow this and additional works at: https://digitalcommons.lsu.edu/mathematics_pubs

Recommended Citation

Hilgemann, M., & Ng, S. (2009). Hopf algebras of dimension $2p^2$. *Journal of the London Mathematical Society, 80* (2), 295-310. https://doi.org/10.1112/jlms/jdp026

This Article is brought to you for free and open access by the Department of Mathematics at LSU Digital Commons. It has been accepted for inclusion in Faculty Publications by an authorized administrator of LSU Digital Commons. For more information, please contact ir@lsu.edu.

J. London Math. Soc. (2) 80 (2009) 295–310 © 2009 London Mathematical Society
doi:10.1112/jlms/jdp026

Hopf algebras of dimension $2p^2$

Michael Hilgemann and Siu-Hung Ng

Dedicated to Susan Montgomery on the occasion of her birthday

Abstract

Let H be a non-semisimple Hopf algebra of dimension $2p^2$ over an algebraically closed field $\Bbbk$ of characteristic zero, where p is an odd prime. We prove that H or H^* is pointed, which completes the classification for Hopf algebras of these dimensions.

Introduction

In recent years, there have been some developments in the classification of finite-dimensional Hopf algebras over an algebraically closed field $\Bbbk$ of characteristic zero. For a prime p, Hopf algebras of dimension p were shown by Zhu [**34**] to be isomorphic to the group algebra $\Bbbk[\mathbb{Z}_p]$. Hopf algebras of dimension p^2 were completely classified in [**13**, **20**]. In the semisimple case, they are isomorphic to either $\Bbbk[\mathbb{Z}_{p^2}]$ or $\Bbbk[\mathbb{Z}_p \times \mathbb{Z}_p]$, and, in the non-semisimple case, they are the Taft algebras of dimension p^2.

Semisimple Hopf algebras of dimension pq, where p and q are distinct primes, were first classified by Masuoka [**12**] for the case $p = 2$. For both p and q odd, they were studied independently in [**8**, **31**]. It was proved by Etingof and Gelaki [**4**] that these Hopf algebras must be trivial, that is, they are isomorphic to group algebras or the duals of group algebras.

It is, in general, an open question as to whether every Hopf algebra over $\Bbbk$ of dimension pq, where p and q are distinct primes, is semisimple. However, there have been some partial results that suggest an affirmative answer to the question. Natale showed that a quasi-triangular Hopf algebra of such a dimension is semisimple in [**18**]. In [**22**, **23**], the second author proved that there is no non-semisimple Hopf algebra of dimension $2p$ for an odd prime p, or of dimension pq with $2 < p < q \leqslant 4p + 11$. The latter improves the main results in [**5**, **21**].

These established classifications have provided a foundation for the investigation of a general Hopf algebra over $\Bbbk$ whose dimension is a product of three primes. The study of Hopf algebras of dimension p^3 was carried out by García [**7**]. In this paper, we address Hopf algebras of dimension $2p^2$ for an odd prime p.

Masuoka began the classification of semisimple Hopf algebras of dimension $2p^2$ in [**14**]. In the paper, he constructed a semisimple Hopf algebra $\mathcal{B}_0$ (denoted by A_ξ in that paper) of dimension $2p^2$, which he showed is the unique semisimple Hopf algebra H of such a dimension with $|G(H)| = p^2$. Natale completed the classification in [**17**] by showing that non-trivial semisimple Hopf algebras of dimension $2p^2$ are isomorphic to $\mathcal{B}_0$ or $\mathcal{B}_0^*$. Since $G(\mathcal{B}_0^*) \cong \mathbb{Z}_{2p}$, it follows that $\mathcal{B}_0$ is not self-dual.

The Hopf algebra $\mathcal{B}_0^*$ is a smash product Hopf algebra $\Bbbk[D_{2p}]^* \# \Bbbk[\mathbb{Z}_p]$, where D_{2p} is the dihedral group of order $2p$ (cf. [**17**]). The left $\Bbbk[\mathbb{Z}_p]$-action on $\Bbbk[D_{2p}]^*$ is induced by the right

---

Received 16 September 2008; published online 19 June 2009.

2000 *Mathematics Subject Classification* 16W30.

The research was partially supported by NSA grant no. H98230-05-1-0020.

action $\triangleleft$ of $\mathbb{Z}_p = \langle g \rangle$ on $D_{2p} = \langle a, b \mid b^p = 1, a^2 = 1, aba = b^{-1} \rangle$ as automorphisms given by

$$b \triangleleft g = b, \quad a \triangleleft g = ba.$$

For the case that H is a pointed non-semisimple Hopf algebra of dimension $2p^2$, it was shown by Andruskiewitsch and Natale [1] that H is isomorphic to one of the four types of Hopf algebras listed in Lemma A.1 of that paper. Specifically, let $j \in \{1, 2, 4, \ldots, 2p-2\}$ and $\mu \in \{0, 1\}$ such that $\mu = 0$ whenever $j \neq 1$. Also let $\tau \in \Bbbk$ be a $2p$th root of unity such that the order of τ is a multiple of p, with the order being p in the case that $j = 1$. Define $\mathcal{A}(\tau, j, \mu)$ to be the Hopf algebra generated by the elements g and x as an algebra subject to the relations

$$g^{2p} = 1, \quad x^p = \mu(1 - g^p), \quad gx = \tau xg,$$

with comultiplication given by

$$\Delta(g) = g \otimes g, \quad \Delta(x) = x \otimes 1 + g^j \otimes x.$$

Then the pointed non-semisimple Hopf algebras of dimension $2p^2$ are isomorphic to exactly one of the following $4(p-1)$ Hopf algebras:

(i) $\mathcal{A}(\omega, 1, 0)$, where ω is a primitive pth root of unity;
(ii) $\mathcal{A}(\omega, 1, 1)$, where ω is a primitive pth root of unity;
(iii) $\mathcal{A}(\tau, 2r, 0)$, for $1 \leqslant r \leqslant p-1$, where τ is a fixed primitive $2p$th root of unity;
(iv) $\mathcal{A}(\omega, 2, 0) \cong T_p \otimes \Bbbk[\mathbb{Z}_2]$, where ω is a primitive pth root of unity.

Here T_p is a Taft algebra of dimension p^2. It was pointed out in [1] that the dual of $\mathcal{A}(\omega, 1, 0)$ is isomorphic to a Hopf algebra of type (iii), and the Hopf algebras of type (iv) are self-dual. Therefore, the dual of a Hopf algebra of type (i), (iii), or (iv) is also pointed. However, the dual of $\mathcal{A}(\omega, 1, 1)$ is not pointed (cf. [25]).

In [6], Fukuda showed that non-semisimple Hopf algebras of dimension 18 are pointed or have a pointed dual. In this paper, we complete the classification of Hopf algebras of dimension $2p^2$ by proving the following main theorem.

Theorem I. *If H is a non-semisimple Hopf algebra of dimension $2p^2$ over an algebraically closed field of characteristic zero, where p is an odd prime, then H or H^* is pointed.*

In particular, this implies that there are exactly $5(p-1)$ isomorphism classes of non-semisimple Hopf algebras of dimension $2p^2$ over $\Bbbk$, and we summarize the classification as follows.

Theorem II. *Let H be a $2p^2$-dimensional Hopf algebra over an algebraically closed field $\Bbbk$ of characteristic zero, where p is an odd prime. Then one of the following holds:*

(a) *H is trivial;*
(b) *H is non-trivial and semisimple, and hence isomorphic to either $\mathcal{B}_0$ or $\mathcal{B}_0^*$;*
(c) *H is non-semisimple and pointed, and hence H is isomorphic to one of the $4(p-1)$ Hopf algebras of the form $\mathcal{A}(\omega, 1, 0)$, $\mathcal{A}(\omega, 1, 1)$, $\mathcal{A}(\tau, 2r, 0)$, or $\mathcal{A}(\omega, 2, 0)$, as described above;*
(d) *H is neither semisimple nor pointed. In this case, $H \cong \mathcal{A}(\omega, 1, 1)^*$ for some primitive pth root of unity $\omega \in \Bbbk$.*

The remainder of this paper is organized as follows. We start in Section 1 with some notation and preliminary results that will be useful in proving the main theorem. We show in Section 2 that a non-semisimple Hopf algebra of dimension $2p^2$ over an algebraically closed field $\Bbbk$ must have an antipode of order $2p$. Finally, in Section 3, we complete the classification of Hopf algebras of dimension $2p^2$ by showing that non-semisimple Hopf algebras of these dimensions are pointed or have a dual that is pointed.

Throughout this paper, $\Bbbk$ denotes an algebraically closed field of characteristic zero unless specifically stated otherwise. The tensor product $\otimes_{\Bbbk}$ will be simply denoted by $\otimes$. The readers are referred to [**15**, **32**] for elementary properties of Hopf algebras.

