TRANSFORMADA DE FOURIER QUÂNTICA NO GRUPO DIEDRAL

Demerson Nunes Gonçalves

TESE SUBMETIDA AO CORPO DOCENTE DA COORDENAÇÃO DE FORMAÇÃO DE RECURSOS HUMANOS DO LABORATÓRIO NACIONAL DE COMPUTAÇÃO CIENTÍFICA COMO PARTE DOS REQUISITOS NECESSÁRIOS PARA A OBTENÇÃO DO GRAU DE MESTRE EM MODELAGEM COMPUTACIONAL

Aprovada por:

Prof. Renato Portugal, D.Sc.

Prof. Maurício Vieira Kritz, D. Sc.

Prof. Gilson Antônio Giraldi, D.Sc.

Prof. Eduardo do Nascimento Marcos, Ph.D

PETROPOLIS, RJ - BRASIL

MARÇO DE 2005

GONÇALVES, DEMERSON NUNES

Transformada de Fourier Quântica no Grupo Diedral [Petropólis] 2005

VIII, 89 p. 29,7 cm (MCT/LNCC), M.Sc., Modelagem Computacional, 2005)

Tese - Laboratório Nacional de Computação Científica, LNCC

1. Transformada de Fourier Quântica

I. MCT/LNCC II. Título (série)

Aos meus pais

Agradecimentos

Agradeço a todos que me ajudaram com seu apoio e suas sugestões, entre os quais, não posso deixar de citar meu orientador, pela sugestão do tema, e pela dedicação e incentivo demonstrados durante o desenvolvimento desta dissertação, à minha família pelo carinho e incentivo nesses dois anos de trabalho e ausência do lar. Agradeço a FAPERJ pelo apoio financeiro e agradeço principalmente a DEUS, por tudo.

Resumo da Tese apresentada à MCT/LNCC como parte dos requisitos necessários para a obtenção do grau de Mestre em Ciências (M.Sc.)

TRANSFORMADA DE FOURIER QUÂNTICA NO GRUPO DIEDRAL

Demerson Nunes Gonçalves

Março/2005

Orientador: Renato Portugal

Modelagem Computacional

Descrevemos a transformada de Fourier em grupos não abelianos motivado por suas aplicações em algoritmos quânticos para a computação quântica. A transformada de Fourier em grupos é descrita em termos das representações irredutíveis da teoria da representação de grupos finitos. Essa teoria é a peça chave para atacar o famoso Problema do Subgrupo Escondido (PSE), que consiste na determinação de geradores de um subgrupo, uma vez dada um "oráculo" que diz se um elemento pertence ou não a esse subgrupo.

Neste trabalho, nós apresentamos um algoritmo quântico para o PSE Diedral (D_N). A complexidade de tempo do nosso algoritmo é $O(N \log^2 N)$. Ele é baseado no método padrão de solução: a transformada de Fourier de um estado quântico $|\psi\rangle$ é calculada e medida. O objetivo do nosso algoritmo é reconstruir o subgrupo H de D_N gerado por uma reflexão, uma vez dado uma função f em D_N, constante nas classes laterais de H e distinta em cada classe lateral.

Abstract of Thesis presented to MCT/LNCC as a partial fulfillment of the requirements for the degree of Master of Science (M.Sc.)

QUANTUM FOURIER TRANSFORM ON THE DIHEDRAL GROUP

Demerson Nunes Gonçalves

March /2005

Advisor: Renato Portugal

Computational Modelling

We describe the Fourier transform in non-abelian groups motivated by its application in quantum algorithms for quantum computation. The Fourier transform is described in terms of the irreducible representation of finite representation group theory. This theory is the main tool to solve the famous Hidden Subgroup Problem (HSP), which consists to find generators of a subgroup once given an "oracle", that tell us if an element belongs to this subgroup.

In this work, we present a quantum algorithm for the Dihedral (D_N) HSP. The time complexity of our algorithm is $O(N \log^2 N)$. It is based on the standard method of solution: the Fourier transform of quantum state $|\psi\rangle$ is computed and measured. The objective of our algorithm is reconstruct the subgroup H of D_N generated by a reflection, once given a function f in D_N, constant in the lefts cosets of H, and distinct in each coset.

