

COMPLETE INVARIANTS FOR COMPLEX SEMISIMPLE HOPF ALGEBRAS

SUMANTH DATT, VIJAY KODIYALAM, AND V.S. SUNDER

ABSTRACT. We obtain a complete (and finite) list of isomorphism invariants of complex semisimple Hopf algebras of a fixed dimension. We do this by proving a generalisation of a theorem due to Procesi and Razmyslov (which, in turn, was used to prove Artin's conjecture).

1. Introduction

In this paper, we consider the problem of distinguishing two complex semisimple Hopf algebras of dimension n specified in terms of their structure constants with respect to some bases. As a solution to this problem, we give a finite list of polynomials in the structure constants that are isomorphism invariant and that distinguish the isomorphism classes.

The methods are those of classical invariant theory [Wyl] supplemented by the diagrammatic formalism of Hopf algebras due to Kuperberg [Kpr] as expounded by Kauffman and Radford [KffRdf]. We also rely on the theorem of Stefan [Stf] that there are only finitely many complex semisimple Hopf algebras of any fixed dimension.

In §2 we show that complex semisimple Hopf algebras (of dimension n) form a nonsingular subvariety of the variety of complex bialgebras (of dimension n) and that polynomial invariants separate their isomorphism classes. We devote §3 - which is self contained - to a proof of a result in invariant theory that generalises the Procesi-Razmyslov theorem proving Artin's conjecture. §4 describes the finite list of polynomial invariants which distinguish Hopf algebras. A final §5 contains some remarks, examples and questions.

2. The variety of semisimple Hopf algebras

For the rest of this paper, we fix a positive integer n which will be the dimension of the bialgebras and Hopf algebras that we consider. Let V be a complex vector space of dimension n and v_1, v_2, \dots, v_n be a fixed basis of V .

A bialgebra structure on V is specified by giving its structure constants with respect to this basis. With the usual notations μ, Δ, η and ϵ for the multiplication, comultiplication, unit and counit maps respectively, a bialgebra structure on V is specified by giving complex numbers $\mu_{jk}^i, \Delta_i^{jk}, \eta^i$ and ϵ_i - here and in

Received September 3, 2002.

the sequel, all indices range from 1 to n and we will use the Einstein summation convention where each index that occurs as an ‘upper’ index and a ‘lower’ index in a product is summed over its range - that satisfy the following equations:

$$\begin{aligned}
 \mu_{jk}^t \mu_{il}^i &= \mu_{kl}^t \mu_{jt}^i \\
 \Delta_i^{jt} \Delta_t^{kl} &= \Delta_i^{tl} \Delta_t^{jk} \\
 \eta^t \mu_{it}^j &= \delta_i^j = \eta^t \mu_{ti}^j \\
 \Delta_i^{tj} \epsilon_t &= \delta_i^j = \Delta_i^{jt} \epsilon_t \\
 \mu_{ij}^t \Delta_t^{kl} &= \Delta_i^{pq} \Delta_j^{rs} \mu_{pr}^k \mu_{qs}^l \\
 \eta^t \Delta_t^{ij} &= \eta^i \eta^j \\
 \mu_{ij}^t \epsilon_t &= \epsilon_i \epsilon_j \\
 \eta^t \epsilon_t &= 1
 \end{aligned}$$

Thus the bialgebra structures on V form an affine variety $B \subseteq \mathbb{A}_{\mathbb{C}}^d$ where $d = 2n^3 + 2n$.

These equations are easier to appreciate in the symbolic notation due to Kuperberg [Kpr] as explained in Kauffman and Radford [KffRdf]. We will give a very brief summary of this. The bialgebra structure maps are represented as:

$$\begin{array}{c} \searrow \\ \mu \rightarrow \\ \nearrow \end{array} \rightarrow \begin{array}{c} \rightarrow \Delta \\ \nearrow \\ \searrow \end{array} \quad \eta \rightarrow \quad \text{and} \quad \rightarrow \epsilon ,$$

while the equations defining the variety B are symbolically written:

$$(2.1) \quad \begin{array}{c} \searrow \\ \rightarrow \mu \rightarrow \mu \rightarrow \\ \nearrow \end{array} = \begin{array}{c} \searrow \\ \rightarrow \mu \rightarrow \mu \rightarrow \\ \nearrow \end{array}$$

$$(2.2) \quad \begin{array}{c} \rightarrow \Delta \nearrow \\ \rightarrow \Delta \rightarrow \\ \searrow \end{array} = \begin{array}{c} \rightarrow \Delta \rightarrow \Delta \nearrow \\ \searrow \end{array}$$

$$(2.3) \quad \eta \begin{array}{c} \searrow \\ \rightarrow \mu \rightarrow \\ \nearrow \end{array} = \begin{array}{c} \rightarrow \\ \rightarrow \end{array} = \eta \begin{array}{c} \rightarrow \mu \rightarrow \\ \nearrow \end{array}$$

$$(2.4) \quad \begin{array}{c} \rightarrow \Delta \rightarrow \epsilon \\ \searrow \end{array} = \begin{array}{c} \rightarrow \\ \rightarrow \end{array} = \begin{array}{c} \rightarrow \Delta \nearrow \\ \rightarrow \epsilon \end{array}$$

$$(2.5) \quad \begin{array}{c} \searrow \\ \mu \rightarrow \Delta \nearrow \\ \nearrow \end{array} = \begin{array}{c} \rightarrow \Delta \rightarrow \mu \rightarrow \\ \rightarrow \Delta \rightarrow \mu \rightarrow \end{array}$$

$$(2.6) \quad \eta \rightarrow \Delta \begin{array}{l} \nearrow \\ \searrow \end{array} = \begin{array}{l} \eta \rightarrow \\ \eta \rightarrow \end{array}$$

$$(2.7) \quad \begin{array}{l} \searrow \\ \nearrow \end{array} \mu \rightarrow \epsilon = \begin{array}{l} \rightarrow \epsilon \\ \rightarrow \epsilon \end{array}$$

$$(2.8) \quad \eta \rightarrow \epsilon = 1.$$

Equations (2.1) - (2.8) are to be interpreted thus. Each is an equality of one or more ‘pictures’. A picture with k inputs and l outputs represents a map from $V^{\otimes k}$ to $V^{\otimes l}$. By convention, the inputs for each picture are read anticlockwise and the outputs clockwise. A general endomorphism ρ of V is represented by $\rightarrow \rho \rightarrow$ while the identity endomorphism of V is represented by \rightarrow .

