PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 49, Number 2, June 1975

HOPF ALGEBRAS WITH NONSEMISIMPLE ANTIPODE

EARL J. TAFT[1] AND ROBERT LEE WILSON[2]

ABSTRACT. An example is given to show that the antipode of a finite dimensional Hopf algebra over a field of prime characteristic $p > 2$ need not be semisimple. (For $p = 2$ examples were previously known.) The example is a pointed irreducible Hopf algebra H (with antipode S) of dimension p^3 such that $S^{2p} = I \neq S^2$.

Radford [4] has recently shown that the antipode S of a finite dimensional Hopf algebra H over a field K has finite order. Consequently, if K is of characteristic zero then the antipode of H is semisimple. On the other hand, if K is of characteristic 2 then S is semisimple only if $S = I$. (For otherwise S has even order, say $2k$, and so $0 = S^{2k} - I = (S^k - I)^2$.) In this note we show that S may fail to be semisimple for any characteristic $p \geq 3$. We do this by constructing a pointed irreducible Hopf algebra of dimension p^3 over an arbitrary field of characteristic $p \geq 3$ in which the antipode has order $2p$ (and hence is not semisimple).

A related problem is that of finding a bound for the order of S. In [7] the authors have shown that if H is pointed, if $G(H)$ has exponent e and if $H_0 \subseteq H_1 \subseteq \cdots \subseteq H_m = H$ is the coradical filtration then $(S^{2e} - I)^m = 0$. Thus if K has characteristic p and $p^{n-1} < m \leq p^n$ then $S^{2ep^n} = I$. Thus the order of S divides $2ep^n$. A number of finite dimensional pointed Hopf algebras are known [2], [3], [6] in which the order of the antipode is $2e$. (In one of these, due independently to Radford [3] and Sweedler (described in [2]), $n = 0$ and hence the upper bound $2ep^n$ is actually attained.) The example given here is the first of a pointed Hopf algebra in which the order of S exceeds $2e$ (here $e = 1$). Whether the order of the antipode can actually equal $2ep^n$ when $n \geq 1$ remains an open question.

Presented to the Society, January 17, 1974 under the title *Some finite dimensional pointed Hopf algebras with nonsemisimple antipode*; received by the editors October 25, 1973.

AMS (MOS) subject classifications (1970). Primary 16A24.

[1]This research was partially supported by National Science Foundation grant GP-38518.

[2]This research was partially supported by National Science Foundation grant GP-33226.

1. **Definition of** H. Let K be a field of characteristic $p \geq 3$ and let R denote the free algebra over K on three noncommuting variables X, Y, and Z. Since R is free there is a unique homomorphism $\Delta : R \longrightarrow R \otimes R$ such that

$$\Delta(X) = 1 \otimes X + X \otimes 1, \quad \Delta(Y) = 1 \otimes Y + Y \otimes 1,$$
$$\Delta(Z) = 1 \otimes Z + Z \otimes 1 + X \otimes Y.$$

It is easily checked that $(I \otimes \Delta)\Delta$ and $(\Delta \otimes I)\Delta$ agree on the free generators X, Y, and Z and hence that Δ is coassociative. We define an algebra homomorphism $\epsilon : R \longrightarrow K$ by $\epsilon(X) = \epsilon(Y) = \epsilon(Z) = 0$. It is immediate that $(I \otimes \epsilon)\Delta = (\epsilon \otimes I)\Delta = I$. Hence R is a bialgebra.

Let $\mathcal{J}$ be the ideal in R generated by $[X, Y] - X$, $[Y, Z] + Z$, $[X, Z] - X^2/2$, X^p, $Y^p - Y$, and Z^p.