1. *Notation and preliminaries*

Let H be a finite-dimensional Hopf algebra over $\Bbbk$ with comultiplication Δ, counit ϵ, and antipode S. We use Sweedler's notation for comultiplication, $\Delta(h) = \sum_{(h)} h_1 \otimes h_2$, or simply $\Delta(h) = h_1 \otimes h_2$, suppressing the summation. The coassociativity of Δ induces two natural H^*-actions, $\rightharpoonup$ and $\leftharpoonup$, on H given by

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

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 the left (or right) integrals of H is always one-dimensional. One can easily see that an element $\lambda \in H^*$ is a right integral if and only if

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

A non-zero element $a \in H$ is said to be *group-like* if $\Delta(a) = a \otimes a$. 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 $\Bbbk$. The *distinguished group-like* elements $g \in G(H)$ and $\alpha \in G(H^*)$ are defined by the conditions:

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

where $\lambda \in H^*$ is a non-zero right integral, and $\Lambda \in H$ is a non-zero left integral. These distinguished group-like elements are closely related to the antipode, as indicated by the following celebrated formula of Radford [**26**]:

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

In particular, we find

$$\operatorname{ord}(S^2) \mid 2 \cdot \operatorname{lcm}(\operatorname{ord}(g), \operatorname{ord}(\alpha)). \tag{1.3}$$

The square of the antipode indeed determines the semisimplicity of a Hopf algebra. The following result, which will be used tacitly in the remaining discussion, was mainly proved by Larson and Radford [**10**, **11**] (see also [**16**] for an alternative treatment of the result by Montgomery).

THEOREM 1.1. *The following statements on a finite-dimensional Hopf algebra H over an algebraically closed field of characteristic zero with antipode S are equivalent:*

(a) *H is semisimple;*
(b) *H^* is semisimple;*
(c) $\operatorname{Tr}(S^2) \neq 0$*;*
(d) $S^2 = \operatorname{id}_H$.

Let $a \in H$ be a group-like element of order m. Then $\Bbbk[a]$ is a commutative Hopf subalgebra of H. Let $\omega \in \Bbbk$ be a primitive mth root of unity and define

$$e_{a,j} = \frac{1}{m} \sum_{i \in \mathbb{Z}_m} \omega^{-ij} a^i \quad \text{for } j \in \mathbb{Z}_m. \tag{1.4}$$

Then $\{e_{a,j}\}_{j\in\mathbb{Z}_m}$ is a complete set of primitive idempotents of $\Bbbk[a]$, that is,

$$e_{a,i}\cdot e_{a,j}=\delta_{ij}e_{a,i},\qquad \sum_{j\in\mathbb{Z}_m} e_{a,j}=1.$$

Therefore, for any right $\Bbbk[a]$-module V, we always have the $\Bbbk[a]$-module decomposition

$$V=\bigoplus_{i\in\mathbb{Z}_m} Ve_{a,i}.$$

Note that $\Bbbk[a]=\bigoplus_{j\in\mathbb{Z}_m}\Bbbk e_{a,j}$ as ideals of $\Bbbk[a]$. If V is a free right $\Bbbk[a]$-module, then $\operatorname{ord}(a)$ divides $\dim V$ and

$$\dim Ve_{a,j}=\frac{\dim V}{\operatorname{ord}(a)}.$$

Obviously, the same conclusion can be drawn for left $\Bbbk[a]$-modules V. Moreover, one can construct the complete set of primitive idempotents $\{e_{\beta,j}\}$ for each group-like element $\beta\in H^*$ in the same way.

LEMMA 1.2. *Let H be a finite-dimensional Hopf algebra over $\Bbbk$ with antipode S. Suppose that $a\in G(H)$ and $\beta\in G(H^*)$ are such that $\beta(a)=1$, and write H_{ij} for $He_{a,i}\leftharpoonup e_{\beta,j}$ for $i\in\mathbb{Z}_{\operatorname{ord}(a)}$ and $j\in\mathbb{Z}_{\operatorname{ord}(\beta)}$. Then the following hold.*

(a) *We have the $\Bbbk$-linear space decomposition $H=\bigoplus_{i,j}H_{ij}$, and*

$$\dim H_{ij}=\frac{\dim H}{\operatorname{ord}(a)\cdot\operatorname{ord}(\beta)}\quad \textit{for all } i,j.$$

(b) *If H is not semisimple, then $\operatorname{Tr}(S^2|_{H_{ij}})=0$ for all i,j.*

Proof. (a) By the Nichols–Zoeller theorem (see [**24**]), H is a free right $\Bbbk[a]$-module. It follows, by the preceding remark, that $\dim He_{a,i}=\dim H/\operatorname{ord}(a)$ for $i\in\mathbb{Z}_{\operatorname{ord}(a)}$, and

$$H=\bigoplus_{i\in\mathbb{Z}_{\operatorname{ord}(a)}} He_{a,i}.$$

Since $\beta(a)=1$, it follows that

$$(ha^i)\leftharpoonup\beta=(h\leftharpoonup\beta)a^i\quad\text{for all integers } i \text{ and } h\in H.$$

Let $e=e_{a,i}$ for some $i\in\mathbb{Z}_{\operatorname{ord}(a)}$. Then $(he)\leftharpoonup\beta=(h\leftharpoonup\beta)e$ for $h\in H$. In particular, He is a right $\Bbbk[\beta]$-module under the action $\leftharpoonup$. Consider the left $\Bbbk[\beta]$-module action on He defined by

$$\beta\rightharpoonup x=x\leftharpoonup(\beta^{-1})\quad\text{for all } x\in He.$$

Since He is a left H-module, it admits a natural right H^*-comodule structure $\rho: He\to He\otimes H^*$ with $\rho(x)=\sum x^{(0)}\otimes x^{(1)}$ defined by $hx=\sum x^{(0)}x^{(1)}(h)$ for all $h\in H$. It is straightforward to check that $\rho(\beta\rightharpoonup x)=\beta\cdot\rho(x)$ for $x\in He$. Hence, He is a Hopf module in ${}_{\Bbbk[\beta]}\mathcal{M}^{H^*}$. By the Nichols–Zoeller theorem, we find that He is a free left $\Bbbk[\beta]$-module under the action $\rightharpoonup$. By the preceding remark again, we have

$$He=\bigoplus_j e_{\beta,j}\rightharpoonup He\quad\text{and}\quad \dim\left(e_{\beta,j}\rightharpoonup He\right)=\frac{\dim He}{\operatorname{ord}(\beta)}=\frac{\dim H}{\operatorname{ord}(a)\cdot\operatorname{ord}(\beta)}.$$

Since $e_{\beta,j}\rightharpoonup x=x\leftharpoonup e_{\beta,-j}$, we obtain

$$He=\bigoplus_j H_{ij}\quad\text{and}\quad \dim H_{ij}=\frac{\dim H}{\operatorname{ord}(a)\cdot\operatorname{ord}(\beta)}.$$

(b) Let E_i and F_j denote the $\Bbbk$-linear operators on H defined by

$$E_i(h) = he_{a,i}, \quad F_j(h) = h \leftharpoondown e_{\beta,j} \text{ for } i \in \mathbb{Z}_{\mathrm{ord}(a)},\ j \in \mathbb{Z}_{\mathrm{ord}(\beta)}.$$

Then both E_i and F_j are projections on H and $H_{ij} = F_j E_i(H)$. Since $S^2(a) = a$ and $\beta \circ S^2 = \beta$, the operator S^2 commutes with both E_i and F_j. Therefore, $S^2(H_{ij}) \subseteq H_{ij}$, and so

$$\mathrm{Tr}(S^2|_{H_{ij}}) = \mathrm{Tr}(S^2 \circ F_j \circ E_i) = \mathrm{Tr}(E_i \circ S^2 \circ F_j).$$

It follows, by [**28**, Proposition 2(a)], that

$$\mathrm{Tr}(S^2|_{H_{ij}}) = \lambda(e_{a,i})e_{\beta,j}(\Lambda) = \sum_{l,k} \gamma_{lk}\lambda(a^l)\beta^k(\Lambda) \tag{1.5}$$

for some $\gamma_{lk} \in \Bbbk$, where $\lambda \in H^*$ is a right integral, and $\Lambda \in H$ is a left integral such that $\lambda(\Lambda) = 1$. The properties of integrals imply the equalities

$$\lambda(a^l)a^l = \lambda(a^l)1, \quad \beta^k(\Lambda)\beta^k = \beta^k(\Lambda)\epsilon \tag{1.6}$$

for all integers l and k. Since H is not semisimple, it follows that $\lambda(1_H) = \epsilon(\Lambda) = 0$. If a^l is not trivial, then the first equality of (1.6) and the linear independence of distinct group-like elements imply that $\lambda(a^l) = 0$. Similarly, we can also conclude that $\beta^k(\Lambda) = 0$ for all integers k. In view of (1.5), $\mathrm{Tr}(S^2|_{H_{ij}}) = 0$ for all i and j. □

Recall that a Hopf subalgebra A of a finite-dimensional Hopf algebra H is *normal* if and only if $\sum_{(h)} h_1 a S(h_2), \sum_{(h)} S(h_1)ah_2 \in A$ for all $h \in H$ and $a \in A$. Since H is finite-dimensional, it follows that A is a normal Hopf subalgebra of H if and only if $A^+H = HA^+$, which is in turn equivalent to $A^+H \subseteq HA^+$ or $HA^+ \subseteq A^+H$, where $A^+ = A \cap \ker \epsilon$ (see [**15**, Section 3.4] or [**19**, Corollary 16], for example).

