UNIVERSIDADE FEDERAL DA BAHIA
INSTITUTO DE FÍSICA
PROGRAMA DE PÓS-GRADUAÇÃO EM FÍSICA

Eric Matos de Assis Pinto

Álgebras de Hopf em Computação Quântica

Salvador
2015

Eric Matos de Assis Pinto

Álgebras de Hopf em Computação Quântica

Dissertação apresentada ao Programa de Pesquisa e Pós-graduação em Física, Instituto de Física, Universidade Federal da Bahia, como requisito parcial para obtenção do grau de Mestre em Física.

Universidade Federal da Bahia – UFBA

Instituto de Física

Programa de Pós-Graduação em Física

Orientador: Dr. José David Mangueira Vianna

Coorientador: Dr. Marco Antônio Silva Trindade

Salvador

2015

Pinto, Eric Matos de Assis
Álgebras de Hopf em Computação Quântica/ Eric Matos de Assis Pinto. – Salvador, 2015-
54 p. : il. (algumas color.) ; 30 cm.

Orientador: Dr. José David Mangueira Vianna

Dissertação de Mestrado – Universidade Federal da Bahia – UFBA
Instituto de Física
Programa de Pós-Graduação em Física, 2015.

1. Física matemática. 2. Computação quântica. 2. Grupos quânticos. I. Orientador. II. Universidade Federal da Bahia. III. Instituto de Física. IV. Álgebras de Hopf em Computação Quântica

CDU 512.54:530.145

Eric Matos de Assis Pinto

Álgebras de Hopf em Computação Quântica

Dissertação apresentada ao Programa de Pesquisa e Pós-graduação em Física, Instituto de Física, Universidade Federal da Bahia, como requisito parcial para obtenção do grau de Mestre em Física.

Aprovado em 04 de fevereiro de 2015:

Dr. José David Mangueira Vianna
Orientador – IF-UFBA/UnB

Dr. Marco Antônio Silva Trindade
Coorientador – UNEB

Dr. Esdras Santana dos Santos
IF-UFBA

Dr. Milton Souza Ribeiro
UEFS

Salvador

Aos meus pais: Walder(em memória) e Cremilda.

Agradecimentos

Em primeiro lugar, peço desculpas à todos que não pude citar, em virtude da minha memória já não tão eficiente. Vocês também fizeram parte deste trabalho. Sem mais, começarei:

A Deus pela Natureza.

Aos meus pais, Walder (em memória) e Cremilda por acreditarem que eu tinha salvação (risos). Sempre presentes, da primeira palavra pronunciada à universidade; sei que vocês fizeram muitos sacrifícios para que eu pudesse ter uma graduação e agora uma pós-graduação. Sinto que nunca poderei agradecer à altura tudo que fizeram por mim e continuam fazendo; mesmo assim tenho de dizer: Obrigado! Emocionado, agora, faltam-me palavras para continuar este agradecimento, porém, gostaria que soubessem que a existência de vocês é a minha força para poder continuar essa jornada; para mim vocês "são o exemplo a seguir e o objetivo a ser alcançado".

Aos tios e tias, Edith(em memória), Maria Dolores (em memória), J. César, Irene, José Cardoso, Nancy, Dedeu (José Carlos), Edson (Mattozão), Pedro Pinto e Cláudio Mattos. Sem o apoio de vocês esta missão seria quase que impossível.

A todos os primos, em especial: Chrystian e Chrystiane.

Ao meu orientador Dr. José David M. Vianna pela orientação e contribuições nesses anos de trabalho. Aproveitando, também agradeço pelo tempo de iniciação científica o qual fiquei sob sua orientação. Valeu!

Ao meu coorientador Dr. Marco Trindade. Sua coorientação com aspecto de orientação teve grande influência neste trabalho.

A Marco Trindade (estendido à Luciene) por ser um amigo de todas as horas. Sempre solícito, esteve presente desde a primeira ficha da biblioteca à apresentação do atual orientador. Agradeço os primeiros artigos sobre álgebras e Física, os vinhos, telefonemas os quais discutíamos assuntos variados, as palavras de incentivo, o auxílio financeiro (já paguei!) e etc. Também faltam-me palavras para expressar como isso tudo foi/é de suma importância para construção deste trabalho. Nunca me esquecerei disto....

A Daiana do Carmo, por ter sido uma pessoa muito especial. Sejam em situações boas ou não, contei com seu apoio e suas opiniões sinceras.

A todos meus amigos, em especial: Gabriela Lima, Arisvaldo Matos, Cintia Santos, Filipe Velame, Juliana Martini, Roberta Martini e Tiago Nariga; incluindo suas respectivas famílias. Por sempre (ou às vezes) entenderem a minha ausência em encontros, festas e

etc. Mesmo assim, vocês de forma ininterrupta me ajudaram de diversas maneiras neste período. Com certeza, vocês tornaram a minha caminhada menos árdua e com mais alegria.

A todos os estudantes da pós do IF. Em particular, aos companheiros[1]: Dion Ribeiro, Dunga (João R. Pessoa), Wilson (Vinícius Mendonça), Alessandro de Barros (*Michael Douglas*), Harliton Jonas, Antonio Lafayette, Sergio Floquet, Wallas Nascimento (Zoo), Mestre (Vinícius Nonato), Marcelo Sandoval, Caio Guimarães (*Harry Potter*), Miralvo Menezes (Chimbinha), Sr. Antônio Pires (*The Old Man*), Caio Porto, Yuri Hamayano, Vitor Damião, Tenilson, Luís Pires, Carla Sena, Maroívo (Landau do Nordeste), William Nogueira, Renato de Jesus, Daniel Prado, João Cláudio, Leandro Cerqueira, Aureliano Sancho(ex-Djavan e representante da "Alphaville") e Manuela. Mais uma vez, agradeço pelo apoio nas disciplinas, palavras de conforto, discussões em diversos tópicos, piadas "não ofensivas", cervejas e bagunças (risos). Eu ratifico, sem dúvidas, que foram vocês que enobreceram a minha vivência no IF e tornaram-na agradável e divertida. Também a Kim Veiga e Érico Novais pelo livros emprestados no CBPF.

Aos professores Lourival da Silva Filho (UNEB), Antônio Ferreira, Humberto Borges e Maria das Graças.

Aos funcionários do IF-UFBA: Marli, João Paulo, Marcos Paulo, Seu Valtério, Dona Eraldina, Elson, Teresa, Jô, Maridalva (Dal), Gilmar, Aloísio, Bruno, Priscila, Geraldo e Seu Nelson.

Ao pessoal da antiga cantina, em particular, Rita e Jorge pela torcida e contas penduradas!

Aos criadores do abnTEX2 por disponibilizarem este modelo de dissertação.

A CAPES pelo apoio financeiro.

[1] "Essa é a minha galera!" Por Nascimento, W. S.

"Um ponto de vista é a vista a partir de um ponto."
(Leonardo Boff)

Resumo

Nesta dissertação apresentamos os conceitos de álgebras de Hopf quase triangulares e suas conexões com a computação quântica, mais especificamente, a computação quântica topológica. Fornecemos então um método para se obter representações do grupo de tranças através de um conjunto de álgebras de Hopf quase triangulares. Em particular, essas álgebras podem ser derivadas a partir das álgebras de grupo dos grupos cíclicos com as estruturas algébricas adicionais. Neste contexto, utilizando o operador *flip*, construímos as R-matrizes que podem ser consideradas como portas lógicas, capazes de preservar o emaranhamento quântico. Além disso, vantagens e perspectivas desta formulação são apresentadas.

Palavras-chaves: Física matemática. Computação quântica. Grupos quânticos.

Abstract

In this work, we have presented the concepts of quasitriangular Hopf algebras and their connections with quantum computation, more specifically, the topological quantum computation. The aim of this work to provide a method to obtain representations of the braid group through a set of quasitriangular Hopf algebras. In particular, these algebras may be derived from group algebras of cyclic groups with additional algebraic structures. In this context, by using the flip operator, we construct R-matrices that can be regarded as quantum logic gates capable of preserving quantum entanglement. Furthermore, we present advantages and prospects in this formulation.

Keywords: Mathematical physics. Quantum computation. Quantum groups.

Lista de ilustrações

Sumário

1 Introdução

No século XX, mais precisamente em 1936, Church e Turing começaram a estabelecer as bases teóricas para a computação, ou seja, conjuntos de conhecimentos matemáticos que formalizaram as ideias de computador e de como resolver algum problema matemático (algoritmo) [1]. Apesar dos bons resultados obtidos, o computador clássico ainda apresentava algumas limitações. Então, em 1982, Feynman publicou um trabalho [2] em que aborda a simulação de sistemas de partículas que se comportam de acordo com a mecânica quântica. Ele observou que problemas simples da física quântica pareciam requerer um número imenso de passos computacionais na sua resolução. Feynman mostrou que se controlássemos com precisão um sistema quântico simples, ele funcionaria como um computador capaz de calcular propriedades quânticas. Em 1985, Deutsch no intuito de generalizar as tarefas do computador dito quântico, propôs o equivalente quântico da máquina de Turing, ou seja, ao invés de passos computacionais usuais, essa máquina utilizaria passos digamos quânticos i.e. usando características quânticas. Essa proposta ficou conhecida como o computador quântico universal [3].

Atualmente, o emaranhamento quântico desempenha um papel fundamental na informação e computação quânticas [3]. A descoberta do emaranhamento quântico tem origens no artigo seminal de Einstein, Podolsky e Rosen (EPR) em 1935 [4]. Neste trabalho foi proposto um experimento mental para mostrar que a teoria da mecânica quântica estava incompleta. O emaranhamento quântico também tem sido amplamente explorado em teletransporte quântico [5], algoritmos quânticos [6] e criptografia quântica [7,8]. Dentre algumas propostas para implementação da computação quântica, uma proposta envolvente é a computação quântica topológica que emprega quase partículas bidimensionais chamadas de *anyons* [9], cujas linhas de universo (trajetórias no espaço-tempo tridimensional) "atravessam" umas às outras para formarem tranças. Essas tranças formam as portas lógicas de um computador quântico. Uma das vantagens dessa proposta é o fato de que ela permite que a computação quântica seja tolerante à falhas. Como se sabe, pequenas perturbações podem causar decoerência e introduzir erros em computação; no entanto, essas pequenas perturbações não alteram as propriedades topológicas de tranças. Evidências experimentais de *anyons* não abelianos aparecem em sistemas Hall quânticos de gases de elétrons bidimensionais sujeitos a elevados campos magnéticos [9].

Do ponto de vista matemático, os *anyons* são descritos por representações dos grupos de tranças, uma estrutura algébrica que foi explicitamente introduzida por Artin em 1925 [10]. Na topologia algébrica e na teoria dos nós, esse grupo pode ser reconhecido como o grupo fundamental de um espaço de configuração, utilizando o conceito de homotopia [11]. Uma ponte entre a teoria dos nós e a informação quântica pode ser

encontrada nas referências [12–16]. Em particular, na referência [17], o teletransporte quântico foi descrito pelo grupo de tranças e pela álgebra de Temperley-Lieb, fornecendo representações esquemáticas de teletransporte. Nessa linha, não é explícita a ligação estabelecida com os *anyons* e com uma perspectiva geral da topológica algébrica. Uma abordagem para *anyons* não abelianos através de álgebras de Hopf quase triangulares [18] foi realizada por Kitaev [19,20]. A estrutura quase triangular [21,22] fornece uma descrição unificada das propriedades de tranças; isso ocorre através da utilização da equação de Yang-Baxter. O produto final é a R-matriz universal que pode ser usada para definir as representações dos grupos de tranças em espaços de fusão, também denominados espaços de Hilbert topológicos.

As álgebras de Hopf [23–25] aparecem naturalmente em topologia algébrica, onde estão relacionadas com o conceito de H-espaço. Sua origem está nas axiomatizações das obras de Hopf sobre propriedades topológicas dos grupos de Lie. A noção de álgebras de Hopf quase triangulares ou grupos quânticos, por sua vez, é devido a Drinfeld [18] como uma abstração de estruturas implícitas nos estudos de Sklyanin [25–27], Jimbo [28] entre outros [25]. Existem muitas aplicações destas estruturas em física, especialmente relacionados com a gravidade quântica [24, 25]. A relação entre os grupos quânticos e emaranhamento quântico pode ser encontrada nas referências [29,30]. Os autores Trindade e Vianna [29] realizaram uma possível conexão entre grupos quânticos, mecânica estatística não extensiva e emaranhamento quântico através do parâmetro entrópico q. Já Korbicz et al. [30], abordaram o problema da separabilidade em termos de grupos quânticos compactos, resultando em um critério análogo ao critério da transposição parcial presente na teoria da informação quântica. Na referência [21] foi mostrado como álgebras de Hopf quase triangulares podem gerar R-matrizes. Este resultado é particularmente interessante porque permite a obtenção de representações do grupo de tranças, uma vez que se tenha estruturas quase triangulares. Neste trabalho, desenvolvemos um método geral para obtenção das representações dos grupos de tranças de um conjunto de álgebras de Hopf; aplicaremos estes resultados para álgebras de Hopf derivadas de grupos cíclico se em particular, investigamos as atuações do grupo CZ_2 e das portas lógicas quânticas geradas em estados de Bell [31].

Esta dissertação está disposta da seguinte forma. No capítulo 2 revisaremos as definições de álgebras associativas, coálgebras, biálgebras e mostraremos alguns exemplos. Apresentaremos o conceito de operador *flip* e suas atuações nas estruturas algébricas supracitadas. Finalizaremos com as definições de álgebras de Hopf.

O capítulo 3 é destinado à uma revisão sucinta da computação quântica. Iremos expor os conceitos de q-bits e portas lógicas quânticas. Uma síntese acerca do emaranhamento quântico também será feita. Serão apresentados alguns tópicos relacionados à computação quântica topológica, os quais foram fontes de motivações para realização deste trabalho. Dentro desse contexto, definiremos grupos de trança e suas relações com a

computação quântica topológica.

Já o capítulo 4 trataremos das álgebras de Hopf quase triangulares e suas relações com a equação de Yang-Baxter. Exibiremos nosso método para se obter representações dos grupos de tranças de um conjunto de álgebras de Hopf. Em seguida, aplicaremos estes resultados para álgebras de Hopf derivadas de grupos cíclicos. Com isso, em particular, investigaremos as atuações das portas lógicas quânticas em pares EPR.

Por fim, no capítulo 5 apresentaremos as conclusões e perspectivas. Nos apêndices A e B, encontram-se alguns resumos dos conceitos usados ao longo da dissertação.

2 Álgebras de Hopf

Este capítulo apresenta uma breve revisão de algumas estruturas matemáticas utilizadas para nossa proposta de construção de portas lógicas quânticas. Essa revisão tem como objetivo principal apresentar as álgebras de Hopf [23,32] que servirão como base para os estudos das álgebras de Hopf quase triangulares [25]. No entanto, para compreensão dessas estruturas, estudaremos as álgebras, coálgebras e biálgebras [33–35]. Ao longo do texto veremos que algumas definições e teoremas são apresentados através da linguagem de categorias, pois o conceito de dualidade, presente entre as estruturas, refere-se à inversão do sentido dos morfismos em certos diagramas comutativos [36]. Algumas aplicações em Física que utilizam a teoria das categorias podem ser vistas na referência [37]. No nosso caso, quando dualizarmos morfismos de álgebras, obteremos morfismos de coálgebras, porém álgebras e coálgebras não são somente noções duais. Já as biálgebras conterão as estruturas de álgebras e coálgebras com uma certa junção de ambas. E por fim, definiremos e exemplificaremos as álgebras de Hopf.

2.1 Álgebras

Definição 2.1.1. *Uma álgebra com unidade é uma coleção (A, μ, η) consistindo de um espaço vetorial A sobre um corpo k e de duas aplicações lineares $\mu : A \otimes A \to A$ e $\eta : k \to A$ que tornam comutativos os diagramas e satisfazem os axiomas a seguir:*

i) Associatividade:

$$\begin{array}{ccc} A \otimes A \otimes A & \xrightarrow{\mu \otimes id} & A \otimes A \\ {\scriptstyle id \otimes \mu}\downarrow & & \downarrow{\scriptstyle \mu} \\ A \otimes A & \xrightarrow{\mu} & A \end{array} \tag{2.1}$$

ou, $\mu \circ (\mu \otimes id) = \mu \circ (id \otimes \mu)$, em que $id : A \to A$ e $\mu : A \otimes A \to A$ são as aplicações identidade e multiplicação respectivamente.

ii) Unidade:

$$\begin{array}{ccccc} k \otimes A & \xrightarrow{\eta \otimes id} & A \otimes A & \xleftarrow{id \otimes \eta} & A \otimes k \\ & {\scriptstyle \cong}\searrow & \downarrow{\scriptstyle \mu} & \swarrow{\scriptstyle \cong} & \\ & & A & & \end{array} \tag{2.2}$$

isto é, $\mu \circ (id \otimes \eta) = \mu \circ (\eta \otimes id) = id$ em que η é denominada aplicação unidade, denotada por $\eta(\lambda) = \lambda 1$ para $\lambda \in k$ e 1 unidade da álgebra; o símbolo "$\circ$" indica a composição de

aplicações e a aplicação $\cong$ *representa o isomorfismo natural entre* A *e* $A \otimes k$*, onde se tem* $\lambda \otimes a = a \otimes \lambda = \lambda a$*,* $a \in A$*.*

A álgebra acima definida é denominada álgebra associativa sobre o corpo k e com unidade.

Exemplo 2.1.1. Seja k um corpo e X um conjunto não vazio qualquer. O conjunto $F(X)$ será composto pelas funções $f : X \to k$. Sejam $f, g \in F(X)$ e $\lambda \in k$, com as operações $f + g$ e λf definidas por:

$$\begin{aligned} (f+g)(x) &= f(x) + g(x) \\ (\lambda f)(x) &= \lambda f(x). \end{aligned}$$

com $\forall x \in X$. Continuando as definições:

$$\begin{aligned} \mu : F(X) \otimes F(X) &\to F(X) \\ f \otimes g &\mapsto f \cdot g, \end{aligned}$$

em que $(f \cdot g)(x) = f(x) \cdot g(x)$, $\forall x \in X$. Tem-se a função constante $1(x) = 1$. Assim, a tripla $(F(X), \mu, 1)$ é uma álgebra com o elemento unidade sendo a função constante 1; em outras palavras:

$$\begin{aligned} \mu \circ (id \otimes \mu)(f \otimes g \otimes h)(x) &= f(x) \cdot (g(x) \cdot h(x)) \\ &= (f(x) \cdot g(x)) \cdot h(x) \\ &= \mu \circ (\mu \otimes id)(f \otimes g \otimes h)(x) \end{aligned}$$

e

$$\mu \circ (1 \otimes f)(x) = 1(x) \cdot f(x) = 1 \cdot f(x) = f(x)$$

□

Há também uma aplicação que usaremos denominada por aplicação transposição[1] ou aplicação *flip*. Ela é definida por $\tau : V_1 \otimes V_2 \to V_2 \otimes V_1$ e $\tau(v_1 \otimes v_2) = v_2 \otimes v_1$, para todo $v_1 \in V_1$ e $v_2 \in V_2$. Observe que $V_1 \otimes V_2$ é o produto tensorial dos espaços vetoriais V_1 e V_2 sobre k. Em alguns casos quando τ possuir subíndices, estes indicarão quais parcelas estão sendo operadas. Por exemplo, $\tau_{34} : V_1 \otimes V_2 \otimes V_3 \otimes V_4 \otimes V_5 \to V_1 \otimes V_2 \otimes V_4 \otimes V_3 \otimes V_5$, logo $\tau_{34}(v_1 \otimes v_2 \otimes v_3 \otimes v_4 \otimes v_5) = v_1 \otimes v_2 \otimes v_4 \otimes v_3 \otimes v_5$, com $v_i \in V_i (i = 1, \ldots, 5)$. Como exemplo da aplicação transposição, apresentaremos a definição de álgebra oposta.