Sumário

1 Introdução **1**
1.1 Notação 4
1.2 Q-bits 5
1.3 Computação Quântica 6

2 Teoria da Representação de Grupos Finitos **9**
2.1 Teoria de Grupos 9
2.2 Teoria da Representação 13
2.2.1 Exemplos de Representações 15
2.2.2 Subrepresentações 17
2.3 Representações Unitárias 18
2.4 Análises de Representações; Redutibilidade; Representações Irredutíveis 20
2.4.1 Critério de Redutibilidade 22
2.5 Teoria de Caráter 26
2.6 Grupos Abelianos 33

3 Transformada de Fourier Quântica e o Problema do Subgrupo Escondido em Grupos Abelianos **36**
3.1 Problema do Subgrupo Escondido 38
3.2 O Problema de Simon 39
3.3 A Transformada de Fourier em Grupos Abelianos 41
3.4 O Subgrupo Ortogonal 43
3.5 O Algoritmo de Shor 48

4 Representações Irredutíveis do Grupo Diedral **50**
4.1 Representações Uni-Dimensionais do Grupo D_N 51
4.2 Representações Induzidas 54
4.3 Representações Bi-Dimensionais para D_N Induzidas por C_N 56

5 Transformada de Fourier no Grupo Diedral **63**
5.1 Transformada de Fourier em Grupos Genéricos 63
5.2 O Método Padrão de Solução 67
5.2.1 A Probabilidade de Medir ρ 71
5.3 O Método Padrão de Solução (MPS) Aplicado ao Grupo Diedral . . 73

6 Conclusão **80**

Referências Bibliográficas **82**

Apêndice **84**

A Demonstrações do Lema de Schur e das Relações de Ortogonalidade de Caráteres **84**

Capítulo 1

Introdução

A motivação para estudar a transformada de Fourier em grupos não abelianos vem da aplicação em algoritmos quânticos para a computação quântica. A transformada de Fourier quântica é a peça chave de algoritmos quânticos com ganho exponencial em relação ao seus equivalentes clássicos, como por exemplo, o algoritmo de Shor para fatoração. Neste trabalho, estaremos particularizando o cálculo da transformada de Fourier para o grupo Diedral por dois motivos: O primeiro é que a transformada de Fourier pode ser calculada eficientemente neste grupo (ROTTELER & BETH, 1998). O segundo motivo, é que uma vez entendido o cálculo da transformada de Fourier no grupo Diedral, estaremos aptos para encarar um problema mais difícil, que é a extensão para grupos genéricos. Faremos agora uma breve revisão do contexto histórico para localizar a importância desse problema.

A computação quântica teve início na década de 80 com os trabalhos de (FEYNMAN, 1982) e (BENIOFF, 1985). Feynman argumentou que um computador clássico pode simular com eficiência a física clássica, mas o mesmo não ocorre com a física quântica, uma vez que a dimensão do espaço de Hilbert cresce exponencialmente em

função do número de partículas acrescentadas ao sistema. Feynman perguntou se um dispositivo que usasse as leis da mecânica quântica para realizar cálculos não poderia simular eficientemente a própria mecânica quântica. Os argumentos de Feynman estimularam David Deutsch a generalizar o modelo mais fundamental da computação clássica, a saber a máquina de Turing, para o seu equivalente quântico num trabalho histórico de 1985 (DEUTSCH, 1985). Posteriormente generalizou também o modelo de circuitos baseado em portas lógicas. Operadores unitários tomaram o lugar das usuais portas lógicas AND, OR e NOT. O modelo de circuitos é o modelo adequado para o desenvolvimento de novos algoritmos. Baseado nele, (SHOR, 1997) elaborou um algoritmo exponencialmente mais rápido para fatoração de números inteiros e cálculo de logaritmo discreto. Esses algoritmos permitem a quebra dos principais códigos de criptografia usado atualmente, como RSA, Diffie-Hellman e ElGamal (KOBLITZ, 1998), caso um computador quântico de tamanho razoável esteja disponível.

Vários novos algoritmos quânticos mais rápidos que os equivalentes clássicos têm sido desenvolvidos, porém são os algoritmos exponencialmente mais rápidos que justificam investimento na difícil tarefa de construção de um computador quântico. Esta última classe tem crescido muito lentamente.

Uma importante conquista neste contexto de algoritmos quânticos exponencialmente mais rápidos, seria a extensão para grupos arbitrários. A extensão para grupos comutativos e grupos não comutativos com subgrupos normais já foi feita (veja (JOZSA, 1998) e (HALLGREN *et al*, 2003)). O fato de que a transformada de Fourier quântica pode ser calculada eficientemente em grupos abelianos é o ponto chave da solução do problema do subgrupo escondido abeliano, do qual o algoritmo

de Shor para fatoração é um caso particular, como veremos no Capítulo 3.