Following [**30**], we say that a sequence of finite-dimensional Hopf algebras

$$1 \longrightarrow A \xrightarrow{\iota} H \xrightarrow{\pi} B \longrightarrow 1 \tag{1.7}$$

is *exact* if ι and π are injective and surjective Hopf algebra maps, respectively, such that $\iota(A)$ is normal in H and $\ker \pi = H\iota(A^+)$. In this case, H is called an *extension* of B by A. Moreover, the dual sequence

$$1 \longrightarrow B^* \xrightarrow{\pi^*} H^* \xrightarrow{\iota^*} A^* \longrightarrow 1 \tag{1.8}$$

of (1.7) is also an exact sequence of Hopf algebras.

The next sequence of propositions on some extensions of finite-dimensional Hopf algebras will be used to show the main theorem in the next two sections, and may be of interest in their own right.

Proposition 1.3. *Let H and A be finite-dimensional Hopf algebras over $\Bbbk$ of dimension $2n$ and n, respectively, where n is an odd integer. Then the following hold.*

(a) *If there exists a Hopf algebra surjection $\pi : H \to A$, then*

$$R = H^{\mathrm{co}\,\pi} = \{h \in H \mid (\mathrm{id}_H \otimes \pi)\Delta(H) = h \otimes 1_A\}$$

is a normal Hopf subalgebra of H that is isomorphic to $\Bbbk[\mathbb{Z}_2]$.

(b) *If A is a Hopf subalgebra of H, then A is a normal Hopf subalgebra of H.*

Proof. (a) It is well known that R is a left coideal subalgebra of H of dimension 2, and $HR^+ \subseteq R^+H$. In view of the preceding remark, it suffices to show that R contains a non-trivial group-like element. Let x be a non-zero element of R such that $\epsilon(x) = 0$. Then $\{1, x\}$ is a basis for R and $\Delta(x) = a \otimes 1 + b \otimes x$ for some $a, b \in H$. By applying $\mathrm{id}_H \otimes \epsilon$ and $\epsilon \otimes \mathrm{id}_H$ to $\Delta(x)$, we find that $a = x$ and $\epsilon(b) = 1$. Noting that $(\mathrm{id}_H \otimes \Delta)\Delta(x) = (\Delta \otimes \mathrm{id}_H)\Delta(x)$, we obtain that b is a group-like element of H, and so x is a $(1, b)$-skew primitive element. Since H is finite-dimensional and $x \neq 0$, we have $b \neq 1$. Note that $\{x\}$ is a basis for $\ker \epsilon|_R$, and $bxb^{-1} \in R$. Since $\epsilon(bxb^{-1}) = 0$, it follows that $bxb^{-1} = \zeta x$ for some primitive Mth root of unity $\zeta \in \Bbbk$, where $M \mid \mathrm{ord}(b)$.

Suppose that x is a non-trivial $(1, b)$-skew primitive element. Then, by [**1**, Proposition 1.8], $\zeta \neq 1$ and x and b generate a Hopf subalgebra $K \cong K_\mu(\mathrm{ord}(b), \zeta)$ for some $\mu \in \{0, 1\}$. In particular, we have

$$M^2 \mid \dim K \mid \dim H.$$

On the other hand, since $\epsilon(x^2) = 0$, it follows that $x^2 = \gamma x$ for some $\gamma \in \Bbbk$. Therefore, $(bxb^{-1})^2 = \gamma bxb^{-1}$, which implies that $\gamma\zeta^2 = \gamma\zeta$. Thus $\gamma = 0$, and hence $x^2 = 0$. As a consequence, $K \cong K_0(\mathrm{ord}(b), \zeta)$ and $M = 2$ is the nilpotency index of x. In particular, $4 \mid \dim H$, which is a contradiction. Therefore, x must be a trivial $(1, b)$-skew primitive element, and hence $x = \nu(1 - b)$ for some non-zero $\nu \in \Bbbk$. This implies that $b \in R$, and so $R = \Bbbk[b]$.

(b) Consider the dual of the inclusion map $A \hookrightarrow H$, which is a Hopf algebra surjection $\pi : H^* \to A^*$. By part (a), $(H^*)^{\mathrm{co}\,\pi} \cong \Bbbk[\mathbb{Z}_2]$ is a normal Hopf subalgebra of H^*, and so we have the following exact sequence of Hopf algebras:

$$1 \to \Bbbk[\mathbb{Z}_2] \to H^* \xrightarrow{\pi} A^* \to 1.$$

Dualizing this exact sequence, the result follows. □

Remark 1.4. Susan Montgomery has pointed out that Proposition 1.3(b) is a generalization of Proposition 2 in [**9**] to non-semisimple Hopf algebras of dimension $2n$ with n odd.

The following result generalizes Lemma 5.1 in [**20**]. This proposition and its corollary provide a useful way of eliminating certain cases in the next section, especially since we are dealing with non-semisimple Hopf algebras.

Proposition 1.5. *Let H be a finite-dimensional Hopf algebra over $\Bbbk$. If there exist semisimple Hopf subalgebras $A \subseteq H$ and $K \subseteq H^*$ such that $\dim H = (\dim A)(\dim K)$ and $\gcd(\dim A, \dim K) = 1$, then H is semisimple.*

Proof. Define the Hopf algebra surjection

$$\pi : H \cong H^{**} \xrightarrow{i^*} K^*,$$

where $i : K \to H^*$ is inclusion. As $\gcd(\dim A, \dim K) = 1$, it follows that the image of A under π is one-dimensional. Moreover, $A^+ \subseteq \ker \pi$, and so

$$\pi(a) = \pi(a - \epsilon(a)1) + \pi(\epsilon(a)1) = \epsilon(a)\pi(1)$$

for all $a \in A$. Therefore, $A \subseteq H^{\mathrm{co}\,\pi} = \{h \in H \mid h_1 \otimes \pi(h_2) = h \otimes 1_{K^*}\}$. However, $\dim H^{\mathrm{co}\,\pi} = \dim H / \dim K = \dim A$, and so $A = H^{\mathrm{co}\,\pi}$. It follows, by [**29**], that H is isomorphic to a cross product algebra $A \#_\sigma K^*$ for some 2-cocycle σ. By [**3**, Theorem 2.6], the semisimplicity of A and K^* implies the semisimplicity of H. □

Corollary 1.6. *Suppose that n is an odd integer. If H is a $2n$-dimensional Hopf algebra over the field $\Bbbk$, and H contains a semisimple Hopf subalgebra of dimension n, then H is semisimple.*

Proof. Let K be a semisimple Hopf subalgebra of H with $\dim K = n$. Then there is a Hopf algebra surjection $\pi : H^* \to K^*$ and K^* is semisimple. By Proposition 1.3, we have the exact sequence of Hopf algebras as follows:

$$1 \longrightarrow \Bbbk[\mathbb{Z}_2] \longrightarrow H^* \xrightarrow{\pi} K^* \longrightarrow 1.$$

By Proposition 1.5, H is semisimple. □

The Taft algebras have been the basic examples of non-semisimple Hopf algebras (see [**33**]). The next proposition implies the existence of some semisimple Hopf subalgebras in the dual of an extension of a finite group algebra by a Taft algebra. We will need this result in the proof of Lemma 3.4 in the last section.

PROPOSITION 1.7. *Let H be a finite-dimensional Hopf algebra over $\Bbbk$ and let A be a normal Hopf subalgebra of H such that H/HA^+ is isomorphic to $\Bbbk[G]$ for some finite group G. If the Jacobson radical J of A is a Hopf ideal of A, then HJ is a Hopf ideal of H, and we have the exact sequence of Hopf algebras as follows:*

$$1 \longrightarrow A/J \longrightarrow H/HJ \longrightarrow \Bbbk[G] \longrightarrow 1.$$

In particular, H^* admits a semisimple Hopf subalgebra of dimension $|G| \dim(A/J)$.

