On the Antipode of a Cosemisimple Hopf Algebra

DAVID E. RADFORD*

Department of Mathematics, Statistics, and Computer Science, University of Illinois at Chicago, Chicago, Illinois 60680

Communicated by Barbara L. Osofsky

Received October 18, 1982

0. INTRODUCTION

Let $A$ be a cosemisimple Hopf algebra over a field $k$ with antipode $s$. A general theoretical question which has remained virtually unsolved is whether or not $s^2 = I$. Suppose further that $A$ is finite-dimensional, and if $k$ has characteristic $p > 0$ then $p > 4 \dim A$. Larson has shown recently [4] that if all simple subcoalgebras $C \subseteq A$ have dimension $\leq 8$ then $s^2 = I$. His proof reduces to the algebraically closed case where the assumption on characteristic means $s^2$ is diagonalizable.

Here we generalize his result. The theorem of this paper is the following. Let $A$ be a cosemisimple Hopf algebra over a field $k$ with antipode $s$. If $s^2$ is diagonalizable and $A$ is generated by its subcoalgebras $C \subseteq A$ of dimension $\leq 8$, then $s$ has order 1, 2, or $\infty$. The proof eventually comes down to the main calculation of [4].

Suppose $A$ is any cosemisimple Hopf algebra over a field $k$ with antipode $s$. Then $T(C) \subseteq C$ for any subcoalgebra $C \subseteq A$ where $T = s^2$. Based on this observation, in Section 2 we are motivated to construct for any coalgebra $C$ over $k$ with endomorphism $T: C \to C$ a Hopf algebra $H_k(C, T)$ with canonical coalgebra map $i: C \to H_k(C, T)$ such that $T$ is realized as the square of the antipode $S$ of $H_k(C, T)$ on $i(C)$ in the sense that $i \circ T = S^2 \circ i$. The pair $(H_k(C, T), i)$ is universal with respect to this property. We study $H_k(C, T)$ in cases relevant to the theorem of this paper to derive relations used in its proof in Section 3. In Section 4 we show that if there exists $\rho \in k$ transcendental over the prime field of $k$ then there is a coalgebra automorphism $T$ of $C = M_2(k)^*$ (dual of $2 \times 2$ matrices) such that $H_k(C, T)$ is cosemisimple, and the antipode $S$ has the property that $S^2$ is diagonalizable and $S$ has infinite order. Thus the possible orders for $S$ described in the theorem cited above are realized.

* Research partially supported by National Science Foundation Grant MCS-8201481.

0021-8693/84 $3.00

Copyright © 1984 by Academic Press, Inc.
All rights of reproduction in any form reserved.
Throughout this paper \( k \) will be a field and \( k^* \) will denote the units of \( k \). We will freely follow the notation and conventions of [5].

1. Preliminaries

Let \( V \) be a vector space over a field \( k \) and suppose \( T: V \rightarrow V \) is linear. For \( \lambda \in k \) let \( V_{(\lambda)} \subseteq V \) be the subspace of eigenvectors belonging to \( \lambda \). \( T \) is diagonalizable if \( V = \bigoplus_{\lambda} V_{(\lambda)} \). Now suppose \( C = V \) is a coalgebra and \( T \) is a coalgebra map. Then \( \varepsilon \circ T = \varepsilon \) means \( \varepsilon(C_{(\lambda)}) = (0) \) if \( \lambda \neq 1 \). Assume \( M \subseteq C \) is a left (or right) coideal. Then \( \varepsilon(M) = (0) \) means \( M = (0) \), so if \( T \) is diagonalizable and \( T(M) \subseteq M \), then \( M_{(1)} = (0) \) implies \( M = (0) \). The Hopf algebras \( A \) in this paper will have the property that \( T = s^* \) is diagonalizable, where \( s \) is the antipode of \( A \).

**Lemma 1.** Let \( A \) be a coalgebra over a field \( k \), and suppose \( M \) is a left (respectively right) \( A \)-comodule. Assume \( m_1, \ldots, m_n \) is a basis for \( M \), and define \( e_{ij} \)'s \( \in A \) by \( \omega(m_i) = \sum_j e_{ij} \otimes m_j \) (respectively \( \omega(m_i) = \sum_j m_j \otimes e_{ji} \)).

(a) \( \Delta e_{ij} = \sum_k e_{ik} \otimes e_{kj} \) and \( \varepsilon(e_{ij}) = \delta_{ij} \) for \( 1 \leq i, j \leq n \).

Now suppose \( M \subseteq A \) is a left (respectively right) coideal.

(b) If \( \varepsilon(m_i) = \delta_{ij} \) for \( 1 \leq i \leq n \) (respectively \( \varepsilon(m_j) = \delta_{ij} \) for \( 1 \leq j \leq n \)) then \( m_i = e_{ij} \) for \( 1 \leq i \leq n \) (respectively \( m_j = e_{ij} \) for \( 1 \leq j \leq n \)).

(c) Suppose \( T: A \rightarrow A \) is a coalgebra map and \( T(m_i) = \lambda_i m_i \), \( T(m_n) = \lambda_n m_n \), where \( \lambda_1, \ldots, \lambda_n \in k^* \). Then \( T(e_{ij}) = \lambda_i \lambda_j^{-1} e_{ij} \) (respectively \( T(e_{ij}) = \lambda_i^{-1} \lambda_j e_{ij} \)) for \( 1 \leq i, j \leq n \).

(d) Assume \( A \) is a Hopf algebra with antipode \( s \) and \( s^2(M) \subseteq M \). If \( x \in A \) then \( xM = (0) \) (respectively \( Mx = (0) \)) implies \( x = 0 \).

**Proof.** We assume \( M \) is a left comodule. The parenthetical parts are left to the reader.

(a) follows by \( \sum_j \Delta e_{ij} \otimes m_j = \sum_j e_{ij} \otimes \omega(m_j) = \sum_{j,k} e_{ij} \otimes e_{jk} \otimes m_k \) and \( m_i = \sum_j \varepsilon(e_{ij}) m_j \). To see (b) note \( m_i = \sum_j e_{ij} \varepsilon(m_j) \) also. For (c) observe that

\[
\lambda_i \Delta m_i = \Delta T(m_i) = \sum_j T(e_{ij}) \otimes T(m_j) = \sum_j T(e_{ij}) \otimes \lambda_j m_j
\]

so \( \Delta m_i = \sum_j \lambda_j^{-1} \lambda_j T(e_{ij}) \otimes m_j \) as well.

(d) \( \varepsilon(m) = 1 \) for some \( m \in M \), so \( 1 = \sum_m s(m) \in As(M) \). Thus \( 1 \in s^2(M)s(A) \) means \( 1 \in MA \) by assumption. From this \( xM = (0) \) implies \( x = 0 \).

Q.E.D.

Of central importance to the study of the Hopf algebras in this paper is the nature of certain integral combinations \( r_i^{(n)}(\rho) \) of \( \ldots, \rho^{-2}, \rho^{-1}, 1, \rho, \rho^2, \ldots \) where \( \rho \in k^* \). Their definition can be made in a relatively simple way.
Let \( k \) be any field and fix \( \rho \in k^* \). Let \( \mathcal{O} \) be the \( k \)-algebra generated by \( a_1, a_2, b_1, b_2 \) subject to the relations

\begin{align*}
a_2 b_2 &= \rho a_1 b_1, \\
b_2 a_2 &= \rho^{-1} b_1 a_1.
\end{align*}

From the equations \((a_2 b_2) a_1 = a_2(b_2 a_1)\) and \((b_2 a_2) b_1 = b_2(a_2 b_1)\) we deduce the relations

\begin{align*}
a_2 b_1 a_1 &= \rho^2 a_1 b_1 a_2, \\
b_2 a_1 b_1 &= \rho^{-2} b_1 a_1 b_2.
\end{align*}

The equations \((a_2 b_2) a_1 b_1 = a_2(b_2 a_1 b_1)\) and \((b_2 a_2) b_1 a_1 = b_2(a_2 b_1 a_1)\) yield no new relations, so by [1, Theorem 1.2].

1.1. The monomials in the \( a_i \)'s and \( b_i \)'s which do not contain one of \( a_2 b_2, a_2 b_1 a_1 \) or \( b_2 a_2, b_2 a_1 b_1 \) form a linear basis for \( \mathcal{O} \).