O problema do subgrupo escondido (PSE) consiste de uma função $f : G \to S$ de um grupo G finitamente gerado, para um conjunto S qualquer, de modo que se H é um subgrupo de G então f será constante nas classes laterais (à esquerda) de H e distinta em cada classe lateral. O problema é achar um conjunto gerador para H. Para grupos abelianos, uma solução eficiente desse problema implica em algoritmos quânticos eficientes para fatoração, como dissemos agora a pouco, e também para o cálculo de logaritmo discreto (AHN, 2002). Mas para o caso não abeliano o PSE é considerado um dos mais importantes desafios presentes na computação quântica atualmente. A principal ferramenta usada por algoritmos quânticos em tempo polinomial para o PSE é a transformada de Fourier. A transformada de Fourier em grupos não abelianos foi desenvolvida na década de 90 com os trabalhos de (MASLEN & ROCKMORE, 1997) e (MASLEN, 1998). A descrição matemática é bem mais complexa do que a transformada de Fourier de funções de variáveis complexas, pois em grupos ela é descrita em termos das representações irredutíveis da teoria da representação de grupos finitos (veja Capítulo 5). Assim para que computadores quânticos possam resolver o PSE eficientemente em grupos genéricos é necessário que existam algoritmos quânticos eficientes para a transformada de Fourier. Uma boa aplicação, caso tenhamos algoritmos quânticos com complexidade polinomial para o PSE, é a resolução de problemas da classe NP, como por exemplo a determinação de isomorfismos de grafos (para maiores detalhes veja (AHN, 2002)).

As próximas subseções destinam-se a dar algum subsídio sobre computação quântica. Entretanto, gostaríamos de alertar o leitor que não se trata de uma revisão, pois o objetivo desta dissertação é abordar um contexto que não foi introduzido nos

cursos de Computação Quântica I e II ministrados no LNCC. Para uma boa revisão sobre estes tópicos consulte as referências (LAVOR *et al*, 2003a), (LAVOR *et al*, 2003b) e (CHUANG & NIELSEN, 2000).

1.1 Notação

Seja $\mathcal{H}_n$ um espaço vetorial complexo de dimensão n com produto interno

$$(|x\rangle, |y\rangle) = \sum_{i}^{n} x_i^* y_i, \tag{1.1}$$

onde $|x\rangle, \ |y\rangle \in \mathcal{H}_n$ e x_i^* é o complexo conjugado de x_i. Os elementos de $\mathcal{H}_n$ são cadeias de bits de tamanho n formados por 0 e 1, ou seja, uma sequênica numérica de n termos formada pelos elementos do conjunto $\{0, 1\}$. Note que usamos a notação de Dirac para representar os vetores em $\mathcal{H}_n$. Esta notação é muito usada na mecânica quântica e agora na computação quântica.

O espaço $\mathcal{H}_n$ é um espaço de Hilbert com o produto interno definido acima. Se $|x\rangle$ é um vetor no espaço de Hilbert de dimensão finita, denotamos o dual de $|x\rangle$ como sendo $\langle x| = |x\rangle^\dagger$, onde o símbolo † indica o transposto conjugado. Isto nos motiva a redenotar o produto interno dado em (1.1) como

$$(|x\rangle, |y\rangle) = \langle x|y\rangle .$$

Assim a norma de um vetor $|x\rangle$ associado a este produto interno é $\| |x\rangle \| = \sqrt{\langle x|x\rangle}$.

Chamaremos de base computacional para o espaço de Hilbert a base formada

pelos vetores

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix}, \quad |1\rangle = \begin{bmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{bmatrix}, \ \ldots |n-1\rangle = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{bmatrix}. \tag{1.2}$$

Note a que base computacional é ortonormal já que $\langle i|j\rangle = \delta_{ij}$, para todo $i, j = 0, \ldots, n$.

1.2 Q-bits

Um q-bit é uma abstração de uma particula quântica de dois níveis, da mesma forma que um bit é uma abstração de um dispositivo clássico que pode armazenar uma de duas posições, 0 ou 1. Enquanto um dispositivo clássico armazena sempre ou na posição 0 ou na posição 1, uma partícula quântica pode assumir uma "superposição" dos dois níveis, e esta superposição pode ser descrita por um vetor unitário em $\mathcal{H}_2$, isto é, um vetor

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle \tag{1.3}$$

onde α, β são números complexos satisfazendo

$$|\alpha|^2 + |\beta|^2 = 1. \tag{1.4}$$

Por sua vez, um sistema quântico de n q-bits é descrito por um vetor unitário no espaço $\mathcal{H}_{2^n}$.

Uma *medida* é a abstração de um procedimento físico que obtêm informações

sobre o estado de uma partícula quântica. Uma medida é representada matematicamente como a projeção de um estado quântico (vetor) num par de subspaços ortogonais. Por exemplo, uma medida do estado (1.3) na base computacional projeta o estado $|\psi\rangle$ nos subspaços gerados por $|0\rangle$ e $|1\rangle$ respectivamente, produzindo o estado $|0\rangle$ com probabilidade $|\alpha|^2$ e $|1\rangle$ com probabilidade $|\beta|^2$.