Proof. Since $H/HA^+ \cong \Bbbk[G]$ as Hopf algebras, by [**29**], the (right) $\Bbbk[G]$-extension $A \subset H$ is H-cleft. Therefore, there exists a convolution invertible right $\Bbbk[G]$-comodule map $\gamma : \Bbbk[G] \to H$ with the convolution inverse $\overline{\gamma}$ such that $\gamma(1) = 1_H$, and $\gamma(g)A\overline{\gamma}(g) \subseteq A$ for all $g \in G$, and $\sigma(g,h) = \gamma(g)\gamma(h)\overline{\gamma}(gh)$ for $g, h \in G$ defines a 2-cocycle on G with coefficients in A. Moreover, the $\Bbbk$-linear map $\Phi : A\#_\sigma\Bbbk[G] \to H$ defined by $a\#g \mapsto a\gamma(g)$ is an algebra isomorphism (cf. [**15**]). In particular, $H = \bigoplus_{g\in G} A\gamma(g)$ as $\Bbbk$-linear spaces.

Note that $\gamma(g)$ is an invertible element of H with inverse $\overline{\gamma}(g)$ for all $g \in G$, since $\gamma * \overline{\gamma}(g) = 1_H$. Therefore, $a \mapsto \gamma(g)a\overline{\gamma}(g)$ defines an algebra automorphism on A. In particular, we find that $J = \gamma(g)J\overline{\gamma}(g)$. Thus, we have

$$\gamma(g)A = A\gamma(g), \quad \gamma(g)J = J\gamma(g) \quad \text{for all } g \in G.$$

Therefore, we have

$$JH = \sum_{g\in G} JA\gamma(g) = \sum_{g\in G} J\gamma(g) = \sum_{g\in G} \gamma(g)J = \sum_{g\in G} \gamma(g)AJ = HJ,$$

and hence HJ is a nilpotent Hopf ideal of H.

If $a \in A \cap HJ$, then $Aa \subseteq HJ$ is also nilpotent, and so $a \in J$. Therefore, the natural map $\iota : A/J \to H/HJ$ induced from the inclusion map $i : A \to H$ is also injective. Since A is normal in H, it follows that $\iota(A/J)$ is normal in H/HJ. Let $\pi : H/HJ \to H/HA^+$ be the natural surjection. It is immediate to see that $\ker \pi = HA^+/HJ = (H/HJ)\iota(A/J)^+$. Therefore, the sequence of finite-dimensional Hopf algebras

$$1 \longrightarrow A/J \xrightarrow{\iota} H/HJ \xrightarrow{\pi} H/HA^+ \longrightarrow 1$$

is exact. Consequently, H/HJ is a crossed product $A/J\#_\tau\Bbbk[G]$, and hence semisimple by [**3**, Theorem 2.6]. Moreover, $\dim H/HJ = |G| \dim(A/J)$. Since $(H/HJ)^*$ is isomorphic to a Hopf subalgebra of H^*, the second statement follows. □

We close this section with a few results on linear algebra that will be used frequently together with Lemma 1.2 to determine the order of an antipode in the next section. The first two results are known, and we prove the third.

Lemma 1.8. *Let V be a finite-dimensional vector space over the field $\Bbbk$, let p be a prime, and let T be a linear automorphism on V such that $\mathrm{Tr}(T) = 0$. Then the following hold.*

(a) *If $T^{2p} = \mathrm{id}_V$, then $\mathrm{Tr}(T^p) = pd$ for some integer d* (*see* [**2**, Lemma 2.6]).

(b) *If $T^{p^n} = \mathrm{id}_V$ for some positive integer n, then p divides the dimension of V* (*see* [**22**, Lemma 1.4]).

(c) *If $\dim V = p$ and $T^m = \mathrm{id}_V$ for some positive integer $m = 2^n p$, where p is odd, then $T^p = \xi\,\mathrm{id}_V$ for some 2^nth root of unity $\xi \in \Bbbk$.*

Proof. We prove part (c). The statement is obviously true for $n = 0$. We assume that $n \geqslant 1$. Let $\omega \in \Bbbk$ be a primitive mth root of unity and let V_b be the eigenspace of T associated to the eigenvalue ω^b. We consider the polynomial $f(x) = \sum_{b=0}^{m-1} (\dim V_b) x^b \in \mathbb{Z}[x]$. Since

$$0 = \mathrm{Tr}(T) = \sum_{b=0}^{m-1} (\dim V_b)\omega^b = f(\omega),$$

we have $f(x) = g(x)\Phi_m(x)$ for some $g(x) \in \mathbb{Z}[x]$, where Φ_k denotes the kth cyclotomic polynomial. Therefore, we have

$$\mathrm{Tr}(T^p) = f(\omega^p) = g(\omega^p)\Phi_m(\omega^p). \tag{1.9}$$

Note that $\{\omega^{pi} \mid i = 0, \dots, 2^{n-1} - 1\}$ is a basis for $\mathbb{Q}(\omega^p)$ and $\Phi_m(x) = \Phi_p(-x^{2^{n-1}})$. Therefore, we have

$$\Phi_m(\omega^p) = \Phi_p(-(\omega^p)^{2^{n-1}}) = \Phi_p(1) = p. \tag{1.10}$$

Let W_i be the eigenspace of T^p associated to the eigenvalue ω^{pi}. Since

$$\omega^{p(i+2^{n-1})} = -\omega^{pi} \quad \text{for } i = 0, \dots, 2^{n-1} - 1,$$

we have

$$\mathrm{Tr}(T^p) = \sum_{i=0}^{2^{n-1}-1} (\dim W_i - \dim W_{2^{n-1}+i})\omega^{pi}.$$

There exists i such that $\dim W_i - \dim W_{2^{n-1}+i} \neq 0$, otherwise $\dim V$ is even. By equations (1.9) and (1.10), $p \mid \dim W_i - \dim W_{2^{n-1}+i}$. Since $\dim V = p$, only one of the eigenspaces W_i and $W_{2^{n-1}+i}$ is non-zero and any other eigenspace of T^p is trivial. Thus, $T^p = \xi \mathrm{id}_V$ for some 2^nth root of unity $\xi \in \Bbbk$. □

2. *The order of the antipode*

Throughout the remainder of this paper, we assume that H is a non-semisimple Hopf algebra of dimension $2p^2$ over $\Bbbk$ with antipode S, where p is an odd prime. We will prove in this section that the antipodes of these Hopf algebras are of order $2p$ (Theorem 2.5).

To establish this result, we first consider the distinguished group-like elements $g \in H$ and $\alpha \in H^*$. Since $4 \nmid \dim H = 2p^2$, it follows, by [**22**, Corollary 2.2], that one of the distinguished group-like elements g or α is non-trivial. In view of the Nichols–Zoeller theorem, we have

$$\mathrm{lcm}(\mathrm{ord}(g), \mathrm{ord}(\alpha)) = 2, p, 2p, p^2, \text{ or } 2p^2.$$

Without loss of generality, we may assume that

$$\mathrm{ord}(g) \geqslant \mathrm{ord}(\alpha) \tag{2.1}$$

by duality. Under this assumption, $\mathrm{ord}(g) > 1$.

We write e_i for the idempotent $e_{g,i} \in \Bbbk[g]$ defined in (1.4), and f_j for $e_{\alpha,j} \in \Bbbk[\alpha]$. We define

$$H_{ij} = He_i \leftharpoonup f_j \quad \text{for all } i \in \mathbb{Z}_{\mathrm{ord}(g)} \text{ and } j \in \mathbb{Z}_{\mathrm{ord}(\alpha)}. \tag{2.2}$$

It follows, by Lemma 1.2, that

$$\dim He_i = \frac{\dim H}{\mathrm{ord}(g)} \quad \text{and} \quad \mathrm{Tr}(S^2|_{He_i}) = 0$$

for all $i \in \mathbb{Z}_{\mathrm{ord}(g)}$. If $\alpha(g) = 1$, then we also have

$$\mathrm{Tr}(S^2|_{H_{ij}}) = 0 \quad \text{for all } i, j.$$

We first eliminate those values of $\mathrm{lcm}(\mathrm{ord}(g), \mathrm{ord}(\alpha))$ that are not possible.

LEMMA 2.1. *The only possible values of* $\mathrm{lcm}(\mathrm{ord}(g), \mathrm{ord}(\alpha))$ *are* p *and* $2p$.

Proof. Assume that either $\mathrm{lcm}(\mathrm{ord}(g), \mathrm{ord}(\alpha)) = 2p^2$ or p^2. Since $\mathrm{ord}(g) \geqslant \mathrm{ord}(\alpha)$, it follows that $\mathrm{ord}(g) = p^2$ in both cases. Thus g generates a p^2-dimensional semisimple Hopf subalgebra of H. By Corollary 1.6, H must be semisimple, which is a contradiction.

