On Hopf Algebras with Positive Bases

J-H. Lu*

Department of Mathematics, University of Arizona
E-mail: jhlu@math.arizona.edu

and

M. Yan†, Y. C. Zhu‡

Department of Mathematics, Hong Kong University of Science and Technology
E-mail: mamyan@ust.hk, mazhu@ust.hk

We show that if a finite dimensional Hopf algebra H over $\mathbb{C}$ has a basis with respect to which all the structure constants are non-negative, then H is isomorphic to the bicrossproduct Hopf algebra constructed by Takeuchi and Majid from a finite group G and a unique factorization $G = G_+G_-$ of G into two subgroups. We also show that Hopf algebras in the category of finite sets with correspondences as morphisms are classified in a similar way. Our results can be used to explain some results on Hopf algebras from the set-theoretical point of view.

Key Words: Hopf algebra, Boolean algebra, correspondence category

1. INTRODUCTION

In this paper, we prove two classification theorems for finite dimensinal Hopf algebras. The first theorem (Theorem 2.1) classifies finite dimensional Hopf algebras over $\mathbb{C}$ which admit *positive bases*. A basis of a Hopf algebra over $\mathbb{C}$ is said to be positive if the structure constants of all the structure maps of the Hopf algebra with respect to this basis are non-negative real numbers (see Section 2 for more precise definitions). This class of Hopf al-

* Research is partially supported by an NSF Postdoctorial Fellowship and NSF Grant DMS 9803624.

† Research is supported by Hong Kong Research Grant Council earmark grant HKUST 629/95P.

‡ Research is supported by Hong Kong Research Grant Council earmark grant HKUST 6071/98P.

gebras is closed under taking tensor products, duals and Drinfel'd doubles. Our theorem says that if a Hopf algebra has a positive basis, it must be isomorphic to the bicrossproduct Hopf algebra constructed by Takeuchi [16] and Majid [12] from a finite group G and a unique factorization $G = G_+G_-$ of G into two subgroups.

The second theorem (Theorem 5.3) classifies Hopf algebras in the correspondence category. In the monoidal category of finite sets, we may formally introduce the concept of Hopf algebras by imposing all the axioms in terms of commutative diagrams. Such a definition is just that of finite groups. The correspondence category under our consideration still has finite sets as objects. But a morphism from X to Y is a subset of $X \times Y$ instead of a map from X to Y. This is a monoidal category in which the concept of Hopf algebras can be similarly defined. Our theorem says that a Hopf algebra in the correspondence category is still given by a finite group G with a unique factorization $G = G_+G_-$ of two subgroups.

There have been many other classifications of finite dimensional Hopf algebras under different assumptions. An incomplete list includes [1, 2, 3, 5, 11].

One of the motivations to consider Hopf algebras with positive bases is that there are many natural Hopf algebras with nearly positive bases. We call a basis nearly positive if all the structure constants with repsect to this basis, except for those of the antipode map, are non-negative real numbers. For example, the modified quantum group $U_q(g)$ in [9] has a nearly positive basis realized in terms certain varieties. Other examples are the direct sums $\oplus_1^\infty R(S_n)$ and $\oplus_1^\infty R(GL_n(F_q))$ of complex representation rings [17], where positive bases are given by irreducible representations. The positivity of structural coefficients are due to the very way the product and the coproduct are defined. All the examples above are infinite dimensional Hopf algebras. In the finite dimensional case, we know of no examples of nearly positive bases that are not positive. It turns out the Hopf algebras in our classification have natural numbers as structure coefficients. It might be interesting to classify inifinite dimensional Hopf algebras with natural numbers as structure coefficients.

In subsequent papers [7, 8], we classify positive quasi-triangular structures on Hopf algebras with positive bases and discuss their relations to set-theoretical Yang-Baxter equations.

The paper is organized as follows: We first present the basic concepts and notations, and state the first classification theorem. In the next two sections, we give detailed proof of the theorem. In the final section, we discuss the correspondence category and outline the proof of the second classification theorem.

2. HOPF ALGEBRAS WITH POSITIVE BASES

Given a group G, the group algebra $\mathbb{C}G$ has the subset G as a positive basis in the sense that all the structure constants are nonnegative. Moreover, the dual basis is also a positive basis of the dual group algebra $(\mathbb{C}G)^*$. In general, we say a basis B of a Hopf algebra H is *positive* if, with respect to this basis,

- the coordinates of the unit 1 are non-negative;
- the coordinates of the counit ϵ (with respect to the dual basis B^*) are non-negative, i.e., $\epsilon(b) \geq 0$ for all $b \in B$;
- for any $b_1, b_2 \in B$, the coordinates of $b_1 b_2$ are non-negative;
- for any $b \in B$, the coordinates of $\Delta(b)$ (with respect to the tensor product basis $B \otimes B$) are non-negative;
- for any $b \in B$, the coordinates of the antipode $S(b)$ are non-negative.

It is easy to see that the duals and the tensor products of Hopf algebras with positive bases still have positive bases. For the antipode S of a finite dimensional Hopf algebra, it is well-known [14] that $S^N = id$ for some positive integer N. This implies that if B is a positive basis of H, then the structure constants of $S^{-1} = S^{N-1}$ with respect to B are still non-negative. Therefore $B^* \otimes B$ is a positive basis of the Drinfel'd double $D(H)$ of H.

The prototypical example of Hopf algebras with positive bases is the bicrossproduct Hopf algebra $H(G; G_+, G_-)$ constructed by Takeuchi [16] and Majid [12] from a finite group G and a unique factorization $G = G_+G_-$ of G into two subgroups. By $G = G_+G_-$, we mean that $G_\pm$ are subgroups of G and that every $g \in G$ can be written as $g = g_+g_-$ for unique $g_+ \in G_+$ and $g_- \in G_-$. By taking inverse, any $g \in G$ can also be written as $g = \bar{g}_-\bar{g}_+$ for unique $\bar{g}_+ \in G_+$ and $\bar{g}_- \in G_-$. Therefore to any $g \in G$ is associated four uniquely determined elements

$$\alpha_+(g) = g_+, \quad \beta_+(g) = \bar{g}_+, \quad \alpha_-(g) = \bar{g}_-, \quad \beta_-(g) = g_-,$$

given by

$$g = g_+g_- = \bar{g}_-\bar{g}_+. \tag{1}$$

It is then easy to see that

$$G_- \times G_+ \to G_+, \qquad (\bar{g}_-, \bar{g}_+) \mapsto (\bar{g}_-\bar{g}_+)_+ = g_+, \tag{2}$$

$$G_- \times G_+ \to G_-, \qquad (\bar{g}_-, \bar{g}_+) \mapsto (\bar{g}_-\bar{g}_+)_- = g_-. \tag{3}$$

$$G_+ \times G_- \to G_+, \qquad (g_+, g_-) \mapsto \overline{(g_+g_-)}_+ = \bar{g}_+, \tag{4}$$

$$G_+ \times G_- \to G_-, \qquad (g_+, g_-) \mapsto \overline{(g_+g_-)}_- = \bar{g}_- \tag{5}$$

are all group actions. Because of this, we also write

$$g_+ = {}^{\bar{g}_-}\bar{g}_+, \quad g_- = \bar{g}_-^{\,\bar{g}_+}, \quad \bar{g}_+ = g_+^{\,g_-}, \quad \bar{g}_- = {}^{g_+}g_-.$$

The third and the fourth actions satisfy the following matching relations

$${}^{g_+}(g_-h_-) = {}^{g_+}g_- \; {}^{(g_+^{\,g_-})}h_-, \qquad (h_+g_+)^{g_-} = h_+^{({}^{g_+}g_-)}\, g_+^{\,g_-}. \tag{6}$$

It is well known that given two actions between two groups $G_\pm$ satisfying the matching relations, we may reconstruct G. Similarly, G can be reconstructed from the first and the second actions, which satisfy similar matching relations. We will not use the first and the second actions in the proof of the classification theorem.

The Hopf algebra $H(G; G_+, G_-)$ is, by definition, the vector space over $\mathbb{C}$ spanned by the set $G = \{\{g\} : g \in G\}$ together with the following Hopf algebra structure:

$$\begin{aligned}
\{g\}\{h\} &= \begin{cases} \{\bar{g}_-h\} = \{gh_-\} & \text{in case } \bar{g}_+ = h_+ \\ 0 & \text{in case } \bar{g}_+ \neq h_+ \end{cases} \\
\Delta\{g\} &= \sum_{h\bar{k}_+ = g, \bar{k}_- = h_-} \{h\} \otimes \{k\} = \sum_{h_+k = g, \bar{k}_- = h_-} \{h\} \otimes \{k\} \\
1 &= \sum_{g_+ \in G_+} \{g_+\} \\
\epsilon\{g\} &= \begin{cases} 1 & \text{in case } g_+ = e \\ 0 & \text{in case } g_+ \neq e \end{cases} \\
S\{g\} &= \{g^{-1}\}
\end{aligned}$$

The construction above is given in the way that best suits the purpose of this paper. It is easy to see that the algebra structure on $H(G; G_+, G_-)$ is the cross-product algebra $(\mathbb{C}G_+)^* \rtimes \mathbb{C}G_-$ defined by the right action of G_- on G_+ given in (5). Similarly, the algebra structure on the dual Hopf algebra $H(G; G_+, G_-)^*$ (corresponding to the coproduct in $H(G; G_+, G_-)$) is the cross-product algebra $\mathbb{C}G_+ \ltimes (\mathbb{C}G_-)^*$ defined by the left action of G_+ on G_- given in (4).

The basis G for $H(G; G_+, G_-)$ is clearly positive. The following theorem says that, up to rescaling, these are all the finite dimensional Hopf algebras with positive bases.