There is also a structure constant interpretation for such a picture as a tensor with l upper and k lower indices. A picture that has a ‘bound’ arrow - one that is neither an input nor an output - involves a contraction of a tensor. In the structure constant interpretation of a pictorial equation, each arrow is decorated with an index, bound arrows correspond to summing over the corresponding index, and the equation is deemed to hold for all values of the indices of the ‘free’ arrows.

We will illustrate these interpretations for a picture that will play a particularly important role in the sequel. Consider the picture in Figure 1 which has one

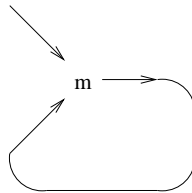


FIGURE 1. An element of V^*

input and no outputs and so represents an element of V^* . In terms of structure constants, this corresponds to the picture of Figure 2 which is read as μ_{it}^t . The free arrow here is labelled by i and the bound arrow by t .

Fix a point $(\mu, \Delta, \eta, \epsilon)$ on B . This gives a bialgebra structure on V for which, for instance, $v_i v_j = \mu_{ij}^t v_t$. The trace of v_i in the left regular representation is therefore μ_{it}^t . Hence the picture in Figure 1 represents the trace on V in its left regular representation.

Similarly, it may be verified that the picture in Figure 3 represents the trace on V^* in its left regular representation. In order to simplify drawing various pictures that we will need, we will henceforth use $\rightarrow \phi$ for the picture in Figure 1 and $h \rightarrow$ for the picture in Figure 3.

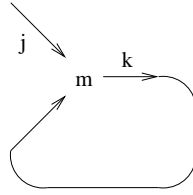


FIGURE 2. Structure constant interpretation

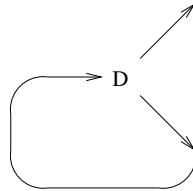


FIGURE 3. An element of V

There is a natural action of the group $G = GL_n(\mathbb{C})$ on $\mathbb{A}_{\mathbb{C}}^d$ defined as follows: For a point $(\mu, \Delta, \eta, \epsilon) = (\mu_{jk}^i, \Delta_i^{jk}, \eta^i, \epsilon_i) \in \mathbb{A}_{\mathbb{C}}^d$ and $g \in G$, define $g \cdot (\mu, \Delta, \eta, \epsilon) = (\tilde{\mu}, \tilde{\Delta}, \tilde{\eta}, \tilde{\epsilon})$ where

$$\begin{aligned} \tilde{\mu}_{jk}^i &= g_p^i (g^{-1})_j^q (g^{-1})_k^r \mu_{qr}^p, \\ \tilde{\Delta}_i^{jk} &= (g^{-1})_i^p g_q^j g_r^k \Delta_p^{qr}, \\ \tilde{\eta}^i &= g_p^i \eta^p, \text{ and} \\ \tilde{\epsilon}_i &= (g^{-1})_i^p \epsilon_p. \end{aligned}$$

It is easy to see that this action carries B onto itself and that points of B lie in the same G -orbit precisely when they correspond to isomorphic bialgebra structures on V .

We will be interested in the points on B that correspond to semisimple Hopf algebra structures. We summarise some well known facts about such Hopf algebras in the following proposition. See [LrsRdf] and [LrsRdf2] for proofs. Recall that a two-sided integral in a Hopf algebra is an element h such that $hx = \epsilon(x)h = xh$ for each x in the algebra.

Proposition 1. *Let H be a complex semisimple Hopf algebra of dimension n with antipode S and let H^* be the dual Hopf algebra. Let $\phi \in H^*$ (resp. $h \in H$) be the trace on H (resp. H^*) in its left regular representation. Then,*

- (a) H^* is also semisimple,
- (b) ϕ (resp. h) is a two-sided integral for H^* (resp. H),
- (c) $\phi(h) = n$, and
- (d) S is involutive, i.e., $S^2 = id_H$.

□

Let SCH be the subset of B of all points that give semisimple Hopf algebra structures on V .

Lemma 2. *For a point $(\mu, \Delta, \eta, \epsilon) \in B$, the following two conditions are equivalent :*

- (i) $(\mu, \Delta, \eta, \epsilon) \in SCH$.
- (ii) *The following pictorial equations hold:*

$$(2.9) \quad \begin{array}{c} \searrow \\ h \rightarrow \mu \rightarrow \\ \end{array} = \begin{array}{c} \rightarrow \epsilon \\ h \rightarrow \\ \end{array} = \begin{array}{c} h \rightarrow \mu \rightarrow \\ \nearrow \end{array}$$

$$(2.10) \quad \begin{array}{c} \rightarrow \Delta \rightarrow \phi \\ \searrow \end{array} = \begin{array}{c} \rightarrow \phi \\ \eta \rightarrow \\ \end{array} = \begin{array}{c} \rightarrow \Delta \rightarrow \phi \\ \nearrow \end{array}$$

$$(2.11) \quad h \rightarrow \phi = n.$$

Proof. Since the pictorial equations are equivalent to the requirements that ϕ and h be two-sided integrals for H and H^* respectively with $\phi(h) = n$, Proposition 1(b,c) show that (i) \Rightarrow (ii). To see the reverse implication, consider a point $(\mu, \Delta, \eta, \epsilon) \in B$ satisfying the equations (2.9) - (2.11) and define an endomorphism S of V by the equation:

$$\rightarrow nS \rightarrow = \begin{array}{c} \rightarrow \mu \leftarrow \Delta \rightarrow \\ \downarrow \quad \uparrow \\ \phi \quad h \end{array}$$