If $\mathrm{lcm}(\mathrm{ord}(g), \mathrm{ord}(\alpha)) = 2$, then $\mathrm{ord}(g) = 2$ and $\mathrm{ord}(\alpha) = 1$ or 2. By Lemma 1.2, $\dim He_i = p^2$ and $\mathrm{Tr}(S^2|_{He_i}) = 0$ for $i \in \mathbb{Z}_2$. Using Radford's formula (1.2), we have that $S^8 = \mathrm{id}_H$. In particular, $(S^2|_{He_i})^4 = \mathrm{id}_{He_i}$. It follows, by Lemma 1.8(b), that $2 \mid \dim He_i = p^2$, which is another contradiction. □

Note that if $\mathrm{lcm}(\mathrm{ord}(g), \mathrm{ord}(\alpha)) = p$ or $2p$, then $\mathrm{ord}(g) = p$ or $2p$ as we are assuming that $\mathrm{ord}(g) \geqslant \mathrm{ord}(\alpha)$. We first eliminate the possibility that $\mathrm{ord}(g) = p$ and $\mathrm{ord}(\alpha) = 2$.

LEMMA 2.2. *The pair* $(\mathrm{ord}(g), \mathrm{ord}(\alpha))$ *cannot be* $(p, 2)$.

Proof. Suppose that $\mathrm{ord}(g) = p$ and $\mathrm{ord}(\alpha) = 2$. Then, by Radford's formula (1.2), $S^{8p} = \mathrm{id}_H$. Since p is an odd prime, we find that $\alpha(g) = 1$. From Lemma 1.2, we get

$$\dim H_{ij} = \frac{\dim H}{\mathrm{ord}(g) \cdot \mathrm{ord}(\alpha)} = p, \quad \mathrm{Tr}(S^2|_{H_{ij}}) = 0$$

for all $i \in \mathbb{Z}_p$ and $j \in \mathbb{Z}_2$, and H is a direct sum of the subspaces H_{ij} defined in (2.2). By Lemma 1.8(c), it follows that $(S^2|_{H_{ij}})^p = \zeta_{ij}\mathrm{id}_{H_{ij}}$ for some fourth root of unity $\zeta_{ij} \in \Bbbk$. Since $e_i \leftharpoonup f_0 = e_i$, and $S^2(e_i) = e_i$, it follows that $\zeta_{i0} = 1$ for all $i \in \mathbb{Z}_p$. Let $V_j = \bigoplus_i He_i \leftharpoonup f_j = H \leftharpoonup f_j$ for $j \in \mathbb{Z}_2$. Then $S^{2p}|_{V_0} = \mathrm{id}_{V_0}$. Thus, for $x \in V_0$, we have

$$x = S^{4p}(x) = \alpha \rightharpoonup x \leftharpoonup \alpha = \alpha \rightharpoonup x.$$

Let $L(\alpha)$ denote the linear operator on H defined by $L(\alpha)(x) = \alpha \rightharpoonup x$. Then $L(\alpha)^2 = \mathrm{id}_H$, $\mathrm{Tr}(L(\alpha)) = 0$, and $\mathrm{Tr}(L(\alpha)|_{V_0}) = p^2$. Since $L(\alpha)(V_1) \subseteq V_1$, it follows that $L(\alpha)|_{V_1} = -\mathrm{id}_{V_1}$. Therefore, $\alpha \rightharpoonup x \leftharpoonup \alpha = x$ for all $x \in V_1$, and hence $S^{4p} = \mathrm{id}_H$. In particular, H is of index p. It follows, by [**21**, Corollary 3.2], that the subspace

$$H_- = \{x \in H \mid S^{2p}(x) = -x\}$$

is of even dimension. Since $S^{2p}|_{V_0} = \mathrm{id}_{V_0}$, it follows that $H_- \subseteq V_1$.

Let V_{j+} and V_{j-} denote the eigenspaces of $S^2|_{V_j}$ associated to the eigenvalues 1 and -1, respectively. Since the p distinct eigenvalues of $S^2|_{H_{i1}}$ are $\zeta_{i1}, \zeta_{i1}\omega, \ldots, \zeta_{i1}\omega^{p-1}$, where $\omega \in \Bbbk$ is a primitive p-th root of unity, we find that

$$\dim\{x \in V_1 \mid S^{2p}(x) = x\} = p \dim V_{1+}, \quad \dim H_- = p \dim V_{1-}.$$

Let $\lambda \in H^*$ be a non-zero right integral. We claim that $(x, y) = \lambda(xy)$ defines a non-degenerate alternating form on V_{1+}. It follows, by [**28**], that

$$(x, y) = \lambda(xy) = \lambda(S^2(y \leftharpoonup \alpha)x) = -\lambda(yx) = -(y, x)$$

for all $x, y \in V_{1+}$. Moreover, we have

$$\lambda(S^2(v)) = \alpha(g)\lambda(v) = \lambda(v) = \lambda(\alpha \rightharpoonup v) \quad \text{for all } v \in H.$$

Therefore, $\lambda(v) = 0$ for any $v \in H$ that satisfies $S^2(v) = \mu v$ or $\alpha \rightharpoonup v = \mu v$ for some $\mu \in \Bbbk$ not equal to 1. Let $x \in V_{1+}$ be such that $\lambda(xy) = 0$ for all $y \in V_{1+}$. Then $\lambda(xy') = 0$ for all $y' \in H$. By the non-degeneracy of λ on H, we have $x = 0$, and hence $(\cdot, \cdot)$ is non-degenerate on V_{1+}. Thus, $\dim V_{1+}$ is even. Note that $p \dim V_{1+} + \dim H_- = \dim V_1 = p^2$. This implies that p^2 is even, which is a contradiction. □

We now proceed to show that $S^{2p} = \mathrm{id}_H$ for the remaining possibilities of $\mathrm{lcm}(\mathrm{ord}(g), \mathrm{ord}(\alpha))$. We shall use this to deduce in the next section that H or H^* is pointed.

Lemma 2.3. *If* $\mathrm{lcm}(\mathrm{ord}(g), \mathrm{ord}(\alpha)) = 2p$, *then* $S^{2p} = \mathrm{id}_H$.

Proof. Under this hypothesis, $S^{8p} = \mathrm{id}_H$ by Radford's formula (1.2). Moreover, either $\mathrm{ord}(g) = 2p$ or $(\mathrm{ord}(g), \mathrm{ord}(\alpha)) = (p, 2)$. The second case can be eliminated by Lemma 2.2. Therefore, $\mathrm{ord}(g) = 2p$, and $\dim He_i = p$ for $i \in \mathbb{Z}_{2p}$. Fix $i \in \mathbb{Z}_{2p}$ and set $T_i = S^2|_{He_i}$. Then $T_i^{4p} = \mathrm{id}_{He_i}$ and $\mathrm{Tr}(T_i) = 0$. By Lemma 1.8(c), we have $T_i^p = \zeta_i \, \mathrm{id}_{He_i}$ where $\zeta_i \in \Bbbk$ is a fourth root of unity. Note that

$$T_i(e_i) = S^2(e_i) = e_i.$$

Therefore, $\zeta_i = 1$, and so $T_i^p = \mathrm{id}_{He_i}$ for all $i \in \mathbb{Z}_{2p}$. Hence, we get that $S^{2p} = \mathrm{id}_H$, as desired. □

We now deal with the remaining case in the following lemma.

Lemma 2.4. *If* $\mathrm{lcm}(\mathrm{ord}(g), \mathrm{ord}(\alpha)) = p$, *then* $S^{2p} = \mathrm{id}_H$.

Proof. The proof will be presented in steps (i)–(v).

(i) Since $\mathrm{lcm}(\mathrm{ord}(g), \mathrm{ord}(\alpha)) = p$, it follows that $S^{4p} = \mathrm{id}_H$ by Radford's formula (1.2). In particular, the possible eigenvalues of S^{2p} are ± 1. Define

$$H_+ = \{x \in H \mid S^{2p}(x) = x\}, \quad H_- = \{x \in H \mid S^{2p}(x) = -x\}.$$

Then we have

$$\dim H_+ + \dim H_- = 2p^2 \quad \text{and} \quad \mathrm{Tr}(S^{2p}) = \dim H_+ - \dim H_-. \tag{2.3}$$

(ii) The pair $(\mathrm{ord}(g), \mathrm{ord}(\alpha))$ can either be $(p, 1)$ or (p, p). In both cases, $\mathrm{ord}(g) = p$. Hence $\mathrm{lcm}(\mathrm{ord}(g), \mathrm{ord}(S^4)) = p$, or, equivalently, H is of index p. It follows, by [**21**, Proposition 1.3], that $\dim H_-$ is an even integer.