THEOREM 2.1. *Given any finite dimensional Hopf algebra H over $\mathbb{C}$ with a positive basis B, we can always rescale B by some positive numbers, so* *that (H,B) is isomorphic to $(H(G;G_+,G_-),G)$ for a unique group G and a unique factorization $G=G_+G_-$.*

The proof of Theorem 2.1 will be given in Sections 3 and 4. A consequence of Theorem 2.1 is that the Drinfel'd double $D(H(G;G_+,G_-))$ of $H(G;G_+,G_-)$ is also of the form $H(\tilde{G};\tilde{G}_+,\tilde{G}_-)$ for some group $\tilde{G}$ and factorization $\tilde{G}=\tilde{G}_+\tilde{G}_-$. By tracing our proof of the theorem, we find

$$\begin{aligned}\tilde{G} &= G\times G,\\ \tilde{G}_+ &= \{(g_+,g_-) : g_+\in G_+, g_-\in G_-\}\cong G_+\times G_-,\\ \tilde{G}_- &= \{(g,g) : g\in G\}\cong G.\end{aligned}$$

The fact $D(H(G;G_+,G_-))\cong H(G\times G;G_+\times G_-,G)$ was previously discovered in [4], and more explicit formula for the isomorphism can be found there.

3. CLASSIFICATION UP TO RESCALING

In this section, we prove the classification theorem 2.1 up to rescaling. In the next section, we work out the necessary rescaling.

Let H be a finite dimensional Hopf algebra over $\mathbb{C}$ with a positive basis B. We denote by $B^*=\{b^* : b\in B\}$ the dual basis of H^*. The basis B^* is still positive. We also have the bases $B\otimes B$ and $B\otimes B^*$ of $H\otimes H$ and $H\otimes H^*$ respectively. We say an element $x\in H$ *contains* a term $b\in B$ if the b-coordinate of x is not zero. We can say similar things in H^*, $H\otimes H$, $H\otimes H^*$ etc..

Given subsets X and Y of a basis B, the notation X^*, $X\otimes Y$, $X\otimes Y^*$ etc. carry the obvious meanings as subsets of B^*, $B\otimes B$, $B\otimes B^*$ etc.. The meanings of phrases like X-term, X^*-term, $X\otimes Y$-term, $X\otimes Y^*$-term etc. are self-evident.

We will often make use of the duality between H and H^*, having positive bases B and B^* respectively. This allows us to turn a result about product into a result about coproduct, and vice versa. The guiding principal for doing this is the following.

Lemma 3.1. *The coefficient of $b_1^*\otimes b_2^*$ in $\Delta(b^*)$ is the same as the coefficient of b in b_1b_2. In particular, $\Delta(b^*)$ contains $b_1^*\otimes b_2^*$ if and only if b_1b_2 contains b. Similarly, we may interchange the roles of H and H^*.*

Proof. Let $b_1b_2=\sum\mu_c c$, and $\Delta(b^*)=\sum_{c_1,c_2\in B}\lambda_{c_1,c_2}c_1^*\otimes c_2^*$. Then

$$\mu_b=\langle b^*,b_1b_2\rangle=\langle\Delta(b^*),b_1\otimes b_2\rangle=\lambda_{b_1,b_2}.$$

∎

The unit element $1 \in H$ has the expression $1 = \sum_{b \in B} \epsilon(b^*)b$. Set $b' = \epsilon(b^*)b$ if $\epsilon(b^*) \neq 0$ and $b' = b$ if $\epsilon(b^*) = 0$. Then $B' = \{b' : b \in B\}$ is also a positive bases for H and

$$1 = d_1 + \cdots + d_k,$$

where $d_1, \cdots, d_k$ are distinct elements of B'. We will replace B by B' and still denote it by B.

Lemma 3.2. *$d_i d_j = \delta_{ij} d_i$ for $i, j = 1, ..., k$, and $\mathbb{C}d_1 + \cdots + \mathbb{C}d_k$ is a commutative Hopf subalgebra of H.*

Proof. From $d_i = d_i \cdot 1 = d_i d_1 + \cdots + d_i d_k$ and positivity, $d_i d_j$ is a nonnegative multiple of d_i. Similarly, from $d_j = 1 \cdot d_j$, we see that $d_i d_j$ is a nonnegative multiple of d_j. Therefore $d_i d_j = 0$ when $i \neq j$. Substituting this into $d_i = d_i d_1 + \cdots + d_i d_k$, we get $d_i = d_i d_i$.

From $\Delta(d_1) + \cdots + \Delta(d_k) = \Delta(1) = 1 \otimes 1 = \sum_{i,j} d_i \otimes d_j$ and positivity, we see that $\mathbb{C}d_1 + \cdots + \mathbb{C}d_k$ is closed under Δ.

From $S(d_1) + \cdots + S(d_k) = S(1) = 1 = d_1 + \cdots + d_k$ and positivity, we see that $\mathbb{C}d_1 + \cdots + \mathbb{C}d_k$ is closed under S.

Therefore $\mathbb{C}d_1 + \cdots + \mathbb{C}d_k$ is a commutative Hopf subalgebra of H. ∎

Commutative Hopf algebras have been well-classified: the Hopf algebra $\mathbb{C}d_1 + \cdots + \mathbb{C}d_k$ is isomorphic to the dual $(\mathbb{C}G_+)^*$ of the group algebra of a finite group G_+. More precisely, we have

$$\{d_1, \cdots, d_k\} = G_+^* = \{d_{g_+} : g_+ \in G_+\}$$

and

$$d_{g_+} d_{h_+} = \delta_{g_+, h_+} d_{g_+}, \qquad \Delta(d_{g_+}) = \sum_{h_+ k_+ = g_+} d_{h_+} \otimes d_{k_+},$$

$$S(d_{g_+}) = d_{g_+^{-1}}, \qquad 1 = \sum_{g_+ \in G_+} d_{g_+}, \qquad \epsilon(d_{g_+}) = \delta_{g_+, e}.$$

Lemma 3.3. *For any $b \in B$, there are unique $g_+, \bar{g}_+ \in G_+$ such that*

$$d_{h_+} b = \delta_{g_+, h_+} b, \qquad b d_{h_+} = \delta_{\bar{g}_+, h_+} b, \qquad \forall h_+ \in G_+.$$

Proof. From $b = 1 \cdot b = \sum_{h_+ \in G_+} d_{h_+} b$ and positivity, we have, for any $h_+ \in G_+$, $d_{h_+} b = \lambda_{h_+} b$ for some nonnegative number λ_{h_+} and not all the λ_{h_+}'s vanish. Then from $d_{g_+}d_{h_+} = \delta_{g_+,h_+}d_{g_+}$, we see that $\lambda_{g_+}\lambda_{h_+} = \delta_{g_+,h_+}\lambda_{g_+}$. Therefore all except one λ_* vanish. Moreover, the nonvanishing λ_* must be 1. ▮

Denote the unique elements in the last lemma by

$$\alpha_+(b) = g_+, \qquad \beta_+(b) = \bar{g}_+.$$

It follows from the lemma that

$$\alpha_+(b) = g_+ \Longleftrightarrow d_{g_+}b = b \Longleftrightarrow d_{g_+}b \neq 0; \tag{7}$$

$$\beta_+(b) = \bar{g}_+ \Longleftrightarrow bd_{\bar{g}_+} = b \Longleftrightarrow bd_{\bar{g}_+} \neq 0. \tag{8}$$

Set

$$\begin{aligned} B_{g_+,\bar{g}_+} &= \{b \in B : \alpha_+(b) = g_+, \beta_+(b) = \bar{g}_+\}, \\ B_{g_+,\bullet} &= \{b \in B : \alpha_+(b) = g_+\}, \\ B_{\bullet,\bar{g}_+} &= \{b \in B : \beta_+(b) = \bar{g}_+\}. \end{aligned}$$

Then B is the disjoint union of all the $B_{g_+,\bar{g}_+}$'s.

Lemma 3.4. *If b_1b_2 contains b, then*

$$\alpha_+(b_1) = \alpha_+(b), \qquad \beta_+(b_2) = \beta_+(b). \tag{9}$$

If $\Delta(b)$ contains $b_1 \otimes b_2$, then

$$\alpha_+(b) = \alpha_+(b_1)\alpha_+(b_2), \qquad \beta_+(b) = \beta_+(b_1)\beta_+(b_2). \tag{10}$$

Proof. Suppose b_1b_2 contains b. Set $g_+ = \alpha_+(b)$, $\bar{g}_+ = \beta_+(b)$. Then $b_1b_2d_{\bar{g}_+}$ and $d_{g_+}b_1b_2$ still contain $d_{g_+}b = b = bd_{\bar{g}_+}$. Therefore $b_2d_{\bar{g}_+} \neq 0$ and $d_{g_+}b_1 \neq 0$. By (7) and (8), this implies (9).

Let $\Delta(b) = \sum_{b_1,b_2\in B} \lambda_{b_1,b_2} b_1 \otimes b_2$. Then

$$\begin{aligned} \Delta(b) = \Delta(d_{g_+}b) &= \sum_{b_1,b_2\in B, h_+k_+=g_+} \lambda_{b_1,b_2} d_{h_+}b_1 \otimes d_{k_+}b_2 \\ &= \sum_{\alpha_+(b_1)=h_+,\alpha_+(b_2)=k_+,h_+k_+=g_+} \lambda_{b_1,b_2} b_1 \otimes b_2. \end{aligned}$$

Therefore $\Delta(b)$ contains only the terms $b_1 \otimes b_2$ satisfying $\alpha_+(b_1)\alpha_+(b_2) = h_+k_+ = g_+ = \alpha_+(b)$. The proof for $\beta_+(b) = \beta_+(b_1)\beta_+(b_2)$ is similar. ▮

We now dualize the discussions above.