1.3 Computação Quântica

Usando um computador clássico, o que seria possível fazer com apenas um bit? A resposta para esta pergunta é bem simples. Num modelo de circuitos clássicos, podemos ver que existem apenas duas possibilidades. A primeira é descrita pela porta lógica NOT. A figura (1.1) mostra que se a entrada do computador for o bit i, a saída será o bit NOT(i). Se $i = 0$ então a saída é 1, se $i = 1$ então a saída é 0. A segunda possibilidade é ter como saída a própria entrada. Neste caso a representação é simplesmente um fio ligando a entrada i na saída i.

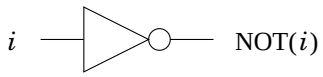

FIGURA 1.1: A porta lógica clássica NOT.

Num computador quântico de apenas 1 q-bit, a entrada é um estado quântico $|\psi\rangle = 0$ ou $|\psi\rangle = 1$. As leis da mecânica quântica determinam que se o computador estiver isolado, a direção de $|\psi\rangle$ pode mudar mas não a sua norma. Na Álgebra Linear isso é descrito pela ação de um operador unitário U, que é uma matriz complexa 2×2 satisfazendo

$$UU^{\dagger} = I.$$

Veja na figura (1.2) um modelo de circuito quântico. Assim a saída do computador

quântico é o estado $U|\psi\rangle$. Este estado pode estar em superposição, entretanto, precisamos observá-lo para obtermos informações úteis. Essa medida faz o estado $U|\psi\rangle$ ser projetado em $|0\rangle$ ou em $|1\rangle$ de acordo com as suas respectivas probabilidades.

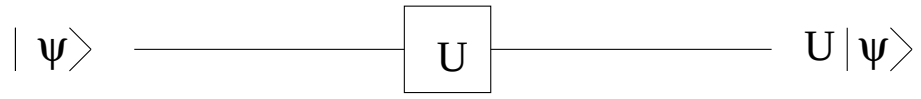

FIGURA 1.2: Um circuito quântico de 1 q-bit.

Para considerarmos um computador quântico com mais de 1 q-bit é necessário introduzirmos os conceitos de *produto tensorial* e *emaranhamento quântico*, mas não faremos isto aqui.

Em linhas gerais podemos definir a computação quântica como estados quânticos que são transformados pelas aplicações de operadores unitários. Assim, da mesma forma que computadores clássicos podem ser vistos como uma transformação num sistema de n bits, o computador quântico pode ser visto como uma máquina de n q-bits, onde são aplicados operadores unitários até que algum estado desejado seja encontrado, e então o resultado é medido.

Este trabalho está organizado como segue. No Capítulo 2, introduziremos de forma rápida o conceito de grupos finitos e daremos mais ênfase ao conceito de representações de grupos. Daremos também alguns exemplos de representações e exploraremos a relação entre representações e caráteres. No Capítulo 3, definiremos a transformada de Fourier em grupos abelianos e a relação com o problema do subgrupo escondido. Veremos que os algoritmos de Simon e Shor para fatoração são casos particulares do PSE abeliano. O Capítulo 4 é voltado para o estudo das representações irredutíveis do grupo Diedral. Mostraremos neste capítulo que as representações irredutíveis de D_N possuem graus no máximo igual a 2. No Capítulo 5, faremos uso destas representações quando aplicarmos a transformada de Fourier

no grupo Diedral, e apresentaremos um algoritmo quântico para o PSE Diedral com complexidade de tempo exponencial. Finalizaremos o capítulo indicando o que está feito na literatura no sentido da resolução PSE Diedral. Finalmente, no Capítulo 6, coligimos as conclusões obtidas neste trabalho. Apresentaremos no apêndice as demonstrações do Lema de Schur e das relações de ortogonalidades de caráteres.

Capítulo 2

Teoria da Representação de Grupos Finitos

2.1 Teoria de Grupos

Nesta seção, daremos alguns conceitos básicos sobre a teoria de grupos finitos e a notação necessária para o entendimento deste capítulo. Para um estudo mais detalhado sobre teoria de grupos veja (GARCIA & LEAQUAIN, 1998).