(iii) *If* $(\mathrm{ord}(g), \mathrm{ord}(\alpha)) = (p, p)$, *then* $\alpha(g) \neq 1$. Otherwise, we can apply Lemma 1.2 and get

$$\dim H_{ij} = 2, \quad \mathrm{Tr}(S^2|_{H_{ij}}) = 0, \quad \text{and} \quad H = \bigoplus_{i,j \in \mathbb{Z}_p} H_{ij},$$

where H_{ij} are defined in (2.2). By (i), we find that $\left(S^2|_{H_{ij}}\right)^{2p} = \mathrm{id}_{H_{ij}}$, and so $S^2|_{H_{ij}}$ has exactly two distinct eigenvalues $\pm\xi$ for some pth root of unity $\xi \in \Bbbk$. Therefore, ± 1 are the two distinct eigenvalues of $S^{2p}|_{H_{ij}}$. This implies that $\dim H_- = \dim H_+ = p^2$, which contradicts (ii).

(iv) *We claim that* $\mathrm{Tr}(S^{2p}) = p^2 d$ *for some integer* d. If $(\mathrm{ord}(g), \mathrm{ord}(\alpha)) = (p, 1)$, then H is a unimodular Hopf algebra of index p by (ii). It follows immediately, by [**20**, Lemma 4.3], that $\mathrm{Tr}\left(S^{2p}\right) = p^2 d$ for some integer d. We may now assume that $(\mathrm{ord}(g), \mathrm{ord}(\alpha)) = (p, p)$. Let

$B = \Bbbk[g]$ and $I = \Bbbk[\alpha]^\perp$, which is a Hopf ideal of H, and $\overline{H} = H/I \cong \Bbbk[\alpha]^* \cong B$. Let $\pi : H \to B$ be such a surjection of Hopf algebras. By (iii), $\alpha(g) \neq 1$, and so $g - 1 \notin \Bbbk[\alpha]^\perp$, or, equivalently, $\pi(g) \neq 1_{\overline{H}}$. Since $\dim \overline{H} = p$, it follows that $\pi(B) = \overline{H}$. Therefore, the composition $\pi \circ i : B \to \overline{H}$ is an isomorphism of Hopf algebras, where $i : B \to H$ is inclusion. Thus, there exists a surjective Hopf algebra map $\nu : H \to B$ such that $\nu \circ i = \mathrm{id}_B$. Hence, by [**27**], H is isomorphic to the biproduct $R \times B$, where R is the right coinvariant given by

$$R = H^{\mathrm{co}\,\nu} = \{h \in H \mid (\mathrm{id}_H \otimes \nu)\Delta(h) = h \otimes 1_B\}.$$

Due to the results in [**2**, Section 4], R is invariant under S^2 and $S^2 = T \otimes S^2|_B$, where $T = S^2|_R$ if one identifies H with $R \times B$. Since $S^2|_B = \mathrm{id}_B$ and

$$0 = \mathrm{Tr}(S^2) = \mathrm{Tr}(T)\mathrm{Tr}(\mathrm{id}_B) = \mathrm{Tr}(T)p,$$

it follows that $\mathrm{Tr}(T) = 0$. Also, we have that $T^{2p} = \mathrm{id}_R$ as $S^{4p} = \mathrm{id}_H$. Thus, by Lemma 1.8(b), $\mathrm{Tr}(T^p) = pd$ for some integer d. Therefore, we have

$$\mathrm{Tr}(S^{2p}) = \mathrm{Tr}(T^p)\mathrm{Tr}(\mathrm{id}_B) = p^2 d,$$

as claimed.

(v) The equalities in (2.3) imply that d is an even integer. Since

$$-2p^2 \leqslant \mathrm{Tr}\big(S^{2p}\big) \leqslant 2p^2,$$

it follows that d can only be $-2, 0$, or 2. Note that, if $d = -2$, then $S^{2p} = -\mathrm{id}_H$, which is not possible as $S^{2p}(1_H) = 1_H$. If $d = 0$, then $\mathrm{Tr}\big(S^{2p}\big) = 0$, and hence $\dim H_+ = \dim H_- = p^2$. However, this contradicts (ii) that asserts that $\dim H_-$ is even. Hence $d = 2$, and so $\mathrm{Tr}(S^{2p}) = 2p^2$, which implies that $S^{2p} = \mathrm{id}_H$, as desired. □

With the beginning remarks and these four lemmas, we have proved the following theorem.

THEOREM 2.5. *Let p be an odd prime and let H be a non-semisimple Hopf algebra over $\Bbbk$ of dimension $2p^2$. Then the order of the antipode of H is $2p$.*

3. *Non-semisimple Hopf algebras of dimension $2p^2$*

In this section, we will show that, if H is a non-semisimple Hopf algebra of dimension $2p^2$ over $\Bbbk$ for an odd prime p, then H or H^* is pointed. This completes the proof of our main result Theorem I. Recall that a Hopf algebra H over $\Bbbk$ is *pointed* if its simple subcoalgebras are all one-dimensional. Therefore, H^* is pointed if all simple H-modules are one-dimensional.

We continue to assume that H is a non-semisimple Hopf algebra of dimension $2p^2$ over the field $\Bbbk$ with the antipode S, where p is an odd prime. Again, we let $g \in G(H)$ and $\alpha \in G(H^*)$ denote the distinguished group-like elements. From Section 2, we know that the order of the antipode S of H is $2p$, and that

$$\mathrm{lcm}(\mathrm{ord}(g), \mathrm{ord}(\alpha)) = p \text{ or } 2p.$$

By duality, we assume that $\mathrm{ord}(\alpha) \geqslant \mathrm{ord}(g)$ *in this section.* Therefore, $\mathrm{ord}(\alpha) = p$ or $2p$. Note that the opposite assumption was made in Section 2.

For any finite-dimensional H-module V, the left dual $V^\vee$ of V is the H-module with the underlying space $V^* = \mathrm{Hom}_\Bbbk(V, \Bbbk)$ and the H-action given by

$$(h \cdot f)(v) = f(S(h)v) \quad \text{for all } f \in V^* \text{ and } v \in V.$$

For an algebra automorphism σ on H, let ${}_\sigma V$ be the H-module with the underlying space V and the action given by $h \cdot_\sigma v = \sigma(h)v$ for all $h \in H$ and $v \in V$. It is easy to verify that the natural isomorphism $j : V \to V^{**}$ of vector spaces is also an H-module map from ${}_{S^2}V$ to $V^{\vee\vee}$. Hence, we have

$$ {}_{S^2}V \overset{j}{\cong} V^{\vee\vee} \quad \text{for } V \in H\text{-}\mathbf{mod}_{\mathsf{fin}}. \tag{3.1}$$

Let $P(V)$ denote the projective cover of $V \in H\text{-}\mathbf{mod}_{\mathsf{fin}}$. For $\beta \in G(H^*)$, we define $\Bbbk_\beta$ as the one-dimensional H-module that affords the irreducible character β. We simply denote by $\Bbbk$ the trivial one-dimensional H-module $\Bbbk_\epsilon$.

We denote by $[V]$ the isomorphism class of a simple H-module V. The cyclic group $G = \langle\alpha\rangle$ acts on the set $\mathrm{Irr}(H)$ of all isomorphism classes of simple H-modules by setting

$$\beta[V] = [\Bbbk_\beta \otimes V]$$

for all $\beta \in G$ and $[V] \in \mathrm{Irr}(H)$. We denote the G-orbit of $[V]$ in $\mathrm{Irr}(H)$ by $O(V)$. Since $\Bbbk_\beta \otimes -$ is a $\Bbbk$-linear equivalence on $H\text{-}\mathbf{mod}_{\mathsf{fin}}$, we have $P(\Bbbk_\beta \otimes V) \cong \Bbbk_\beta \otimes P(V)$, and thus $\dim P(W) = \dim P(V)$ for all $[W] \in O(V)$. In particular, $\dim P(\Bbbk) = \dim P(\Bbbk_\beta)$ for all $\beta \in G$. Suppose that $\{[V_0], [V_1], \ldots, [V_t]\}$ is a complete set of representatives of G-orbits in $\mathrm{Irr}(H)$ with $V_0 = \Bbbk$. The left H-module H has the decomposition of principal modules as follows:

$$\begin{aligned} H &\cong \bigoplus_{[V]\in \mathrm{Irr}(H)} (\dim V)\cdot P(V) \\ &\cong \bigoplus_{\beta\in\langle\alpha\rangle} P(\Bbbk_\beta) \oplus \bigoplus_{i=1}^{t} \dim V_i \left(\bigoplus_{[W]\in O(V_i)} P(W)\right). \end{aligned} \tag{3.2}$$

This decomposition implies the following equation:

$$\dim H = \mathrm{ord}(\alpha)\dim P(\Bbbk) + \sum_{i>0} |O(V_i)| \dim V_i \cdot \dim P(V_i). \tag{3.3}$$

We can now demonstrate that $\dim P(\Bbbk)$ can only take two possible values.

LEMMA 3.1. *The value of* $\dim P(\Bbbk)$ *can either be* p *or* $2p$.