The set B^* is a positive basis of the dual Hopf algebra H^*. In particular, we have $\epsilon = \lambda_1 e_1^* + \cdots + \lambda_l e_l^*$, where $e_i \in B$ and $\lambda_i > 0$ for $i = 1, ..., l$. Clearly, b^* appears in the sum if and only if $\epsilon(b) > 0$. Since $d_e \in G_+^*$ is the only element in G_+^* with positive ϵ-value, the intersection between $\{e_1, \cdots, e_l\}$ and G_+^* is exactly d_e. Moreover, by $1 = \epsilon(1) = \epsilon(d_e)$, we see that the coefficient of d_e^* in the summation for ϵ is 1. Thus we may rescale the e_i's to get $\epsilon = e_1^* + \cdots + e_l^*$, without affecting G_+^*.

As in Lemma 3.2, $\mathbb{C}e_1^* + \cdots + \mathbb{C}e_l^*$ is a commutative Hopf subalgebra of H^*. Therefore $\{e_1, \cdots, e_l\}$ form a group G_- under the product in H, with d_e as the unit. To indicate the group structure, we denote

$$\{e_1, \cdots, e_l\} = G_- = \{e_{g_-} : g_- \in G_-\}.$$

Then

$$e_{g_-} e_{h_-} = e_{g_- h_-}, \qquad \Delta(e_{g_-}) = e_{g_-} \otimes e_{g_-} + \text{terms not in } G_- \otimes G_-,$$

$$S(e_{g_-}) = e_{g_-^{-1}} + \text{terms not in } G_-, \qquad \epsilon = \sum_{g_- \in G_-} e_{g_-}^*.$$

Since $d_e \in G_+^*$ is also the identity of G_-, we will abuse the notation and also denote $e = d_e$.

The dual of Lemma 3.3 is the following: For any $b^* \in B^*$, we have unique $g_-, \bar{g}_- \in G_-$ such that

$$e_{h_-}^* b^* = \delta_{\bar{g}_-, h_-} b^*, \qquad b^* e_{h_-}^* = \delta_{g_-, h_-} b^*, \qquad \forall h_- \in G_-. \tag{11}$$

This enables us to define the maps $\alpha_-, \beta_- : B \to G_-$:

$$\alpha_-(b) = \bar{g}_-, \qquad \beta_-(b) = g_-.$$

We may reinterpret (11) as in the following lemma. We note that formula (12), being equivalent to (11), also serves as the characterizations of α_- and β_-.

Lemma 3.5. *Suppose $\alpha_-(b) = \bar{g}_-$ and $\beta_-(b) = g_-$. Then*

$$\Delta(b) = e_{\bar{g}_-} \otimes b + b \otimes e_{g_-} + \text{terms not in } B \otimes G_- \text{ or } G_- \otimes B. \tag{12}$$

Proof. By Lemma 3.1, the equalities $e_{h_-}^* c^* = \delta_{\alpha_-(c), h_-} c^*$ mean that $\Delta(b)$ contains $e_{h_-} \otimes c$ if and only if $c = b$ and $h_- = \alpha_-(c)$. Moreover, when the containment happens, the coefficient is 1. This means exactly that the only $G_- \otimes B$-term of $\Delta(b)$ is $e_{\alpha_-(b)} \otimes b$, and the coefficient is 1. Similarly, the only $B \otimes G_-$-term of $\Delta(b)$ is $b \otimes e_{\beta_-(b)}$, also with coefficient 1. ▮

With the help of Lemma 3.1, we may also dualize Lemma 3.4.

Lemma 3.6. *If $b_1 \otimes b_2$ is contained in $\Delta(b)$, then*

$$\alpha_-(b_1) = \alpha_-(b), \qquad \beta_-(b_2) = \beta_-(b). \tag{13}$$

If $b_1 b_2$ contains b, then

$$\alpha_-(b) = \alpha_-(b_1)\alpha_-(b_2), \qquad \beta_-(b) = \beta_-(b_1)\beta_-(b_2). \tag{14}$$

Having found G_+ and G_-, we need to further construct $G = G_+G_-$. One approach is to make use of the Drinfel'd double $D(H)$, which has $B^* \otimes B$ as a positive basis. From $D(H)$ we can also construct a "positive group" $\tilde{G}_+$ and a "negative group" $\tilde{G}_-$. The group $\tilde{G}_-$ consists of exactly the pairs $b_1^* \otimes b_2 \in B^* \otimes B$ such that

$$\epsilon(b_1^* \otimes b_2) = \langle b_1^*, 1\rangle\, \epsilon(b_2) > 0$$

Thus $\tilde{G}_- = G_+ \otimes G_-$ and this is a unique factorization. It remains to verify that $H(\tilde{G}_-; G_+, G_-)$ is isomorphic to the Hopf algebra H.

Instead of making use of the Drinfel'd double, we will continue with a more elementary approach. The approach will also be applicable to Hopf algebras in the correspondence category, where the notion of Drinfel'd double is yet to be defined.

Lemma 3.7. *The following are equivalent*
(1) $\alpha_+(b) = e$;
(2) $\beta_+(b) = e$;
(3) $b \in G_-$.
In particular, $B_{e,g_+} = B_{g_+,e} = \emptyset$ for $g_+ \neq e$.

Proof. Since $d_e = e$ is also the multiplicative unit for G_-, we see that (3) implies (1). Conversely, from the last lemma, $\Delta(b)$ contains $e_{\bar{g}_-} \otimes b$, where $\bar{g}_- = \alpha_-(b)$. Then by $\epsilon = m(S \otimes 1)\Delta$, we know that $\epsilon(b)$ contains $S(e_{\bar{g}_-})b$, which further contains $e_{\bar{g}_-^{-1}}b$. If b satisfies (1), then $e_{\bar{g}_-}\epsilon(b)$ contains $e_{\bar{g}_-}e_{\bar{g}_-^{-1}}b = d_e b = b$, so that $\epsilon(b) \neq 0$. This implies $b \in G_-$. Similarly, by using $\epsilon = m(1 \otimes S)\Delta$, we can prove that (2) and (3) are equivalent. ▮

Lemma 3.8. *Given $g_+ \in G_+$ and $g_- \in G_-$, there is a unique $B_{g_+^{-1},\bullet} \otimes B_{g_+,\bullet}$-term $c \otimes b$ contained in $\Delta(e_{g_-})$. Moreover, b is the unique element such that $\alpha_+(b) = g_+$ and $\beta_-(b) = g_-$.*

Proof. We begin by finding a $B_{g_+^{-1},\bullet} \otimes B_{g_+,\bullet}$-term in $\Delta(e_{g_-})$. Since $m(1 \otimes S)\Delta(e_{g_-}) = \epsilon(e_{g_-}) = 1 = \sum_{h_+ \in G_+} d_{h_+}$, $\Delta(e_{g_-})$ must contain a term $c \otimes b$ such that $cS(b) = \sum_{h_+ \in G_+} \lambda_{h_+} d_{h_+}$ with $\lambda_{g_+^{-1}} > 0$. Then we have $d_{g_+^{-1}} cS(b) = \lambda_{g_+^{-1}} d_{g_+^{-1}}$. Thus $d_{g_+^{-1}} c \neq 0$, and by (7), $\alpha_+(c) = g_+^{-1}$. Then by Lemmas 3.4, 3.6, and 3.7, we have $\alpha_+(b) = \alpha_+(c)^{-1}\alpha_+(e_{g_-}) = g_+$.

Next we would like to compare the $B_{g_+,\bullet} \otimes B_{g_+^{-1},\bullet} \otimes B_{g_+,\bullet}$-terms in $(\Delta \otimes 1)\Delta(b)$ and $(1 \otimes \Delta)\Delta(b)$. For $(\Delta \otimes 1)\Delta(b)$, such terms can only be obtained from applying $\Delta \otimes 1$ to $B \otimes B_{g_+,\bullet}$-terms in $\Delta(b)$. Now for any $B \otimes B_{g_+,\bullet}$-term $b_1 \otimes b_2$ contained in $\Delta(b)$, we apply Lemma 3.4 and find $g_+ = \alpha_+(b) = \alpha_+(b_1)\alpha_+(b_2) = \alpha_+(b_1)g_+$. Therefore $\alpha_+(b_1) = e$, so that by Lemma 3.7, we have $b_1 \in G_-$. Thus $b_1 \otimes b_2$ is really a $G_- \otimes B_{g_+,\bullet}$-term contained in $\Delta(b)$. It then follows from Lemma 3.5 that $b_1 \otimes b_2 = e_{\bar{g}_-} \otimes b$, where $\bar{g}_- = \alpha_-(b)$, and the $B_{g_+,\bullet} \otimes B_{g_+^{-1},\bullet} \otimes B_{g_+,\bullet}$-terms in $(\Delta \otimes 1)\Delta(b)$ come from $\Delta(e_{\bar{g}_-}) \otimes b$. Similarly, the $B_{g_+,\bullet} \otimes B_{g_+^{-1},\bullet} \otimes B_{g_+,\bullet}$-terms in $(1 \otimes \Delta)\Delta(b)$ come from $b \otimes \Delta(e_{g_-})$.

