ILLINOIS JOURNAL OF MATHEMATICS
Volume 42, Number 4, Winter 1998

SOLUTIONS TO THE QUANTUM YANG-BAXTER EQUATION HAVING CERTAIN BIALGEBRAS AS THEIR REDUCED FRT CONSTRUCTION

LARRY LAMBE AND DAVID E. RADFORD

Suppose that M is a finite-dimensional vector space over a field k and that $R: M \otimes M \longrightarrow M \otimes M$ is solution to the quantum Yang-Baxter equation(QYBE). The FRT construction [3] is a bialgebra $A(R)$ associated with R in a natural way. There is a quotient of the FRT construction, referred to as the reduced FRT construction and denoted by $\widetilde{A(R)}$, which seems rather useful in computation [11]. The bialgebra $A(R)$ is Hopf algebra only when $M = (0)$, whereas the bialgebra $\widetilde{A(R)}$ may very well be a Hopf algebra.

Given a bialgebra A over the field k, a natural question to ask is for which solutions R to the quantum Yang-Baxter equation is $A \simeq \widetilde{A(R)}$ as bialgebras. The question suggests a way of going about classifying and studying solutions to the quantum Yang-Baxter equation.

In this paper we consider three classes of bialgebras as reduced FRT constructions: the semigroup algebras $k[S]$ of semigroups S over k, the universal enveloping algebras $U(L)$ of finite-dimensional abelian Lie algebras over k when k has characteristic 0, and the class of finite-dimensional Hopf algebras over k.

The first two classes provide an interesting contrast. The polynomial algebra $k[x_1, \ldots, x_r]$ in commuting indeterminants $x_1, \ldots, x_r$ is the underlying algebra of $U(L)$, when $\operatorname{Dim} L = r$, and is also the underlying algebra of $k[S]$, when S is the free commutative semigroup on r generators. For the enveloping algebra, one has

$$\Delta(x_i) = 1 \otimes x_i + x_i \otimes 1$$

for all $1 \leq i \leq r$ and for the semigroup algebra, one has

$$\Delta(x_i) = x_i \otimes x_i$$

for all $1 \leq i \leq r$.

We show that every finite-dimensional Hopf algebra H over k is the reduced FRT construction for some solution to the QYBE. This is not difficult to prove and is very

Received August 8, 1997.
1991 Mathematics Subject Classification. Primary 16W30.
Research of the first-named author supported in part by EPSRC.
Research of the second-named author supported by part by a grant from the National Science Foundation.

interesting theoretically. As one might suspect, the quantum double $D(H)$ of H is instrumental in the construction of such a solution.

A special case ($r = 1$) of Corollary 1 was found during the preparation of [7] and inspired this paper. This special case was presented by the first author in [5].

Throughout this paper k is a field.

1. Preliminaries

In this section we discuss basic definitions and results used in this paper. We assume that the reader has some familiarity with the theory of coalgebras and related structures. A good general reference is [14] from which we draw freely. Other books on Hopf algebras adequate for our purposes are [1] and [9].

Let U and V be vector spaces over the field k. We use the notation $f\colon U \longrightarrow V$ to denote a linear map f from U to V. Composition of linear maps will be denoted by juxtaposition. We will omit the subscript k from the familiar notations $\mathrm{Hom}_k(U, V)$, $\mathrm{End}_k(U)$, and $U \otimes_k V$.

Let $\alpha \in \mathrm{Hom}\,(U, k) = U^*$ be a linear functional on U. We denote the image of $u \in U$ under α by $\langle \alpha, u\rangle$ or $\alpha(u)$. Suppose that $\mathcal{U}$ is a subspace of U^*. Then $\mathcal{U}^\perp = \{u \in U \,|\, \mathcal{U}(u) = (0)\}$ is a subspace of U. We say that $\mathcal{U}$ is a *dense subspace of* U^* if $\mathcal{U}^\perp = (0)$. Suppose that $\mathcal{U}$ is a dense subspace of U^* and let V be a finite-dimensional subspace of U. Then for a given $\beta \in U^*$ there exists an $\alpha \in \mathcal{U}$ such that $\alpha|_V = \beta|_V$, where $\gamma|_V$ denotes the restriction of $\gamma \in U^*$ to V.

Various notions of rank will be useful to us. If $f\colon U \longrightarrow V$ is linear then $\mathrm{rank}\, f = \mathrm{Dim}\,\mathrm{Im}\, f$ has the usual meaning. If S is a subset of U then by $\mathrm{rank}\, S$ we mean the dimension of the span of S. Suppose that $\nu \in U \otimes V$ is not zero. Then ν has many representations $\sum_{i=1}^r u_i \otimes v_i$, where $u_i \in U$ and $v_i \in V$ for $1 \le i \le r$. We will denote the smallest r which occurs in these representations by $\mathrm{Rank}\,\nu$. When $r = \mathrm{Rank}\,\nu$ observe that $\{u_1, \ldots, u_r\}$ and $\{v_1, \ldots, v_r\}$ are linearly independent. We set $\mathrm{Rank}\, 0 = 0$.

We let $\tau_U\colon U \otimes U \longrightarrow U \otimes U$ denote the "twist" map defined by $\tau_U(u \otimes v) = v \otimes u$ for all $u, v \in U$.

1.1. The quantum Yang-Baxter equation. Let M be a vector space over the field k and let $R\colon M \otimes M \longrightarrow M \otimes M$ be a linear map. For $1 \le i < j \le 3$ we define $R_{(i,j)}$ by

$$R_{(1,2)} = R \otimes 1_M, \quad R_{(2,3)} = 1_M \otimes R,$$

and

$$R_{(1,3)} = (1_M \otimes \tau_M)(R \otimes 1_M)(1_M \otimes \tau_M).$$

The equation

$$R_{(2,3)}R_{(1,3)}R_{(1,2)} = R_{(1,2)}R_{(1,3)}R_{(2,3)} \tag{1}$$

is called the *quantum Yang-Baxter equation* (QYBE). The reader can check that $B = \tau_M R$ satisfies

$$B_{(2,3)}B_{(1,2)}B_{(2,3)} = B_{(1,2)}B_{(2,3)}B_{(1,2)} \tag{2}$$

if and only if R satisfies (1). Equation (2) is called the *braid equation.* Solutions to the braid equation are important in connection with invariants of knots and links. See [4] for a discussion of knot and link invariants and also as a source for other references.

1.2. Coalgebras and related structures. Let (C, Δ, ϵ) be a coalgebra over the field k. A common way of denoting the coproduct $\Delta\colon C \longrightarrow C \otimes C$ applied to $c \in C$ is the variation of the Heyneman-Sweedler notation $\Delta(c) = \sum c_{(1)} \otimes c_{(2)}$. We drop the summation symbol and write

$$\Delta(c) = c_{(1)} \otimes c_{(2)}$$

for all $c \in C$. Throughout this paper coalgebras, algebras, and bialgebras are usually denoted by their underlying vector spaces. We let C^{cop} be the coalgebra $(C, \Delta^{\mathrm{cop}}, \epsilon)$, where $\Delta^{\mathrm{cop}} = \tau_C \Delta$. Thus

$$\Delta^{\mathrm{cop}}(c) = c_{(2)} \otimes c_{(1)}$$

for all $c \in C$. The coalgebra C is *cocommutative* if $C = C^{\mathrm{cop}}$.

Likewise, if (A, m, η) is an algebra over k, then A^{op} denotes the algebra $(A, m^{\mathrm{op}}, \eta)$, where $m^{\mathrm{op}} = m\tau_A$. Thus

$$m^{\mathrm{op}}(a \otimes b) = m(b \otimes a) = ba$$

for $a, b \in A$. The algebra A is *commutative* if $A = A^{\mathrm{op}}$.

Suppose that (M, ρ) is a right C-comodule. There are various notations for representing $\rho(m) \in M \otimes C$. We will write

$$\rho(m) = m^{(1)} \otimes m^{(2)}$$

for all $m \in M$, again omitting the summation symbol.

Definition 1. We denote the unique minimal subspace V of C such that $\rho(M) \subseteq M \otimes V$ by $C(\rho)$.

It is not hard to see that $C(\rho)$ is in fact a subcoalgebra of C. Let $m \in M$ and suppose that N is the subcomodule of M which m generates. Then N is finite-dimensional. We may assume that $N \neq (0)$ and $\{m_1, \ldots, m_r\}$ is a basis for N. For $1 \le j \le r$ write $\rho(m_j) = \sum_{i=1}^{r} m_i \otimes c^i_j$. Then the comodule axioms imply that $\epsilon(c^i_j) = \delta^i_j$ and $\Delta(c^i_j) = \sum_{\ell=1}^{r} c^i_\ell \otimes c^\ell_j$ for all $1 \le i \le r$.

The right C-comodule structure (M, ρ) accounts for a left C^*-module structure on M which is described by

$$\alpha \rightharpoonup m = (1_M \otimes \alpha)(\rho(m)) = m^{(1)} \langle \alpha, m^{(2)} \rangle$$

for all $\alpha \in C^*$ and $m \in M$. We will denote this module structure by (M, μ_ρ) and refer to it as the *rational left C^*-module structure on M arising from (M, ρ).*

An element $c \in C$ is said to be *grouplike* if $\Delta(c) = c \otimes c$ and $\epsilon(c) = 1$. We let $G(C)$ denote the set of all grouplike elements of C. Then by [14, Proposition 3.2.1.b)] we have:

LEMMA 1. *Suppose that C is a coalgebra over the field k. Then $G(C)$ is linearly independent.*

If C is a bialgebra over k then $G(C)$ is a semigroup under the multiplication of C. If C is a Hopf algebra with antipode s then the semigroup $G(C)$ is a group since $s(c) \in G(C)$ for $c \in C$ and is a multiplicative inverse for c.

Suppose that C is a coalgebra over the field k which is spanned by a subset S of its grouplike elements $G(C)$. Then by Lemma 1 it follows that $S = G(C)$ and $C = k[S]$ is the free k-module on the set S. For $s \in G(C)$ define $e_s \in C^*$ by $\langle e_s, s' \rangle = \delta_{s,s'}$ for $s' \in G(C)$. Then

$$e_s e_{s'} = \delta_{s,s'} e_s \tag{3}$$

for all $s, s' \in G(C)$ and

$$\sum_{s \in G(C)} e_s = \epsilon. \tag{4}$$

Notice that the left hand side of (4) is meaningful since for $c \in C$, only finitely many of the $e_s(c)$'s are non-zero. Therefore for each $c \in C$, the sum $\sum_{s \in G(C)} e_s(c)$ can be interpreted as a finite sum.