We wish to show that $\mathcal{J}$ is a bi-ideal, i.e., that $\Delta(\mathcal{J}) \subseteq R \otimes \mathcal{J} + \mathcal{J} \otimes R$ (obviously $\epsilon(\mathcal{J}) = (0)$). It is sufficient to check this on generators for $\mathcal{J}$. For the generators $[X, Y] - X$, X^p, and $Y^p - Y$ the result follows from the fact that in a bialgebra over a field of characteristic p the primitive elements form a restricted Lie algebra. For the remaining generators we compute:

$$\begin{aligned}
\Delta([Y, Z] + Z) &= [\Delta Y, \Delta Z] + \Delta Z \\
&= [1 \otimes Y + Y \otimes 1, 1 \otimes Z + Z \otimes 1 + X \otimes Y] \\
&\quad + 1 \otimes Z + Z \otimes 1 + X \otimes Y \\
&= 1 \otimes [Y, Z] + [Y, Z] \otimes 1 + [Y, X] \otimes Y \\
&\quad + 1 \otimes Z + Z \otimes 1 + X \otimes Y \\
&= 1 \otimes ([Y, Z] + Z) + ([Y, Z] + Z) \otimes 1 - ([X, Y] - X) \otimes Y;
\end{aligned}$$

$$\begin{aligned}
\Delta([X, Z] - X^2/2) &= [\Delta X, \Delta Z] - (\Delta X)^2/2 \\
&= [1 \otimes X + X \otimes 1, 1 \otimes Z + Z \otimes 1 + X \otimes Y] \\
&\quad - (X^2/2) \otimes 1 - X \otimes X - 1 \otimes (X^2/2) \\
&= 1 \otimes [X, Z] + [X, Z] \otimes 1 + X \otimes [X, Y] \\
&\quad - (X^2/2) \otimes 1 - X \otimes X - 1 \otimes (X^2/2) \\
&= 1 \otimes ([X, Z] - (X^2/2)) + X \otimes ([X, Y] - X) \\
&\quad + ([X, Z] - (X^2/2)) \otimes 1;
\end{aligned}$$

$$\Delta(Z^p) = (\Delta Z)^p = (1 \otimes Z + Z \otimes 1 + X \otimes Y)^p.$$

Jacobson [1, formula (63), p. 187] has shown that if a and b are elements of an associative algebra over a field of characteristic p then

$$(a+b)^p = a^p + b^p + \sum_{i=1}^{p-1} s_i \tag{$*$}$$

where is_i is the coefficient of λ^{i-1} in $a(\operatorname{ad}(\lambda a+b))^{p-1}$.

Hence

$$\Delta(Z^p) = (1\otimes Z)^p + (Z\otimes 1 + X\otimes Y)^p + \sum_{i=1}^{p-1} s_i$$

where is_i is the coefficient of λ^{i-1} in

$$(1\otimes Z)(\operatorname{ad}(\lambda(1\otimes Z) + Z\otimes 1 + X\otimes Y))^{p-1}.$$

Now

$$[1\otimes Z,\ \lambda(1\otimes Z) + Z\otimes 1 + X\otimes Y] = X\otimes [Z,\ Y] \equiv X\otimes Z$$

(where all congruences are modulo $\mathfrak{I}\otimes R + R\otimes \mathfrak{I}$). Now since $[X,\ Z]\equiv X^2/2$ (and $[ab,\ c] = a[b,\ c] + [a,\ c]b$ for any elements a, b, and c in an associative algebra) we have $[X^n,\ Z]\equiv (n/2)X^{n+1}$. Hence

$$[X^i\otimes Z,\ \lambda(1\otimes Z) + (Z\otimes 1 + X\otimes Y)] = [X^i,\ Z]\otimes Z + X^{i+1}\otimes [Z,\ Y]$$

$$\equiv ((i+2)/2)X^{i+1}\otimes Z.$$

Thus by induction we see that

$$(1\otimes Z)(\operatorname{ad}(\lambda(1\otimes Z) + Z\otimes 1 + X\otimes Y))^i \equiv ((i+1)!/2^i)X^i\otimes Z$$

and so

$$(1\otimes Z)(\operatorname{ad}(\lambda(1\otimes Z) + Z\otimes 1 + X\otimes Y))^{p-1}\equiv 0.$$

