
Um Estudo sobre Computação Quântica Topológica: Novas Portas para o Modelo de Fibonacci

Dissertação apresentada à Faculdade de Engenharia Elétrica e de Computação da Universidade Estadual de Campinas como parte dos requisitos exigidos para a obtenção do título de Mestre em Engenharia Elétrica. Área de concentração: Telecomunicações e Telemática.

por

Maicon Henrique Cunha

Orientador: **Prof. Dr. Reginaldo Palazzo Júnior** FEEC/UNICAMP

Co-orientador: **Dra. Clarice Dias de Albuquerque** FEEC/UNICAMP

Banca Examinadora:

Dra. Clarice Dias de Albuquerque(FEEC/UNICAMP) (Presidente)

Prof. Dr. Henrique Lazari (IGCE/UNESP-Rio Claro)

Prof. Dr. Romis Ribeiro de Faissol Attux(FEEC/UNICAMP)

FICHA CATALOGRÁFICA ELABORADA PELA
BIBLIOTECA DA ÁREA DE ENGENHARIA E ARQUITETURA - BAE - UNICAMP

C914e

Cunha, Maicon Henrique

Um estudo sobre computação quântica topológica: novas portas para o modelo de fibonacci / Maicon Henrique Cunha. --Campinas, SP: [s.n.], 2012.

Orientadores: Reginaldo Palazzo Júnior, Clarice Dias de Albuquerque.

Dissertação de Mestrado - Universidade Estadual de Campinas, Faculdade de Engenharia Elétrica e de Computação.

1. Computação quântica. 2. Anyons. 3. Topologia. 4. Grupos. I. Palazzo Júnior, Reginaldo. II. Albuquerque, Clarice Dias de. III. Universidade Estadual de Campinas. Faculdade de Engenharia Elétrica e de Computação. IV. Título.

Título em Inglês: A Study on topological quantum computation: new gates to the fibonacci model

Palavras-chave em Inglês: Quantum computation, Anyons, Topology, Groups

Área de concentração: Telecomunicações e Telemática

Titulação: Mestre em Engenharia Elétrica

Banca examinadora: Henrique Lazari, Romis Ribeiro de Faissol Attux

Data da defesa: 29-02-2012

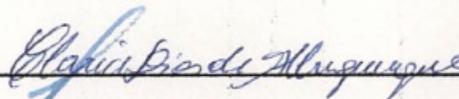
Programa de Pós Graduação: Engenharia Elétrica

Candidato: Maicon Henrique Cunha

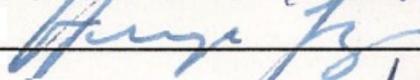
Data da Defesa: 29 de fevereiro de 2012

Título da Tese: "Um Estudo sobre Computação Quântica Topológica: Novas Portas para o Modelo de Fibonacci"

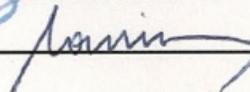
Dra. Clarice Dias de Albuquerque (Presidente):



Prof. Dr. Henrique Lazari:



Prof. Dr. Romis Ribeiro de Faissol Attux:



Agradecimentos

À UNICAMP e à FEEC, por possibilitarem um excelente ambiente de pesquisa.

Ao meu orientador Reginaldo Palazzo Jr., uma pessoa admirável por sua educação, conhecimento e humildade. Uma pessoa disposta a desbravar fronteiras da ciência e incumbir em seus alunos esse espírito inovador. Obrigado por acreditar em mim e ser meu orientador.

A minha co-orientadora Clarice Dias Albuquerque, por todas as discussões importantíssimas nesse trabalho. Obrigado também por aceitar esse desafio e ser minha co-orientadora.

A todos os professores que tive na minha vida, pois cada parte desse trabalho tem um pouco de cada um deles.

A CAPES pelo auxílio financeiro fornecendo minha bolsa de estudos.

Aos amigos e familiares pela convivência e por terem me apoiado sempre.

Aos amigos do LTIA pela boa convivência.

Aos membros da banca por aceitarem o convite, pela atenção dedicada a este trabalho, pelas sugestões e considerações.

A todos que, direta ou indiretamente, contribuíram para a conclusão deste trabalho.

*Um amor, uma carreira, uma
revolução. Outras tantas coisas que se
começam sem saber como acabarão.*

Jean Paul Sartre

*A mente que se abre a uma nova idéia
jamais voltará ao seu tamanho original.*

Oliver Wendell Holmes

Resumo

Neste trabalho, apresentamos um estudo sobre Computação Quântica Topológica, uma área de pesquisa inserida na computação quântica que busca resolver o problema da decoerência na construção do computador quântico de uma maneira inovadora. Essa computação envolve aspectos de áreas distintas relacionadas a mecânica quântica: teoria de grupos, representação de grupo, anyons e outras. Por isso, uma fundamentação teórica básica nesses tópicos é necessária e será apresentada para embasar o modelo geral de Computação Quântica Topológica. O modelo de Fibonacci é um caso específico que será tratado com ênfase por ser o mais difundido e o único universal conhecido até o momento. Com o modelo de Fibonacci, construímos novas portas quânticas, cuja análise possibilitou conclusões e um refinamento no algoritmo existente para encontrar tais portas.

Palavras-Chave: computação quântica topológica, computação quântica, anyons, grupo de trança, anyons de Fibonacci.

Abstract

In this work, we present a study about Topological Quantum Computation, a research area included in quantum computation that seeks to solve the problem of decoherence in building a quantum computer according to an innovative way. This involves computing aspects of different areas related to quantum mechanics: group theory, group representation, anyons and others. Thus a basic theoretical foundation in these topics is necessary and will be presented to support the general model of Topological Quantum Computation. The Fibonacci model is a particular case, which will be discussed with emphasis, being the most widespread and the only universally known until this moment. With the Fibonacci model, we construct new quantum gates, whose analysis allowed a number of conclusions to be drawn, as well as a refinement of the existing algorithm to find such ports.

Key-words: topological quantum computation, quantum computation, anyons, braid group, Fibonacci anyons.

Conteúdo

Agradecimentos	iv
Epígrafe	v
Resumo	vi
Abstract	vii
Conteúdo	viii
Lista de Figuras	x
Lista de Tabelas	xii
1 Introdução	1
1.1 O Novo Mundo Quântico	1
1.2 Origens da Computação Quântica	3
1.2.1 Vantagens da computação quântica	4
1.2.2 Computação quântica topológica	4
1.3 Proposta do Trabalho	5
1.4 Descrição da Dissertação	5
2 Conceitos Básicos	7
2.1 Computação Quântica	7
2.1.1 O bit quântico	7
2.1.2 Portas quânticas	8
2.1.3 Universalidade em computação quântica	10
2.2 Grupo de Permutação	11
2.3 Grupo de Trança	12
2.3.1 Representações do Grupo de Trança	13

3	Computação Quântica Bidimensional	17
3.1	O Surgimento dos Anyons	17
3.1.1	O efeito Hall quântico fracionário	19
3.2	A Dinâmica dos Anyons	20
3.2.1	Espaços de fusão	20
3.2.2	O operador de trança R	21
3.2.3	O operador de mudança de base F	22
3.2.4	O operador de trança B	23
3.2.5	Axiomas de consistência	24
3.3	Modelo Geral de Computação Quântica Topológica	26
4	Computação Quântica via Modelo de Fibonacci	28
4.1	Leis de Fusão dos Anyons de Fibonacci	28
4.1.1	Anyons de Fibonacci e o Espaço de Hilbert	30
4.2	Construção das Matrizes do Modelo de Fibonacci a Partir dos Axiomas de Consistência	32
4.2.1	A matriz F	33
4.2.2	A matriz R	34
4.2.3	A matriz B	35
4.3	Construção das Matrizes do Modelo de Fibonacci a Partir da Álgebra de Temperley-Lieb	35
4.3.1	As matrizes R e F	36
4.4	Construção das Portas de Um Qubit do Modelo de Fibonacci	39
4.4.1	Porta i-NOT	42
4.5	Construção de Portas de Dois Qubits do Modelo de Fibonacci	43
4.5.1	Porta i-CNOT	44
4.6	Novas Portas de Um Qubit do Modelo de Fibonacci	45
4.7	Além dos Anyons de Fibonacci	47
5	Conclusões	48
	Bibliografia	50
A	Apêndice A: programas utilizados para gerar novas portas	53

Lista de Figuras

2.1	Esfera de Bloch.	8
2.2	Geradores do grupo de trança de ordem n	12
2.3	Elemento inverso e elemento neutro em B_3	12
2.4	Operações em B_4	13
2.5	Geradores de B_3	13
2.6	Geradores da álgebra de Temperley-Lieb.	14
2.7	Propriedades 1 e 2 da álgebra de Temperley-Lieb.	15
3.1	Bóson e Férmions.	18
3.2	Permutação e entrançamentos.	18
3.3	Representação gráfica do vetor da base e seu dual.	21
3.4	Matriz de entrançamento R	22
3.5	Dois modos de fusão de três partículas.	22
3.6	Matriz F de mudança de ordem de fusão.	23
3.7	Matriz de entrançamento B	23
3.8	Matriz B em função de R e F	24
3.9	Axioma do pentágono.	25
3.10	Axioma do hexágono.	25
3.11	Modelo geral de CQT.	27
4.1	Anyons de Fibonacci e o espaço de Hilbert.	31
4.2	Bases do modelo de Fibonacci.	31
4.3	Modelo de Fibonacci de CQT.	32
4.4	Bases do modelo de Fibonacci.	36
4.5	Entrançamentos do modelo de Fibonacci.	36
4.6	Interpretação da matriz F	37
4.7	A álgebra de Temperley-Lieb e as tranças.	38
4.8	A álgebra de Temperley-Lieb e as tranças para o caso $n=5$	38
4.9	Exemplo de porta de um qubit do modelo de Fibonacci.	40

4.10 Exemplo de <i>weave</i> em B_3	41
4.11 Exemplo de trança efetiva.	42
4.12 Porta i-NOT do modelo de Fibonacci.	42
4.13 Portas de dois qubits do modelo de Fibonacci.	43
4.14 Porta não efetiva.	44
4.15 Porta injeção.	44
4.16 Modelo da porta i-CNOT.	45
4.17 A porta iH.	46
4.18 A porta iZ.	46
4.19 A porta XZ.	46

Lista de Tabelas

4.1	Operações em $SU(2)_3$	29
4.2	Definição de $0 \equiv [0, \frac{3}{2}]$ e $1 \equiv [\frac{1}{2}, 1]$ em $SU(2)_3$	29
4.3	Resultado da definição de $0 \equiv [0, \frac{3}{2}]$ e $1 \equiv [\frac{1}{2}, 1]$ em $SU(2)_3$	30

Introdução

A invenção do transistor ficou marcada no século XX e possibilitou entre outras coisas a evolução dos microprocessadores e a revolução tecnológica decorrente desse processo. Porém outras revoluções na ciência estavam em curso, como a física quântica e seus subprodutos que agora começam a despontar em áreas como criptografia e computação.

A computação quântica surge como uma nova alternativa para a computação tradicional. Provavelmente seja um novo paradigma [24], já que alguns algoritmos quânticos se mostram muito mais rápidos [29, 24] que os equivalentes clássicos. Além disso a miniaturização dos processadores atuais está cada vez mais se aproximando do raio de relevância da mecânica quântica e, por isso, essa nova alternativa também é necessária.

A Computação Quântica Topológica [20] é uma linha de pesquisa dentro da computação quântica e se preocupa em resolver alguns problemas presentes na construção do computador quântico de uma maneira inovadora.

Neste capítulo, é feita uma breve revisão histórica dos processos que levam a mecânica quântica e sua conexão com o mundo real através dos postulados. Em seguida, é feita uma introdução à computação quântica, e apresentado seu histórico e suas vantagens. É apresentada também a motivação para se estudar a computação quântica topológica, objeto de estudo desta dissertação. Por fim, descrevemos nosso objetivo e como ele será tratado na dissertação.

1.1 O Novo Mundo Quântico

Os primórdios da mecânica quântica datam do final do século XIX, quando Max Planck oferece ao mundo uma maneira de solucionar o problema da catástrofe do ultravioleta. Planck descreve o processo de produção de luz de corpos aquecidos através de pacotes de energia, denominados “quanta”,

que significa quantidade em Latim. Porém como dito por Planck “*Tratou-se de uma hipótese puramente formal, e não refleti muito sobre ela, mas apenas sobre o fato de que, sobre quaisquer circunstâncias, custasse o que custasse, um resultado positivo tinha de ser obtido*”¹. Mal sabia o quão abrangente e consistente se tornaria a teoria que ajudou a criar.

Apesar de inicialmente a proposta de Planck ter sido bastante debatida, mesmo com certas ressalvas, alguns pesquisadores a utilizaram. Um exemplo foi Einstein, que, em 1905, em um de seus cinco célebres artigos, propõe a quantização do campo eletromagnético e, com isso, explica entre outros fenômenos o efeito fotoelétrico, que lhe rende o prêmio Nobel de Física em 1921.

Além de Einstein, Bohr, Heisenberg e Schrödinger também desenvolvem trabalhos nessa fase construtiva da mecânica quântica, sendo os dois últimos nomes citados em associação com o processo de formalização da teoria quântica, processo esse que se estabelece plenamente em 1926 com Paul Dirac.

A mecânica quântica preocupa-se em estudar sistemas físicos nos quais os efeitos quânticos são relevantes, e isso se dá próximo ou abaixo da escala atômica; porém ela deve ser compatível com a física clássica em escala macroscópica, sendo dessa maneira mais universal. Matematicamente falando, ela é uma estrutura para o estudo de teorias físicas e a conexão com o mundo real é dada através dos postulados da mecânica quântica [24].

Postulado 1

A qualquer sistema físico isolado existe associado um espaço vetorial complexo com produto interno (ou seja, um espaço de Hilbert), conhecido como espaço de estados do sistema. O sistema é completamente descrito pelo seu vetor de estado, um vetor unitário no espaço de estados.

Postulado 2

A evolução de um sistema quântico fechado é descrita por uma transformação unitária. Ou seja, o estado $|\psi\rangle$ de um sistema em um tempo t_1 está relacionado ao estado $|\psi'\rangle$ do sistema em t_2 por um operador unitário U que depende somente de t_1 e t_2 :

$$|\psi'\rangle = U|\psi\rangle.$$

Postulado 2'

A evolução temporal do estado de um sistema quântico fechado é descrita pela equação de

¹H. Fleming, Max Planck e a Idéia do Quantum de Energia. In: M. Hussein e S. Salinas (Orgs.). 100 Anos de Física Quântica (Editora Livraria da Física, São Paulo, 2001), p. 10.

Schrödinger:

$$i\hbar \frac{d|\psi\rangle}{dt} = H|\psi\rangle.$$

Nessa equação, \hbar é uma constante física chamada de constante de Planck, cujo valor é determinado experimentalmente. Na prática, é comum absorver o fator \hbar dentro de H , efetivamente convencionando-se $\hbar = 1$. H é um operador Hermitiano conhecido como Hamiltoniano do sistema.

Postulado 3

As medidas quânticas são descritas por determinados operadores de medida $\{M_m\}$. Esses operadores atuam sobre o espaço de estados do sistema. O índice m se refere aos possíveis resultados da medida.

Postulado 4

O espaço de estados de um sistema físico composto é o produto tensorial dos espaços de estados dos sistemas individuais.

Interpretando os postulados vemos que o primeiro postulado estabelece a arena para a mecânica quântica, já o postulado 2 nos diz que a dinâmica de um sistema fechado é governada pela equação de Schrödinger e, portanto, por transformações unitárias. O postulado 3 especifica como extrair informações de sistemas quânticos e o postulado 4 estabelece como compor diferentes sistemas quânticos.

Algumas propriedades da mecânica quântica decorrentes dos postulados são, a princípio, estranhas, como a impossibilidade de observar diretamente um vetor de estado e o fato de que a observação em mecânica quântica é um processo invasivo que muda o estado do sistema. No entanto, essas propriedades contra-intuitivas são fundamentais para a computação quântica.

1.2 Origens da Computação Quântica

A ciência da computação moderna se inicia com o artigo de Alan Turing em 1936, onde é descrita a noção abstrata de computador programável e, não muito tempo depois desse artigo, surgiram os primeiros computadores construídos a partir de componentes eletrônicos. Além disso, a formulação da tese de Church-Turing que estabelece que qualquer algoritmo pode ser simulado por uma máquina de Turing universal se tornou amplamente aceita e estabeleceu bases para o desenvolvimento de uma teoria da computação.

No final da década de 1960 e início da década de 1970, a tese de Church-Turing foi modificada para uma versão mais forte, porém, problemas como o algoritmo de Solovay-Strassen sobre a fatoração de primos e a computação analógica levaram a uma modificação ad-hoc na tese forte de Church-Turing.