Now suppose that (M, ρ) is a right C-comodule and let (M, μ_ρ) be the left rational C^*-module structure on M arising from (M, ρ). For $m \in M$ only finitely many of the $e_s \rightharpoonup m$'s are not zero. Thus $\sum_{s \in G(C)} e_s \rightharpoonup m$ can be regarded as a finite sum and $m = \sum_{s \in G(C)} e_s \rightharpoonup m$ by (4). Let $M_s = e_s \rightharpoonup M$. We have shown that $M = \sum_{s \in G(C)} M_s$. By (3) this sum is direct. Since $\rho(e_s \rightharpoonup m) = m^{(1)} \otimes (e_s \rightharpoonup m^{(2)})$ for all $m \in M$ and $s \in S$ it is easy to see that $M_s = \rho^{-1}(M \otimes ks)$. Note the $\mathcal{U}$ is a sub-semigroup of C^*.

The difference of two grouplike elements in a coalgebra spans a coideal of the coalgebra. By virtue of Lemma 1 it follows that a coideal of C is spanned by differences of grouplike elements. We summarize all of this in the following:

LEMMA 2. *Suppose that C is a coalgebra over the field k spanned by a subset of grouplike elements S. Then:*

(a) *$S = G(C)$ and $C = k[S]$ is the free k-module on S.*

(b) *Let* (M, ρ) *be a right* C*-comodule and* $M_s = \rho^{-1}(M \otimes ks)$ *for* $s \in G(C)$. *Then* M_s *is a subcomodule of* M *and* $M = \oplus_{s \in G(C)} M_s$.
(c) *Let* I *be a coideal of* C. *Then* I *is spanned by certain differences* $s - s'$, *where* $s, s' \in G(C)$.

If A is a bialgebra over k, then $v \in A$ is said to be *primitive* if $\Delta(v) = 1 \otimes v + v \otimes 1$. The subspace $P(A)$ of primitives of A is a Lie algebra under the product $[u, v] = uv - vu$ for all $u, v \in P(A)$. Let A^o be the dual bialgebra of A. Recall that $\alpha \in A^*$ belongs to A^o if and only if α vanishes on a cofinite ideal of A. It is not hard to see that $\alpha \in A^*$ belongs to A^o if and only if there exists $\nu = \sum_{i=1}^{r} \alpha_i \otimes \beta_i \in A^* \otimes A^*$ such that

$$\langle \alpha, ab \rangle = \sum_{i=1}^{r} \langle \alpha_i, a \rangle \langle \beta_i, b \rangle$$

for all $a, b \in A$. If this is the case, and in addition $r = \operatorname{Rank} \nu$, then $\alpha_i, \beta_i \in A^o$ for $1 \leq i \leq r$.

We note in particular that $P(A^o)$ is the set of all $\alpha \in A^*$ which satisfy

$$\langle \alpha, ab \rangle = \langle \epsilon, a \rangle \langle \alpha, b \rangle + \langle \alpha, a \rangle \langle \epsilon, b \rangle$$

for all $a, b \in A$.

1.3. The reduced FRT construction. Throughout this subsection A is a bialgebra over the field k.

Definition 2. Let A be a bialgebra over the field k. A *left quantum Yang-Baxter* A*-module* is a triple (M, μ, ρ), where (M, μ) is a left A-module and (M, ρ) is a right A-comodule, such that

$$a_{(1)} \cdot m^{(1)} \otimes a_{(2)} m^{(2)} = (a_{(2)} \cdot m)^{(1)} \otimes (a_{(2)} \cdot m)^{(2)} a_{(1)} \tag{5}$$

holds for all $a \in A$ and $m \in M$.

For a discussion of the origin of quantum Yang-Baxter modules the reader is referred to [13]. For their connection with the FRT construction and for a discussion of their structure the reader is referred to [12, 6, 7].

Left quantum Yang-Baxter A-modules give rise to solutions to the QYBE (see [12], [6], [7] for example). Let (M, μ, ρ) be a left quantum Yang-Baxter A-module and define a linear map $R_{(\mu,\rho)}\colon M \otimes M \longrightarrow M \otimes M$ by

$$R_{(\mu,\rho)}(m \otimes n) = m^{(1)} \otimes m^{(2)} \cdot n \tag{6}$$

for all $m, n \in M$. Then $R_{(\mu,\rho)}$ is a solution to the quantum Yang-Baxter equation [12, 6, 7].

Definition 3. Let A be a bialgebra over the field k and let (M, μ, ρ) be a left quantum Yang-Baxter A-module. Then $R_{(\mu,\rho)}$ defined by (6) is the *QYBE solution associated with* (M, μ, ρ).

In [7, Section 8.5] we noted that (5) has the more natural formulation

$$(a{\cdot}m)^{\langle 1\rangle} \otimes (a{\cdot}m)^{(2)} = a{\cdot}m^{\langle 1\rangle} \otimes m^{(2)} \tag{7}$$

for all $a \in A$ and $m \in M$ when A is a commutative cocommutative Hopf algebra with antipode s. In this case (7) implies (5) since A is a commutative cocommutative bialgebra. Since A is commutative, s is an antipode of A^{op}. Starting with the equation

$$(a{\cdot}m)^{\langle 1\rangle} \otimes (a{\cdot}m)^{(2)} = (a_{(3)}{\cdot}m)^{\langle 1\rangle} \otimes (a_{(3)}{\cdot}m)^{(2)} a_{(2)} s(a_{(1)})$$

it is not hard to see that (5) implies (7).

Consider a triple (M, μ, ρ) where (M, μ) is a left A-module and (M, ρ) is a right A-comodule. Let (M, μ_ρ) be the left rational A^*-module structure on M arising from (M, ρ). Then (7) is equivalent to

$$\alpha \rightharpoonup (a{\cdot}m) = a{\cdot}(\alpha \rightharpoonup m) \tag{8}$$

for all $\alpha \in M^*$, $a \in A$, and $m \in M$. Thus (5) and (8) are equivalent when A is a commutative cocommutative Hopf algebra over k.

We need the notion of M-reduced [11, Section 3] in order to describe the reduced FRT construction.

Definition 4. Let A be a bialgebra over k and suppose (M, μ) is a left A-module. Then A is *M-reduced* if the only coideal of A contained in $\mathrm{ann}_A(M)$ is (0).

Let (M, μ) be a left A-module. Then the sum I of all coideals of A contained in $\mathrm{ann}_A(M)$ is a bi-ideal of A. Thus $\widetilde{A} = A/I$ is a bialgebra over k with the quotient bialgebra structure. Let π: $A \longrightarrow \widetilde{A}$ be the projection. Then $(M, \widetilde{\mu})$ is a left $\widetilde{A}$-module, where $\widetilde{\mu}$ is determined by $\widetilde{\mu}(\pi \otimes 1_M) = \mu$, and $\widetilde{A}$ is $(M, \widetilde{\mu})$-reduced. We leave the reader to work out the details.

In the finite-dimensional case solutions to the quantum Yang-Baxter equation have the form $R_{(\mu,\rho)}$ by the next result. The following proposition is Theorem 4.2.2 in [7] which is a slight variation of Theorem 2 in [11].

PROPOSITION 1. *Suppose that M is a finite-dimensional vector space over the field k and that R: $M \otimes M \longrightarrow M \otimes M$ is a solution to the quantum Yang-Baxter equation. Then the bialgebra $\widetilde{A(R)}$ satisfies the following properties*:

(a) *There exists a left quantum Yang-Baxter $\widetilde{A(R)}$-module structure (M, μ, ρ) on M such that $\widetilde{A(R)}$ is M-reduced and $R = R_{(\mu,\rho)}$.*

(b) *Suppose that A is a bialgebra over the field k and (M, μ', ρ') is a left quantum Yang-Baxter A-module structure on M such A is M-reduced and $R = R_{(\mu',\rho')}$. There is a bialgebra map $F\colon \widetilde{A(R)} \longrightarrow A$ uniquely defined by $(1_M \otimes F)\rho = \rho'$. Furthermore $\mu = \mu'(F \otimes 1_M)$, F is one-one, and F is an isomorphism when $A(\rho')$ (see Definition 1) generates A as an algebra.*

Definition 5. Let M be a finite-dimensional vector space over the field k and suppose that $R\colon M \otimes M \longrightarrow M \otimes M$ is a solution to the quantum Yang-Baxter equation. The bialgebra $\widetilde{A(R)}$ described in the previous proposition is the *reduced FRT construction.*

The reduced FRT construction $\widetilde{A(R)}$ is a quotient of the FRT construction $A(R)$ which has a universal mapping property similar to that of Proposition 1. See Theorem 2 in [12].

Suppose that M is a finite-dimensional vector space over k and (M, μ, ρ) is a left quantum Yang-Baxter A-module structure on M. Let R be the solution to the quantum Yang-Baxter equation associated with (M, μ, ρ). Then $\widetilde{A(R)}$ is a sub-bialgebra of a quotient of A.

To establish this, we first let I be the bi-ideal of A which is the sum of the coideals of A contained in $\mathrm{ann}_A(M)$. Set $\widetilde{A} = A/I$ and let $\pi\colon A \longrightarrow \widetilde{A}$ and $(M, \widetilde{\mu})$ be as above. Since π is a coalgebra map, $\widetilde{\rho}\colon M \longrightarrow M \otimes \widetilde{A}$ defined by $\widetilde{\rho} = (1_M \otimes \pi)\rho$ gives M a right $\widetilde{A}$-comodule structure $(M, \widetilde{\rho})$. It is easy to see that $(M, \widetilde{\mu}, \widetilde{\rho})$ is a left quantum Yang-Baxter $\widetilde{A}$-module and that $R_{(\mu,\rho)} = R_{(\widetilde{\mu},\widetilde{\rho})}$. Since $\widetilde{A}$ is $(M, \widetilde{\mu})$-reduced, it follows that $\widetilde{A(R)} \simeq \widetilde{A}(\widetilde{\rho})$ by Proposition 1.