Let $\sum_i \lambda_i c_i \otimes b_i$ be all the $B_{g_+^{-1},\bullet} \otimes B_{g_+,\bullet}$-terms in $\Delta(e_{g_-})$. Let $\sum_j \lambda'_j b'_j \otimes c'_j$ be all the $B_{g_+,\bullet} \otimes B_{g_+^{-1},\bullet}$-terms in $\Delta(e_{\bar{g}_-})$. Then by comparing the $B_{g_+,\bullet} \otimes B_{g_+^{-1},\bullet} \otimes B_{g_+,\bullet}$-terms in $\Delta(e_{\bar{g}_-}) \otimes b$ and $b \otimes \Delta(e_{g_-})$, we get

$$\sum_i \lambda_i b \otimes c_i \otimes b_i = \sum_j \lambda'_j b'_j \otimes c'_j \otimes b.$$

Consequently, all $b_i = b$, all $b'_j = b$, and

$$\Delta(e_{g_-}) = (\sum_i \lambda_i c_i) \otimes b + \text{no } B_{g_+^{-1},\bullet} \otimes B_{g_+,\bullet}\text{-terms} \tag{15}$$

$$\Delta(e_{\bar{g}_-}) = b \otimes (\sum_i \lambda_i c_i) + \text{no } B_{g_+,\bullet} \otimes B_{g_+^{-1},\bullet}\text{-terms} \tag{16}$$

The equality (15) shows that for any $g_+ \in G_+$ and $g_- \in G_-$, all the $B_{g_+^{-1},\bullet} \otimes B_{g_+,\bullet}$-terms in $\Delta(e_{g_-})$ have the same right component. Now apply this fact to $g_+^{-1} \in G_+$ and $\bar{g}_- \in G_-$, we see that all the $B_{g_+,\bullet} \otimes B_{g_+^{-1},\bullet}$-terms in $\Delta(e_{\bar{g}_-})$ have the same right component. Then (16) tells us that $\sum_i \lambda_i c_i$ is really only one term. We thus conclude that for any $g_+ \in G_+$ and $g_- \in G_-$, the $B_{g_+^{-1},\bullet} \otimes B_{g_+,\bullet}$-term in $\Delta(e_{g_-})$ is unique.

Now let us prove the uniqueness of the element b satisfying $\alpha_+(b) = g_+$ and $\beta_-(b) = g_-$. We already have one such element appearing in

$$\Delta(e_{g_-}) = c \otimes b + \text{no } B_{g_+^{-1},\bullet} \otimes B_{g_+,\bullet}\text{-terms}$$

Now suppose b' is another basis element satisfying $\alpha_+(b') = g_+$ and $\beta_-(b') = g_-$. Let $\alpha_-(b') = \bar{g'}_-$. As before, we write (we do not know a priori that $\bar{g'}_- = \bar{g}_-$)

$$\Delta(b') = e_{\bar{g'}_-} \otimes b' + b' \otimes e_{g_-} + \text{terms not in } B \otimes G_- \text{ or } G_- \otimes B$$

and compare the $B_{g_+,\bullet} \otimes B_{g_+^{-1},\bullet} \otimes B_{g_+,\bullet}$-terms in $(\Delta \otimes 1)\Delta(b')$ and $(1 \otimes \Delta)\Delta(b')$. We get

$$[B_{g_+,\bullet} \otimes B_{g_+^{-1},\bullet}\text{-term in } \Delta(e_{\bar{g'}_-})] \otimes b' = b' \otimes c \otimes b.$$

Comparing the rightmost components, we conclude that $b = b'$. ∎

We make some remarks about the lemma above.

First of all, observe that $c \otimes b$ is also the unique $B \otimes B_{g_+,\bullet}$-term (as well as the unique $B_{g_+^{-1},\bullet} \otimes B$-term) in $\Delta(e_{g_-})$. As a matter of fact, by Lemma 3.4, any $B \otimes B_{g_+,\bullet}$-term in $\Delta(e_{g_-})$ must be a $B_{g_+^{-1},\bullet} \otimes B_{g_+,\bullet}$-term.

Secondly, if we start with $\bar{g}_+ \in G_+$ and $\bar{g}_- \in G_-$, similar proof also tells us that there is a unique $B_{\bullet,\bar{g}_+} \otimes B_{\bullet,\bar{g}_+^{-1}}$-term $b \otimes c$ contained in $\Delta(e_{\bar{g}_-})$. Moreover, b is the unique element such that $\beta_+(b) = \bar{g}_+$ and $\alpha_-(b) = \bar{g}_-$. Briefly speaking, one may start with $m(S \otimes 1)\Delta(e_{\bar{g}_-}) = 1$ and conclude $\Delta(e_{\bar{g}_-})$ contains a $B_{\bullet,\bar{g}_+} \otimes B_{\bullet,\bar{g}_+^{-1}}$-term $b \otimes c$. Then by comparing the $B_{\bullet,\bar{g}_+} \otimes B_{\bullet,\bar{g}_+^{-1}} \otimes B_{\bullet,\bar{g}_+}$-terms in $(\Delta \otimes 1)\Delta(b)$ and $(1 \otimes \Delta)\Delta(b)$, our claim follows. In particular, we also see that $b \to (\beta_+(b), \alpha_-(b))$ is a one-to-one correspondence between B and $G_+ \times G_-$.

Thirdly, we have the one-to-one correspondences

$$(g_+, g_-) \overset{(\alpha_+,\beta_-)}{\longleftarrow} b \overset{(\beta_+,\alpha_-)}{\longrightarrow} (\bar{g}_+, \bar{g}_-), \tag{17}$$

and the equalities

$$\Delta(e_{g_-}) = \lambda c \otimes b + \cdots \tag{18}$$

$$\Delta(e_{\bar{g}_-}) = \lambda b \otimes c + \cdots \tag{19}$$

The one-to-one correspondences in (17) enable us to define a right action of G_- on G_+

$$G_+ \times G_- \to G_+ : \qquad (g_+, g_-) \mapsto g_+^{g_-} = \bar{g}_+, \tag{20}$$

and a left action of G_+ on G_-

$$G_+ \times G_- \to G_- : \qquad (g_+, g_-) \mapsto {}^{g_+}g_- = \bar{g}_-. \tag{21}$$

In Lemma 3.12, we will show that they are the actions (4) and (5) in our standard model and that they satisfy the matching relations (6).

The action (20) has the following interpretation: Given g_+ and g_-, we use (18) to find the unique $b \in B_{g_+,\bullet}$. Then $\bar{g}_+ = \beta_+(b)$ is ${}^{g_-}g_+$ (i.e., $b \in B_{g_+,\bar{g}_+}$).

The action (21) has the following interpretation: Given g_+ and g_-, we establish (18) and (19) with $b \in B_{g_+,\bullet}$. Then the element $\bar{g}_-$ in (19) is $g_-^{g_+}$.

The reason for the interpretations above follows from (15), (16), and the uniqueness. We may also find g_+, g_- from $(\bar{g}_+, \bar{g}_-)$ in the similar way. These are the other two actions in the standard model, and we will not use them.

Lemma 3.9. *For any $b \in B_{g_+,\bar{g}_+}$, there is $b' \in B_{\bar{g}_+,g_+}$ such that $bb' = \lambda d_{g_+}$ and $b'b = \lambda d_{\bar{g}_+}$ for some $\lambda > 0$.*

Proof. Let $\beta_-(b) = g_-$. From Lemma 3.8 and the first two of the subsequent remarks, we have a unique $B \otimes B_{\bullet,\bar{g}_+}$-term $c \otimes b$ in $\Delta(e_{g_-})$. Then by $m(S \otimes 1)\Delta(e_{g_-}) = \epsilon(e_{g_-}) = 1$, we have $S(c)b = \mu d_{\bar{g}_+}$ for some $\mu > 0$. By positivity, there is some term b' in $S(c)$ such that $b'b = \lambda d_{\bar{g}_+}$ for some $\lambda > 0$.

We claim that $b' \in B_{\bar{g}_+,g_+}$. From $d_{\bar{g}_+}b'b = \lambda d_{\bar{g}_+}^2 = \lambda d_{\bar{g}_+} \neq 0$, we have $d_{\bar{g}_+}b' \neq 0$, so that $\alpha_+(b') = \bar{g}_+$. From $(b'd_{g_+})b = b'(d_{g_+}b) = b'b = \lambda d_{\bar{g}_+} \neq 0$, we have $b'd_{g_+} \neq 0$, so that $\beta_+(b') = g_+$.

We have shown that for any $b \in B_{g_+,\bar{g}_+}$, there is $b' \in B_{\bar{g}_+,g_+}$ such that $b'b = \lambda d_{\bar{g}_+}$ for some $\lambda > 0$. Applying this conclusion to b', there is $b'' \in B_{g_+,\bar{g}_+}$ such that $b''b' = \lambda' d_{g_+}$ for some $\lambda' > 0$. Then we have

$$b''b'b = (b''b')b = \lambda' d_{g_+}b = \lambda' b, \qquad b''b'b = b''(b'b) = \lambda b'' d_{\bar{g}_+} = \lambda b''.$$

This implies that $\lambda = \lambda'$ and $b'' = b$. ∎

The next lemma shows that the antipode S is a permutation on B up to rescaling. We give a proof that is also valid in the correspondence category. For Hopf algebras over $\mathbb{C}$, it can also be proved more directly by using the positivity of S and the fact that $S^N = id$ for some positive integer N.

Lemma 3.10. *Given any $b \in B$, $S(b) = \lambda b'$ for some $b' \in B$ and $\lambda > 0$. Moreover, we have $\alpha_-(b') = \beta_-(b)^{-1}$, $\beta_+(b') = \alpha_+(b)^{-1}$, and these uniquely determine b'.*

Proof. First we show that $S(e_{g_-}) = e_{g_-^{-1}}$ for any $g_- \in G_-$. We already know $S(e_{g_-}) = e_{g_-^{-1}}$ + terms not in G_-. Suppose $g_- \neq e$, and $S(e_{g_-})$ contains $b \notin G_-$. Then by Lemma 3.7, $h_+ = \alpha_+(b) \neq e$, so that $d_{h_+}S(e_{g_-}) = S(e_{g_-}d_{h_+^{-1}}) = 0$. On the other hand, $d_{h_+}S(e_{g_-})$ still contains $d_{h_+}b = b$ and cannot vanish. The contradiction shows that $S(e_{g_-}) = e_{g_-^{-1}}$. On the other hand, suppose $g_- = e$. Then we already know $e_{g_-} = d_e$ and $S(d_e) = d_e$.

