Available online at www.sciencedirect.com

ScienceDirect

Electronic Notes in Theoretical Computer Science 265 (2010) 337–350

Electronic Notes in Theoretical Computer Science

www.elsevier.com/locate/entcs

Bialgebras in Rel

Masahito Hasegawa[1,2]

Research Institute for Mathematical Sciences
Kyoto University
Kyoto, Japan

Abstract

We study bialgebras in the compact closed category **Rel** of sets and binary relations. We show that various monoidal categories with extra structure arise as the categories of (co)modules of bialgebras in **Rel**. In particular, for any group G we derive a ribbon category of crossed G-sets as the category of modules of a Hopf algebra in **Rel** which is obtained by the quantum double construction. This category of crossed G-sets serves as a model of the braided variant of propositional linear logic.

Keywords: monoidal categories, bialgebras and Hopf algebras, linear logic

1 Introduction

For last two decades it has been shown that there are plenty of important examples of *traced monoidal categories* [21] and *ribbon categories (tortile monoidal categories)* [32,33] in mathematics and theoretical computer science. In mathematics, most interesting ribbon categories are those of representations of *quantum groups* (*quasi-triangular Hopf algebras*) [9,23] in the category of finite-dimensional vector spaces. In many of them, we have non-symmetric braidings [20]: in terms of the graphical presentation [19,31], the braid $c = \times$ is distinguished from its inverse $c^{-1} = \times$, and this is the key property for providing non-trivial invariants (or denotational semantics) of knots, tangles and so on [12,23,33,35] as well as solutions of the quantum Yang-Baxter equation [9,23]. In theoretical computer science, major examples include categories with fixed-point operators used in denotational and algebraic semantics [5,15,16], and the category of sets and binary relations and its variations used in models of linear logic [13] and game semantics [29]. Moreover, the Int-construction [21] provides a rich class of models of Geometry of Interaction [3,14]. In most of them, braidings are symmetric, hence $\times$ is identified with $\times$.

[1] This work was partly supported by the Grant-in-Aid for Scientific Research (C) 20500010.

[2] Email: `hassei@kurims.kyoto-u.ac.jp`

doi:10.1016/j.entcs.2010.08.020

Although it is nice to know that all these examples share a common structure, it is also striking to observe that important examples from mathematics and those from computer science are almost disjoint [3]. Is it just a matter of taste of mathematicians and computer scientists? Or is it the case that categories used in computer science cannot host structures interesting for mathematicians (non-symmetric braidings in particular)?

In this paper we demonstrate that we do have mathematically interesting structures in a category preferred by computer scientists. Specifically, we focus on the category **Rel** of sets and binary relations. **Rel** is a compact closed category [25], that is, a ribbon category in which braiding is symmetric and twist is trivial. We study bialgebras and Hopf algebras in **Rel**, and show that various monoidal categories with extra structure like traces and autonomy can be derived as the categories of (co)modules of bialgebras in **Rel**. As a most interesting example, for any group G we consider the associated Hopf algebra in **Rel**, and apply the *quantum double construction* [9] to it. The resulting Hopf algebra is equipped with a universal R-matrix as well as a universal twist. We show that the category of its modules is the category of *crossed G-sets* [12,34] and suitable binary relations, featuring non-symmetric braiding and non-trivial twist.

Related work

Hopf algebras in connection to quantum groups [9] have been extensively studied: standard references include [23,28]. The idea of using Hopf algebras for modelling various non-commutative linear logic goes back to Blute [6], where the focus is on Hopf algebras in the $*$-autonomous category of topological vector spaces. As far as we know, there is no published result on Hopf algebras in **Rel**. Since Freyd and Yetter's work [12], categories of crossed G-sets have appeared frequently as typical examples of braided monoidal categories. In the standard setting of finite-dimensional vector spaces, modules of the quantum double of a Hopf algebra A amount to the crossed A-bimodules [23,24], and our result is largely an adaptation of such a standard result to **Rel**. However we are not aware of a characterization of crossed G-sets in terms of a quantum double construction in the literature.

Organization of this paper

In Section 2, we recall basic notions and facts on monoidal categories and bialgebras. In Section 3, we examine some bialgebras in **Rel** which arise from monoids and groups, and study the categories of (co)modules. Section 4 is devoted to a quantum double construction in **Rel**, which gives rise to a category of crossed G-sets. We discuss how this category can be used as a model of braided linear logic in Section 5. Section 6 concludes the paper.

---

[3] An important exception would be dagger compact closed categories used in the study of quantum information protocols [2], though they do not feature non-symmetric braidings. We shall note that our category of crossed G-sets is actually a dagger tortile category in the sense of Selinger [31].

2 Monoidal categories and bialgebras

2.1 Monoidal categories

A *monoidal category* (*tensor category*) [26,20] $\mathcal{C} = (\mathcal{C}, \otimes, I, a, l, r)$ consists of a category $\mathcal{C}$, a functor $\otimes : \mathcal{C} \times \mathcal{C} \to \mathcal{C}$, an object $I \in \mathcal{C}$ and natural isomorphisms $a_{A,B,C} : (A \otimes B) \otimes C \xrightarrow{\sim} A \otimes (B \otimes C)$, $l_A : I \otimes A \xrightarrow{\sim} A$ and $r_A : A \otimes I \xrightarrow{\sim} A$ subject to the standard coherence diagrams. It is said to be strict if a, l, r are the identity morphisms.

A *braiding* [20] is a natural isomorphism $c_{A,B} : A \otimes B \xrightarrow{\sim} B \otimes A$ such that both c and c^{-1} satisfy the following "bilinearity" (the case for c^{-1} is omitted):

$$\begin{tikzcd}
(A \otimes B) \otimes C \arrow[r, "a_{A,B.C}"] \arrow[d, "c_{A,B} \otimes C"'] & A \otimes (B \otimes C) \arrow[r, "c_{A,B \otimes C}"] & (B \otimes C) \otimes A \arrow[d, "a_{B,C,A}"] \\
(B \otimes A) \otimes C \arrow[r, "a_{B,A,C}"'] & B \otimes (A \otimes C) \arrow[r, "B \otimes c_{A,C}"'] & B \otimes (C \otimes A)
\end{tikzcd}$$

A *symmetry* is a braiding such that $c_{A,B} = c^{-1}_{B,A}$. A *braided/symmetric monoidal category* is a monoidal category equipped with a braiding/symmetry.