Dado um conjunto não vazio G e uma operação binária $* : G \times G \to G$, dizemos que G é um *Grupo* com respeito a operação $*$ se as seguintes propriedades forem satisfeitas:

(1) Associatividade: dados $a, b, c \in G$

$$a * (b * c) = (a * b) * c.$$

(2) Elemento Neutro: existe um elemento $e \in G$ tal que para todo $a \in G$ temos

$$a * e = e * a = a.$$

(3) Elemento Inverso: dado um elemento $a \in G$ qualquer, existe um elemento $a' \in G$ (o inverso de a) tal que

$$a * a' = a' * a = e.$$

Por simplicidade denotaremos $a * b$ por ab para todo $a, b \in G$.

Dizemos que um grupo G é finito se G possui uma quantidade finita de elementos e denotaremos esta quantidade (ordem de G) por $|G|$. Daqui por diante assumiremos sempre G finito.

Sabemos que um subgrupo H de G (denotamos $H \leq G$), é um subconjunto de G que é fechado com respeito a operação do grupo. Uma *classe lateral* (à esquerda) de H em G é um conjunto da forma $gH = \{gh : h \in H\}$, com $g \in G$. Note que $|H| = |gH|$ (pois a aplicação $h \longmapsto gh$ é uma bijeção). Para quaisquer $g_1, g_2 \in G$, g_1H e g_2H ou são idênticas ou disjuntas. De fato, sejam x, y elementos em H tais que $g_1x = g_2y$ (isto é, g_1H e g_2H possuem pelo menos um elemento em comum). Daí vem $g_1 = g_2yx^{-1}$. Mas yx^{-1} é elemento de H. Se g_1x' é um elemento arbitrário de g_1H, com $x' \in H$, então $g_1x' = g_2(yx^{-1})x'$. Como $(yx^{-1})x'$ pertence a H, concluímos que g_1x' pertence a g_2H. Dessa forma, g_1H está contido em g_2H. Analogamente, g_2H está contido em g_1H, e assim $g_1H = g_2H$. Em particular, para qualquer subgrupo H de G podemos decompor G como uma união disjunta de classes laterais de H, isto é, qualquer elemento de G pertence a uma, e somente uma, classe lateral de H (veja figura 2.1 abaixo). Temos também, que o número total de *diferentes*

classes laterais de H em G, denotado por $[G : H]$, é dado por $[G : H] = \frac{|G|}{|H|}$.

Para $g \in G$ e H um subgrupo de G, usaremos o símbolo gHg^{-1} para denotar o conjunto $gHg^{-1} = \{ghg^{-1} \ : h \in H\}$. Recordamos também que um subgrupo H de G é dito *normal* se $H = gHg^{-1}$ para todo $g \in G$. Se H é um subgrupo normal de um grupo G, então o conjunto formado pelas classes laterais (à esquerda) de H em G forma um grupo com respeito a operaçao em G. Este grupo, denotado por G/H, é chamado de grupo *quociente*.

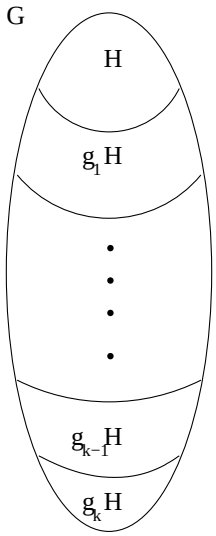

FIGURA 2.1: Decomposição de G em classes laterais disjuntas de H.

Um conceito importante (principalmente quando tratamos grupos em ciência da computação) é o de conjunto de geradores. Em qualquer grupo G, um subconjunto S de G, com a propriedade de que todo elemento de G pode ser escrito como um produto de elementos de S e seus inversos, é chamado um *conjunto de geradores* de G, e indicaremos por $G = \langle S \rangle$. Também, dados elementos $g_1, \ldots, g_k$ de um grupo G, denotaremos por $\langle g_1, \ldots, g_k \rangle$ o subgrupo gerado por $g_1, \ldots, g_k$, isto é, o subgrupo que resulta se tomarmos todos os possíveis produtos dos elementos de $\{g_1, \ldots, g_k\}$ e seus inversos. Se tomarmos G como sendo o conjunto dos inteiros sob a operação de adição, podemos ver facilmente que $G = \langle 1 \rangle$. O seguinte teorema é importante,

pois ele têm implicações em algoritmos quânticos, como veremos no Capítulo 3.

Teorema 2.1 *Todo grupo G de tamanho $|G| > 1$ tem um conjunto gerador de tamanho no máximo $\lfloor \log_2 |G| \rfloor$.*

Prova. Seja $g_1 \in G$ tal que $g_1 \neq e$. Então $|\langle g_1 \rangle| \geq 2$, pois, pelo menos g_1 e g_1^2 estão em $\langle g_1 \rangle$. Se $G \neq \langle g_1 \rangle$ então seja $g_2 \in G - \langle g_1 \rangle$. Agora temos que $|\langle g_1, g_2 \rangle| \geq 2^2$, pois, $g_1, g_1^2, g_2 g_1,$ e $g_2 g_1^2$ são todos diferentes. Se $\langle g_1, g_2 \rangle \neq G$ então seja $g_3 \in G - \langle g_1, g_2 \rangle$. Agora temos que $|\langle g_1, g_2, g_3 \rangle| \geq 2^3$. Continuando este procedimente vemos que $|\langle g_1, \ldots, g_{\log_2 |G|} \rangle| \geq 2^{\log_2 |G|} = |G|$. Assim concluímos nossa prova.