Motivado pelo problema de enunciar um modelo de computação universal, Deutsch, em 1985, perguntou se as leis da física poderiam ser utilizadas para derivar uma versão ainda mais forte da tese de Church-Turing e, como as leis da física são em última análise quânticas, Deutsch foi naturalmente levado a considerar aparatos quânticos, e isso culminou na concepção moderna de computador quântico [24].

1.2.1 Vantagens da computação quântica

Dois são os pilares fundamentais que explicam a necessidade de se construir um computador quântico. O primeiro está relacionado com a miniaturização dos componentes dos processadores, que se deve à busca por maior rapidez no processo de computação. Essa miniaturização poderá levar a processos que se aproximem do raio de relevância da mecânica quântica, que, portanto, deverá ser levada em consideração no futuro na construção de computadores. Porém, o mais fascinante na mecânica quântica são os algoritmos que propiciam ganho de velocidade com relação à computação clássica.

Boa parte do problema de se transmitir informações entre pessoas de maneira privada com a velha arte da criptografia reside na dificuldade da transmissão de chaves de maneira confiável: isso é feito em [28] e em [5] utilizando os problemas do logaritmo discreto e da fatoração de números grandes. No entanto, para surpresa da comunidade científica, Shor propõe, em 1994, um algoritmo [29], em que soluciona os problemas apresentados em [28, 5] com redução exponencial em termos de complexidade computacional através da computação quântica, sendo esse realmente um fator importante e que motivou estudos na área, já que o sistema RSA e similares são amplamente utilizados até hoje.

Além do algoritmo de Shor, outro algoritmo importante é o de Grover, que faz a busca em uma lista com redução quadrática em termos de complexidade computacional. E apesar de o ganho não ser extraordinário, é de extrema importância, pois esse processo é corriqueiro em computação.

1.2.2 Computação quântica topológica

No desenvolvimento do computador quântico, muitas dificuldades são recorrentes, sendo uma das principais a *decoerência*, que é a perda de informação quando o sistema quântico interage com o ambiente. Para lidar com esse problema, foram propostos os códigos corretores de erros quânticos [26, 1],

em princípio utilizando ideias semelhantes aos códigos corretores de erros clássicos, mas com o viés da computação quântica. Porém, dentre os códigos corretores de erros quânticos, Kitaev [20] propõe uma linguagem alternativa utilizando topologia, possibilidade já considerada por Michael H. Freedman em 1988, mas só posteriormente publicada [23]. A ideia foi utilizar certas propriedades de partículas confinadas em um plano para realizar computação quântica, partículas estas chamadas *anyons*. As propriedades do sistema estariam relacionadas à topologia do sistema físico: assim, deformações contínuas causadas pelo ambiente não seriam capazes de alterar tais propriedades. Essa proposta de Kitaev dá origem à Computação Quântica Topológica (CQT), como observado em [23], uma das áreas mais notáveis de desenvolvimento envolvendo processos quânticos. Essa computação é naturalmente tolerante a falhas, já que a proteção da informação ocorre durante o processo de computação.

1.3 Proposta do Trabalho

A partir da proposta inicial de Kitaev [20], houve um grande avanço na CQT, como a construção do modelo geral de computação [27], a construção de portas de modelos específicos que levam a universalidade [2], a descrição algébrica da dinâmica de anyons apresentada em [25] e referências, a partir da teoria de categoria, além da abordagem distinta desses mesmos problemas apresentada em [17, 19].

A construção propriamente dita do computador quântico topológico esbarra na dificuldade física de encontrar e controlar essas partículas bidimensionais responsáveis por realizar a CQT, os anyons, mas também possui entraves teóricos que serão abordados nesse trabalho. Acreditamos que, assim como aconteceu com a computação clássica, é preciso um desenvolvimento teórico da CQT para estabelecer um avanço tecnológico pleno, sendo esse o nosso ponto de partida.

Neste trabalho, são apresentados os diversos avanços obtidos na área de CQT, com abordagens e enfoques diferentes, de uma maneira organizada e crítica. Também serão mostradas novas portas quânticas para um modelo específico de CQT, além de propostas de trabalhos futuros em alguns pontos específicos. Pretende-se, com isso, tornar a CQT mais acessível e encorajar futuras pesquisas nessa área ainda pouco difundida no Brasil.

1.4 Descrição da Dissertação

Esta dissertação está organizada da seguinte maneira:

O **Capítulo 2** contém elementos básicos para o entendimento da CQT. Possui seções independentes que tratam da computação quântica, do grupo de permutação e do grupo de trança.

O **Capítulo 3** é dedicado exclusivamente aos anyons, objetos fundamentais da CQT. A maneira como naturalmente surgem em sistemas quânticos bidimensionais, seu embasamento físico e sua dinâmica são abordados. Por fim, apresentamos um modelo geral de CQT.

O **Capítulo 4** é dedicado, em boa parte, ao modelo de Fibonacci, o único modelo de CQT universal conhecido até o momento. São mostradas as leis de fusão, a construção das matrizes de representação de duas maneiras diferentes, a construção das portas de um qubit e a construção de uma porta de dois qubits. São apresentadas também novas portas de um qubit para o modelo de Fibonacci, e, um novo algoritmo para encontrar tais portas. Por fim, é mostrado o que existe na literatura além dos anyons de Fibonacci.

No **Capítulo 5** são apresentadas as conclusões e sugestões de trabalhos futuros.

Conceitos Básicos

Na primeira seção deste capítulo, é feita uma abordagem dos processos que envolvem computação quântica. O bit quântico, as portas quânticas e a questão da universalidade em computação quântica são assuntos tratados. Na segunda seção, o grupo de permutação é abordado. E, por fim, o grupo de trança e suas representações são explorados na última seção. Essas seções são independentes, contudo, estão intimamente relacionadas à CQT.

2.1 Computação Quântica

A computação quântica é baseada em premissas quânticas, e isso possibilita novos conceitos sobre a unidade fundamental denominada *qubit*, novas possibilidades de portas básicas e de conjuntos universais. A arena em que a computação quântica é realizada são os espaços vetoriais complexos com produto interno, chamados espaços de Hilbert.

2.1.1 O bit quântico

O análogo na computação quântica do bit clássico é denominado *bit quântico* ou *qubit*, e, ao contrário do bit clássico, que assume apenas dois valores, o qubit pode assumir uma infinidade de valores, uma vez que sua caracterização se dá através das superposições dos estados $|0\rangle$ e $|1\rangle$, isto é,

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle,$$

onde $\alpha, \beta \in \mathbb{C}$ com $|\alpha|^2 + |\beta|^2 = 1$. Porém, é importante salientar que, apesar de o qubit ser caracterizado como uma superposição de estados, no momento em que é feita a medida, o estado colapsa para $|0\rangle$ com probabilidade α^2 e $|1\rangle$ com probabilidade β^2 .

Como o qubit é um vetor unitário em um espaço de Hilbert, é possível visualizá-lo através da *esfera de Bloch*, como mostrado na Figura 2.1.

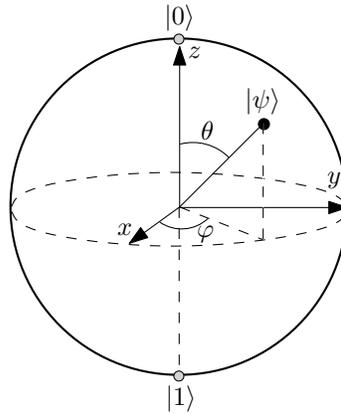


Figura 2.1: Esfera de Bloch.

O qubit também pode ser representado na forma matricial, partindo de:

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \quad |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}.$$

Desse modo, a superposição $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ pode ser escrita da seguinte maneira:

$$|\psi\rangle = \begin{bmatrix} \alpha \\ \beta \end{bmatrix}.$$

Essa representação é importante para entender as operações que são realizadas sobre qubits, ou seja, como operar com as portas quânticas.

No caso geral de n qubits, podemos ter 2^n superposição dos estados, $|00\dots 0\rangle, |00\dots 1\rangle, \dots, |11\dots 1\rangle$, que são representados por:

$$|v\rangle = \sum_{i=0}^{2^n-1} \alpha_i |i\rangle,$$

satisfazendo a condição

$$\sum_{i=0}^{2^n-1} |\alpha_i|^2 = 1.$$

2.1.2 Portas quânticas

Na computação clássica, existem apenas duas portas de um bit: uma é trivial, a identidade, e a outra é a NOT. Podemos nos perguntar primeiramente quais são os análogos quânticos dessas portas.

Utilizando a representação matricial, verificamos que a porta identidade para um qubit pode ser expressa da seguinte maneira:

$$I \equiv \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

visto que $I(|\psi\rangle) \stackrel{def}{=} I \cdot |\psi\rangle = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} \alpha \\ \beta \end{bmatrix}$.

A porta quântica análoga à NOT pode ser representada por

$$X \equiv \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

visto que $X(|1\rangle) = |0\rangle$ e $X(|0\rangle) = |1\rangle$.

A condição necessária para que uma matriz $M_{2n \times 2n}$ com coeficientes em \mathbb{C} seja uma porta quântica de n qubits é que ela seja unitária¹, ou seja, $M^\dagger M = MM^\dagger = I$. Matrizes com essa característica fazem parte do grupo $SU(n)$, onde n é a dimensão da matriz e a operação é a multiplicação de matrizes. Note que essa propriedade é satisfeita por I e por X .

As principais portas de um qubit são conhecidas como *matrizes de Pauli* e são representadas por:

$$I \equiv \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad X \equiv \sigma_x \equiv \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix},$$

$$Y \equiv \sigma_y \equiv \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \quad Z \equiv \sigma_z \equiv \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

Outra porta de um qubit importante é a *Hadamard*, que gera estados emaranhados:

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}.$$

A CNOT é um exemplo de porta de dois qubits:

$$\text{CNOT} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}.$$

Analisando a porta CNOT, podemos verificar que sua atuação pode ser separada em dois qubits, o qubit de controle e o qubit alvo. Assim, se o qubit de controle estiver no estado $|0\rangle$, o qubit alvo não é alterado, porém se o qubit de controle estiver no estado $|1\rangle$, então é feita a operação X no qubit alvo, disso decorre o nome *Controlled-Not*, ou não-controlado em português.

¹O símbolo \dagger na equação de unitariedade indica a matriz conjugada transposta.

2.1.3 Universalidade em computação quântica

Primeiramente, definiremos o *produto tensorial* de dois espaços de Hilbert.

Definição 1 (Produto tensorial) *Sejam V e W espaços de Hilbert de dimensões m e n respectivamente. O produto tensorial $V \otimes W$ é um espaço vetorial de dimensão mn , cujos elementos são combinações lineares de produtos tensoriais $|v\rangle \otimes |w\rangle$ dos elementos $|v\rangle \in V$ e $|w\rangle \in W$. O produto tensorial deve satisfazer as propriedades:*

- $z(|v\rangle \otimes |w\rangle) = (z|v\rangle) \otimes |w\rangle = |v\rangle \otimes (z|w\rangle)$, onde $|v\rangle \in V$, $|w\rangle \in W$ e $z \in \mathbb{C}$;
- $(|v_1\rangle + |v_2\rangle) \otimes |w\rangle = |v_1\rangle \otimes |w\rangle + |v_2\rangle \otimes |w\rangle$, onde $|v_1\rangle, |v_2\rangle \in V$ e $|w\rangle \in W$;
- $|v\rangle \otimes (|w_1\rangle + |w_2\rangle) = |v\rangle \otimes |w_1\rangle + |v\rangle \otimes |w_2\rangle$, onde $|v\rangle \in V$ e $|w_1\rangle, |w_2\rangle \in W$.

Além disso, se A e B são operadores em V e W , pode-se definir o operador $A \otimes B$ em $V \otimes W$ como

$$(A \otimes B)(|v\rangle \otimes |w\rangle) \equiv A|v\rangle \otimes B|w\rangle. \quad (2.1)$$

Como exemplo, considere $A_{2m \times 2m}$, $B_{2n \times 2n}$ portas quânticas de m e n qubits respectivamente, então $A \otimes B$ é dado pela matriz $4mn \times 4mn$

$$A \otimes B = \begin{bmatrix} a_{11}B & a_{12}B & \dots & a_{1(2m)}B \\ a_{21}B & a_{22}B & \dots & a_{2(2m)}B \\ \vdots & \vdots & \ddots & \vdots \\ a_{(2m)1}B & a_{(2m)2}B & \dots & a_{(2m)(2m)}B \end{bmatrix},$$

onde a_{ij} é o elemento localizado na linha i e coluna j da matriz A e cada termo $a_{ij}B$ denota uma sub-matriz $2n \times 2n$ cujos elementos são os produtos de a_{ij} por cada elemento da matriz B .

Com isso, podemos introduzir o conceito de *universalidade* em computação quântica.

Definição 2 (Portas quânticas universais) *Sejam U e V portas quânticas. U é dita universal se qualquer porta V puder ser decomposta em função de U e de um conjunto de portas de um qubit. Nesse caso, decompor V significa escrever V como produto de portas que são produto tensorial de U por portas de um qubit.*

Como exemplo de porta universal temos a CNOT [24]. Observe que podemos decompor a porta V , descrita abaixo, como:

$$V = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & -1 & 0 \end{bmatrix} = (I \otimes Y). \text{CNOT}. (I \otimes Y).$$

2.2 Grupo de Permutação

O grupo de permutação desempenha papel importante na evolução de sistemas quânticos tridimensionais. Basicamente, o grupo de permutação é formado por todas as bijeções de um conjunto finito nele mesmo, com a operação composição de funções. O conteúdo desta seção está contido em [6], assim como as demonstrações que serão omitidas.

Como podemos colocar um conjunto finito em bijeção com o conjunto $\{1, 2, \dots, n\}$ temos a seguinte definição.

Definição 3 (Grupo de Permutação S_n) *Seja A o conjunto finito $\{1, 2, \dots, n\}$, o grupo de todas as permutações de A é denotado por S_n .*

Um exemplo de grupo de permutação é o S_3 , cujos elementos são:

$$\sigma_0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad \sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \quad \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix},$$

$$\sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \quad \sigma_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad \sigma_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}.$$

Como exemplo de operação, considere a composição $\sigma_1 \circ \sigma_4$ em S_3 , realizada da esquerda para a direita. Temos então:

- $1 \rightarrow 1 \rightarrow 2$;
- $2 \rightarrow 3 \rightarrow 1$;
- $3 \rightarrow 2 \rightarrow 3$.

Com isso, conclui-se que $\sigma_1 \circ \sigma_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \sigma_3$. Além disso, toda permutação de S_n pode ser escrita de uma maneira mais conveniente através de *transposições*.

Definição 4 (Transposições em S_n) *Uma transposição em S_n é uma permutação que não altera $n - 2$ elementos e troca os dois restantes.*

Do exemplo sobre S_3 , vemos que σ_1, σ_2 e σ_3 são transposições.

Corolário 1 *Toda permutação σ em S_n pode ser escrita como o produto de transposições.*

A Definição 5 está relacionada ao número de transposições na decomposição de uma permutação.

Definição 5 (Sinal de uma permutação em S_n) *O sinal de uma permutação σ , $\text{sin}(\sigma)$, é 0 se σ for escrita com um número par de multiplicação de transposições e 1 se for escrita com um número ímpar.*

2.3 Grupo de Trança

O grupo de trança é mais rico que o grupo de permutação pois considera a ordem em que ocorrem as trocas dos elementos. O grupo de trança de ordem n será denotado por B_n , do inglês *braid*, que significa trança. Geometricamente, cada elemento pode ser visto como entrançamentos de n cordas presas em cima e em baixo por barras horizontais. Uma maneira conveniente de representar os elementos do grupo de trança é em função dos geradores do grupo. Na Figura 2.2 são mostrados os $n - 1$ geradores de um grupo de trança de ordem n .

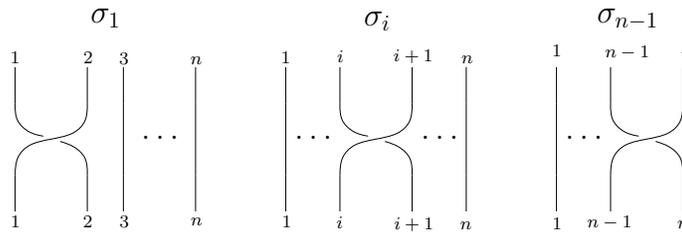


Figura 2.2: Geradores do grupo de trança de ordem n .

O elemento inverso de um grupo de trança é obtido trocando-se a ordem de entrançamentos, e o elemento neutro I é composto de cordas verticais sem nenhum entrançamento, como mostrado na Figura 2.3.

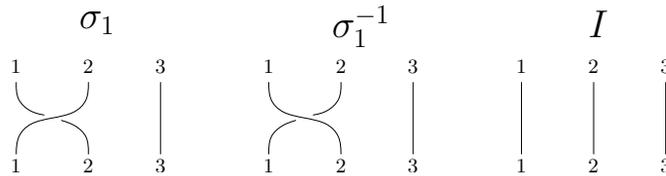


Figura 2.3: Elemento inverso e elemento neutro em B_3 .