A *twist* or a *balance* for a braided monoidal category is a natural isomorphism $\theta_A : A \xrightarrow{\sim} A$ such that $\theta_I = id_I$ and $\theta_{A \otimes B} = c_{B,A} \circ (\theta_B \otimes \theta_A) \circ c_{A,B}$ hold. A *balanced monoidal category* is a braided monoidal category with a twist. Note that a symmetric monoidal category is a balanced monoidal category with $\theta_A = id_A$ for every A.

A *(left) dual* of an object A in a monoidal category is an object A^* equipped with a pair of morphisms $d : I \to A \otimes A^*$, called unit, and $e : A^* \otimes A \to I$, called counit, making the composites

$$A \xrightarrow{l_A^{-1}} I \otimes A \xrightarrow{d \otimes A} (A \otimes A^*) \otimes A \xrightarrow{a_{A,A^*,A}} A \otimes (A^* \otimes A) \xrightarrow{A \otimes e} A \otimes I \xrightarrow{r_A} A$$

$$A^* \xrightarrow{r_{A^*}^{-1}} A^* \otimes I \xrightarrow{A^* \otimes d} A^* \otimes (A \otimes A^*) \xrightarrow{a^{-1}_{A^*,A,A^*}} (A^* \otimes A) \otimes A^* \xrightarrow{e \otimes A^*} I \otimes A^* \xrightarrow{l_{A^*}} A^*$$

the identity morphisms. A *ribbon category* [33] (*tortile monoidal category* [32]) is a balanced monoidal category in which every object A has a dual $(A^*, \eta_A : I \to A \otimes A^*, \varepsilon_A : A^* \otimes A \to I)$ and moreover ${\theta_A}^* = \theta_{A^*}$ holds, where, for $f : A \to B$, $f^* : B^* \to A^*$ is given by (omitting l, r and a)

$$B^* \xrightarrow{B^* \otimes \eta_A} B^* \otimes A \otimes A^* \xrightarrow{B^* \otimes f \otimes A^*} B^* \otimes B \otimes A^* \xrightarrow{\varepsilon_B \otimes A^*} A^*.$$

It follows that $(-)^*$ extends to a contravariant equivalence, there is a natural isomorphism $A^{**} \simeq A$, and the functor $(-) \otimes A$ is left (and right) adjoint to $(-) \otimes A^*$. Note that a ribbon category in which twist is the identity (and braiding is a symmetry) is a familiar compact closed category [25].

A *traced monoidal category* [21] is a balanced monoidal category $\mathcal{C}$ equipped with a trace operator $Tr^X_{A,B} : \mathcal{C}(A \otimes X, B \otimes X) \to \mathcal{C}(A, B)$ satisfying a few coherence axioms. Alternatively, by the structure theorem in *ibid.*, traced monoidal categories are characterized as monoidal full subcategories of ribbon categories. Any ribbon category has a unique trace, called *canonical trace* [21] (for uniqueness see e.g. [16]). For a morphism $f : A\otimes X \to B\otimes X$ in a ribbon category, its trace $Tr^X_{A,B} f : A \to B$ is given by

$$Tr^X_{A,B} f \;=\; (id_B \otimes (\varepsilon_X \circ (id_{X^*} \otimes \theta_X) \circ c_{X,X^*})) \circ (f \otimes id_{X^*}) \circ (id_A \otimes \eta_X).$$

For monoidal categories $\mathcal{C} = (\mathcal{C}, \otimes, I, a, l, r)$ and $\mathcal{C}' = (\mathcal{C}', \otimes', I', a', l', r')$, a *monoidal functor* from $\mathcal{C}$ to $\mathcal{C}'$ is a tuple (F, m, m_I) where F is a functor from $\mathcal{C}$ to $\mathcal{C}'$, m is a natural transformation from $F(-) \otimes' F(=)$ to $F(-\otimes =)$ and $m_I : I' \to FI$ is an arrow in $\mathcal{C}'$, satisfying three coherence conditions. It is called *strong* if $m_{A,B}$ and m_I are all isomorphisms. A *balanced monoidal functor* from a balanced $\mathcal{C}$ to another $\mathcal{C}'$ is a monoidal functor (F, m, m_I) which additionally satisfies $m_{B,A} \circ c_{FA,FB} = Fc_{A,B} \circ m_{A.B}$ and $F(\theta_A) = \theta_{FA}$.

For monoidal functors (F, m, m_I), (G, n, n_I) with the same source and target monoidal categories, a *monoidal natural transformation* from (F, m, m_I) to (G, n, n_I) is a natural transformation $\varphi : F \to G$ such that $\varphi_{A\otimes B} \circ m_{A,B} = n_{A,B} \circ \varphi_A \otimes \varphi_B$ and $\varphi_I \circ m_I = n_I$ hold. A *(balanced/symmetric) monoidal adjunction* between (balanced/symmetric) monoidal categories is an adjunction in which both of the functors are (balanced/symmetric) monoidal and the unit and counit are monoidal natural transformations.

2.2 Monoids, comonoids and (co)modules

A *monoid* in a monoidal category $\mathcal{C} = (\mathcal{C}, \otimes, I, a, l, r)$ is an object A equipped with morphisms $m : A\otimes A \to A$, called the *multiplication*, and $1 : I \to A$, called the *unit*, such that the following diagrams commute (for the sake of simplicity, we omit the coherence isomorphisms a, l, r, and pretend as if $\mathcal{C}$ is a strict monoidal category).

$$\begin{tikzcd} A\otimes A\otimes A \arrow[r, "A\otimes m"] \arrow[d, "m\otimes A"'] & A\otimes A \arrow[d, "m"] \\ A\otimes A \arrow[r, "m"'] & A \end{tikzcd} \qquad \begin{tikzcd} A \arrow[r, "A\otimes 1"] \arrow[d, "1\otimes A"'] \arrow[dr, "id"] & A\otimes A \arrow[d, "m"] \\ A\otimes A \arrow[r, "m"'] & A \end{tikzcd}$$