Let $g_\pm$ and $\bar{g}_\pm$ be associated to b as in (17). Then from Lemma 3.8 we have

$$\Delta(e_{g_-}) = \lambda c \otimes b + \cdots$$

Applying S, we have

$$\Delta(e_{g_-^{-1}}) = \lambda S(b) \otimes S(c) + \cdots$$

The proof of the last lemma implies that $S(c)$ contains a term $c' \in B_{g_+,\bar{g}_+}$. Therefore if $S(b)$ contains b', then $b' \otimes c'$ must be contained in $\Delta(e_{g_-^{-1}})$. By the first remark after Lemma 3.8, the $B \otimes B_{g_+,\bar{g}_+}$-term in $\Delta(e_{g_-^{-1}})$ must be unique. Therefore for the fixed c', there is only one term like $b' \otimes c'$ in $\Delta(e_{g_-^{-1}})$. This implies that there is only one term, a constant multiple of b', contained in $S(b)$.

Thus we conclude the first part of the lemma, and have

$$S(b) = \mu b', \quad S(c) = \nu c', \qquad \Delta(e_{g_-^{-1}}) = \lambda\mu\nu b' \otimes c' + \cdots.$$

Moreover, we have also assumed that $c' \in B_{g_+,\bar{g}_+}$. By Lemmas 3.4 and 3.6, we know that $\alpha_-(b') = \beta_-(b)^{-1}$ and $\beta_+(b') = \alpha_+(b)^{-1}$. By the second remark after Lemma 3.8, this uniquely determines b'. ∎

Lemma 3.11. *For $b \in B_{g_+,\bar{g}_+}$ and $c \in B_{h_+,\bar{h}_+}$, there are two possibilities for bc:*

(1) *If $\bar{g}_+ = h_+$, then bc is a positive multiple of an element in $B_{g_+,\bar{h}_+}$;*
(2) *If $\bar{g}_+ \neq h_+$, then $bc = 0$.*

Proof. If $\bar{g}_+ \neq h_+$, then $bc = (bd_{\bar{g}_+})(d_{h_+}c) = b(d_{\bar{g}_+}d_{h_+})c = 0$.

If $\bar{g}_+ = h_+$, then Lemma 3.9 immediately implies $bc \neq 0$. Suppose bc contains two different terms $d, d' \in B$. Then by $d_{g_+}bc = bc = bcd_{\bar{h}_+}$ and positivity, we see that $d, d' \in B_{g_+,\bar{h}_+}$. By Lemma 3.9, there is $b' \in B_{\bar{g}_+,g_+}$ such that $bb' = \lambda d_{g_+}$ and $b'b = \lambda d_{\bar{g}_+}$ for some $\lambda > 0$. Then $b'bc = \lambda c$ contains $b'd$ and $b'd'$. By positivity, we must have $b'd = \mu c$ and $b'd' = \mu' c$

for some $\mu > 0$ and $\mu' > 0$. Thus

$$\lambda d = \lambda d_{g_+} d = bb'd = \mu bc, \qquad \lambda d' = \lambda d_{g_+} d' = bb'd' = \mu' bc.$$

This is in contradiction with the assumption that d and d' are distinct. ▮

Lemma 3.10 implies that S^{-1} exists, and for any $b \in B$, the coordinates of $S^{-1}(b)$ are non-negative. Therefore B^* is also a positive basis for $(H^*)^{op}$. In particular, all the proofs we have done so far are valid in $(H^*)^{op}$. Note that the two actions (20) and (21) are related by duality in the following way.

H	H^*	$(H^*)^{op}$
$\alpha_+(b) = g_+$	$\alpha_-(b^*) = \bar{g}_-$	$\alpha_-^{op}(b^*) = g_-$
$\beta_+(b) = \bar{g}_+$	$\beta_-(b^*) = g_-$	$\beta_-^{op}(b^*) = \bar{g}_-$
$\alpha_-(b) = \bar{g}_-$	$\alpha_+(b^*) = g_+$	$\alpha_+^{op}(b^*) = \bar{g}_+$
$\beta_-(b) = g_-$	$\beta_+(b^*) = \bar{g}_+$	$\beta_+^{op}(b^*) = g_+$
$\bar{g}_+ = g_+^{g_-}$	$g_- = \bar{g}_-^{\bar{g}_+}$	$\bar{g}_- = {}^{g_+}g_-$
$\bar{g}_- = {}^{g_+}g_-$	$g_+ = {}^{\bar{g}_-}\bar{g}_+$	$\bar{g}_+ = g_+^{g_-}$

Therefore by restating the results we have proved in $(H^*)^{op}$, we may exchange the two actions in these results.

Lemma 3.12. (20) *and* (21) *are indeed actions. Moreover, the two actions satisfy the matching relations* (6).

Proof. Given $g_+^{g_-} = h_+$ and $h_+^{h_-} = k_+$, we may find (by the third remark after Lemma 3.8) $b \in B_{g_+,h_+}$ and $b' \in B_{h_+,k_+}$, with $g_- = \beta_-(b)$ and $h_- = \beta_-(b')$. Then by Lemma 3.11, we have $bb' = \lambda c$, with $\lambda > 0$ and $c \in B_{g_+,k_+}$. By Lemma 3.6, we have $\beta_-(c) = g_-h_-$. Therefore $g_+^{g_-h_-} = k_+ = h_+^{h_-} = (g_+^{g_-})^{h_-}$. This proves (20) is a right action.

As explained in the remark above, we may exchange the two actions and still get an equality. Applying the principle to $g_+^{g_-h_-} = (g_+^{g_-})^{h_-}$, we get ${}^{h_+g_+}g_- = {}^{h_+}({}^{g_+}g_-)$. This proves (21) is a left action.

Now we prove the matching relations. By the third remark after Lemma 3.8, we interpret the actions $\bar{g}_+ = g_+^{g_-}$ and $\bar{g}_- = {}^{g_+}g_-$ as the following equalities

$$\begin{cases} \Delta(e_{g_-}) = \lambda c \otimes b + \cdots, \\ \Delta(e_{\bar{g}_-}) = \lambda b \otimes c + \cdots, \end{cases} \qquad b \in B_{g_+,\bar{g}_+}. \tag{22}$$

We also interpret the action $\bar{h}_- = {}^{\bar{g}_+}h_-$ as the following equalities

$$\begin{cases} \Delta(e_{h_-}) &= \lambda' c' \otimes b' + \cdots, \\ \Delta(e_{\bar{h}_-}) &= \lambda' b' \otimes c' + \cdots, \end{cases} \qquad b \in B_{\bar{g}_+,\bullet}. \tag{23}$$

Multiplying (22) and (23) together, we have (using Lemma 3.11 so that cc' and bb' are elements of B up positive rescaling)

$$\begin{cases} \Delta(e_{g_-h_-}) = \Delta(e_{g_-})\Delta(e_{h_-}) &= \lambda\lambda' cc' \otimes bb' + \cdots, \\ \Delta(e_{\bar{g}_-\bar{h}_-}) = \Delta(e_{\bar{g}_-})\Delta(e_{\bar{h}_-}) &= \lambda\lambda' bb' \otimes cc' + \cdots, \end{cases} \qquad bb' \in B_{g_+,\bullet}. \tag{24}$$

By the third remark after Lemma 3.8, (24) means $\bar{g}_-\bar{h}_- = {}^{g_+}(g_-h_-)$. Therefore

$${}^{g_+}(g_-h_-) = \bar{g}_-\bar{h}_- = {}^{g_+}g_- \; {}^{\bar{g}_+}h_- = {}^{g_+}g_- \; {}^{(g_+^{g_-})}h_-.$$

This is the matching relation. Applying the remark before the lemma, we get the other matching relation

$$(h_+g_+)^{g_-} = h_+^{({}^{g_+}g_-)} \, g_+^{g_-}.$$

∎

With a matching pair of groups G_+, G_-, we may construct a group $G = G_+G_-$ and projections $\alpha_\pm, \beta_\pm : G \to G_\pm$. Furthermore, we have a standard Hopf algebra $H(G; G_+, G_-)$ with G as a positive basis. The next Lemma shows that up to positive scaling, the product between the basis elements of H is the same as the product between the basis elements of $H(G; G_+, G_-)$.

Lemma 3.13. *bb' is a positive multiple of c if and only if*

$$\alpha_+(b) = \alpha_+(c), \qquad \beta_+(b) = \alpha_+(b'), \qquad \alpha_-(b)\alpha_-(b') = \alpha_-(c).$$

Moreover, for fixed c, $(b, b') \mapsto \alpha_-(b)$ is a one-to-one correspondence between the pairs (b, b') and G_-.

Proof. The necessity follows from (9), (14), and Lemma 3.11. For sufficiency, the condition $\beta_+(b) = \alpha_+(b')$ implies $bb' = \lambda c'$ for some $\lambda > 0$ and $c' \in B$. Then we have $\alpha_+(c) = \alpha_+(b) = \alpha_+(c')$ and $\alpha_-(c) = \alpha_-(b)\alpha_-(b') = \alpha_-(c')$. If we can show $(\alpha_+(c), \alpha_-(c))$ are in one-to-one correspondence with $(\alpha_+(c), \beta_-(c))$, then it follows from Lemma 3.8 that $c = c'$.

By the definition of the action of G_+ on G_-, from $(\alpha_+(c), \beta_-(c))$ we have $\alpha_-(c) = {}^{\alpha_+(c)}\beta_-(c)$. Since this is a group action, from $(\alpha_+(c), \beta_-(c))$ we also have $\beta_-(c) = {}^{\alpha_+(c)^{-1}}\alpha_-(c)$. This proves the sufficiency.

For the one-to-one correspondence, we fix $\alpha_-(b) \in G_-$. The condition $\alpha_+(b) = \alpha_+(c)$ then uniquely determines b. Moreover, the conditions $\beta_+(b) = \alpha_+(b')$, $\alpha_-(b)\alpha_-(b') = \alpha_-(c)$ give us $\alpha_+(b')$ and $\alpha_-(b')$, which also has a unique corresponding b'. This proves the one-to-one correspondence between pairs (b, b') and G_-. ∎

By making use of Lemma 3.1 and the remark before Lemma 3.12, we get the following dual of Lemma 3.13. It shows that up to positive scaling, the coproduct of basis elements of H is the same as the coproduct of basis elements of $H(G; G_+, G_-)$.