A operação de composição entre os geradores do grupo de trança é realizada através de justaposição vertical de cada elemento em sequência. A Figura 2.4 ilustra um exemplo de uma sequência dada por $\sigma_1 \sigma_2^{-1} \sigma_3$ em termos dos geradores do grupo.

Definição 6 (Grupo de Trança) *Seja B_n , consistindo dos geradores $\sigma_1, \sigma_2, \dots, \sigma_{n-1}$ com as seguintes relações, $\sigma_i \sigma_j \sigma_i = \sigma_j \sigma_i \sigma_j$ se $|i - j| = 1$ e $\sigma_i \sigma_j = \sigma_j \sigma_i$ se $|i - j| \geq 2$. Denotaremos B_n por*

$$B_n = \left\langle \sigma_1, \sigma_2, \dots, \sigma_{n-1} \left| \begin{array}{ll} \sigma_i \sigma_j \sigma_i = \sigma_j \sigma_i \sigma_j & \text{se } |i - j| = 1 \\ \sigma_i \sigma_j = \sigma_j \sigma_i & \text{se } |i - j| \geq 2 \end{array} \right. \right\rangle.$$

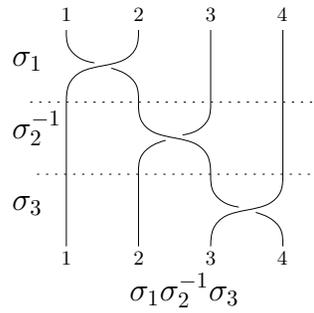


Figura 2.4: Operações em B_4 .

Considere como exemplo o grupo de trança B_3 . Como mostrado na Figura 2.5, os geradores de B_3 , σ_1 e σ_2 obedecem a relação $\sigma_1 \sigma_2 \sigma_1 = \sigma_2 \sigma_1 \sigma_2$. Essa é uma relação importante e está conectada fortemente aos anyons de Fibonacci, como veremos no capítulo 4.

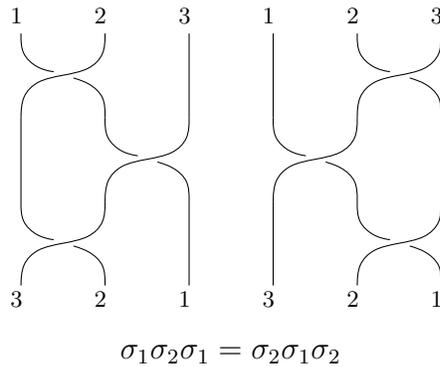


Figura 2.5: Geradores de B_3 .

2.3.1 Representações do Grupo de Trança

Representações do grupo de trança são de fundamental importância na CQT. Apresentaremos nesta seção duas maneiras distintas de se obter representações do grupo de trança. A primeira é a partir de soluções da equação de Yang-Baxter.

Seja R solução da equação da equação de *Yang-Baxter*:

$$(R \otimes I)(I \otimes R)(R \otimes I) = (I \otimes R)(R \otimes I)(I \otimes R). \tag{2.2}$$

E R com dimensão 4×4 . Uma representação do grupo de trança B_n por matrizes $2^n \times 2^n$ é dada por:

$$\sigma_i = I \otimes \dots \otimes R \otimes \dots I \quad (i = 1, \dots, n - 1). \tag{2.3}$$

A equação (2.3) envolve $n - 1$ matrizes, e a matriz R atua no i -ésimo termo do produto tensorial. Os outros termos são matrizes identidades I de dimensão 2. Em [16] são mostradas três soluções para a equação(2.2), sendo uma dessas soluções a seguinte matriz,

$$R = \begin{pmatrix} \frac{1}{\sqrt{2}} & 0 & 0 & \frac{1}{\sqrt{2}} \\ 0 & \frac{1}{\sqrt{2}} & \frac{-1}{\sqrt{2}} & 0 \\ 0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 \\ \frac{-1}{\sqrt{2}} & 0 & 0 & \frac{1}{\sqrt{2}} \end{pmatrix}.$$

Que assim como a CNOT pode ser vista com uma porta quântica universal.

A outra representação do grupo de trança é obtida a partir da *álgebra de Temperley-Lieb*.

Definição 7 A *álgebra de Temperley-Lieb* de ordem n , denotada por TL_n possui os seguintes geradores $\{I, U_1, U_2, \dots, U_{n-1}\}$, onde I é o elemento identidade e o outros geradores satisfazem as relações:

1. $U_i^2 = \delta U_i$;
2. $U_i U_{i\pm 1} U_i = U_i$;
3. $U_i U_j = U_j U_i, |i - j| > 1$.

Geometricamente o conjunto $\{I, U_1, U_2, \dots, U_{n-1}\}$ tem a seguinte interpretação ilustrada na Figura 2.6.

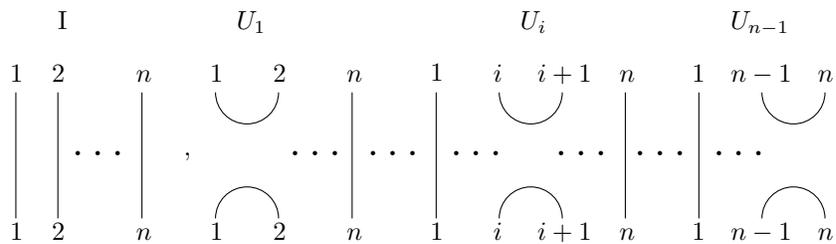


Figura 2.6: Geradores da álgebra de Temperley-Lieb.

As operações de composição com os geradores da álgebra de Temperley-Lieb são feitas de maneira semelhante as tranças, ou seja, opera-se fazendo justaposição vertical. Como exemplo, as propriedades 1 e 2 dos geradores da álgebra de Temperley-Lieb são verificadas para um caso particular mostrado na Figura 2.7. Observe que o δ da Definição 7, está associado geometricamente a um círculo.

Em [13] mostra-se que é possível construir uma representação do grupo de trança, a partir da álgebra de Temperley-Lieb. Ou seja, primeiro representam-se os geradores da álgebra de Temperley-Lieb, e, como consequência, obtém-se a representação do grupo de trança.

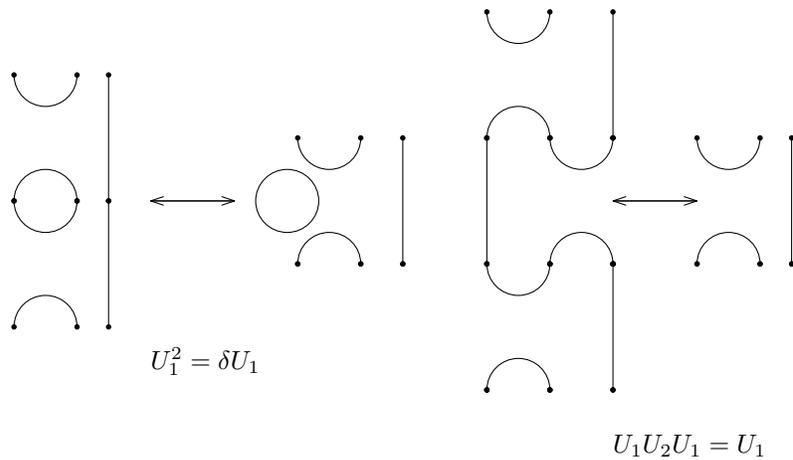


Figura 2.7: Propriedades 1 e 2 da álgebra de Temperley-Lieb.

Teorema 1 *Seja B_n o grupo de trança de ordem n e TL_n a álgebra de Temperley-Lieb de ordem n . Sejam ainda $\sigma_1, \sigma_2, \dots, \sigma_{n-1}$ os geradores de B_n e $\{I, U_1, U_2, \dots, U_{n-1}\}$ os geradores de TL_n . Se tomarmos $\delta = -A^2 - A^{-2}$ e definirmos $\rho(\sigma_i) = AU_i + A^{-1}$ e $\rho(\sigma_i^{-1}) = A^{-1}U_i + A$, obtemos uma representação do grupo de trança.*

Demonstração: É preciso verificar as três propriedades:

1. $\rho(\sigma_i)\rho(\sigma_i^{-1}) = 1$;
2. $\rho(\sigma_i)\rho(\sigma_{i+1})\rho(\sigma_i) = \rho(\sigma_{i+1})\rho(\sigma_i)\rho(\sigma_{i+1})$;
3. $\rho(\sigma_i)\rho(\sigma_j) = \rho(\sigma_j)\rho(\sigma_i)$, para $|i - j| > 1$.

$$\begin{aligned}
 1. \rho(\sigma_i)\rho(\sigma_i^{-1}) &= (AU_i + A^{-1})(A^{-1}U_i + A) \\
 &= U_i^2 + (A^2 + A^{-2})U_i + 1 \\
 &= (-A^2 - A^{-2})U_i + (A^2 + A^{-2})U_i + 1 \\
 &= 1.
 \end{aligned}$$

$$\begin{aligned}
 2. \rho(\sigma_i)\rho(\sigma_{i+1})\rho(\sigma_i) &= (AU_i + A^{-1})(AU_{i+1} + A^{-1})(AU_i + A^{-1}) \\
 &= (A^2U_iU_{i+1}U_i + U_i + U_{i+1} + A^{-2})(AU_i + A^{-1}) \\
 &= A^3U_i + AU_iU_{i+1} + \delta AU_i + A^{-1}U_i + AU_{i+1}U_i + A^{-1}U_{i+1} + A^{-1}U_i + A^{-3} \\
 &= A^3U_i + A(U_iU_{i+1} + U_{i+1}U_i) + 2A^{-1}U_i + A^{-1}U_{i+1} + (-A^2 - A^{-2})AU_i + A^{-3} \\
 &= A(U_iU_{i+1} + U_{i+1}U_i) + A^{-1}(U_i + U_{i+1}) + A^{-3}
 \end{aligned}$$

Observe que a expressão anterior não altera se trocarmos i por $i + 1$, e $i + 1$ por i , com isso conclui-se que $\rho(\sigma_i)\rho(\sigma_{i+1})\rho(\sigma_i) = \rho(\sigma_{i+1})\rho(\sigma_i)\rho(\sigma_{i+1})$.

3. Como $U_i U_j = U_j U_i$ para $|i - j| > 1$, segue que $\rho(\sigma_i)\rho(\sigma_j) = \rho(\sigma_j)\rho(\sigma_i)$.

Um exemplo de representação de B_3 utilizando o teorema 1 é mostrado na seção 4.3.

Computação Quântica Bidimensional

O título do capítulo é bem sugestivo pois realmente trataremos de um novo mundo quântico, porém agora bidimensional. Veremos como isso possibilita novas partículas com comportamentos diferentes do “antigo” mundo quântico. O surgimento dos *anyons* será abordado, ou seja, como eles naturalmente emergem de processos quânticos bidimensionais. O efeito Hall quântico fracionário também será apresentado, pois teoricamente possibilita a existência de anyons. Além disso, a dinâmica dos anyons será explorada, os espaços de fusão, as matrizes de representação e os axiomas de consistência. Por fim, apresentaremos um modelo geral de CQT, com todas as suas características e peculiaridades.

3.1 O Surgimento dos Anyons

Considere um sistema com n partículas idênticas no espaço *tridimensional*. A permutação dessas partículas deixa o sistema físico inalterado do ponto de vista da mecânica clássica, no entanto, pela mecânica quântica o estado do sistema pode mudar, adquirindo uma fase [25]. Dessa maneira, o espaço de estado do sistema deve carregar uma representação unitária ρ do grupo de permutação S_n . Assim, sendo σ uma permutação, $\rho(\sigma) = e^{i\theta}I$.

Se τ é uma transposição, então $\tau^2 = id$, onde id é a permutação identidade, com isso obtemos $\rho(\tau^2) = [\rho(\tau)]^2 = I$, então $\rho(\tau) = \pm I$. Vamos supor agora que τ_1 e τ_2 compartilhem um elemento, ou seja, τ_1 realiza a troca de a por c e τ_2 realiza a troca de b por c , então $\tau_1\tau_2\tau_1 = \tau_2\tau_1\tau_2$. Da igualdade anterior, podemos afirmar que $\rho(\tau_1) = \rho(\tau_2)$. Dessa maneira inferimos que para todas as transposições τ_i , $\rho(\tau_i) = I$ ou $\rho(\tau_i) = -I$. E como toda permutação pode ser escrita em função de transposições, podemos generalizar ainda mais e afirmar que dada uma permutação σ , então $\rho(\sigma) = (-1)^{sin(\sigma)}I$. Portanto, $\theta = 0, \pi$.

Definição 8 (Bóson e Férmions) *Partículas que obedecem $\rho(\sigma) = I$ são chamadas bósons, e partículas*

que obedecem $\rho(\sigma) = -I$ são chamadas *férmions*.

Essa evolução de sistemas quânticos dada pelas representações do grupo de permutação, pode ser chamada também de função de onda (ψ), com isso temos a seguinte característica para bósons e férmions ilustrada na Figura 3.1.

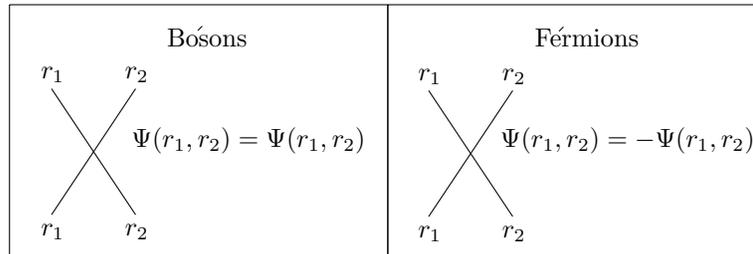


Figura 3.1: Bóson e Férmions.

Consideremos agora um sistema com n partículas no espaço *bidimensional*. A permutação dessas partículas pode alterar o estado do sistema, adquirindo uma fase. No entanto a evolução desse sistema é dada pelo grupo de trança, ao invés do grupo de permutação [25, 23, 27], como ilustrado na Figura 3.2, onde do ponto de vista tridimensional possuem a mesma permutação, porém vistos bidimensionalmente os entrançamentos são diferentes.

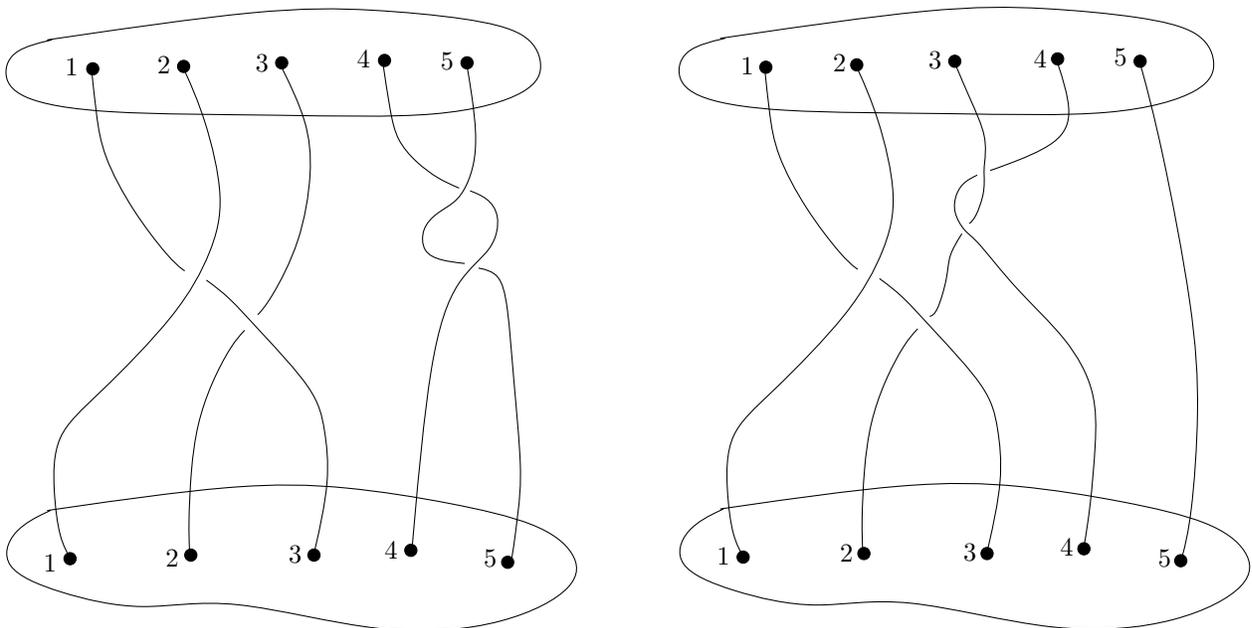


Figura 3.2: Permutação e entrançamentos.