■

Outro conceito que vem da teoria de grupos e que é de grande importância na computação quântica é o de *classes de conjugação.*

Seja G um grupo, vamos definir uma relação de equivalência em G da seguinte forma:

$$x, y \in G,\ x \overset{G}{\sim} y \Leftrightarrow \exists\ g \in G \text{ tal que } y = g^{-1} x g.$$

Proposição 2.1 *Seja G um grupo. A relação $\overset{G}{\sim}$ define uma relação de equivalência em G.*

Prova.

(i) $x \overset{G}{\sim} x\ \forall\ x \in G$, pois $x = e^{-1} x e,\ \forall\ x \in G$.

(ii) se $x \overset{G}{\sim} y$ então $y \overset{G}{\sim} x$. Se $x \overset{G}{\sim} y$ existe $g \in G$ tal que $y = g^{-1} x g$. Assim, se $u = g^{-1}$ temos $x = u^{-1} y u$, isto é, $y \overset{G}{\sim} x$.

(iii) Se $x \overset{G}{\sim} y$ e $y \overset{G}{\sim} z$ então $x \overset{G}{\sim} z$. De fato, se $y = g^{-1} x g$ e $z = h^{-1} y h$ onde $g, h \in G$ temos $z = u^{-1} x u$ onde $u = gh$, e isto demonstra a proposição (2.1).

■

Se $x \overset{G}{\sim} y$ dizemos que x e y são elementos conjugados em G. Assim podemos definir a classe de conjugação (em G) determinada pelo elemento $x \in G$ como sendo

$$\mathcal{C}_x = \{y : x \overset{G}{\sim} y\}.$$

2.2 Teoria da Representação

A principal ferramenta usada por algoritmos quânticos em tempo polinomial para o Problema do Subgrupo Escondido é a transformada de Fourier. Para definir a transformada de Fourier em grupos, nós necessitamos de um conhecimento básico de teoria da representação, que daremos logo a seguir. Nesta seção, introduziremos o conceito de representação, e mais tarde o conceito de caráteres, e a fundamental correspondência entre estes. Um estudo mais completo desses tópicos podem ser encontrados em (SERRE, 1997).

Seja V um espaço vetorial sobre o corpo $\mathbb{C}$ dos números complexos e seja $GL(V)$ o grupo dos *isomorfismos* de V em V. Assumiremos que V é de dimensão finita. Um elemento $a \in GL(V)$ é, por definição, uma função linear de V em V que tem um inverso a^{-1}; esta inversa é linear. Como assuminos V de dimensão finita, temos que V possui uma base finita (e_i) de n elementos, cada aplicação linear $a : V \to V$ é definida por uma matriz quadrada (a_{ij}) de ordem n. Os coeficientes a_{ij} são números complexos e eles são obtidos expressando as imagens $a(e_j)$ em função da base (e_i):

$$a(e_j) = \sum_i a_{ij} e_i.$$

Assim identificamos $GL(V)$ como o grupo das matrizes invertíveis (com a opera-

ção do grupo sendo a multiplicação ususal de matrizes) de ordem n com coeficientes complexos. Antes de darmos a definição formal de uma representação, consideraremos a seguinte defição de homomorfismo de grupos.

Definição 2.1 *Sejam G e H grupos. Uma aplicação $\rho : G \to H$ que satisfaz $\psi(xy) = \rho(x)\rho(y)$ para todo $x, y \in G$ é chamada de homomorfismo.*

Definição 2.2 *Seja G um grupo finito e V um espaço vetorial de dimensão finita sobre $\mathbb{C}$. Uma representação linear de G em V é um homomorfismo ρ de G em $GL(V)$. Em outras palavras, associamos com cada elemento $g \in G$ um elemento $\rho(g)$ de $GL(V)$ de modo que $\rho(gh) = \rho(g)\rho(h)$ para todo $g, h \in G$ (escreveremos freqüentemente ρ_g em vez de $\rho(g)$). Se a dimensão de V é n, então dizemos que ρ é uma representação de grau n.*

Segue das propriedades de homomorfismo que

$$\rho(e) = I, \tag{2.1}$$

onde I denota a matriz identidade em $GL(V)$. Uma consequência imediata de (2.1) e o fato $\rho(gh) = \rho(g)\rho(h)$ é que

$$\rho(g^{-1}) = \rho(g)^{-1}. \tag{2.2}$$

Quando ρ é dado, dizemos que V é um espaço representação de G. Na maior parte do tempo, contudo, usaremos um abuso de linguagem e diremos que V é uma representação de G.