Exemplo 2.1.2. Seja (A, μ, η) uma álgebra. Seja a tripla (A, μ^{op}, η) em que definimos a aplicação multiplicação como sendo $\mu^{op} = \mu \circ \tau$. Verifica-se que

[1] Também conhecida por aplicação *twist*

$$\mu^{op} \circ (id \otimes \mu^{op}) = \mu^{op} \circ (\mu^{op} \otimes id)$$

e

$$\mu^{op} \circ (\eta \otimes id) = \mu^{op} \circ (id \otimes \eta) = id$$

Logo, a coleção (A, μ^{op}, η) é uma álgebra e denotamos por A^{op}. Essa álgebra é a que chamamos de álgebra oposta à álgebra A. Dizemos que uma álgebra A é comutativa se sua multiplicação satisfaz $\mu = \mu^{op}$. □

Agora, consideremos as álgebras A_1 e A_2. Definimos a aplicação

$$\mu_{A_1 \otimes A_2} : (A_1 \otimes A_2) \otimes (A_1 \otimes A_2) \to A_1 \otimes A_2$$

em que $\mu_{A_1 \otimes A_2} = (\mu_{A_1} \otimes \mu_{A_2}) \circ (id \otimes \tau \otimes id)$, e também a aplicação

$$\eta_{A_1 \otimes A_2} : k \to A_1 \otimes A_2$$

por $\eta_{A_1 \otimes A_2} = \eta_{A_1} \otimes \eta_{A_2}$. As aplicações $\mu_{A_1 \otimes A_2}$ e $\eta_{A_1 \otimes A_2}$ são lineares e satisfazem os axiomas tornando comutativos os diagramas (2.1) e (2.2). Portanto, $(A_1 \otimes A_2, \mu_{A_1 \otimes A_2}, \eta_{A_1 \otimes A_2})$ é uma álgebra com unidade $1_{A_1} \otimes 1_{A_2}$. A essa álgebra atribuímos o nome de álgebra produto tensorial entre A_1 e A_2.

Definição 2.1.2. *Seja A uma álgebra. Diz-se que $B \subseteq A$ é uma subálgebra se $\mu(B \otimes B) \subseteq B$.*

Entende-se por homomorfismo de álgebras, entre as álgebras A_1 e A_2, como sendo uma aplicação linear $\varphi : A_1 \to A_2$ que torna comutativo os diagramas:

$$\begin{array}{ccc} A_1 \otimes A_1 & \xrightarrow{\varphi \otimes \varphi} & A_2 \otimes A_2 \\ \downarrow{\scriptstyle \mu_{A_1}} & & \downarrow{\scriptstyle \mu_{A_2}} \\ A_1 & \xrightarrow{\varphi} & A_2 \end{array} \tag{2.3}$$

$$\begin{array}{ccc} k & \xrightarrow{id} & k \\ \downarrow{\scriptstyle \eta_{A_1}} & & \downarrow{\scriptstyle \eta A_2} \\ A_1 & \xrightarrow{\mu} & A_2 \end{array} \tag{2.4}$$

ou, $\varphi \circ \mu_{A_1} = \mu_{A_2} \circ (\varphi \otimes \varphi)$ e $\varphi \circ \eta_{A_1} = \eta_{A_2}$, ou seja a unidade é preservada. Denotamos o homomorfismo entre essas álgebras por $\mathrm{Hom}(A_1, A_2)$.

2.2 Coálgebras

Definição 2.2.1. *Uma coálgebra é uma tripla (C, Δ, ε) consistindo de um espaço vetorial C sobre um corpo k e de duas aplicações lineares $\Delta : C \to C \otimes C$ e $\varepsilon : C \to k$ que tornam comutativos os diagramas e satisfazem os axiomas:*

i) Coassociatividade:

$$\begin{array}{ccc} C \otimes C \otimes C & \xleftarrow{\Delta \otimes id} & C \otimes C \\ {\scriptstyle id \otimes \Delta}\uparrow & & \uparrow{\scriptstyle \Delta} \\ C \otimes C & \xleftarrow{\Delta} & C \end{array} \tag{2.5}$$

em símbolos, $(\Delta \otimes id) \circ \Delta = (id \otimes \Delta) \circ \Delta$, em que a aplicação Δ é chamada comultiplicação ou aplicação coproduto.

ii) Counidade:

$$\begin{array}{ccccc} k \otimes C & \xleftarrow{\varepsilon \otimes id} & C \otimes C & \xrightarrow{id \otimes \varepsilon} & C \otimes k \\ & \nwarrow^{\cong} & \uparrow{\scriptstyle \Delta} & \nearrow_{\cong} & \\ & & C & & \end{array} \tag{2.6}$$

ou, $(id \otimes \varepsilon) \circ \Delta = (\varepsilon \otimes id) \circ \Delta = id$ em que ε é conhecida como a aplicação counidade.

Exemplo 2.2.1. Seja G um grupo e kG o módulo livre gerado por G sobre k. Definimos $\Delta : kG \to kG \otimes kG$ e $\varepsilon : kG \to k$, coproduto e counidade, respectivamente, por:

$$\Delta(g) = g \otimes g$$

$$\varepsilon(g) = 1$$

para $g \in G$(kG). Assim,

$$\begin{aligned} (\Delta \otimes id) \circ \Delta(g) &= g \otimes g \otimes g \\ &= (id \otimes \Delta) \circ \Delta(g) \end{aligned}$$

e

$$(id \otimes \varepsilon) \circ \Delta(g) = g = (\varepsilon \otimes id) \circ \Delta(g)$$

em que Δ é um coproduto coassociativo e ε é uma counidade em kG, logo, $(FG, \Delta, \varepsilon)$ é uma coálgebra. □

O homomorfismo de coálgebras pode ser definido como sendo uma aplicação linear $\varphi : C_1 \to C_2$ de uma coálgebra C_1 em uma coálgebra C_2 tornando comutativos os diagramas

a seguir:

$$\begin{array}{ccc} C_2 \otimes C_2 & \xleftarrow{\varphi\otimes\varphi} & C_1 \otimes C_1 \\ {\scriptstyle \Delta_{C_2}}\uparrow & & \uparrow{\scriptstyle \Delta_{C_1}} \\ C_2 & \xleftarrow{\varphi} & C_1 \end{array} \tag{2.7}$$

$$\begin{array}{ccc} k & \xleftarrow{id} & k \\ {\scriptstyle \varepsilon_{C_2}}\uparrow & & \uparrow{\scriptstyle \varepsilon_{C_1}} \\ C_2 & \xleftarrow{\varphi} & C_1 \end{array} \tag{2.8}$$

ou seja $(\varphi \otimes \varphi) \circ \Delta_{C_1} = \Delta_{C_2} \circ \varphi$ e $\varepsilon_{C_2} \circ \varphi = \varepsilon_{C_1}$.

A aplicação *flip*, assim como na álgebra, pode ser definida de forma similar:

$$\begin{aligned} \tau : C \otimes C &\to C \otimes C \\ (x \otimes y) &\mapsto (y \otimes x) \end{aligned}$$

em que $x, y \in C$. Denotamos o coproduto oposto por $\Delta^{op} = \tau \circ \Delta$. Portanto, $(C, \Delta^{op}, \varepsilon)$ é uma coálgebra oposta. Também dizemos que C é cocomutativa quando $\Delta^{op} = \Delta$.

2.2.1 Notação de Sweedler

É oportuno falarmos de uma notação bastante utilizada, que fora introduzida por Moss E. Sweedler [32]. Essa notação expressa as relações dadas pelos diagramas (2.5) e (2.6), em termos dos elementos de C. Consideremos x um elemento qualquer da coálgebra (C, Δ, ε) e o elemento $\Delta(x) \in C \otimes C$ como sendo:

$$\Delta(x) = \sum_i x_{i_1} \otimes x_{i_2}$$

ou,

$$\Delta(x) = \sum_{(x)} x_{(1)} \otimes x_{(2)} = \sum x_{(1)} \otimes x_{(2)} \tag{2.9}$$

Denotando de forma compacta, temos:

$$\Delta(x) = x' \otimes x'' \tag{2.10}$$

Utilizando a notação de Sweedler, podemos expressar a coassociatividade do coproduto, isto é, a comutatividade do diagrama (2.5) da seguinte forma:

$$\begin{aligned} \sum_{(x)} \left(\sum_{(x')} (x')' \otimes (x')'' \right) \otimes x'' &= \sum_{(x)} x' \otimes \left(\sum_{(x'')} (x'')' \otimes (x'')'' \right) \\ &= \sum_{(x)} x' \otimes x'' \otimes x''' \end{aligned} \tag{2.11}$$

Notemos que a coassociatividade nos diz que não importa qual parte de $\Delta(x)$ é "separada". Ademais, se aplicarmos o coproduto à equação (2.11), teremos três novas expressões:

$$\Delta(x') \otimes x'' \otimes x''' = x' \otimes \Delta(x'') \otimes x''' = x' \otimes x'' \otimes \Delta(x''').$$

Por convenção, reescrevemos:

$$x' \otimes x'' \otimes x''' \otimes x'''' \tag{2.12}$$

ou $x^{(1)} \otimes x^{(2)} \otimes x^{(3)} \otimes x^{(4)}$.

Generalizando,

$$\Delta^{(n)} : C \longrightarrow C^{\otimes(n+1)}$$

$$\Delta^{(n)} = (\Delta \otimes id_{C^{\otimes(n-1)}}) \circ \Delta^{(n-1)} = (id_{C^{\otimes(n-1)}} \otimes \Delta^{(n-1)}) \circ \Delta^{n-1} \tag{2.13}$$

em que $n \geq 1$ e $\Delta^{(1)} = \Delta$. E portanto, podemos escrever:

$$\Delta^n(x) = \sum_{(x)} x^{(1)} \otimes x^{(2)} \otimes \cdots \otimes x^{(n+1)}. \tag{2.14}$$

Naturalmente, utilizando a notação de Sweedler (2.10), o axioma da counidade (2.6) pode ser reescrito para qualquer $x \in C$, como:

$$\sum_{(x)} \varepsilon(x')x'' = x = \sum_{(x)} x'\varepsilon(x''). \tag{2.15}$$

A implicação das equações (2.14) e (2.15), será:

$$x^{(1)} \otimes \cdots \otimes \varepsilon(x^{(i)}) \otimes \cdots \otimes x^{(n+1)} = x^{(1)} \otimes \cdots \otimes x^{(n)}. \tag{2.16}$$

Exemplo 2.2.2. Seja x um elemento da coálgebra C. Devemos mostrar que $\Delta(x) = \Delta(x')\varepsilon(x'')$. Inicialmente, mostraremos a partir das propriedades das aplicações lineares Δ e ε, isto é:

$$\begin{aligned}
\Delta(x')\varepsilon(x'') &= (\Delta \otimes \varepsilon) \circ \Delta(x) \\
&= (id \otimes id \otimes \varepsilon) \circ (\Delta \otimes id) \circ \Delta(x) \\
&= (id \otimes id \otimes \varepsilon) \circ (id \otimes \Delta) \circ \Delta(x) \\
&= (id \otimes ((id \otimes \varepsilon) \circ \Delta)) \circ \Delta(x) \\
&= (id \otimes id) \circ \Delta(x) \\
&= \Delta(x).
\end{aligned}$$

Agora, utilizando a notação de Sweedler, tem-se

$$\begin{aligned}\Delta(x')\varepsilon(x'') &= (x')' \otimes (x')'' \otimes \varepsilon(x'') \\ &= x' \otimes (x'')' \otimes \varepsilon((x'')'') \\ &= x' \otimes x'' \\ &= \Delta(x).\end{aligned}$$

□

Em dessemelhantes textos sobre álgebras de Hopf inúmeras demonstrações são feitas utilizando a notação de Sweedler, sempre objetivando a clarificação das demonstrações. Outras nuances desta notação podem ser vistas, também de forma didática, no apêndice B da referência [35].

Um outro exemplo interessante é o caso que surge ao considerarmos duas coálgebras C e D sobre o corpo k, sendo o produto tensorial $C \otimes D$ sobre k; as aplicações lineares coproduto e counidade dar-se-ão neste caso da seguinte forma:

$$\Delta_{C\otimes D} : C \otimes D \to (C \otimes D) \otimes (C \otimes D)$$
$$\Delta_{C\otimes D} = (id \otimes \tau \otimes id) \circ (\Delta_C \otimes \Delta_D)$$

e

$$\varepsilon_{C\otimes D} : C \otimes D \to k$$
$$\varepsilon_{C\otimes D} = \varepsilon_C \otimes \varepsilon_D = \varepsilon_C \varepsilon_D$$

respectivamente; assim a tripla $(C, \Delta_{C\otimes D}, \varepsilon_{C\otimes D})$ é uma coálgebra. Considere $(c \otimes d)$ um elemento pertencente a $C \otimes D$. Mostraremos que o coproduto é coassociativo e o diagrama da counidade é também comutativo. De fato, tem-se:

$$\begin{aligned}(id \otimes \Delta_{C\otimes D}) \circ \Delta_{C\otimes D}(c \otimes d) &= (id \otimes \Delta_{C\otimes D})((c' \otimes d') \otimes (c'' \otimes d'')) \\ &= ((c')' \otimes (d')') \otimes ((c')'' \otimes (d')'') \otimes (c'' \otimes d'') \\ &= (\Delta_{C\otimes D} \otimes id)(c' \otimes d') \otimes (c'' \otimes d'') \\ &= (\Delta_{C\otimes D} \otimes id) \circ \Delta_{C\otimes D}(c \otimes d)\end{aligned}$$

e

$$\begin{aligned}(id \otimes \varepsilon_{C\otimes D}) \circ \Delta_{C\otimes D}(c \otimes d) &= (id \otimes \varepsilon_{C\otimes D})((c' \otimes d') \otimes (c'' \otimes d'')) \\ &= c'\varepsilon_C(c'') \otimes d'\varepsilon_D(d'') \\ &= c \otimes d \\ &= (\varepsilon_C(c') \otimes \varepsilon_D(d')) \otimes (c'' \otimes d'') \\ &= (\varepsilon_{C\otimes D} \otimes id) \circ \Delta_{C\otimes D}(c \otimes d)\end{aligned}$$

Portanto, $(C, \Delta_{C\otimes D}, \varepsilon_{C\otimes D})$ é uma coálgebra. Consequentemente, $\Delta_{C\otimes D}(c \otimes d) = c' \otimes d' \otimes c'' \otimes d'' = (c \otimes d)' \otimes (c \otimes d)''$.

2.3 Biálgebras

Nas seções anteriores estudamos álgebra e coálgebra de forma independente, sem que houvessem quaisquer relações entre elas. Nesta seção, porém, vamos perscrutar uma estrutura algébrica que é dotada de ambas as estruturas concomitantemente — a biálgebra.

Proposição 2.3.1. *Seja H um espaço vetorial que possua uma estrutura de álgebra (H, μ, η) e uma de coálgebra (H, Δ, ε), simultaneamente. Portanto, as afirmações a seguir são equivalentes:*

i) As aplicações $\mu : H \otimes H \to H$ e $\eta : k \to H$ são morfismos de coálgebras.

ii) As aplicações $\Delta : H \to H \otimes H$ e $\varepsilon : H \to k$ são morfismos de álgebras.

Demonstração. O fato que μ um morfismo[2] de coálgebras, isto equivale dizer que há comutatividade dos diagramas:

$$\begin{array}{ccc} H \otimes H & \xrightarrow{\mu} & H \\ {\scriptstyle (id\otimes\tau\otimes id)(\Delta\otimes\Delta)}\downarrow & & \downarrow{\scriptstyle \Delta} \\ (H \otimes H) \otimes (H \otimes H) & \xrightarrow{\mu\otimes\mu} & H \otimes H \end{array} \qquad \begin{array}{ccc} H \otimes H & \xrightarrow{\varepsilon\otimes\varepsilon} & k \otimes k \\ {\scriptstyle \mu}\downarrow & & \downarrow{\scriptstyle id} \\ H & \xrightarrow{\varepsilon} & k \end{array}$$

e sabe-se que η é um morfismo de coálgebras, ou seja, existe comutatividade dos dois diagramas a seguir:

$$\begin{array}{ccc} k & \xrightarrow{\eta} & H \\ {\scriptstyle id}\downarrow & & \downarrow{\scriptstyle \Delta} \\ k \otimes k & \xrightarrow{\eta\otimes\eta} & H \otimes H \end{array} \qquad \begin{array}{ccc} k & \xrightarrow{\eta} & H \\ {\scriptstyle id}\downarrow & \swarrow{\scriptstyle \varepsilon} & \\ k & & \end{array}$$

o que conclui nossa demonstração. ■

Definição 2.3.1. *A estrutura $(H, \mu, \eta, \Delta, \varepsilon)$ sobre o corpo k é uma biálgebra se o espaço vetorial H sobre k for uma álgebra (H, μ, η), uma coálgebra (H, Δ, ε) e as condições equivalentes da Proposição 2.3.1 são satisfeitas com as seguintes relações de compatibilidades entre elas:*

$$\Delta(hg) = \Delta(h)\Delta(g), \quad \Delta(1) = 1 \otimes 1, \quad \varepsilon(hg) = \varepsilon(h)\varepsilon(g), \quad \varepsilon(1) = 1 \tag{2.17}$$

em que $h, g \in H$.