The calculation in Figure 4 below shows that $\sum_{(x)} S(x_{(1)})x_{(2)} = \epsilon(x) 1$ (in ‘Sweedler’s notation’), while another such similar calculation shows that $\sum_{(x)} x_{(1)}S(x_{(2)}) = \epsilon(x).1$. Hence this bialgebra structure on V admits an antipode and is therefore a Hopf algebra structure on V . Consider now the calculation in Figure 5 where the first equality follows from equation (2.4) and the second since the trace of the identity endomorphism of V is n . This shows that $\epsilon(h) = n \neq 0$ and therefore by [LrsSwd] the Hopf algebra structure on V is semisimple. Thus (ii) \Rightarrow (i). \square

Corollary 3. *Every point of SCH satisfies the following pictorial equation:*

$$(2.12) \quad \begin{array}{c} \rightarrow \mu \leftarrow \Delta \rightarrow \\ \downarrow \quad \uparrow \\ \phi \quad h \end{array} \begin{array}{c} \rightarrow \mu \leftarrow \Delta \rightarrow \\ \downarrow \quad \uparrow \\ \phi \quad h \end{array} = n^2 (\rightarrow)$$

Proof. The lemma states an equality of two endomorphisms of V - the right side being n^2 times the identity endomorphism, and the left side being the square of the endomorphism

$$\begin{array}{c} \rightarrow \mu \leftarrow \Delta \rightarrow \\ \downarrow \quad \uparrow \\ \phi \quad h \end{array} ;$$

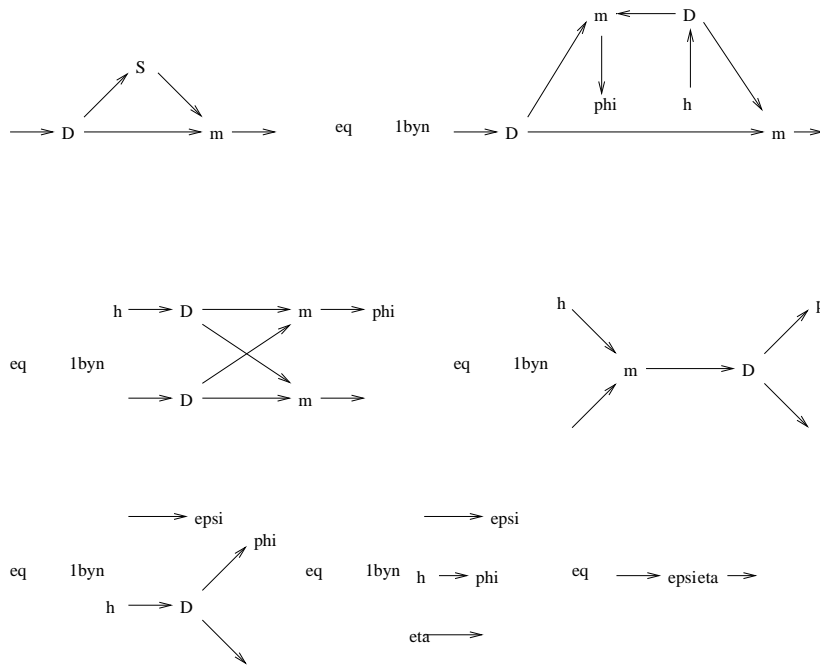


FIGURE 4. Antipode verification

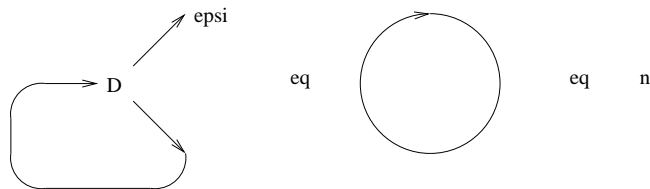


FIGURE 5. Semisimplicity verification

this latter endomorphism is, however, seen to be nothing but nS (see the displayed picture defining nS in the proof of Lemma 2). An appeal to Proposition 1(d) completes the proof. \square

Proposition 4. *The subset SCH is a nonsingular G -stable (closed) subvariety of B that is a union of finitely many closed G -orbits.*

Proof. Since isomorphic bialgebra structures on V lie in the same G -orbit, SCH is a union of G -orbits and hence G -stable, while Lemma 2 shows that SCH is a closed subvariety of B . By the results of Stefan - see Corollary 1.5, Corollary

1.6, Theorem 2.1 of [Stf] - and Proposition 1(a), there are only finitely many orbits of semisimple Hopf algebras in B each of which is open in B and therefore also in SCH . Thus each such orbit is also closed in SCH and being the finite disconnected union of closed nonsingular orbits, SCH is itself nonsingular. \square

Consider the dual action of the group G on the coordinate ring $R = \mathbb{C}[\mu_{jk}^i, \Delta_i^{jk}, \eta^i, \epsilon_i]$ of $\mathbb{A}_{\mathbb{C}}^d$, which is a polynomial ring in $d = 2n^3 + 2n$ variables. Let R^G denote the ring of invariants. Given a bialgebra A of dimension n and an element $f \in R^G$ one may ‘evaluate f on A ’ by taking the structure constants of A with respect to an arbitrary basis as the coordinates of a point on B and evaluating f at that point. The result, which we will denote $f(A)$, is independent of the chosen basis since a change of basis corresponds to moving in a G -orbit on B and $f \in R^G$.