1.4. The Hopf algebra $\mathrm{U}(r, k)$. Let L be an r-dimensional abelian Lie algebra over the field k. We denote the universal enveloping algebra $U(L)$ by $\mathrm{U}(r, k)$. Choose a basis $\mathcal{B} = \{x_1, \ldots, x_r\}$ for L. Then as a k-algebra $\mathrm{U}(r, k) = k[x_1, \ldots, x_r]$ is the polynomial algebra over k in commuting indetermants $x_1, \ldots, x_r$. For $\boldsymbol{n} = (n_1, \ldots, n_r) \in \mathrm{N} \times \cdots \times \mathrm{N} = \mathrm{N}^r$ define

$$x^{\boldsymbol{n}} = x_1^{n_1} \cdots x_r^{n_r}. \tag{9}$$

Thus the $x^{\boldsymbol{n}}$'s form a linear basis for $\mathrm{U}(r, k)$. Let $\mathrm{U}(r, k)_n$ be the homogeneous (total) degree n subspace of $\mathrm{U}(r, k)$ for all $n \geq 0$, i.e. $\mathrm{U}(r, k)_n$ is the span of the $x^{\boldsymbol{n}}$'s which satisfy $|x^{\boldsymbol{n}}| = n$, where $|\boldsymbol{n}| = n_1 + \cdots + n_r$. Thus $\mathrm{U}(r, k)$ is a graded algebra since

$$\mathrm{U}(r, k) = \oplus_{n=0}^{\infty} \mathrm{U}(r, k)_n$$

and

$$\mathrm{U}(r, k)_m \mathrm{U}(r, k)_n = \mathrm{U}(r, k)_{m+n}$$

for all $m, n \geq 0$.

Set $\mathrm{U}(r, k)_{(0)} = \mathrm{U}(r, k)$ and let $\mathrm{U}(r, k)_{(n)}$ be the span of the $x^{\boldsymbol{n}}$'s where $|\boldsymbol{n}| \geq n$. Notice that

$$\mathrm{U}(r, k)_{(m)}\mathrm{U}(r, k)_{(n)} = \mathrm{U}(r, k)_{(m+n)} \tag{10}$$

for all $m, n \geq 0$ and

$$\mathrm{U}(r, k)_{(0)} \supseteq \mathrm{U}(r, k)_{(1)} \supseteq \mathrm{U}(r, k)_{(2)} \supseteq \cdots \quad . \tag{11}$$

For $1 \leq i \leq r$ let $\epsilon_i = (0, \ldots, 1, \ldots, 0)$ be the r-tuple whose entries are 0 except for the i^{th}, which is 1. Define $X_i \in \mathrm{U}(r, k)^*$ by

$$\langle X_i, x^{\boldsymbol{n}} \rangle = \delta_{\epsilon_i, \boldsymbol{n}} \tag{12}$$

for all $\boldsymbol{n} \in \mathrm{N}^{\mathrm{r}}$. Let $\boldsymbol{n} = (n_1, \ldots, n_r) \in N^r$. Set

$$X^{\boldsymbol{n}} = X_1^{n_1} \cdots X_r^{n_r} \tag{13}$$

and set $\boldsymbol{n}! = n_1! \cdots n_r!$. The notation $\boldsymbol{m} \leq \boldsymbol{n}$ means that $m_i \leq n_i$ for all $1 \leq i \leq r$, where $\boldsymbol{m} = (m_1, \ldots, m_r)$. Set

$$\binom{\boldsymbol{n}}{\boldsymbol{m}} = \prod_{i=1}^{r} \binom{n_i}{m_i}.$$

Thus $\binom{\boldsymbol{n}}{\boldsymbol{m}} = 0$ unless $\boldsymbol{m} \leq \boldsymbol{n}$, in which case

$$\binom{\boldsymbol{n}}{\boldsymbol{m}} = \frac{\boldsymbol{n}!}{\boldsymbol{m}!(\boldsymbol{n} - \boldsymbol{m})!}.$$

We are nearly ready to describe the structure of $\mathrm{U}(r, k)$ as a Hopf algebra. First some more notation. Let $\mathrm{P}(r, k) = P(\mathrm{U}(r, k))$ be the space of primitive elements of $\mathrm{U}(r, k)$, let $\mathrm{P}^o(r, k)$ be the space of primitive elements of $\mathrm{U}(r, k)^o$, and let $\mathrm{U}^o(r, k)$ be the subalgebra of $\mathrm{U}(r, k)^*$ generated by $\mathrm{P}^o(r, k)$.

The reader is left with with the details of proof of the following lemma.

LEMMA 3. *Let $r \geq 1$ and suppose that the field k has characteristic 0. Let $\mathcal{B} = \{x_1, \ldots, x_r\}$ be a basis for* $\mathrm{U}(r, k)_1$ *and suppose that $x^{\boldsymbol{n}}$ and $X^{\boldsymbol{n}}$ are defined by* (9)–(13). *Then*:

(a) $\mathrm{P}(r, k) = \mathrm{U}(r, k)_1$. *In particular $\mathcal{B}$ is a basis for the subspace of primitive elements of* $\mathrm{U}(r, k)$, *and the $x^{\boldsymbol{n}}$'s form a basis for* $\mathrm{U}(r, k)$.

(b) $\Delta(x^{\boldsymbol{n}}) = \sum_{\boldsymbol{m} \leq \boldsymbol{n}} \binom{\boldsymbol{n}}{\boldsymbol{m}} x^{\boldsymbol{n}-\boldsymbol{m}} \otimes x^{\boldsymbol{m}}$ *for all $\boldsymbol{n} \in \mathrm{N}^{\mathrm{r}}$.*

(c) $X^{\boldsymbol{n}}(x^{\boldsymbol{m}}) = \boldsymbol{n}!\delta_{\boldsymbol{n},\boldsymbol{m}}$ *for all $\boldsymbol{n}, \boldsymbol{m} \in \mathrm{N}^{\mathrm{r}}$. Thus the $X^{\boldsymbol{n}}$'s form a linearly independent set.*

(d) $\mathrm{P}^o(r,k)$ *has linear basis* $\{X_1,\ldots,X_r\}$. *In particular* $\mathrm{Dim}\,\mathrm{P}^o(r,k) = \mathrm{Dim}\,\mathrm{P}(r,k) = r$.
(e) $\mathrm{U}^o(r,k)$ *is a sub-bialgebra of* $\mathrm{U}(r,k)$ *and the correspondence* $x_i \mapsto X_i$ *determines a bialgebra isomorphism* $\mathrm{U}(r,k) \simeq \mathrm{U}^o(r,k)$.
(f) $\mathrm{U}^o(r,k)$ *is a dense subalgebra of* $\mathrm{U}(r,k)^*$.

We now consider the subalgebras and quotients of $\mathrm{U}(r,k)$. The bialgebra $\mathrm{U}(r,k)$ belongs to the class of pointed irreducible cocommutative bialgebras. It is clear that sub-bialgebras and quotients of cocommutative bialgebras are cocommutative. Subcoalgebras of pointed irreducible coalgebras are pointed irreducible. Quotients of pointed irreducible coalgebras are pointed irreducible by [14, Corollary 8.0.9]. Therefore sub-bialgebras and quotients of cocommutative pointed irreducible bialgebras are themselves cocommutative and pointed irreducible. By [14, Lemma 9.2.3], a pointed irreducible bialgebra is a Hopf algebra.

Now assume that the characteristic of k is 0 and H is a cocommutative pointed irreducible Hopf algebra over k. Then $H \simeq U(P(H))$ as Hopf algebras by [14, Theorem 13.0.1]. We make the following definition.

Definition 6. Let H be a cocommutative pointed irreducible Hopf algebra over the field k. Then $\mathrm{rank}\,H = \mathrm{Dim}\,P(H)$.

By part (a) of Lemma 3 we have:

LEMMA 4. *Suppose that the field k has characteristic* 0. *Then* $\mathrm{rank}\,\mathrm{U}(r,k) = r$.

The conclusion of the lemma is false when the characteristic of k is not 0 except in the case when $r = 0$.

PROPOSITION 2. *Suppose that the field k has characteristic* 0.

(a) *Let B be a sub-bialgebra of* $\mathrm{U}(r,k)$. *Then B is a sub-Hopf algebra of* $\mathrm{U}(r,k)$ *and* $B \simeq \mathrm{U}(s,k)$ *for some* $s \le r$. *Furthermore* $B = \mathrm{U}(r,k)$ *if and only if* $s = r$, *or equivalently* $\mathrm{rank}\,B = \mathrm{rank}\,\mathrm{U}(r,k)$.
(b) *Suppose that I is a bi-ideal of* $\mathrm{U}(r,k)$. *Then* $\mathrm{U}(r,k)/I \simeq \mathrm{U}(s,k)$ *for some* $s \le r$. *Furthermore* $I = (0)$ *if and only if* $s = r$, *or equivalently* $\mathrm{rank}\,\mathrm{U}(r,k)/I = \mathrm{rank}\,\mathrm{U}(r,k)$.

Proof. In light of the preceding comments we need only establish part (b). Suppose that I is a bi-ideal of $\mathrm{U}(r,k)$ and let $\pi\colon \mathrm{U}(r,k) \longrightarrow \mathrm{U}(r,k)/I$ be the projection. Set $L = \mathrm{P}(r,k)$. Then $\pi(L) \subseteq P(\mathrm{U}(r,k)/I)$. Since L generates $\mathrm{U}(r,k)$ as an algebra it follows that $\pi(L)$ generates $\mathrm{U}(r,k)/I$ as an algebra. Since the monomials in a linear basis for $P(\mathrm{U}(r,k)/I)$ form a linear basis for $\mathrm{U}(r,k)/I$ it follows that $\pi(L) = P(\mathrm{U}(r,k)/I)$. Therefore $\mathrm{U}(r,k)/I \simeq \mathrm{U}(s,k)$, where $s = \mathrm{Dim}\,P(\mathrm{U}(r,k)/L)$. Now

π is an isomorphism if and only if $\pi|_L\colon L \longrightarrow \pi(L)$ is a linear isomorphism. This is the case if and only if $s = r$ which happens if and only if $\operatorname{Ker}\pi|_L = I \cap L = (0)$. But $I \cap L = (0)$ if and only if $I = (0)$ by [14, Lemma 11.0.1]. □

2. The semigroup algebra as a reduced FRT construction

Throughout this section S is a (multiplicative) semigroup with neutral element e and $A = k[S]$ is the semigroup algebra over k. We give A a bialgebra structure by making $s \in S$ grouplike. By part (a) of Lemma 2 it follows that $S = G(A)$. In this section we characterize the left quantum Yang-Baxter A-modules and for the associated solution R to the quantum Yang-Baxter equation we compute the reduced FRT construction $\widetilde{A(R)}$. It turns out that $\widetilde{A(R)} \simeq k[\mathcal{S}]$ where $\mathcal{S}$ is a quotient of a sub-semigroup of S.