Observemos que as relações de compatibilidades são uma condição necessária e suficiente para que H seja uma biálgebra. Dada uma biálgebra H, pela proposição 2.3.1,

[2] Em teoria de categorias, os morfismos se referem aos mapeamentos de uma estrutura matemática à outra de forma que a estrutura é preservada, ou seja, morfismos são funções que preservam as estruturas [36].

tem-se:

$$\begin{aligned}\Delta(hg) &= \Delta(\mu(h\otimes g))\\ &= (\Delta\mu)(h\otimes g) = (\mu(\Delta\otimes\Delta))(h\otimes g)\\ &= \mu(\Delta(h)\otimes\Delta(g))\\ &= \Delta(h)\Delta(g)\end{aligned}$$

e

$$\begin{aligned}\varepsilon(hg) &= \varepsilon(\mu(h\otimes g))\\ &= (\varepsilon\mu)(h\otimes g) = (\mu(\varepsilon\otimes\varepsilon))(h\otimes g)\\ &= \mu(\varepsilon(h)\otimes\varepsilon(g))\\ &= \varepsilon(h)\varepsilon(g)\end{aligned}$$

In pari causa, temos

$$\begin{aligned}\Delta(1) &= \Delta(\eta(1))\\ &= (\Delta\eta)(1) = ((\eta\otimes\eta)\Delta)(1)\\ &= (\eta\otimes\eta)(1\otimes 1) = \eta(1)\otimes\eta(1)\\ &= 1\otimes 1\end{aligned}$$

e

$$\begin{aligned}\varepsilon(1) &= \varepsilon(\eta(1))\\ &= (\varepsilon\eta)(1)\\ &= \varepsilon(1)\\ &= 1.\end{aligned}$$

Uma aplicação linear $\varphi : H_1 \to H_2$ entre biálgebras H_1 e H_2 é um homomorfismo de biálgebras se for simultaneamente homomorfismo de álgebras e homomorfismo de coálgebras. Isto é: $\varphi\mu_{H_1} = \mu_{H_2}(\varphi\otimes\varphi)$, $\varphi\eta_{H_1} = \eta_{H_2}$, $\Delta_{H_2}\varphi = (\varphi\otimes\varphi)\Delta_{H_1}$ e $\varepsilon_{H_2}\varphi = \varepsilon_{H_1}$.

Exemplo 2.3.1. Seja G um grupo. Sabe-se que (kG, μ, η) define uma álgebra e $(kG, \Delta, \varepsilon)$ define uma coálgebra. Estas duas estruturas mostram-se compatíveis porque

$$\Delta(ab) = ab\otimes ab = (a\otimes a)(b\otimes b) = \Delta(a)\Delta(b)$$

e

$$\varepsilon(ab) = 1 = \varepsilon(a)\varepsilon(b)$$

Logo $(kG, \mu, \eta, \Delta, \varepsilon)$ é uma biálgebra. □

Um segundo exemplo a ser considerado é a biálgebra oposta. Considere a estrutura $H^{op} = (H, \mu^{op}, \eta, \Delta, \varepsilon)$ conhecida por biálgebra oposta, em que $x, y \in H$. Com efeito:

$$\begin{aligned} \Delta(xy) &= \Delta\mu^{op}(y \otimes x) = \mu^{op}(\Delta \otimes \Delta)(y \otimes x) \\ &= \mu^{op}(\Delta(y) \otimes \Delta(x)) = \mu(\Delta(x) \otimes \Delta(y)) \\ &= \Delta(x)\Delta(y) \end{aligned}$$

e

$$\begin{aligned} \varepsilon(xy) &= \varepsilon(\mu^{op}(y \otimes x)) = \mu(\varepsilon \otimes \varepsilon)(y \otimes x) \\ &= \mu^{op}(\varepsilon(y) \otimes \varepsilon(x)) \\ &= \varepsilon(x)\varepsilon(y). \end{aligned}$$

Existem também os casos de estruturas denominadas por cooposta $H^{cop} = (H, \mu, \eta, \Delta^{op}, \varepsilon)$ e oposta/cooposta $(H, \mu^{op}, \eta, \Delta^{op}, \varepsilon)$ que são biálgebras.

De posse das definições de álgebras, coálgebras e biálgebras passemos à definição de álgebra de Hopf.

2.4 Álgebras de Hopf

Definição 2.4.1. *Uma álgebra de Hopf $(H, \mu, \eta, \Delta, \varepsilon, S)$ é uma biálgebra com uma aplicação linear $S : H \to H$ que torna comutativo o seguinte diagrama:*

$$\begin{array}{ccccc} H \otimes H & \xleftarrow{\Delta} & H & \xrightarrow{\Delta} & H \otimes H \\ \downarrow{\scriptstyle id \otimes S} & & \downarrow{\scriptstyle \eta \circ \varepsilon} & & \downarrow{\scriptstyle S \otimes id} \\ H \otimes H & \xrightarrow{\mu} & H & \xleftarrow{\mu} & H \otimes H \end{array} \tag{2.18}$$

De forma similar, temos:

$$\mu \circ (id \otimes S) \circ \Delta = \eta \circ \varepsilon = \mu \circ (S \otimes id) \circ \Delta \tag{2.19}$$

A aplicação S é chamada antípoda de H.

O papel do antípoda S é como a de uma inversa. No entanto, não exigi-se que $S^2 = id$. Também nem supomos que a aplicação linear S possua uma inversa S^{-1}. Notemos que a notação de Sweedler nos diz que a relação (2.19), também conhecida por axioma da antípoda, pode ser reescrita como

$$\sum h' S(h'') = \varepsilon(h)1 = \sum S(h')h'', \tag{2.20}$$

em que $h \in H$ com $\Delta(h) = \sum h' \otimes h''$.

Diz-se que um homomorfismo de álgebras de Hopf é um homomorfismo de biálgebras φ entre duas álgebras de Hopf H_1 e H_2 sendo expressado pela comutatividade do diagrama

$$\begin{array}{ccc} H_1 & \xrightarrow{\varphi} & H_2 \\ {\scriptstyle S_1}\downarrow & & \downarrow{\scriptstyle S_2} \\ H_1 & \xrightarrow{\varphi} & H_2 \end{array}$$

ou $\varphi \circ S_1 = S_2 \circ \varphi$, em que S_1 e S_2 são aplicações antípodas de H_1 e H_2, respectivamente.

Um outra interpretação do axioma da antípoda dar-se-á através da álgebra de convolução; notaremos o produto de convolução por "$*$". Seja $(H, \mu, \eta, \Delta, \varepsilon, S)$ uma álgebra de Hopf. Diz-se que S é um endomorfismo de H se

$$S * id = id * S = \eta \circ \varepsilon \tag{2.21}$$

ou seja, S é o elemento inverso da aplicação id na álgebra de convolução. Esta definição também nos diz que a antípoda de uma álgebra de Hopf é única, de fato: suponha S_1 e S_2 sejam antípodas de H, então $S_1 = S_1 * (\eta \circ \varepsilon) = S_1 * (id * S_2) = (S_1 * id) * S_2 = (\eta \circ \varepsilon) * S_2 = S_2$.

Proposição 2.4.1. *Seja H uma álgebra de Hopf e S sua antípoda, com $g, h \in H$. Então S goza das seguintes propriedades:*

i) $S(gh) = S(h)S(g)$;

ii) $S(1) = 1$;

iii) $(S \otimes S) \circ \Delta = \tau \circ \Delta \circ S$;

iv) $\varepsilon \circ S = \varepsilon$.

Demonstração. *i)* Usando a relação (2.19) e o fato de que Δ e ε serem morfimos de álgebras, tem-se:

$$\begin{aligned} S(h)S(g) &= \sum S(h'\varepsilon(h''))S(g'\varepsilon(g'')) \\ &= \sum S(h')S(g')\varepsilon(g'')\varepsilon(h'') \\ &= \sum S(h')S(g')\varepsilon(g''h'') \\ &= \sum S(h')S(g')\eta(\varepsilon(g''h'')) \\ &= \sum S(h')S(g')(g''h'')'S((g''h'')'') \\ &= \sum S(h')S(g')g''h''S(g'''h''') \\ &= \sum S(h')\eta(\varepsilon(g'))h''S(g''h''') \\ &= \sum S(h')h''\varepsilon(g')S(g''h''') \\ &= \sum \eta(\varepsilon(h'))\varepsilon(g')S(g''h'') \\ &= \sum \varepsilon(h')\varepsilon(g')S(g''h'') \\ &= S\left(\left(\sum \varepsilon(g')g''\right)\left(\sum \varepsilon(h')h''\right)\right) \\ &= S(gh). \end{aligned}$$

ii)

$$S(1) = S(1)1 = \mu(S \otimes id)\Delta(1) = \eta(\varepsilon(1)) = \varepsilon(1)1 = 1.$$

iii) Para esta demonstração, utilizamos a relação *ii*) e $\Delta(1) = 1 \otimes 1$. Então:

$$\begin{aligned}
\tau(S \otimes S)\Delta(h) &= \sum S(h^{(2)}) \otimes S(h^{(1)}) \\
&= \sum S(h^{(2)}\varepsilon(h^{(3)})) \otimes S(h^{(1)}) \\
&= \sum (S(h^{(2)}) \otimes S(h^{(1)}))(\varepsilon(h^{(1)})1 \otimes 1) \\
&= \sum (S(h^{(2)}) \otimes S(h^{(1)}))(\Delta(h^{(3)}S(h^{(4)}))) \\
&= \sum (S(h^{(2)}) \otimes S(h^{(1)}))((h^{(3)}S(h^{(4)}))^{(1)} \otimes (h^{(3)}S(h^{(4)}))^{(2)}) \\
&= \sum (S(h^{(2)}) \otimes S(h^{(1)}))(h^{(3)(1)} \otimes h^{(3)(2)})(S(h^{(4)(1)}) \otimes S(h^{(4)(2)}) \\
&= \sum (S(h^{(2)}) \otimes S(h^{(1)}))(h^{(3)} \otimes h^{(4)})\Delta(S(h^{(5)})) \\
&= \sum (S(h^{(2)})h^{(3)} \otimes S(h^{(1)})h^{(4)})(\Delta(S(h^{(4)}))) \\
&= \sum (\varepsilon(h^{(2)})1 \otimes S(h^{(1)})h^{(3)})(\Delta(S(h^{(4)}))) \\
&= \sum (1 \otimes S(h^{(1)})h^{(2)})(\Delta(S(h^{(3)}))) \\
&= \sum (1 \otimes \varepsilon(h^{(1)})1)(\Delta(S(h^{(2)}))) \\
&= \sum \Delta(\varepsilon(h^{(1)})S(h^{(2)})) \\
&= \Delta(S\left(\sum \varepsilon(h^{(1)}h^{(2)})\right) \\
&= \Delta(S(h)).
\end{aligned}$$

iv) Por último, temos:

$$\begin{aligned}
\varepsilon(S(h)) &= \varepsilon\left(S\left(\sum \varepsilon(h')\right)h''\right) \\
&= \sum \varepsilon(h'S(h'')) \\
&= \varepsilon(\varepsilon(h)1) \\
&= \varepsilon(h)\varepsilon(1) \\
&= \varepsilon(h).
\end{aligned}$$

■

De um ponto de vista mais rigoroso, dizemos que as propriedades *i*) e *ii*) definem S como um anti-homomorfismo de álgebras, enquanto as propriedade *iii*) e *iv*) definem S como anti-homomorfismo de coálgebras. Em outras palavras, $S : H \to H^{op}$ é um homomorfismo de álgebras e $S : H \to H^{cop}$ é um homomorfismo de coálgebras. Quando H for uma álgebra de Hopf comutativa ou cocomutativa, então $S^2 = S \circ S = id$.

Exemplo 2.4.1. Considere $F(G)$ a biálgebra das funções de um grupo finito G em k. A antípoda é definida por:

$$\begin{aligned} S : F(G) &\rightarrow F(G) \\ f &\mapsto s(f), \end{aligned}$$

em que $S(f)(x) = f(x^{-1})$. Então, a estrutura $(F(G), \mu, \eta, \Delta, \varepsilon, S)$ é uma álgebra de Hopf. De fato, a S obedece a relação (2.19), i.e,

$$\begin{aligned} \mu(id \otimes S)\Delta(f)(x) &= \sum \mu(f' \otimes S(f''))(x) \\ &= \sum f'(x) \cdot f''(x^{-1}) \\ &= \sum (f' \otimes f'')(x, x^{-1}) \\ &= \Delta(f)(x, x^{-1}) \\ &= \varepsilon(f)(x) \\ &= (\eta \circ \varepsilon)(f(x)). \end{aligned}$$

□

As álgebras de Hopf foram introduzidas pelo matemático Heinz Hopf em 1941 [25]; além da computação quântica, suas aplicações, por exemplo, abrangem as teorias quânticas deformadas [38, 39]. No que diz respeito à sua conexão com a computação quântica, iremos apresentar alguns aspectos nos próximos capítulos.

3 Computação Quântica

Iniciaremos este capítulo apresentando alguns conceitos básicos da computação e informação quânticas, são eles: os q-bits, as portas lógicas quânticas, o emaranhamento e alguns tópicos especiais sobre aplicações [3, 40]. No que tange à implementação da computação quântica, introduziremos uma proposta denominada computação quântica topológica. Em seguida, mostraremos algumas vertentes desta proposta.

3.1 Bits quânticos

De forma análoga aos computadores clássicos, construídos a partir de circuitos elétricos contendo fios e portas lógicas, um computador quântico é constituído de um circuito quântico[1]contendo fios e de portas lógicas quânticas. Dentro da computação e da informação clássicas existe um conceito fundamental: bit[2]. O bit pode assumir valores lógicos — que são 0 ou 1. Sobre um conceito análogo a computação quântica possui o bit quântico ou *qubit* (q-bit[3]). Note que os q-bits, assim como os bits clássicos, são implementados como objetos físicos reais (como exemplo, o experimento de Stern - Gerlach). Entretanto, os q-bits são descritos como objetos matemáticos abstratos, pois assim a teoria geral da computação quântica não depende de nenhum sistema específico para sua implementação. A diferença entre bits e q-bits é que os q-bits podem estar em estados quânticos diferentes de $|0\rangle$ ou $|1\rangle$.

Definição 3.1.1. *Um q-bit é um estado quântico pertencente a um espaço de Hilbert* $\mathbb{H}$ *de duas dimensões, ou seja:*

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle\,, \tag{3.1}$$

em que α *e* $\beta \in \mathbb{C}$ *e* $\mid \alpha \mid^2 + \mid \beta \mid^2 = 1$.

Os vetores $|0\rangle$ e $|1\rangle$ são chamados de estados da base computacional e formam uma base ortonormal nesse espaço. Uma outra propriedade que um q-bit goza é a superposição, também conhecida como um postulado da mecânica quântica. Um bit clássico pode ser comparado a uma moeda: cara ou coroa. Em contraste, um q-bit pode existir em um estado contínuo entre $|0\rangle$ e $|1\rangle$ — até que ele seja observado. Quando um q-bit é medido, o resultado será sempre 0 ou 1. Por exemplo:

$$\frac{1}{\sqrt{2}}\,|0\rangle + \frac{1}{\sqrt{2}}\,|1\rangle\,, \tag{3.2}$$

[1] Neste trabalho não trataremos sobre esse tema.

[2] Binary digit.

[3] Termo criado pelos físicos Alfredo M. Ozorio de Almeira (CBPF) e Luiz Davidovich (UFRJ), apropriado à lingua portuguesa; essa nomenclatura também é utilizada por Amir O. Caldeira (UNICAMP).

quando medido, dará resultado "0" em 50% das vezes e o valor "1" em 50% das vezes.

É possível obter uma visualização geométrica dos estados de um q-bit. Considere a seguinte equação:

$$\begin{aligned} |\psi\rangle &= \alpha\,|0\rangle + \beta\,|1\rangle \\ &= |\alpha|e^{i\gamma}\,|0\rangle + e^{i\eta}|\beta|\,|1\rangle\,, \end{aligned} \tag{3.3}$$

em que definimos $|\alpha| = cos(\theta/2)$ e $|\beta| = sen(\theta/2)$, o que mantém a condição de normalização; assim,

$$|\psi\rangle = e^{i\gamma}\left(cos(\frac{\theta}{2})\,|0\rangle + e^{i(\eta-\gamma)}sen(\frac{\theta}{2})\,|1\rangle\right),$$

em que $e^{i\gamma}$ é um fator de fase global que pode ser desconsiderado por não alterar a amplitude de probabilidade. Fazendo $\eta - \gamma = \varphi$, encontramos que

$$|\psi\rangle = cos(\theta/2)\,|0\rangle + e^{i\varphi}sen(\theta/2)\,|1\rangle\,. \tag{3.4}$$

Podemos usar os números θ e φ para definir um ponto sobre a superfície de uma esfera de raio unitário. Nessa esfera (Figura 1) conhecida como esfera de Bloch[4], cada ponto da superfície representa então um possível q-bit. De fato, da relação (3.4) segue que se $\theta = 0$ tem-se $|\psi\rangle = |0\rangle$, se $\theta = \pi$ tem-se $|\psi\rangle = |1\rangle$ e se $\theta = \pi/2$, por exemplo, temos

$$|\psi\rangle = \frac{1}{\sqrt{2}}\,|0\rangle + \frac{1}{\sqrt{2}}\,|1\rangle\,e^{i\varphi}. \tag{3.5}$$

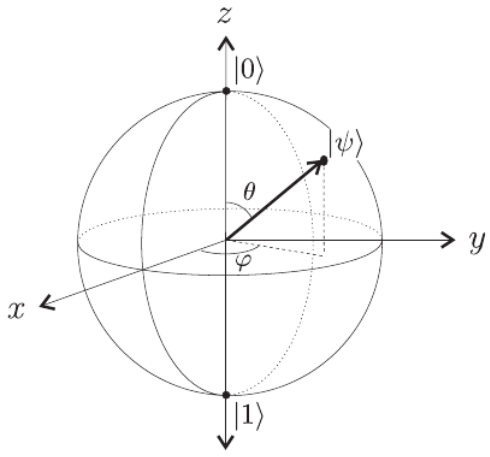


Figura 1: Representação do q-bit $|\psi\rangle$ na esfera de Bloch.

Devemos manter em mente que essa representação geométrica é limitada, pois não existe uma generalização simples da esfera de Bloch para muitos q-bits [3]. Pelos

[4] Figura retirada da referência [3]

postulados da Teoria Quântica, para o sistema constituído por dois q-bits, por exemplo, o estado é formado pelo produto tensorial dos estados de dois q-bits, ou seja,

$$\begin{aligned} |\psi\rangle &= (\alpha_1 |0\rangle + \beta_1 |1\rangle) \otimes (\alpha_2 |0\rangle + \beta_2 |1\rangle) \\ &= \alpha_1\alpha_2 |00\rangle + \alpha_1\beta_2 |01\rangle + \beta_1\alpha_2 |10\rangle + \beta_1\beta_2 |11\rangle \\ &= \alpha_{00} |00\rangle + \alpha_{01} |01\rangle + \alpha_{10} |10\rangle + \alpha_{11} |11\rangle , \end{aligned} \tag{3.6}$$

com $|\alpha_{00}|^2 + |\alpha_{01}|^2 + |\alpha_{10}|^2 + |\alpha_{11}|^2 = 1$; de modo análogo são construídos os 3 q-bits, 4 q-bits etc.