O grupo de trança é muito mais rico que o grupo de permutação [25]. Note por exemplo que $\sigma_1^2 \neq I$ no grupo de trança, o que não ocorre para transposições no grupo de permutações S_n , onde

$\tau^2 = id$. O fato de o grupo de trança ser mais rico possibilita representações não triviais para a evolução do sistema, ou seja, valores para θ diferentes de 0 e π . Como observado primeiramente em [22], a evolução de sistemas quânticos bidimensionais possibilita um contínuo de valores para θ , e isso define os *anyons*.

Definição 9 (Anyons) *Suponha que tenhamos duas partículas idênticas, r_1 e r_2 , em duas dimensões. Quando trocamos essas partículas em sentido anti-horário, a função de onda (3.1) adquire uma fase arbitrária:*

$$\Psi(r_1, r_2) = e^{i\theta} \Psi(r_1, r_2) \quad (3.1)$$

Os casos $\theta = 0, \pi$ correspondem a bósons e férmions, respectivamente, enquanto partículas com outros valores para θ são chamadas *anyons*.

3.1.1 O efeito Hall quântico fracionário

Suponha que exista uma faixa no plano xy , limitada na direção y e com corrente circulando na direção x . Quando um campo magnético é aplicado entrando perpendicularmente na direção z , produz-se uma tensão na direção y , conhecida como tensão de Hall, V_H , que deve obedecer a seguinte relação:

$$\frac{e}{c} v B = \frac{V_H}{w}, \quad (3.2)$$

onde v é a velocidade dos elétrons, B o campo magnético, e é a carga dos elétrons e c é a velocidade da luz. A equação (3.2) pode ser rearranjada da seguinte maneira:

$$R_{xy} = \frac{V_H}{I} = \frac{B}{nec}, \quad (3.3)$$

utilizando o fato de que $I = nev w$, com n sendo a densidade de elétrons.

A razão $\frac{V_H}{I}$ em (3.3) é conhecida como resistência de Hall, e é denotada por $R_{xy} = -R_{yx}$ ou R_H . No entanto, quando o processo de obtenção da resistência Hall é realizado em baixas temperaturas, coisas diferentes acontecem. Nesse caso, a resistência Hall deixa de ser linear no campo magnético, em contraste com (3.3), e passa a apresentar platôs e vales [23], cuja descrição é feita elegantemente através da mecânica quântica e da equação (3.4):

$$R_H = \frac{h}{e^2} \frac{1}{\nu}, \quad (3.4)$$

onde h é a constante de Planck, e é a carga de um elétron e ν indica um platô, que assume valores inteiros. Além disso, $\frac{h}{e^2}$ é denominado o quantum da resistência.

Experimentalmente, foi observado que ν assumia valores inteiros e a isso foi dado o nome de *efeito Hall quântico inteiro* (IQHE). Klaus von Klitzing, responsável por esta descoberta, recebeu o prêmio Nobel de Física em 1985 por este feito. Valores fracionários para ν foram observados teoricamente e, a isso, deu-se o nome *efeito Hall quântico fracionário* (FQHE). Os valores para ν que, segundo experimentos, seriam possíveis, são do tipo $\nu = \frac{p}{2p+1}$, com p um inteiro positivo. O FQHE sugere a existência física de anyons, porém, até o momento, tal existência não foi verificada [23].

3.2 A Dinâmica dos Anyons

Um modelo que comporte a dinâmica dos anyons é descrito em [27], e deve, a princípio, possuir três características básicas:

1. Uma lista de tipos de partículas. Os tipos devem representar as cargas que as partículas conservam.
2. Regras de fusão e separação, que especificam valores de cargas quando duas partículas se fundem ou se separam.
3. Regras para entrançamentos, que especificam o que ocorre quando duas partículas são trocadas.

Assumiremos também que a quantidade de tipos de partículas é finita e denotaremos essas partículas por $\{a, b, c, \dots\}$. Dentre os tipos, existe o tipo especial que será denotado por 1, a partícula identidade, que não altera o sistema. Além disso, cada partícula a deve possuir uma partícula conjugada \bar{a} que, quando fundidas, produzem a partícula identidade 1.

3.2.1 Espaços de fusão

Duas partículas a e b , quando combinadas, podem produzir outras partículas, e essa **lei de fusão** é denotada por:

$$a \times b = \sum_c N_{ab}^c c. \quad (3.5)$$

Cada N_{ab}^c é um inteiro não negativo e indica de quantas maneiras é possível combinar a com b para obter c . Se $N_{ab}^c = 0$, então c não pode ser obtido a partir de a e b . Se $N_{ab}^c = 1$, então c pode ser obtido a partir de a e b de uma única maneira e, se $N_{ab}^c > 1$, então c pode ser obtido de mais de uma maneira a partir de a e b . Um exemplo de lei de fusão para anyons:

$$a \times b = a + 2b + 3c. \quad (3.6)$$

Na equação (3.6) temos $N_{ab}^a = 1$, $N_{ab}^b = 2$ e $N_{ab}^c = 3$. O que significa que se combinarmos a e b , podemos obter a de uma maneira, b de duas maneiras distintas, e c de três maneiras distintas.

Definição 10 (Espaço de fusão) Chamaremos de espaço de fusão V_{ab}^c o espaço cuja base é composta dos elementos $\{|ab; c, \mu\rangle, \mu = 1, 2, \dots, N_{ab}^c\}$, onde $|ab; c, \mu\rangle$ indica a base obtida quando funde-se a com b e obtém-se c da maneira μ .

O vetor dual de $|ab; c, \mu\rangle$ é definido como $\langle ab; c, \mu|$, e indica que c está sendo separado em a e b da maneira μ . É conveniente nesse momento introduzir uma representação gráfica para esses vetores, como ilustrado na Figura 3.3.

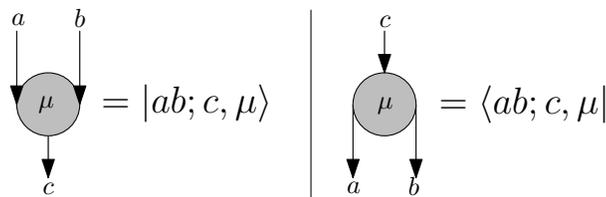


Figura 3.3: Representação gráfica do vetor da base e seu dual.

Note que, em (3.6), temos os seguintes espaços de fusão: $V_{ab}^a, V_{ab}^b, V_{ab}^c$, com dimensão 1, 2, 3, respectivamente. E, pelo fato de V_{ab}^b ter dimensão 2 e as bases serem ortonormais, é possível simular o espaço de Hilbert.

Definição 11 (Anyons não-abelianos) Um modelo anyonico é não-abeliano se

$$N_{ab}^c \geq 2 \quad (3.7)$$

para no mínimo algum par de tipos ab ; se isso não ocorrer, o modelo é chamado abeliano.

Anyons não-abelianos são de fundamental importância, pois possibilitam simular o espaço de Hilbert, o que chamaremos de “espaço de Hilbert topológico”. O caso (3.6) e os anyons de Fibonacci, do capítulo 4, são modelos anyonicos não-abelianos.

3.2.2 O operador de trança R

Quando duas partículas com cargas a e b são trocadas em sentido anti-horário, isso não altera a carga total, que denotaremos por c ; no entanto, essa operação pode produzir uma ação não trivial no espaço de Hilbert, já que leva o estado V_{ba}^c para V_{ab}^c . Temos então o operador de trança:

$$R : V_{ba}^c \longrightarrow V_{ab}^c. \quad (3.8)$$

Além disso, se escolhermos as bases canônicas $\{|ba; c, \mu\rangle\}$ e $\{|ab; c, \mu'\rangle\}$ para esses espaços, podemos escrever R como a matriz unitária:

$$R : |ba; c, \mu\rangle \mapsto \sum_{\mu'} |ab; c, \mu'\rangle (R_{ab}^c)_{\mu}^{\mu'} . \quad (3.9)$$

Na forma de diagrama, a matriz R pode ser ilustrada através da Figura 3.4.

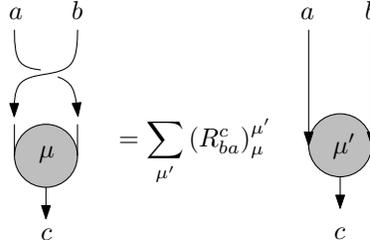


Figura 3.4: Matriz de entrançamento R .

3.2.3 O operador de mudança de base F

Suponha que existam três partículas com cargas a, b e c , respectivamente, que se fundem para obter uma partícula com carga d . Note que não é possível fundir as três partículas ao mesmo tempo, mas apenas de duas em duas, e isso produz dois modos de fusão distintos.

A Figura 3.5 indica esses dois modos de fusão. No diagrama à esquerda a primeira fusão é do par (ab) e o resultado é fundido com c para obter d , já no diagrama à direita, a primeira fusão é do par (bc) e o resultado é fundido com a para obter d .

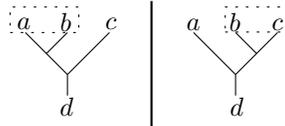
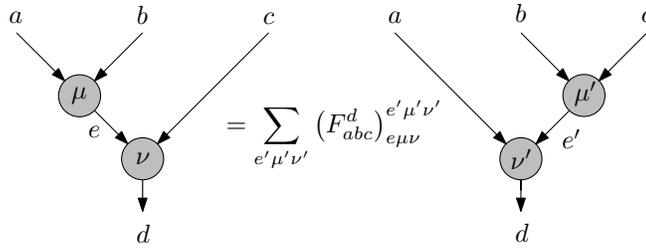


Figura 3.5: Dois modos de fusão de três partículas.

A matriz F não está relacionada propriamente aos entrançamentos, mas sim com a mudança na ordem de fusão, e é definida da seguinte maneira:

$$|(ab)c; d, e\mu\nu\rangle = \sum_{e'\mu'\nu'} |a(bc); d, e'\mu'\nu'\rangle (F_{abc}^d)_{e\mu\nu}^{e'\mu'\nu'} , \quad (3.10)$$

cuja representação é ilustrada através da Figura 3.6.

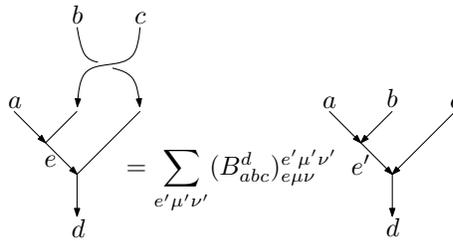
Figura 3.6: Matriz F de mudança de ordem de fusão.

3.2.4 O operador de trança B

A matriz B é semelhante à matriz R , pois realiza uma troca de partículas em sentido anti-horário, porém no segundo par. A matriz B leva o estado V_{acb}^d no estado V_{abc}^d :

$$B : V_{acb}^d \longrightarrow V_{abc}^d, \quad (3.11)$$

cuja representação é ilustrada através da Figura 3.7.

Figura 3.7: Matriz de entrançamento B .

Além disso, como observado na Figura 3.8, B pode ser escrita em função de R e F , como $B = F^{-1}RF$.

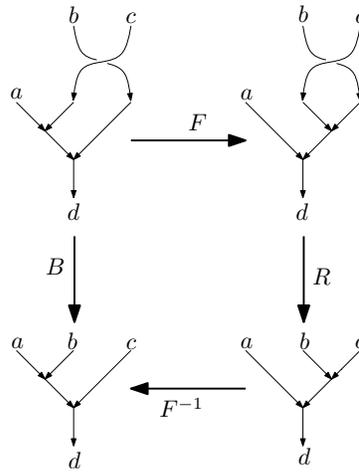


Figura 3.8: Matriz B em função de R e F .

3.2.5 Axiomas de consistência

É possível, a partir das operações F e R , definidas anteriormente, estabelecer relações que, independentemente das leis de fusão, devem ser satisfeitas, são os chamados *axiomas de consistência* [25]; isto é, o axioma do pentágono e o do hexágono, respectivamente ilustrados nas Figuras 3.9 e 3.10. Esses axiomas serão utilizados na construção do modelo de Fibonacci no capítulo 4.

O axioma do pentágono leva esse nome pois envolve cinco estados distintos, pictoricamente colocados em forma de pentágono na Figura 3.9. Além disso, descreve dois modos diferentes de se atingir o estado final (*). Para facilitar a visualização, indicamos por linha contínua onde o operador F realmente está atuando e por linha pontilhada onde não ocorre essa atuação.

Os dois modos diferentes de se obter o estado final (*) resultam na seguinte equação de consistência associada ao axioma do pentágono:

$$(F_{12c}^5)_a^d (F_{a34}^5)_b^c = \sum_e (F_{234}^d)_e^c (F_{1e4}^5)_b^d (F_{123}^b)_a^e. \quad (3.12)$$

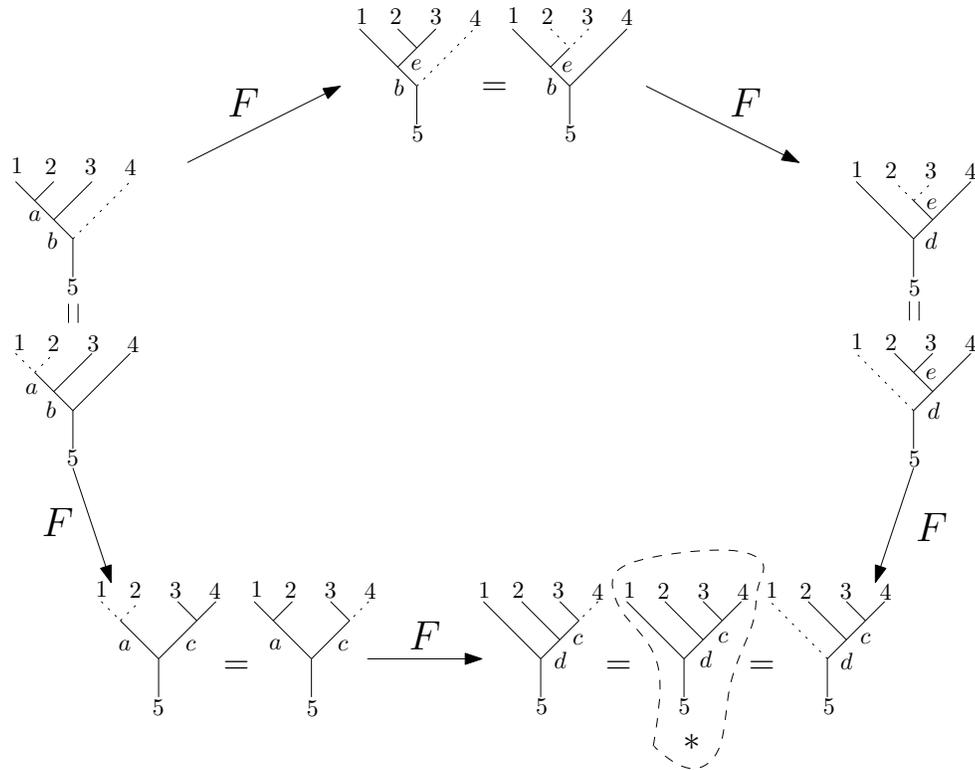


Figura 3.9: Axioma do pentágono.

O axioma do hexágono leva esse nome pois envolve seis estados distintos, pictoricamente colocados em forma de hexágono na Figura 3.10, e da mesma maneira que no axioma do pentágono, existem duas maneiras de se atingir o estado final (*). Para facilitar a visualização indicamos por linha contínua onde os operadores F e R realmente estão atuando e por linha pontilhada onde não ocorre essa atuação.

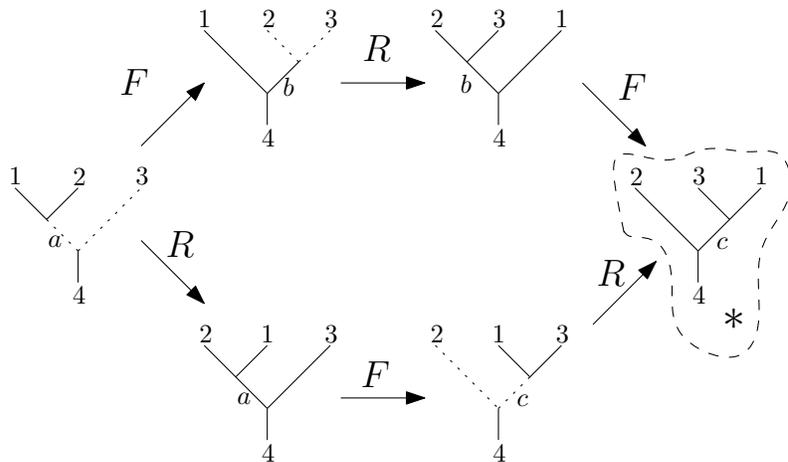


Figura 3.10: Axioma do hexágono.