Lemma 3.14. *For any $b \in B$, $\Delta(b)$ contains exactly those $c \otimes c'$ satisfying*

$$\alpha_-(c) = \alpha_-(b), \quad \beta_-(c) = \alpha_-(c'), \quad \alpha_+(c)\alpha_+(c') = \alpha_+(b).$$

Moreover, for fixed b, $c \otimes c' \mapsto \alpha_+(c)$ is a one-to-one correspondence between $c \otimes c'$ and G_+.

4. RESCALING

Given a finite dimensional Hopf algebra H with a positive basis B, we have identified H with a standard Hopf algebra $H(G; G_+, G_-)$ (as well as B with G) up to positive scaling. In this section, we will rescale the elements of G by positive scalars so that the Hopf algebra structure in H and $H(G; G_+, G_-)$ are exactly the same.

The problem may be viewed in the following way. On the vector space $V = \mathbb{C}G$, we have the standard Hopf algebra structure $H(G; G_+, G_-)$. We also have the given Hopf algebra structure H. The problem is to find a function $\tau : G \to \mathbb{R}_+$ such that $g \mapsto \tau(g)g$ is a Hopf algebra isomorphism from H to $H(G; G_+, G_-)$.

The Hopf algebra structure H is determined by

$$\begin{aligned} \{g\}\{h\} &= \begin{cases} \lambda(g,h)\{gh_-\} & \text{in case } \bar{g}_+ = h_+ \\ 0 & \text{in case } \bar{g}_+ \neq h_+ \end{cases} \\ \Delta\{g\} &= \sum_{h_+ k = g, \bar{k}_- = h_-} \mu(h,k)\{h\} \otimes \{k\} \\ S\{g\} &= \nu(g)\{g^{-1}\} \end{aligned} \tag{25}$$

The structure constants $\lambda(g,h)$, $\mu(h,k)$, $\nu(g)$ are positive and defined exactly when the conditions indicated above are satisfied. We assume H is already well-scaled on G_+^* and G_-, i.e., with canonical products, coproducts, and antipodes, $(\mathbb{C}G_+)^*$ is a sub-Hopf algebra of H and $(\mathbb{C}G_-)^*$ is a sub Hopf algebras of H^*. Then the Hopf algebra condition means the following compatibility equations (in cases both sides are defined):

$$\begin{aligned}
\lambda(g,h)\lambda(gh_-,k) &= \lambda(g,hk_-)\lambda(h,k),\\
\mu(g,h)\mu(g_+h,k) &= \mu(g,h_+k)\mu(h,k),\\
\lambda(h_+k,h'_+k')\mu(hh'_-,kk'_-) &= \lambda(h,h')\lambda(k,k')\mu(h,k)\mu(h',k'),\\
\lambda(h_+,h) &= 1,\\
\lambda(h,\bar{h}_+) &= 1,\\
\mu(h,h_-) &= 1,\\
\mu(\bar{h}_-,h) &= 1,\\
\nu(h)\lambda(h^{-1},h_+^{-1}\bar{h}_-) &= 1,\\
\nu(h)\lambda(h_+^{-1}\bar{h}_-,h) &= 1.
\end{aligned}$$

It is clear from the equations above that for any real number ϵ, λ^ϵ, μ^ϵ, ν^ϵ still satisfy the compatibility equations. Therefore if we replace λ, μ, ν in (25) with λ^ϵ, μ^ϵ, ν^ϵ, we still get a Hopf algebra (which is also well-scaled on G_+^* and G_-), which we denote by H_ϵ. Then we have $H = H_1$ and $H(G;G_+,G_-) = H_0$.

Lemma 4.15. *The Hopf algebras H_ϵ are semisimple and cosemisimple.*

Proof. Let $\Lambda = \sum_{g_-\in G_-}\{g_-\}$. Because H_ϵ is already well-scaled on G_-, we have $x\Lambda = \epsilon(x)\Lambda$. Therefore Λ is a left integral of the Hopf algebra. Since $\epsilon(\Lambda) = |G_-| \neq 0$, it follows from [6] that H_ϵ is semi-simple.

Similarly, the integral $\sum_{g_+\in G_+}\{g_+\}^*$ tells us that H_ϵ^* is also semi-simple. ∎

Consider H_0 as a point in the space X of all bialgebra structures on V. We have natural action of the general linear group $GL(V)$ on X. The orbit $GL(V)H_0$ consists of all the bialgebra structures linearly isomorphic to H_0. According to Corollary 1.5 and Theorem 2.1 of [15], the semisimplicity and the cosemisimplicity of H_0 implies that the orbit $GL(V)H_0$ is a Zariski open subset of X. Therefore for sufficiently small ϵ, H_ϵ belongs to the orbit $GL(V)H_0$. In particular, for any $\delta > 0$, we can find an $\epsilon > 0$ and a linear transformation T, such that $T(H_\epsilon) = H_0$ and

$$T\{g\} = \sum_{h\in G}\tau_{g,h}\{h\}, \quad |\tau_{g,g}-1| < \delta, \quad |\tau_{g,h}| < \delta \quad \text{for } h \neq g. \qquad (26)$$

Lemma 4.16. *For sufficiently small ϵ, T preserves $\mathbb{C}G_-$.*

Proof. Consider $T\{g_-\} = \sum_{h\in G} \tau_{g_-,h}\{h\}$. We would like to show $\tau_{g_-,h} = 0$ for $h \notin G_-$. If not, we find a term $\tau_{g_-,k}\{k\}$, $k \notin G_-$, with

$$|\tau_{g_-,k}| = \max\{|\tau_{g_-,h}| : h \notin G_-\}.$$

Since $k \notin G_-$, we have $k_+ \neq e$. Therefore $\{k_+\}\{g_-\} = 0$ in H_ϵ. Since T preserves products, we have $T\{k_+\}T\{g_-\} = 0$. On the other hand, we will show that for sufficiently small ϵ, the coefficient of $\{k\}$ in $T\{k_+\}T\{g_-\}$ cannot be zero. The contradiction proves the Lemma.

Write

$$\begin{aligned} T\{k_+\} &= \tau_{k_+,k_+}\{k_+\} + \sum_{h\neq k_+} \tau_{k_+,h}\{h\} = P + Q; \\ T\{g_-\} &= \tau_{g_-,k}\{k\} + \sum_{h\in G_-} \tau_{g_-,h}\{h\} + \sum_{h\notin G_-, h\neq k} \tau_{g_-,h}\{h\} = L + M + N. \end{aligned}$$

Suppose (26) is satisfied for some small $\delta > 0$. Then we have

1. $PL = \tau_{k_+,k_+}\tau_{g_-,k}\{k\}$, with $|\tau_{k_+,k_+}\tau_{g_-,k}| \geq (1-\delta)|\tau_{g_-,k}|$;
2. $P(M+N)$ can never produce $\{k\}$;
3. $Q(L+N)$ may produce some $\{k\}$-terms. However, the total number of product terms is no more than $(\dim H)^2$, and the coefficients are all smaller than $\delta|\tau_{g_-,k}|$. Therefore the k-coefficient of this part is bounded by $\delta|\tau_{g_-,k}|(\dim H)^2$;
4. QM is a sum of G_--terms, so that it can never produce $\{k\}$.

Now for sufficiently small ϵ, we can find T satisfying (26), with δ small enough so that $(1-\delta) > \delta(\dim H)^2$. Then we conclude that the $\{k\}$-term in $T\{k_+\}T\{g_-\}$ is nontrivial. ∎

Lemma 4.17. *For sufficiently small ϵ, $T(\mathbb{C}(G_+ - \{e\})) \subset \mathbb{C}(G - G_-)$.*

Proof. For any $g_+ \in G_+$, $g_+ \neq e$, write

$$T\{g_+\} = \sum_{h_-\in G_-} \tau_{g_+,h_-}\{h_-\} + \sum_{h\notin G_-} \tau_{g_+,h}\{h\} = P + Q.$$

If P is not zero, we have some $k_- \in G_-$ such that

$$|\tau_{g_+,k_-}| = \max\{|\tau_{g_+,h_-}| : h_- \in G_-\}.$$

Since $g_+ \neq e$, we have $\{g_+\}\{e\} = 0$ in H_ϵ, which implies $T\{g_+\}T\{e\} = 0$. On the other hand, we will show that for sufficiently small ϵ, the coefficient of $\{k_-\}$ in $T\{g_+\}T\{e\}$ cannot be zero. The contradiction proves the lemma.

For sufficiently small ϵ, we have

$$T\{e\} = \tau_{e,e}\{e\} + \sum_{h_- \in G_-, h_- \neq e} \tau_{e,h_-}\{h_-\} = L + M$$

from Lemma 4.16. Suppose (26) is further satisfied for some small $\delta > 0$. Then we have

1. The k_--term in PL is $\tau_{g_+,k_-}\tau_{e,e}\{k_-\}$ with $|\tau_{g_+,k_-}\tau_{e,e}| > (1-\delta)|\tau_{g_+,k_-}|$;
2. PM may have some $\{k\}$-terms, but the total number of product terms is no more than $|G_-|^2$, and the coefficients are all smaller than $\delta|\tau_{g_+,k_-}|$. Thus the k-coefficient of this part is bounded by $\delta|\tau_{g_+,k_-}||G_-|^2$;
3. $Q(L+M)$ is contains no G_--terms, so that it can never produce $\{k_-\}$.

Now for sufficiently small ϵ, we can find T satisfying Lemma 4.16 and (26), with δ small enough so that $(1-\delta) > \delta|G_-|^2$. Then we conclude that the $\{k_-\}$-term in $T\{g_+\}T\{e\}$ is nontrivial. ▮

LEMMA 4.18. *For sufficiently small ϵ, T preserves $\mathbb{C}(G - G_-)$.*

Proof. Let $g \notin G_-$. Then $g_+ \neq e$, so that by Lemma 4.17, $T\{g_+\}$ contains no G_--terms.