Se um homomorfismo de G em $GL(V)$ é um isomorfismo, então a representação é dita ser *fiel*. Neste caso teremos $|G| = |GL(V)|$. Em geral muitos elementos em G

são levados na matriz identidade. É um resultado conhecido da teoria de grupos que o núcleo deste homomorfismo, que denotaremos por H, forma um subgrupo normal de G, e o grupo de matrizes $\rho(G)$ é uma representação fiel do grupo quociente G/H. Logo, se temos uma representação para o grupo quociente G/H relativa ao subgrupo normal H, automaticamente temos uma representação para todo o grupo G. Nesta representação todos os elementos numa classe lateral são levados na mesma matriz.

Agora introduziremos o conceito de isomorfismo de representações.

Definição 2.3 *Sejam ρ e ρ' duas representações do mesmo grupo G nos espaços vetoriais V e V' respectivamente. Estas representações são ditas isomorfas se existe um isomorfismo linear $\tau : V \to V'$ que "transforma" ρ em ρ', isto é, que satisfaz a identidade $\tau \circ \rho(g) = \rho'(g) \circ \tau$ para todo $g \in G$.*

Considere agora R_g e R'_g como sendo as matrizes das respectivas representações ρ_g e ρ'_g numa base (e_i) de V. Dizer que ρ e ρ' são representações isomorfas equivale a dizer que existe uma matriz invertível T tal que $TR_g = R'_g T$ para todo $g \in G$. Isto é,

$$R'_g = TR_gT^{-1}.$$

2.2.1 Exemplos de Representações

Exemplo 2.1 *A Representação Trivial.*

A representação trivial 1_G leva cada elemento do grupo $g \in G$ no elemento identidade $1 \in \mathbb{C}^*$ (neste contexto $\mathbb{C}^*$ denota o grupo multiplicativo dos números complexos não nulos). De forma equivalente, 1_G leva todo elemento do grupo $g \in G$ na matriz $(1)_{1\times 1}$.

Exemplo 2.2 *Representação Permutação.*

Suponha que o grupo G atua num conjunto $X = \{1, 2, \ldots, n\}$ de modo que para cada $g \in G$ temos uma permutação de X da forma

$$i^g = j, \ \text{ com } 1 \leq i, j \leq n.$$

Agora seja V um espaço n-dimensional com base $B = \{e_1, \ldots, e_n\}$. Para cada $g \in G$ definimos $\rho(g)$ tal que

$$e_i\rho(g) = e_{i^g} = e_j, \ \text{ com } 1 \leq i, j \leq n.$$

Então $\rho(g)$ permuta os elementos da base de V da mesma maneira que G atua no conjunto X.

Vamos mostrar que a representação permutação é uma representação de G. Com efeito,

$$e_i\rho(gh) = e_{i^{gh}} = e_{(i^g)^h} = e_{i^g}\rho(h) = e_i\rho(g)\rho(h).$$

Portanto, a aplicação ρ_G é um homomorfismo definindo uma representação para G.

Vamos mostrar agora que esse homomorfismo é bijetivo, i.e.

$$g = h \Leftrightarrow \rho(g) = \rho(h), \ g, h \in G.$$

($\Rightarrow$) Trivial.

($\Leftarrow$) $\rho(g) = \rho(h) \Rightarrow e_i\rho(g) = e_i\rho(h) \Rightarrow e_{i^g} = e_{i^h}$

$\Rightarrow i^g = i^h \Rightarrow g = h, \ \forall \ i.$

Portanto, ρ definido acima é um isomorfismo. O exemplo a seguir é um caso

particular da representação permutação.

Exemplo 2.3 *A Representação Regular.*

Seja V um espaço vetorial de dimensão $|G|$, com base $\{e_h\}_{h\in G}$ indexada pelos elementos h de G. A representação regular $\mathrm{reg}_G : G \to GL(V)$ resulta se mapearmos $\mathrm{reg}_G(g) : V \to V$ de modo que $e_h \mapsto e_{gh},\ \ \forall\, g, h \in G$.

De fato $\mathrm{reg}_G : G \to GL(V)$ é um homomorfismo, pois $\mathrm{reg}_G(gh)e_i = e_{ghi} = e_{g(hi)} = \mathrm{reg}_G(g)e_{hi} = \mathrm{reg}_G(g)\mathrm{reg}_G(h)e_i$.