Os dois modos diferentes de se obter o estado final (*) resultam na seguinte equação de consistência associada ao axioma do hexágono:

$$R_{13}^c (F_{213}^4)_a^c R_{12}^a = \sum_b (F_{231}^4)_b^c R_{1b}^4 (F_{123}^4)_a^b. \quad (3.13)$$

3.3 Modelo Geral de Computação Quântica Topológica

A partir dos conhecimentos adquiridos neste capítulo podemos estabelecer procedimentos que conduzem à concepção de um modelo geral de CQT;

1. O computador quântico topológico trabalha com os anyons;
2. Diferentes maneiras de combinar anyons não-abelianos geram espaços vetoriais complexos (simulam o espaço de Hilbert);
3. A computação é iniciada com a criação de pares de partículas/anti-partículas;
4. Quando anyons são trocados eles formam entrançamentos;
5. Cada entrançamento acarreta uma alteração no sistema, e essa alteração é descrita por representações do grupo de trança;
6. Um conjunto de entrançamentos com ação unitária será uma porta quântica;
7. Uma medida é feita no final observando o resultado da fusão.

Esse modelo de computação é esquematizado na Figura 3.11.

O capítulo 4 une os elementos que irão esclarecer esses pontos, pois apresentará um modelo específico de CQT com todo o aparato descrito por esse modelo geral de CQT.

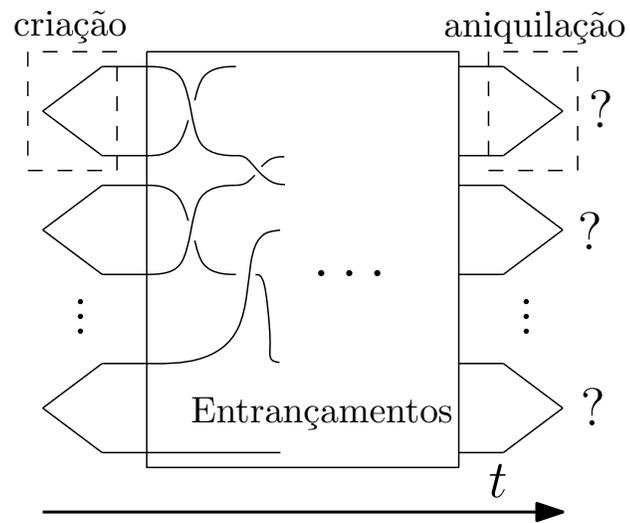


Figura 3.11: Modelo geral de CQT.

Computação Quântica via Modelo de Fibonacci

O foco deste capítulo são os *anyons de Fibonacci*, que possibilitam um modelo específico de CQT. Veremos como tais anyons de Fibonacci se fundem na seção 4.1, e como essas fusões podem ser interpretadas de maneiras diferentes. Também serão construídas as matrizes R , F e B para o modelo de Fibonacci de dois modos distintos nas seções 4.2 e 4.3, um a partir dos axiomas de consistência e o outro utilizando propriedades da álgebra de Temperley-Lieb. Com as matrizes R e B construiremos, na seção 4.4, portas de um qubit para o modelo de Fibonacci, e uma única porta de dois qubits chamada i-CNOT na seção 4.5, que torna o modelo de Fibonacci universal. A seção 4.6 será dedicada exclusivamente às novas portas de um qubit para o modelo de Fibonacci que construímos, e ao novo algoritmo para encontrar tais portas. Finalmente, a seção 4.7 aborda modelos diferentes do modelo de Fibonacci.

4.1 Leis de Fusão dos Anyons de Fibonacci

O nome *anyons de Fibonacci* foi introduzido em [27], mas as leis de fusão que serão abordadas já eram conhecidas, porém pelo nome de “*Modelo de Yang-Lee*”. As razões para alterar esse nome estão estritamente ligadas à CQT. O modelo de Fibonacci possui apenas duas partículas, $\{\tau, 1\}$, onde 1 é a partícula trivial, e deve satisfazer as seguintes leis de fusão:

- $\tau \times 1 = 1 \times \tau = \tau$;
- $1 \times 1 = 1$;
- $\tau \times \tau = 1 + \tau$.

O nome anyons de Fibonacci, decorre do fato que $\tau^{\times n} = F_{n-2} + F_{n-1}\tau$, onde F_i denota o i -ésimo termo da sequência de Fibonacci e $\tau^{\times n}$ denota a fusão de τ por ele mesmo n vezes. Observe também

que os anyons de Fibonacci satisfazem a Definição 11 para $\tau^{\times n}$, com $n \geq 3$. Na verdade, o modelo de Fibonacci é o mais simples com a característica de ser não-abeliano [27].

As leis de fusão do modelo de Yang-Lee estão relacionadas à *teoria de Chern-Simons* associada ao grupo $SU(2)$, indexada por um inteiro positivo k , $SU(2)_k$.

Em $SU(2)_k$, partículas podem ter spins $0, \frac{1}{2}, 1, \frac{3}{2}, \dots, \frac{k}{2}$. E as leis de fusão são do tipo:

$$s_1 \otimes s_2 = |s_1 - s_2| \oplus |s_1 - s_2| \oplus 1 \dots \oplus \min(s_1 + s_2, k - s_1 - s_2). \quad (4.1)$$

Essas leis se assemelham às leis de fusão de $SU(2)$, porém truncadas em um nível k . Um exemplo das leis de fusão utilizando a equação (4.1) é mostrado na Tabela 4.1 para $k = 3$. Essa discussão em torno de $SU(2)_k$ se deve ao fato de que as leis de fusão dos anyons de Fibonacci podem ser vistas como a parte inteira dos elementos de $SU(2)_3$: se associarmos $(0 \rightarrow 1)$ e $(1 \rightarrow \tau)$, e as operações $(+ \rightarrow \oplus)$ e $(\times \rightarrow \otimes)$, ambas na Tabela 4.1.

\otimes	(0)	$\frac{1}{2}$	(1)	$\frac{3}{2}$
(0)	(0)	$\frac{1}{2}$	(1)	$\frac{3}{2}$
$\frac{1}{2}$	$\frac{1}{2}$	$0 \oplus 1$	$\frac{1}{2} \oplus \frac{3}{2}$	1
(1)	(1)	$\frac{1}{2} \oplus \frac{3}{2}$	$(0 \oplus 1)$	$\frac{1}{2}$
$\frac{3}{2}$	$\frac{3}{2}$	1	$\frac{1}{2}$	0

Tabela 4.1: Operações em $SU(2)_3$.

Os elementos entre parênteses na Tabela 4.1 possuem exatamente as leis de fusão dos anyons de Fibonacci: sendo assim, a escolha de uma ou outra nomenclatura é apenas questão de propósito. No entanto, [12, 10] sugerem uma outra possibilidade, que é associar todo $SU(2)_3$ ao modelo de Fibonacci. Para isso basta definir $0 \equiv [0, \frac{3}{2}]$ e $1 \equiv [\frac{1}{2}, 1]$, como realizado através da Tabela 4.2.

\otimes	0	$\frac{1}{2} \rightarrow 1$	1	$\frac{3}{2} \rightarrow 0$
0	0	$\frac{1}{2} \rightarrow 1$	1	$\frac{3}{2} \rightarrow 0$
$\frac{1}{2} \rightarrow 1$	$\frac{1}{2} \rightarrow 1$	$0 \oplus 1$	$\frac{1}{2} \oplus \frac{3}{2} \rightarrow 0 \oplus 1$	1
1	1	$\frac{1}{2} \oplus \frac{3}{2} \rightarrow 0 \oplus 1$	$0 \oplus 1$	$\frac{1}{2} \rightarrow 1$
$\frac{3}{2} \rightarrow 0$	$\frac{3}{2} \rightarrow 0$	1	$\frac{1}{2} \rightarrow 1$	0

Tabela 4.2: Definição de $0 \equiv [0, \frac{3}{2}]$ e $1 \equiv [\frac{1}{2}, 1]$ em $SU(2)_3$.

Feitas as operações acima obtemos a Tabela 4.3. Note que obtemos as mesmas leis do modelo de Fibonacci, a menos de um fator de fase global [12, 10].

A abordagem de [14] sobre o modelo de Fibonacci é semelhante às encontradas em [27, 12], no quesito leis de fusão, que são as mesmas do modelo de Fibonacci se associarmos $(\tau \rightarrow P)$ e $(1 \rightarrow *)$, mas difere quando sequências maiores são construídas, pois, na definição de [14], o único resultado

\otimes	0	1	1	0
0	0	1	1	0
1	1	$0 \oplus 1$	$0 \oplus 1$	1
1	1	$0 \oplus 1$	$0 \oplus 1$	1
0	0	1	1	0

Tabela 4.3: Resultado da definição de $0 \equiv [0, \frac{3}{2}]$ e $1 \equiv [\frac{1}{2}, 1]$ em $SU(2)_3$.

possível de uma composição de operações é P . Em [14], a fusão $\tau \times \tau$ é indicada por (PP) e, se tomarmos sequências do tipo $(\tau \times \tau) \times \tau$, equivalentemente $(PP)P$, obteremos apenas dois resultados:

- $(PP)P \rightarrow (*)P \rightarrow P$;
- $(PP)P \rightarrow (P)P \rightarrow P$.

Porém em [27, 12], as possibilidades de $(\tau \times \tau) \times \tau$ incluem o caso a mais de

$$(\tau \times \tau) \times \tau \rightarrow \tau \times \tau \rightarrow 1.$$

Essa diferença de como as sequências são construídas interfere na construção das matrizes R, F e B , como veremos nas próximas seções.

Os anyons de Fibonacci são importantes não somente pela sua simplicidade, com relação aos processos de fusão, mas principalmente por estarem associados ao FQHE [23], no nível $\nu = \frac{12}{5}$.

4.1.1 Anyons de Fibonacci e o Espaço de Hilbert

Conhecidas as leis de fusão do modelo de Fibonacci, iremos agora simular o espaço de Hilbert, isto é, simular um qubit propriamente. Observe que:

$$\begin{aligned}
(\tau \times \tau) \times \tau &= (1 + \tau) \times \tau \\
&= \tau + (\tau \times \tau) \\
&= \tau + (1 + \tau) \\
&= 1 + 2\tau.
\end{aligned} \tag{4.2}$$

Graficamente a interpretação de $(\tau \times \tau) \times \tau$ é ilustrada na Figura 4.1.

O que a Figura 4.1 e a equação (4.2) nos diz com respeito ao processo de fusão $(\tau \times \tau) \times \tau$, é que obtemos τ como resultado de dois modos distintos, e 1 de um modo apenas. Com isso, o modelo com os anyons de Fibonacci torna-se não-abeliano. Como consequência, podemos construir as bases

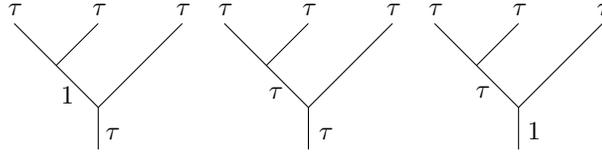


Figura 4.1: Anyons de Fibonacci e o espaço de Hilbert.

ortonormais da seguinte maneira:

$$|0\rangle = |(\tau \times \tau) \times \tau; \tau, \mathbf{1}\rangle, \quad (4.3)$$

$$|1\rangle = |(\tau \times \tau) \times \tau; \tau, \mathbf{2}\rangle. \quad (4.4)$$

Os números destacados nas equações (4.3) e (4.4) indicam as maneiras distintas de se obter o mesmo resultado final τ : **1** corresponde a primeira maneira de se obter τ na figura 4.1 e **2** corresponde a segunda maneira de se obter τ na mesma figura. Com isso, estamos aptos a simular o espaço de Hilbert. A outra base obtida é denominada não-computacional (NC):

$$|NC\rangle = |(\tau \times \tau) \times \tau; 1, \mathbf{1}\rangle.$$

Esse nome decorre do fato de que ela não será utilizada no processo de computação.

As bases $|0\rangle$, $|1\rangle$ e $|NC\rangle$, podem ser visualizadas de uma outra forma, como mostrado na Figura 4.2.

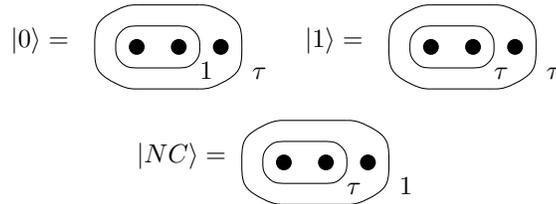


Figura 4.2: Bases do modelo de Fibonacci.

Portanto, o modelo de computação utilizando anyons de Fibonacci deverá ser realizado como esquematizado na Figura 4.3. Dois pares de partículas/anti-partículas são criados e, inicialmente encontram-se no estado $|0\rangle$. Dentre essas quatro partículas do tipo τ , a primeira é descartada e as outras três partículas são entrançadas: isso causará uma alteração no espaço de Hilbert, que será verificada observando o processo de fusão no final da computação.

Todavia, é necessário obter uma representação do grupo de trança B_3 que esteja em consonância com o modelo de Fibonacci, para que seja realizada a computação quântica topológica. Isso será realizado nas próximas seções.



Figura 4.3: Modelo de Fibonacci de CQT.

Observe que a possibilidade de simular o espaço de Hilbert a princípio, sem nos preocuparmos com as representações, se deve ao fato de existirem dois modos distintos de se obter τ . Por esse motivo, existem outras maneiras de simular o espaço de Hilbert com os anyons de Fibonacci, como, por exemplo, em [33], onde é realizado o processo de fusão $(\tau \times \tau) \times (\tau \times \tau)$, e, obtém-se o resultado:

$$\begin{aligned}
 (\tau \times \tau) \times (\tau \times \tau) &= (1 + \tau) \times (1 + \tau) \\
 &= (1 + \tau) + (\tau + (\tau \times \tau)) \\
 &= (1 + \tau) + (\tau + (1 + \tau)) \\
 &= 2 + 3\tau.
 \end{aligned}$$

Com isso, podem ser definidas as bases

$$\begin{aligned}
 |0\rangle &= |(\tau \times \tau) \times (\tau \times \tau); 1, 1\rangle, \\
 |1\rangle &= |(\tau \times \tau) \times (\tau \times \tau); 1, 2\rangle.
 \end{aligned}$$

Só que, neste caso, teríamos três bases não-computacionais relacionadas aos processo de fusão que resultam em τ . Por esse motivo, essa abordagem não será muito utilizada nesta dissertação, já que a quantidade de bases não-computacionais dificulta o processo de computação. Porém, salientamos que, para generalizar as leis do modelo de Fibonacci, a construção de bases dessa maneira é mais adequada, como proposto em [33].

4.2 Construção das Matrizes do Modelo de Fibonacci a Partir dos Axiomas de Consistência

Um teorema proveniente da teoria de categoria mostra que, para as operações de fusão serem consistentes, devem satisfazer os axiomas do pentágono e do hexágono. Se os axiomas forem satisfeitos, ou seja, se as equações (3.12) e (3.13) possuírem solução, então o modelo é viável [27], e, nesse caso, é possível obter uma única representação do grupo de trança. No nosso caso, resolveremos essas equações para o modelo de Fibonacci. Determinaremos primeiramente $F_{\tau\tau\tau}^{\tau}$ e $F_{\tau\tau\tau}^1$, para encontrar a

matriz F . Em seguida, determinaremos $R_{\tau\tau}^\tau$ e $R_{\tau\tau}^1$ para encontrar a matriz R . A matriz B será mais fácil de se obter, já que ela é escrita em função de F e R .

4.2.1 A matriz F

Observe que $F_{\tau\tau\tau}^1 = [1]$, onde $[1]$ representa a matriz que contém apenas o elemento 1, pois, como existe apenas uma maneira de se obter o resultado 1 fundindo $(\tau \times \tau) \times \tau$, não ocorre alteração nenhuma na base [25, 27]. Porém, é mais complicado obter $F_{\tau\tau\tau}^\tau$, já que isso envolve cálculos com o axioma do pentágono.

Na equação (3.12), relacionada ao axioma do pentágono, podemos fixar alguns valores e com isso obter informações sobre a solução, além disso, $F_{\tau\tau\tau}^\tau$ deve ser unitária. Se fixarmos $a = c = 1$ e $b = d = \tau$ na equação (3.12) do axioma do pentágono, obtemos:

$$\begin{aligned} (F_{\tau\tau\tau}^1)^\tau (F_{1\tau\tau}^1)_\tau &= \sum_{e \in \{1, \tau\}} (F_{\tau\tau\tau}^\tau)_e^1 (F_{\tau e \tau}^1)_\tau^\tau (F_{\tau\tau\tau}^\tau)_1^e \\ 1 &= [(F_{\tau\tau\tau}^\tau)_1^1]^2 + (F_{\tau\tau\tau}^\tau)_\tau^1 (F_{\tau\tau\tau}^\tau)_1^\tau, \end{aligned}$$

que pode ser escrita como

$$1 = F_{11}^2 + F_{\tau 1} F_{1\tau}, \quad (4.5)$$

se adotarmos a notação $F_{\tau\tau\tau}^\tau = \begin{bmatrix} F_{11} & F_{1\tau} \\ F_{\tau 1} & F_{\tau\tau} \end{bmatrix}$.