When $\mathcal{C}$ is braided and $m \circ c_{A,A} = m$ holds, we say A is *commutative.*

Dually, a *comonoid* in a monoidal category $\mathcal{C}$ is an object A equipped with morphisms $\Delta : A \to A\otimes A$, called the *comultiplication*, and $\epsilon : A \to I$, called the *counit*, satisfying

$$\begin{tikzcd} A \arrow[r, "\Delta"] \arrow[d, "\Delta"'] & A\otimes A \arrow[d, "A\otimes\Delta"] \\ A\otimes A \arrow[r, "\Delta\otimes A"'] & A\otimes A\otimes A \end{tikzcd} \qquad \begin{tikzcd} A \arrow[r, "\Delta"] \arrow[d, "\Delta"'] \arrow[dr, "id"] & A\otimes A \arrow[d, "A\otimes\epsilon"] \\ A\otimes A \arrow[r, "\epsilon\otimes A"'] & A \end{tikzcd}$$

When $\mathcal{C}$ is braided and $c_{A,A} \circ \Delta = \Delta$ holds, we say A is *co-commutative.*

Suppose that $A = (A, m, 1)$ is a monoid. A gives rise to a monad $A \otimes (-)$ whose multiplication is $m \otimes X : A \otimes A \otimes X \to A \otimes X$ and unit is $1 \otimes X : X \to A \otimes X$. An A-*module* is an Eilenberg-Moore algebra of this monad. More explicitly, an A-module consists of an object X and a morphism $\alpha : A \otimes X \to X$, called the action, satisfying

$$\begin{tikzcd} X \arrow[r, "1\otimes X"] \arrow[dr, "id"'] & A \otimes X \arrow[d, "\alpha"] \\ & X \end{tikzcd} \qquad \begin{tikzcd} A \otimes A \otimes X \arrow[r, "A\otimes\alpha"] \arrow[d, "m\otimes X"'] & A \otimes X \arrow[d, "\alpha"] \\ A \otimes X \arrow[r, "\alpha"'] & X \end{tikzcd}$$

A morphism of A-modules from (X, α) to (Y, β) is a morphism $f : X \to Y$ satisfying

$$\begin{tikzcd} A \otimes X \arrow[r, "A\otimes f"] \arrow[d, "\alpha"'] & A \otimes Y \arrow[d, "\beta"] \\ X \arrow[r, "f"'] & Y \end{tikzcd}$$

Let us denote the category of A-modules and morphisms by $\mathbf{Mod}(A)$.

Dually, given a comonoid $A = (A, \Delta, \epsilon)$, an A-*comodule* is an Eilenberg-Moore coalgebra of the comonad $A \otimes (-)$ whose comultiplication is $\Delta \otimes X : A \otimes X \to A \otimes A \otimes X$ and counit is $\epsilon \otimes X : A \otimes X \to X$. Explicitly, an A-comodule consists of an object X and a morphism $\alpha : X \to A \otimes X$, called the coaction, satisfying the axioms dual to the those of modules. A morphism of A-comodules from (X, α) to (Y, β) is then a morphism $f : X \to Y$ making the evident diagram commute. We will denote the category of A-comodules and morphisms by $\mathbf{Comod}(A)$.

2.3 Bialgebras and Hopf algebras

Now suppose that $\mathcal{C}$ is a symmetric monoidal category with a symmetry $c_{X,Y} : X \otimes Y \xrightarrow{\simeq} Y \otimes X$. A *bialgebra* in $\mathcal{C}$ is given by a tuple $A = (A, m, 1, \Delta, \epsilon)$ where A is an object of $\mathcal{C}$ and $(A, m, 1)$ is a monoid in $\mathcal{C}$ while (A, Δ, ϵ) is a comonoid in $\mathcal{C}$, satisfying

$$\begin{tikzcd} A \otimes A \arrow[rr, "m"] \arrow[d, "\Delta\otimes\Delta"'] & & A \arrow[d, "\Delta"] \\ A \otimes A \otimes A \otimes A \arrow[r, "A\otimes c_{A,A}"'] & A \otimes A \otimes A \otimes A \arrow[r, "m\otimes m"'] & A \otimes A \end{tikzcd}$$

$$\begin{tikzcd} A \otimes A \arrow[rr, "m"] \arrow[dr, "\epsilon\otimes\epsilon"'] & & A \arrow[dl, "\epsilon"] \\ & I & \end{tikzcd} \qquad \begin{tikzcd} & I \arrow[dl, "1"'] \arrow[dr, "1\otimes 1"] & \\ A \arrow[rr, "\Delta"'] & & A \otimes A \end{tikzcd} \qquad \begin{tikzcd} I \arrow[rr, "id"] \arrow[dr, "1"'] & & I \\ & A \arrow[ur, "\epsilon"'] & \end{tikzcd}$$

We say A is commutative (resp. co-commutative) when it is commutative (resp. co-commutative) as a monoid (resp. comonoid). For a bialgebra A, we can consider the category of modules $\mathbf{Mod}(A)$ as well as that of comodules $\mathbf{Comod}(A)$. The functor $A \otimes (-)$ is both monoidal and comonoidal. Moreover, as a monad $A \otimes (-)$ is comonoidal, while as a comonad it is monoidal. It follows that (cf. [7,30]) both

Mod(A) and **Comod**(A) are monoidal categories. Explicitly, in **Mod**(A), the tensor unit is $(I, A \otimes I \simeq A \xrightarrow{\epsilon} I)$ and the tensor product of (X, α) and (Y, β) is

$$(X \otimes Y, A \otimes X \otimes Y \xrightarrow{\Delta \otimes X \otimes Y} A \otimes A \otimes X \otimes Y \xrightarrow{A \otimes c_{A,X} \otimes Y} A \otimes X \otimes A \otimes Y \xrightarrow{\alpha \otimes \beta} X \otimes Y).$$

The monoidal structure of **Comod**(A) is given by dualizing that of **Mod**(A).