Corollary 5. *Two complex semisimple Hopf algebras H_1 and H_2 of dimension n are isomorphic if and only if for each $f \in R^G$, we have $f(H_1) = f(H_2)$.*

Proof. If H_1 and H_2 are isomorphic, then they have the same structure constants with respect to appropriately chosen bases and therefore for each $f \in R^G$, $f(H_1) = f(H_2)$. Conversely, if H_1 and H_2 are not isomorphic, then their structure constants with respect to any choice of bases belong to different G -orbits in SCH . Since the G -orbits in SCH are closed by Proposition 4, it follows from what [MmfFgrKrw] refers to as the ‘only really important geometric property implied by the reductivity of G ’ - see Corollary 1.2 of Chapter 1, §2 - that there is an $f \in R^G$ that is 1 on H_1 and 0 on H_2 . \square

Remark 6. *The results of this section hold, mutatis mutandis, when SCH is the subset of semisimple and cosemisimple Hopf algebra structures - and therefore the choice of notation SCH - of the variety B of bialgebra structures on an n -dimensional vector space over an algebraically closed field of arbitrary characteristic.*

3. Invariants of tensors

Let V be a complex vector space of dimension n , and let $G = GL(V)$. For non-negative integers t and b , let V_b^t be the G -module $V^{\otimes t} \otimes (V^*)^{\otimes b}$.

Given tuples (t_i, b_i) of non-negative integers, for $i = 1, 2, \dots, k$, consider the G -module defined by $W (= W(\{(t_i, b_i) : i = 1, 2, \dots, k\})) = \bigoplus_{i=1}^k V_{b_i}^{t_i}$. We wish to describe, in this section, the polynomial invariants of the G -module W - by which is meant the following: regard W as an affine variety with a G action and consider the dual action on the coordinate ring $\mathbb{C}[W^*]$; a polynomial invariant of W is just a G -invariant element of $\mathbb{C}[W^*]$.

Explicitly, choose a basis v_1, \dots, v_n of V and let v^1, \dots, v^n be the dual basis of V^* . Then, a basis of V_b^t is given by all $v_{u_1} \otimes v_{u_2} \otimes \dots \otimes v_{u_t} \otimes v^{l_1} \otimes \dots \otimes v^{l_b}$ where the indices $u_1, \dots, u_t, l_1, \dots, l_b$ all range from 1 to n . Let $T_{l_1 \dots l_b}^{u_1 \dots u_t}$ be the coordinate function on V_b^t that gives the coefficient of $v_{u_1} \otimes v_{u_2} \otimes \dots \otimes v_{u_t} \otimes v^{l_1} \otimes \dots \otimes v^{l_b}$. Thus $\mathbb{C}[(V_b^t)^*]$ is identified with the polynomial ring $\mathbb{C}[T_{l_1 \dots l_b}^{u_1 \dots u_t}]$ in n^{b+t} variables.

The group G is identified with $GL_n(\mathbb{C})$ using the basis of V . The dual action of G on this polynomial ring is then given by:

$$g(T_{l_1 \dots l_b}^{u_1 \dots u_t}) = \prod_{i=1}^t (g^{-1})_{\tilde{u}_i}^{u_i} \prod_{j=1}^b (g)_{l_j}^{\tilde{l}_j} T_{\tilde{l}_1 \dots \tilde{l}_b}^{\tilde{u}_1 \dots \tilde{u}_t},$$

where, of course, the summation convention is used.

More generally, for $W = W(\{(t_i, b_i) : i = 1, 2, \dots, k\})$, we identify the coordinate ring $\mathbb{C}[W^*]$ with the polynomial ring $\mathbb{C}[T(i)_{l_1 \dots l_{b_i}}^{u_1 \dots u_{t_i}}]$ in $\sum_{i=1}^k n^{b_i+t_i}$ variables. Here, i ranges from 1 to k and all the indices of the $T(i)$ from 1 to n . This polynomial ring has an \mathbb{N}^k -grading where $\deg(T(i)_{l_1 \dots l_{b_i}}^{u_1 \dots u_{t_i}}) = (0, 0, \dots, 0, 1, 0, \dots, 0)$ - where the 1 is in the i^{th} place - independent of the sub- and super-scripts. The G -action preserves this grading and so the ring of invariants is a graded subring of $\mathbb{C}[W^*]$.

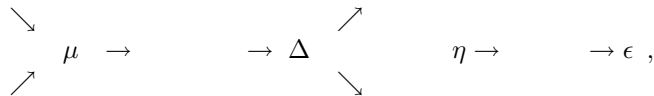
Fix $W = W(\{(t_i, b_i) : i = 1, 2, \dots, k\})$. By a **picture invariant on W** we shall mean the following: it is determined by the data of (a) a k -tuple of non-negative integers $\underline{m} = (m_1, \dots, m_k)$ such that $\sum_{i=1}^k m_i t_i = \sum_{i=1}^k m_i b_i = N$ for some $N \in \mathbb{N}$, and (b) a permutation $\sigma \in \Sigma_N$ - the symmetric group on N letters. The associated picture invariant is the following element of $\mathbb{C}[W^*]$:

$$\prod_{i=1}^k \left(\prod_{j=1}^{m_i} T(i)_{r_{\sigma(\sum_{p<i} m_p t_p + (j-1)t_i + 1)} \dots r_{\sigma(\sum_{p<i} m_p t_p + jt_i)}}^{\sigma(\sum_{p<i} m_p b_p + (j-1)b_i + 1) \dots \sigma(\sum_{p<i} m_p b_p + jb_i)} \right),$$

i.e., we take N dummy indices r_1, \dots, r_N , take a product of m_1 $T(1)$'s, m_2 $T(2)$'s, \dots , m_k $T(k)$'s and write the lower indices in order and the upper indices in the permuted order given by σ . It should be clear that this 'picture invariant' is homogeneous of degree (m_1, \dots, m_k) in the \mathbb{N}^k -grading. (We will soon show - see Proposition 7 - that picture invariants are indeed invariant.)

By means of one example - which is the main case of interest for our purposes - we will explain how picture invariants are represented by pictures. Suppose that $W = V_2^1 \oplus V_1^2 \oplus V_0^1 \oplus V_1^0$. We will use μ, Δ, η and ϵ instead of $T(1), T(2), T(3)$ and $T(4)$. Consider, for instance, the 4-tuple $(2, 1, 1, 0)$ for which $2(1, 2) + 1(2, 1) + 1(1, 0) + 0(0, 1) = (5, 5)$ and the permutation $(123)(45) \in \Sigma_5$. The picture invariant associated to this data is equal to $\mu_{r_1 r_2}^{r_2} \mu_{r_3 r_4}^{r_3} \Delta_{r_5}^{r_1 r_5} \eta^{r_4}$. To this 'picture invariant', we shall associate the pictures in Figure 6.