Hence we have

$$\Delta(Z^p)\equiv 1\otimes Z^p + (Z\otimes 1 + X\otimes Y)^p.$$

Using $(*)$ again we see that

$$(Z\otimes 1 + X\otimes Y)^p = (Z\otimes 1)^p + (X\otimes Y)^p + \sum_{i=1}^{p-1} t_i$$

where it_i is the coefficient of λ^{i-1} in

$$(Z\otimes 1)(\operatorname{ad}(\lambda(Z\otimes 1) + X\otimes Y))^{p-1}.$$

Now

$$[Z\otimes 1,\ \lambda(Z\otimes 1) + X\otimes Y] = [Z,\ X]\otimes Y \equiv -\tfrac{1}{2}X^2\otimes Y.$$

Furthermore,

$$[X^i \otimes Y, \lambda(Z \otimes 1) + X \otimes Y] = \lambda[X^i, Z] \otimes Y \equiv (\lambda i/2)X^{i+1} \otimes Y.$$

It follows by induction that $(Z \otimes 1)(\operatorname{ad}(\lambda(Z \otimes 1) + X \otimes Y))^i$ is congruent to a multiple of $X^{i+1} \otimes Z$ and hence that $(Z \otimes 1)(\operatorname{ad}(\lambda(Z \otimes 1) + X \otimes Y))^{p-1} \equiv 0$. Hence $\Delta(Z^p) \equiv 1 \otimes Z^p + Z^p \otimes 1$. This completes the proof that $\mathfrak{J}$ is a bi-ideal.

Let S be the unique antihomomorphism of R such that

$$S(X) = -X, \qquad S(Y) = -Y, \qquad S(Z) = XY - Z.$$

We claim that $S(\mathfrak{J}) \subseteq \mathfrak{J}$. It is sufficient to check this on generators. We do this as follows (where all congruences are modulo $\mathfrak{J}$):

$$S([X, Y] - X) = [S(Y), S(X)] - S(X) = [-Y, -X] + X = -([X, Y] - X);$$

$$\begin{aligned} S([Y, Z] + Z) &= [S(Z), S(Y)] + S(Z) = [XY - Z, -Y] + XY - Z \\ &= -[X, Y]Y - [Y, Z] + XY - Z \equiv -([Y, Z] + Z); \end{aligned}$$

$$\begin{aligned} S([X, Z] - X^2/2) &= [S(Z), S(X)] - S(X)^2/2 = [XY - Z, -X] - X^2/2 \\ &= X[X, Y] + [Z, X] - X^2/2 \equiv -([X, Z] - X^2/2); \end{aligned}$$

$$S(X^p) = (S(X))^p = -X^p;$$

$$S(Y^p - Y) = (S(Y))^p - S(Y) = -(Y^p - Y);$$

$$S(Z^p) = (S(Z))^p = (XY - Z)^p = (XY)^p - Z^p + \sum_{i=1}^{p-1} u_i$$

where iu_i is the coefficient of λ^{i-1} in $(XY)(\operatorname{ad}(\lambda XY - Z))^{p-1}$ (again by $(*)$). Now as $[X, Y] \equiv X$ it is immediate that $(XY)^p \equiv 0$. Also $Z^p \equiv 0$. Now $[X, XY] = X[X, Y] \equiv X^2$ and so $[X^i, XY] \equiv iX^{i+1}$. Also $[X^i, Z] \equiv (i/2)X^{i+1}$. Thus $[X^i, \lambda XY - Z] \equiv i(\lambda - \tfrac{1}{2})X^{i+1}$. Furthermore,

$$\begin{aligned} [(XY/2) - Z, \lambda XY - Z] &= (\lambda - \tfrac{1}{2})[XY, Z] = (\lambda - \tfrac{1}{2})([X, Z]Y + X[Y, Z]) \\ &\equiv (\lambda - \tfrac{1}{2})X((XY/2) - Z). \end{aligned}$$

Thus

$$\begin{aligned} [X^i((XY/2) - Z), \lambda XY - Z] &= [X^i, \lambda XY - Z]((XY/2) - Z) + X^i[(XY/2) - Z, \lambda XY - Z] \\ &\equiv (i + 1)(\lambda - \tfrac{1}{2})X^{i+1}((XY/2) - Z). \end{aligned}$$