We note that $\widetilde{A(R)}$ has been studied, when $\widetilde{A(R)}$ is spanned by grouplike elements, in special cases in [11] and [7, Chapter 4].

Let M be a left A-module. To say that A is M-reduced is to say that A is faithfully represented by endomorphisms of M.

PROPOSITION 3. *Suppose that S is a semigroup and $A = k[S]$ is the semigroup algebra of S over the field k. Let (M, μ) be a left A-module and suppose that $\pi\colon A \longrightarrow \operatorname{End}(M)$ is the representation afforded by (M, μ). Then the following are equivalent*:

(a) *A is M-reduced.*
(b) *The restriction $\pi|_S\colon S \longrightarrow \operatorname{End}(M)$ is one-one.*

Proof. Suppose that A is M-reduced and let $s, s' \in S$ satisfy $\pi(s) = \pi(s')$. Then $s - s' \in \operatorname{ann}_A(M)$ and spans a coideal of A. Therefore $s - s' = 0$. We have shown part (a) implies part (b).

To show part (b) implies part (a), suppose that the restriction $\pi|_S$ is one-one. Let I be a coideal of A contained in $\operatorname{ann}_A(M)$. Suppose that $s, s' \in S$ and $s - s' \in I$. Then $\pi(s) = \pi(s')$ which means that $s - s' = s - s = 0$. By part (c) of Lemma 2 we conclude that $I = (0)$. Thus A is M-reduced. □

It is convenient to express a representation of S by endomorphisms of M in a slightly different terminology.

Definition 7. Let S be a multiplicative semigroup with neutral element e and suppose that M is a vector space over the field k. A set of endomorphisms $\{T_s\}_{s\in S}$ is a *representing set of endomorphisms of S in M* if $T_e = 1_M$ and $T_sT_{s'} = T_{ss'}$ for $s, s' \in S$.

PROPOSITION 4. *Suppose that S is a semigroup and $A = k[S]$ is the semigroup algebra of S over the field k. Let (M, ρ) be a right A-comodule and suppose that $\pi\colon A \longrightarrow \mathrm{End}(M)$ is the representation afforded by the rational left A^*-module structure (M, μ_ρ) arising from (M, ρ). Then $A(\rho)$ is the span of the $s \in S$ such that $\pi(e_s) \neq 0$, where $e_s \in A^*$ is defined by $\langle e_s, s'\rangle = \delta_{s,s'}$ for all $s' \in S$.*

Proof. By part (b) of Lemma 2 we have $M = \oplus_{s\in S} M_s$ where $M_s = \rho^{-1}(M \otimes ks)$ for $s \in S$. Now $A(\rho)$ is the span of the $s \in S$ such that $M_s \neq (0)$. Since $\pi(e_s)(M_{s'}) = \delta_{s,s'} M_s$ it follows that $M_s \neq (0)$ if and only if $\pi(e_s) \neq (0)$. □

Let $\pi\colon S \longrightarrow \mathrm{End}(M)$ be the representation of S implicit in the previous proposition. Then the endomorphisms $E_s = \pi(s)$ of M satisfy the conditions of the following definition.

Definition 8. Let S be a set and suppose that M is a vector space over the field k. A set $\{E_s\}_{s\in S}$ of endomorphisms of M is a *spanning orthogonal set of endomorphisms of M* if $E_s E_{s'} = \delta_{s,s'} E_s$ for all $s, s' \in S$ and $\sum_{s\in S} \mathrm{Im}\, E_s = M$.

Observe that the sum $M = \sum_{s\in S} \mathrm{Im}\, E_s$ described in the definition is direct. Also for $m \in M$ the set of $s \in S$ such that $E_s(m) \neq 0$ is finite. Therefore $\sum_{s\in S} E_s$ defined by $(\sum_{s\in S} E_s)(m) = \sum_{s\in S} E_s(m)$ for $m \in M$ is a well-defined endomorphism of M since the right hand side of the last equation can be regarded as a finite sum.

Our next result characterizes the left A-modules, right A-comodules, and the left quantum Yang-Baxter A-modules of a semigroup algebra $A = k[S]$.

PROPOSITION 5. *Suppose that S is a semigroup and M is a vector space over k. Then*:

(a) *There is a one-one correspondence*

$$\mathcal{T} \mapsto (M, \mu_{\mathcal{T}})$$

between the set of representing sets of endomorphisms $\mathcal{T} = \{T_s\}_{s\in S}$ of S in M and the set of left A-module structures on M, where $s\cdot m = T_s(m)$ for all $s \in S$ and $m \in M$.

(b) *There is a one-one correspondence*

$$\mathcal{N} \mapsto (M, \rho_{\mathcal{E}})$$

between the set of spanning orthogonal sets of endomorphisms $\mathcal{E} = \{E_s\}_{s\in S}$ of M and the set of right A-comodule structures on M, where

$$\rho_{\mathcal{E}}(m) = \sum_{s\in S} E_s(m) \otimes s$$

for all $m \in M$.

Suppose that $(M, \mu_{\mathcal{T}})$ and $(M, \rho_{\mathcal{E}})$ are as described in parts (a) and (b) respectively. Then:

(c) *$(M, \mu_{\mathcal{T}}, \rho_{\mathcal{E}})$ is a left quantum Yang-Baxter A-module if and only if the endomorphisms of $\mathcal{T}$ and $\mathcal{E}$ commute. In this case the associated solution to the quantum Yang-Baxter equation is given by*

$$R = \sum_{s \in S} E_s \otimes T_s,$$

where $R = R_{(\mu_{\mathcal{T}}, \rho_{\mathcal{E}})}$.

Proof. Part (a) follows since we are really characterizing the representations $\pi \colon S \longrightarrow \mathrm{End}\,(M)$ which are in one-one correspondence with the representations of A as endomorphisms of M. Part (b) is a straightforward exercise based on part (b) of Lemma 2.

It remains to establish part (c). Recall from Section 1 that the e_s's defined by $\langle e_s, s' \rangle = \delta_{s,s'}$ for $s, s' \in S$ span a dense subspace of A^*. Now $(M, \mu_{\mathcal{T}}, \rho_{\mathcal{E}})$ is a left quantum Yang-Baxter A-module if and only if (8) holds, namely

$$\alpha \rightharpoonup (a \cdot m) = a \cdot (\alpha \rightharpoonup m)$$

for all $\alpha \in A^*$ and $m \in M$. Since the e_s's span a dense subspace of A^* and S is a basis for A this last condition holds if and only if

$$e_s \rightharpoonup (s' \cdot m) = s' \cdot (e_s \rightharpoonup m)$$

for all $s, s' \in S$. Fix $s, s' \in S$. Since $e_s \rightharpoonup m = E_s(m)$ and $s \cdot m = T_s(m)$ for all $m \in M$, this last equation is the same as $E_s T_{s'} = T_{s'} E_s$. We have established part (c), and the proof is complete. □

We leave the proof of the following to the reader.

THEOREM 1. *Suppose that S is a semigroup and $A = k[S]$ is the semigroup algebra of S over the field k. Let M be a vector space over k. Suppose that $\{T_s\}_{s \in S}$ is a set of endomorphisms of M representing S and $\{E_s\}_{s \in S}$ is a spanning orthogonal set of endomorphisms of M. Assume that the members of $\mathcal{T}$ and $\mathcal{E}$ commute and set*

$$R = \sum_{s \in S} E_s \otimes T_s.$$

Then:

(a) *R is a solution to the quantum Yang-Baxter equation.*
(b) *Assume that M is finite-dimensional. Let $S(\rho)$ be the sub-semigroup of S generated by the $s \in S$ such that $E_s \neq 0$, and let $\mathcal{S}$ be the set of equivalence classes of $S(\rho)$ under the relation $s \sim s'$ if and only if $T_s = T_{s'}$. Then $\mathcal{S}$ is a multiplicative semigroup with neutral element $[e]$ and product $[s][s'] = [ss']$ for $s, s' \in S$, and $\widetilde{A(R)} \simeq k[\mathcal{S}]$.*

3. The enveloping algebra of an abelian Lie algebra as a reduced FRT construction

Let M be a finite-dimensional vector space over the field k. In this section we find all solutions R: $M \otimes M \longrightarrow M \otimes M$ to the quantum Yang-Baxter equation such that $\widetilde{A(R)} \simeq \mathrm{U}(r, k)$ for some $r \geq 1$ when the characteristic of k is 0.

We describe the left $\mathrm{U}(r, k)$-modules, the right $\mathrm{U}(r, k)$-comodules, and the left quantum Yang-Baxter $\mathrm{U}(r, k)$-modules in terms of r-tuples of endomorphisms of M. Initially we do not assume that M is finite-dimensional.

We begin this section with a study of the left $\mathrm{U}(r, k)$-modules M.