A *Hopf algebra* is a bialgebra $A = (A, m, 1, \Delta, \epsilon)$ equipped with a morphism $S : A \to A$, called an *antipode*, such that

$$\begin{tikzcd}
 & A \otimes A \arrow[rr, "S \otimes A"] & & A \otimes A \arrow[dr, "m"] & \\
A \arrow[ur, "\Delta"] \arrow[dr, "\Delta"'] \arrow[rr, "\epsilon"] & & I \arrow[rr, "1"] & & A \\
 & A \otimes A \arrow[rr, "A \otimes S"'] & & A \otimes A \arrow[ur, "m"'] &
\end{tikzcd}$$

commutes.

Lemma 2.1 *If $\mathcal{C}$ is a compact closed category and A is a Hopf algebra in $\mathcal{C}$, every object in* **Mod**(A) *has a dual, where a dual of a module (X, α) is*

$$A \otimes X^* \xrightarrow{c} X^* \otimes A \xrightarrow{X^* \otimes S \otimes \eta} X^* \otimes A \otimes X \otimes X^* \xrightarrow{X^* \otimes \alpha \otimes X^*} X^* \otimes X \otimes X^* \xrightarrow{\varepsilon \otimes X^*} X^*.$$

2.4 Braiding and twist on (co)modules of a bialgebra

If a bialgebra A is co-commutative (resp. commutative), the monoidal category **Mod**(A) (resp. **Comod**(A)) has a symmetry inherited from the base symmetric monoidal category. However, (whether A is (co-)commutative or not) there can be some non-trivial braiding and twist on **Mod**(A) or **Comod**(A): we shall look at the case of **Mod**(A). Suppose that **Mod**(A) is braided with a braiding σ (while we use c for the symmetry of the base symmetric monoidal category). Since $A = (A, m)$ is a A-module, we have $\sigma_{A,A} : A \otimes A \to A \otimes A$, and $c_{A,A} \circ \sigma_{A,A} \circ (1 \otimes 1) : I \to A \otimes A$ which we shall denote by R. Conversely, from this $R : I \to A \otimes A$ we can recover $\sigma_{X,Y} : X \otimes Y \to Y \otimes X$ for modules $X = (X, \alpha)$ and $Y = (Y, \beta)$ as

$$X \otimes Y \xrightarrow{R \otimes X \otimes Y} A \otimes A \otimes X \otimes Y \xrightarrow{A \otimes c_{A,X} \otimes Y} A \otimes X \otimes A \otimes Y \xrightarrow{\alpha \otimes \beta} X \otimes Y \xrightarrow{c_{X,Y}} Y \otimes X.$$

In fact, there is a bijective correspondence between braidings on **Mod**(A) and morphisms of $I \to A \otimes A$ satisfying certain equations [23,28]. Such a morphism of $I \to A \otimes A$ is called a *universal R-matrix* or a *braiding element*. A bialgebra equipped with a universal R-matrix is called a *quasi-triangular bialgebra*.

Next, let A be a quasi-triangular Hopf algebra and suppose that **Mod**(A) is a ribbon category, i.e., not just braided but also with a twist θ. We then have a morphism $v = \theta_A \circ 1 : I \to A$, from which we can recover $\theta_X : X \to X$ for a module $X = (X, \alpha)$ as $X \xrightarrow{v \otimes X} A \otimes X \xrightarrow{\alpha} X$. It follows that we have a bijective correspondence between twists on **Mod**(A) and certain morphisms $v : I \to A$ satisfying a few axioms [23,28,33]. Such a v is called a *universal twist* or a *twist* *element*. A quasi-triangular Hopf algebra equipped with a universal twist is called a *ribbon Hopf algebra*.

Proposition 2.2 *(cf. [23,33])*

(i) *If A is a quasi-triangular bialgebra in a symmetric monoidal category $\mathcal{C}$, then* $\mathbf{Mod}(A)$ *is a braided monoidal category.*

(ii) *If A is a ribbon Hopf algebra in a compact closed category $\mathcal{C}$, then* $\mathbf{Mod}(A)$ *is a ribbon category.*

We will give a non-commutative non-co-commutative ribbon Hopf algebra in **Rel** in Section 4.

2.5 Examples

We shall look at a few basic cases.

Example 2.3 As a classical example, let us consider the category $\mathbf{Vect}_k$ of vector spaces over a field k and linear maps. $\mathbf{Vect}_k$ is a symmetric monoidal category whose monoidal product is given by the tensor product of vector spaces, and k serves as the tensor unit. A monoid in $\mathbf{Vect}_k$ is nothing but an algebra in the standard sense. Similarly, a comonoid in $\mathbf{Vect}_k$ is what is normally called a coalgebra. Modules, comodules, bialgebras and Hopf algebras in $\mathbf{Vect}_k$ are exactly those in the classical sense; a detailed account can be found in [23].

Example 2.4 Let **Set** be the category of sets and functions. By taking finite products as tensor products, **Set** forms a symmetric monoidal category. A monoid in **Set** is just a monoid in the usual sense. For any set X, the diagonal map $X \to X \times X$ and the terminal map $X \to 1$ give a commutative comonoid structure on X — and this is the unique comonoid structure on X. Given a monoid M, its modules are just the M-sets, i.e., sets on which M acts, and $\mathbf{Mod}(M)$ is isomorphic to the category M-**Set** of M-sets and functions respecting M-actions. For any set X, a comodule $(A, \alpha : A \to X \times A)$ of the unique comonoid $X = (X, \Delta, \epsilon)$ on X is determined by the function $\pi \circ \alpha : A \to X$, and $\mathbf{Comod}(X)$ is isomorphic to the slice category $\mathbf{Set}/X$. A bialgebra in **Set** is a monoid equipped with the unique comonoid structure. A Hopf algebra in **Set** is then a group with the unique comonoid structure, where the antipode is given by the inverse $(-)^{-1}$.