In Figure 6, in the picture on the left, we have numbered the input and output arrows so as to make clear the role of the permutation in drawing the invariant. So briefly, a picture invariant - in this case, i.e., when $k = 4$ and W is specified by the tuple $\{(1, 2), (2, 1), (1, 0), (0, 1)\}$ as above - is constructed by taking, in order, a collection of basic pictures of the types



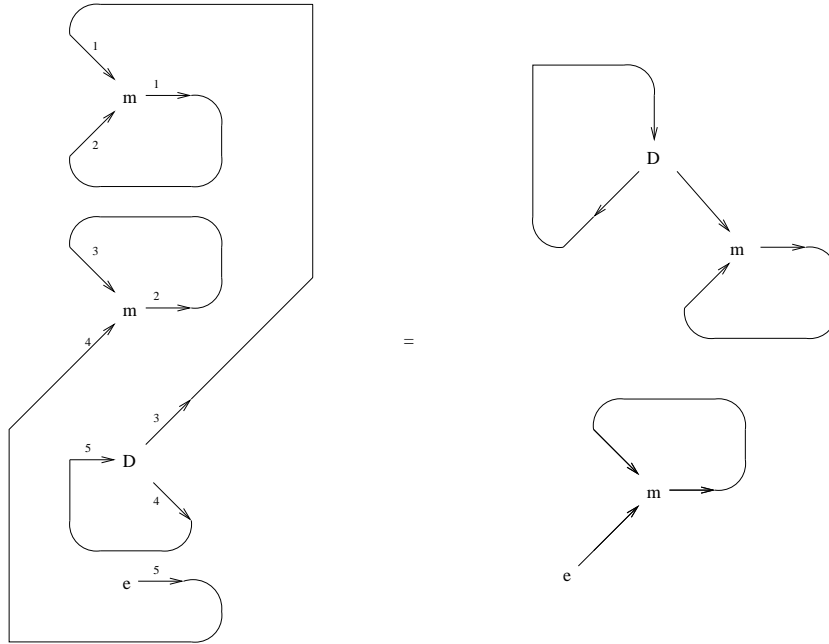


FIGURE 6. An example of a picture invariant

the numbers of each of which are specified by the 4-tuple, and then joining the i^{th} output arrow to the $\sigma(i)^{th}$ input arrow for each i to get a ‘closed picture’, i.e., one with no free arrows. We will not distinguish between a picture invariant and any picture that represents it.

Note that if a picture invariant is disconnected - as in the example considered - then, its components also define picture invariants, the product of all of which gives the full picture invariant.

We may now state our main observation about the picture invariants.

Proposition 7. *Let V be a finite dimensional complex vector space and (t_i, b_i) for $i = 1, 2, \dots, k$ be tuples of non-negative integers. Let $W = \bigoplus_{i=1}^k V_{b_i}^{t_i}$ and set $R = \mathbb{C}[W^*]$. Then, R^G , for the $G = GL(V)$ action, is linearly spanned by the picture invariants on W .*

Before proving this, we pause to point out a corollary - see Theorem 1.3 of [Prc] and [Rzm].

Corollary 8. *The ring of invariants of the group $GL_n(\mathbb{C})$ acting by simultaneous conjugation on k square matrices $A(1), \dots, A(k)$ is linearly spanned by monomials in the $\text{tr}(A(i_1)A(i_2) \cdots A(i_j))$ where $A(i_1)A(i_2) \cdots A(i_j)$ is any possible (non-commutative) monomial.*

Proof. This corresponds to choosing all the k tuples to be equal to $(1, 1)$. The basic pictures in this case are $\rightarrow A(i) \rightarrow$ and so any connected picture invariant must be as illustrated in Figure 7. In terms of the entries of the ma-

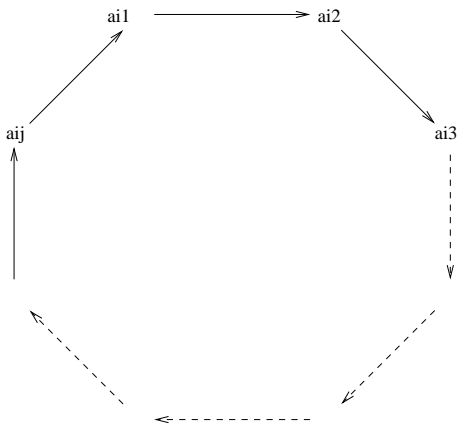


FIGURE 7. A connected picture invariant

trices $A(i)$, this picture invariant evaluates to $tr(A(i_1)A(i_2)\cdots A(i_j))$. A general picture invariant that is possibly disconnected is therefore a monomial in the $tr(A(i_1)A(i_2)\cdots A(i_j))$ and now an appeal to Proposition 7 completes the proof. \square

Proof of Proposition 7. We need to see that the picture invariants span the invariant ring $\mathbb{C}[W^*]^G$. Note that $\mathbb{C}[W^*] = Sym_{\mathbb{C}}(W^*) = \bigoplus_{d \geq 0} Sym_{\mathbb{C}}^d(W^*) = \bigoplus_{d \geq 0} \bigoplus_{\{(m_1, \dots, m_k) : \sum_i m_i = d\}} \otimes_{i=1}^k Sym_{\mathbb{C}}^{m_i}((V_{b_i}^{t_i})^*)$ - as G -modules. Hence it suffices to see that picture invariants span each $(\otimes_{i=1}^k Sym_{\mathbb{C}}^{m_i}((V_{b_i}^{t_i})^*))^G$.