PROPOSITION 6. *Suppose that M is a vector space over the field k, $r \geq 1$, and π: $\mathrm{U}(r, k) \longrightarrow \mathrm{End}\,(M)$ is a representation of $\mathrm{U}(r, k)$. Let (M, μ) be the resulting left $\mathrm{U}(r, k)$-module structure on M. Assume that the characteristic of k is 0. Then the following are equivalent*:

(a) *$\mathrm{U}(r, k)$ is (M, μ)-reduced.*
(b) *For all bases $\{x_1, \ldots, x_r\}$ for $\mathrm{P}(r, k)$ the set $\{T_1, \ldots, T_r\}$ of endomorphisms of M is linearly independent, where $T_i = \pi(x_i)$ for all $1 \leq i \leq r$.*
(c) *There exists a basis $\{x_1, \ldots, x_r\}$ for $\mathrm{P}(r, k)$ such that the set $\{T_1, \ldots, T_r\}$ of endomorphisms of M is linearly independent, where $T_i = \pi(x_i)$ for all $1 \leq i \leq r$.*

Proof. Let $L = \mathrm{P}(r, k)$ and I be the largest coideal of $\mathrm{U}(r, k)$ contained in $\mathrm{ann}_{\mathrm{U}(r,\, k)}(M)$. Consider the restriction map $\pi|_L$: $L \longrightarrow \mathrm{End}\,(M)$. Since $\mathrm{Ker}\,\pi|_L = L \cap I$, and I is a coideal of $\mathrm{U}(r, k)$, it follows by [14, Lemma 11.0.1] that $I = (0)$ if and only if $L \cap I = (0)$. The proposition now follows. □

PROPOSITION 7. *Suppose that M is a vector space over the field k, $r \geq 1$ and (M, ρ) is a right $\mathrm{U}(r, k)$-comodule. Assume that the characteristic of k is 0 and let π: $\mathrm{U}(r, k)^* \longrightarrow \mathrm{End}\,(M)$ be the representation of $\mathrm{U}(r, k)^*$ afforded by the rational left $\mathrm{U}(r, k)^*$-module structure (M, μ_ρ). Then the following are equivalent*:

(a) *$\mathrm{U}(r, k)(\rho)$ generates $\mathrm{U}(r, k)$ as an algebra.*
(b) *For all bases $\{X_1, \ldots, X_r\}$ for $\mathrm{P}^o(r, k)$ the set $\{N_1, \ldots, N_r\}$ of endomorphisms of M is linearly independent, where $N_i = \pi(X_i)$ for all $1 \leq i \leq r$.*
(c) *There exists a basis $\{X_1, \ldots, X_r\}$ for $\mathrm{P}^o(r, k)$ such that the set of endomorphisms $\{N_1, \ldots, N_r\}$ of M is linearly independent, where $N_i = \pi(X_i)$ for all $1 \leq i \leq r$.*

Proof. Let $A = \mathrm{U}(r, k)$, let B be the subalgebra of A generated by $A(\rho)$, and consider the map Res: $P(A^o) \longrightarrow P(B^o)$ defined by $\mathrm{Res}(p) = p|_B$. Let $p \in P(A^o) = \mathrm{P}^o(r, k)$. Then $\mathrm{Ker}\, p$ is a subalgebra of A. Thus it follows that

$p(A(\rho)) = (0)$ if and only if $p(B) = (0)$. Since $\mathrm{ann}_{A^*}(M) = A(\rho)^{\perp}$ we conclude that $p \in \mathrm{ann}_{A^*}(M)$ if and only if $p(B) = (0)$.

We have shown that $\mathrm{Ker\,Res} = \mathrm{P}^o(r, k) \cap \mathrm{ann}_{A^*}(M) = \mathrm{Ker}\,\pi|_{\mathrm{P}^o(r,k)}$. Therefore $\mathrm{Rank\,Res} = \mathrm{Rank}\,\pi|_{\mathrm{P}^o(r,k)}$. By part (a) of Proposition 2 and Lemma 3, Res is onto. Thus we compute

$$\mathrm{Dim}\,P(B) = \mathrm{Dim}\,P(B^o) = \mathrm{Rank\,Res} = \mathrm{Rank}\,\pi|_{\mathrm{P}^o(r,k)}.$$

By part (a) of Proposition 2 again we have $A = B$ if and only if $r = \mathrm{Dim}\,P(B)$, and $r = \mathrm{Dim}\,\mathrm{P}^o(r, k)$ by part (d) of Lemma 3. Thus it follows that $A = B$ if and only if $\pi|_{\mathrm{P}^o(r,k)}$ is one-one. Now the proof is easily completed. □

We next characterize the left modules, right comodules, and the left quantum Yang-Baxter modules for $\mathrm{U}(r, k)$ when the field k has characteristic 0. We will find the following notation conventions very convenient. Let V be a vector space over k and $r \geq 1$ be a fixed integer. For an r-tuple $\mathcal{T} = (T_1, \ldots, T_r)$ of endomorphisms of M we define

$$\mathcal{T}^{\boldsymbol{n}} = T_1^{n_1} \cdots T_r^{n_r}$$

for all $\boldsymbol{n} = (n_1, \ldots, n_r) \in \mathrm{N} \times \cdots \times \mathrm{N} = \mathrm{N}^{\mathrm{r}}$.

To characterize the right comodules for $\mathrm{U}(r, k)$ we will need the notion of locally nilpotent endomorphism.

Definition 9. A linear endomorphism $T\colon V \longrightarrow V$ of a vector space over V over the field k is *locally nilpotent* if for every $v \in V$ there is an integer $n \geq 0$ such that $T^n(v) = 0$.

A basic example of a locally nilpotent endomorphism is the following. Let (M, ρ) be a right C-comodule for a coalgebra C over the field k and let (M, μ_ρ) be the resulting rational left C^*-module structure on M. Let $\pi\colon C^* \longrightarrow \mathrm{End}\,(M)$ be the representation of C^* afforded by (M, μ_ρ). Then

$$\pi(\alpha)(m) = \alpha \rightharpoonup m = m^{(1)}\langle \alpha, m^{(2)} \rangle$$

for all $\alpha \in C^*$ and $m \in M$. Since every $m \in M$ generates a finite-dimensional subcomodule $(N, \rho|_N)$ of (M, ρ), and thus $C(\rho|_N)$ is a finite-dimensional subcoalgebra of C, it follows that $\pi(\alpha)$ is a locally nilpotent endomorphism of M for all $\alpha \in \mathrm{Rad}(C^*)$.

Now suppose that V is a vector space over the field k and $N \in \mathrm{End}\,(V)$ is locally nilpotent. Then

$$T = \sum_{\ell=0}^{\infty} \alpha_\ell N^\ell$$

is a well-defined endomorphism of V for any $\alpha_0, \alpha_1, \alpha_2, \ldots \in k$. To see this, note that for a given $v \in V$ there are only finitely many $\ell \geq 0$ such that $N^\ell(v) \neq 0$. Thus

$$T(v) = \sum_{\ell=0}^{\infty} N^\ell(v)$$

has finitely many non-zero summands and can thus be regarded as a finite sum. For the same reason if $\mathcal{N} = (N_1, \ldots, N_r)$ is an r-tuple of locally nilpotent endomorphism of V then

$$T = \sum_{\boldsymbol{n} \in N^r} \alpha_{\boldsymbol{n}} \mathcal{N}^{\boldsymbol{n}}$$

is a well-defined endomorphism of V for all choices of coefficients $\alpha_{\boldsymbol{n}} \in k$. If in addition $\mathcal{T} = (T_1, \ldots, T_r)$ is an r-tuple of endomorphisms of V then

$$T = \sum_{\boldsymbol{n} \in N^r} \alpha_{\boldsymbol{n}} \mathcal{N}^{\boldsymbol{n}} \otimes \mathcal{T}^{\boldsymbol{n}}$$

is a well-defined endomorphism of $V \otimes V$ for any choice of coefficients $\alpha_{\boldsymbol{n}} \in k$. There are obvious generalizations of the latter to the tensor product of a finite number of vector spaces over k.

PROPOSITION 8. *Suppose that M is a vector space over the field k and $r \geq 1$. Assume that the characteristic of k is 0. Let $\mathcal{B} = \{x_1, \ldots, x_r\}$ be a fixed basis for the space of primitives* $\mathrm{P}(r, k)$ *of* $\mathrm{U}(r, k)$. *Then*:

(a) *There is a one-one correspondence*

$$\mathcal{T} \mapsto (M, \mu_{\mathcal{T},\mathcal{B}})$$

between the set of r-tuples $\mathcal{T} = (T_1, \ldots, T_r)$ of commuting endomorphisms of M and the set of left $\mathrm{U}(r, k)$*-module structures on M, where $x_i \cdot m = T_i(m)$ for all $1 \leq i \leq r$ and $m \in M$.*

(b) *There is a one-one correspondence*

$$\mathcal{N} \mapsto (M, \rho_{\mathcal{N},\mathcal{B}})$$

between the set of r-tuples $\mathcal{N} = (N_1, \ldots, N_r)$ of commuting locally nilpotent endomorphisms of M and the set of right $\mathrm{U}(r, k)$*-comodule structures on M, where*

$$\rho_{\mathcal{N},\mathcal{B}}(m) = \sum_{\boldsymbol{n} \in N^r} \mathcal{N}^{\boldsymbol{n}}(m) \otimes \frac{x^{\boldsymbol{n}}}{\boldsymbol{n}!}$$

for all $m \in M$.

Suppose that $(M, \mu_{\mathcal{T},\mathcal{B}})$ *and* $(M, \rho_{\mathcal{N},\mathcal{B}})$ *are as described in parts* (*a*) *and* (*b*) *respectively. Then*:

(c) $(M, \mu_{\mathcal{T},\mathcal{B}}, \rho_{\mathcal{N},\mathcal{B}})$ *is a left quantum Yang-Baxter* $\mathrm{U}(r, k)$*-module if and only if the components of* $\mathcal{T}$ *and* $\mathcal{N}$ *commute. In this case the associated solution to the quantum Yang-Baxter equation is given by*

$$R = \sum_{\boldsymbol{n}\in N^r} \frac{1}{\boldsymbol{n}!}\mathcal{N}^{\boldsymbol{n}} \otimes \mathcal{T}^{\boldsymbol{n}},$$

where $R = R_{(\mu_{\mathcal{N},\mathcal{B}},\rho_{\mathcal{T},\mathcal{B}})}$.

Proof. Part (a) follows from the usual formulation of left A-module structures (M, μ) on M in terms of representations $\pi_\mu\colon A \longrightarrow \mathrm{End}(M)$ given by $\mu(a \otimes m) = \pi_\mu(a)(m)$ for any algebra A over k, where $a \in A$ and $m \in M$, together with the observation that as an algebra $A = \mathrm{U}(r, k)$ is the (commutative) polynomial algebra over k on any basis for $P(A)$.

To show part (b) we first note that the subalgebra $\mathcal{A} = \mathrm{U}^o(r, k)$ of $A^o = \mathrm{U}(r, k)^o$ generated by $\mathrm{P}^o(r, k) = P(A^o)$ is a dense subspace of A^* by part (f) of Lemma 3. Thus if $\rho\colon M \longrightarrow M \otimes A$ is a linear map we have that (M, ρ) is a right A-comodule if and only if (M, μ_ρ) is a left $\mathcal{A}$-module, where this module action is given by

$$\alpha{\cdot}m = (1_M \otimes \alpha)(\rho(m))$$

for all $\alpha \in \mathcal{A}$ and $m \in M$.