We refer to a monomial described in 1.1 as irreducible. An alternating monomial is one containing no product \( a_i a_j \) or \( b_i b_j \) for \( 1 \leq i, j \leq 2 \). Let \( m = a_{i_1} b_{i_2} \ldots \) be an alternating irreducible monomial beginning with \( a_1 \) or \( a_2 \). If \( i_j = 2 \) for some \( j \), then the subscripts starting with \( i_j \) must alternate. Thus for \( n \geq 1 \) there are \( n + 1 \) such monomials of length \( n \) which we denote \( e_0^{(n)}, \ldots, e_n^{(n)} \), where \( e_i^{(n)} \) (\( 1 \leq i \leq n \)) is the one having left-hand most subscript 2 in position \( i \) (counting from right to left). Thus

\begin{align*}
e_n^{(n)} &= a_2 b_1 a_2 \cdot \\
e_{n-1}^{(n)} &= a_1 b_2 a_1 \cdot \\
e_{n-2}^{(n)} &= a_1 b_1 a_2 \cdot \\
&\vdots \\
e_0^{(n)} &= a_1 b_1 a_1 \cdot \quad \text{(no subscript is 2)}.
\end{align*}

Let \( m = a_{i_1} b_{i_2} \cdot \ldots \) be an alternating monomial of length \( n \) starting with \( a_1 \) or \( a_2 \). Then (1)–(4) imply \( m = \rho^l e_i^{(n)} \) for some \( 0 \leq i \leq n \) and \( l \in \mathbb{Z} \). Define \( r_i^{(n)}(\rho) \) for \( 0 \leq i \leq n \) by the equation

\[
\sum_{1 \leq i_1, \ldots, i_n \leq 2} a_{i_1} b_{i_2} \cdot \ldots = \sum_{i=0}^{n} r_i^{(n)}(\rho) e_i^{(n)}
\]
where the left-hand sum runs over all alternating monomials of length \( n \) beginning with \( a_1 \) or \( a_2 \).

Observe that

\[
a_2b_2a_1 = \rho^2a_1b_2a_2 \quad \text{and} \quad b_2a_1b_1 = \rho^{-2}b_1a_1b_2 \quad \text{for } i = 1, 2. \tag{5}
\]

We record some of the elementary properties of the \( r_i^{(n)}(\rho) \)'s.

1.2. (a) For \( 0 \leq i \leq n \), \( r_i^{(n)}(\rho) \) is a finite integral combination of \( \ldots, \rho^{-2}, \rho^{-1}, 1, \rho, \rho^2, \ldots \). More specifically \( r_i^{(n)}(\rho) = \sum_{d \leq d} z_d \rho^d \) for some \( d \in \mathbb{Z} \), where \( z_d \) is a nonnegative integer and \( z_d = 1 \).

(b) \( r_n^{(n)}(\rho) = 1 \).

(c) If \( n \geq 2 \) then \( r_{n-2}^{(n)}(\rho) = 1 + \rho + \cdots + \rho^{n-1} \).

Proof: Let \( m = a_i b_j \cdot \ldots \cdot \) be an alternating monomial of length \( n \) starting with \( a_1 \) or \( a_2 \). It is useful to conceptualize \( m \) as

\[
\begin{align*}
a_{i_1} & \quad a_{i_2} & \quad \cdots & \quad a_{i_t} \\
b_{j_1} & \quad b_{j_2} & \quad \cdots & \quad b_{j_t}
\end{align*}
\]

if \( n = 2s \) is even,

or

\[
\begin{align*}
a_{i_1} & \quad a_{i_2} & \quad \cdots & \quad a_{i_{j_t+1}} \\
b_{j_1} & \quad b_{j_2} & \quad \cdots & \quad b_{j_t}
\end{align*}
\]

if \( n = 2s + 1 \) is odd,

and to initially reduce the strings \( a_1a_2 \cdot \ldots \cdot \) and \( b_1b_2 \cdot \ldots \cdot \) separately using the reductions \( a_2a_1 = \rho^2a_1a_2 \) and \( b_2b_1 = \rho^{-2}b_1b_2 \) derived from (5).

(a) That \( r_i^{(n)}(\rho) \) is a finite integral combination of \( \ldots, \rho^{-2}, \rho^{-1}, 1, \rho, \rho^2, \ldots \) with non-negative coefficients has been established. We may assume \( \rho \) is transcendental over the prime field of \( k \). We may suppose \( n \geq 2 \).

Let \( m = a_i b_j \cdot \ldots \cdot \) be an alternating monomial such that \( m = \rho^d e_i^{(n)} \). First observe that \( a_1a_2 \) does not appear in the string \( a_1a_2 \cdot \ldots \cdot \). For if so, the rule \( a_2a_1 = \rho^2a_1a_2 \) means there is an alternating monomial \( m' \) such that \( m' = \rho^2m \). Likewise \( b_2b_1 \) does not appear in \( b_1b_2 \cdot \ldots \cdot \). Thus the \( a_i \)'s (if any) in \( a_1a_2 \cdot \ldots \cdot \) appear in a block starting at the left of the string, and the \( b_j \)'s (if any) in \( b_1b_2 \cdot \ldots \cdot \) appear in a block ending at the right of the string. The proof of (a) comes down to the fact that for integers \( p, q, \) and \( r \), the quadratic \( f(x) = 2x(p - x) + (2q + 1)x + r \) attains its maximum on any given finite set of integers exactly once. Indeed if \( x_1 < x_2 \) are integers, then \( f(x_1) \neq f(x_2) \) since the solution \( x = \frac{1}{2}(p + q + 1) \) to \( f'(x) = 0 \) is not the average of two integers.
Let \( x \) be the number of \( a_i \)'s in \( a_i, a_{i_1}, \ldots \) and \( y \) be the number of \( b_j \)'s in \( b_j, b_{j_1}, \ldots \). We represent \( m \) schematically by the configuration:

\[
\begin{array}{c}
\overline{x} \\
\overline{a_i \text{'s}} \\
\overline{a_i \text{'s}} \\
\overline{y} \\
\overline{b_j \text{'s}} \\
\overline{b_{j_1} \text{'s}}
\end{array}
\]

**Case 1.** \( y \geq x \). We reduce to \( e_i^{(n)} \) in two operations as depicted below.

![Diagram](image)

First shift the block of \( a_i \)'s \( s - y \) units to the right, according to (5), and then use (1). Thus \( m = \rho^{2x(5-y)}p^x e_i^{(n)} \). Clearly \( y \geq x \) is true for all \( m \) reducing to \( e_i^{(n)} \), and \( y - x = e \) is the number of \( b_j \)'s in \( e_i^{(n)} \). Since \( f(x) = 2x(s - y) + x = 2x(s - e - x) + x \) assumes its maximum once on the possible \( x \)'s, (a) is proved in this case.

**Case 2.** \( y < x \). We reduce to \( e_i^{(n)} \) in three operations:

![Diagram](image)

where \( t = s \) and \( u = x - y \) if \( n \) is even, \( t = s + 1 \) and \( u = x - 1 - y \) if \( n \) is odd. Clearly \( y < x \) holds for all \( m \) reducing to \( e_i^{(n)} \), and \( x - y = e \) is the number of \( a_i \)'s in \( e_i^{(n)} \). Thus \( m = \rho^{2x(t-x)}p^y p^{2uy} e_i^{(n)} \). Since \( u \) does not depend on \( x \), we see \( f(x) = 2x(t - x) + y + 2uy = 2x(t - x) + (2u + 1)y = 2x(t - x) + (2u + 1)x - (2u + 1)e \) assumes its maximum once on the possible \( x \)'s, so (a) is proved in this case.

(b) Is straightforward.

(c) Let \( m = a_{i_1}, b_{j_1}, \ldots \) reduce to \( e_{n-2}^{(n)} \). Then \( m \) has form (A), \( i_1 = \cdots = \)
\[ i_j = 2 (= i_{j+1} \text{ if } n \text{ is odd}), \text{ and } j_k = 2 \text{ for exactly one } 1 \leq k \leq s, \text{ or } m \text{ has form (B), } j_1 = \cdots = j_s = 1 \text{ and } i_k = 1 \text{ for exactly one } k. \]

If \( m \) has form (A), then moving \( b_2 \) to the left and applying (1) yields \( m = \rho^{2(k-1)} \rho e_{n-2}^{(n)} \). If \( m \) has form (B) then moving \( a_1 \) to the left yields \( m = \rho^{2(k-1)} \rho e_{n-2}^{(n)} \). Thus if \( n \) is even \( r_1^{(n)}(\rho) = \sum_{k=1}^{s} \rho^{2(k-1)} + \sum_{k=1}^{s} \rho^{2(k-1)} \), and if \( n \) is odd \( r_1^{(n)}(\rho) = \sum_{k=1}^{s} \rho^{2(k-1)} + \sum_{k=1}^{s} \rho^{2(k-1)} \), so (c) follows. Q.E.D.

We will show in the next section that if \( \rho \) is a primitive \( n \)th root of unity \( (n \geq 2) \) then \( r_0^{(n)}(\rho) = \cdots = r_{n-2}^{(n)}(\rho) = 0 \). If \( n \) is even the proof is elementary—it is not so evident when \( n \) is odd. The proof of the theorem of this paper rests essentially on the vanishing of the \( r_i^{(n)}(\rho) \)'s for \( 0 \leq i \leq n-2 \).