As the natural map of $\otimes_{i=1}^k ((V_{b_i}^{t_i})^*)^{\otimes m_i}$ onto $\otimes_{i=1}^k Sym_{\mathbb{C}}^{m_i}((V_{b_i}^{t_i})^*)$ is a G -map, the reductivity of G implies that $(\otimes_{i=1}^k ((V_{b_i}^{t_i})^*)^{\otimes m_i})^G$ maps onto $(\otimes_{i=1}^k Sym_{\mathbb{C}}^{m_i}((V_{b_i}^{t_i})^*))^G$. Clearly, $\otimes_{i=1}^k ((V_{b_i}^{t_i})^*)^{\otimes m_i}$ is isomorphic as a G -module to V_M^N where $N = \sum_i m_i b_i$ and $M = \sum_i m_i t_i$.

We now appeal to the fact from classical invariant theory - see Theorem 4.3.1 in [GdmWll] - that non-zero $GL(V)$ invariants exist in V_M^N only if $N = M$ and in that case the space of invariants is spanned by all $v_{r_1} \otimes v_{r_2} \otimes \cdots \otimes v_{r_N} \otimes v^{r_{\sigma(1)}} \otimes v^{r_{\sigma(2)}} \otimes \cdots \otimes v^{r_{\sigma(N)}}$ as σ ranges over Σ_N .

Chasing through the isomorphisms, the images of the G -invariants in V_N^N are seen to be precisely the picture invariants, thereby completing the proof. \square

4. Invariants of semisimple Hopf algebras

Let V be a finite dimensional complex vector space, $G = GL(V)$ and $W = V_2^1 \oplus V_1^2 \oplus V_0^1 \oplus V_1^0$ for which we label the coordinate tensors μ, Δ, η and ϵ .

Corollary 5 may be restated to say that isomorphism classes of complex semisimple Hopf algebras are separated by the polynomial invariants of W . By Proposition 7, the phrase ‘polynomial invariants’ of the previous sentence may be replaced by the phrase ‘picture invariants’ in this case, i.e., built out of μ, Δ, η and ϵ . Our goal is to identify a suitable ‘small’ subset of the picture invariants which accomplishes the same task. In this section, we shall be slightly sloppy and also refer to a scalar multiple of a picture invariant as a picture invariant.

Definition 9. *Two picture invariants on W are said to be equivalent modulo SCH if they agree on SCH .*

Pictorially, if a picture invariant can be transformed into another by ‘moves’ that locally replace a subpicture appearing on one side of an equality in equations (2.1)-(2.12) by one appearing on the other, then, the two picture invariants are equivalent modulo SCH . Thus, for instance, Corollary 3 shows that any arrow in a picture may be replaced by a more complicated sub-picture which contains no directed path from the beginning to the end, so that the resulting picture is equivalent modulo SCH to the initial one.

In order to state our next proposition we will find it convenient to introduce some notation for iterated products and coproducts - see p.108 of [Kpr] - as well as for certain picture invariants. First, let

$$\rightarrow \Delta_1 \rightarrow = \rightarrow = \rightarrow \mu_1 \rightarrow$$

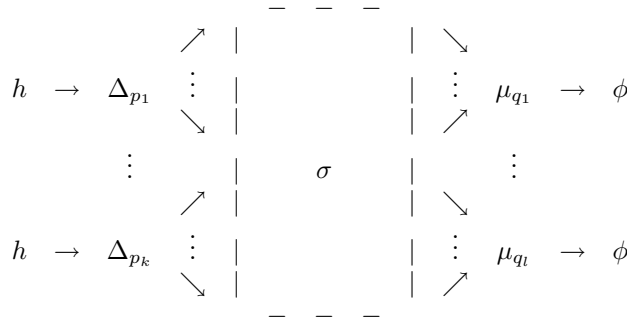
and for $p, q > 1$, inductively define

$$\rightarrow \Delta_p \begin{array}{c} \nearrow \\ \vdots \\ \searrow \end{array} = \rightarrow \Delta \rightarrow \Delta_{p-1} \begin{array}{c} \nearrow \\ \vdots \\ \searrow \end{array}$$

and

$$\begin{array}{c} \searrow \\ \vdots \\ \nearrow \end{array} \mu_q \rightarrow = \begin{array}{c} \searrow \\ \vdots \\ \nearrow \end{array} \mu_{q-1} \rightarrow \mu \rightarrow$$

Also, if $\mathbf{p} = (p_1, \dots, p_k)$, $\mathbf{q} = (q_1, \dots, q_l)$ are tableaux of equal size N (say) - i.e., $p_1 \geq \dots \geq p_k > 0$, $q_1 \geq \dots \geq q_l > 0$, and $\sum_{i=1}^k p_i = \sum_{j=1}^l q_j = N$ - and if $\sigma \in \Sigma_N$, we shall define the picture invariant $\mathcal{I}(\mathbf{p}, \mathbf{q}, \sigma)$ to be the following picture:



where the central ‘box’ labelled σ is meant to indicate that the i -th output of the picture to the left of the box is to be joined to the $\sigma(i)$ -th input of the picture to the right of the box, and we have used the symbols h and ϕ for the pictures associated with them in Figures 3 and 1 respectively.

Proposition 10. *Any picture invariant on W is equivalent modulo SCH to an $\mathcal{I}(\mathbf{p}, \mathbf{q}, \sigma)$. If the total number of μ ’s and Δ ’s in a picture invariant is k , then we may choose $\mathcal{I}(\mathbf{p}, \mathbf{q}, \sigma)$ so that $\sum p_i = \sum q_j \leq 13k/2$.*

Proof. Begin with a picture invariant, say P , on W . From its ‘equivalence class modulo SCH ’, pick a picture invariant, say P_1 , for which the total number $k(P_1)$ of μ ’s and Δ ’s is minimal. Next, pick a picture invariant, say P_2 , in the ‘equivalence class modulo SCH ’ of P such that the total number of η ’s and ϵ ’s in P_2 is minimal among all picture invariants Q in the ‘equivalence class modulo SCH ’ of P for which $k(Q) = k(P_1)$.