Proof. We have that

$$P(\Bbbk) \cong P(\Bbbk^{\vee\vee}) \cong P(\Bbbk)^{\vee\vee} \cong {}_{S^2}P(\Bbbk).$$

Since $S^{2p} = \mathrm{id}_H$, by Lemma A.2 in the Appendix, there exists an H-module isomorphism

$$\phi : P(\Bbbk) \longrightarrow {}_{S^2}P(\Bbbk)$$

such that $\phi^p = \mathrm{id}_{P(\Bbbk)}$. It follows, by [**23**, Lemma 1.3], that $\mathrm{Tr}(\phi) = 0$. In view of [**2**, Lemma 2.6] or Lemma 1.8(b), $\dim P(\Bbbk) = np$ for some positive integer n, but then, by equation (3.3), we have

$$2p^2 = \dim H \geqslant p \dim P(\Bbbk) = np^2,$$

and so $n = 1$ or 2. □

In view of Lemma 3.1 and the beginning remark of this section, we find

$$(\mathrm{ord}(\alpha), \dim P(\Bbbk)) = (2p, 2p), (p, 2p), (2p, p), \text{ or } (p, p). \tag{3.4}$$

The following lemma settles the first three cases.

LEMMA 3.2. *The pair* $(\mathrm{ord}(\alpha), \dim P(\Bbbk)) \neq (2p, 2p)$. *If* $(\mathrm{ord}(\alpha), \dim P(\Bbbk))$ *is equal to either* $(p, 2p)$ *or* $(2p, p)$, *then* H^* *is pointed.*

Proof. Let

$$H_\alpha = \bigoplus_{\beta \in \langle \alpha \rangle} P(\Bbbk_\beta).$$

Then H_α is isomorphic to a left submodule of ${}_H H$, and so $\dim H_\alpha \leqslant \dim H = 2p^2$. By the preceding remark, $\dim H_\alpha = \operatorname{ord}(\alpha) \dim P(\Bbbk)$. Therefore, it is not possible to have $(\operatorname{ord}(\alpha), \dim P(\Bbbk)) = (2p, 2p)$. If $(\operatorname{ord}(\alpha), \dim P(\Bbbk)) = (p, 2p)$ or $(2p, p)$, then $\dim H_\alpha = \dim H$, and hence $H \cong H_\alpha$ as left H-modules. Since all of the simple quotients of H_α are one-dimensional, every simple H-module is one-dimensional. Therefore, H^* is pointed. □

Next we handle the remaining case that $\operatorname{ord}(\alpha) = \dim P(\Bbbk) = p$. Following the terminology in [**5**], an H-module V is called *α-stable* if $\Bbbk_\alpha \otimes V \cong V$. We have two subcases: either there exists an α-stable simple H-module, or all simple H-modules are not α-stable.

Lemma 3.3. *If $\operatorname{ord}(\alpha) = \dim P(\Bbbk) = p$, and all of the simple H-modules are not α-stable, then H^* is pointed.*

Proof. Since $\dim P(\Bbbk) = p = \operatorname{ord}(\alpha)$, it follows, by (3.3), that there exists a simple H-module V such that $[V] \notin O(\Bbbk)$. Since

$$\operatorname{Hom}_H(V^\vee \otimes P(V), \Bbbk) \cong \operatorname{Hom}_H(P(V), V \otimes \Bbbk) \cong \operatorname{Hom}_H(P(V), V)$$

and $\dim \operatorname{Hom}_H(P(V), V) = 1$, we obtain $\dim \operatorname{Hom}_H(V^\vee \otimes P(V), \Bbbk) = 1$. Thus, $P(\Bbbk)$ is a direct summand of $V^\vee \otimes P(V)$. In particular, we have

$$\dim V \dim P(V) = \dim(V^\vee \otimes P(V)) \geqslant \dim P(\Bbbk) = p.$$

Since V is not α-stable, it follows that $|O(V)| = p$, and so (3.3) implies that

$$2p^2 = \dim H \geqslant p \dim P(\Bbbk) + p \dim V \dim P(V) \geqslant 2p^2.$$

Therefore, $\dim V \dim P(V) = p$, which forces $\dim V = 1$ and $\dim P(V) = p$. Thus all simple H-modules are one-dimensional, and so H^* is pointed. □

Lemma 3.4. *If $\operatorname{ord}(g) = \dim P(\Bbbk) = p$, and there exists an α-stable simple H-module, then H is pointed.*

Proof. Assume that V is an α-stable simple H-module. Then $O(V) = \{[V]\}$ and $P(V)$ is also α-stable. By [**23**, Lemma 1.4], both $\dim V$ and $\dim P(V)$ are multiples of p. Let $\dim V = np$ and $\dim P(V) = mp$ for some positive integers $n \leqslant m$. By (3.3), we have the inequality

$$2p^2 = \dim H \geqslant p \dim P(\Bbbk) + \dim V \dim P(V) \geqslant p^2 + nmp^2 = (nm+1)p^2,$$

which implies that $n = m = 1$. Hence $P(V) = V$ and $\operatorname{Irr}(H) = O(\Bbbk) \cup \{[V]\}$ by (3.3). Recall from [**23**, Lemma 1.1] that the socle of $P(\Bbbk)$ is $\Bbbk_{\alpha^{-1}}$. Therefore,

$$\operatorname{Hom}_H(P(V), P(\Bbbk)) = \operatorname{Hom}_H(V, P(\Bbbk)) = 0.$$

Since V is the only simple H-module of dimension greater than 1, all of the composition factors of $P(\Bbbk)$ are one-dimensional. Now let $\mathbf{E}$ be the full subcategory of all $M \in H\text{-}\mathbf{mod}_{\mathrm{fin}}$ whose composition factors are one-dimensional. Thus $\mathbf{E}$ is a proper tensor subcategory of $H\text{-}\mathbf{mod}_{\mathrm{fin}}$ with $P(\Bbbk) \in \mathbf{E}$, and all of the simple objects of $\mathbf{E}$ are one-dimensional. There is a Hopf ideal I of H such that $\mathbf{E}$ is equivalent to $H/I\text{-}\mathbf{mod}_{\mathrm{fin}}$. Since $P(\Bbbk)$ is indecomposable of dimension p, it follows that H/I is not semisimple. Thus, the Hopf algebra H/I is a proper quotient, and it must have dimension p^2 as all other possibilities (being $2, p$, or $2p$) are semisimple Hopf algebras (cf. [**22**, **34**]). It follows, by [**20**], that $H/I \cong T_p$, where T_p is a Taft algebra of dimension p^2. By Proposition 1.3, we have an exact sequence of Hopf algebras as follows:

$$1 \longrightarrow \Bbbk[\mathbb{Z}_2] \longrightarrow H \longrightarrow T_p \longrightarrow 1.$$

Dualizing this sequence, we get the exact sequence as follows:

$$1 \longrightarrow T_p \longrightarrow H^* \longrightarrow \Bbbk[\mathbb{Z}_2] \longrightarrow 1$$

since both T_p and $\Bbbk[\mathbb{Z}_2]$ are self-dual. It is well known that the Jacobson radical J of the Taft algebra T_p is a Hopf ideal, and $T_p/J \cong \Bbbk[\mathbb{Z}_p]$. Applying Proposition 1.7, we find that H contains a semisimple Hopf subalgebra K of dimension $2p$. Since $S^{2p} = \mathrm{id}_H$, Proposition 5.1 in [**2**] implies that K is the coradical of H. It follows immediately by [**1**, Lemma A.2] that H is pointed. □

Combining Lemmas 3.1–3.4, we complete the proof of our main result, Theorem I.

Appendix

The following lemma was used in [**23**, Lemmas 1.4, 2.2]. We believe the result is known but we provide a proof for the sake of completeness.

Lemma A.1. *Let A be an algebra over an algebraically closed field $\Bbbk$ and let σ be a diagonalizable* (*or semisimple*) *algebra automorphism on A. If V is a finite-dimensional A-module that is isomorphic to ${}_\sigma V$, then there exists an isomorphism of A-modules $\phi : V \to {}_\sigma V$ such that ϕ is diagonalizable.*

Proof. Let $\psi : V \to {}_\sigma V$ be an isomorphism of A-modules and let $\rho : A \to \mathrm{End}_\Bbbk(V)$ be the representation of A associated with the A-module V. Then we have

$$\psi \circ \rho(a) = \rho(\sigma(a)) \circ \psi \quad \text{for all } a \in A.$$

Suppose that $a \in A$ is an eigenvector of σ corresponding to the eigenvalue γ such that $\rho(a) \neq 0$. Then we have $C_\psi(\rho(a)) = \gamma\rho(a)$, where $C_\psi : \mathrm{End}_\Bbbk(V) \to \mathrm{End}_\Bbbk(V)$ is defined by $g \mapsto \psi \circ g \circ \psi^{-1}$. In particular, $\rho(a)$ is an eigenvector of C_ψ. If $\psi = \psi_s \circ \psi_u$ is the Jordan–Chevalley decomposition of ψ with ψ_s being the semisimple part and ψ_u the unipotent part of ψ, then C_{ψ_s} is diagonalizable, C_{ψ_u} is unipotent, and $C_\psi = C_{\psi_s} \circ C_{\psi_u}$ is the Jordan–Chevalley decomposition of C_ψ. Thus, $C_{\psi_s}(\rho(a)) = \gamma\rho(a)$ or

$$\psi_s \circ \rho(a) = \rho(\sigma(a)) \circ \psi_s.$$

Since σ is diagonalizable, this equality holds for all $a \in A$. Therefore, ψ_s is our desired isomorphism of A-modules. □

For the purpose of this paper and future development, we need to establish a more general version of a part of the results obtained in [**23**, Lemmas 1.4, 2.2(i)].