3 Bialgebras in Rel

Now let us turn our attention to the category **Rel** of sets and binary relations. **Rel** is a compact closed (hence ribbon) category, where the tensor product is given by the direct products of sets. First, we shall note that there is an identity-on-object, strict symmetric monoidal functor $J : \mathbf{Set} \to \mathbf{Rel}$ sending a set to itself and a function $f : X \to Y$ to a binary relation $\{(x, f(x)) \mid x \in X\}$ from X to Y, and recall a standard result:

Lemma 3.1 *A strong symmetric monoidal functor preserves the structure of monoids, comonoids, bialgebras and Hopf algebras.*

¿From this and Example 2.4, it follows that a monoid $M = (M, \cdot, e)$ (in **Set**) gives rise to a co-commutative bialgebra $\overline{M} = (M, m, 1, \Delta, \epsilon)$ in **Rel**, with

$$\begin{aligned} m &= \{((a_1, a_2), a_1 \cdot a_2) \mid a_1, a_2 \in M\} : M \times M \to M \\ 1 &= \{(*, e)\} : I \to M \\ \Delta &= \{(a, (a, a)) \mid a \in M\} : M \to M \times M \\ \epsilon &= \{(a, *) \mid a \in M\} : M \to I \end{aligned}$$

$\overline{M}$ is commutative if M is commutative. Similarly, a group $G = (G, \cdot, e, (-)^{-1})$ gives rise to a co-commutative Hopf algebra $\overline{G} = (G, m, 1, \Delta, \epsilon, S)$ in **Rel**, with an antipode $S = \{(g, g^{-1}) \mid g \in G\} : G \to G$.

Let us examine the category $\mathbf{Mod}(\overline{G})$ for a group $G = (G, \cdot, e, (-)^{-1})$ (it makes sense to think about $\mathbf{Mod}(\overline{M})$ for a monoid M, but when M is not a group the description of $\mathbf{Mod}(\overline{M})$ can be rather complicated). A module of $\overline{G}$ is a set X equipped with a binary relation $\alpha : G \times X \to X$ subject to the two axioms given before. It is not hard to see that α is actually a function, in fact a G-action on X: for $g \in G$ and $x \in X$, by letting $g \bullet x$ be the unique $x' \in X$ such that $((g, x), x') \in \alpha$, we have $e \bullet x = x$ and $(g \cdot h) \bullet x = g \bullet (h \bullet x)$. Therefore we can identify objects of $\mathbf{Mod}(\overline{G})$ with G-sets: a morphism from a G-set $(X, \bullet)$ to $(Y, \bullet)$ is then a binary relation $r : X \to Y$ such that $(x, y) \in r$ implies $(g \bullet x, g \bullet y) \in r$. Since $\overline{G}$ is a co-commutative Hopf algebra, $\mathbf{Mod}(\overline{G})$ is a symmetric monoidal category with duals, i.e., a compact closed category which is actually very similar to **Rel**. Explicitly, the tensor of $(X, \bullet)$ and $(Y, \bullet)$ is $(X \times Y, (g, (x, y)) \mapsto (g \bullet x, g \bullet y))$, while the tensor unit is $(\{*\}, (g, x) \mapsto *)$. A dual of $(X, \bullet)$ is $(X, \bullet)$ itself.

Next, we shall look at $\mathbf{Comod}(\overline{M})$ for a monoid $M = (M, \cdot, e)$. A comodule of $\overline{M}$ is a set X with a binary relation $\alpha : X \to G \times X$ subject to the comodule axioms — but the axioms imply that α is a function whose second component is the identity on X. Hence an object of $\mathbf{Comod}(\overline{M})$ can be identified with a set X equipped with a function $|\_| : X \to M$; a morphism from $(X, |\_|)$ to $(Y, |\_|)$ is then a binary relation $r : X \to Y$ such that $(x, y) \in r$ implies $|x| = |y|$. $\mathbf{Comod}(\overline{M})$ is a monoidal category, with $(X, |\_|) \otimes (Y, |\_|) = (X \times Y, (x, y) \mapsto |x| \cdot |y|)$ and $I = (\{*\}, x \mapsto e)$.

Proposition 3.2

(i) *If G is a group, every object $(X, |\_|)$ of $\mathbf{Comod}(\overline{G})$ has a dual $(X, |\_|^{-1})$ (and $\mathbf{Comod}(\overline{G})$ is pivotal [12]).*

(ii) *If G is an Abelian group, $\mathbf{Comod}(\overline{G})$ is a compact closed category.*

(iii) *If M is a commutative monoid, $\mathbf{Comod}(\overline{M})$ is symmetric monoidal.*

(iv) *If M is a commutative cancellable monoid, $\mathbf{Comod}(\overline{M})$ is a traced symmetric monoidal category.*

(v) *If M is a left (resp. right)-cancellable monoid,* **Comod**$(\overline{M})$ *has a left (resp. right) trace in the sense of Selinger [31].*

Thus we can derive a number of monoidal categories with symmetry, duals, and trace as categories of (co)modules of (the associated bialgebra of) a monoid or a group. However, they do not have a non-symmetric braiding; in the next section we give a Hopf algebra in **Rel** whose category of modules has a non-symmetric braiding and a non-trivial twist.

4 A quantum double construction in Rel

In the previous section, we have observed that every group $G = (G, \cdot, e, (-)^{-1})$ gives rise to a co-commutative Hopf algebra $\overline{G} = (G, m, 1, \Delta, \epsilon, S)$ in **Rel**. We shall apply Drinfel'd's *quantum double construction* [9,27] to $\overline{G}$. Here we recall the quantum double construction given in terms of Hopf algebras in compact closed categories:

Proposition 4.1 *(cf. [8,23,24]) Suppose that $\mathcal{C}$ is a compact closed category and $A = (A, m, 1, \Delta, \epsilon, S)$ is a Hopf algebra in $\mathcal{C}$, where the antipode S is invertible. Then there exists a quasi-triangular Hopf algebra $D(A)$ on $A^* \otimes A$.*

For lack of space, we shall only give an outline of the construction and some informal remarks. Given a Hopf algebra $A = (A, m, 1, \Delta, \epsilon, S)$ with S invertible, let $A^{\mathrm{op}*} = (A^*, \Delta^*, \epsilon^*, (m^{\mathrm{op}})^*, 1^*, (S^{-1})^*)$ be the dual Hopf algebra (where $m^{\mathrm{op}} = m \circ c_{A,A}$, and we omit the isomorphisms $(X \otimes Y)^* \simeq Y^* \otimes X^*$ and $I^* \simeq I$). It follows that there are suitable actions of A on $A^{\mathrm{op}*}$ and $A^{\mathrm{op}*}$ on A, and with them we can form a bicrossed product [27,28] of $A^{\mathrm{op}*}$ with A, which is the Hopf algebra $D(A)$. We shall note that $D(A)$ is almost like a tensor product of $A^{\mathrm{op}*}$ with A itself — except some clever adjustment on the multiplication and antipode. Also let us remark that **Mod**$(A^{\mathrm{op}*})$ is isomorphic to **Comod**(A), and **Mod**$(D(A))$ can be regarded as a combination of **Comod**(A) and **Mod**(A), as we soon see for the case of $\overline{G}$ in **Rel** below.