Uma solução geral para a equação (4.5) é do tipo $F_{11} = \varphi$, $F_{1\tau} = F_{\tau 1} = e^{i\theta} \sqrt{\varphi}$, com $\varphi^2 + \varphi = 1$. Então, podemos considerar a solução particular $F_{1\tau} = F_{\tau 1} = \sqrt{\varphi}$, se $\theta = 0$.

Utilizaremos agora o fato de F ser unitária para encontrar $F_{\tau\tau}$. Através da solução da equação (4.6), onde é realizada a operação $FF^\dagger = I$.

$$\begin{bmatrix} \varphi & \sqrt{\varphi} \\ \sqrt{\varphi} & a+bi \end{bmatrix} \begin{bmatrix} \varphi & \sqrt{\varphi} \\ \sqrt{\varphi} & a-bi \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \quad (4.6)$$

$$\begin{bmatrix} 1 & \varphi\sqrt{\varphi} + \sqrt{\varphi}(a-bi) \\ \varphi\sqrt{\varphi} + \sqrt{\varphi}(a+bi) & \varphi + a^2 + b^2 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

Cuja solução é $b = 0$ e $a = -\varphi$. Com isso concluímos que

$$F_{\tau\tau\tau}^\tau = \begin{bmatrix} \varphi & \sqrt{\varphi} \\ \sqrt{\varphi} & -\varphi \end{bmatrix}.$$

Além disso será considerada apenas a solução positiva da equação $\varphi^2 + \varphi = 1$ para que F seja unitária, ou seja, $\varphi = \frac{\sqrt{5}-1}{2} \approx 0.618034$.

Portanto, a matriz F que atua em $(\tau \times \tau) \times \tau$ é dada por:

$$F = \left[\begin{array}{cc|c} \varphi & \sqrt{\varphi} & 0 \\ \sqrt{\varphi} & -\varphi & 0 \\ \hline 0 & 0 & 1 \end{array} \right]. \quad (4.7)$$

Observe que a sub-matriz 2×2 no canto superior esquerdo de F , limitada por traços, atua propriamente na base computacional, e a sub-matriz $[1]$, associada a $F_{\tau\tau\tau}^1$, atua na base não-computacional.

4.2.2 A matriz R

A matriz R será obtida a partir dos cálculos com o axioma do hexágono, cuja equação (3.13), com as hipóteses do modelo de Fibonacci, pode ser escrita como

$$R_{\tau\tau}^c (F_{\tau\tau\tau}^\tau)_a R_{\tau\tau}^a = \sum_{b \in \{1, \tau\}} (F_{\tau\tau\tau}^\tau)_b R_{\tau b}^\tau (F_{\tau\tau\tau}^\tau)_a^b. \quad (4.8)$$

Porém, a matriz $R_{2 \times 2}$, que descreve a troca de duas partículas do tipo τ , tem apenas dois valores não triviais. Um é quando $\tau \times \tau = \tau$ e outro é quando $\tau \times \tau = 1$. Com isso a equação (4.8) se torna

$$R^c F_{\tau\tau} R^a = F_{1\tau} F_{\tau 1} + F_{\tau\tau} R^\tau F_{\tau\tau}, \quad (4.9)$$

onde R^τ representa o valor de R obtido quando $\tau \times \tau = \tau$ e R^1 representa o valor obtido de R quando $\tau \times \tau = 1$.

Da mesma maneira que foi feito com a matriz F , atribuiremos alguns valores para a e c na equação (4.9). Como resultado obteremos equações envolvendo R^τ e R^1 . Se substituirmos $a = c = \tau$ na equação (4.9), obtemos:

$$\begin{aligned} R^\tau F_{\tau\tau} R^\tau &= F_{1\tau} F_{\tau 1} + F_{\tau\tau} R^\tau F_{\tau\tau} \\ \Rightarrow -\varphi (R^\tau)^2 &= \varphi + \varphi^2 R^\tau \\ \Rightarrow 0 &= \varphi ((R^\tau)^2 + \varphi (R^\tau) + 1) \\ \Rightarrow 0 &= (R^\tau)^2 + \varphi (R^\tau) + 1 \\ \Rightarrow R^\tau &= -e^{\frac{\pm 2\pi i}{5}}. \end{aligned}$$

Se substituirmos $a = c = 1$ na equação (4.9), obtemos:

$$\begin{aligned}
 R^1 F_{11} R^1 &= F_{11} F_{11} + F_{\tau 1} R^\tau F_{1\tau} \\
 \Rightarrow (R^1)^2 \varphi &= \varphi^2 + \varphi R^\tau \\
 \Rightarrow R^1 &= \sqrt{\varphi + R^\tau} \\
 \Rightarrow R^1 &= -e^{\frac{\pm 4\pi i}{5}}.
 \end{aligned}$$

Com isso, obtemos a solução:

$$R = \left[\begin{array}{cc|c} R^1 & 0 & 0 \\ 0 & R^\tau & 0 \\ \hline 0 & 0 & R^\tau \end{array} \right] = \left[\begin{array}{cc|c} -e^{\frac{+4\pi i}{5}} & 0 & 0 \\ 0 & -e^{\frac{+2\pi i}{5}} & 0 \\ \hline 0 & 0 & -e^{\frac{+2\pi i}{5}} \end{array} \right] \quad (4.10)$$

A outra solução para R é a complexa conjugada dessa, que pode ser vista como o mesmo modelo, porém, com o sentido dos entrançamentos trocados [27].

Observe que a sub-matriz 2×2 no canto superior esquerdo de R , limitada por traços, atua propriamente na base computacional, e $-e^{\frac{2\pi i}{5}}$ atua na base não-computacional. É importante ressaltar que R é a representação de σ_1 no grupo de trança B_3 . Além disso, note que as matrizes R e F satisfazem todas as equações do axioma do hexágono e do pentágono, associadas às particularidades das equações (3.12) e (3.13).

4.2.3 A matriz B

Na seção 3.2.4, foi observado que $B = F R F^{-1}$. Logo,

$$B = \left[\begin{array}{cc|c} \varphi e^{\frac{-i\pi}{5}} & -i\sqrt{\varphi} e^{\frac{-i\pi}{10}} & 0 \\ -i\sqrt{\varphi} e^{\frac{-i\pi}{10}} & -\varphi & 0 \\ \hline 0 & 0 & -e^{\frac{2\pi i}{5}} \end{array} \right]. \quad (4.11)$$

Note que a sub-matriz 2×2 no canto superior esquerdo de B , limitada por traços, atua propriamente na base computacional, e $-e^{\frac{2\pi i}{5}}$ atua na base não-computacional. É importante ressaltar que B é a representação de σ_2 no grupo de trança B_3 .

4.3 Construção das Matrizes do Modelo de Fibonacci a Partir da Álgebra de Temperley-Lieb

Construiremos nesta seção as matrizes R , F e B do modelo de Fibonacci, de uma maneira alternativa, sem a utilização dos axiomas do pentágono e do hexágono. Essa construção encontra-se em [17], e decorre da álgebra de Temperley-Lieb.

Note que, na abordagem de [17] do modelo de Fibonacci, o processo $(PP)P$, equivalente à fusão $(\tau \times \tau) \times \tau$, possibilita apenas dois resultados, ou seja, duas bases. A base não-computacional não é considerada. A Figura 4.4 ilustra esse processo.

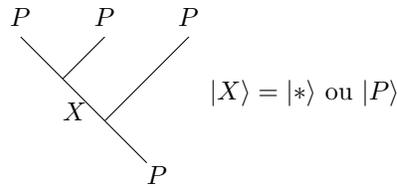


Figura 4.4: Bases do modelo de Fibonacci.

Com isso, a matriz R que descreve a troca de partículas é do tipo:

$$R = \begin{bmatrix} \mu & 0 \\ 0 & \lambda \end{bmatrix},$$

onde μ e λ representam os entrançamentos ilustrados na Figura 4.5.

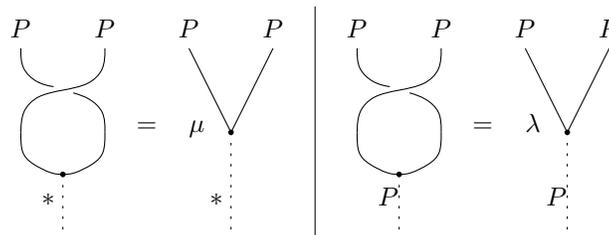


Figura 4.5: Entrançamentos do modelo de Fibonacci.

A matriz F de mudança de base é do tipo:

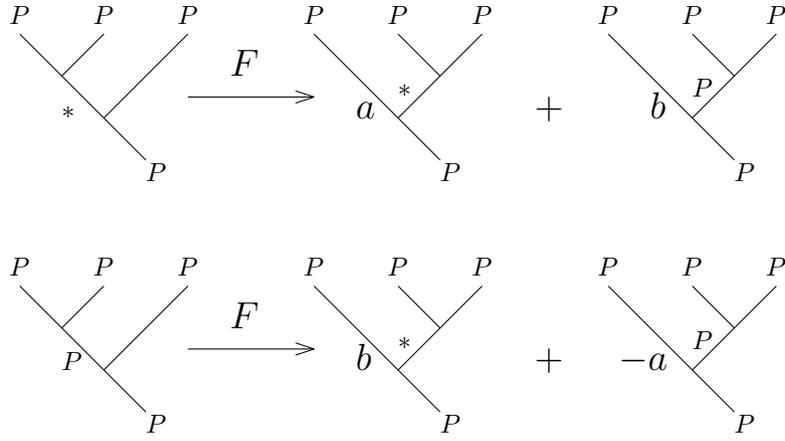
$$F = \begin{bmatrix} a & b \\ b & -a \end{bmatrix}, \text{ satisfazendo } a^2 + b^2 = 1.$$

Pois admite-se que F é real, ou seja, $F^2 = I$. A interpretação de F é dada através da Figura 4.6.

Da mesma maneira que descrito na Figura 3.8, obtemos $B = FRF^{-1}$.

4.3.1 As matrizes R e F

A construção das matrizes R e F será simultânea, já que, utilizando a álgebra de Temperley-Lieb, esses processos estão intimamente relacionados. Para facilitar os cálculos os geradores U_1, U_2 serão chamados de U, V respectivamente. Observe que:


 Figura 4.6: Interpretação da matriz F .

$$R = \begin{bmatrix} \mu & 0 \\ 0 & \lambda \end{bmatrix} = \begin{bmatrix} \lambda & 0 \\ 0 & \lambda \end{bmatrix} + \begin{bmatrix} \mu - \lambda & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} \lambda & 0 \\ 0 & \lambda \end{bmatrix} + \lambda^{-1} \begin{bmatrix} \delta & 0 \\ 0 & 0 \end{bmatrix}, \quad (4.12)$$

ou seja, escrevemos $R = \lambda I + \lambda^{-1}U$, onde $\delta = \lambda(\mu - \lambda)$ e U é a última matriz da equação 4.12. Porém, para que U seja gerador da álgebra de Temperley-Lieb, $\delta = -\lambda^2 - \lambda^{-2}$, e, com isso, obtemos $\mu = -\lambda^{-3}$.

Por outro lado, $B = \lambda I + \lambda^{-1}U_2 = \lambda I + \lambda^{-1}V$. Se considerarmos $V = FUF$, verificamos que:

$$V^2 = (FUF)(FUF) = FU^2F = \delta(FUF) = \delta V.$$

Com isso, uma possível representação de V é dada por:

$$V = FUF = \begin{bmatrix} a & b \\ b & -a \end{bmatrix} \begin{bmatrix} \delta & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} a & b \\ b & -a \end{bmatrix} = \delta \begin{bmatrix} a^2 & ab \\ ab & b^2 \end{bmatrix},$$

mas V deve satisfazer também $VUV = V$ e $UVU = U$. Como $VUV = \delta^2 a^2 V$, devemos ter $\delta^2 a^2 = 1$, ou seja, $a = \delta^{-1}$. Condição igual é encontrada fazendo $UVU = U$. Lembrando que $a^2 + b^2 = 1$, basta agora encontrarmos o valor de δ para obter uma representação do grupo de trança compatível com o modelo de Fibonacci. Até o momento, temos as seguintes matrizes:

$$F = \begin{bmatrix} a & b \\ b & -a \end{bmatrix} = \begin{bmatrix} \frac{1}{\delta} & \sqrt{1 - \delta^{-2}} \\ \sqrt{1 - \delta^{-2}} & \frac{1}{\delta} \end{bmatrix}, \quad (4.13)$$

$$U = \begin{bmatrix} \delta & 0 \\ 0 & 0 \end{bmatrix}, \quad (4.14)$$

$$V = \delta \begin{bmatrix} a^2 & ab \\ ab & b^2 \end{bmatrix} = \begin{bmatrix} a & b \\ b & \delta b^2 \end{bmatrix} = \begin{bmatrix} \frac{1}{\delta} & \sqrt{1 - \delta^{-2}} \\ \sqrt{1 - \delta^{-2}} & \delta - \delta^{-1} \end{bmatrix}. \quad (4.15)$$

Existe uma relação entre os processos realizados com as tranças e a álgebra de Temperley-Lieb, ilustrada na Figura 4.7.

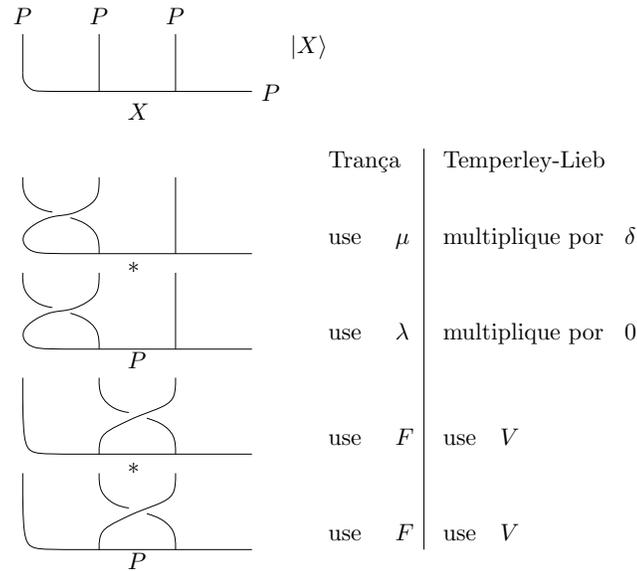


Figura 4.7: A álgebra de Temperley-Lieb e as tranças.

O processo descrito na Figura 4.7 pode ser estendido para uma base $|X_1 X_2 \dots X_n\rangle$. No caso $n = 5$, temos as seguintes características descritas na Figura 4.8.

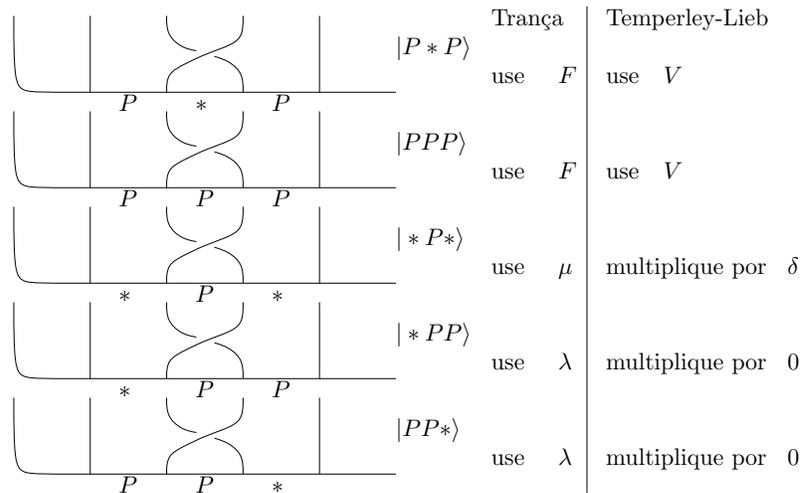


Figura 4.8: A álgebra de Temperley-Lieb e as tranças para o caso n=5.

Tendo por base a Figura 4.8, podemos construir as seguintes equações:

$$\begin{aligned}
U_3|P*P\rangle &= a|P*P\rangle + b|PPP\rangle, \\
U_3|PPP\rangle &= b|P*P\rangle + \delta b^2|PPP\rangle, \\
U_3|*P*\rangle &= \delta|*P*\rangle, \\
U_3|*PP\rangle &= 0, \\
U_3|PP*\rangle &= 0.
\end{aligned}$$

Ao realizar o cálculo de $U_4U_3U_4 = U_4$, encontramos as condições sobre δ .

$$\begin{aligned}
U_4U_3U_4|PPPP\rangle &= U_4U_3(b|PP*P\rangle + \delta b^2|PPPP\rangle) \\
&= U_4(bU_3|PP*P\rangle + \delta b^2U_3|PPPP\rangle) \\
&= \delta b^2(bU_4|P*PP\rangle + \delta b^2U_4|PPPP\rangle) \\
&= \delta^2 b^4 U_4|PPPP\rangle \\
\delta^2 b^4 &= 1.
\end{aligned}$$

Mas $\delta^2 b^4 = \delta^2(1 - \delta^{-2})^2 = \left(\frac{\delta}{1 - \delta^{-2}}\right)^2$. E portanto, obtemos as equações $\frac{\delta}{1 - \delta^{-2}} = \pm 1$, cujas soluções são $\delta = \frac{\pm 1 \pm \sqrt{5}}{2}$. Porém, se utilizarmos a equação de unitariedade da matriz F , obtemos apenas como solução $\frac{\pm(-1 + \sqrt{5})}{2}$. Assim, a menos do sinal dos elementos da matriz F , encontramos a mesma solução, que na seção 4.1, para R, F e B , se utilizarmos o teorema 1, de representação do grupo de trança a partir da álgebra de Temperley-Lieb e as equações (4.13), (4.14) e (4.15).