3.2 Portas Lógicas Quânticas

Como dito anteriormente, os computadores quânticos também possuem portas lógicas. Essas portas lógicas quânticas manipulam a informação, convertendo-a de uma forma para outra. A seguir, mostraremos alguns exemplos de portas lógicas quânticas.

i) Porta NÃO

A porta NÃO[5], no caso clássico, opera trocando os valores binários um pelo outro, i.e., 0→1 e 1→0. O análogo quântico da porta NÃO deverá ter ação sobre os estados $|0\rangle$ e $|1\rangle$. Suponha uma matriz X para representar a porta quântica NÃO da seguinte forma:

$$X \equiv \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \tag{3.7}$$

A representação matricial do q-bit (3.1) será:

$$\begin{aligned} |\psi\rangle &= \alpha |0\rangle + \beta |1\rangle \\ &= \alpha \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \beta \begin{pmatrix} 0 \\ 1 \end{pmatrix} \\ &= \begin{pmatrix} \alpha \\ \beta \end{pmatrix} . \end{aligned} \tag{3.8}$$

Aplicando a porta NÃO ao q-bit (3.8):

$$\begin{aligned} X |\psi\rangle &= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \\ &= \begin{pmatrix} \beta \\ \alpha \end{pmatrix} \\ &= \beta |0\rangle + \alpha |1\rangle , \end{aligned} \tag{3.9}$$

[5] Do inglês "NOT". Também conhecida por porta negação.

isto é, permutam-se as amplitudes de probabilidades das bases $|0\rangle$ e $|1\rangle$; note que as portas lógicas quânticas sobre um q-bit podem ser descritas por matrizes 2 x 2. A condição necessária para que uma matriz, de dimensão 2, seja porta é que ela seja unitária: $U^\dagger U = I$. Verifica-se que $X^\dagger X = I$.

ii) Porta $\bar{Z}$

A porta lógica $\bar{Z}$ possui a seguinte característica:

$$\bar{Z}\,|0\rangle = |0\rangle\,; \quad \bar{Z}\,|1\rangle = -\,|1\rangle\,, \tag{3.10}$$

ou seja, não altera o estado $|0\rangle$, e muda o sinal de $|1\rangle$. Sua representação matricial é:

$$\bar{Z} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{3.11}$$

Quando aplicamos a um q-bit (3.8), teremos:

$$\begin{aligned} \bar{Z}\,|\psi\rangle &= \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \\ &= \begin{pmatrix} \alpha \\ -\beta \end{pmatrix} \\ &= \alpha\,|0\rangle - \beta\,|1\rangle\,. \end{aligned} \tag{3.12}$$

Note que ao compararmos com a mecânica quântica, as matrizes X e $\bar{Z}$ são as conhecidas matrizes de Pauli σ_x e σ_z, respectivamente.

iii) Porta Hadamard - H_d

Outro exemplo importante de porta lógica quântica é a porta Hadamard[6]. Essa porta age da seguinte forma:

$$H_d\,|0\rangle = \frac{1}{\sqrt{2}}[|0\rangle + |1\rangle]$$

e

$$H_d\,|1\rangle = \frac{1}{\sqrt{2}}[|0\rangle - |1\rangle], \tag{3.13}$$

i.e. gera superposições. Logo, sua representação matricial é:

$$H_d = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}. \tag{3.14}$$

Observa-se que:

[6] Em homenagem ao matemático Jacques Hadamard (1865 -1963)

$$\begin{aligned} {H_d}^2 |0\rangle &= H_d \frac{1}{\sqrt{2}} [|0\rangle + |1\rangle] \\ &= \frac{1}{\sqrt{2}} [H_d |0\rangle + H_d |1\rangle] \\ &= \frac{1}{\sqrt{2}} \{ [\frac{1}{\sqrt{2}} (|0\rangle + |1\rangle)] + [\frac{1}{\sqrt{2}} (|0\rangle - |1\rangle)] \} \\ &= |0\rangle . \end{aligned} \tag{3.15}$$

e

$$\begin{aligned} {H_d}^2 |1\rangle &= H_d \frac{1}{\sqrt{2}} [|0\rangle - |1\rangle] \\ &= \frac{1}{\sqrt{2}} [H_d |0\rangle - H_d |1\rangle] \\ &= \frac{1}{\sqrt{2}} \{ [\frac{1}{\sqrt{2}} (|0\rangle + |1\rangle)] - [\frac{1}{\sqrt{2}} (|0\rangle - |1\rangle)] \} \\ &= |1\rangle . \end{aligned} \tag{3.16}$$

iv) Porta NÃO Controlado - CNOT

Para muitos q-bits é interessante utilizar a porta lógica quântica NÃO controlado ou porta CNOT[7]. Um exemplo é o caso de dois q-bits de entrada, denominados por q-bit de controle e q-bit alvo. A ação dessa porta acontece então da seguinte forma: quando o q-bit de controle for colocado no estado 0, nada acontece com q-bit alvo. Caso o q-bit de controle seja colocado em 1, o q-bit alvo troca de estado. Em outras palavras, dada a representação matricial de dois q-bits:

$$|00\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} ; |10\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} ; |01\rangle = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} ; |11\rangle = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} , \tag{3.17}$$

aplicando-se a porta CNOT aos estados, obtém-se:

$$\begin{aligned} CNOT\,|00\rangle &= |00\rangle , \\ CNOT\,|01\rangle &= |01\rangle , \\ CNOT\,|10\rangle &= |11\rangle , \\ CNOT\,|11\rangle &= |10\rangle , \end{aligned} \tag{3.18}$$

[7] Do inglês *Controlled-NOT*

Portanto, a representação matricial da porta CNOT é dada por

$$CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}. \tag{3.19}$$

3.3 Estados Quânticos Emaranhados

Os estados quânticos emaranhados são o principal recurso para o processamento da informação quântica. O emaranhamento quântico é a característica que possibilita a criação de pares de partículas que revelam correlações surpreendentemente fortes entre suas propriedades. Matematicamente, um dos critérios para caracterizar o estado puro emaranhado de um sistema físico é o fato que ele não pode ser escrito como o produto tensorial de estados que caracterizariam cada subsistema que o compõe; de um modo geral, um estado $|\psi\rangle$ é dito ser emaranhado, se e somente se, não existem estados $|\psi_1\rangle$ e $|\psi_2\rangle$ tais que $|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle$.

Para entender como são essas correlações, apresentaremos um exemplo comum na literatura: a polarização de fótons gêmeos [41].

Considere um sistema de dois fótons que se propagam na mesma direção z em sentidos opostos, na representação em que o vetor de estado de polarização na direção θ é $\begin{pmatrix} \cos\theta \\ sen\theta \end{pmatrix}$, tem-se a base formada pelos seguintes vetores de estado:

$$|0\rangle \equiv |\rightarrow\rangle = |\theta = 0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \tag{3.20}$$

$$|1\rangle \equiv |\uparrow\rangle = \left|\theta = \frac{\pi}{2}\right\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \tag{3.21}$$

os quais representam fótons linearmente polarizados nas direções x e y, respectivamente. Como nossa intenção é descrever um sistema de dois fótons, usaremos vetores coluna de quatro componentes, pois teremos de representar amplitudes de probabilidade para que, com analisadores orientados nas direções x e y, cada um dos dois fótons possa ser encontrado com cada uma dessas polarizações (quatro possibilidades).

Utilizando o produto tensorial dos vetores da base (3.20) e (3.21), teremos:

$$|0\rangle_1 |0\rangle_2 = |00\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}_1 \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix}_2 = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \tag{3.22}$$

em que os subscritos 1 e 2 significam, respectivamente, fóton 1 e fóton 2. A equação (3.22) descreve a situação do fóton 1 linearmente polarizado na direção x e o fóton 2 também. Da mesma forma, obtivemos os demais. Assim,

$$|0\rangle_1 |1\rangle_2 = |01\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}_1 \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix}_2 = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} \tag{3.23}$$

$$|1\rangle_1 |0\rangle_2 = |10\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}_1 \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix}_2 = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} \tag{3.24}$$

$$|1\rangle_1 |1\rangle_2 = |11\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}_1 \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix}_2 = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} \tag{3.25}$$

O vetor de estado geral de polarização para dois fótons é:

$$|\psi\rangle = \alpha_{00} |0\rangle_1 |0\rangle_2 + \alpha_{01} |0\rangle_1 |1\rangle_2 + \alpha_{10} |1\rangle_1 |0\rangle_2 + \alpha_{11} |1\rangle_1 |1\rangle_2 = \begin{pmatrix} \alpha_{00} \\ \alpha_{01} \\ \alpha_{10} \\ \alpha_{11} \end{pmatrix}, \tag{3.26}$$

em que, por exemplo, α_{01} é a amplitude de probabilidade de achar o fóton 1 linearmente polarizado na direção x e o fóton 2 na direção y.

Consideremos o seguinte estado normalizado:

$$|\psi\rangle = \frac{1}{\sqrt{2}}[|0\rangle_1 |0\rangle_2 + |1\rangle_1 |1\rangle_2] = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}. \tag{3.27}$$

Esse estado (3.27) chamamos de emaranhado, pois não pode ser decomposto num produto de um estado do fóton 1 por um estado do fóton 2. Caso o estado não esteja emaranhado, ele é dito ser separável. Pela interpretação física da equação (3.26), esse é um estado em que há probabilidades 1/2 de achar ambos os fótons polarizados na

direção x e achar ambos polarizados na direção y, i.e., as polarizações dos dois fótons estão correlacionadas — ambas têm a mesma direção(x ou y). Assim, se ao utilizar um analisador for verificado que o fóton 1 tem polarização y, com certeza, o fóton 2 também terá a mesma polarização y. Agora, considere dois fótons em direções opostas descritos pela equação (3.27) e com os dois analisadores de polarização distantes um do outro. Se uma medida do fóton 1 indicar que está polarizado na direção x, sem uma ação sobre o sistema poder-se-á afirmar que o fóton 2 também está polarizado na direção x; sabe-se, no entanto, que o mesmo é verdadeiro para qualquer outra direção x' que forme um ângulo arbitrário φ com x, ou seja, o fóton 2 teria assim também uma polarização bem definida nesta direção x' (cf. apêndice B). Porém, polarizações em direções diferentes são observáveis incompatíveis, ou seja, um fóton não pode ter simultaneamente valores bem definidos para elas. Essa manifestação não local foi denominada por Einstein, Podolsky e Rosen (EPR) de "ação fantasmagórica à distância", concluindo eles que a teoria quântica seria incompleta [4].

Sabemos que dado um estado quântico geral, a pergunta se há ou não emaranhamento está, em geral, longe de ter uma resposta trivial. Sendo assim, a procura por métodos para tentar resolver essa questão é um dos objetivos do estudo do emaranhamento. Esses métodos são chamados de critérios de emaranhamento. Há uma vasta classe de critérios na literatura [43, 44], a exemplos, a decomposição de Schmidt [45], critério de Peres-Horodecki [46, 47], de Simon [48] e entre outros. Na nossa linha algébrica, existe também um critério desenvolvido por Trindade, Vianna e Fernandes [49].

Os exemplos mais conhecidos e aplicados são os estados de Bell[8] ou pares EPR [4,31]:

$$\left|\Phi^{\pm}\right\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle) \tag{3.28}$$

$$\left|\Psi^{\pm}\right\rangle = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle) \tag{3.29}$$

Uma aplicação dos pares de Bell bastante conhecida é a codificação superdensa [3]. A codificação superdensa envolve dois parceiros, conhecidos como Alice e Bob, que se encontram separados por uma grande distância um do outro. O objetivo de Alice é enviar dois bits clássicos para Bob, mas deve fazer isso usando um único q-bit. Alice e Bob inicialmente compartilham um par de q-bits no estado emaranhado:

$$|\psi\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}. \tag{3.30}$$

Alice possui um q-bit, e o segundo q-bit se encontra com Bob. Essa situação inicial é mostrada na figura abaixo:

[8] Também são conhecidos por serem estados maximamente emaranhados, ou seja, qualquer outro estado de dois q-bits pode ser obtido a partir destes por operações que não criam emaranhamento [50].

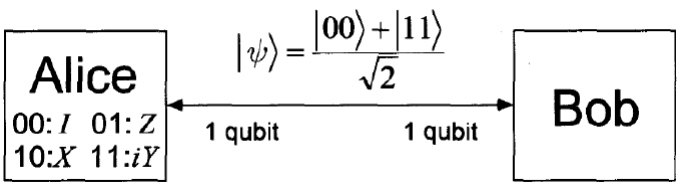


Figura 2: Arranjo inicial para a codificação superdensa.

Ao enviar o seu q-bit para Bob é possível para Alice comunicar dois bits de informação clássica. Por convenção [51], o procedimento adotado por Alice é o seguinte:

- enviar a sequência **00**, não deve fazer nada com o seu q-bit.
- enviar a sequência **01**, deve aplicar o inversor de fase $\bar{Z}$ ao seu q-bit.
- enviar a sequência **10**, deve aplicar uma porta NÃO, ou X, ao seu q-bit.
- enviar a sequência **11**, deve aplicar a porta iY ao seu q-bit.

Os estados resultantes são:

$$00 : |\psi\rangle \rightsquigarrow \frac{|00\rangle + |11\rangle}{\sqrt{2}} \tag{3.31}$$

$$01 : |\psi\rangle \rightsquigarrow \frac{|00\rangle - |11\rangle}{\sqrt{2}} \tag{3.32}$$

$$10 : |\psi\rangle \rightsquigarrow \frac{|10\rangle + |01\rangle}{\sqrt{2}} \tag{3.33}$$

$$11 : |\psi\rangle \rightsquigarrow \frac{|01\rangle - |10\rangle}{\sqrt{2}} \tag{3.34}$$

Observe que esses quatros estados são os pares EPR. Dessa forma, se Alice enviar o seu q-bit para Bob, uma vez de posse dos dois q-bits, ele pode realizar uma medida na base de Bell e determinar qual dentre as quatro sequências Alice enviou. Portanto, Alice enviou dois bits de informação clássica para Bob, enviando apenas um q-bit de informação quântica. Os dois q-bits estão envolvidos no protocolo, mas Alice nunca precisa interagir com o segundo [3].

3.4 Computação Quântica Topológica

Os computadores quânticos têm como promessa superar as habilidades de computadores clássicos. Por exemplo, seria a possibilidade de resolver em tempo menor a fatoração

em primos de números naturais [3]. A redução do tempo de resolução deste problema possibilitaria a quebra da maioria dos sistemas de criptografia usados atualmente; contudo, também possibilitaria a implementação de protocolos de criptografia quântica que têm como objetivo proteger mensagens em canais de comunicação [3]. Porém, na computação quântica os estados quânticos são frágeis, e as mais fracas pertubações do ambiente podem danificá-los [52]. Uma proposta de computação quântica tolerante à falhas é a computação quântica topológica, que utiliza as quase partículas bidimensionais chamadas de *anyons* e seus cálculos são realizados por meio de cordas entrançadas [9, 19, 53]. Essa proposta é particularmente interessante, pois as propriedades topológicas não se alteram quando sofrem pequenas pertubações, o que de certa forma acaba fornecendo uma resistência a erros causados por pertubações do ambiente externo.

3.4.1 *Anyons*

Sabemos que do ponto de vista da mecânica clássica se permutarmos n partículas idênticas, no espaço tridimensional, o sistema físico permanecerá inalterado, todavia, quando essa análise é feita pela mecânica quântica o estado do sistema pode mudar, adquirindo uma fase [54, 55]. Assim, o espaço de Hilbert do sistema deve "carregar" uma representação unitária U do grupo de permutações Γ_n.

Considere o caso de duas partículas, com $x = (\mathbf{r_1}, \mathbf{r_2})$ denotando as variáveis associadas as duas partículas (coordenadas e *spin*). No espaço de Hilbert, os estados correspondem a *rayons* — um mesmo estado é representado por $\psi(x)$ e $e^{i\theta}\psi(x)$, em que θ é uma fase arbitrária. Sabemos que em mecânica quântica as simetrias do sistema têm como consequência que as funções de onda se transformam de acordo com uma representação unitária do grupo. Então, sua função de onda no caso de partículas idênticas se transforma sob transposições[9]. Seja um operador $U(P)$ que representa uma permutação P, e para esta representação a "base" seja formada pelo conjunto $\{U(\gamma_i)\}$ que satisfaz as condições:

$$U(\gamma_i)U(\gamma_{i+1})U(\gamma_i) = U(\gamma_{i+1})U(\gamma_i)U(\gamma_{i+1}); \tag{3.35}$$

$$U(\gamma_i)U(\gamma_j) = U(\gamma_j)U(\gamma_i) \quad |i-j| \geq 2; \tag{3.36}$$

$$U(\gamma_i)U(\gamma_i) = id. \tag{3.37}$$

Entretanto, se ψ pertencer a um espaço de representação complexo unidimensional, esta representação deve ser unidimensional, e os fatores de fase aparecem: $\psi(\gamma_j x) = U(\gamma_j)\psi(x) = e^{i\theta_j}\psi(x)$.

[9] Toda permutação pode ser escrita como produto de transposições γ_j. As transposições geram assim o grupo simétrico; então podemos usar o conjunto de transposições como "base" para Γ_n.

A equivalência entre todas as fases é imposta através da relação (3.35), donde $U(\gamma_j)\psi(x) = e^{i\theta}\psi(x)$ e com o mesmo θ para todo γ_j. Da mesma forma a relação (3.36) diz que

$$U^2(\gamma_j)\psi(x) = U(\gamma_j^2)\psi(x) = e^{i2\theta}\psi(x) = \psi(x),$$

o que resulta $e^{i\theta} = \pm 1$. Então, quando permutamos duas partículas idênticas, a função de onda pode permanecer inalterada ou não. Quando a função de onda é invariante, essas partículas são chamadas de bósons[10], uma vez que obedecem a estatística de Bose. Caso contrário, as partículas são chamadas de férmions[11] e obedecem a estatística de Fermi.

Agora, consideremos o caso de duas partículas idênticas em um espaço bidimensional.