We assert that P_2 has no η ’s or ϵ ’s. For suppose that there is an η . Its output must go into either a μ or a Δ or a ϵ . In these cases, it follows from equations (2.3), (2.6) and (2.8) that the minimality requirements defining P_2 (on μ ’s and Δ ’s in the first two cases, and on η ’s and ϵ ’s in the last case) are violated. A similar argument shows that P_2 cannot have any ϵ ’s either.

Since P_2 is a closed picture - i.e., has no free arrows - it is easy to see that the number of μ ’s = number of Δ ’s = l , where $2l = k(P_2) \leq k(P) = k$; from which it follows that the total number of arrows in P_2 is $3l$. Now use Corollary 3 to replace each arrow of P_2 to get an equivalent picture modulo SCH , say P_3 , with $13l$ each of the μ ’s and Δ ’s - the original l together with the 4 new ones introduced for each of the $3l$ arrows replaced. (Recall that each h (resp., ϕ) is a picture with a self-loop containing one Δ (resp., μ).)

We claim that P_3 has no directed loops - except possibly for self loops on the μ ’s and Δ ’s that are inherent in h and ϕ . Note first that the only arrows of P_3 are the newly introduced ones; and the newly introduced substitutes for the edges of P_2 are seen to not contain any edges that can be part of a non-trivial loop. This establishes the claim about ‘no loops in P_3 ’. Further, an inspection of

the newly introduced substitutes for the edges of P_2 also reveals that P_3 contains no directed edge from a μ to a Δ .

To finish the proof it suffices to see that if a picture invariant on W (a) involves only μ 's and Δ 's, (b) has no directed loops except for self loops, and (c) has no directed edge from a μ to a Δ , then such a picture invariant is necessarily equivalent modulo SCH to an $\mathcal{I}(\mathbf{p}, \mathbf{q}, \sigma)$.

We prove this as follows. Begin with such a picture invariant and delete all arrows that go from a Δ to a μ . Consider a connected component of the picture that remains. Each such component contains either only μ 's or only Δ 's. Fix a component, say C , containing only Δ 's, say p of them. Each edge of C feeds into a different Δ (since the 'in-degree' of Δ is one) so there are exactly p edges.

Let C_1 denote the graph obtained by removing self-loops from C and regarding the remaining graph as an undirected graph. We assert that C_1 is a tree. To see this, since it is clearly connected, it is enough to verify that C_1 contains no loops. Suppose L were such a loop. Let us associate the ordered pair (d_{in}, d_{out}) of 'in-' and 'out'-degrees to every vertex of L when regarded as a vertex of the directed subgraph of C corresponding to L . Each such ordered pair must *a priori* be $(1, 1)$, $(2, 0)$ or $(0, 2)$; but our observation about 'no directed loops in C ' means that not all pairs can be $(1, 1)$. So at least one vertex must correspond to $(2, 0)$ or $(0, 2)$. Since the sum of the in-degrees (as also the out-degrees) of all the vertices of L must be equal to the number of edges of L , we may conclude that at least one vertex of L must have in-degree 2; but our graph C contains only Δ 's which have in-degree 1.

Since a tree with p vertices has exactly $(p - 1)$ edges, we deduce that C contains exactly one self loop.

Let C_2 be the picture obtained from C as a result of adding all those arrows of P_3 which emanated from a Δ of C and terminated in a μ . It is a consequence of co-associativity in Hopf algebras, that C is 'equivalent modulo SCH ' to the standard picture (independent of the structure of the tree C_1):

$$h \rightarrow \Delta_p \begin{array}{c} \nearrow \\ \vdots \\ \searrow \end{array} \cdot$$

(We have been slightly glib in using the expression 'equivalent modulo SCH ' for general pictures which are not picture invariants (but more general tensors); we trust the meaning should be clear.)

A dual verification shows that a component containing only μ 's - say q of them - is equivalent modulo SCH to the picture

$$\begin{array}{c} \searrow \\ \vdots \\ \nearrow \end{array} \mu_q \rightarrow \phi \cdot$$

Let k denote the number of components (such as C above) which contain only Δ 's, and suppose $p_1 \geq \dots \geq p_k$ is the non-increasing sequence of the numbers of vertices in these components. Let l and $q_1 \geq \dots \geq q_l$ denote the corresponding numbers for the 'only μ components'. It should then be clear that our picture invariant P_3 (and hence also P) is equivalent modulo SCH to $\mathcal{I}(\mathbf{p}, \mathbf{q}, \sigma)$ for an appropriately chosen permutation σ .

Finally, $\Sigma p_i = \Sigma q_j = 13l \leq 13k/2$. □

Theorem 11. *Two complex semisimple Hopf algebras H_1 and H_2 of dimension n are isomorphic if and only if for every positive integer N , tableaux \mathbf{p}, \mathbf{q} of size N and permutation $\sigma \in \Sigma_N$, we have $\mathcal{I}(\mathbf{p}, \mathbf{q}, \sigma)(H_1) = \mathcal{I}(\mathbf{p}, \mathbf{q}, \sigma)(H_2)$. It suffices to verify this only for $N \leq (2n + 1)^{(2n^2+5)}$.*

Proof. By Corollary 5, H_1 and H_2 are isomorphic if and only if $f(H_1) = f(H_2)$ for all $f \in R^G$. Now Proposition 7 and Proposition 10 immediately imply the first assertion of the theorem. The bound on N follows from computational invariant theory - see §4.7 of [DrkKmp]. By Proposition 4.7.16 and Theorem 4.7.4 of [DrkKmp] R^G is generated as an algebra by its elements of degree at most $k = \frac{3}{8}(2n^3 + 2n)(n+1)^2(2n+1)^{2n^2}$ - the numbers $2n^3 + 2n$, $n+1$, $2n+1$ and n^2 being upper bounds for what they call r, C, A and m respectively. Therefore picture invariants involving at most k μ 's and Δ 's separate isomorphism classes of semisimple Hopf algebras. Now the second assertion of Proposition 10 finishes the proof. □

5. Remarks and questions

This section is a collection of a simple example, some possibly naive questions and a possibly rash conjecture.