Now since $[XY, \lambda XY - Z] = -[XY, Z] \equiv -X((XY/2) - Z)$ it follows by induction that

$$(XY)(\mathrm{ad}(\lambda XY - Z))^i \equiv -\, i!(\lambda - \tfrac{1}{2})^{i-1} X^i((XY/2) - Z)$$

and so

$$(XY)(\mathrm{ad}(\lambda XY - Z))^{p-1} \equiv -(p-1)!(\lambda - \tfrac{1}{2})^{p-2} X^{p-1}((XY/2) - Z)$$

$$\equiv -(\lambda - \tfrac{1}{2})^{p-2} X^{p-1} Z.$$

But then

$$\sum_{i=1}^{p-1} u_i \equiv \left(-\int_0^1 (\lambda - \tfrac{1}{2})^{p-2}\, d\lambda\right) X^{p-1} Z = 0.$$

Hence $S(Z^p) \equiv 0$, as required.

Now let $H = R/\mathfrak{I}$ and let $x = X + \mathfrak{I}$, $y = Y + \mathfrak{I}$, and $z = Z + \mathfrak{I}$. As $\mathfrak{I}$ is a bi-ideal, H is a bialgebra. We denote the coalgebra structure maps in H by Δ and ϵ. Also, since $S(\mathfrak{I}) \subseteq \mathfrak{I}$, S induces an antihomomorphism of H, which we again denote by S. Then $S(x) = -x$, $S(y) = -y$, and $S(z) = xy - z$. We claim that H is a Hopf algebra with antipode S. To verify this we must check that $m(S \otimes I)\Delta = m(I \otimes S)\Delta = \mu\epsilon$ (where m and μ are the algebra structure maps for H). Now it is sufficient to check this on generators for H. For x and y this is immediate, and for z we have

$$m(S \otimes I)\Delta(z) = m(I \otimes S)\Delta(z) = S(z) + z - xy = 0 = \mu\epsilon(z),$$

as required.

2. **A basis for H.** It is clear that H is spanned by $\{x^i y^j z^k \mid 0 \le i, j, k \le p-1\}$. We will now show that this is a basis for H.

Consider the following p by p matrices over K (where E_{ij} denotes the usual matrix unit):

$$A_i = E_{p-i,p}, \qquad 1 \le i \le p-1, \qquad B = \sum_{i=1}^{p} (i+1)E_{ii},$$

and

$$C = \sum_{i=1}^{p-1} ((i+1)/2)E_{i,i+1}.$$

It is easily checked that $[A_i, A_j] = 0$ for $1 \le i, j \le p-1$, $[A_i, B] = iA_i$ for $1 \le i \le p-1$, $[A_i, C] = (i/2)A_{i+1}$ for $1 \le i \le p-2$, $[A_{p-1}, C] = 0$, $[B, C] = -C$, $A_i^p = 0$ for $1 \le i \le p-1$, $B^p = B$, and $C^p = 0$. Thus $\{A_i \mid 1 \le i \le p-1\} \cup \{B\} \cup \{C\}$ forms a basis for a restricted Lie algebra. Denote this algebra by

$\mathfrak{B}$ and its restricted enveloping algebra by $\mathfrak{U}$.

Let $\mathfrak{J}$ denote the linear span of the set $\{A_i - A_1^i \mid 2 \leq i \leq p-1\}$ of elements of $\mathfrak{U}$. It is easily seen that $[\mathfrak{J}, \mathfrak{B}] \subseteq \mathfrak{J}\mathfrak{U}$. (The only nontrivial verifications are

$$\begin{aligned}[A_i - A_1^i, C] &= (i/2)(A_{i+1} - A_1^{i-1}A_2) \\ &= (i/2)((A_{i+1} - A_1^{i+1}) - (A_2 - A_1^2)A_1^{i-1}) \quad \text{for } 2 \leq i < p-1\end{aligned}$$

and

$$[A_{p-1} - A_1^{p-1}, C] = \cdot\tfrac{1}{2}A_1^{p-2}A_2 = \tfrac{1}{2}(A_2 - A_1^2)A_1^{p-2}.)$$