Since the antipode S of $\overline{G}$ is invertible, we can apply the quantum double construction to $\overline{G}$, and we obtain a quasi-triangular (in fact, ribbon) Hopf algebra $D(\overline{G})$:

Theorem 4.2 *Suppose that $G = (G, \cdot, e, (-)^{-1})$ is a group. There is a ribbon Hopf* *algebra* $D(\overline{G}) = (G \times G, m^{\mathrm{d}}, 1^{\mathrm{d}}, \Delta^{\mathrm{d}}, \epsilon^{\mathrm{d}}, S^{\mathrm{d}}, R, v)$ *in* **Rel***, with*

$$\begin{aligned}
m^{\mathrm{d}} &= \{(((g,h_1),(h_1^{-1}gh_1,h_2)),(g,h_1h_2)) \mid g,h_1,h_2 \in G\} \\
1^{\mathrm{d}} &= \{(*,(g,e)) \mid g \in G\} \\
\Delta^{\mathrm{d}} &= \{((g_1g_2,h),((g_1,h),(g_2,h)) \mid g_1,g_2,h \in G\} \\
\epsilon^{\mathrm{d}} &= \{((e,g),*) \mid g \in G\} \\
S^{\mathrm{d}} &= \{((g,h),(h^{-1}g^{-1}h,h^{-1})) \mid g,h \in G\} \\
R &= \{(*,((g,e),(h,g))) \mid g,h \in G\} \\
v &= \{(*,(g,g)) \mid g \in G\}
\end{aligned}$$

where R is the universal R-matrix and v is the universal twist.

When G is not Abelian, $D(\overline{G})$ is neither commutative nor co-commutative. Below we shall observe that modules of $D(\overline{G})$ can be identified with the *crossed G-sets* [12,34].

4.1 Crossed G-sets

Let $G = (G, \cdot, e, (-)^{-1})$ be a group. A *crossed G-set* $X = (X, \bullet, |\_|)$ is given by a set X together with a group action $\bullet : G \times X \to X$ and a function $|\_|$ from X to G such that, for any $g \in G$ and $x \in X$, $|g \bullet x| = g \cdot |x| \cdot g^{-1}$ holds. For instance, G itself can be seen a crossed G-set with $g \bullet h = g \cdot h \cdot g^{-1}$ and $|h| = h$. Another trivial example is a G-set with $|x| = e$.

Proposition 4.3 *For any set X, there is a bijective correspondence between $D(\overline{G})$-modules on X and crossed G-sets on X.*

Indeed, if $\alpha : G \times G \times X \to X$ is a $D(\overline{G})$-module, for any $g \in G$ and $x \in X$ there are unique $h \in G$ and $y \in X$ such that $(((h,g),x),y) \in \alpha$, and X carries the structure of crossed G-set where $g \bullet x$ is this uniquely determined y and $|x|$ is the unique h such that $(((h,e),x),x) \in \alpha$. Conversely, a crossed G-set $(X, \bullet, |\_|)$ gives rise to a module $\{((((|g \bullet x|, g), x), g \bullet x) \mid g \in G, x \in X\} : G \times G \times X \to X$.

A morphism of crossed G-sets from $(X, \bullet, |\_|)$ to $(Y, \bullet, |\_|)$, corresponding to the morphism of $D(\overline{G})$-modules, is a binary relation $r : X \to Y$ such that $(x,y) \in r$ implies $(g \bullet x, g \bullet y) \in r$ as well as $|x| = |y|$. The identity and composition of morphisms are just the same as those of binary relations. Let us denote the category of crossed G-sets and morphisms by $\mathbf{XRel}(G)$ which is isomorphic to $\mathbf{Mod}(D(\overline{G}))$. We note that the category G-$\mathbb{XSf}$ of crossed G-sets of Freyd and Yetter [12] is the subcategory of $\mathbf{XRel}(G)$ whose morphisms are restricted to functions and objects are restricted to finite ones. A variant of $\mathbf{XRel}(G)$ where G is not a group but a commutative monoid has appeared in [1].

4.2 *The ribbon structure on* $\mathbf{XRel}(G)$

By Proposition 2.2, $\mathbf{Mod}(D(\overline{G}))$, hence $\mathbf{XRel}(G)$, is a ribbon category. In $\mathbf{XRel}(G)$, the tensor unit is $I = (\{*\}, (g,x) \mapsto x, x \mapsto e)$, and the tensor product of $X = (X, \bullet, |\_|)$ and $Y = (Y, \bullet, |\_|)$ is

$$X \otimes Y = (X \times Y, (g,(x,y)) \mapsto (g \bullet x, g \bullet y), (x,y) \mapsto |x| \cdot |y|).$$

The tensor product of morphisms, as well as the coherence isomorphisms a, l, r, are inherited from **Rel**. For this monoidal structure we have a braiding $\sigma_{X,Y} : X \otimes Y \xrightarrow{\simeq} Y \otimes X$ induced by the universal R-matrix R as

$$\sigma_{X,Y} = \{((x,y),(|x| \bullet y, x)) \mid x \in X, y \in Y\}.$$

There is a twist $\theta_X : X \xrightarrow{\simeq} X$ induced by the universal twist v:

$$\theta_X = \{(x, |x| \bullet x) \mid x \in X\}.$$

For a crossed G-set $X = (X, \bullet, |\_|)$, its dual is $X^* = (X, \bullet, |\_|^{-1})$, with unit $\eta_X = \{(*, (x,x)) \mid x \in X\} : I \to X \otimes X^*$ and counit $\varepsilon_X = \{((x,x),*) \mid x \in X\} : X^* \otimes X \to I$. We note that the canonical trace on $\mathbf{XRel}(G)$ is given just like that on **Rel**: for $f : A \otimes X \to B \otimes X$, its trace $Tr^X_{A,B} f : A \to B$ is

$$Tr^X_{A,B} f = \{(a,b) \in A \times B \mid \exists x \in X \ ((a,x),(b,x)) \in f\}.$$