2. The Free Hopf Algebra on a Coalgebra Endomorphism

Let \( A \) be a cosemisimple Hopf algebra over a field \( k \) with antipode \( s \). Then \( s^2(C) = C \) for all subcoalgebras \( C \subseteq A \). This observation motivates the construction of a Hopf algebra \( H_k(C, T) \) with canonical map \( i: C \rightarrow H_k(C, T) \), where \( T: C \rightarrow C \) is any coalgebra endomorphism, such that \( T \) is the square of the antipode \( S \) of \( H_k(C, T) \) on \( C \) in the sense that \( i \circ T = S^2 \circ i \). The pair \((H_k(C, T), i)\) is universal with respect to this property. The construction is based on:

**Lemma 2 (The Free Hopf Algebra on a Coalgebra Antiendomorphism).** Let \( C \) be a coalgebra over a field \( k \), and suppose \( \phi: C \rightarrow C \) is a coalgebra antiendomorphism. There exists a pair \((H_k(C, \phi), i)\) satisfying the following properties: (1) \( H_k(C, \phi) \) is a Hopf algebra over \( k \) with antipode \( S \) and \( i: C \rightarrow H_k(C, \phi) \) is a coalgebra map such that \( i \circ \phi = S \circ i \), and (2) if \( A \) is a Hopf algebra over \( k \) with antipode \( s \) and \( f: C \rightarrow A \) is a coalgebra map satisfying \( f \circ \phi = s \circ f \), then there is a unique Hopf algebra map \( F: H_k(C, \phi) \rightarrow A \) making the diagram

\[
\begin{array}{ccc}
H_k(C, \phi) & \xrightarrow{i} & C \\
\downarrow{\phi} & & \downarrow{f} \\
C & \xrightarrow{f} & A
\end{array}
\]

commute.

**Proof.** The coalgebra structure on \( C \) extends uniquely to a bialgebra structure on the tensor algebra \( T(C) \) of the space \( C \), and \( \phi \) extends to a
unique algebra antiendomorphism \( \mathcal{S} : T(C) \to T(C) \) which is necessarily a coalgebra antiendomorphism as well. Let \( I \subseteq T(C) \) be the ideal generated by the elements of the form \( \sum c_{(1)} \delta(c_{(2)}) - \varepsilon(c)1 \) and \( \sum \delta(c_{(1)}) c_{(2)} - \varepsilon(c)1 \) for \( c \in C \). Since \( C \) is a subcoalgebra of \( T(C) \) it follows \( I \) is a bideal, and \( \delta(C) \subseteq C \) means \( \mathcal{S}(I) \subseteq I \). Since \( C \) generates \( T(C) \) the quotient \( H_k(C, \delta) = T(C)/I \) is a Hopf algebra with antipode \( S \) induced by \( \mathcal{S} \). Note \( i : C \to H_k(C, \delta) \) (\( c \mapsto c + I \)) defines a coalgebra map where \( i \circ \delta = S \circ i \). Noting that a bialgebra map of Hopf algebras is automatically a Hopf algebra map [5, Lemma 4.0.41], the reader can easily see the mapping property holds.

Q.E.D.

The free Hopf algebra on a coalgebra antiendomorphism has been used often informally. Note \( \delta \) is the antipode of \( H_k(C, \delta) \) on \( C \) in the sense that \( i \circ \delta = S \circ i \).

**Proposition 1 (The Free Hopf Algebra on a Coalgebra Endomorphism).** Let \( C \) be a coalgebra over a field \( k \), and suppose \( T : C \to C \) is a coalgebra endomorphism. There exists a pair \( (H_k(C, T), i) \) satisfying the following properties: (1) \( H_k(C, T) \) is a Hopf algebra over \( k \) with antipode \( S \) and \( i : C \to H_k(C, T) \) is a coalgebra map such that \( i \circ T = S^2 \circ i \), and (2) if \( A \) is a Hopf algebra over \( k \) with antipode \( s \) and \( f : C \to A \) is a coalgebra map such that \( f \circ T = s^2 \circ f \), there is a unique Hopf algebra map \( F : H_k(C, T) \to A \) making the diagram

\[
\begin{array}{ccc}
C & \xrightarrow{f} & A \\
\downarrow{i} & & \downarrow{f} \\
H_k(C, T) & \xrightarrow{S^2 \circ i} & A \\
\end{array}
\]

commute.

**Proof.** We construct a coalgebra \( \mathcal{E} = C \oplus \delta(C) \) where \( \delta : \mathcal{E} \to \mathcal{E} \) is a coalgebra antiendomorphism such that \( \delta|_C : C \to \delta(C) \) is bijective and \( \delta^2(c) = T(c) \) for \( c \in C \). This is done by setting \( \mathcal{E} = C \oplus C^{op} \) and defining \( \delta \) by \( (c, 0) \mapsto (0, c) \) and \( (0, c) \mapsto (T(c), 0) \) for \( c \in C \). Set \( H_k(C, T) = H_k(\mathcal{E}, \delta) \) and let \( i = f|_C \), where \( (H_k(C, \delta), f) \) is the free Hopf algebra on \( \delta \).

Suppose \( A \) is a Hopf algebra over \( k \) with antipode \( s \) and \( f : C \to A \) is a coalgebra map satisfying \( f \circ T = s^2 \circ f \). Extend \( f \) to a coalgebra map \( f : \mathcal{E} \to A \) by \( f(\delta(c)) = s \circ f(c) \) for \( c \in C \). Now since \( f \circ \delta(\delta(c)) = f \circ T(c) = s^2 \circ f(c) = s \circ f(\delta(c)) \), it follows \( f \circ \delta = s \circ f \). Thus \( F \) exists by the previous
lemma. To show uniqueness note that the subcoalgebra \( i(C) \) generates \( H_k(\mathcal{C}, \delta) \) as a Hopf algebra. Q.E.D.

Let \( k \) be a field and \( n \geq 1 \). Let \( C \) be the coalgebra over \( k \) with basis \( \{a_{ij}\}_{1 \leq i,j \leq n} \) whose structure is determined by \( \Delta a_{ij} = \sum a_{ik} \otimes a_{kj} \). For \( \lambda_1, \ldots, \lambda_n \in k^* \) the linear automorphism \( T: C \to C \) defined by \( T(a_{ij}) = \lambda_i \lambda_j^{-1} a_{ij} \) is a coalgebra map. The presentation of \( H_k(C, T) \) is rather explicit. Writing \( b_{ij} = \sigma(a_{ij}) \) (hence \( \sigma(b_{ij}) = \sigma^2(a_{ij}) = T(a_{ij}) = \lambda_{ij} a_{ij} \), where \( \lambda_{ij} = \lambda_i \lambda_j^{-1} \)) we see that \( H_k(C, T) \) is the \( k \)-algebra on the set of symbols \( X = \{a_{ij}, b_{ij}; 1 \leq i, j \leq n\} \) subject to the relations

\[
\begin{align*}
(r.1) & \quad \sum_k a_{ik} b_{kj} = \delta_{ij} 1 \\
(r.2) & \quad \sum_k b_{ki} a_{kj} = \delta_{ij} 1 \\
(r.3) & \quad \sum_k b_{ik} (\lambda_{jk} a_{jk}) = \delta_{ij} 1 \\
(r.4) & \quad \sum_k (\lambda_{ki} a_{ki}) b_{kj} = \delta_{ij} 1 \
\end{align*}
\]

(the translation of \( \sum a_{ij} \sigma(a_{ij}) = \varepsilon(a) 1 \) and \( \sum \sigma(a_{ij}) a_{ij} = \varepsilon(a) 1 \) for \( a = a_{ij} \) and \( a = b_{ij} \)) with coalgebra structure determined by \( \Delta a_{ij} = \sum_k a_{ik} \otimes a_{kj} \) and \( \Delta b_{ij} = \sum_k b_{ik} \otimes b_{kj} \).

There is a great deal of formal redundancy in these relations, and we shall exploit this.

2.1. (a) (Reversing subscripts) Let \( A_{ij} = a_{ij} \) and \( B_{ij} = \lambda_{ij} b_{ij} \). Then

\[
\begin{align*}
(1) & \quad \sum_k (\lambda_{ki} A_{ki}) B_{kj} = \delta_{ij} 1 \\
(2) & \quad \sum_k B_{ki} (\lambda_{jk} A_{jk}) = \delta_{ij} 1 \\
(3) & \quad \sum_k B_{ki} A_{kj} = \delta_{ij} 1 \\
(4) & \quad \sum_k A_{ik} B_{kj} = \delta_{ij} 1.
\end{align*}
\]

(b) (Exchanging \( a \)'s and \( b \)'s) Let \( A_{ij} = b_{ij} \) and \( B_{ij} = \lambda_{ij} a_{ij} \). Then

\[
\begin{align*}
(1) & \quad \sum_k B_{ik} (\lambda_{jk} A_{jk}) = \delta_{ij} 1 \\
(2) & \quad \sum_k (\lambda_{ki} A_{ki}) B_{kj} = \delta_{ij} 1 \\
(3) & \quad \sum_k A_{ik} B_{kj} = \delta_{ij} 1 \\
(4) & \quad \sum_k B_{ki} A_{kj} = \delta_{ij} 1.
\end{align*}
\]

To prove 2.1(a) multiply (r.1) and (r.2) by \( \lambda_{ji} \), and (r.3) and (r.4) by \( \lambda_{ij} \), noting \( \lambda_{uu} = 1 \) and \( \lambda_{uv} \lambda_{uw} = \lambda_{uw} \lambda_{uv} \) for \( 1 \leq u, v, w \leq n \). Similarly for 2.1(b), multiply (r.1) and (r.2) by \( \lambda_{ij} \).

Note that the relations of 2.1(a) are formally (r.1)–(r.4), and those of 2.1(b) are formally (r.1)–(r.4) with \( \lambda_i \) replaced by \( \lambda_i^{-1} \) for all \( i \).