Since $\mathfrak{B}$ generates $\mathfrak{U}$ this shows that $\mathfrak{U}\mathfrak{J}\mathfrak{U} = \mathfrak{J}\mathfrak{U}$. Let $\mathfrak{A} = \mathfrak{U}/(\mathfrak{J}\mathfrak{U})$. Let $A_1 + \mathfrak{J}\mathfrak{U} = a$, $B + \mathfrak{J}\mathfrak{U} = b$, and $C + \mathfrak{J}\mathfrak{U} = c$. Clearly $\{a^i b^j c^k \mid 0 \leq i, j, k \leq p-1\}$ spans $\mathfrak{A}$. We wish to show that this set is linearly independent. To this end assume

$$\sum_{i,j,k} \alpha_{ijk} a^i b^j c^k = 0$$

where $\alpha_{ijk} \in K$. Then

$$\sum_{i,j,k} \alpha_{ijk} A_1^i B^j C^k \in \mathfrak{J}\mathfrak{U}.$$

Since

$$\{A_1^{i_1} \cdots A_{p-1}^{i_{p-1}} B^j C^k \mid 0 \leq i_1, \cdots, i_{p-1}, j, k \leq p-1\}$$

is a basis for $\mathfrak{U}$ it follows that for each j and k, $\sum_i \alpha_{ijk} A_1^i \in \mathfrak{J}\mathfrak{V}$ where $\mathfrak{V}$ is the linear span of

$$\{A_1^{i_1} \cdots A_{p-1}^{i_{p-1}} \mid 0 \leq i_1, \cdots, i_{p-1} \leq p-1\}.$$

Define a homomorphism $\phi: \mathfrak{V} \to \mathfrak{V}$ by

$$\phi(A_1^{i_1} \cdots A_{p-1}^{i_{p-1}}) = A_1^{i_1 + 2i_2 + \cdots + (p-1)i_{p-1}}$$

Note that $\mathfrak{J}$ and hence $\mathfrak{J}\mathfrak{V}$ are contained in ker ϕ. On the other hand $\phi(\sum_i \alpha_{ijk} A_1^i) = \sum_i \alpha_{ijk} A_1^i$. Thus $\sum_i \alpha_{ijk} A_1^i \in \mathfrak{J}\mathfrak{V}$ implies $\sum_i \alpha_{ijk} A_1^i = 0$ so $\alpha_{ijk} = 0$ for all i, j, and k, as required. Thus $\mathfrak{A}$ is of dimension p^3.

Now define a homomorphism $\psi: R \to \mathfrak{A}$ by $\psi(X) = a$, $\psi(Y) = b$, and $\psi(Z) = c$. Then ker $\psi \supseteq \mathfrak{I}$ so ψ induces a homomorphism of H onto $\mathfrak{A}$. Hence dim $H \geq p^3$. Since we already have that $\{x^i y^j z^k \mid 0 \leq i, j, k \leq p-1\}$ spans H this shows that $\{x^i y^j z^k \mid 0 \leq i, j, k \leq p-1\}$ is a basis for H.

3. **Properties of** H. We will now show that H is pointed and irreducible and that the antipode of H has order $2p$.

Lemma 1. *If C is a coalgebra and W is a simple subcoalgebra, then $\bigwedge^n W$ is an irreducible subcoalgebra of C.*

Proof. That $\bigwedge^n W$ is a subcoalgebra follows from Proposition 9.0.0(i) of [5]. We prove irreducibility by induction on n. Since $\bigwedge^1 W = W$ is simple the result holds for $n = 1$. Assume the result for $n - 1$. Let Y be a simple subcoalgebra of $\bigwedge^n W$. Then

$$(0) \neq \Delta Y \subseteq (Y \otimes Y) \cap (C \otimes \textstyle\bigwedge^{n-1} W + W \otimes C)$$

$$\subseteq (Y \otimes Y) \cap (C \otimes \textstyle\bigwedge^{n-1} W + \bigwedge^{n-1} W \otimes C).$$

It then follows that $Y \cap \bigwedge^{n-1} W \neq (0)$ and so, since Y is simple, $Y \subseteq \bigwedge^{n-1} W$. Then by the induction assumption $Y = W$.