4.3 *Interpreting tangles in* $\mathbf{XRel}(G)$

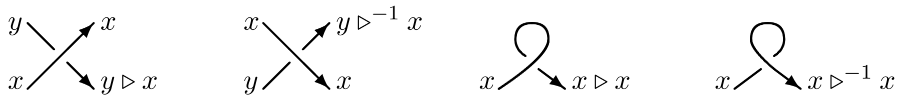
To understand how a crossed G-set gives rise to an invariant of (oriented, framed) tangles, it is helpful to consider the *rack* [10] associated to the crossed G-set [4]. Given a crossed G-set $(X, \bullet, |\_|)$, let us define operators $\triangleright, \triangleright^{-1} : X \times X \to X$ as $x \triangleright y = |y| \bullet x$ and $x \triangleright^{-1} y = |y|^{-1} \bullet x$. Then $(X, \triangleright, \triangleright^{-1})$ forms a rack; that is, the following equations hold [5].

$$\begin{array}{rcll} (x \triangleright y) \triangleright^{-1} y \;=\; x & = & (x \triangleright^{-1} y) \triangleright y & \text{(bijectivity of } (-) \triangleright y) \\ (x \triangleright y) \triangleright z & = & (x \triangleright z) \triangleright (y \triangleright z) & \text{(self-distributivity)} \end{array}$$

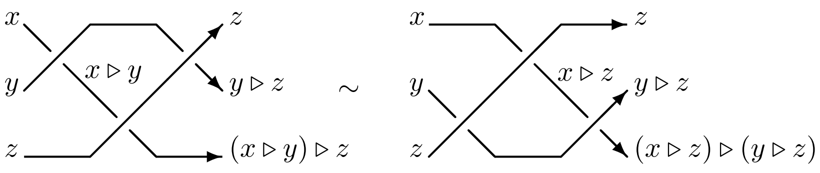
Now the braiding and twist can be described in terms of this rack: $\sigma_{X,Y} = \{((x,y),(y \triangleright x, x)) \mid x \in X, y \in Y\}$ and $\theta_X = \{(x, x \triangleright x) \mid x \in X\}$. The interpretation of a tangle diagram in $\mathbf{XRel}(G)$ with a crossed G-set X is then determined by all possible X-labelings of the segments from a underpass to the next underpass satisfying "y under x from left gives $y \triangleright x$" and "y under x from right gives $y \triangleright^{-1} x$".

[4] Indeed, another name for crossed G-sets coined by Fenn and Rourke is *augmented racks*. They have shown that every rack arises from an augmented rack, hence a crossed G-set.

[5] However, this may not be a *quandle* in the sense of Joyce [22], since the idempotency $x \triangleright x = x$ does not hold in general.



For instance, the self-distributivity justifies the Reidemeister move III:



5 A model of braided linear logic

In this section, we outline the notion of models of (fragments of) braided linear logic, and see how $\mathbf{XRel}(G)$ in the previous section gives such a model.

5.1 Models of braided linear logic

By a model of braided multiplicative linear logic (braided MLL), we mean a braided $*$-autonomous category [4]; note that a ribbon category is braided $*$-autonomous, hence is a model of braided MLL. A model of braided multiplicative additive linear logic (braided MALL) is then a braided $*$-autonomous category with finite products.

For exponential, we employ the following generalization of the notion of linear exponential comonads [18] on symmetric monoidal categories: by a linear exponential comonad on a braided monoidal category we mean a braided monoidal comonad whose category of coalgebras is a category of commutative comonoids. A model of braided MELL is then a braided $*$-autonomous category with a linear exponential comonad. (An implication of this definition is that braiding becomes symmetry on exponential objects: $\sigma^{-1}_{!X,!Y} = \sigma_{!Y,!X}$.) A model of braided LL is a model of MALL with a linear exponential comonad (or a model of MELL with finite products).

5.2 $\mathbf{XRel}(G)$ as a model of braided linear logic

$\mathbf{XRel}(G)$ is a ribbon category with finite products, hence is a model of braided MALL.

There is a strict balanced monoidal functor $F : \mathbf{Rel} \to \mathbf{XRel}(G)$ which sends a set X to $FX = (X, (g, x) \mapsto x, x \mapsto e)$. F has a right adjoint $U : \mathbf{XRel}(G) \to \mathbf{Rel}$ which sends $X = (X, \bullet, |\_|)$ to $UX = \{x \in X \mid |x| = e\}/_\sim$ where $x \sim y$ iff $g \bullet x = y$ for some g. By composing F and U with a linear exponential comonad ! on $\mathbf{Rel}$ (e.g. the finite multiset comonad), we obtain a linear exponential comonad $F!U$ on $\mathbf{XRel}(G)$ whose category of coalgebras is equivalent to that of !. Hence $\mathbf{XRel}(G)$ is a model of braided LL. As a result, there exists a linear fixed-point operator on $\mathbf{XRel}(G)$ as given in [16].

$\mathbf{XRel}(G)$ is degenerate as a model of LL in the sense that it cannot distinguish tensor from par. As an easy remedy, by applying the simple self-dualization construction [18] to $\mathbf{XRel}(G)$ we obtain a "non-compact" model of braided LL

$(\mathbf{XRel}(G) \times \mathbf{XRel}(G)^{\mathrm{op}})$.

6 Concluding remarks

We have demonstrated that there are many non-trivial Hopf algebras in the category of sets and binary relations. In particular, by applying the quantum double construction we have constructed a non-commutative non-co-commutative Hopf algebra with a universal R-matrix and a universal twist, and the ribbon category of its modules turns out to be a category of crossed G-sets.