Well-order \( X = \{a_{ij}, b_{ij}; 1 \leq i, j \leq n\} \) by setting \( a_{ij} < a_{i'j'} \) (and \( b_{ij} < b_{i'j'} \)) if \( i < i' \), or \( i = i' \) and \( j < j' \), and set \( a_{ij} < b_{ij} \) for all \( 1 \leq i, i', j, j' \leq n \). Let \( \langle X \rangle \) be the free semigroup generated by \( X \), and let \( x_1, \ldots, x_s, x'_1, \ldots, x'_{s'} \in \langle X \rangle \). Then \( x_1 \cdots x_s < x'_1 \cdots x'_{s'} \) if \( s < s' \), or \( s = s' \) and \( x_1 = x'_1, \ldots, x_{l-1} = x'_{l-1}, \ldots, x_s > x'_s \).
$x_i < x'_i$ for some $1 < i < s$, determines a well order $\leq$ on the monomials $m \in \langle X \rangle$, $m \neq 1$. Let 1 be the smallest member of $\langle X \rangle$. The well-ordering $\leq$ is a semigroup ordering—meaning if $A$, $B$, $B'$, $C \in \langle X \rangle$ and $B < B'$ then $ABC < AB'C$.

We rewrite (r.1)–(r.4) in the form $W = f$ (a substitution rule), where $W \in \langle X \rangle$ is a monomial and $f$ is a linear combination of monomials $m < W$, and also classify these relations into types.

(R.1) $a_{in}b_{jn} = \delta_{ij}1 - \sum_{k<n} a_{ik}b_{jk}$ (type $a_n b_{n-}$)

(R.2) $b_{nl}a_{nj} = \delta_{ij}1 - \sum_{k<n} b_{ki}a_{kj}$ (type $b_n a_{n-}$)

(R.3) $b_{ln}a_{jn} = \lambda_{nl}\delta_{ij}1 - \sum_{k<n} b_{ik}(\lambda_{nk}a_{jk})$ (type $b_{n-} a_n$)

(R.4) $a_{nl}b_{nj} = \lambda_{ln}\delta_{ij}1 - \sum_{k<n} (\lambda_{kn}a_{ki})b_{kj}$ (type $a_{n-} b_n$).

Observe that $\lambda_{ij} = \lambda_i\lambda_j^{-1} = (\lambda_i\lambda_{i_0}^{-1})(\lambda_j\lambda_{j_0}^{-1})^{-1}$, so without loss of generality we can assume $\lambda_{i_0} = 1$ for any choice of $i_0$ for convenience.

**Proposition 2.** Let $k$ be any field and $C$ be the coalgebra over $k$ with basis $\{a_{ij}\}_{1 \leq i, j \leq n}$ whose structure is determined by $\Delta a_{ij} = \sum k a_{ik} \otimes a_{kj}$. Let $\lambda_1, ..., \lambda_n \in k^*$ and let $T: C \rightarrow C$ be the coalgebra automorphism defined by $T(a_{ij}) = \lambda_i\lambda_j^{-1}a_{ij}$. Then a linear basis for $H_k(C, T)$ consists of the monomials in the $a_{ij}$'s and $b_{ji} = S(a_{ij})$'s containing no term of the form: $a_{n-}b_{n-}$, $a_{n-}b_{n-1}a_{n-1}$, $a_{n-}b_{n-1}a_{n-1}$, or $b_{n-}a_{n-}$, $b_{n-}a_{n-1}b_{n-1}$, $b_{n-}a_{n-1}b_{n-1}$. (A monomial in this basis is called irreducible.)

**Proof.** (a) We will use [1, Theorem 1.2]. Accordingly, starting with (R.1)–(R.4) we need to derive a set of substitution rules $W = f$ such that the following ambiguities arising from the application of these is resolvable. Let $W = f$ and $W' = f'$ be substitution rules and $A$, $B$, $C \in \langle X \rangle$.

**Inclusion ambiguities:** If $B = W''$ and $ABC = W$ then $Af'C$ and $f$ must reduce to a common expression through substitutions. (Here $W = f$ and $W' = f'$ are different rules.)

**Overlap ambiguities:** If $AB = W$ and $BC = W'$ then $fC$ and $Af'$ must reduce to a common expression through substitutions. We informally write $(AB)C = A(BC)$. (Here none of $A$, $B$, or $C$, is 1.)

There are two inclusion ambiguities arising from (R.1)–(R.4).

\[ABC = a_{nn}b_{nn}, \quad W = W'\] (rules of type $a_{n-}b_{n-}$ and $a_{n-}b_{n-}$). \hspace{1cm} (1)

\[ABC = b_{nn}a_{nn}, \quad W = W'\] (rules of type $b_{n-}a_{n-}$ and $b_{n-}a_{n-}$). \hspace{1cm} (2)
The first is resolvable, and the second is formally the first by 2.1. Therefore the second is also resolvable. (A rigorous justification is given at the end of the proof.)

Consider the overlap ambiguities arising from (R.1)–(R.4) with $W = f$ of type $a_n b_n$. There are two categories.

\[(a_n b_n) a_n = a_n (b_n a_n), \quad W' = b_n a_n = f' \text{ of type } b_n a_n.\]  \hfill (3)

\[(a_n b_n) a_n = a_n (b_n a_n), \quad W' = b_n a_n = f' \text{ of type } b_n a_n.\]  \hfill (4)

The first of these is resolvable. The second yields the new relation

\[(R.5) \quad a_{nl} b_{n-1j} a_{n-1k} = \delta_{jk} a_{nl} - \lambda_{ln} \delta_{ij} a_{nk} - \sum_{l<n-1} a_{nl} b_{lj} a_{lk} \]
\[+ \sum_{l<n} \lambda_{ln} a_{ll} b_{lj} a_{nk}.\]

By 2.1 we generate from (R.5) the relations

\[(R.6) \quad a_{ln} b_{jn-1} a_{kn-1} = \lambda_{n-1k} \delta_{jk} a_{ln} - \lambda_{n-1n} \delta_{ij} a_{kn} \]
\[- \sum_{l<n-1} \lambda_{n-1l} a_{ln} b_{lj} a_{kl} + \sum_{l<n} \lambda_{n-1n} a_{ll} b_{lj} a_{kn}.\]

\[(R.7) \quad b_{nl} a_{n-1j} b_{n-1k} = \lambda_{jn-1} \delta_{jk} b_{nl} - \lambda_{nn-1} \delta_{ij} b_{nk} \]
\[- \sum_{l<n-1} \lambda_{ln-1} b_{nl} a_{lj} b_{lk} + \sum_{l<n} \lambda_{nn-1} b_{ll} a_{lj} b_{nk}.\]

\[(R.8) \quad b_{ln} a_{jn-1} b_{kn-1} = \delta_{jk} b_{ln} - \lambda_{nj} \delta_{ij} b_{kn} \]
\[- \sum_{l<n-1} b_{ln} a_{lj} b_{kl} \]
\[+ \sum_{l<n} \lambda_{nl} b_{ll} a_{lj} b_{kn}.\]

We will refer to the relations of (R.5)–(R.8) as type $a_n b_{n-1} a_{n-1}$, $a_n b_{n-1} a_{n-1}$, $a_n b_{n-1} a_{n-1}$, $b_n a_{n-1} b_{n-1}$, and $b_n a_{n-1} b_{n-1}$, respectively.

There are three categories of inclusion ambiguities arising from (R.1)–(R.8) where $W = f$ is of type $a_n b_{n-1} a_{n-1}$.

\[ABC = a_{nn} b_{n-1n} a_{n-1}, \quad W' = a_{nn} b_{n-1n} = f' \text{ of type } a_n a_{n-1}.\]  \hfill (5)

\[ABC = a_n b_{n-1n} a_{n-1}, \quad W' = b_{n-1n} a_{n-1} = f' \text{ of type } b_n a_{n-1}.\]  \hfill (6)

\[ABC = a_{nn} b_{n-1n-1} a_{n-1}, \quad W' = a_{nn} b_{n-1n-1} a_{n-1} = f' \text{ of type } a_n b_{n-1} a_{n-1}.\]  \hfill (7)
There are three categories of overlap ambiguities arising from (R.1)–(R.8) where \( W = f \) is of type \( a_n b_{n-1} a_{n-1} \).

\[
(a_n b_{n-1} a_{n-1}) b_{n-1} = a_n b_{n-1} (a_{n-1} b_n),
\]

\[
W' = a_n b_{n-1} = f'
\]

of type \( a_n b_{n-1} \).

\[
(a_n b_{n-1} a_{n-1} b_{n-1} = a_n (b_{n-1} a_{n-1} b_{n-1}),
\]

\[
W' = b_{n-1} a_{n-1} b_{n-1} = f'
\]

of type \( b_{n-1} a_{n-1} b_{n-1} \).

\[
(a_n b_{n-1} a_{n-1} b_{n-1} = a_n b_{n-1} (a_{n-1} b_n a_n),
\]

\[
W' = a_n b_{n-1} a_{n-1} = f'
\]

of type \( a_n b_{n-1} a_{n-1} \).