First of all assume that $\mathcal{N} = (N_1 \dots, N_r)$ is an r-tuple whose components are commuting locally nilpotent endomorphisms of M. Define $\rho_{\mathcal{N},B}\colon M \longrightarrow M \otimes A$ by

$$\rho_{\mathcal{N},B}(m) = \sum_{\boldsymbol{n}\in \mathrm{N}^r} \mathcal{N}^{\boldsymbol{n}}(m) \otimes \frac{x^{\boldsymbol{n}}}{\boldsymbol{n}!}$$

for all $m \in M$. By part (b) of Lemma 3 it follows that

$$\Delta\left(\frac{x^{\boldsymbol{n}}}{\boldsymbol{n}!}\right) = \sum_{\boldsymbol{m}\le\boldsymbol{n}} \frac{x^{\boldsymbol{n}-\boldsymbol{m}}}{(\boldsymbol{n}-\boldsymbol{m})!} \otimes \frac{x^{\boldsymbol{n}}}{\boldsymbol{m}!}$$

for all $\boldsymbol{n} \in \mathrm{N}^r$. Therefore $(M, \rho_{\mathcal{N},\mathcal{B}})$ is a right $\mathrm{U}(r, k)$-comodule.

Conversely, suppose that (M, ρ) is a right $A = \mathrm{U}(r, k)$-comodule. Let $\pi\colon A^* \longrightarrow \mathrm{End}(M)$ be the representation of the induced left rational A^*-module structure (M, μ_ρ) on M. By parts (b) and (d) of Lemma 3 the set $\{X_1, \dots, X_r\}$ is a basis for $P(A^o)$, where $X_i(x^{\boldsymbol{n}}) = \delta_{\epsilon_i,\boldsymbol{n}}$ for all $\boldsymbol{n} \in \mathrm{N}^r$, and $X^{\boldsymbol{n}}(x^{\boldsymbol{m}}) = \boldsymbol{n}!\delta_{\boldsymbol{n},\boldsymbol{m}}$ for all $\boldsymbol{n}, \boldsymbol{m} \in \mathrm{N}^r$. Let $N_i = \pi(X_i)$. Then $N_1, \dots, N_r$ commute since $X_1, \dots, X_r$ commute. Now let $m \in M$ and suppose that N is the finite-dimensional sub-comodule of M which m generates. Then $\rho(N) \subseteq N \otimes V$ for some finite-dimensional subspace

V of A. Therefore there exist an integer $n_{\min} \geq 0$ such that V is in the span of the $x^{\boldsymbol{n}}$'s, where $\boldsymbol{n} = (n_1, \ldots, n_r)$ satisfies $n_i \leq n_{\min}$ for all $1 \leq i \leq r$. This means

$$\mathcal{N}^{\boldsymbol{n}}(m) = X^{\boldsymbol{n}} \rightharpoonup m \in M\langle X^{\boldsymbol{n}}, V\rangle = (0)$$

whenever $n_i > n_{\min}$ holds for one of the components n_i of $\boldsymbol{n}$. In particular N_i is a locally nilpotent endomorphism of M for $1 \leq i \leq r$. Since $\mathcal{A}$ is a dense subspace of A^* and is spanned by the $X^{\boldsymbol{n}}$'s, the calculation

$$\begin{aligned}(1_M \otimes X^{\boldsymbol{m}})\left(\sum_{\boldsymbol{n} \in \mathrm{N}^r} \mathcal{N}^{\boldsymbol{n}}(m) \otimes \frac{x^{\boldsymbol{n}}}{\boldsymbol{n}!}\right) &= \mathcal{N}^{\boldsymbol{m}}(m) \\ &= X^{\boldsymbol{m}} \rightharpoonup m \\ &= (1_M \otimes X^{\boldsymbol{m}})(\rho(m))\end{aligned}$$

for all $\boldsymbol{m} \in \mathrm{N}^r$ and $m \in M$ shows that $\rho = \rho_{\mathcal{N},\mathcal{B}}$. We leave it to the reader to complete the proof of part (b) by showing for r-tuples $\mathcal{N}$ and $\mathcal{N}'$ whose components are commuting locally nilpotent endomorphisms of M that $\rho_{\mathcal{N},\mathcal{B}} = \rho_{\mathcal{N}',\mathcal{B}}$ implies $\mathcal{N} = \mathcal{N}'$.

We now show part (c). By parts (a) and (b) any left quantum Yang-Baxter A-module has the form $(M, \mu_{\mathcal{T},B}, \rho_{\mathcal{N},B})$ where $\mathcal{T} = (T_1, \ldots, T_r)$ and $\mathcal{N} = (N_1, \ldots, N_r)$ are r-tuples of commuting endomorphisms, where $N_1, \ldots, N_r$ are locally nilpotent. The formula for $R = R_{(\mu_{\mathcal{T},\mathcal{B}}, \rho_{\mathcal{N},\mathcal{B}})}$ follows from the calculation

$$\begin{aligned}R(m \otimes n) &= m^{\langle 1\rangle} \otimes m^{(2)} \cdot n \\ &= \sum_{\boldsymbol{n} \in \mathrm{N}^r} \mathcal{N}^{\boldsymbol{n}}(m) \otimes \left(\frac{x^{\boldsymbol{n}}}{\boldsymbol{n}!}\right) \cdot n \\ &= \sum_{\boldsymbol{n} \in \mathrm{N}^r} \mathcal{N}^{\boldsymbol{n}}(m) \otimes \frac{1}{\boldsymbol{n}!} \mathcal{T}^{\boldsymbol{n}}(n)\end{aligned}$$

for all $m, n \in M$.

We complete the proof of part (c) by showing that (8) holds, namely

$$\alpha \rightharpoonup (a \cdot m) = a \cdot (\alpha \rightharpoonup m)$$

for all $\alpha \in A^*$, $a \in A$, and $m \in M$ if and only if the T_i's and N_j's commute. Since $\mathcal{A}$ is a dense subalgebra of A^* it is not hard to see that (8) is equivalent to

$$X_i \rightharpoonup (x_j \cdot m) = x_j \cdot (X_i \rightharpoonup m)$$

for all $1 \leq i, j \leq r$ and $m \in M$. This last equation is equivalent to $N_i T_j = T_j N_i$ for all $1 \leq i, j \leq r$. We have shown part (c), and thus the proof of the proposition is complete. $\square$

The solution to the quantum Yang-Baxter equation described in part (c) of Proposition 8 can be described in terms of the exponential map. Assume that the characteristic of k is 0 and that N is a locally nilpotent endomorphism of a vector space V over k. Then

$$\exp N = \sum_{n=0}^{\infty} \frac{N^n}{n!}$$

is a well-defined endomorphism of V. The endomorphism of part (c) of Proposition 8 can be written

$$R = \exp(N_1 \otimes T_1) \cdots \exp(N_r \otimes T_r).$$

When M is finite-dimensional, observe that $R = 1_{M\otimes M} + N$ for some nilpotent endomorphism N of $M \otimes M$; thus R is unipotent.

Suppose that $A = \mathrm{U}(r, k)$ and that $(M, \rho_{\mathcal{N},\mathcal{B}})$ is a finite-dimensional right A-comodule. To prove the theorem of this section we need to know the rank of the subalgebra B of A generated by $A(\rho)$.

LEMMA 5. *Suppose that M is a finite-dimensional vector space over the field k and $\mathcal{N} = (N_1, \dots, N_r)$ is an r-tuple of nilpotent endomorphisms of M. Assume that the characteristic of k is 0, let $\mathcal{B}$ be a basis for* $\mathrm{P}(r, k)$, *and suppose that B is the subalgebra of* $\mathrm{U}(r, k)$ *generated by* $\mathrm{U}(r, k)(\rho_{\mathcal{N},\mathcal{B}})$. *Then* $\operatorname{rank} B = \operatorname{rank} \mathcal{N}$.

Proof. First of all suppose that C is a coalgebra over k and that (M, ρ) is a finite-dimensional right C-comodule. Let $\{m_1, \dots, m_s\}$ be a basis for M and write $\rho(m_j) = \sum_{i=1}^{s} m_i \otimes c^i_j$ where $c^i_j \in C$. Then $C(\rho)$ is the span of the c^i_j's. Therefore

$$C(\rho) = (M^* \otimes 1_C)(\rho(M)). \tag{14}$$

Now let $A = \mathrm{U}(r, k)$ and consider (M, ρ), where $\rho = \rho_{\mathcal{N},\mathcal{B}}$. Choose a basis $\{\mathcal{N}^{\boldsymbol{n}_1}, \dots, \mathcal{N}^{\boldsymbol{n}_t}\}$ for the span of the $\mathcal{N}^{\boldsymbol{n}}$'s. Since

$$\rho(m) = \sum_{\boldsymbol{n}\in \mathrm{N}^r} \mathcal{N}^{\boldsymbol{n}}(m) \otimes \frac{x^{\boldsymbol{n}}}{\boldsymbol{n}!}$$

for all $m \in M$, there exist $c_1, \dots, c_t \in A$ such that

$$\rho(m) = \sum_{i=1}^{t} \mathcal{N}^{\boldsymbol{n}_i}(m) \otimes c_i \tag{15}$$

for all $m \in M$.

We claim that $A(\rho)$ is the span of the c_i's. First note that $A(\rho)$ is contained in the span of the c_i's by (14) and (15). To see that the c_i's are contained in $A(\rho)$ we note that $M^* \otimes M \simeq \operatorname{End}(M)$, where $\langle \alpha \otimes m, n\rangle = \langle \alpha, n\rangle m$ for all $\alpha \in M^*$ and $m, n \in M$. Thus we can think of $M \otimes M^*$ as $\operatorname{End}(M)^*$ via the composite

$M \otimes M^* \simeq (M^* \otimes M)^* \simeq \mathrm{End}\,(M)^*$ which is given by $\langle m \otimes \alpha, T \rangle = \langle \alpha, T(m) \rangle$ for all $m \in M, \alpha \in M^*$, and $T \in \mathrm{End}\,(M)$. Now fix $1 \leq j \leq t$ and let

$$f = \sum_{\ell=1}^{p} m_\ell \otimes \alpha_\ell \in \mathrm{End}\,(M)^*$$

be the functional which satisfies $\langle f, \mathcal{N}^{\boldsymbol{n}_i} \rangle = \delta_{i,j}$. Then

$$\begin{aligned} c_j &= \sum_{i=1}^{t} \langle f, \mathcal{N}^{\boldsymbol{n}_i} \rangle c_i \\ &= \sum_{i=1}^{t} \left(\sum_{\ell=1}^{p} \langle \alpha_\ell, \mathcal{N}^{\boldsymbol{n}_i}(m_\ell) \rangle \right) c_i \\ &= \sum_{\ell=1}^{p} (\alpha_\ell \otimes 1_{C^*})(\rho(m_\ell)) \end{aligned}$$

which means that $c_j \in A(\rho)$. Therefore $A(\rho)$ is the span of the c_i's.