Definição 3.4.1. *Sejam* $\mathbf{r_1}$ *e* $\mathbf{r_2}$ *coordenadas de duas partículas idênticas, em duas dimensões. Após as permutações, infere-se que:*

$$\psi(\mathbf{r_1}, \mathbf{r_2}) = e^{i\theta}\psi(\mathbf{r_2}, \mathbf{r_1}), \tag{3.38}$$

em que $\theta = 0, \pi$ *e as partículas são chamadas de bósons e férmions, respectivamente; para outros valores de* θ *são chamadas anyons. Partículas bidimensionais, que não são bósons nem férmions, são também conhecidas por quase partículas.*

Como já citado, os *anyons* existem nesses espaços de duas dimensões. Se as partículas indistinguíveis estiverem em um plano, num espaço tridimensional, existe uma propriedade topológica que diz que todo caminho fechado neste espaço pode ser suavemente contraído a um ponto, porém, se o espaço for bidimensional não existe essa propriedade *a priori* e θ pode assumir qualquer valor [56–58]. Ademais, a evolução do sistema no espaço bidimensional é dada pelas representações do chamado grupo de tranças, em vez das representações do grupo de permutações, como no espaço tridimensional.

Apesar da computação quântica topológica ainda ser uma área em desenvolvimento inicial, alguns experimentos já foram feitos com o objetivo de comprovar a existência dos *anyons* [9, 56, 59]. Por exemplo, um gás bidimensional de elétrons pode existir na interface de duas placas semicondutoras de arseneto de gálio: o movimento dos elétrons se dá de forma livre, mas esses elétrons são impedidos de se mover na direção ortogonal à camada que os tiraria do plano. Nesse processo os elétrons estão submergidos a um campo magnético suficientemente forte e em baixas temperaturas; com isso, o gás bidimensional de elétrons atinge um estado emaranhado que é separado de todos os estados excitados por um intervalo de energia diferente de zero [56]. Camino et al. [59] sugeriram que as quase partículas do efeito Hall quântico fracionário são *anyons*. Porém, tal existência ainda não foi verificada [9].

[10] A representação $U(P) = 1$ é dita totalmente simétrica.
[11] A representação $U(P) = -1$ é dita totalmente antissimétrica.

Os percursos que os *anyons* seguem são no sentidos horário e anti-horário. Os dois sentidos são topologicamente distintos, pois não é possível deformar continuamente um percurso horário em um anti-horário sem cruzar trajetos e as partículas envolvidas colidirem. Há dois tipos de *anyons*: abelianos e não abelianos [9, 56]. Para a computação quântica topológica acredita-se que os *anyons* deverão ser do tipo não abelianos, pois para *anyons* desse tipo, o fator que modifica a função de onda é uma matriz de números, e o resultado da multiplicação de matrizes depende da ordem em que elas são colocadas.

3.4.2 Grupo de tranças, equação de Yang-Baxter e portas lógicas

Como já mencionado, na computação quântica topológica o computador realiza seus cálculos seguindo operações de cordas trançadas, o que na verdade são linhas de universo[12] [19, 20]. O movimento dos *anyons* pode ser representado pela figura[13]:

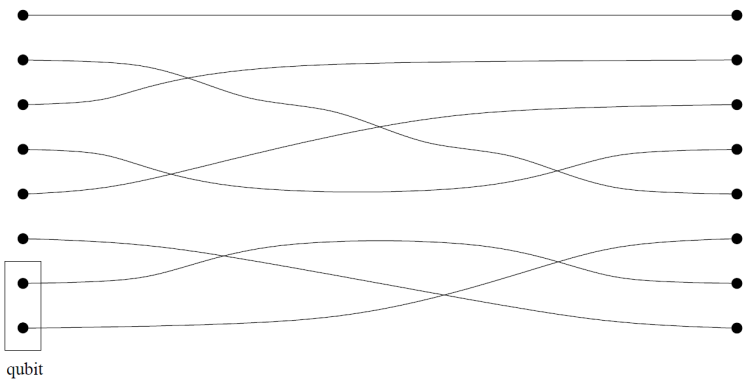


Figura 3: Movimento de anyons no espaço-tempo.

Observe que dados dois planos $\mathbb{R}^2$, imersos no espaço tridimensional $\mathbb{R}^3$ e paralelos um ao outro, basta se tomar três pontos distintos de um deles e ligá-los com fios a três pontos distintos do outro plano para se construir uma trança [54]. A descrição dos *anyons* é dada pelas representações do grupo de tranças[14], que é homomórfico ao grupo simétrico. Entretanto, o grupo de tranças se mostra mais rico, pois considera a ordem em que ocorrem as trocas dos elementos. Existem várias definições para o grupo de tranças, mas para interesse da computação quântica topológica, é utilizada a seguinte definição [11]:

Definição 3.4.2. *Diz-se que B_n é um grupo de tranças quando seu conjunto de $n-1$ geradores $\sigma_1, \sigma_2, \ldots, \sigma_{n-1}$ obedece as relações:*

$$\sigma_i \sigma_j \quad = \quad \sigma_j \sigma_i, \tag{3.39}$$

[12] Representações do movimento de partículas no espaço-tempo; neste contexto se diz que o comprimento dessas cordas representa o movimento da partícula ao longo do tempo, e sua espessura corresponde a suas dimensões físicas [56].

[13] Todas as figuras desta subseção foram retiradas das referências [15, 57, 58].

[14] Do inglês *Braid Groups*.

para todo $i, j = 1, 2, \ldots, n-1$ *com* $|i-j| \geq 2$, *e*

$$\sigma_i \sigma_{i+1} \sigma_i \quad = \quad \sigma_{i+1} \sigma_i \sigma_{i+1}, \tag{3.40}$$

em que $i = 1, 2, \ldots, n-2$ *e* n *é um número natural.*

A relação (3.39) significa que permutações de pares disjuntos de partículas comutam. O inverso é obtido trocando a ordem dos trançamentos, sendo definido por:

$$\sigma_i {\sigma_i}^{-1} = {\sigma_i}^{-1} \sigma_i = I \tag{3.41}$$

em que $I \in B_n$ é o elemento unitário. Os elementos $b \in B_n$, i.e. tranças distintas, podem ser expressos de uma forma geral:

$$b = {\sigma_i}^{m_i} {\sigma_j}^{m_j} {\sigma_k}^{m_k} \ldots \in B_n \tag{3.42}$$

em que $i, j, k, \ldots = 1, \ldots, n-1$ e $m_i, m_j, m_k, \ldots \in \mathbb{Z}$, ou seja, qualquer trança pode ser escrita por um produto de potências de geradores. Caso, além da relação (3.39), o grupo possua a condição:

$${\sigma_i}^m = I \tag{3.43}$$

em que $m \geq 3$ e $m \in \mathbb{Z}$, o grupo de trança torna-se finito e o chamamos de grupo de tranças truncado, sendo denotado por $B_{n,m}$.

Na figura 4 são mostrados os $n-1$ geradores de um grupo de tranças B_n. Por convenção histórica, as cordas devem ser consideradas como partindo do topo para a parte inferior; elas são ilustradas partindo de planos, de tal modo que a dimensão adicional, perpendicular ao desenho, permite que as cordas passem por detrás umas das outras [54]. É claro que cada trança pode ser interpretada também como uma aplicação $\mathbb{R}^2 \to \mathbb{R}^2$, levando pontos distintos de um plano em pontos distintos de outro plano [11, 54].

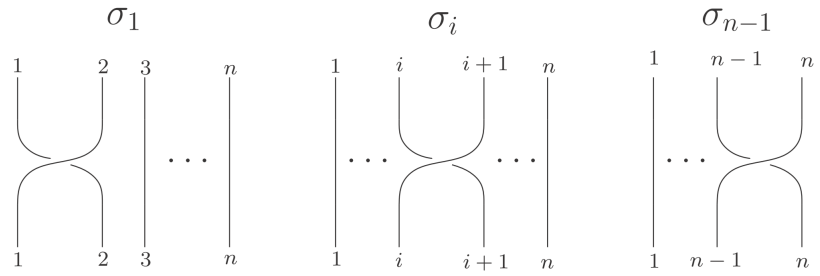


Figura 4: Geradores do grupo de tranças B_n.

Exemplo 3.4.1. Considere o grupo B_3. Os geradores obedecem a relação (3.40), em símbolos, $\sigma_1 \sigma_2 \sigma_1 = \sigma_2 \sigma_1 \sigma_2$. Podemos ilustrar os elementos inverso e unitário como:

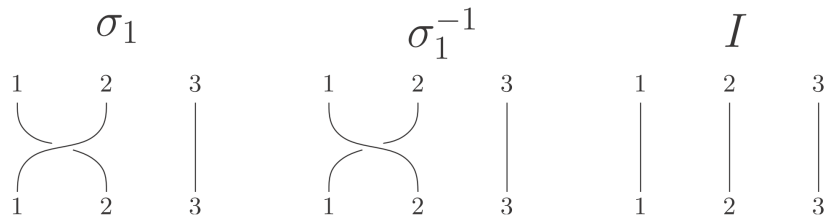
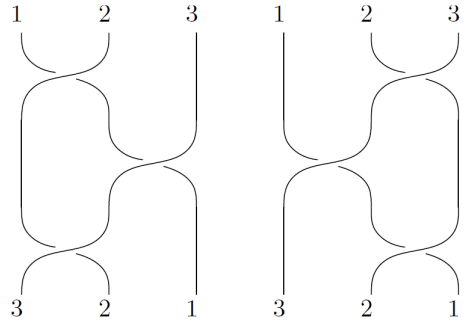


Figura 5: Elemento inverso e elemento unitário em B_3.

E a relação (3.39) por:



$$\sigma_1\sigma_2\sigma_1 = \sigma_2\sigma_1\sigma_2$$

Figura 6: Geradores de B_3.

Existem algumas formas para se obter representações do grupo de tranças, entre elas, a álgebra de Temperley-Lieb [16] e a álgebra de Hecke [60]. Trindade [61] mostrou que as relações (3.39) e (3.40), conhecidas também por relações *braid*, são satisfeitas quando os estados são elementos de ideais à esquerda minimais da álgebra e podem ser construídos a partir dos geradores da álgebra.

Uma outra forma para se obter representação do grupo de tranças é através da relação (3.40), também chamada equação de Yang-Baxter e que sob a condição [53]

$$\sigma_i \mapsto R_i = I^{\otimes(i-1)} \otimes R \otimes I^{\otimes(n-i-1)} \tag{3.44}$$

em que n é o número de partículas, I é o operador unidade e R é a solução da equação, ela pode ser expressa na forma:

$$(R \otimes I)(I \otimes R)(R \otimes I) = (I \otimes R)(R \otimes I)(I \otimes R), \tag{3.45}$$

satisfazendo portanto a relação que define os geradores do grupo de tranças. Considerando $\sigma_1 \mapsto R \otimes I$ e $\sigma_2 \mapsto I \otimes R$, podemos representar a equação (3.45) através da Figura 7.

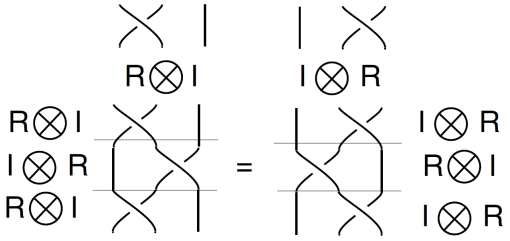


Figura 7: Equação de Yang-Baxter.

Em um trabalho seminal, Kauffman e Lomanaco Jr. [15] afirmaram que uma solução unitária R da equação de Yang-Baxter pode ser vista topologicamente como um matriz *braiding* (ou operador *braiding*) ou como uma porta lógica quântica universal. Esses autores também introduziram como solução da equação de Yang-Baxter a matriz a seguir:

$$R = \begin{pmatrix} a & 0 & 0 & 0 \\ 0 & 0 & d & 0 \\ 0 & c & 0 & 0 \\ 0 & 0 & 0 & b \end{pmatrix} \tag{3.46}$$

em que a, b, c e d são quaisquer escalares no círculo unitário em um plano complexo. Foi mostrado [15] que se R é escolhido de modo que $ab \neq cd$, então o estado $R(\psi \otimes \psi)$, com $\psi = |0\rangle + |1\rangle$, é emaranhado. Todas as matrizes unitárias 4x4 que são soluções para a equação de Yang-Baxter foram obtidas por Dye [62] que também para esta dimensão, classificou as famílias de soluções. No intuito de obter equações para o teletransporte e suas representações diagramáticas, Zhang [63] explorou a seguinte solução:

$$B = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & -1 & 0 \\ 0 & 1 & 1 & 0 \\ -1 & 0 & 0 & 1 \end{pmatrix} \tag{3.47}$$

chamada de matriz de Bell; a ação desta matriz em estados base resulta em estados do tipo Bell:

$$B|00\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) = \left|\Phi^-\right\rangle \tag{3.48}$$

$$B|01\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) = \left|\Psi^+\right\rangle \tag{3.49}$$

$$-B|10\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) = \left|\Psi^-\right\rangle \tag{3.50}$$

$$B|11\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = \left|\Phi^+\right\rangle \tag{3.51}$$

De posse dessas informações, nosso objetivo é desenvolver um método geral para obtenção das representações do grupo de tranças de um conjunto de álgebras de Hopf.

Para isso necessitaremos da estrutura quase triangular, o que nos fornecerá as R-matrizes que são soluções da equação de Yang-Baxter. Utilizaremos portanto as chamadas álgebras de Hopf quase triangulares, e apresentaremos resultados para álgebras de Hopf derivadas de grupos cíclicos. Em particular, investigaremos as atuações do grupo CZ_2 e das portas lógicas quânticas sobre os estados de Bell.

4 Álgebras de Hopf Quase Triangulares e Uma Proposta para Construções de Portas Lógicas Quânticas

Esse capítulo trata do método por nós desenvolvido neste trabalho [64] que visa propor soluções algébricas da equação de Yang-Baxter, e consequentemente portas lógicas quânticas. Iniciaremos com uma sucinta revisão de álgebras de Hopf quase triangulares e suas relações com a equação de Yang-Baxter. Em seguida, mostraremos algumas generalizações de resultados já postos na literatura [21]. Por fim, aplicaremos nossos resultados em estados do tipo Bell.

4.1 Álgebras de Hopf Quase Triangulares e Grupo de Tranças

Nesta seção, a partir dos conceitos apresentados no Capítulo 2, revisaremos algumas definições e resultados acerca das álgebras de Hopf quase triangulares [21, 22, 25] e suas relações com a equação de Yang-Baxter.

Definição 4.1.1. *Seja $(H, \mu, \eta, \Delta, \varepsilon)$ uma biálgebra. Uma biálgebra é dita quase cocomutatitiva se existe um elemento R, com inverso, da álgebra $H \otimes H$ de tal modo que para todo $x \in H$ tenhamos*

$$\Delta^{op}(x) = R\Delta(x)R^{-1} \tag{4.1}$$

em que $\Delta^{op} = \tau_{H,H} \circ \Delta$ denota o coproduto oposto em H; μ e η são as aplicações produto e unidade, respectivamente; Δ é o coproduto e ε a counidade. O elemento R que satisfaça essas condições é chamada R-matriz universal.

Definição 4.1.2. *Uma álgebra de Hopf quase cocomutativa $(H, \mu, \eta, \Delta, \varepsilon, S, R)$ é quase triangular se a R-matriz universal satisfaz as seguintes relações:*

$$(\Delta \otimes id_H)(R) = R_{13}R_{23} \tag{4.2}$$

e

$$(id_H \otimes \Delta)(R) = R_{13}R_{12}, \tag{4.3}$$

em que pela notação de Sweedler $R = \sum R^{(1)} \otimes R^{(2)}$. Isto nos sugere que

$$R_{ij} = 1 \otimes \cdots \otimes R^{(1)} \otimes 1 \otimes \cdots \otimes R^{(2)} \otimes \cdots \otimes 1,$$

para $R \in H \otimes H \otimes \cdots \otimes H$.

Note que $R_{ij} \in H^{\otimes m}$ em que $R^{(1)}$ é o i-ésimo fator, $R^{(2)}$ é o j-ésimo fator e todos os demais são 1, até que a sua dimensão seja completada. Uma forma alternativa para representar a R-matriz é utilizando elementos arbitrários da álgebra, o que nos dá $R = \sum_i s_i \otimes t_i$. Com isso, as expressões (4.2) e (4.3) podem ser reescritas, respectivamente, como:

$$\sum_{i,s_i} (s_i)' \otimes (s_i)'' \otimes t_i = \sum_{i,j} s_i \otimes s_j \otimes t_i t_j \tag{4.4}$$

e

$$\sum_{i,t_i} s_i \otimes (t_i)' \otimes (t_i)'' = \sum_{i,j} s_i s_j \otimes t_j \otimes t_i. \tag{4.5}$$

Exemplo 4.1.1. Seja H uma álgebra de Hopf gerada pelos dois elementos 1, g e x, satisfazendo as relações

$$g^2 = 1, \qquad x^2 = 0, \qquad xg = -gx.$$

O conjunto $\{1, g, x, gx\}$ formam uma base desse espaço vetorial. Como se trata de uma álgebra de Hopf, logo, teremos estrutura de coálgebra e aplicação antípoda dadas por

$$\Delta(g) = g \otimes g, \qquad \varepsilon(g) = 1, \qquad S(g) = g,$$

$$\Delta(x) = x \otimes 1 + g \otimes x, \qquad \varepsilon(x) = 0, \qquad S(x) = -gx.$$

Para qualquer $x \in H$, temos que $S^2(x) = gxg^{-1}$ e neste exemplo, a R-matriz universal será

$$R = \frac{1}{2}(1 \otimes 1 + 1 \otimes g + g \otimes 1 - g \otimes g) + \frac{\lambda}{2}(x \otimes x + x \otimes gx + gx \otimes gx - gx \otimes x)$$

em que λ é um parâmetro qualquer (cf. [25], p. 39).