There are four categories of overlap ambiguities arising from (R.1)–(R.8) with \( W' = f' \) of type \( a_n b_{n-1} a_{n-1} \).

\[
(b_n a_n) b_{n-1} a_{n-1} = b_n (a_n b_{n-1} a_{n-1}),
\]

\[
W = b_n a_n = f
\]

of type \( b_n a_n \).

\[
(b_n a_n) b_{n-1} a_{n-1} = b_n (a_n b_{n-1} a_{n-1}),
\]

\[
W = b_n a_n = f
\]

of type \( b_n a_n \).

\[
(b_n a_{n-1} b_{n-1}) a_{n-1} = b_n (a_{n-1} b_{n-1} a_{n-1}),
\]

\[
W = b_n a_{n-1} b_{n-1} = f
\]

of type \( b_n a_{n-1} b_{n-1} \).

\[
(a_n b_{n-1} a_{n-1}) b_{n-1} a_{n-1} = a_n b_{n-1} (a_{n-1} b_{n-1} a_{n-1}),
\]

\[
W = a_n b_{n-1} a_{n-1} = f
\]

of type \( a_n b_{n-1} a_{n-1} \).

By 2.1 we see (13) is formally (9) and (14) is formally (10). It is straightforward (but very tedious) to show that (5)–(12) are resolvable. Any other inclusion or overlap ambiguity arising from (R.1)–(R.8) is formally one of these by 2.1. Once we give a rigorous justification that the above-mentioned cases are the only real ones, the proof of the proposition will be complete by [1, Theorem 1.2].

The justification involves some minor observations on the material of [1, Section 1]. For us \( k \) is a field. Continuing the notation and terminology of this section, let \( \lambda_x \in k^* \) for \( x \in X \) and set \( x = \lambda_x x \). For a monomial \( A = x_1 \cdots x_n \) define \( A = \lambda_A A \), where \( \lambda_A = \lambda_{x_1} \cdots \lambda_{x_n} \). Observe that \( k(X) \) is also the free semigroup algebra on \( X \). Define \( A < B \) if \( A < B \). Suppose \( S \) is a reduction system for \( X \). Define a reduction system \( S \) for \( X \) by \( \sigma = (W, f) = (\lambda_W W, \lambda_W f) \) for \( \sigma = (W, f) \in S \). It is easy to see that \( r_{A W, B} = r_{A W, B} \), so the set of reductions for \( S \) is the set of reductions for \( S \).

Suppose \( AB = W' \), \( BC = W' \), where \( A, B, C \neq 1 \). Then the overlap ambiguity \( (AB)C = A(BC) \) is resolvable if and only if \( (AB)C = A(BC) \) is
resolvable. If neither is resolvable, the new relations derived are related by \((W, f) = (\lambda_\mu W, \lambda_\nu f)\) again. Likewise for inclusion ambiguities.

Note that when we apply 2.1 we impose a different ordering on \(X\) which does not alter the form of (R.1)-(R.8). This last observation completes the proof. Q.E.D.

**Corollary 1.** Let \(k\) be any field and \(C\) be the coalgebra over \(k\) with basis \(\{a_{ij}\}_{1 \leq i, j \leq 2}\) whose structure is determined by \(\Delta a_{ij} = \sum k a_{ik} \otimes a_{kj}\). Let \(\lambda_1 = 1, \lambda_2 = \rho \in k^*\) and let \(T: C \to C\) be the coalgebra automorphism determined by \(T(a_{ij}) = \lambda_i^{-1} a_{ij}\). For \(n \geq 1\) and \(0 \leq i, j \leq n\) let \(e_{ij}^{(n)} = a_{ij} b_{ij} \cdots\), where \(a_{i_1} b_{i_1} \cdots = e_i^{(n)}\) and \(a_{i_1} b_{i_1} \cdots = e_j^{(n)}\) (as defined in Section 1).

(a) The \(e_{ij}^{(n)}\)s are irreducible for \(0 \leq i, j \leq n\).

(b) \(\Delta e_{ij}^{(n)} = \sum_{k=0}^n E_{ik}^{(n)} e_{kj}^{(n)}\), where \(E_{ij}^{(n)} = r_{ij}^{(n)}(\rho) e_{ij}^{(n)} + u_{ij}^{(n)}\) and \(u_{ij}^{(n)}\) is in the span of the \(e_{kl}^{(m)}\)s, \(0 \leq k, l \leq m \leq n - 2\). \((E_{in}^{(n)} = e_{in}^{(n)}\) for \(0 \leq i \leq n\).)

For the \(E_{ij}^{(n)}\)s of (b):

(c) \(\Delta E_{ij}^{(n)} = \sum_{k=0}^n E_{ik}^{(n)} \otimes E_{kj}^{(n)}\) and \(e(E_{ij}^{(n)}) = \delta_{ij}\).

(d) \(S^2(E_{ij}^{(n)}) = \lambda_i^{(n)}(\lambda_j^{(n)})^{-1} E_{ij}^{(n)}\), where

\[
\lambda_i^{(n)} = \begin{cases} 
\rho^{-m}; & i = 2m \text{ even} \\
\rho^{m+1}; & i = 2m + 1 \text{ odd}
\end{cases}
\]

For \(n = 2s\) is even

If \(n = 2s + 1\) is odd

(e) Suppose \(r_{ij}^{(n)}(\rho) = 0\). Then \(r_{ij}^{(n)}(\rho) u_{ij}^{(n)} = 0\) and \(\Delta u_{ij}^{(n)} = \sum_k u_{ik}^{(n)} \otimes u_{kj}^{(n)}\) for \(0 \leq i \leq n\). (In particular, the \(u_{ij}^{(n)}\)s, where \(r_{ij}^{(n)}(\rho) = r_{ij}^{(n)}(\rho) = 0\), form a subcoalgebra.)

Proof. (a) follows from the previous proposition and the nature of (R.1)-(R.8).

(b) \(\Delta e_{in}^{(n)} = \sum_{k=1}^n a_{ik} b_{ik} \cdots \otimes a_{kj} b_{kj} \cdots\), so (b) follows by the reduction rules (R.1)-(R.8) and the definition of \(r_{ij}^{(n)}(\rho)\). Since \(r_{in}^{(n)}(\rho) = 1\) by 1.2(b) the parenthetical remark is evident.

(c) If \(m_i = e_{in}^{(n)}\) then \(m_1, \ldots, m_n\) is the basis of a left coideal by (a) and (b), so (c) follows by Lemma 1(a).

(d) \(S^2(e_{in}^{(n)}) = \rho_i e_{in}^{(n)}\) for some \(\rho_i \in k^*\), so by Lemma 1(c) \(S^2(E_{ij}^{(n)}) = \rho_i \rho_j^{(n)} E_{ij}^{(n)}\) for \(0 \leq i, j \leq n\). Set \(\lambda_i^{(n)} = \rho_i \rho_0^{(n)}\). Then \(\lambda_i^{(n)}(\lambda_j^{(n)})^{-1} = \rho_i \rho_j^{-1}\), and \(S^2(E_{0i}^{(n)}) = \lambda_i^{(n)} E_{0i}^{(n)}\) for \(0 \leq i \leq n\). It is easy to see that the eigenvalues of \(e_{0i}^{(n)}\), \(e_{0\cdots}^{(n)}\), form the sequence 1, \(\rho, \rho^{-1}, \rho, \rho^{-2}, \ldots\) if \(n\) is even, and form the sequence 1, \(\rho^{-1}, \rho, \rho^{-2}, \rho^2, \ldots\) if \(n\) is odd. This is sufficient for (d).
(e) Suppose $r_{j}(p) = 0$. Then $E_{kj}^{(n)} = u_{kj}^{(n)}$ for $0 \leq k \leq n$, so by (b) and (c) we have for all $i$ that

$$
\Delta u_{ij}^{(n)} = \sum_{k=0}^{n} E_{ik}^{(n)} \otimes u_{kj}^{(n)} = \sum_{k=0}^{n} (r_{k}^{(n)}(p) e_{ik}^{(n)} + u_{ik}^{(n)}) \otimes u_{kj}^{(n)}
$$

$$
= \sum_{k=0}^{n} e_{ik}^{(n)} \otimes r_{k}^{(n)}(p) u_{kj}^{(n)} + \sum_{k} u_{ik}^{(n)} \otimes u_{kj}^{(n)}.
$$

Thus by (a) and (b) it follows that $r_{k}^{(n)}(p) u_{kj}^{(n)} = 0$ for all $k$ and $\Delta u_{ij}^{(n)} = \sum_{k} u_{ik}^{(n)} \otimes u_{kj}^{(n)}$. The parenthetical comment is left to the reader. Q.E.D.

As a consequence of part (e) of the above we have:

**PROPOSITION 3.** Let $k$ be a field and suppose $p \in k$ is a primitive $n$th root of unity, $n \geq 2$. Then $r_{0}^{(n)}(p) = \cdots = r_{n-2}^{(n)}(p) = 0$.