We will assume that the basis $\mathcal{B}$ has been chosen in the following way. Reorder $\{N_1, \ldots, N_r\}$ if necessary so that $\{N_1, \ldots, N_s\}$ is a basis for the span of the N_i's. Now there are only finitely many $\boldsymbol{n}$'s such that $\mathcal{N}^{\boldsymbol{n}}$ is not zero. Choose a basis for the span of the $\mathcal{N}^{\boldsymbol{n}}$'s, consisting of $\mathcal{N}^{\boldsymbol{n}}$'s, so that any $\mathcal{N}^{\boldsymbol{n}}$ is a linear combination of basis elements $\mathcal{N}^{\boldsymbol{m}}$ which satisfy $|\boldsymbol{m}| \geq |\boldsymbol{n}|$. Since $\mathcal{N}^{\boldsymbol{n}}$ is nilpotent whenever $\boldsymbol{n} \neq \boldsymbol{o}$, it follows that $\mathcal{N}^{\boldsymbol{o}} = 1_M$ must be in the basis. Also observe that

$$P(A) \subseteq A_{(1)}, \tag{16}$$

$$c_i \in A_{(2)} \quad \text{if} \quad |\boldsymbol{n}_i| > 1, \tag{17}$$

and

$$c_{\boldsymbol{o}} = 1. \tag{18}$$

Let B be the subalgebra of A generated by $C = A(\rho)$. Since $\{N_1, \ldots, N_s\}$ is a basis for the span of $\{N_1, \ldots, N_r\}$ for $s < j \leq r$ we have

$$N_j = \sum_{i=1}^{s} \alpha_j^i N_i,$$

where $\alpha_j^i \in k$. We calculate

$$\rho_{\mathcal{N},\mathcal{B}}(m) = m \otimes 1 + \sum_{j=1}^{r} \mathcal{N}_j(m) \otimes x_j + \nabla$$

$$= m \otimes 1 + \sum_{i=1}^{s} \mathcal{N}_i(m) \otimes x_i + \sum_{j=s+1}^{r} \left(\sum_{i=1}^{s} \alpha^i_j N_i(m) \right) \otimes x_j + \nabla$$

$$= m \otimes 1 + \sum_{i=1}^{s} N_i(m) \otimes (x_i + \sum_{j=s+1}^{r} \alpha^i_j x_j) + \nabla$$

$$= m \otimes 1 + \sum_{i=1}^{s} N_i(m) \otimes x'_i + \nabla,$$

where $x'_i = x_i + \sum_{j=s+1}^{r} \alpha^i_j x_j$ for all $1 \le i \le s$ and $\nabla = \sum_{|\boldsymbol{n}|>1} \mathcal{N}^{\boldsymbol{n}} \otimes \frac{x^{\boldsymbol{n}}}{\boldsymbol{n}!} \in M \otimes A_{(2)}$. By the way we chose our basis for the span of the $\mathcal{N}^{\boldsymbol{n}}$'s it follows by (16)–(18) that $A(\rho) \subseteq k1 \oplus \mathrm{sp}(x'_1, \dots, x'_s) \oplus A_{(2)}$. Thus the primitives of B lie in the span of $x'_1, \dots, x'_s$ which form a linearly independent set.

Let $\mathcal{A} = k[x'_1, \dots, x'_s]$ be the subalgebra of A generated by $x'_1, \dots, x'_s$. Then $\mathcal{A}$ is a sub-Hopf algebra of A and $\mathcal{A} \simeq \mathrm{U}(s, k)$ as Hopf algebras. Since $A(\rho) \subseteq B \subseteq \mathcal{A}$ we may consider $(M, \rho_{\mathcal{N},\mathcal{B}})$ to be a right $\mathcal{A}$-comodule. Let $\pi\colon \mathcal{A}^* \longrightarrow \mathrm{End}(M)$ be the representation of $\mathcal{A}^*$ arising from the left rational $\mathcal{A}^*$-module structure on M determined by $(M, \rho_{\mathcal{N},\mathcal{B}})$. Let $X'_i = X_i|_{\mathcal{A}}$ for $1 \le i \le s$. Then $X'_1, \dots, X'_s \in P(\mathcal{A}^o)$ form a linear independent set, and thus form a basis for $P(\mathcal{A}^o)$ by Lemma 3. Since $N_i = \pi(X'_i)$ for $1 \le i \le s$ we can apply Proposition 7 to conclude that $B = \mathcal{A}$. This completes the proof. □

By part (c) of Proposition 8 we have an explicit formulation of the solution R to the quantum Yang-Baxter equation associated to a left quantum Yang-Baxter $\mathrm{U}(r, k)$-module structure. Our next result characterizes $\widetilde{A(R)}$.

THEOREM 2. *Let M be a vector space over the field k. Suppose that the characteristic of k is 0. Let $\mathcal{T} = (T_1, \dots, T_r)$ and $\mathcal{N} = (N_1, \dots, N_r)$ be r-tuples of commuting endomorphisms of M such that the N_i's are locally nilpotent and the N_i's commute with the T_j's. Set*

$$R = \sum_{\boldsymbol{n} \in N^r} \frac{1}{\boldsymbol{n}!} \mathcal{N}^{\boldsymbol{n}} \otimes \mathcal{T}^{\boldsymbol{n}}$$

and

$$\mathfrak{R} = \sum_{i=1}^{r} N_i \otimes T_i.$$

Then:

(a) *R is a solution to the quantum Yang-Baxter equation.*
(b) *If M is finite-dimensional, then $\widetilde{A(R)} \simeq \mathrm{U}(\mathrm{Rank}\,\mathfrak{R}, k)$.*

Proof. By part (c) of Proposition 8 there exists a left quantum Yang-Baxter U(r, k)-module structure $(M, \mu_{\mathcal{T},\mathcal{B}}, \rho_{\mathcal{N},\mathcal{B}}) = (M, \mu, \rho)$ on M such that R described in the statement of the theorem is the associated solution to the QYBE. Thus part (a) follows. In the finite-dimensional case, we note that the fact that R satisfies the QYBE also follows from the fact that the N_i's and T_j's generate a commutative subalgebra $\mathcal{A}$ of End(M) and that $R \in \mathcal{A} \otimes \mathcal{A}$.

Assume further that M is finite-dimensional. Let $A = \mathrm{U}(r, k)$ and write $\mathcal{B} = \{x_1, \ldots, x_r\}$. Reorder $\{T_1, \ldots, T_r\}$ if necessary so that $\{T_1, \ldots, T_s\}$ is a basis for the span of the T_i's. Recall that the representation $\pi\colon A \longrightarrow \mathrm{End}(M)$ afforded by (M, μ) is determined by $\pi(x_i) = T_i$ for all $1 \le i \le r$ and that the representation $\pi_{\mathrm{rat}}\colon A^* \longrightarrow \mathrm{End}(M)$ afforded by (M, μ_ρ) is determined by $\pi_{\mathrm{rat}}(X_i) = N_i$ for all $1 \le i \le r$, where the X_i's are defined for $\mathcal{B}$ as in Lemma 3. To compute $\widetilde{A(R)}$ we will pass to a quotient of A and then to a subalgebra of the quotient.

Let $s < j \le r$ and write

$$T_j = \sum_{i=1}^{s} \alpha_j^i T_i$$

where $\alpha_j^i \in k$. Let I be the sum of the coideals of $\mathrm{ann}_A(M)$. Then $x_j - \sum_{i=1}^{s} \alpha_j^i x_i \in I$ for $s < j \le r$. Since $\{T_1, \ldots, T_s\}$ is linearly independent, the quotient A/I is the free algebra on the set of cosets $\overline{\mathcal{B}} = \{\overline{x_1}, \ldots, \overline{x_s}\}$ by Lemma 3. Observe that

$$\begin{aligned}\mathfrak{R} &= \sum_{i=1}^{s} N_i \otimes T_i + \sum_{j=s+1}^{r} N_j \otimes \left(\sum_{i=1}^{s} \alpha_j^i T_i\right)\\ &= \sum_{i=1}^{s}\left(N_i + \sum_{j=s+1}^{r} \alpha_j^i N_j\right) \otimes T_i\end{aligned}$$

so

$$\mathfrak{R} = \sum_{i=1}^{s} \overline{N}_i \otimes T_i,$$

where $\overline{N}_i = N_i + \sum_{j=s+1}^{r} \alpha_j^i N_j$ for all $1 \le i \le s$.

Let $(M, \overline{\mu}_{\mathcal{T},\mathcal{B}})$ be the left A/I-module structure on M given by $\overline{\mu}_{\mathcal{T},\mathcal{B}} = \mu_{\mathcal{T},\mathcal{B}}(\pi \otimes 1_M)$ and let $(M, \overline{\rho}_{\mathcal{N},\mathcal{B}})$ be the right A/I-comodule structure on M defined by $\overline{\rho}_{\mathcal{N},\mathcal{B}} = (1_M \otimes \pi)\rho_{\mathcal{N},\mathcal{B}}$, where $\pi\colon A \longrightarrow A/I$ is the projection. Then $(M, \overline{\mu}_{\mathcal{T},\mathcal{B}}, \overline{\rho}_{\mathcal{N},\mathcal{B}})$ is a left quantum Yang-Baxter A-module and R is the associated quantum Yang-Baxter equation solution. Let $\overline{\mathcal{T}} = \{T_1, \ldots, T_s\}$. Then $(M, \overline{\mu}_{\mathcal{T},\mathcal{B}}) = (M, \mu_{\overline{\mathcal{T}},\overline{\mathcal{B}}})$. Observe that for $m \in M$ we have

$$\overline{\rho}_{\mathcal{N},\mathcal{B}}(m) = \sum_{\boldsymbol{n} \in N^r} \mathcal{N}^{\boldsymbol{n}}(m) \otimes \overline{\left(\frac{x^{\boldsymbol{n}}}{\boldsymbol{n}!}\right)}$$

$$= m \otimes \overline{1} + \sum_{i=1}^{s} N_i(m) \otimes \overline{x_i} + \sum_{j=s+1}^{r} N_j(m) \otimes \overline{x_j} + \nabla$$

$$= m \otimes \overline{1} + \sum_{i=1}^{s} N_i(m) \otimes \overline{x_i} + \sum_{j=s+1}^{r} N_j(m) \otimes \left(\sum_{i=1}^{s} \alpha^i_j \overline{x_i}\right) + \nabla$$

$$= m \otimes \overline{1} + \sum_{i=1}^{s} (N_i(m) + \sum_{j=s+1} \alpha^i_j N_j(m)) \otimes \overline{x_i} + \nabla$$

$$= m \otimes \overline{1} + \sum_{i=1}^{s} \overline{N_i}(m) \otimes \overline{x_i} + \nabla$$

where $\nabla \in M \otimes (A/I)_{(2)}$. Thus $\overline{\rho}_{\mathcal{N},\mathcal{B}} = \rho_{\overline{\mathcal{N}},\overline{\mathcal{B}}}$, where $\overline{\mathcal{N}} = (\overline{N_1}, \ldots, \overline{N}_s)$. Thus we may replace A by A/I and $(M, \mu_{\mathcal{T},\mathcal{B}}, \rho_{\mathcal{N},\mathcal{B}})$ by $(M, \mu_{\overline{\mathcal{T}},\overline{\mathcal{B}}}, \rho_{\overline{\mathcal{N}},\overline{\mathcal{B}}})$. In particular we may assume that $\{T_1, \ldots, T_r\}$ is linearly independent.