4.4 Construção das Portas de Um Qubit do Modelo de Fibonacci

Para construir portas de um qubit utilizando o modelo de Fibonacci, devemos utilizar as matrizes R e B , encontradas na seção 4.2, e através das operações de multiplicação com as respectivas matrizes, tentar aproximar uma porta quântica. Encontrando essa aproximação, podemos estabelecer os entrançamentos necessários que realizam a porta quântica na CQT. Por exemplo, suponhamos que uma aproximação P , para uma porta P_0 , inicialmente dada, seja,

$$\left[\begin{array}{c|c} P_0 & 0 \\ \hline & 0 \\ \hline 0 & 0 & 1 \end{array} \right] \approx \left[\begin{array}{c|c} P & 0 \\ \hline & 0 \\ \hline 0 & 0 & X \end{array} \right] = R^{-1}B^2 \dots R, \quad (4.16)$$

então, como ilustrado através da Figura 4.9, o estado inicial $|\psi_i\rangle$ é alterado pelos entrançamentos da porta P , resultando no estado final ψ_f . Deve-se lembrar que P e P_0 são sub-matrizes complexas de

dimensão 2×2 , que a matriz P atua apenas na base computacional, e X indica a atuação na base não-computacional, que (para efeito de portas de um qubit) não necessariamente precisa valer 1.

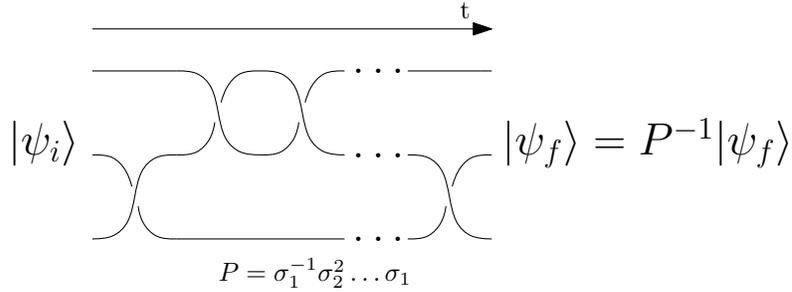


Figura 4.9: Exemplo de porta de um qubit do modelo de Fibonacci.

Esse processo de encontrar as portas quânticas topológicas, ou seja, encontrar a sequência de entrançamentos que aproxima uma porta inicial dada, é chamado em [32] de “black art”¹, ou magia negra em português, pois não existe até o momento uma forma sistemática de realizá-lo.

Utilizaremos, nesta dissertação, a abordagem de [10] para a construção de portas de um qubit do modelo de Fibonacci, trabalho em que se mostra como reduzir o conjunto de buscas de possíveis portas. Primeiramente, definiremos a distância entre matrizes, como encontrado em [10].

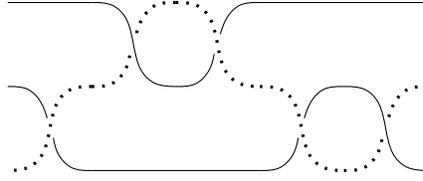
Definição 12 (Distância entre matrizes) *Sejam U e V matrizes quadradas com coeficientes em \mathbb{C} . Denotamos $d(U, V) = \|U - V\|$ a distância entre as matrizes U e V , onde $\|O\|$ é a raiz quadrada do maior auto-valor de $O^\dagger O$.*

A métrica d é uma medida de proximidade, e sua utilização é feita simplesmente pelo fato da baixa complexidade computacional envolvida em seu cálculo.

Em [30], é mostrado que um conjunto particular de entrançamentos, chamado *weave*, possibilita uma computação universal quando entrançamos partículas do mesmo tipo, como no caso dos anyons de Fibonacci, onde combinamos três partículas do tipo τ .

Definição 13 (Weave) *Uma weave é qualquer trança que é topologicamente equivalente a uma trança onde apenas uma única partícula se move.*

O termo *topologicamente equivalente*, na definição anterior, se refere ao fato de que, quando a trança não for constituída de apenas uma partícula se movendo, mas se utilizarmos as propriedades do grupo e obtermos uma *weave*, então ela é também considerada *weave*.

Figura 4.10: Exemplo de *weave* em B_3 .

A Figura 4.10 ilustra uma *weave* em B_3 , onde a corda pontilhada entrança as cordas com linha contínua.

Outra restrição realizada em [10] com relação à busca por essas sequências que aproximam a porta quântica, é feita observando o fato de que $R^{10} = B^{10} = 1$. Com isso, segue que $R^6 = R^{-4}$ e $B^6 = B^{-4}$. Além disso, em [10, 2], é mostrado experimentalmente, que o conjunto das matrizes do tipo R^2, B^2, R^4, B^4 , e suas respectivas inversas, geram todas as possíveis portas de um qubit. Com essas observações, as portas quânticas topológicas do modelo de Fibonacci podem ser descritas por sequências do tipo:

$$P = R^{n_1} B^{n_2} R^{n_3} \dots B^{n_{m-1}} R^{n_m}, \quad (4.17)$$

onde n_2, n_3, \dots, n_{m-1} assumem valores no conjunto $\{\pm 2, \pm 4\}$, e, n_1, n_m assumem valores no conjunto $\{0, \pm 2, \pm 4\}$.

Portanto, para se obter uma porta do modelo de Fibonacci, faremos uma busca computacional em sequências possíveis na equação (4.17). O comprimento máximo dessa sequência, ou seja, o número de entrançamentos máximo é $4m$, e o número exato de entrançamentos é dado por $\sum_i^m n_i$.

Uma restrição que pode ser considerada, e que será necessária quando construirmos portas de dois qubits para o modelo de Fibonacci, é com relação à base não-computacional. Observe que, nas matrizes R e B , o elemento que atua na base não computacional é $-e^{\frac{2\pi i}{5}}$. Como $(-e^{\frac{2\pi i}{5}})^{10} = 1$, devemos ter $\sum_i^m n_i \equiv 0 \pmod{10}$ para que a porta P , da equação (4.17), não altere a base não-computacional. A alteração da base não-computacional pode levar a erros que são chamados *leakage-errors* no caso de mais de um qubit: esse é um problema complicado que será abordado na seção 4.5.

A definição das sequências, como na equação (4.17), faz com que os entrançamentos não alterem a ordem dos anyons, ou seja, o anyon da primeira posição antes dos entrançamentos permanece efetivamente na primeira posição depois dos entrançamentos, e assim com todos os outros anyons, como ilustrado na Figura 4.11.

¹Página 94.

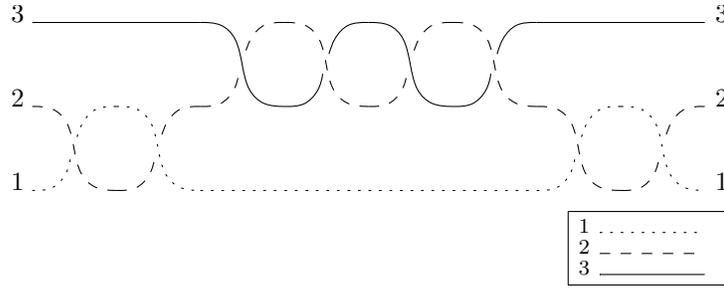


Figura 4.11: Exemplo de trança efetiva.

Essa característica é importante na CQT, pois, no final, é realizada uma medida, como observado no modelo geral da seção 3.3 e no modelo de CQT com anyons de Fibonacci, na seção 4.1.1 através da Figura 4.3.

Definição 14 (Trança efetiva) *Uma trança é efetiva se não alterar as posições iniciais e finais dos anyons.*

4.4.1 Porta i-NOT

A porta quântica i-NOT = $\begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}$ foi aproximada em [2] por uma porta P do modelo de Fibonacci com uma distância de $2,3 \cdot 10^{-3}$ da seguinte maneira:

$$P = R^{-2}B^{-4}R^4B^{-2}R^2B^2R^{-2}B^4R^{-2}B^4R^2B^{-4}R^2B^{-2}R^2B^{-2}R^{-2} \approx \left[\begin{array}{cc|c} 0 & i & 0 \\ i & 0 & 0 \\ \hline 0 & 0 & 1 \end{array} \right].$$

Os entrançamentos são ilustrados através da Figura 4.12.

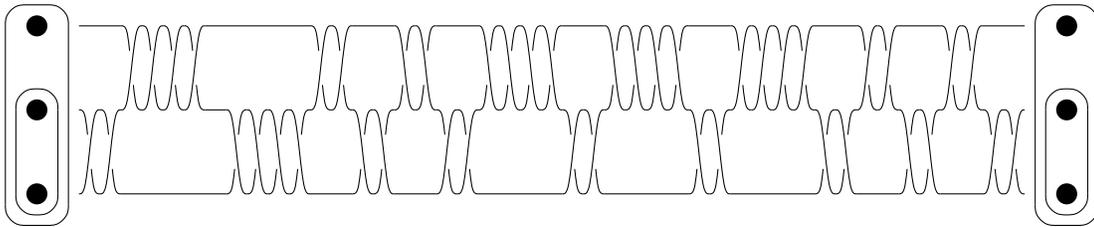


Figura 4.12: Porta i-NOT do modelo de Fibonacci.

A porta i-NOT será utilizada na seção 4.5 para a construção de uma porta de dois qubits denominada i-CNOT.

4.5 Construção de Portas de Dois Qubits do Modelo de Fibonacci

A construção de portas de mais de um qubit para o modelo de Fibonacci torna-se muito difícil [2, 23], pois a quantidade de bases computacionais e não-computacionais aumenta de maneira expressiva. Além disso, como não existe um método sistemático de buscar essas portas, o simples aumento de dimensão, por exemplo de matrizes 2×2 para matrizes 4×4 , no caso de portas de dois qubits, torna o processo computacionalmente complexo. De maneira natural, poderíamos tentar estender o processo das portas de um qubit para portas de dois qubits para o modelo de Fibonacci, como ilustrado na Figura 4.13.

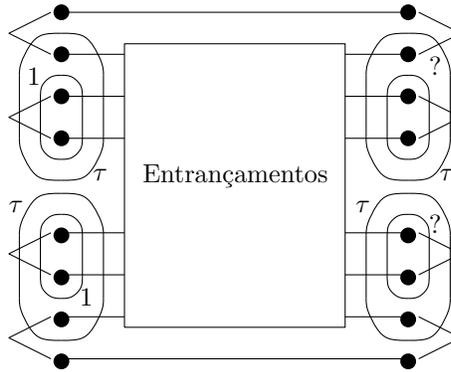


Figura 4.13: Portas de dois qubits do modelo de Fibonacci.

Portanto, necessitaríamos de uma representação de B_6 que fosse densa no conjunto das portas de dois qubits. Porém, note que:

$$\begin{aligned}
 ((\tau \times \tau) \times \tau) \times ((\tau \times \tau) \times \tau) &= (1 + 2\tau) \times (1 + 2\tau) \\
 &= 1 + 2\tau + 2\tau + 4(\tau \times \tau) \\
 &= 1 + 4\tau + 4\tau + 4 \\
 &= 5 + 8\tau,
 \end{aligned}$$

ou seja, esse processo na verdade terá oito bases computacionais e cinco bases não-computacionais, o que o torna inviável computacionalmente. Em [2, 10], é exibida uma alternativa a esse processo na construção da porta de dois qubits i-CNOT,

$$\begin{bmatrix} i & 0 & 0 & 0 \\ 0 & i & 0 & 0 \\ 0 & 0 & 0 & i \\ 0 & 0 & i & 0 \end{bmatrix}. \quad (4.18)$$

4.5.1 Porta i-CNOT

Vamos supor que P seja um conjunto de entrançamentos que é uma trança efetiva em B_3 . Se realizarmos as operações BPR , como ilustrado através da Figura 4.14, esse novo entrançamento altera o anyon da posição 3 para a posição 1.

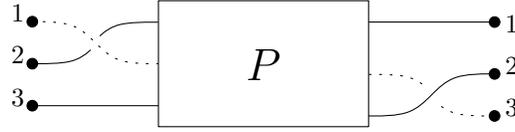


Figura 4.14: Porta não efetiva.

Além disso, note que se BPR puder aproximar o operador identidade, então poderíamos construir uma porta que insere um qubit [2] sem alterar o sistema. Esse tipo de porta foi encontrado em [2]:

$$P = B^3 R^{-2} B^{-4} R^2 B^4 R^2 B^{-2} R^{-2} B^{-4} R^{-4} B^{-2} R^4 B^2 R^{-2} B^2 R^2 B^{-2} R^3 \approx \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \quad (4.19)$$

A porta P mostrada em (4.19) será denominada *injeção*, e sua distância é $1,5 \times 10^{-3}$ da identidade. Seus entrançamentos são ilustrados na Figura 4.15. Note a troca de posição dos anyons em destaque e o fato de a base não-computacional permanecer inalterada, não produzindo assim *leakage-errors*, ou seja, não alterando os demais estados.

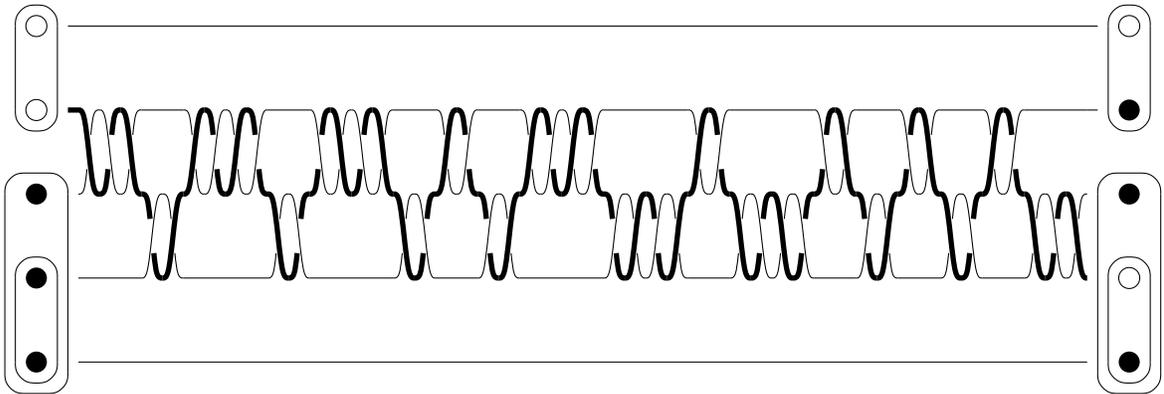


Figura 4.15: Porta injeção.

Um modelo para a construção da i-CNOT, baseado na proposta em [2], é esquematizado na Figura 4.16. Dois anyons são inseridos através da porta I , que, nesse caso, denota a porta injeção. Esses anyons funcionam como o qubit de controle. Se o qubit de controle estiver no estado $|0\rangle$, então

nenhuma alteração ocorre no sistema. Porém, se eles estiverem no estado $|1\rangle$, a porta i -NOT é realizada e os anyons de controle são retirados do sistema, através da porta inversa da injeção, denotada por I^{-1} . Sendo assim, obtém-se a i -CNOT se utilizarmos como porta injeção e porta i -NOT as portas encontradas anteriormente.

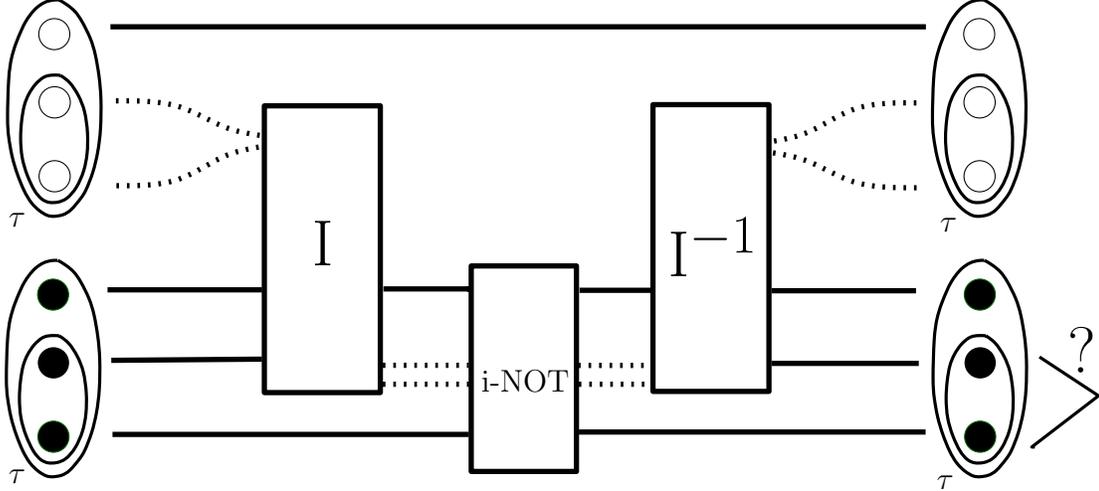


Figura 4.16: Modelo da porta i -CNOT.