**Proof.** By 1.2(c) $r_{l}^{(n)}(p) = 1 + p + \cdots + p^{n-1}$, so $r_{n-2}^{(n)}(p) = 0$. Thus by Corollary 2(e) to show $r_{l}^{(n)}(p) = 0$ we need only show $u_{l}^{(n)} \neq 0$, where $0 \leq l \leq n-2$. Write $n = 2s$ if $n$ is even and $n = 2s + 1$ if $n$ is odd. To compute $u_{l}^{(n)}$ we examine the computation of $E_{l}^{(n)}$ by the reduction rules. Fix $0 \leq l \leq n-2$ and symbolically write

$$
\Delta e_{l}^{(n)} = \sum_{1 \leq i_{1}, j_{1}, \ldots, k_{2}} a_{-i_{1}} b_{-j_{1}} a_{-i_{2}} \cdots \otimes a_{i_{1}} b_{j_{1}} a_{i_{2}} \cdots
$$

where the first string of blanks represents the subscripts of $e_{l}^{(n)}$ and the second string represents those of $e_{l}^{(n)}$. There are two types of tensors which reduce to $- \otimes e_{n-2}^{(n)}$—namely, those of the form (1) $A_{k} \otimes R_{k}$, where $j_{1} = \cdots = j_{s} = 1$ and $i_{k} = 1$ (hence $i_{l} = 2$ for $l \neq k$), and those of the form (2) $B_{k} \otimes S_{k}$, where $i_{l} = \cdots = i_{s} = 2$ ($-i_{s+1}$ if $n$ is odd) and $j_{k} = 2$ (hence $j_{l} = 1$ for $l \neq k$). Set $e = e_{l}^{(n-2)}$, $E = e_{l}^{(n-2)}$, and $F = e_{n-2}^{(n)}$. Let $\kappa - 1$ be the largest integer $k$ such that the subscripts represented by the blanks of $a_{-i_{1}} b_{j_{1}} a_{-i_{2}} \cdots a_{-i_{k}} b_{-j_{k}}$ are all 1’s (if $i = 0$ and $n$ is odd then $\kappa = s + 2$). Since $i \leq n-2$ it follows $\kappa \geq 2$.

2.2. $R_{k} = \rho^{k-1} F$ and $S_{k} = -\rho^{k-1} F$.

Since the blanks of $a_{-i_{1}} b_{-j_{k}} \cdots$ represent an alternating string if $\kappa \leq s$, it follows that

2.3. $B_{k} = e - A_{k}$ if $k < \kappa$ and $B_{k} = -A_{k}$ if $k \geq \kappa$. 
2.4. 

\[ A_k = \begin{cases} 
E : & k = 1 \\
(1 - \rho)e + \rho A_{k-1} : & 1 < k < \kappa \\
x e + \rho A_{\kappa-1} : & k = \kappa \\
\rho A_{k-1} : & k > \kappa.
\end{cases} \]

where \( x = 1 - \rho \) or \( x = -\rho \).

From 2.4 it follows that

2.5. 

\[ A_k = \begin{cases} 
(1 - \rho^{k-1})e + \rho^{k-1}E : & 1 \leq k < \kappa \\
\rho^{k-\kappa}(x, e + \rho^{\kappa-1}E) : & k \geq \kappa.
\end{cases} \]

where \( x, = 1 - \rho^{k-1} \) or \( x, = -\rho^{k-1} \).

For convenience define \( x, = 0 \) if \( n = 2s \) is even and \( \kappa = s + 1 \). From 2.2–2.5 we see that \( u_{in-2} = \alpha e \) for some \( \alpha \in k \). We will first show that

2.6. 

\[ \alpha = \left(1 - \frac{\rho^{k-1}}{1 - \rho}\right) \left(1 - (1 + \rho^{k-1})(1 + \rho^{-(\kappa-1)}x,)\right) \quad \text{if} \quad \kappa \leq s + 1. \]

Case 1. \( n = 2s \) even. First note that \( 0 = \sum_{k=1}^{s} (1 + \rho) \rho^{2(k-1)} = \sum_{k=1}^{s} (\rho^{k-1} + \rho^{k-1}) \rho^{k-1} \), so

\[ \sum_{k=\kappa}^{s} (\rho^{k-1} + \rho^{k-1}) \rho^{k-1} = -\sum_{k=1}^{\kappa-1} (\rho^{k-1} + \rho^{k-1}) \rho^{k-1} \]

\[ = -\left(1 - \frac{\rho^{2(k-1)}}{1 - \rho}\right) \quad \text{for} \quad 2 \leq \kappa \leq s + 1. \]

Now \( E(n)_{in-2} = \sum_{k=1}^{\kappa-1} (\rho^{k-1}A_k - \rho^{k-1}B_k) \) in this case, so

\[ \alpha = \sum_{k=1}^{\kappa-1} (\rho^{k-1} + \rho^{k-1})(1 - \rho^{k-1}) \]

\[ - \sum_{k=1}^{\kappa-1} \rho^{k-1} + \sum_{k=\kappa}^{s} (\rho^{k-1} + \rho^{k-1}) x, \rho^{k-\kappa} \]

\[ = \left(1 - \frac{\rho^{k-1}}{1 - \rho}\right) - \left(1 - \frac{\rho^{2(k-1)}}{1 - \rho}\right) - \left(1 - \frac{\rho^{2(k-1)}}{1 - \rho}\right) x, \rho^{-(\kappa-1)} \]

which is the equation of 2.6.
Case 2. $n = 2s + 1$ odd. We make the observation that

$$\sum_{k=1}^{s} (\rho^{k-1} + \rho \rho^{k-1}) \rho^{k-1} + \rho^{2s} = 0,$$

so from this it follows

$$\sum_{k=1}^{s} (\rho^{k-1} + \rho \rho^{k-1}) \rho^{k-1} + \rho^{2s} = -\left(\frac{1 - \rho^{2(k-1)}}{1 - \rho}\right)$$

for $2 \leq \kappa \leq s + 1$.

Since

$$E_{n-2}^{(n)} = \sum_{k=1}^{s+1} \rho^{k-1} A_k - \sum_{k=1}^{s} \rho \rho^{k-1} B_k$$

$$= \sum_{k=1}^{s} (\rho^{k-1} A_k - \rho \rho^{k-1} B_k) + \rho^s A_{s+1},$$

for $\kappa \leq s + 1$ we compute as above

$$\alpha = \left(\frac{1 - \rho^{s-1}}{1 - \rho}\right) - \left(\frac{1 - \rho^{2(k-1)}}{1 - \rho}\right) + \left[\sum_{k=1}^{s} (\rho^{k-1} + \rho \rho^{k-1}) + \rho^{2s}\right] x_\kappa \rho^{-(\kappa-1)}$$

which has the form of 2.6.

If $\kappa = s + 2$ we compute

$$\alpha = \sum_{k=1}^{s} (\rho^{k-1} + \rho \rho^{k-1})(1 - \rho^{k-1}) - \sum_{k=1}^{s} \rho \rho^{k-1} + \rho^s(1 - \rho^s)$$

$$= \left(\frac{1 - \rho^s}{1 - \rho}\right) + \rho^s = \frac{1 - \rho^{s+1}}{1 - \rho},$$

so

2.7.

$$\alpha = \left(\frac{1 - \rho^{s+1}}{1 - \rho}\right) \quad \text{if} \quad n = 2s + 1 \text{ is odd and } \kappa = s + 2.$$

To complete the proof of the proposition we need to show the expression of 2.6 is not 0 if $x_\kappa = 1 - \rho^{-s-1}$ or $x_\kappa = -\rho^{-s-1}$. If $x_\kappa = 1 - \rho^{-s-1}$ then

$$1 - (1 + \rho^{s-1})(1 + \rho^{-(\kappa-1)}(1 - \rho^{s-1})) = 1 - (1 + \rho^{s-1})(\rho^{-(\kappa-1)})$$

$$= -\rho^{-(\kappa-1)},$$
so

\[ \alpha = -\left( \frac{1 - \rho^{-1}}{1 - \rho} \right) \rho^{-1}. \]

If \( x = -\rho^{-1} \) then

\[ \alpha = \left( \frac{1 - \rho^{-1}}{1 - \rho} \right). \]

Q.E.D.

3. The Main Result

In this section we prove that the antipode \( s \) of a certain class of cosemisimple Hopf algebra over a field \( k \) has order 1, 2, or \( \infty \). In the next section we show that the infinite order is realizable.

PROPOSITION 4. Let \( C \) be a coalgebra over an algebraically closed field \( k \), and suppose \( T: C \to C \) is a coalgebra automorphism.

(a) If \( C \) is simple then \( T(M) \subseteq M \) for some simple left (respectively right) coideal \( M \subseteq C \).

(b) If \( C \) is simple and \( T \) is diagonalizable then \( C \) has a basis \( \{e_{ij}\}_{1 \leq i, j \leq n} \) such that for all \( i, j \)

(i) \( \Delta e_{ij} = \sum_k e_{ik} \otimes e_{kj} \) and \( \varepsilon(e_{ij}) = \delta_{ii} \),

(ii) \( T(e_{ij}) = \lambda_i \lambda_j^{-1} e_{ij} \), where \( \lambda_1, \ldots, \lambda_n \in k^* \).

(c) Assume \( T \) is diagonalizable and \( T(E) = E \) for all simple subcoalgebras \( E \subseteq C \). Let \( M \subseteq C \) be a left (respectively right) coideal such that \( T(M) \subseteq M \). If \( \dim M_{(1)} = 1 \) then \( M \) is indecomposable (hence \( M \) is simple if it is semisimple).