Assume that $\{T_1, \ldots, T_r\}$ is linearly independent and A is M-reduced. Notice that $\operatorname{Rank} \mathfrak{R} = \operatorname{Rank} \mathcal{N}$. Let B be the subalgebra of A generated by $A(\rho)$. Then $\widetilde{A(R)} \simeq B$. But $\operatorname{Rank} \mathcal{N} = \operatorname{rank} B$ by Lemma 5. This completes the proof of part b), and we are done. □

COROLLARY 1. *Suppose that M is a finite-dimensional vector space over the field k and let R: $M \otimes M \longrightarrow M \otimes M$ be a solution to the quantum Yang-Baxter equation. Assume that the characteristic of k is* 0. *Then the following are equivalent*:

(a) $\widetilde{A(R)} \simeq \mathrm{U}(r, k)$ *as bialgebras.*
(b) *There exists r-tuples $\mathcal{T} = \{T_1, \ldots, T_r\}$ and $\mathcal{N} = \{N_1, \ldots, N_r\}$ of endomorphisms of M such that*
   (i) $\{T_1, \ldots, T_r, N_1, \ldots, N_r\}$ *is a commuting family,*
   (ii) $N_1, \ldots, N_r$ *are nilpotent,*
   (iii) $\{T_1, \ldots, T_r\}$ *and* $\{N_1, \ldots, N_r\}$ *are linearly independent, and*
   (iv) $R = \sum_{\boldsymbol{n} \in \mathrm{N}^r} \frac{1}{\boldsymbol{n}!} \mathcal{N}^{\boldsymbol{n}} \otimes \mathcal{T}^{\boldsymbol{n}}$.

Proof. Part (b) implies part (a) by Theorem 2. To show part (a) implies part (b) we first observe that there is a left quantum Yang-Baxter $\widetilde{A(R)}$-module structure on M with associated quantum Yang-Baxter equation solution R. Thus part (a) implies part (b) by Proposition 8 and Theorem 2. □

4. Finite-dimensional Hopf algebras as reduced FRT constructions

Every finite-dimensional Hopf algebra H over the field k can be embedded into the underlying Hopf algebra $D(H)$ of the quantum double $(D(H), \mathfrak{R})$ of H. In this section we show that $M = D(H)$ has a left quantum Yang-Baxter H-module structure (M, μ, ρ) such that H is (M, μ)-reduced and $H(\rho) = H$. As a consequence $H \simeq \widetilde{A(R)}$, where R is the solution to the quantum Yang-Baxter equation associated to (M, μ, ρ).

The quantum double is a quasitriangular Hopf algebra.

Definition 10. A *quasitriangular bialgebra* (respectively quasitriangular Hopf algebra) over the field k is a pair (A, R), where A is a bialgebra (respectively Hopf algebra) over k and $R = \sum_{i=1}^{r} a_i \otimes b_i \in A \otimes A$ satisfies the following:

(QT.1) $\sum_{i=1}^{r} \Delta(a_i) \otimes b_i = \sum_{i,j=1}^{r} a_i \otimes a_j \otimes b_i b_j$,

(QT.2) $\sum_{i=1}^{r} \epsilon(a_i) b_i = 1$,

(QT.3) $\sum_{i=1}^{r} a_i \otimes \Delta^{\text{cop}}(b_i) = \sum_{i,j=1}^{r} a_i a_j \otimes b_i \otimes b_j$,

(QT.4) $\sum_{i=1}^{r} a_i \epsilon(b_i) = 1$, and

(QT.5) $(\Delta^{\text{cop}}(a))R = R(\Delta(a))$ for all $a \in A$.

Let $R_{(\ell)} = (1_A \otimes A^*)(R)$ and $R_{(r)} = (A^* \otimes 1_A)(R)$. If $r = \operatorname{Rank} R$ observe that $\{a_1, \dots, a_r\}$ is a basis for $R_{(\ell)}$ and $\{b_1, \dots, b_r\}$ is a basis for $R_{(r)}$.

Suppose that A is a finite-dimensional quasitriangular Hopf algebra over the field k. Then $R_{(\ell)}$ and $R_{(r)}$ are sub-Hopf algebras of A by [10, Proposition 2.a)] and $R_{(\ell)} R_{(r)} = R_{(r)} R_{(\ell)}$ by [10, Theorem 1.a)]. Let $H = R_{(\ell)}$ and regard $M = A$ as a left H-module under multiplication. Define ρ: $M \longrightarrow M \otimes H$ by

$$\rho(m) = \sum_{i=1}^{r} b_i m \otimes a_i$$

for all $m \in M$. Then (M, ρ) is a right H-comodule by virtue of (QT.1) and (QT.2). Using (QT.5) we deduce that (5) holds for (M, μ, ρ). Therefore (M, μ, ρ) is a left quantum Yang-Baxter H-module. Since (M, μ) is a faithful H-module we conclude that H is (M, μ)-reduced. Now suppose that $r = \operatorname{Rank} R$. We have noted that $H = R_{(\ell)}$ has basis $\{a_1, \dots, a_r\}$ and $\{b_1, \dots, b_r\}$ is linearly independent. Since $\rho(1) = \sum_{i=1}^{r} b_i \otimes a_i$ it follows that $H(\rho) = H$ (see Definition 1). Therefore $\widetilde{A(R)} \simeq H$ by Proposition 1(b), where R: $M \otimes M \longrightarrow M \otimes M$ is the quantum Yang-Baxter equation solution $R = R_{(\mu,\rho)}$. Since

$$R(m \otimes n) = \sum_{i=1}^{r} m^{(1)} \otimes m^{(2)} \cdot n = \sum_{i=1}^{r} b_i m \otimes a_i n$$

the solution R is given by

$$R(m \otimes n) = \sum_{i=1}^{r} b_i m \otimes a_i n$$

for all $m, n \in M$.

Now suppose that $(D(H), \mathfrak{R})$ is the quantum double of H. Then there exists an embedding of Hopf algebras ι: $H \longrightarrow D(H)$ such that $\iota(H) = \mathfrak{R}_{(\ell)}$. See [2, page 816] for the definition of the quantum double and its construction and see [10, Section 3] for the conventions regarding the double we are following here. Since $\operatorname{Dim} D(H) = (\operatorname{Dim} H)^2$ we have shown:

THEOREM 3. *Suppose that H is an n-dimensional Hopf algebra over the field k. Then there exists an n^2-dimensional vector space M over k and a solution R: $M \otimes M \longrightarrow M \otimes M$ to the quantum Yang-Baxter equation such that $H \simeq \widetilde{A(R)}$.*

REFERENCES

1. E. Abe, *Hopf Algebras*, Cambridge Tracts in Mathematics, vol. 74, Cambridge University Press, Cambridge, UK, 1980.
2. V. G. Drinfel'd, *Quantum groups*, Proceedings of the International Congress of Mathematicians, Berkeley, California, 1987, 798–820.
3. L. D. Faddeev, N. Y. Reshetihkin and L. A. Takhtadzhan, *Quantization of Lie algebras and Lie groups*, Leningrad Math. J. **1** (1990), 193–225; Translation from Algebra Anal. **1** (1989), 178–206.
4. Louis Kauffman, *Knots and physics*, Series on Knots and Everything, vol. 1, World Scientific, Singapore.
5. L. Lambe, *The* 1996 *Adams Lectures at Manchester University: New Computational Methods in Algebra and Topology, Part I, Solving the Quantum Yang-Baxter Equation*, May 20, 1996, preprint.
6. L. Lambe and D. E. Radford, *Algebraic aspects of the quantum Yang-Baxter equation*, J. Algebra **154** (1993), 228–288.
7. ———, *Introduction to the quantum Yang-Baxter equation and quantum groups: an algebraic approach*, Mathematics and its Applications, no. 423, Kluwer Academic Publishers, Dordrecht, 1997.
8. Shahn Majid, *Quasitriangular Hopf algebras and Yang-Baxter equations*, Internat. J. Mod. Physics A **5** (1990), 1–91.
9. S. Montgomery, *Hopf algebras and their actions on rings*, Regional Conference Series in Mathematics, no. 82, AMS, Providence, RI, 1993.
10. D. E. Radford, *Minimal quasitriangular Hopf algebras*, J. Algebra **157** (1993), 285–315.
11. ———, *Solutions to the quantum Yang-Baxter equation arising from pointed bialgebras*, Trans. Amer. Math. Soc. **343** (1994), 455–477.
12. ———, *Solutions to the quantum Yang-Baxter equation and the Drinfel'd double*, J. Algebra **161** (1993), 20–32.
13. D. N. Yetter, *Quantum groups and representations of monoidal categories*, Math. Proc. Cambridge Philos. Soc. **108** (1990), 261–290.
14. M. E. Sweedler, *Hopf algebras*, Benjamin, New York, 1969.

Larry Lambe, Department of Mathematics, University of Wales, Bangor, Bangor, Gwynedd LL57 1UT, United Kingdom
llambe@caip.rutgers.edu

David E. Radford, Department of Mathematics, Statistics, and Computer Science,
University of Illinois at Chicago, Chicago, Illinois 60607-7045
radford@uic.edu