Lemma 2. *If M is a bialgebra and W is a subbialgebra then*

$$(\textstyle\bigwedge^m W)(\bigwedge^n W) \subseteq \bigwedge^{m+n-1} W$$

for all m and $n \geq 1$.

Proof. Since multiplication is a coalgebra map this follows from Lemmas 9.1.3 and 9.2.1 of [5].

Corollary. *H is a pointed irreducible Hopf algebra.*

Proof. Take $W = K$. Then W is a subbialgebra and a simple coalgebra. Now x and $y \in \bigwedge^2 W$ and $z \in \bigwedge^3 W$. Then since $\{x, y, z\}$ generates H, Lemma 2 shows that $H = \bigwedge^n W$ for some n. Hence by Lemma 1 H is irreducible (and is pointed since W is pointed). We have already shown that H is a Hopf algebra with antipode S (although we could have avoided doing this, since by Theorem 9.2.2 of [5] every irreducible bialgebra is a Hopf algebra).

It remains only to determine the order of S. Now

$$S^2(z) = S(y)S(x) - S(z) = yx - xy + z = [y, x] + z = z - x.$$

Then $S^{2i}(z) = z - ix$ for all i. Hence S has order $2p$.

We summarize our results in the following

Proposition. *H is a pointed irreducible Hopf algebra of dimension p^3. The antipode of H has order $2p$.*

4. **A property of** H^*. Let J be the ideal of H generated by x and z. Then J is a nilpotent ideal in H. (For when a monomial is straightened its

total degree in x and z is preserved.) The quotient H/J has basis $\{y^j + J \mid 0 \leq j \leq p-1\}$ and is hence isomorphic to $K[t]/(t^p - t)$, i.e., it is isomorphic to a direct product of p copies of K. It follows that $J = \text{Rad } H$, that H^* is pointed, and that $G(H^*)$ has order p. Thus order of S^* = order of S = $2p$ = 2(exponent of $G(H^*)$).

Whether or not there exists a finite dimensional pointed Hopf algebra H with H^* pointed, order $S >$ 2(exponent of $G(H)$), and order $S >$ 2(exponent of $G(H^*)$) remains an open question.

REFERENCES

1. N. Jacobson, *Lie algebras*, Interscience Tracts in Pure and Appl. Math., no. 10, Interscience, New York, 1962. MR 26 #1345.

2. R. G. Larson, *Orders in Hopf algebras*, J. Algebra 22 (1972), 201–210. MR 45 #8706.

3. D. E. Radford, *A free rank 4 Hopf algebra with antipode of order 4*, Proc. Amer. Math. Soc. 30 (1971), 55–58. MR 43 #4887.

4. ———, *The order of the antipode of a finite dimensional Hopf algebra is finite*, Amer. J. Math. (to appear).

5. M. E. Sweedler, *Hopf algebras*, Math. Lecture Notes Series, Benjamin, New York, 1969. MR 40 #5705.

6. E. J. Taft, *The order of the antipode of finite-dimensional Hopf algebra*, Proc. Nat. Acad. Sci. U.S.A. 68 (1971), 2631–2633. MR 44 #4075.

7. E. J. Taft and R. L. Wilson, *On antipodes in pointed Hopf algebras*, J. Algebra 29 (1974), 27–32.

SCHOOL OF MATHEMATICS, INSTITUTE FOR ADVANCED STUDY, PRINCETON, NEW JERSEY 08540

DEPARTMENT OF MATHEMATICS, RUTGERS UNIVERSITY, NEW BRUNSWICK, NEW JERSEY 08903 (Current address of both authors)