In H_ϵ, we have $\{g_+\}\{g\} = \{g\}$, which implies $T\{g\} = T\{g_+\}T\{g\}$. Since $T\{g_+\}$ contains no G_--terms, $T\{g_+\}T\{g\}$ also contains no G_--terms. Consequently, $T\{g\}$ contains no G_--terms. ▮

Lemmas 4.16 and 4.18 shows that if we decompose $\mathbb{C}G$ into $\mathbb{C}G_- \oplus \mathbb{C}(G - G_-)$, then $T : H_\epsilon \to H_0$ takes the form

$$T = \begin{pmatrix} * & 0 \\ 0 & * \end{pmatrix} \begin{matrix} \leftarrow G_- \\ \leftarrow G - G_- \end{matrix} . \tag{27}$$

Now we apply this to the dual $(T^*)^{-1} : H_\epsilon^* \to H_0^*$. Of course to do so may require the choice of an even smaller ϵ, so that all the lemmas work for $(T^*)^{-1}$. Since the groups G_+ and G_- derived from H^* are the same as the groups G_- and G_+ derived from H, we conclude that with regard to the decomposition $(\mathbb{C}G)^* = (\mathbb{C}G_+)^* \oplus (\mathbb{C}(G - G_+))^*$,

$$(T^*)^{-1} = \begin{pmatrix} * & 0 \\ 0 & * \end{pmatrix} \begin{matrix} \leftarrow G_+^* \\ \leftarrow G^* - G_+^* \end{matrix} .$$

Consequently, we get

$$T = \begin{pmatrix} * & 0 \\ 0 & * \end{pmatrix} \begin{matrix} \leftarrow G_+ \\ \leftarrow G - G_+ \end{matrix}.$$

In particular, T preserves $(\mathbb{C}G_+)^*$.

LEMMA 4.19. *For sufficiently small ϵ, T is identity on G_+.*

Proof. Let $g_+ \in G_+$. For sufficiently small ϵ, from the discussion above we have

$$T\{g_+\} = \sum_{h_+ \in G_+} \tau_{g_+,h_+}\{h_+\},$$

where τ_{g_+,g_+} is close to 1 and τ_{g_+,h_+} is small for $h_+ \neq g_+$. Moreover, since H_ϵ is already well-scaled on G_+^*, we have $\{g_+\}^2 = \{g_+\}$ in H_ϵ. Therefore in H_0, we have

$$\sum_{h_+ \in G_+} \tau_{g_+,h_+}\{h_+\} = T\{g_+\} = (T\{g_+\})^2 = \sum_{h_+ \in G_+} \tau_{g_+,h_+}^2\{h_+\}.$$

Comparing the two sides, we have $\tau_{g_+,h_+} = \tau_{g_+,h_+}^2$. Since τ_{g_+,g_+} is the only coefficient close to 1, we conclude that $\tau_{g_+,h_+} = \delta_{g_+,h_+}$. ∎

The lemma also applies to the dual Hopf algebras. Taking the adjoint and then the inverse of (27), we have

$$(T^*)^{-1} = \begin{pmatrix} * & 0 \\ 0 & * \end{pmatrix} \begin{matrix} \leftarrow G_-^* \\ \leftarrow G^* - G_-^* \end{matrix}. \tag{28}$$

Since G_-^* in H^* plays the role of G_+ in H, the dual of Lemma 4.19 then shows that $(T^*)^{-1}$ is identity on G_-^*, so that

$$(T^*)^{-1} = \begin{pmatrix} I & 0 \\ 0 & * \end{pmatrix} \begin{matrix} \leftarrow G_-^* \\ \leftarrow G^* - G_-^* \end{matrix}. \tag{29}$$

By taking the inverse and then the adjoint of (29), we see that T is also identity on G_-.

Having proved T is identity on $G_\pm$, we are ready to show T is a scaling everywhere.

LEMMA 4.20. *For sufficiently small ϵ, T is a scaling on G.*

Proof. For any $g = g_+g_- \in G$, we have $\{g_+\}\{g\} = \{g\}$ in H_ϵ and $T\{g_+\} = \{g_+\}$. Then $T\{g\} = T(\{g_+\}\{g\}) = \{g_+\}T\{g\}$ implies that $T\{g\}$ is a linear combination of terms $\{h\}$ with $h_+ = g_+$. This is equivalent to the fact that, with regard to the disjoint union decomposition $\coprod_{g_+\in G_+}\{h \in G : \alpha_+(h) = g_+\}$, the matrix of T is a block diagonal one.

Similarly, the matrix of $(T^*)^{-1}$ is a block diagonal one with regard to the decomposition $\coprod_{g_-\in G_-}\{h^* \in G^* : \beta_-(h) = g_-\}$. Therefore the matrix of T is also block diagonal with regard to the decomposition $\coprod_{g_-\in G_-}\{h \in G : \beta_-(h) = g_-\}$. This is equivalent to $T\{g\}$ is a linear combination of terms $\{h\}$ with $h_- = g_-$.

Thus we conclude that $T\{g\}$ is a linear combination of terms $\{h\}$ with $h_+ = g_+$ and $h_- = g_-$. There is only one such term, namely $\{g\}$. Therefore $T\{g\}$ is a scalar multiple of $\{g\}$. ∎

The fact that $g \mapsto \tau(g)g$ is a Hopf algebra isomorphism from H_ϵ to H_0 means exactly the following equalities

$$\begin{aligned}
\lambda(g,h)^\epsilon &= \frac{\tau(g)\tau(h)}{\tau(gh_-)} \quad \text{in case } \bar{g}_+ = h_+ \\
\mu(g,h)^\epsilon &= \frac{\tau(g_+h)}{\tau(g)\tau(h)} \quad \text{in case } g_- = \bar{h}_- \\
\nu(g)^\epsilon &= \frac{\tau(g)}{\tau(g^{-1})}
\end{aligned}$$

The scaling function in Lemma 4.20 provides us with a function τ satisfying such equalities. Since all the structure constants λ, μ, ν are positive, this implies that the positive scaling $g \mapsto |\tau(g)|^{\frac{1}{\epsilon}}$ satisfies the similar equalities without ϵ power. In other words,

$$g \mapsto |\tau(g)|^{\frac{1}{\epsilon}} g : \qquad H_1 \to H_0$$

is an isomorphism of Hopf algebras.

5. HOPF ALGEBRAS IN THE CORRESPONDENCE CATEGORY

In this section, we study the set-theoretical version of Theorem 1. We will assume all the sets are finite.

As pointed out in the introduction, if we restrict ourselves to the usual category of finite sets, with maps as morphisms, then we will end up with only finite groups. Therefore we enlarge the category to include correspondences, so that we may get a more interesting class of Hopf algebras.

A *correspondence* from a set X to a set Y is a subset F of $X \times Y$. Given a correspondence F from X to Y and a correspondence from Y to Z, we have the composition

$$F \circ G = \{(x,z) : \text{there is } y \in Y \text{ such that } (x,y) \in F \text{ and } (y,z) \in G\}.$$

With correspondences as morphisms, the finite sets form a category, which we call the *correspondence category*. With the usual product of sets as tensor product, a one point set as an identity object, and the diagonal $I_X = \{(x,x) : x \in X\} \subset X \times X$ as the identity morphism, the correspondences category becomes a *monoidal category* as defined in [10].

One may introduce the concept of an algebra (called monoid in [10]) in any symmetric monoidal category. By reversing the directions of arrows in all diagrams used in defining an algebra, we have the concept of a coalgebra. In the correspondence category, the product of two algebras is also an algebra. A *correspondence bialgebra* consists of an algebra structure and a coalgebra structure, such that the coalgebra map is an algebra morphism. A *correspondence Hopf algebra* is a correspondence bialgebra with an antipode making the usual diagrams commutative.

The purpose of this section is to classify correspondence Hopf algebras.

It is not convenient to work with correspondences directly. So we take the following Boolean viewpoint. First we observe that a correspondence $F \subset X \times Y$ from X to Y gives rise to a map on the power sets

$$P_F : P(X) \to P(Y),$$

$$P_F(A) = \{b \in Y : \text{there is } a \in A \text{ such that } (a,b) \in F\}.$$

The map P_F preserves union and sends the empty set to the empty set. Conversely, if a map $P : P(X) \to P(Y)$ preserves union and sends the empty set to the empty set, then we have $P = P_F$ for the unique F given by $F = \{(a,b) : b \in P(\{a\})\}$.

Power sets can be considered as modules over the simplest *Boolean algebra* $\mathbb{B}$. $\mathbb{B}$ consists of two elements 0 and 1, and has the commutative sum and product

$$0+0=0, \quad 1+0=1+1=1, \quad 0\cdot 0 = 1 \cdot 0 = 0, \quad 1 \cdot 1 = 1.$$

$\mathbb{B}$ satisfies all the axioms of a ring except the existence of additive inverse. A $\mathbb{B}$-*module* is a set M with addition $+$, a special element 0, and a scalar multiplication $\mathbb{B} \times M \to M$, such that

1. $+$ is commutative, associative, and $0 + x = x$ for all $x \in M$;
2. $1 \cdot x = x$, $0 \cdot x = 0$;
3. $(b_1 + b_2) \cdot x = b_1 \cdot x + b_2 \cdot x, \qquad b \cdot (x_1 + x_2) = b \cdot x_1 + b \cdot x_2.$

It is straightforward to check that, under the first two conditions, the third condition means exactly

$$x + x = x, \qquad \text{for all } x \in M. \tag{30}$$

In fact, a $\mathbb{B}$-module is equivalent to a lattice. In view of our assumption that all sets are finite, we will also assume all $\mathbb{B}$-modules are finite.