Proof. (a) Suppose we can find a minimal left coideal \( M \subseteq C \) such that \( T(M) \subseteq M \). Then the parenthetical part will follow since \( C^{op}(\Delta c - \sum c_{(2)} \otimes c_{(1)}) \) is simple and \( T \) is also an automorphism of \( C^{op} \).

Let \( L \subseteq C^* \) be a maximal left ideal. Then \( M = L^\perp \subseteq C \) is a simple left coideal, and \( T^*(L) \subseteq L \) implies \( T(M) \subseteq M \). Now \( C^* \cong \text{End}_k(V) \) for some finite-dimensional vector space \( V \) over \( k \). Thus to prove (a) it suffices to show that if \( f \) is an algebra automorphism of \( A = \text{End}(V) \) then \( f(L) \subseteq L \) for some maximal left ideal \( L \subseteq A \).

By the Noether–Skolem theorem there is an invertible \( x \in A \) such that \( f(a) = x^{-1}ax \) for all \( a \in A \). Since \( k \) is algebraically closed, \( x(v) = \lambda v \) for some \( v \in V \setminus 0 \) and \( \lambda \in k \). Now \( L = \{a \in A : a(v) = 0\} \) is a maximal left ideal of \( A \), and \( x^{-1}Lx(v) = x^{-1}L(\lambda v) = 0 \) means \( f(L) \subseteq L \).
(b) By (a) \( T(M) \subseteq M \) for some simple left coideal \( M \subseteq C \). Since \( T \) is diagonalizable, \( M \) has a basis of eigenvectors \( m_1, \ldots, m_n \). Now (b) follows by Lemma 1 since the \( e_{ij} \)'s therein defined form a basis for \( C \).

(c) By considering \( C^o \), we see to prove (c) we may assume \( M \) is a right coideal of \( C \). Let \( M \subseteq C \) be a right coideal. We will show that \( M \) contains a unique simple subcomodule. First note that \( L = M \cap C_o \) is the sum of the simple subcomodules of \( M \). \( T(C_o) \subseteq C_o \) so \( T(M) \subseteq M \) implies \( T(L) \subseteq L \). Hence we may assume \( M \) is semisimple. Write the coradical \( C_o = \bigoplus_a E_a \) of \( C \) as the direct sum of simple subcoalgebras. Then \( M_a = M \cap E_a \) is a subcomodule and \( M = \bigoplus_a M_a \). Now \( T(M_a) \subseteq M_a \) by assumption, so \( \dim M_{(1)} = 1 \) means \( M_a = (0) \) for all but one \( \alpha \). Therefore we may assume \( C \) is a simple subcoalgebra.

Let \( \{ e_{ij} \}_{1 \leq i, j \leq n} \) be any basis for \( C \) satisfying (i) and (ii) of part (b), and let \( m \in M \setminus 0 \) satisfy \( T(m) = \rho m \) for some \( \rho \in k \). Write \( m = \sum_{i,j} \alpha_{ij} e_{ij} \). Note that \( \alpha_{ij} \neq 0 \) implies \( \lambda_i \lambda_j^{-1} = \rho \). Now

\[
\Delta m = \sum_{i,j,k} \alpha_{ij} e_{ik} \otimes e_{kj} = \sum_{j,k} \left( \sum_i \alpha_{ij} e_{ik} \right) \otimes e_{kj}.
\]

Suppose \( \alpha_{i_0 j_0} \neq 0 \). Then \( \sum_i \alpha_{i j_0} e_{i j_0} \in M_{(1)} \setminus 0 \). Since \( M_{(1)} \) is one dimensional, we conclude \( \alpha_{ij} \neq 0 \) implies \( i = i_0 \). Thus \( m \in \left( e_{i_0 1}, \ldots, e_{i_0 n} \right) \equiv S \), a simple subcomodule of \( C \) satisfying \( T(S) \subseteq S \). Since \( \dim M_{(1)} = 1 \) we conclude \( M = S \).

Q.E.D.

The proof of the main theorem of this paper essentially reduces to the following lemma. Our formulation is a minor refinement of the basic computation of [4].

**Lemma 3.** Let \( A \) be a Hopf algebra over a field \( k \) with antipodes. Assume \( M \subseteq A \) is a right coideal with basis \( m_1, m_2 \) which satisfy \( s^2(m_1) = m_1 \) and \( s^2(m_2) = \rho m_2 \) for some \( \rho \in k^* \). If \( m_1 s(m_2) = 0 \) (or equivalently \( m_2 s(m_1) = 0 \)) then \( \rho = 1 \).

**Proof.** The fact that \( m_1 s(m_2) = 0 \) if and only if \( m_2 s(m_1) = 0 \) is clear.

Assume \( \rho \neq 1 \) and set \( T = s^2, \lambda_1 = 1, \) and \( \lambda_2 = \rho \). Since \( \varepsilon(M_{(\rho)}) = 0 \) we may assume \( \varepsilon(m_j) = \delta_{ij} \) for \( j = 1, 2 \). Now let \( \{ e_{ij} \}_{1 \leq i, j \leq 2} \) be defined for this basis as in Lemma 1(a). By the same lemma we see \( m_j = e_{ij} \) and \( s^2(e_{ij}) = \lambda_i^{-1} \lambda_j e_{ij} \) for \( 1 \leq i, j \leq 2 \). Suppose \( m_1 s(m_2) = 0 \). Then \( e_{12} s(e_{12}) = e_{11} s(e_{11}) = 0 \). Let \( x = e_{11} s(e_{11}) \). Note that \( s(x) = x \) and \( \varepsilon(x) = 1 \).

We first show that \( x^2 = x \) and \( x e_{12} = 0 \). The calculation \( e_{11} = e_{11} 1 = e_{11} (s(e_{11}) e_{11} + s(e_{12}) e_{21}) = e_{11} s(e_{11}) e_{11} \) shows \( x^2 = x \), and the calculation \( 0 = e_{11} 0 = e_{11} (s(e_{11}) e_{12} + s(e_{12}) e_{22}) = e_{11} s(e_{11}) e_{12} \) shows \( x e_{12} = 0 \).
To compute $\Delta x$ observe that $e_{12} s(e_{12}) = 1 - e_{11} s(e_{11}) = 1 - x$, and that $e_{21} s(e_{12}) = s^2(e_{21} s(e_{12})) = s(\rho e_{12} s(e_{12}))$, so

$$\Delta x = (e_{11} \otimes e_{11} + e_{12} \otimes e_{21})(s(e_{11}) \otimes s(e_{11}) + s(e_{21}) \otimes s(e_{12}))$$

$$= e_{11} s(e_{11}) \otimes e_{11} s(e_{11}) + e_{12} s(e_{21}) \otimes e_{21} s(e_{12})$$

$$= x \otimes x + (1 - x) \otimes \rho(1 - x) = ((1 + \rho)x - \rho 1) \otimes x + \rho(1 - x) \otimes 1.$$

Therefore $g = (1 + \rho)x - \rho 1$ is grouplike. Since $x^2 = x$ we have

$$g^2 = ((1 + \rho)^2 - 2\rho(1 + \rho))x + \rho^2 1 = (1 - \rho)(1 + \rho)x + \rho^2 1$$

$$= (1 - \rho)g + \rho 1,$$

so $g^{-1} = \rho^{-1}(g - (1 - \rho)1)$. Now $g^{-1}$ is grouplike, and distinct grouplikes are independent, so $g = 1$. Therefore $(1 + \rho)x = (1 + \rho)1$, so $xe_{12} = 0$ means $-1 = \rho$ ($\neq 1$). But then $x - 1$ is primitive, whence $-(x - 1) = s(x - 1) = x - 1$. This forces $x - 1 = 0$, or $x = 1$. But this is impossible since $xe_{12} = 0$. Therefore $\rho = 1$.

The main result of this paper is the following Theorem.

**Theorem.** Let $A$ be a cosemisimple Hopf algebra over a field $k$ with antipode $s$. If $s^2$ is diagonalizable and $A$ is generated by its subcoalgebras of dimension $\leq 8$, then $s$ has order 1, 2, or $\infty$.

**Proof.** Let $\bar{k}$ be an algebraic closure of $k$. Then $A \otimes_k \bar{k}$ is cosemisimple, so we may assume $k$ is algebraically closed. In this case $A$ is generated by its simple subcoalgebras of dimension 1 or 4. Assume $s$ has finite order. To prove the theorem it suffices to show that $s^2 \equiv I$ on the 4-dimensional simple subcoalgebras of $A$.

Set $T = s^2$. By [3, Theorem 3.3] $T$ is an automorphism since $A$ is cosemisimple. Let $C \subseteq A$ be a 4-dimensional simple subcoalgebra. Then $T(C) \subseteq C$ since $C$ is simple by the same theorem. By Proposition 4(b) $C$ has a basis $\{e_{ij}\}_{1 \leq i, j \leq 2}$ satisfying $\Delta e_{ij} = \sum_k e_{ik} \otimes e_{kj}$ and $T(e_{ij}) = \lambda_i \lambda_j^{-1} e_{ij}$ for some $\lambda_1, \lambda_2 \in k^*$. Set $\lambda_{ij} = \lambda_i \lambda_j^{-1}$ and define $\rho = \lambda_{12}$. Then $\lambda_{11} - \lambda_{22} = 1$ and $\lambda_{21} = \rho^{-1}$. To prove the theorem we need only show $\rho = 1$.