Technically, most of our results are variations or instances of the already established theory of quantum groups, and we do not claim much novelty in this regard. What is much more important in this work, we believe, is that our results show that it is indeed possible to carry out a substantial part of quantum group theory in a category used for semantics of computation and logic. Although we have spelled out just a particular case of **Rel**, we expect that the same can be done meaningfully in various other settings, including

- the category of coherent spaces and linear stable maps [13], and its variations used as models of linear logic,
- various categories of games, in particular that of Conway games [29], and
- the category of sets (or presheaves on discrete categories) and linear normal functors [17], as well as the bicategory of small categories and profunctors.

The first two would lead to models of braided linear logic and braided game semantics. The third case is a direct refinement of **Rel**, in that we replace binary relations $X \times Y \to 2$ with **Set**-valued functors $X \times Y \to \mathbf{Set}$ (which amount to linear normal functors from $\mathbf{Set}^X$ to $\mathbf{Set}^Y$).

Finally, we should say that the computational significance of braided monoidal structure is yet to be examined. A potentially related direction would be the area of topological quantum computation [11].

Acknowledgement

I thank Shin-ya Katsumata and Craig Pastro for helpful discussions.

References

[1] Abramsky, S., R. Blute and P. Panangaden, *Nuclear and trace ideals in tensored $*$-categories*, J. Pure Appl. Algebra **143** (1999), 3–47.

[2] Abramsky, S. and B. Coecke, *A categorical semantics of quantum protocols*, In Proc. 19th IEEE Symposium on Logic in Computer Science, pp.415–425, 2004.

[3] Abramsky, S., E. Haghverdi and P.J. Scott, *Geometry of Interaction and linear combinatory algebras.* Math. Struct. Comp. Sci. **12**(5) (2002), 625–665.

[4] Barr, M., *Nonsymmetric $*$-autonomous categories*, Theoret. Comput. Sci. 139 (1995), 115–130.

[5] Bloom, S. and Z. Ésik, "Iteration Theories," EATCS Monographs on Theoretical Computer Science, Springer-Verlag, 1993.

[6] Blute, R., *Hopf algebras and linear logic*, Math. Struct. Comput. Sci. **6** (1996), 189–217.

[7] Bruguieres, A. and A. Virelizier, *Hopf monads,* Adv. Math. **215** (2007), 679–733.

[8] Chen, H.-X., *Quantum doubles in monoidal categories*, Comm. Algebra **28** (2000), 2303–2328.

[9] Drinfel'd, V.G., *Quantum groups*, In Proc. Intrn. Congr. Math., Berkley, 1986, vol. 1, pp. 798–820, 1987.

[10] Fenn, R. and C. Rourke, *Racks and links in codimension two.* J. Knot Theory Ramifications **1** (1992), 343–406.

[11] Freedman, M.H., A. Kitaev and Z. Wang, *Simulation of topological field theories by quantum computers*, Commun. Math. Phys. **227** (2002), 587–603.

[12] Freyd, P. and D.N. Yetter, *Braided compact closed categories with applications to low dimensional topology*, Adv. Math. **77** (1989), 156–182.

[13] Girard, J.-Y., *Linear logic*, Theoret. Comp. Sci. **50** (1987), 1–102.

[14] Girard, J.-Y., *Geometry of Interaction I: interpretation of system F*, in Proc. Logic Colloquium '88, pp. 221–260, 1989.

[15] Hasegawa, M., "Models of Sharing Graphs: A Categorical Semantics of let and letrec," Distinguished Dissertations Series, Springer-Verlag, 1999.

[16] Hasegawa, M., *On traced monoidal closed categories*, Math. Struct. Comput. Sci. **19** (2009), 217–244.

[17] Hasegawa, R., *Two applications of analytic functors*, Theoret. Comput. Sci. **272** (2002), 113–175.

[18] Hyland, J.M.E. and A. Schalk, *Glueing and orthogonality for models of linear logic*, Theoret. Comp. Sci. **294** (2003), 183–231.

[19] Joyal, A. and R. Street, *The geometry of tensor calculus, I*, Adv. Math. **88** (1991), 55–113.

[20] Joyal, A. and R. Street, *Braided tensor categories*, Adv. Math. **102** (1993), 20–78.

[21] Joyal, A., R. Street and D. Verity., *Traced monoidal categories*, Math. Proc. Cambridge Phils. Soc. **119** (1996), 447–468.

[22] Joyce, D., *A classifying invariant of knots, the knot quandle*, J. Pure Appl. Algebra **23** (1982), 37–65.

[23] Kassel, C., "Quantum Groups," Graduate Texts in Mathematics **155**, Springer-Verlag, 1995.

[24] Kassel, C. and V.G. Turaev, *Double construction for monoidal categories*, Acta Math., **175** (1995), 1–48.

[25] Kelly, G.M. and M.L. Laplaza, *Coherence for compact closed categories*, J. Pure Appl. Algebra **19** (1980), 193–213.

[26] Mac Lane, S., "Categories for the Working Mathematician," Graduate Texts in Mathematics **5**, Springer-Verlag, 1971.

[27] Majid, S., *Physics for algebraists: noncommutative and noncocommutative Hopf algebras by a bicrossproduct construction*, J. Algebra **130** (1990), 17–64.

[28] Majid, S., "Foundations of Quantum Group Theory," Cambridge University Press, 1995.

[29] Melliès, P.-A., *Asynchronous games 3: an innocent model of linear logic*, in Proc. Category Theory and Computer Science, Electr. Notes Theor. Comput. Sci. **122**, pp. 171–192, 2004.

[30] Pastro, C. and R. Street, *Closed categories, star-autonomy, and monoidal comonads*, J. Algebra **321** (2009), 3494-3520.

[31] Selinger, P., *A survey of graphical languages for monoidal categories,* in "New Structures for Physics," Springer Lecture Notes in Phys., to appear.

[32] Shum, M.-C., *Tortile tensor categories*, J. Pure Appl. Algebra **93** (1994), 57–110.

[33] Turaev, V.G., "Quantum Invariants of Knots and 3-Manifolds," de Gruyter, 1994.

[34] Whitehead, J.H.C., *Combinatorial homotopy. II*, Bull. Amer. Math. Soc. **55** (1949), 453–496.

[35] Yetter, D.N., "Functorial Knot Theory," World Scientific, 2001.