With the obvious notion of homomorphisms, (finite) $\mathbb{B}$-modules form a category. The power set $P(X)$ is a $\mathbb{B}$-module by

$$A + B = A \cup B, \qquad 0 = \emptyset.$$

It is easy to see that

$$P : X \mapsto P(X), F \mapsto P_F$$

is a functor from the correspondence category to the category of $\mathbb{B}$-modules.

A subset B of a $\mathbb{B}$-module M is called a *basis* if every $x \in M$ is a unique linear combination of elements in B. A $\mathbb{B}$-module is said to be *free* if it has a basis. Clearly, the collection $\{\{x\} : x \in X\}$ is a basis of $P(X)$. The following lemma (especially the third property) implies P is a one-to-one correspondence between finite sets and finite free $\mathbb{B}$-modules.

Lemma 5.21. *Let B be a basis of a $\mathbb{B}$-module M. Let $b \in B$.*

1.If the b-coordinate of $x \in M$ is 1, then for any $y \in M$, the b-coordinate of $x + y$ is also 1;
2.If $b = x_1 + \cdots + x_k$ for some $x_i \in M$, then each $x_i = b$ or 0;
3.The basis of M is unique.

Proof. In the first property, we have $x = b + \xi$, where ξ is a sum of elements in $B - \{b\}$. We also have two possibilities for y:

$$y = b + \eta, \quad \text{or} \quad y = \eta,$$

where η is a sum of elements in $B - \{b\}$. Then by (30), we have

$$x + y = \begin{cases} b + b + \xi + \eta & \text{if } y = b + \eta \\ b + \xi + \eta & \text{if } y = \eta \end{cases} = b + \xi + \eta,$$

and $\xi + \eta$ is still a sum of elements in $B - \{b\}$. This proves the first property.

In the second property, if x_1 is neither b nor 0, then we have $b' \in B - \{b\}$ such that the b'-coordinate of x_1 is 1. By taking $x = x_1$, $y = x_2 + \cdots + x_k$, and $b = b'$ in the first property, we see that the b'-coordinate of b is also 1. The contradiction shows that $x_1 = b$ or 0. The proof for x_i is similar.

If we take the expression $b = x_1 + \cdots + x_k$ in the second property as the expansion of b (in one basis B) in terms of another basis (consisting of $x_1, \cdots, x_k$ and some others), then we immediately see that B is the only basis of M. $\blacksquare$

The tensor product of $\mathbb{B}$-modules can be defined in the same way as modules over commutative rings. With $\mathbb{B}$ as the unit object, $\mathbb{B}$-modules then form a monoidal category. Since we clearly have $P(X) \otimes P(Y) = P(X \times Y)$ and $P(\text{one point}) = \mathbb{B}$, P is a functor of monoidal categories.

Concepts such as $\mathbb{B}$-algebra, $\mathbb{B}$-coalgebra, and $\mathbb{B}$-Hopf algebra can be introduced just like the corresponding concepts over commutative rings. Since P is a functor of monoidal categories, P sends correspondence Hopf algebras to free $\mathbb{B}$-Hopf algebras. Moreover, because of the third property in Lemma 5.21, P is a one-to-one correspondence between correspondence Hopf algebras and free $\mathbb{B}$-Hopf algebras.

Motivated by the classification of Hopf algebras with positive bases, we may introduce free $\mathbb{B}$-Hopf algebras $H(G; G_+, G_-)$ as in Section 2 and conjecture that these are all the free $\mathbb{B}$-Hopf algebras. This is indeed the case.

Theorem 5.2. *Any free $\mathbb{B}$-Hopf algebra is isomorphic to $H(G; G_+, G_-)$ for a unique group G and a unique factorization $G = G_+G_-$.*

Proof. The theorem may be proved by basically repeating the contents of Section 3. There is no need to do rescaling (and all the positive coefficients in Section 3 can be replaced by 1) since the only nonzero element of $\mathbb{B}$ is 1.

Instead of repeating all the details, we discuss some key points involved in Section 3, and prove only one lemma to illustrate that the whole section works in the category of $\mathbb{B}$-modules.

There are two key technical points in the proofs in Section 3: one is the use of duality, opposite, and co-opposite in translating a proven lemma into another lemma in similar or dual settings. The other is the use of positivity.

The dual of $\mathbb{B}$-modules can be defined in the same way as modules over commutative rings, and satisfies similar properties such as $(M^*)^* = M$. The opposite and co-opposite of $\mathbb{B}$-Hopf algebras can be introduced similarly, as far as the antipode is invertible.

As for the positivity, the role can be replaced by the three properties in Lemma 5.21. Here we only illustrates how this works by proving Lemma 3.2. Assume B is the basis of a $\mathbb{B}$-Hopf algebra H. The identity element

1 of H is a sum $1 = d_1 + \cdots + d_k$ of basis elements. Then we have $d_i = d_i \cdot 1 = d_i d_1 + \cdots + d_i d_k$. Because d_i is a basis element, by the second property in Lemma 5.21 we see that $d_i d_j = 0$ or d_i. Similarly, from $d_j = 1 \cdot d_j$, we see that $d_i d_j = 0$ or d_j. Then we may conclude $d_i d_j = 0$ when $i \neq j$ and $d_i d_i = d_i$, as before.

Similarly, from $\Delta(d_1)+\cdots+\Delta(d_k) = \Delta(1) = 1\otimes 1 = \sum_{i,j} d_i \otimes d_j$, we may prove $\mathbb{B}d_1+\cdots+\mathbb{B}d_k$ is closed under Δ. From $S(d_1)+\cdots+S(d_k) = S(1) = 1 = d_1+\cdots+d_k$, we may prove $\mathbb{B}d_1+\cdots+\mathbb{B}d_k$ is closed under S. Therefore $\mathbb{B}d_1 + \cdots + \mathbb{B}d_k$ is a Hopf subalgebra of H. The standard argument for classifying commutative Hopf algebras also applies to $\mathbb{B}$-modules. Then we know that $\mathbb{B}d_1 + \cdots + \mathbb{B}d_k$ must be the dual $\mathbb{B}$-Hopf algebra of the group algebra $\mathbb{B}G_+$. This completes the proof of the Lemma 3.2 for $\mathbb{B}$-Hopf algebras. ∎

By the one-to-one correspondence between correspondence Hopf algebras and free $\mathbb{B}$-Hopf algebras, we may translate Theorem 5.2 into the following classification of correspondence Hopf algebras.

Theorem 5.3. *Any finite correspondence Hopf Algebra is a finite group G, with a unique factorization $G = G_+G_-$ such that*

$$\begin{aligned}
m &= \{(g_-h_+, h_+k_-, g_-h_+k_-) : h_+ \in G_+, g_-, k_- \in G_-\} \subset (G\times G)\times G \\
\Delta &= \{(g_+h_-k_+, g_+h_-, h_-k_+) : g_+, k_+ \in G_+, h_- \in G_-\} \subset G\times (G\times G) \\
1 &= \{(pt, g_+) : g_+ \in G_+\} \subset \{pt\}\times G \\
\epsilon &= \{(g, pt) : g_- \in G_-\} \subset G\times \{pt\} \\
S &= \{(g, g^{-1}) : g \in G\} \subset G\times G
\end{aligned}$$

REFERENCES

1. N. Andruskiewitsch and H.J. Schneider, Finite quantum groups and Cartan matrices, *to appear in Adv. Math.* (2000).
2. N. Andruskiewitsch and H.J. Schneider, Finite quantum groups over abelian groups of prime exponent, preprint (1999).
3. M. Beattie, S. Bascalescu, and L. Grunenfelder, On pointed Hopf algebras of dimension p^n. *Proc. Amer. Math. Soc.* **128** (2000), 361–367.
4. E. Beggs, J. Gould, and S. Majid, Finite group factorisations and braiding, *J. Alg.* **181** (1996), 112–151.
5. P. Etingof and S. Geleki, Semisimple Hopf algebras of dimension pq is trivial, *J. Alg.* **210** (1998), 664–669.
6. R.G. Larson and M. Sweedler, An associative orthogonal bilinear form for Hopf algebras, *Amer. J. Math.* **91** (1969), 75–93.

7. J. Lu, M. Yan, M. and Y. C. Zhu, On the set-theoretical Yang-Baxter equation, *to appear in Duke Math. J.* (2000).

8. J. Lu, M. Yan, M. and Y. C. Zhu, Quasi-triangular structures on Hopf algebras with positive bases. *to appear in* "Proceedings of Coloquio de Grupos Cuanticos y Algebras de Hopf, La Falda, Argentina, Aug 1999" (N. Andruskiewitsch et. al., Ed.), Contemp. Math., Amer. Math. Soc., 2000.

9. G. Lusztig, "Introduction to Quantum Groups," Progress in Mathematics **110**, Birkhauser, Boston, 1993.

10. S. MacLane, "Categories for the Working Mathmatician," Graduate Texts in Math. **5**, Springer-Verlag, New York, 1971.

11. A. Masuoka, The p^n theorem for semisimple Hopf algebras, *Proc. Amer. Math. Soc.* **124** (1996), 735–737.

12. S. Majid, Physics for algebraists: non-commutative and non-cocommutative Hopf algebras by a bicrossproduct construction, *J. Alg.* **130** (1990), 17–64.

13. S. Majid, "Fundations of Quantum Group Theory," Cambridge University Press, 1995.

14. D. Radford, The order of the antipode of a finite dimensional Hopf algebra is finite, *Amer. J. Math.* **98** (1976), 333–355.

15. D. Stefan, The set of types of n-dimensional semisimple and cosemisimple Hopf algebras is finite, *J. Alg.* **193** (1997), 571–580.

16. M. Takeuchi, Matched pairs of groups and bismash products of Hopf algebras, *Comm. Alg.* **9** (1981), 841–882.

17. A. Zelevinski, "Representations of Finite Classical Groups," Lectures Notes in Math. **869**, Springer-Verlag, Berlin and New York, 1981.