Assume $\rho \neq 1$. Then applying Lemma 3 to the right coideal $M \subseteq C$ with basis $m_1 = e_{11}$ and $m_2 = e_{12}$ it follows that $e_{12} s(e_{11}) \neq 0$. Since $s$ has finite order, $\rho$ is a primitive $n$th root of unity for some $n \geq 2$. Let $\pi$ be the Hopf algebra map $\pi: H_k(C, T) \rightarrow A(a_{ij} \mapsto e_{ij}, \, b_{ij} \mapsto s(e_{ij}))$ and set $\mathcal{E}_{ij}^{(n)} = \pi(E_{ij}^{(n)})$. Since $\pi$ is a Hopf algebra map it follows $T(\mathcal{E}_{ij}^{(n)}) = t_i(\lambda_j^{(n)})^{-1} \mathcal{E}_{ij}^{(n)}$ for $0 \leq i, j \leq n$ by Corollary 1(d).

We will obtain the contradiction $e_{12} s(e_{11}) = 0$, so $\rho = 1$ after all. First of all note that $e_{12} s(e_{11}) \mathcal{E}_{in-2}^{(n-2)} = \mathcal{E}_{in}^{(n)}$ for $0 \leq i \leq n - 2$. It suffices to show
\( f_{in}^{(n)} = (0) \) for \( 0 \leq i \leq n - 2 \). For if this is the case, then \( e_{12}s(e_{11})M = (0) \), where \( M \) is the span of the \( f_{in}^{(n-2)} \)'s. By Corollary 1(c) \( M \) is a left coideal of \( A \), and since \( s^2(M) \subseteq M \) we conclude \( e_{12}s(e_{11}) = 0 \) by Lemma 1(d).

Fix \( 0 \leq i \leq n - 2 \). By Proposition 4(c), parts (c) and (d) of Corollary 1, it follows \( f_{i0}^{(n)}, \ldots, f_{in}^{(n)} \) span a simple right coideal \( M \). By Proposition 3, \( r_0^{(n)}(\rho) = \cdots = r_{n-2}^{(n)}(\rho) = 0 \). Thus by Corollary 1(e), \( f_{i0}^{(n)}, \ldots, f_{in-2}^{(n)} \) span a (non-zero) subcomodule \( L \subseteq M \). Hence \( L = M \) since \( M \) is simple. But the eigenvalue of \( f_{in}^{(n)} \) is not among those of \( f_{i0}^{(n)}, \ldots, f_{in-2}^{(n)} \), so \( f_{in}^{(n)} = 0 \). Q.E.D.

By [3, Corollary 5.6] the order of the antipode of a finite-dimensional cosemisimple Hopf algebra over a field is finite.

**Corollary 2.** Let \( A \) be a finite-dimensional cosemisimple Hopf algebra over a field \( k \) with antipode \( s \). Assume \( A \) is generated by its subcoalgebras of dimension \( \leq 8 \).

(a) If the characteristic of \( k \) is 0 then \( s^2 = I \).

(b) If the characteristic of \( k \) is \( p > 0 \) and \( p \) does not divide the order of \( s^2 \), then \( s^2 = I \).

**Proof.** We may assume \( k \) is algebraically closed, in which case \( s^2 \) is diagonalizable. Q.E.D.

**Corollary 3.** Let \( A \) be a cosemisimple Hopf algebra over a field \( k \) of characteristic 0 with antipode \( s \). Assume \( A \) is generated by its subcoalgebras of dimension \( \leq 8 \). Then \( s^2 = I \) or \( s \) has infinite order.

4. **An Example**

Let \( k \) be a field having an element \( \rho \in k \) transcendental over the prime field. Then the Hopf algebra \( H_k(C, T) \) of Corollary 1 has antipode \( S \) of infinite order, and \( S^2 \) is diagonalizable. We will show that \( A = H_k(C, T) \) is cosemisimple—thus all the possibilities described in the Theorem are realized.

By the matrix coalgebra \( cM_S(k) \) over a field \( k \), where \( S \) is a non-void finite set, we mean the \( k \)-vector span with basis \( \{ e_{xy} \}_{x,y \in S} \) with coalgebra structure determined by \( \Delta e_{xy} = \sum_z e_{xz} \otimes e_{zy} \). Observe that

4.1. \( cM_S(k) \otimes cM_{\tau}(k) \rightarrow cM_{S \times \tau}(k) \) \( (e_{x,x} \otimes e_{u,u} \rightarrow e_{(x,u),(y,v)}) \) is a coalgebra isomorphism.

Recall \( C \subseteq A \) is the span of the \( a_{ij} \)'s, and \( B = S(C) \) is the span of the \( b_{ij} \)'s, where \( 1 \leq i, j \leq 2 \). Let \( M \subseteq A \) be a subcoalgebra of the form \( M = \)
\[X_1 \cdots X_n, \text{ where } X_i = C \text{ or } B \text{ for each } i, \text{ and formally define } |M| = n. \text{ Set } M(-1) = (0), M(0) = k \cdot 1, \text{ and let } M(n) \subseteq A \text{ be the sum of those } M' \text{'s where } |M| \leq n. \]

For \( M = X_1 \cdots X_n \), where \( n \geq 1 \), \( x_i \in X_i \) will denote a member of the basis for \( X_i \) described above.

4.2. Let \( M = X_1 \cdots X_n \), where \( n \geq 1 \) and \( X_i = C \) or \( B \) for each \( i \). Then \( M \subseteq E + M(n-1) \), where \( E \) is a matrix coalgebra with basis \( e_{uv} = r_{uv}x_1 \cdots x_n + l \), where \( r_{uv} \in k^* \), \( x_1 \cdots x_n \) is irreducible, and \( l \in M(n-1) \).

**Proof.** \( r_i^n(\rho) \) has integer coefficients and is monic by 1.2. Therefore \( r_i^n(\rho) \neq 0 \) for all \( n \geq 0 \) and \( 0 \leq i \leq n \). Suppose \( X_1 = C \) and the string \( X_1, \ldots, X_n \) is an alternating pattern of \( C \)’s and \( B \)’s. Then 4.2 is true for \( M \) by virtue of Proposition 2 and Corollary 1. Likewise, 4.2 holds for \( M \) if the string is alternating and \( X_1 = B \) by virtue of 2.1(b).

Assume \( X_i = X_{i+1} = C \) for some \( i \). Let \( M_1 = X_1 \cdots X_i \) and \( M_2 = X_{i+1} \cdots X_n \). By induction on \( n \) we may write \( M_1 \subseteq E_1 + M(i-1) \) and \( M_2 \subseteq E_2 + M(n-i-1) \) as in the conclusion of 4.2. Therefore

\[
M = M_1 M_2 \subseteq E_1 E_2 + E_1 M(n-i-1) + M(i-1) E_2 + M(i-1) M(n-i-1),
\]

so \( M \subseteq E + M(n-1) \), where \( E = E_1 E_2 \). By Proposition 2 and 4.1, \( E \) is the desired matrix coalgebra for \( M \). By 2.1 again the argument holds when \( X_i = X_{i+1} = B \). Q.E.D.

The sum of cosemisimple subcoalgebras is cosemisimple. Thus \( M(n) \) is cosemisimple by induction on \( n \). The case \( n = 0 \) is trivial. Assume \( M(n-1) \) is cosemisimple. By 4.2 \( M(n) = \sum E + M(n-1) \), where \( E \) is simple. Thus \( M(n) \) is cosemisimple for all \( n \geq 0 \). Now since \( A = \sum_{n=0}^{\infty} M(n) \), it follows \( A = H_k(C, T) \) is cosemisimple.

Let \( \varphi : C \to C \) be the coalgebra antiautomorphism defined by \( \varphi(a_{ij}) = \lambda_i^{-1} \lambda_j a_{\tau(j)\tau(i)} \), where \( \tau = (12) \). Then the free Hopf algebra \( H_k(C, \varphi) \) on \( \varphi \) has antipode \( S \) which also has the properties that \( S^2 \) is diagonalizable and \( S \) has infinite order. The argument follows the lines of the above (with \( X_1 = \cdots = X_n \) in 4.2) but the details are far simpler to work out.

This particular \( \varphi \) has a natural generalization. Let \( k \) be any field, and for \( n \geq 1 \) let \( C = cM_S(k) \), where \( S = \{1, \ldots, n\} \). For \( \lambda_1, \ldots, \lambda_n \in k^* \) and an involution \( \tau : S \to S \) with \( \tau(n) = n - 1 \) define a linear automorphism \( \varphi : C \to C \) by \( \varphi(e_{ij}) = \lambda_i^{-1} \lambda_j e_{\tau(j)\tau(i)} \). It is easy to see that \( \varphi \) is a coalgebra antiautomorphism. By resolving three ambiguities (actually only two are necessary) one can show that the monomials in the \( e_{ij} \)’s which contain no term of the form \( e_n e_{n-1} \) or \( e_{-n} e_{-n-1} \) constitute a linear basis for \( H_k(C, \varphi) \).
REFERENCES