Com a construção da porta i -CNOT, que é universal, o modelo de Fibonacci torna-se o único modelo de CQT universal conhecido até o momento.

4.6 Novas Portas de Um Qubit do Modelo de Fibonacci

Dentre as portas de um qubit conhecidas, foi realizada uma busca, primeiro utilizando o programa 1 (Apêndice A), baseado na equação (4.17), para se obter uma aproximação com distância máxima de 0,1 da porta original. Depois de encontradas essas possíveis portas, foi utilizado o programa 2 (Apêndice A) para uma melhor aproximação. A primeira porta é a seguinte:

$$P = R^4 B^2 R^{-4} B^{-4} R^4 B^4 R^4 B^4 R^4 B^4 R^{-4} B^{-2} R^2 B^{-2} R^4 \approx \frac{i}{\sqrt{2}} \left[\begin{array}{cc|c} 1 & 1 & 0 \\ 1 & -1 & 0 \\ 0 & 0 & 1 \end{array} \right].$$

Cujos entrançamentos são ilustrados através da Figura 4.17, com distância $1,3 \times 10^{-3}$ da porta original. Denotaremos essa porta por $i\mathbf{H}$.

Outra porta encontrada é:

$$P = B^{-2} R^2 B^4 R^4 B^{-4} R^{-4} B^2 R^{-2} B^2 R^{-4} B^4 R^4 B^2 R^2 \approx \left[\begin{array}{cc|c} i & 0 & 0 \\ 0 & -i & 0 \\ 0 & 0 & 1 \end{array} \right].$$

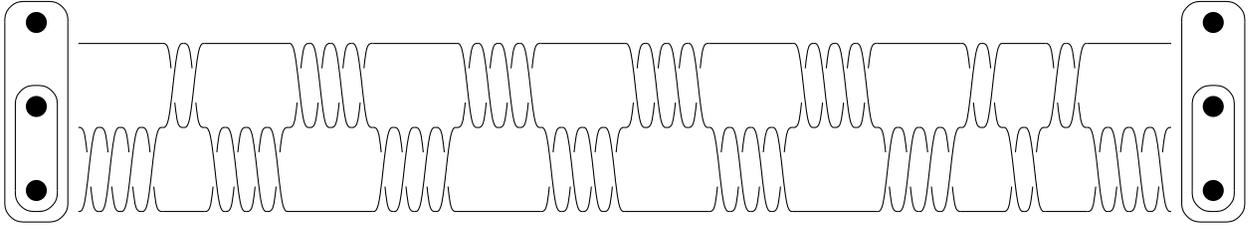


Figura 4.17: A porta iH.

Cujos entrançamentos são ilustrados através da Figura 4.18, com distância $5,6 \times 10^{-3}$ da porta original. Denotaremos essa porta por **iZ**.

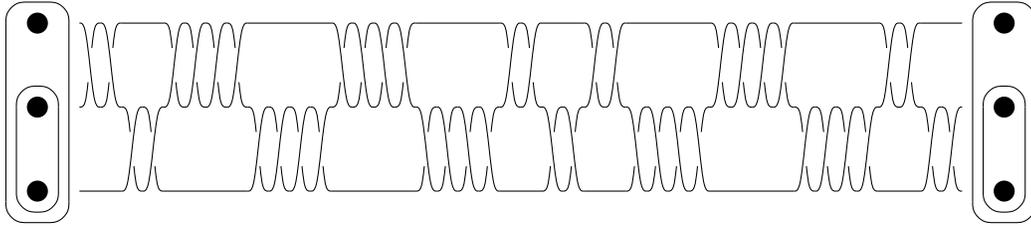


Figura 4.18: A porta iZ.

A terceira e última porta encontrada é:

$$P = R^{-4}B^{-4}R^{-2}B^{-4}R^4B^2R^{-2}B^4R^{-2}B^2R^2B^2R^{-4}B^{-4} \approx \left[\begin{array}{cc|c} 0 & -1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{array} \right].$$

Cujos entrançamentos são ilustrados através da Figura 4.19, com distância 7×10^{-3} da porta original. Denotaremos essa porta por **XZ**.

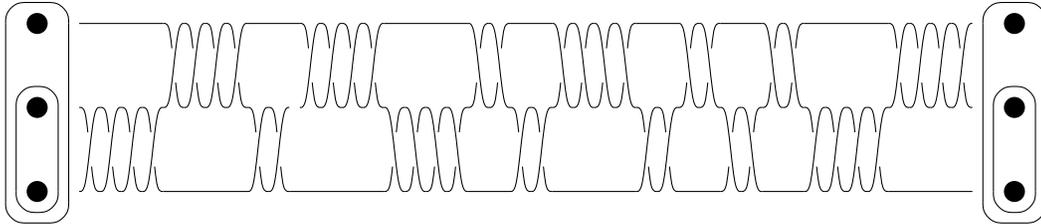


Figura 4.19: A porta XZ.

As portas iH, iZ e XZ são originais. Além disso, observou-se com esses testes uma grande dificuldade de encontrar portas de um qubit para o modelo de Fibonacci, pois muitas portas foram testadas e apenas essas três foram possíveis de aproximar. Por fim, notou-se que essas portas possuem duas

características especiais. A primeira é que todas as portas P encontradas até o momento, inclusive a i -NOT [2], possuem ordem 4, ou seja $P^4 = I$. A outra característica comum a todas as portas é que os elementos da diagonal principal possuem o sinal trocado. Assim, propomos um novo método para encontrar uma porta P de um qubit do modelo de Fibonacci:

Método para encontrar portas de um qubit do modelo de Fibonacci

1. Decomponha P em portas de ordem 4, A_1, A_2, \dots, A_n , cujos elementos da diagonal principal tem sinal trocado, $P = A_1 A_2 \dots A_n$;
2. Aproxime A_1, A_2, \dots, A_n utilizando a equação (4.17);
3. Utilize $A_1 A_2 \dots A_n$ para aproximar P .

Note que nosso método não engloba todas as portas de um qubit: por exemplo, a porta NOT não pode ser decomposta em portas de ordem 4, pois possui ordem 2. Porém, a porta NOT não possui nenhuma aproximação para o modelo de Fibonacci conhecida, como dito em [32].

4.7 Além dos Anyons de Fibonacci

A CQT não se resume apenas ao modelo de Fibonacci, que tem sua importância, pois é o único conhecido até o momento que possibilita uma computação universal e possui essas portas construídas propriamente. Em [8], por exemplo, mostra-se que, para todo $k \geq 3, k \neq 4$, $SU(2)_k$ possibilita uma computação universal. No entanto, para $K \neq 3$, a complexidade aumenta com relação ao problema de encontrar as representações do grupo de trança em consonância com o modelo e também com relação ao problema de encontrar as portas quânticas. A capacidade de $SU(2)_k$ possibilitar uma computação universal decorre do fato de gerar anyons não-abelianos e poder simular o espaço de Hilbert, além do fato de poder simular portas de dois qubits. Em [23, 11], são construídas portas para $SU(2)_5$, porém, o número de portas é reduzido e não se tem propriamente uma computação universal.

A universalidade de $SU(2)_k$ é abordada também em [33], onde é exibida uma maneira geral de construir bases para $SU(2)_k$. Além disso, uma porta específica, denominada *Toffoli*², é construída. Todavia, na abordagem de [33], o problema da representação do grupo de trança para esses modelos não é considerado.

Um modelo conhecido como *Ising* é exibido em [32, 23]. Esse modelo, apesar de possuir algumas portas construídas e relação com o FQHE, não possibilita computação universal [32, 23].

²Porta de três qubits, semelhante a CNOT, porém com um qubit de controle a mais.

Conclusões

Esta dissertação apresentou a CQT como alternativa na construção do computador quântico. A CQT é tolerante a falhas pois o meio físico, os anyons, naturalmente possibilitam evitar o problema da perda de informação quando o sistema quântico interage com o ambiente.

Para construir um computador quântico topológico, é necessário descobrir se os anyons realmente existem na natureza e se podemos controlá-los. Além disso, baseado nas leis de fusão, devemos construir representações do grupo de trança que estejam em consonância com o modelo, e construir portas com essas representações. Observou-se uma grande dificuldade nesses processos, já que existe apenas um modelo de CQT universal, e, mesmo para o modelo mais simples envolvendo os anyons de Fibonacci, a construção de representações do grupo de tranças e das portas quânticas acarretou complexidade elevada.

O processo de construção de portas quânticas para o modelo de Fibonacci adotado nesta dissertação, e que possibilitou a construção de novas portas quânticas originais, não é sistemático, e impede que em outros modelos, sobre outras condições, essas portas sejam encontradas. No entanto, o fato de, entre as portas quânticas encontradas, existirem duas características em comum, sugere que existe uma estrutura matemática envolvida nesse processo, o que possibilitaria um método sistemático de encontrar tais portas. Essa falta de sistematicidade ao buscar as portas quânticas é um entrave teórico, e isso pode ser observado na construção da *i*-CNOT para o modelo de Fibonacci, onde é utilizado um artifício diferente, visto que a busca computacional que existe até o momento seria inviável.

Sugestões para Futuras Pesquisas

Para dar prosseguimento a este trabalho, sugerimos os seguintes tópicos:

- Analisar a utilização da álgebra de Temperley-Lieb na construção de matrizes de representação

para modelos diferentes do modelo de Fibonacci, como por exemplo as leis obtidas de $SU(2)_k$.

- Como alternativa à sistematização no processo de encontrar as portas quânticas, podemos decompor as portas quânticas pelas matrizes de representação da álgebra de Temperley-Lieb e com isso analisar possíveis características sobre as portas quânticas topológicas decorrentes desse processo.
- Como alternativa à sistematização no processo de encontrar as portas quânticas, podemos analisar o método de redução de Gauss, e sua aplicação para encontrar portas quânticas topológicas.
- Analisar a CQT do ponto de vista criptográfico, ou seja, quais seriam as implicações e as possíveis implementações necessárias para proteger a informação na CQT.

Comentário Final

A computação quântica é uma área de estudos ampla e diversificada, que tem atraído a curiosidade de pessoas em todo o mundo, além de pesquisadores empenhados em extrair os benefícios que essa computação pode proporcionar. A CQT é uma área dentro da computação quântica que está em processo de construção, muitos avanços ainda devem ocorrer para que ela se estabeleça plenamente, como tecnologia. Com esta dissertação, esperamos avançar nesse processo, difundindo esse assunto ainda pouco conhecido no Brasil, e que está na fronteira da ciência.

Bibliografia

- [1] Albuquerque C. D. “Análise e Construção de Códigos Quânticos Topológicos sobre Variedades Bidimensionais”. 2009. 139 f. Tese (Doutorado em Engenharia Elétrica). FEEC, UNICAMP.
- [2] Bonesteel N. E.; Hormozi L.; Zikos G.; Simon S.H. “Braid Topologies for Quantum Computation”. *Phys. Rev. Lett.*, **95**, pp.140503-1, (september 2005).
- [3] Brilinski J.L. “Universal quantum gates”. *Mathematics of Quantum Computation*, (Florida, USA, 2002).
- [4] Burrello M.; Mussardo G.; Wan X. “Topological quantum gate construction by iterative pseudogroup hashing”. *New Journal of Physics*, **13** 025023 (2011)
- [5] Diffie W.; Hellman M.E. “New Directions in Cryptography”. (1976).
- [6] Fraleigh J. B. *A First Course in Abstract Algebra*. Addison Wesley, (2002). 520 p.
- [7] Freedman M.; Larsen M.; Wang Z. “A modular functor which is universal for quantum computation”. *arXiv:quant-ph/0001108 v2*, (2000).
- [8] Freedman M.; Larsen M.; Wang Z. “The two-eigenvalue problem and density of Jones representation of braid groups”. 2001, Disponível em <http://stationq.cnsi.ucsb.edu/freedman/Publications/77.pdf>. Acesso em 29 de setembro de 2011
- [9] Ho C. -L.; Solomon A.I.; Oh C. -H. “Quantum entanglement, unitary braid representation and Temperley-Lieb algebra”. Disponível em <http://iopscience.iop.org/0295-5075/92/3/30002>. Acesso em 29 de setembro de 2011.
- [10] Hormozi L. “Topological Quantum Compiling”. 2007. 134 f. PhD thesis. The Florida State University.

- [11] Hormozi L.; Bonesteel N. E.; Simon S.H. “Topological Quantum Computing with Read-Rezayi States”. *Phys. Rev. Lett.*, **103**, pp.160501-1, (october 2005).
- [12] Hormozi L.; Zikos G.; Bonesteel N. E.; Simon S.H. “Topological quantum compiling”. *Phys. Rev. B*, **75**, pp.165310-1, (2007).
- [13] Kauffman H. L. “An Invariant of Regular Isotopy”. *Transaction of The American Mathematical Society* , **Vol 318, número 2**, pp 417, (Abril 1990)
- [14] Kauffman H. L. “The Fibonacci Model and the Temperley-Lieb Algebra”. *arXiv:quant-ph/0407224v2 quant-ph*, (2005)
- [15] Kauffman H. L.; Lomonaco Jr. S. L. “Comparing Quantum Entanglement and Topological Entanglement”. *arXiv:quant-ph/0205137v1*, (2002)
- [16] Kauffman H. L.; Lomonaco Jr. S. L. “Braiding Operators are universal quantum gates”. *New Journal of Physics* , **6**, pp 134, (2004)
- [17] Kauffman H. L.; Lomonaco Jr. S. L. “The Fibonacci Model and the Temperley-Lieb Algebra”. *arXiv:0804.4304v1 quant-ph*, (2008)
- [18] Kauffman H. L.; Lomonaco Jr. S. L. “A Categorical Model for the Virtual Group”. *arXiv:1103.3158v1 math.GT* , (2011)
- [19] Kauffman H. L.; Lomonaco Jr. S. L. “Topological Quantum Information Theory”. Disponível em <http://www.math.uic.edu/~kauffman/Quanta.pdf>. Acesso em 29 de setembro de 2011.
- [20] Kitaev A. I. “Fault-tolerant quantum computation by anyons”. *Annals of Physics*, **303**, pp. 2–30, (2003).
- [21] Kitaev A. I. “Anyons in an exactly solved model and beyond”. *Annals of Physics*, **321**, pp. 2–110, (2006).
- [22] Leinass J. M.; Myrheim J. “On the Theory of Identical Particles,” *Il Nuovo Cimento*, **37 B, N.1** pp. 1–23, (1977).
- [23] Nayak C.; Simon S.H.; Stern A.; Freedman M.; Das Sarma S. “Non-Abelian anyons and topological quantum computation”. *Rev. of mod. phys.*, **80**, pp.1083, (july-september 2008).

- [24] Nielsen M. A.; Chuang I. L. *Computação Quântica e Informação Quântica*. Bookman, (2003). 733 p.
- [25] 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 29 de setembro de 2011.
- [26] Preskill J. “Lectures notes for physics 219: quantum error correction”. *California Institute of Technology*, (1999).
- [27] Preskill J. “Lectures notes for physics 219: quantum computation”. *California Institute of Technology*, (2004).
- [28] Rivest R.L.; Shamir A.; Adleman L. “A Method for Obtaining Digital Signatures and Public-Key Cryptosystems”. (1977).
- [29] Shor P. W. “Algorithms for quantum computation: Discrete logarithms and factoring,” *Proceedings of the 35th Annual Symposium on Foundations of Computer Science*, pp. 124, (1994).
- [30] Simon S. H.; Bonesteel N. E.; Freedman M. H.; Petrovic N.; Hormozi L. “Topological Quantum Computing with Only One Mobile Quasiparticle”. *Phys. Rev. Lett.*, **96**, pp. 070503-1, (february 2006).
- [31] Stern A. “Anyons and the quantum Hall effect-A pedagogical review”. *Annals of Physics*, **323**, pp. 204–249, (2008).
- [32] Wang Z. *Topological Quantum Computation*. Regional Conferences Series in Mathematics number 112, AMS, (2010). 115 p.
- [33] Xu H.; Taylor J. M. “Unified approach to topological quantum computation with anyons: From qubit encoding to Toffoli gate”. *Phys. Rev. A*, **84**, pp.012332-1, (2011).