Os lemas a seguir contêm informações importantes acerca das características das R-matrizes universais [25]. Para simplificar a notação indicaremos uma álgebra de Hopf quase triangular por um par (H, R)

Lema 4.1.1. *Considere o par (H,R) uma álgebra de Hopf quase triangular. Então R, um elemento de $H \otimes H$, obedece as relações*

$$(\varepsilon \otimes id_H)(R) = (id_H \otimes \varepsilon)(R) = 1, \tag{4.6}$$

$$(S \otimes id_H)(R) = R^{-1} = (id_H \otimes S^{-1})(R) \tag{4.7}$$

e

$$(S \otimes S)(R) = R. \tag{4.8}$$

Demonstração. *i)* A prova de (4.6) dar-se-á aplicando $(\varepsilon \otimes id_H \otimes id_H)$ à expressão (4.2):

$$\begin{aligned} R &= (\varepsilon \otimes id_H \otimes id_H)(\Delta \otimes id_H)(R) = (\varepsilon \otimes id_H \otimes id_H)(R_{13}R_{23}) \\ &= (\varepsilon \otimes id_H)(R) \cdot R \end{aligned}$$

E quando aplicamos $(id_H \otimes id_H \otimes \varepsilon)$ à expressão (4.3) obtemos

$$\begin{aligned} R &= (id_H \otimes id_H \otimes \varepsilon)(id_H \otimes \Delta)(R) = (id_H \otimes id_H \otimes \varepsilon)(R_{13}R_{12}) \\ &= R \cdot (id_H \otimes \varepsilon)(R). \end{aligned}$$

ii) Mostra-se (4.7), calculando

$$\begin{aligned} R \cdot (S \otimes id_H)(R) &= (\mu \otimes id_H)(id_H \otimes S \otimes id_H)(R_{13}R_{23}) \\ &= (\mu \otimes id_H)(id_H \otimes S \otimes id_H)(\Delta \otimes id_H)(R) \\ &= (\mu(id_H \otimes S)\Delta \otimes id_H)(R) \\ &= (\varepsilon \otimes id_H)(R) = 1 \end{aligned}$$

e

$$\begin{aligned} (id_H \otimes S)(R^{-1}) \cdot R^{-1} &= (id_H \otimes \mu)(id_H \otimes S \otimes id_H)(R_{12}^{-1}R_{13}^{-1}) \\ &= (id_H \otimes \mu)(id_H \otimes S \otimes id_H)(id_H \otimes \Delta)(R^{-1}) \\ &= (id_H \otimes \mu(S \otimes id_H)\Delta)(R^{-1}) \\ &= (id_H \otimes \varepsilon)(R^{-1}) = 1. \end{aligned}$$

iii) Por fim, a relação (4.8) é mostrada por

$$\begin{aligned} (S \otimes S)(R) &= (id_H \otimes S)(S \otimes id_H)(R) \\ &= (id_H \otimes S)(R^{-1}) \\ &= (id_H \otimes S)(id_H \otimes S^{-1})(R) \\ &= (id_H \otimes id_H)(R) \\ &= R. \end{aligned}$$

■

Observe que para $R = \sum_i s_i \otimes t_i$ as relações (4.6) e (4.7) são equivalentes a:

$$\sum_i \varepsilon(s_i)t_i = \sum_i s_i \varepsilon t_i = 1 \tag{4.9}$$

e

$$R^{-1} = \sum_i S(s_i) \otimes t_i = \sum_i s_i \otimes S^{-1}t_i, \tag{4.10}$$

respectivamente.

Lema 4.1.2. *Seja (H, R) uma álgebra de Hopf quase triangular. Então a R-matriz universal satisfaz a equação*

$$R_{12}R_{13}R_{23} = R_{23}R_{13}R_{12} \tag{4.11}$$

denominada equação de Yang-Baxter quântica.

Demonstração. Aplica-se τ_{12} a ambos os lados de (4.2), obtendo $(\Delta^{op} \otimes id_H)(R) = R_{23}R_{13}$; assim

$$\begin{aligned} R_{23}R_{13}R_{12} &= (\Delta \otimes id_H)(R) \\ &= R_{12}(\Delta \otimes id_H)R_{12}^{-1}R_{12} \\ &= R_{12}R_{13}R_{23}. \end{aligned}$$

■

Naturalmente, quando $R = \sum_i s_i \otimes t_i$ a equação (4.11) pode ser reescrita então como:

$$\sum_{i,j,k} s_i s_k \otimes t_k s_i \otimes t_j t_i = \sum_{i,j,k} s_j s_i \otimes s_k t_i \otimes t_k t_j. \tag{4.12}$$

Definição 4.1.3. *Seja V um espaço vetorial sobre o corpo k. Chama-se automorfismo linear R' de $V \otimes V$ uma R-matriz solução da equação de Yang-Baxter*

$$(R' \otimes id_V)(id_V \otimes R')(R' \otimes id_V) = (id_V \otimes R')(R' \otimes id_V)(id_V \otimes R'), \tag{4.13}$$

em que $R' = \tau R$, com τ sendo o operador flip.

A relação supracitada é de fundamental importância, pois através da identificação

$$R'_i = \mathbb{I}^{\otimes(i-1)} \otimes R' \otimes \mathbb{I}^{\otimes(n-i)}, \tag{4.14}$$

em que $\mathbb{I}$ é o operador identidade, essa relação nos permite construir representações do grupo de tranças B_n uma vez que satisfazem as relações correspondentes a (3.39) e (3.40):

$$R'_i R'_j = R'_j R'_i, \quad |i - j| \geq 2 \tag{4.15}$$

e

$$R'_i R'_{i+1} R'_i = R'_{i+1} R'_i R'_{i+1}, \quad i = 1, \ldots, n-2 \tag{4.16}$$

4.2 Generalização de resultados

Nesta seção, realizaremos generalizações de alguns resultados de Kassel [21] utilizando um conjunto de álgebras, e exploraremos esses resultados no contexto de grupos cíclicos. É importante destacar que muitos algoritmos quânticos são descritos por meio do produto semidireto e/ou direto de grupos. Um possível caminho de descrever isto por meio de uma formulação algébrica seria a partir de um conjunto de álgebras, o qual construímos produtos tensoriais de elementos.

Lema 4.2.1. *Sejam* $(H_1, \mu_1, \eta_1, \Delta_1, \varepsilon_1, S_1, S_1^{-1}, R_1), \ldots,$ $(H_n, \mu_n, \eta_n, \Delta_n, \varepsilon_n, S_n, S_n^{-1}, R_n)$ *álgebras de Hopf quase triangulares. Portanto, há um elemento inversível* R *tal que para todo* $x \in H_1 \otimes \cdots \otimes H_n$*, tem-se*

$$\Delta^{op}(x)R = R\Delta(x) \tag{4.17}$$

com $R_1 = \sum_{i_1} s_{i_1} \otimes t_{i_1}, \ldots,$ $R_n = \sum_{i_n} s_{i_n} \otimes t_{i_n}$*, e*

$$R = \sum_{i_n, \ldots, i_n} s_{i_1} \otimes \cdots \otimes s_{i_n} \otimes t_{i_1} \otimes \cdots \otimes t_{i_n} \tag{4.18}$$

Além disso, temos as seguintes relações

$$(\Delta \otimes id_{H_1 \otimes \cdots \otimes H_n})(R) = R_{13}R_{23} \tag{4.19}$$

$$(id_{H_1 \otimes \cdots \otimes H_n} \otimes \Delta)(R) = R_{13}R_{12} \tag{4.20}$$

$$R_{12}R_{13}R_{23} = R_{23}R_{13}R_{12} \tag{4.21}$$

em que $R_{12} = \sum_{i_1 \ldots i_n} s_{i_1} \otimes \ldots s_{i_n} \otimes t_{i_1} \otimes \cdots \otimes t_{i_n} \otimes 1 \otimes \cdots \otimes 1$*,* $R_{13} = \sum_{i_1 \ldots i_n} s_{i_1} \otimes \cdots s_{i_n} \otimes 1 \otimes \cdots \otimes 1 \otimes t_{i_1} \otimes \cdots \otimes t_{i_n}$ *e* $R_{23} = \sum_{i_1 \ldots i_n} 1 \otimes \cdots \otimes 1 \otimes s_{i_1} \otimes \cdots \otimes s_{i_n} \otimes t_{i_1} \otimes \cdots \otimes t_{i_n}$ *são satisfeitas.*

Demonstração. Seja o coproduto:

$$\Delta(x) = \sum_{(x)} x' \otimes x''$$

na notação de Sweedler

$$\begin{aligned} \Delta(x_1 \otimes \cdots \otimes x_n) &= \sum_{(x_1 \otimes \cdots \otimes x_n)} (x_1 \otimes x_2 \otimes \cdots \otimes x_n)' \otimes (x_1 \otimes x_2 \otimes \cdots \otimes x_n)'' \\ &= \sum_{(x_1 \otimes \cdots \otimes x_n)} x_1' \otimes \cdots \otimes x_n' \otimes x_1'' \otimes \cdots \otimes x_n'' \end{aligned}$$

Então, no caso geral

$$\Delta^{op}(x_1 \otimes \cdots \otimes x_n) = \sum_{(x_1 \otimes \cdots \otimes x_n)} x_1'' \otimes \cdots \otimes x_n'' \otimes x_1' \otimes \cdots \otimes x_n'$$

Consequentemente

$$\begin{aligned}
\Delta^{op}(x_1 \otimes \cdots \otimes x_n)R &= \sum_{(x_1 \otimes \cdots \otimes x_n)} (x_1'' \otimes \cdots \otimes x_n'' \otimes x_1' \otimes \cdots \otimes x_n') \sum_{i_1 \ldots i_n} s_{i_1} \otimes \cdots \otimes s_{i_n} \otimes t_{i_1} \otimes \cdots \otimes t_{i_n} \\
&= \sum_{(x_1,\ldots,x_n;i_1,\ldots,i_n)} x_1'' s_{i_1} \otimes x_2'' s_{i_2} \otimes \cdots \otimes x_n'' s_{i_n} \otimes x_1' t_{i_1} \otimes \cdots \otimes x_n' t_{i_n} \\
&= \left(\sum_{(x_1,\ldots,x_n;i_1,\ldots,i_n)} x_1'' s_{i_1} \otimes 1 \otimes \cdots \otimes x_1' t_{i_1} \otimes \cdots \otimes 1 \right) \ldots \\
&\quad \left(\sum_{(x_1,\ldots,x_n;i_1,\ldots,i_n)} 1 \otimes \cdots \otimes x_{i_n}'' s_{i_n} \otimes 1 \otimes \cdots \otimes x_n' t_{i_n} \right) \\
&= \left(\sum_{(x_1,\ldots,x_n;i_1,\ldots,i_n)} s_{i_1} x_1' \otimes 1 \otimes \cdots \otimes t_{i_1 x_1''} \otimes \cdots \otimes 1 \right) \ldots \\
&\quad \left(\sum_{(x_1,\ldots,x_n;i_1,\ldots,i_n)} 1 \otimes \cdots \otimes s_{i_n} x_{i_n}' \otimes 1 \otimes \cdots \otimes t_{i_n} x_n'' \right) \\
&= \left(\sum_{(x_1,\ldots,x_n;i_1,\ldots,i_n)} s_{i_1} x_1' \otimes s_{i_2} x_2' \otimes \cdots \otimes s_{i_n} x_n' \otimes t_{i_1} x_1'' \otimes \cdots \otimes t_{i_n} x_n'' \right) \\
&= R\Delta(x)
\end{aligned}$$

Motivados pelas relações (4.19) e (4.20), temos

$$\begin{aligned}
(\Delta \otimes id_H) \left(\sum_{i_1 \ldots i_n} s_{i_1} \otimes \cdots \otimes s_{i_n} \otimes t_{i_1} \otimes \cdots \otimes t_{i_n} \right) &= \sum_{i_1 \ldots i_n} \Delta(s_{i_1} \otimes \cdots \otimes s_{i_n}) \otimes id_H(t_{i_1} \otimes \cdots \otimes t_{i_n}) \\
&= \sum_{i_1 \ldots i_n} s_{i_1}' \otimes s_{i_2}' \otimes \cdots s_{i_n}' \otimes s_{i_1}'' \otimes \cdots \otimes s_{i_n}'' \\
&\quad \otimes t_{i_1} \otimes \cdots \otimes t_{i_n} \\
&= (\sum_{i_1 s_1} s_{i_1}' \otimes 1 \otimes \cdots \otimes s_{i_1}'' \otimes \cdots \otimes t_{i_1}' \\
&\quad \otimes \cdots \otimes 1) \ldots (\sum_{i_n s_n} 1 \otimes \cdots \otimes s_{i_n}' \otimes \cdots \otimes s_{i_n}'' \\
&\quad \otimes \cdots \otimes t_{i_n}) \\
&= (\sum_{i_1 j_1} s_{i_1} \otimes 1 \otimes \cdots \otimes s_{j_1} \otimes 1 \otimes \cdots \otimes t_{i_1} t_{j_1} \\
&\quad \otimes \cdots \otimes 1) \ldots (\sum_{i_n j_n} 1 \otimes \cdots \otimes s_{i_n} \otimes \cdots \otimes s_{j_n} \\
&\quad \otimes 1 \otimes \cdots \otimes t_{i_n} t_{j_n}) \\
&= R_{13} R_{23}
\end{aligned}$$

De forma similar

$$(id_{H_1 \otimes \cdots \otimes H_n} \otimes \Delta) = R_{13} R_{12}$$

Segue então que

$$\begin{aligned}
R_{12}R_{13}R_{23} &= \sum_{i_1\ldots i_n,j_1\ldots j_n,k_1\ldots k_n} s_{k_1}s_{j_1}\otimes\cdots\otimes s_{k_n}s_{j_n}\otimes t_{k_1}s_{i_1}\otimes\cdots\otimes t_{k_n}s_{i_n}\otimes t_{j_1}t_{i_1}\otimes\cdots\otimes t_{j_n}t_{i_n}\\
&= (\sum_{i_1,j_1,k_1} s_{k_1}s_{j_1}\otimes\cdots\otimes 1\otimes t_{k_1}s_{i_1}\otimes\cdots\otimes 1\otimes t_{j_1}t_{i_1}\otimes\cdots\otimes 1)...(\sum_{i_n,j_n,k_n} 1\otimes\cdots\\
&\quad \otimes s_{k_n}s_{j_n}\otimes\cdots\otimes 1\otimes t_{k_n}s_{i_n}\otimes\cdots\otimes t_{j_n}t_{i_n})\\
&= \sum_{i_1\ldots i_n} (s_{j_1}s_{i_1}\otimes\cdots\otimes 1\otimes s_{k_1}t_{k_1}\otimes\cdots\otimes t_{k_1}t_{j_1}\otimes\cdots\otimes 1)...(\sum_{i_n,j_n,k_n} 1\otimes\cdots\otimes s_{j_n}s_{i_n}\otimes\cdots\\
&\quad \otimes 1\otimes s_{k_n}t_{i_n}\otimes\cdots\otimes t_{k_n}t_{j_n})\\
&= \sum_{i_1\ldots i_n,j_1\ldots j_n,k_1\ldots k_n} s_{j_1}s_{i_1}\otimes\cdots\otimes s_{j_n}s_{i_n}\otimes\cdots\otimes s_{k_n}t_{i_n}\otimes t_{k_1}t_{j_1}\otimes\cdots\otimes t_{k_n}t_{j_n}\\
&= R_{23}R_{13}R_{12}
\end{aligned}$$

■

Sejam $V_1,\ldots,V_n$ e $W_1,\ldots,W_n$ H-módulos. Podemos estabelecer um isomorfismo $C^R_{V_1\ldots V_n,W_1\ldots W_n}$ de $H_1,\ldots,H_n$-módulos entre $V_1\otimes\cdots\otimes V_n\otimes W_1\otimes\cdots\otimes W_n$ e $W_1\otimes\cdots\otimes W_n\otimes V_1\otimes\cdots\otimes V_n$, definido por

$$\begin{aligned}
C^R_{V_1\ldots V_n,W_1\ldots W_n}(v_1\otimes\cdots\otimes v_n\otimes w_1\otimes\cdots\otimes w_n) &= \tau_{V_1\ldots V_n,W_1\ldots W_n}(R\rhd(v_1\otimes\cdots\otimes v_n\otimes w_1\otimes\cdots\otimes w_n)\\
&= \sum_{i_1\ldots i_n} t_{i_1}\rhd w_1\otimes\cdots\otimes t_{i_n}\rhd w_n\otimes s_{i_1}\rhd v_1\otimes\cdots\\
&\quad \otimes s_{i_n}\rhd v_n
\end{aligned}$$

em que $\rhd$ denota a ação de H em U, V e W.

Teorema 4.2.1. *Para qualquer tripla $(U_1\otimes\cdots\otimes U_n, V_1\otimes\cdots\otimes V_n, W_1\otimes\cdots\otimes W_n)$ de $H_1\otimes\cdots\otimes H_n$-módulo, temos:*

a) A aplicação $C^R_{V_1\ldots V_n,W_1\ldots Wn}$ é um isomorfismo de $H_1\otimes\cdots\otimes H_n$-módulo.

b) $\left(C^R_{V_1\ldots V_n,W_1\ldots W_n}\otimes id_{U_1\ldots U_n}\right)\left(id_{V_1\ldots V_n}\otimes C^R_{U_1\ldots U_n,W_1\ldots W_n}\right)\left(C^R_{U_1\ldots U_n,V_1\ldots V_n}\otimes id_{W_1\ldots W_n}\right) =$

$\left(id_{W_1\ldots W_n}\otimes C^R_{U_1\ldots U_n,V_1\ldots V_n}\right)\left(C^R_{U_1\ldots U_n,W_1\ldots W_n}\otimes id_{V_1\ldots V_n}\right)\left(id_{U_1\ldots U_n}\otimes C^R_{V_1\ldots V_n,W_1\ldots W_n}\right)$

Demonstração. *a)* Para qualquer $x_1\otimes\cdots\otimes x_n\in H_1\otimes\cdots\otimes H_n$-módulo, usando a definição