Example 12 (Group algebras). *Evaluated on a semisimple Hopf algebra H , we may write*

$$\mathcal{I}(\mathbf{p}, \mathbf{q}, \sigma)(H) = \langle \Delta_{p_1}(h) \otimes \dots \otimes \Delta_{p_k}(h) \mid \sigma \mid \Delta_{q_1}(\phi) \otimes \dots \otimes \Delta_{q_l}(\phi) \rangle$$

where this means: compute the elements of $H^{\otimes N}$ and $(H^*)^{\otimes N}$ given by the left and the right sides of the above expression and pair them off by pairing the i -th tensor factor on the left with the $\sigma(i)$ -th tensor factor on the right. In the case when H is the complex group algebra of a finite group G , it is not hard to see that these picture invariants give essentially the data of the number of solutions in G of all systems of equations of the form $m_1 = m_2 = \dots = m_l = 1$ where 1 is the identity element of G and m_1, \dots, m_l are monomials in the (non-commuting) variables X_1, \dots, X_k . Theorem 11 then implies that - as can also be seen by a pleasant application of the inclusion-exclusion principle - these numbers determine the group G .

Question 13 (Relations between invariants and reconstruction). *A natural question that arises is what the "second fundamental theorem" for these invariants is. Explicitly, consider a polynomial ring in the infinitely many variables $X_{(\mathbf{p}, \mathbf{q}, \sigma)}$*

and determine the ideal I_n of all polynomials that vanish when evaluated on any n -dimensional semisimple Hopf algebra. A related problem is to reconstruct the Hopf algebra from the invariants.

Conjecture 14 (The characteristic p case). *We conjecture that the picture invariants separate isomorphism classes of semisimple and cosemisimple Hopf algebras over an algebraically closed field of arbitrary characteristic. Note that the analogue to the Procesi-Razmyslov theorem has been proved by Donkin in [Dnk] and it is not clear how to interpret this pictorially. Our “justifications” for making this conjecture are the results of Etingof and Gelaki - see [TngGlk] - on lifting theorems from characteristic p to characteristic 0.*

Question 15 (subfactors). *The original motivation for considering this problem comes from subfactor theory where the problem we wish to solve is: decide whether or not two finite-depth hyperfinite subfactors are isomorphic. Considering the gauge group action on the space of flat connections on the graph invariants, we expect that a similar invariant theoretic answer must exist. The difference now will be that the groups involved are real Lie groups acting on smooth manifolds. This question is settled in [KdlSnd].*

Question 16 (The general isomorphism problem). *Is there an explicit decision procedure for the isomorphism problem for general (not necessarily semisimple) finite - dimensional complex Hopf algebras ?*

Question 17 (Efficient computability). *This relates to finding better bounds on the number and size of invariants needed to distinguish semisimple Hopf algebras. In particular, can this be ‘done in polynomial time’?*

Acknowledgements

We would like to thank Bhaskar Bagchi for providing us with a proof that the invariants in Example 12 distinguish isomorphism classes of groups and Akira Masuoka for some helpful e-mails.

References

- [Dnk] S. Donkin, *Invariants of several matrices*, *Inventiones Math.*, **110**, (1992) 389–401.
- [DrkKmp] H. Derksen and G. Kemper, *Computational invariant theory*, *Encyc. of Math. Sc.* **130**, Springer-Verlag, 2002.
- [TngGlk] P. Etingof, and S. Gelaki, *On finite-dimensional semisimple and cosemisimple Hopf algebras in positive characteristic*. *Internat. Math. Res. Notices* 1998, 851–864.
- [GdmWll] R. Goodman and N.R. Wallach, *Representations and invariants of the classical groups*, *Encyc. of Math. and Its Appl.*, **68**, Cambridge Univ. Press, 1998.
- [KffRdf] L. H. Kauffman and D. E. Radford, *On two proofs of the existence and uniqueness of integrals for finite-dimensional Hopf algebras*, *New trends in Hopf algebra theory*, *Contemp. Math.*, **267**, (2000) 177–194.
- [KdlSnd] Vijay Kodiyalam and V.S. Sunder, *Complete family of numerical invariants for a subfactor*, preprint.
- [Kpr] G. Kuperberg, *Non-involutory Hopf algebras and 3-manifold invariants*, *Duke. J. Math.*, **84**, (1996) 83–129.

- [LrsRdf] G. Larson and D. E. Radford, *Finite dimensional cosemisimple Hopf algebras in characteristic 0 are semisimple*, J. Algebra, **117**, (1988), 267–289.
- [LrsRdf2] ———, *Semisimple cosemisimple Hopf algebras*, Amer. J. Math, **110**, (1998), 187–195. **117**, (1988), 267–289.
- [LrsSwd] G. Larson and M. Sweedler, *An associative orthogonal bilinear form for Hopf algebras*, American Journal of Mathematics, **91**, (1969), 71–94.
- [MmfFgrKrw] D. Mumford, J. Fogarty and F. Kirwan, *Geometric Invariant theory, Third Edition*, Ergebnisse der Mathematik und ihre Grenzgebiete 34, Springer Verlag, Berlin (1994).
- [Prc] C. Procesi, *The invariant theory of $n \times n$ matrices*, Adv. in Math., **19**, (1976), 306–381.
- [Rzm] J. Razmyslov, *Identities with trace in full matrix algebras over a field of characteristic zero*, Izv. Akad. Nauk SSR Ser. Mat., **38**, (1974), 723–756.
- [Stf] D. Stefan, *The set of types of n -dimensional semisimple and cosemisimple Hopf algebras is finite*, J. Alg., **193**, (1997), 571–580.
- [Wyl] H. Weyl, *The classical groups: Their invariants and representations*, Princeton University Press, 1997.

UNIVERSITY OF HYDERABAD
E-mail address: msdsm@uohyd.ernet.in

INSTITUTE OF MATHEMATICAL SCIENCES, INDIA
E-mail address: vijay@imsc.res.in

INSTITUTE OF MATHEMATICAL SCIENCES, INDIA
E-mail address: sunder@imsc.res.in