Lemma A.2. *Let A be a finite-dimensional algebra over an algebraically closed field $\Bbbk$ of characteristic zero and let σ be an algebra automorphism on A of order n. If V is a finite-dimensional indecomposable A-module that is isomorphic to ${}_\sigma V$, then there exists an isomorphism of A-modules $\phi : V \to {}_\sigma V$ such that $\phi^n = \mathrm{id}_V$.*

Proof. We simply extract the proof from [**23**, Lemma 1.4]. It follows, by Lemma A.1, that there exists a diagonalizable operator ϕ on V such that $\phi(av) = \sigma(a)\phi(v)$ for $a \in A$ and $v \in V$. Thus, ϕ^n is an A-module automorphism on V. Since $\mathrm{End}_A(V)$ is a finite-dimensional local $\mathbb{k}$-algebra, it follows that $\phi^n = c \cdot \mathrm{id}_V$ for some non-zero scalar c. Therefore, if we take $t \in \mathbb{k}$ to be an nth root of c, then $(1/t)\phi$ is a desired A-module isomorphism. □

Acknowledgements. The authors would like to thank Akira Masuoka for his invaluable suggestion on the proof of Proposition 1.7, and Susan Montgomery for her suggestion of several references. The second author also thanks the National Center for Theoretical Sciences in Taiwan, where the present work was carried out, for the generous hospitality, and Ching-Hung Lam for being a wonderful host.

References

1. N. Andruskiewitsch and S. Natale, 'Counting arguments for Hopf algebras of low dimension', *Tsukuba J. Math.* 25 (2001) 187–201. MR 1846876 (2002d:16046).

2. N. Andruskiewitsch and H.-J. Schneider, 'Hopf algebras of order p^2 and braided Hopf algebras of order p', *J. Algebra* 199 (1998) 430–454. MR 1489920 (99c:16033).

3. R. J. Blattner and S. Montgomery, 'Crossed products and Galois extensions of Hopf algebras', *Pacific J. Math.* 137 (1989) 37–54. MR 983327 (90a:16007).

4. P. Etingof and S. Gelaki, 'Semisimple Hopf algebras of dimension pq are trivial', *J. Algebra* 210 (1998) 664–669. MR 1662308 (99k:16079).

5. P. Etingof and S. Gelaki, 'On Hopf algebras of dimension pq', *J. Algebra* 277 (2004) 668–674. MR 2067625 (2005d:16061).

6. D. Fukuda, 'Classification of Hopf algebras of dimension 18', *Israel J. Math.* 168 (2008) 119–123. MR 2448053.

7. G. A. García, 'On Hopf algebras of dimension p^3', *Tsukuba J. Math.* 29 (2005) 259–284. MR 2162840 (2006d:16056).

8. S. Gelaki and S. Westreich, 'On semisimple Hopf algebras of dimension pq', *Proc. Amer. Math. Soc.* 128 (2000) 39–47. MR 2000c:16050.

9. T. Kobayashi and A. Masuoka, 'A result extended from groups to Hopf algebras', *Tsukuba J. Math.* 21 (1997) 55–58. MR 1467221 (98h:16064).

10. R. G. Larson and D. E. Radford, 'Semisimple cosemisimple Hopf algebras', *Amer. J. Math.* 109 (1987) 187–195. MR 89a:16011.

11. R. G. Larson and D. E. Radford, 'Finite-dimensional cosemisimple Hopf algebras in characteristic 0 are semisimple', *J. Algebra* 117 (1988) 267–289. MR 89k:16016.

12. A. Masuoka, 'Semisimple Hopf algebras of dimension $2p$', *Comm. Algebra* 23 (1995) 1931–1940. MR 1323710 (96e:16050).

13. A. Masuoka, 'The p^n theorem for semisimple Hopf algebras', *Proc. Amer. Math. Soc.* 124 (1996) 735–737. MR 1301036 (96f:16046).

14. A. Masuoka, 'Some further classification results on semisimple Hopf algebras', *Comm. Algebra* 24 (1996) 307–329. MR 1370538 (96k:16070).

15. S. Montgomery, *Hopf algebras and their actions on rings*, CBMS Regional Conference Series in Mathematics 82 (Conference Board of the Mathematical Sciences, Washington, DC, 1993). MR 1243637 (94i:16019).

16. S. Montgomery, 'Representation theory of semisimple Hopf algebras', *Algebra – representation theory*, Constanta, 2000, NATO Science Series II: Mathematics, Physics and Chemistry 28 (ed. K. W. Roggenkamp and M. Stefănescu; Kluwer, Dordrecht, 2001) 189–218. MR 1858037 (2002g:16062).

17. S. Natale, 'On semisimple Hopf algebras of dimension pq^2', *J. Algebra* 221 (1999) 242–278. MR 1722912 (2000k:16050).

18. S. Natale, 'Quasitriangular Hopf algebras of dimension pq', *Bull. London Math. Soc.* 34 (2002) 301–307. MR 2003h:16066.

19. S.-H. Ng, 'On the projectivity of module coalgebras', *Proc. Amer. Math. Soc.* 126 (1998) 3191–3198. MR 1469428 (99a:16035).

20. S.-H. Ng, 'Non-semisimple Hopf algebras of dimension p^2', *J. Algebra* 255 (2002) 182–197. MR 1935042 (2003h:16067).

21. S.-H. Ng, 'Hopf algebras of dimension pq', *J. Algebra* 276 (2004) 399–406. MR 2054403 (2005d:16066).

22. S.-H. Ng, 'Hopf algebras of dimension $2p$', *Proc. Amer. Math. Soc.* 133 (2005) 2237–2242 (electronic). MR 2138865 (2006a:16055).

23. S.-H. Ng, 'Hopf algebras of dimension pq. II', *J. Algebra* 319 (2008) 2772–2788. MR 2397407.

24. W. D. Nichols and M. Bettina Zoeller, 'A Hopf algebra freeness theorem', *Amer. J. Math.* 111 (1989) 381–385. MR 987762 (90c:16008).

25. D. E. Radford, 'On a coradical of a finite-dimensional Hopf algebra', *Proc. Amer. Math. Soc.* 53 (1975) 9–15. MR 0396652 (53 #514).
26. D. E. Radford, 'The order of the antipode of a finite dimensional Hopf algebra is finite', *Amer. J. Math.* 98 (1976) 333–355. MR 0407069 (53 #10852).
27. D. E. Radford, 'The structure of Hopf algebras with a projection', *J. Algebra* 92 (1985) 322–347. MR 778452 (86k:16004).
28. D. E. Radford, 'The trace function and Hopf algebras', *J. Algebra* 163 (1994) 583–622. MR 1265853 (95e:16039).
29. H.-J. Schneider, 'Normal basis and transitivity of crossed products for Hopf algebras', *J. Algebra* 152 (1992) 289–312. MR 1194305 (93j:16032).
30. H.-J. Schneider, 'Some remarks on exact sequences of quantum groups', *Comm. Algebra* 21 (1993) 3337–3357. MR 1228767 (94e:17026).
31. Y. Sommerhäuser, 'Yetter-Drinfel'd Hopf algebras over groups of prime order', PhD Thesis, 1999.
32. M. E. Sweedler, *Hopf algebras*, Mathematics Lecture Note Series 44 (W. A. Benjamin, New York, 1969). MR 0252485 (40 #5705).
33. E. J. Taft, 'The order of the antipode of finite-dimensional Hopf algebra', *Proc. Nat. Acad. Sci. USA* 68 (1971) 2631–2633. MR 44 #4075.
34. Y. Zhu, 'Hopf algebras of prime dimension', *Int. Math. Res. Not.* (1994) 53–59. MR 1255253 (94j:16072).

Michael Hilgemann and Siu-Hung Ng
Department of Mathematics
Iowa State University
Ames, IA 50011
USA

hilgem1@iastate.edu
rng@iastate.edu