$C^R_{V_1\ldots V_n,W_1\ldots W_n}(x_1\otimes\cdots\otimes x_n)\rhd(v_1\otimes\cdots\otimes v_n\otimes w_1\otimes\cdots\otimes w_n) = \tau_{v_1\ldots v_n,w_1\ldots w_n}(R\rhd\Delta(x_1\otimes\cdots\otimes x_n)\rhd(v_1\otimes\cdots\otimes v_n\otimes w_1\otimes\cdots\otimes w_n))$, o Lema 4.2.1 e a notação $C^R_{V_1\ldots V_n,W_1\ldots W_n}(x_1\otimes\cdots\otimes x_n)\rhd(v_1\otimes\cdots\otimes v_n\otimes w_1\otimes\cdots\otimes w_n) = \mathcal{C}$, obtemos

$$
\begin{aligned}
\mathcal{C} &= \tau_{v_1\ldots v_n,w_1\ldots w_n}(\Delta^{op}(x_1\otimes\cdots\otimes x_n)R(v_1\otimes\cdots\otimes v_n\otimes w_1\otimes\cdots\otimes w_n)) \\
&= \tau_{v_1\ldots v_n,w_1\ldots w_n}(\sum_{x_1\ldots x_n,i_1\ldots i_n} x_1''s_{i_1}\rhd v_1\otimes x_2''s_{i_2}\rhd v_2\otimes\cdots\otimes x_n''s_{i_n}\rhd v_n\otimes x_1't_{i_1}\rhd w_1\otimes x_2't_{i_2} \\
&\quad \rhd w_2\otimes\cdots\otimes x_n't_{i_n}\rhd w_n) \\
&= \sum_{x_1\ldots x_n,i_1\ldots i_n} x_1't_{i_1}\rhd w_1\otimes x_2't_{i_2}\rhd w_2\otimes\cdots\otimes x_n't_{i_n}\rhd w_n\otimes x_1''s_{i_1}\rhd v_1\otimes x_2''s_{i_2}\rhd v_2\otimes \\
&\quad \cdots\otimes x_n''s_{i_n}\rhd v_n \\
&= \Delta(x_1\otimes\cdots\otimes x_n)\sum_{i_1\ldots i_n} t_{i_1}\rhd w_1\otimes\cdots\otimes t_{i_n}\rhd w_n\otimes x_1''s_{i_1}\rhd v_1\otimes\cdots\otimes x_n''s_{i_n}\rhd v_n \\
&= \Delta(x_1\otimes\cdots\otimes x_n)\tau_{v_1\ldots v_n,w_1\ldots w_n}(R\rhd[v_1\otimes\cdots\otimes v_n\otimes w_1\otimes\cdots\otimes w_n]) \\
&= (x_1\otimes\cdots\otimes x_n)(C^R_{V_1\ldots V_n,W_1\ldots W_n}[v_1\otimes\cdots\otimes v_n\otimes w_1\otimes\cdots\otimes w_n])
\end{aligned}
$$

b) Com a utilização do Lema 4.2.1 é fácil verificar que

$$
\begin{aligned}
&\left(C^R_{V_1\ldots V_n,W_1\ldots W_n}\otimes id_{U_1\ldots U_n}\right)\left(id_{V_1\ldots V_n}\otimes C^R_{U_1\ldots U_n,W_1\ldots W_n}\right)\left(C^R_{U_1\ldots U_n,V_1\ldots V_n}\otimes id_{W_1\ldots W_n}\right) = \\
&\sum_{i_1\ldots i_n,j_1\ldots j_n,k_1\ldots k_n} t_{k_1}t_{j_1}\rhd w_1\otimes\cdots\otimes t_{k_n}t_{j_n}\rhd w_n\otimes s_{k_1}t_{i_1}\rhd v_1\cdots\otimes s_{k_n}t_{i_n}\rhd v_n\otimes s_{j_1}s_{i_1}\rhd \\
&u_1\otimes\cdots\otimes s_{j_n}s_{i_n}\rhd u_n
\end{aligned}
$$

$$
\begin{aligned}
&= \left(\sum_{i_1,j_1,k_1} t_{k_1}t_{j_1}\rhd w_1\otimes\cdots\otimes s_{k_1}t_{i_1}\rhd v_1\otimes\cdots\otimes s_{j_1}s_{i_1}\rhd u_1\otimes\cdots\otimes 1\right)\ldots \\
&\quad \left(\sum_{i_n,j_n,k_n} 1\otimes t_{k_n}t_{j_n}\rhd w_n\otimes\cdots\otimes s_{k_n}t_{i_n}\rhd v_n\otimes\cdots\otimes 1\otimes s_{j_n}s_{i_n}\rhd u_n\right)
\end{aligned}
$$

$$
\begin{aligned}
&= \left(\sum_{i_1,j_1,k_1} t_{j_1}t_{i_1}\rhd w_1\otimes\cdots\otimes t_{k_1}s_{i_1}\rhd v_1\otimes\cdots\otimes s_{j_1}s_{i_1}\rhd u_1\otimes\cdots\otimes 1\right)\ldots \\
&\quad \left(\sum_{i_n,j_n,k_n} 1\otimes t_{j_n}t_{i_n}\rhd w_n\otimes\cdots\otimes t_{k_n}s_{i_n}\rhd v_n\otimes\cdots\otimes 1\otimes s_{k_n}s_{j_n}\rhd u_n\right)
\end{aligned}
$$

$$
= \left(id_{W_1\ldots W_n}\otimes C^R_{U_1\ldots U_n,V_1\ldots V_n}\right)\left(C^R_{U_1\ldots U_n,W_1\ldots W_n}\otimes id_{V_1\ldots V_n}\right)\left(id_{U_1\ldots U_n}\otimes C^R_{V_1\ldots V_n,W_1\ldots W_n}\right)
$$

o que demonstra o teorema. ■

Observe que se $U_1 = V_1 = W_1, \ldots, U_n = V_n = W_n$, conclui-se que $C^R_{V_1\ldots V_n,W_1\ldots W_n}$ é solução da equação de Yang-Baxter e portanto pode ser usada para gerar representação do grupo de tranças.

Considere agora $Z_{/\eta_1}, Z_{/\eta_2}, \ldots, Z_{/\eta_n}$ grupos cíclicos finitos de ordem $\eta_1, \eta_2, \ldots, \eta_n$ e $CZ_{/\eta_1}, CZ_{/\eta_2}, \ldots, CZ_{/\eta_n}$ suas álgebras de grupo respectivamente. Podemos construir

álgebras de Hopf [25] com estruturas quase triangulares

$$R_1 = \frac{1}{\eta_1} \sum_{a_1,b_1=0}^{\eta_1-1} e^{\frac{-2\pi I a_1 b_1}{\eta_1}} g^{a_1} \otimes g^{b_1} \tag{4.22}$$

$$R_2 = \frac{1}{\eta_2} \sum_{a_2,b_2=0}^{\eta_2-1} e^{\frac{-2\pi I a_2 b_2}{\eta_2}} g^{a_2} \otimes g^{b_2} \tag{4.23}$$

$$\vdots$$

$$R_n = \frac{1}{\eta_n} \sum_{a_n,b_n=0}^{\eta_n-1} e^{\frac{-2\pi I a_n b_n}{\eta_n}} g^{a_n} \otimes g^{b_n} \tag{4.24}$$

e tem coproduto $\Delta g^{a_1} = g^{a_1} \otimes g^{a_1}, \Delta g^{a_2} = g^{a_2} \otimes g^{a_2}, \ldots, \Delta g^{a_n} = g^{a_n} \otimes g^{a_n}$. A counidade é dada por $\epsilon g^{a_1} = \epsilon g^{a_2} = \cdots = \epsilon g^{a_n} = 1$ e a antípoda $Sg^{a_1} = (g^{a_1})^{-1}, Sg^{a_2} = (g^{a_2})^{-1}, \ldots, Sg^{a_n} = (g^{a_n})^{-1}$. A unidade imaginária é representado por I. Em (4.22) – (4.24) g^{a_i} são os elementos do grupo.

De acordo com a nossa formulação, temos:

$$R = \frac{1}{\eta_1\eta_2\ldots\eta_n} \sum_{a_1,a_2,\ldots,a_n;b_1,b_2,\ldots,b_n=0}^{\eta_1-1,\eta_2-1,\ldots,\eta_n-1} e^{\frac{-2\pi I a_1 b_1 \ldots a_n b_n}{\eta_1\eta_2\ldots\eta_n}} g^{a_1} \otimes g^{a_2} \otimes \cdots \otimes g^{a_n} \otimes g^{b_1} \otimes g^{b_2} \otimes \cdots \otimes g^{b_n} \tag{4.25}$$

Usando a notação $C^R_{U_1\ldots U_n,V_1\ldots V_n}(u_1 \otimes u_2 \otimes \cdots \otimes u_n \otimes v_1 \otimes v_2 \otimes \cdots \otimes v_n) = \mathcal{C}_1$, podemos mostrar [21] que:

$$\begin{aligned} \mathcal{C}_1 \;=\; & \frac{1}{\eta_1\eta_2\ldots\eta_n} \sum_{a_1,a_2,\ldots,a_n b_1,b_2,\ldots,b_n}^{\eta_1-1,\eta_2-1,\ldots,\eta_n-1} e^{\frac{-2\pi I a_1 b_1 a_2 b_2 \ldots a_n b_n}{\eta_1\eta_2\cdots\eta_n}} g^{b_1} \rhd v_1 \otimes g^{b_2} \rhd v_2 \otimes \cdots \otimes g^{b_n} \rhd v_n \\ & \otimes g^{a_1} \rhd u_1 \otimes g^{a_2} \rhd u_2 \otimes \cdots \otimes g^{a_n} \rhd u_n \end{aligned} \tag{4.26}$$

4.3 Aplicação

Para ilustrar nosso método desenvolvido em [64], consideramos a álgebra de grupo $CZ_{/2}$ com o grupo $G = \{\epsilon, x\}$, em que ϵ é a identidade. Neste caso, utilizando (4.25) tem-se

$$\begin{aligned} R \;&=\; \frac{1}{2} \sum_{a,b=0}^{1} e^{-\pi I a b} g^a \otimes g^b \\ &=\; \frac{1}{2}(\epsilon \otimes \epsilon + x \otimes \epsilon + \epsilon \otimes x - x \otimes x). \end{aligned} \tag{4.27}$$

Usando a representação regular Ξ da álgebra [66], temos

$$\Xi(\epsilon\otimes\epsilon)=\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&1\end{pmatrix};\Xi(x\otimes\epsilon)=\begin{pmatrix}0&0&1&0\\0&0&0&1\\1&0&0&0\\0&1&0&0\end{pmatrix}$$

$$\Xi(\epsilon\otimes x)=\begin{pmatrix}0&1&0&0\\1&0&0&0\\0&0&0&1\\0&0&1&0\end{pmatrix};\Xi(x\otimes x)=\begin{pmatrix}0&0&0&1\\0&0&1&0\\0&1&0&0\\1&0&0&0\end{pmatrix}$$

e utilizando a expressão (4.27) tem-se

$$\Xi(R)=\frac{1}{2}\begin{pmatrix}1&1&1&-1\\1&1&-1&1\\1&-1&1&1\\-1&1&1&1\end{pmatrix}. \tag{4.28}$$

Consideraremos $\Xi(R)\equiv R$. O operador *flip* associado é dado por [15]:

$$\tau=\begin{pmatrix}1&0&0&0\\0&0&1&0\\0&1&0&0\\0&0&0&1\end{pmatrix} \tag{4.29}$$

Consequentemente,

$$R'=\tau R=\frac{1}{2}\begin{pmatrix}1&1&1&-1\\1&-1&1&1\\1&1&-1&1\\-1&1&1&1\end{pmatrix} \tag{4.30}$$

Esta matriz satisfaz a relação de trança (3.45), ou seja:

$$(\mathbb{I}\otimes R')(R'\otimes\mathbb{I})(\mathbb{I}\otimes R')=(R'\otimes\mathbb{I})(\mathbb{I}\otimes R')(R'\otimes\mathbb{I}) \tag{4.31}$$

em que $\mathbb{I}$ é a matriz identidade 2×2, e pode ser interpretada como uma porta lógica quântica.

Sua ação sobre os estados de Bell é dada por

$$R'\left[\frac{1}{\sqrt{2}}(|00\rangle+|11\rangle)\right]=\frac{1}{\sqrt{2}}(|01\rangle+|10\rangle)=\left|\Psi^{+}\right\rangle; \tag{4.32}$$

$$R'\left[\frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)\right] = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = \left|\Phi^+\right\rangle; \tag{4.33}$$

$$R'\left[\frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)\right] = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) = \left|\Phi^-\right\rangle; \tag{4.34}$$

$$R'\left[\frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)\right] = \frac{1}{\sqrt{2}}(|10\rangle - |01\rangle) = -\left|\Psi^-\right\rangle, \tag{4.35}$$

i.e. o emaranhamento é preservado sob a ação desta porta. É importante ressaltar que muitos grupos de simetria podem ser escritos em termos de grupos cíclicos [66]. Portanto, os grupos cíclicos podem refletir indiretamente simetrias de sistemas físicos transformando estados maximamente emaranhados em si mesmos. Curiosamente, a partir de um caso extremamente simples, é possível gerar uma estrutura não trivial.

Ao contrário das abordagens de outros autores [15, 62, 63], nossa proposta é a obtenção de representações de grupos de trança de uma forma sistemática para dimensões arbitrárias, explorando a estrutura de simetrias subjacentes. Isto é interessante para física *anyônica*, porque, por exemplo Monchon [67] mostrou que para *anyons* obtidos a partir de uma teoria de calibre finito, o poder computacional depende do grupo de simetria. É importante mencionar que apesar da análise ter sido feito para grupos cíclicos, qualquer grupo ou álgebra poderia ter sido utilizado, assim o nosso método é geral.

5 Conclusões

Neste trabalho, visando desenvolver portas lógicas quânticas algébricas, abordamos inicialmente as álgebras de Hopf que serviram como base para os estudos das álgebras de Hopf quase triangulares apresentadas em capítulo posterior. Neste contexto foram apresentadas as definições de álgebras, coálgebras e biálgebras. Em um segundo momento apresentamos alguns conceitos básicos da computação e informação quânticas; foram eles: os q-bits, as portas lógicas quânticas, o emaranhamento quântico e a codificação super-densa. Como motivação e justificativa para nosso desenvolvimento fizemos uma discussão sobre a possibilidade de implementação da computação quântica, mais especificamente, a computação quântica topológica que emprega quase partículas bidimensionais chamadas *anyons*; exploramos a estrutura matemática da computação quântica topológica através do grupo de tranças que aparece associado aos *anyons* e estudamos a equação de Yang-Baxter e sua importância dentro da computação quântica topológica.

Na segunda parte deste trabalho, revisamos conceitos de álgebras de Hopf quase triangulares e a suas relações com o grupo de tranças e a equação de Yang-Baxter. Apresentamos então no capítulo 4 nossa contribuição, ou seja, um método sistemático para encontrar representações do grupo de tranças obtidas considerando um conjunto de álgebras de Hopf quase triangulares derivadas de um grupo cíclico. Em particular, mostramos como obter uma porta lógica quântica de uma estrutura simples abeliana gerada pela álgebra do grupo CZ_2, sendo essas portas lógicas capazes de preservar os estados emaranhados do tipo Bell.

Como perspectivas, exploraremos outros grupos cíclicos, bem como, a possível estrutura topológica associada. Investigaremos o nosso método dentro do conceito de emaranhamento topológico [14], buscando desenvolver um critério algébrico para esse emaranhamento. Também perscrutaremos as atuações dessas porta lógicas dentro da criptografia quântica, por exemplo os protocolos BB84 e E91.

Concluindo, devemos citar que a computação e informação quânticas, como processos em desenvolvimento, ainda apresentam lacunas (por exemplo, novas portas lógicas e protocolos de criptografia) a serem preenchidas tanto no âmbito experimental quanto teórico. Acreditamos que assim como foi com a computação clássica, para implementação do computador quântico, é preciso buscar bases teóricas eficientes que sanem os problemas detectados sendo a linguagem algébrica uma dos domínios de interesse nessa base e onde insere-se nosso trabalho.

APÊNDICE A – Elementos de Álgebra e de Categorias

Este apêndice foi fortemente influenciado pelas referências [36, 68–70]. A ideia deste apêndice é que o leitor se familiarize com as estruturas algébricas e com as categorias apresentadas ao longo do texto.

A.1 Tópico em Categorias

Em teoria de categoria, observamos que muitas propriedades de sistemas matemáticos podem ser unificadas e simplificadas por uma apresentação com diagramas de flechas. Por exemplo, considere a flecha $f : A \to B$ representando uma função; isto é, tem-se um conjunto A, um conjunto B e uma regra $x \mapsto f(x)$ que atribui a cada elemento $x \in A$ um elemento $f(x) \in B$. Sendo assim, um diagrama geral da situação

$$\begin{array}{ccc} & B & \\ {\scriptstyle f}\nearrow & & \searrow{\scriptstyle g} \\ A & \xrightarrow[h]{} & C \end{array} \quad , \tag{A.1}$$

é comutativo quando $h = g \circ f$, em que "$\circ$" é a composição usual de funções, ou seja $g \circ f : A \to C$ e é definido por $x \mapsto g(f(x))$.

A.2 Grupo

Definição A.2.1. *Um conjunto G com uma operação*[1] $\centerdot : G \to G \times G$ *é um grupo se satisfaz os seguintes axiomas:*

i) Sejam $a, b, c \in G$ então a operação é associativa, isto é $a \centerdot (b \centerdot c) = (a \centerdot b) \centerdot c$;

ii) Para todo $a \in G$, existe elemento neutro $e \in G$ tal que $e \centerdot a = a \centerdot e = a$;

iii) Para todo elemento $a \in G$, existe um elemento inverso $b \in G$ tal que $a \centerdot b = b \centerdot a = e$.

Nota-se um grupo G por com operação $\centerdot$ por $(G, \centerdot)$.

[1] Esta operação não necessariamente significa o produto dos elementos; também não induz previamente a comutatividade dos elementos.

Exemplo A.2.1. *a)* $(\mathbb{Z}, +)$ é um grupo abeliano infinito, em que $\mathbb{Z}$ é conjunto dos inteiros.

b) $(\mathbb{R}^*, .)$ é um grupo multiplicativo abeliano, em que $\mathbb{R}^*$ é o conjunto dos reais não nulos.

Um grupo em que todos os elementos comutam é chamado comutativo ou abeliano.

Definição A.2.2. *Seja $(G, .)$ um grupo. Um subconjunto não vazio H de G é um subgrupo de G (detonamos por $H < G$) quando, com a operação de G, o conjunto H é um grupo.*

Os resultados das operações sucessivas entre dois elementos quaisquer do grupo, pode ser representado por meio de uma tabela de multiplicação (ver as referências [68, 69]).

A.2.1 Grupo de Permutações

Consideremos um conjunto de todas as permutações de n elementos: Toda permutação de n objetos pode ser representada por

$$\begin{pmatrix} 1 & 2 & \cdots & n \\ m_1 & m_2 & \cdots & m_n \end{pmatrix}$$

com significa que a permutação desloca o objeto originalmente na posição 1 para posição m_1, o objeto na posição 2 para m_2 e etc.

Definamos o produto $\gamma_1\gamma_2$ de duas permutações γ_1 e γ_2 como a permutação obtida primeiro executando γ_2 e depois γ_1. Por exemplo para $n = 4$:

$$\gamma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}; \gamma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix}$$

Então

$$\gamma_1\gamma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$$

Esse conjunto de elementos forma um grupo denominado grupo das permutações. O grupo das permutações de n elementos é designado por Γ_n e chamado grupo simétrico.

A.2.2 Grupo Cíclico

Uma potência n de um elemento a de um conjunto pode ser definida como sendo n repetições de uma operação sobre esse elemento, isto é, $a^n = a . a . a . \cdots$. Se, a partir de um elemento a, um conjunto com sequência de n elementos $a, a^2, \ldots, a^n = e$ pode ser gerado, então, este conjunto satisfaz todos os axiomas de grupo. Esse grupo é chamado grupo cíclico de ordem n, e o elemento a é chamado gerador. Vale ressaltar que todo grupo cíclico é abeliano mas nem todo grupo abeliano é cíclico.

A.2.3 Anel

Definição A.2.3. *Um anel ou anel comutativo $(A, +, \cdot)$ é um conjunto com pelo menos dois elementos, munido de uma operação denotado por $+$ (adição) e de uma operação denotada por $\cdot$ (multiplicação) que satisfazem as condições seguintes (quaisquer $a_1, a_2, a_3 \in A$):*

i) *Associatividade:* $(a_1 + a_2) + a_3 = a_1 + (a_2 + a_3)$ *e* $(a_1 \cdot a_2) \cdot a_3 = a_1 \cdot (a_2 \cdot a_3)$;

ii) *Comutatividade:* $a_1 + a_2 = a_2 + a_1$ *e* $a_1 \cdot a_2 = a_2 \cdot a_1$;

iii) *Elemento neutro:* $0 + a_1 = a_1$ *e* $1 \cdot a_1 = a_1$;

vi) *Elemento inverso:* $a_1 + a_2 = 0 = a_2 + a_1$;

v) $a_1 \cdot (m_1 + m_2) = a_1 \cdot m_1 + a_1 \cdot m_2$.

Caso a comutatividade não seja satisfeita, então o anel é chamado anel não comutativo.

Definição A.2.4. *Um anel $(k, +, \cdot)$ é chamado corpo se todo elemento diferente de 0 de k possui um inverso com respeito à multiplicação.*

A.2.4 Módulo

Definição A.2.5. *Sejam A um anel comutativo com unidade. Um grupo abeliano aditivo $(M, +)$ dotado de uma multiplicação escalar*

$$\begin{aligned} A \times M &\to M \\ (a, m) &\mapsto a \cdot m \end{aligned}$$

é dito um A-módulo, para quaisquer $a_1, a_2 \in A$ e $m_1, m_2 \in M$, se satisfaz os seguintes axiomas:

i) $1 \cdot m_1 = m_1$;

ii) $(a_1 \cdot a_2) \cdot m_1 = a_1 \cdot (a_2 \cdot m_1)$;

iii) $(a_1 + a_2) \cdot m_1 = a_1 \cdot m_1 + a_2 \cdot m_1$;

iv) $a_1 \cdot (m_1 + m_2) = a_1 \cdot m_1 + a_1 \cdot m_2$.

Sejam A um anel e M um A-módulo. O módulo M é dito finitamente gerado quando existe um número finito de elementos $m_1, \ldots, m_t$ de M ($t \in \mathbb{N}$) tais que

$$M = Am_1 + Am_2 + \cdots + Am_t = a_1 \cdot m_1 + \cdots + a_t m_t$$

sendo $\{a_1, \ldots, a_t\} \in A$ e $\{m_1, \ldots, m_t\}$ o conjunto de geradores para o módulo M e também pertencentes a um subconjunto de M.

A.3 Tópico em Representação de Grupos

A.3.1 Álgebra de Grupo

Considere o grupo G. Seja A o conjunto de elementos $\sum_R a_R R$ em que $a_R \in \mathbb{C}$ um número e um elemento $R \in G$. Se $\sum_R a_R R$ e $\sum_S b_S S$ são dois elementos de A e c é um número complexo, segue que

a) $\sum_R a_R R + \sum_R b_R R = \sum_R (a_R + b_R) R \in A$;

b) $(\sum_R a_R R) \times (\sum_S b_S S) = \sum_{R,S} a_R b_S RS \in A$;

c) $c(\sum_R a_R R) = \sum_R (c a_R) R \in A$;

A álgebra assim definida é chamada álgebra de grupo e os elementos $\sum_{R \in G} a_R R$ chamados elementos da álgebra.

Consideremos A como o espaço de representação de G. Neste caso as matrizes que constituirão a representação serão matrizes $n \times n$ em que n é a ordem do grupo. Com isso, temos:

i) Se R é algum elemento de G, sendo $G = \{E, R, S, T, ...\}$ e a base f_ν ($\nu = 1, 2, 3, \ldots, n$) de A, segue que:

$$R f_\nu = \sum_\mu \Gamma_{\mu\nu}(R) f_\nu$$

com f_ν elementos de G. Daí

$$\Gamma_{\mu\nu}(R) = \begin{cases} 1 & \text{se } R = f_\mu f_\mu^{-1} \\ 0 & \text{se } R \neq f_\mu f_\mu^{-1} \end{cases}$$

e para $\mu = \nu$ temos:

$$\Gamma_{\mu\mu}(R) = \begin{cases} 1 & \text{se } R = f_\mu f_\mu^{-1} = E \\ 0 & \text{se } R \neq E, \end{cases}$$

ou seja somente $\Gamma(E)$ terá elementos diagonais nulos;

b) Considerando os caracteres, a última expressão $\Gamma_{\mu\mu}$ segue que

$$X(R) = \begin{cases} n & \text{se } R = E \\ 0 & \text{se } R \neq E, \end{cases}$$

isto é, numa representação regular somente o elemento identidade possue carater diferente de zero.

APÊNDICE B – Complemento Sobre Estados Emaranhados

Desenvolvemos neste apêndice uma complementação da explicação sobre estados emaranhados [41].

Vamos mostrar que no estado $|\psi\rangle$ dado por (3.27) as polarizações lineares dos dois fótons são paralelas qualquer que seja a direção escolhida. Com esse objetivo, consideremos uma rotação T de ângulo φ no plano (xy) Assim, teremos (vide figura 8) a matriz

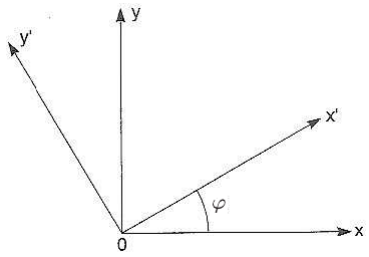


Figura 8: Rotação no plano (xy).

$T = \begin{pmatrix} \cos\varphi & -sen\varphi \\ sen\varphi & \cos\varphi \end{pmatrix}$. Daí,

$$x' = Tx = \begin{pmatrix} \cos\varphi & -sen\varphi \\ sen\varphi & \cos\varphi \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} \cos\varphi \\ sen\varphi \end{pmatrix} \equiv |0'\rangle\,, \tag{B.1}$$

e de forma similar tem-se

$$y' = Ty = \begin{pmatrix} \cos\varphi & -sen\varphi \\ sen\varphi & \cos\varphi \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} -sen\varphi \\ \cos\varphi \end{pmatrix} \equiv |1'\rangle\,. \tag{B.2}$$

Definimos o estado

$$|\psi'\rangle = \frac{1}{\sqrt{2}}[|0'\rangle_1 |0'\rangle_2 + |1'\rangle_1 |1'\rangle_2]. \tag{B.3}$$

Assim

$$|\psi'\rangle = \frac{1}{\sqrt{2}}\left[\begin{pmatrix} \cos\varphi \\ sen\varphi \end{pmatrix}_1 \otimes \begin{pmatrix} \cos\varphi \\ sen\varphi \end{pmatrix}_2 + \begin{pmatrix} -sen\varphi \\ \cos\varphi \end{pmatrix}_1 \otimes \begin{pmatrix} -sen\varphi \\ \cos\varphi \end{pmatrix}_2\right] \tag{B.4}$$

$$= \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix} = |\psi\rangle\,. \tag{B.5}$$

Q.E.D.

Referências

[1] Galvão, E. F. *O que é computação quântica?*. Rio de Janeiro: Vieira e Lent, (2007).

[2] Feynman, R. P. *Simulating physics with computers*, Int. J. Theor. Phys. **21**, 467 (1982).

[3] Nielsen, M. A.; Chuang, I. B. *Quantum Computation and Quantum Information*. United Kingdom: Cambridge University Press, (2001).

[4] Einstein, A.; Podolsky, B.; Rosen, N. *Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?*, Phys. Rev. **47**, 10 777 (1935).

[5] Bennett, C.H., Brassard, G., Crepeau, C., Jozsa, R., Peres, A.; Wootters, W. K., *Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels*, Phys. Rev. Lett. **70**, 1895 (1993).

[6] Shor, P. W.: *Algorithms for Quantum Computation: Discrete Logrithms and Factoring*. In S. Goldwasser, editor, Proceedings of the 35th Annual Symposium on the Foundations of Computer Science, p. 124-134, Los Alamitos,CA, 1994. IEEE Computer Society Press.

[7] Bennet, C. H.; Brassard, G., *Proceedings of IEEE International Conference on Computers, Systems Signal Processing, Bangalore, India*, IEEE, New York, p.175 (1984).

[8] Ekert, A. K., *Quantum cryptography based on Bell's theorem*, Phys. Rev. Lett. **67**, 661–663 (1991).

[9] Nayak,C.; Simon, S. H.; Stern, A.; Freedman, M.; Sarma, S. D., *Non-Abelian anyons and topological quantum computation*, Rev. Mod. Phys. **80**, 1083, (2008).

[10] Magnus,W., *Braid groups: A survey*. In Lecture Notes in Mathematics, Springer, **372** 463–487 (1974).

[11] Kassel, C.; Turaev, V. *Braid Groups*. New York: Springer, (2008).

[12] Kauffman, L. H., *Knots and Physics*. Singapore: World Scientific Publishers, (2002).

[13] Kauffman, L. H.; Lomonaco Jr., S. J. *Quantum Knots*, in E. Donkor, A.R.Pirich and H.E. Brandt (eds.), Quantum Information and Computation II, Spie Proceedings, (12-14 April, Orlando, FL, 2004), Vol. 5436, pp. 268–284.

[14] Kauffman, L. H.; Lomonaco Jr., S. J. *Quantum entanglement and topological entanglement*, New J. Phys. **4**, 73.1 (2002).

[15] Kauffman, L. H.; Lomonaco Jr., S. J. *Braiding operators are universal quantum gates*, New J. Phys. **6**, 134 (2004).

[16] Zhang, Y.; Kauffman, L. H.; Ge, M. L. *Universal Quantum Gate, Yang–Baxterization and Hamiltonian*, Int. J. Quant. Inf. **3**, 4 669 (2005).

[17] Zhang, Y. *AMS Contemporary Mathematics*, **482**, 51–92 (2009).

[18] Drinfeld, V. G. *Quantum Groups*. In Proc. Int. Cong. Math., Berkley, 798–820 (1987).

[19] Kitaev, A. Y. *Fault-tolerant quantum computation by anyons*, Ann. Phys. **303**, 2 (2003).

[20] Kitaev, A. Y., *Anyons in an exactly solved model and beyond*, Ann. Phys. **321**, 2 (2006).

[21] Kassel, C. *Quantum Groups*. New York: Springer-Verlag, (1995).

[22] Majid, S. *Quasitriangular Hopf algebras and Yang-Baxter equations*, Int. J. Mod. Phys. **A5**, 1–91 (1990).

[23] Abe, E., *Hopf Algebras*. Cambridge: Cambridge University Press, (1980).

[24] Chari, V.; Pressley, A., *A Guide to Quantum Groups*. Cambridge: Cambridge University Press, (1994).

[25] Majid, S. *Foundations of Quantum Group Theory*. Cambridge: Cambridge University Press, (1995).

[26] Sklyanin, E. K. *Some algebraic structures connected with the Yang-Baxter equation*, Funct. Anal. Appl. **16**, 4 263–270 (1982).

[27] Sklyanin, E. K. *Some algebraic structures connected with the Yang—Baxter equation. Representations of quantum algebras*, Funct. Anal. Appl. **17**, 4 273–284 (1982).

[28] Jimbo, M. *A q-difference analogue of U(g) and the Yang-Baxter equation*, Lett. Math. Phys. **10**, 63–69 (1985).

[29] Trindade, M. A. S.; Vianna, J D. M. *Non-extensive statistical entropy, quantum groups and quantum entanglement*, Physica A **391**, 3413–3416 (2012).

[30] Korbicz, J. K., Wehr, J., Lewenstein, M. *Entanglement and quantum groups*, J. Math. Phys. **50**, 062104 (2009).

[31] Bell, J. S. *On the Einstein Podolsky Rosen Paradox*, Phys. **1**, 195 (1964).

[32] Sweedler, M. E. *Hopf Algebras*. New York: W. A. Benjamin Inc., (1969).

[33] Pierce, R. S. *Associative Algebras*. New York: Springer-Verlag, (1982).

[34] Schutzer, W. *Álgebras de Lie, Álgebras de Hopf e Grupos Quânticos*. Dissertação (Mestrado em Matemática) - Instituto de Ciências Matemáticas, Universidade de São Paulo, São Paulo, (1996).

[35] Gonçalves, G. *Geometria de Fibrados Não-Comutativos*. Dissertação (Mestrado em Matemática) - Departamento de Matemática, Universidade Federal de Santa Catarina, Florianópolis, (2005).

[36] Mac Lane, S. *Categories for the Working Matematican*. New York: Springer-Verlag, (1998).

[37] Geroch, R. *Mathematical Physics*. Chicago: The University of Chicago Press, (1985).

[38] Castro, P. G.; Chakraborty, B.; Toppan, F. *Wigner oscillators, twisted Hopf algebras, and second quantization*, J. Math. Phys. **49** 8 082106 (2008).

[39] Castro, P. G.; Chakraborty, B.; Kullock, R.; Toppan, F. *Noncommutative oscillators from a Hopf algebra twist deformation. A first principles derivation*, J. Math. Phys. **52** 3 032102 (2011).

[40] Cunha, M. O. T. *Noções de Informação Quântica*. Rio de Janeiro: IMPA, (2007).

[41] Nussenzveig, H. M. *Curso de Física Básica 4*. São Paulo: Editora Blucher, (1998).

[42] Cunha, M. O. T. *Emaranhamento: Caracterização, Manipulação e Consequências*. Tese (Doutorado em Física) - Instituto de Física, Universidade Federal de Minas Gerais, Belo Horizonte, (2005).

[43] Sales, S. F. *Informação Quântica: Efeitos da Temperatura Utilizando a Dinâmica de Campos Térmicos*. Dissertação (Mestrado em Física) - Instituto de Física, Universidade Federal da Bahia, Salvador, (2011).

[44] Santos, D. C. *Em Busca de Um Entendimento Completo Acerca do Emaranhamento*. Dissertação (Mestrado em Física) - Instituto de Física, Universidade Federal de Minas Gerais, Belo Horizonte, (2006).

[45] Ekert, A.; Knight, P. L. *Entangled quantum systems and the Schmidt decomposition*, Am. J. Phys. **63**, 415 (1995).

[46] Peres, A. *Separability Criterion for Density Matrices*, Phys. Rev. Lett. **77**, 1413 (1996).

[47] Horodecki, M.; Horodecki, P.; Horodecki, R. *Separability of Mixed States: Necessary and Sufficient Conditions*, Phys. Lett. A **223**, 1 (1996).

[48] Simon, R. *Peres-Horodecki Separability Criterion for Continuous Variable Systems*, Phys. Rev. Lett. **84**, 2726 (2000).

[49] Vianna, J. D. M.; Trindade, M. A. S.; Fernandes, M. C. B. *Algebraic Criteria for Entanglement in Multipartite Systems*, Int. J. Theor. Phys. **47**, 961 (2008).

[50] Vedral, V.; Plenio, M. B.; Rippin, M. A.; Knight, P. L. *Quantifying Entanglement*, Phys. Rev. Lett. **78**, 2275 (1997).

[51] Bennett, C. H.; Wiesner, S. J. *Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states*, Phys. Rev. Lett. **69** 20, 2881-2884 (1992).

[52] Collins, G. P. *Nós quânticos na computação*. Scientific American Brasil, **48** 49–55 (2006).

[53] Pachos, J. *Introduction to Topological Quantum Computation*. United Kingdom: Cambridge University Press, (2012).

[54] Aldrovani, R.; Jr. Rocha, R. *A Geometria e a Física dos Nós e das Tranças*. São Paulo: Livraria da Física, (2013).

[55] Panagaden, P.; Paquete, E. O. *A categorical presentation of quantum computation with anyons*. Disponível em : <http://www.cs.mcgill.ca/ prakash/Pubs/MTCanyons.pdf>. Acesso em: 27 nov.2012.

[56] Preskill, J. *Lecture Notes for Physics 219: Quantum Computation*. cap.9. Disponível em: <http://www.theory.caltech.edu/ preskill/ph219/topological.pdf>. Acesso em: 20 set.2012.

[57] Albuquerque, C. D. *Análise e Construção de Códigos Quânticos Topológicos sobre Variedades Bidimensionais*. Tese (Doutorado em Engenharia Elétrica) - Faculdade de Engenharia Elétrica e Computação, Universidade Estadual de Campinas, Campinas, (2009).

[58] Cunha, M. H. *Um Estudo sobre Computação Quântica Topológica: Novas Portas para o Modelo de Fibonacci*. Dissertação (Mestrado em Engenharia Elétrica) - Faculdade de Engenharia Elétrica e Computação, Universidade Estadual de Campinas, Campinas, (2012).

[59] Camino, F. E.; Zhou, W.; Goldman, V. J. *Realization of a Laughlin quasiparticle interferometer: Observation of fractional statistics*, Phys. Rev. B. **72**, 075342 (2005).

[60] Jones, V. R. *Hecke algebra representations of braid groups and link polynomials*, Ann. Math. **126**, 335–388 (1987).

[61] Trindade, M. A. S. *Estruturas Algébricas em Informação Quântica e Dinâmica de Campos Térmicos*. Tese (Doutorado em Física) - Instituto de Física, Universidade Federal da Bahia, Salvador, (2010).

[62] Dye, H. A. *Unitary Solutions to the Yang–Baxter Equation in Dimension Four*, Quant. Inf. Proc. **2**, 117–150 (2003).

[63] Zhang, Y. *Teleportation, braid group and Temperley–Lieb algebra*, J. Phys. A **39**, 11599–11622 (2006).

[64] Pinto, E.; Trindade, M. A. S.; Vianna, J. D. M. *Quasitriangular Hopf Algebras, Braid Groups and Quantum Entanglement*, Int. J. Quant. Inf. **11**, 7 1350065 (2013).

[65] Klimyk, A.; Schüdgen, K. *Quantum Groups and Their Representations*. Berlin Heidelberg: Springer-Verlag, (1997).

[66] Hamermesh, M. *Group Theory and Its Apliccation to Physical Problems*. New York: Dover Publication, (1989).

[67] Monchon, C. *Anyon computers with smaller groups*, Phys. Rev. A **69**, 032306 (2004).

[68] Vianna, J. D. M. *Teoria de Grupos Aplicada à Física*. Notas de Aulas - Instituto de Física, Universidade Federal da Bahia, Salvador, (1979).

[69] Fazzio, A.; Watari, K. *Introdução à Teoria de Grupos aplicada em moléculas e sólidos*. Santa Maria: Editora UFSM, (2009).

[70] Garcia, A.; Lequain, Y. *Elementos de Álgebra*. Rio de Janeiro: IMPA, (2005).