2.2.2 Subrepresentações

Seja $\rho : G \to GL(V)$ uma representação linear e seja W o subspaço de V. Suponha que W seja invariante pela ação de G, isto é $\forall\ x \in W$ e $\forall\ g \in G$ temos $\rho_g x \in W$. A restrição ρ_g^W de ρ_g para W é um isomorfismo de W em W, e temos $\rho_{gh}^W = \rho_g^W \rho_h^W$. Assim $\rho^W : G \to GL(W)$ é uma representação linear de G em W. Dizemos que W é uma *subrepresentação* de V.

Exemplo 2.4 *Neste exemplo determinaremos uma subrepresentação para a representação regular.*

Seja $\rho = \mathrm{reg}_G$ uma representação regular de G e seja W um subspaço de dimensão 1 de V gerado por $x = \sum_{h\in G} e_h$. Então temos que $\rho_g(x) = x$ para todo $g \in G$. Consequentemente temos que ρ^W é uma subrepresentação de ρ isomorfa a representação trivial.

Antes de encerrarmos esta seção, vamos recordar alguns conceitos da álgebra linear necessários para o nosso trabalho. Sejam W e W' dois subspaços de V. Dizemos que V é uma *soma direta* de W e W' (escrevemos $V = W \oplus W'$) se para

cada $x \in V$ podemos escrever de forma única $x = w + w'$, com $w \in W$ e $w' \in W'$. Neste caso dizemos que W' é um complemento de W em V.

2.3 Representações Unitárias

Definição 2.4 *Se os operadores da representação de um grupo G são operadores unitários (ou as matrizes da representação são unitárias), então dizemos que a representação é unitária.*

Vimos que toda representação de G admite muitas (infinitas em geral) representações equivalentes. O teorema que vamos enunciar logo abaixo, nos diz que para grupos finitos, toda representação é equivalente a uma representação unitária.

Teorema 2.2 *Dada $\rho : G \to GL(V)$ uma representação. Existe pelo menos uma representação $\rho' : G \to GL(V)$ que é unitária e equivalente a ρ.*

Prova. Considere o espaço $V = \mathbb{C}^n$. Logo para todo $x, y \in V$ definimos o produto escalar

$$(x, y) = \sum_{i=1}^{n} x_i^* y_i.$$

Para quaisquer pares de vetores $x, y \in \mathbb{C}^n$, construímos a expressão

$$\{x, y\} = \frac{1}{|G|} \sum_{g \in G} (\rho_g(x), \rho_g(y)). \tag{2.3}$$

Podemos ver facilmente que a expressão (2.3) acima define um produto interno. Assim, note que $\forall\, h \in G$ temos:

$$\begin{aligned}\{\rho_h x, \rho_h y\} &= \frac{1}{|G|}\sum_{g\in G}(\rho_g\rho_h(x), \rho_g\rho_h(y)) \\ &= \frac{1}{|G|}\sum_{g\in G}(\rho_{gh}(x)\rho_{gh}(y)).\end{aligned}$$

Mas para h fixo, g percorre todos os elementos do grupo G, logo

$$\frac{1}{|G|}\sum_{g\in G}(\rho_g(x), \rho_g(y)) = \frac{1}{|G|}\sum_{g\in G}(\rho_{gh}(x)\rho_{gh}(y)),$$

e portanto,

$$\{\rho_h x, \rho_h y\} = \{x, y\}. \tag{2.4}$$

Agora, consideremos as bases u_i e v_i de V tais que:

$$(u_i, u_j) = \delta_{ij} = \{v_i, v_j\}.$$

Definimos o operador T tal que

$$v_i = Tu_i.$$

Já que $Tx = Tx_iu_i = x_iTu_i = x_iv_i$, temos então que

$$\begin{aligned}\{Tx, Ty\} = \{x_iv_i, y_jv_j\} &= x_i^*y_j\{v_i, v_j\} \\ &= x_i^*y_i = (x, y).\end{aligned} \tag{2.5}$$

Agora consideremos a representação equivalente definida por

$$R'_g = T^{-1}R_gT.$$

Segue que

$$\begin{aligned}(T^{-1}R_gTx, T^{-1}R_gTy) &= \{R_gTx, R_gTy\} \\ &\qquad\qquad\qquad\qquad [\text{de } 2.5] \\ &= \{Tx, Ty\} \qquad\qquad [\text{de } 2.4] \\ &= (x, y). \qquad\qquad [\text{de } 2.5]\end{aligned}$$

e, $R'_g = T^{-1}R_gT$ é unitária. Então para grupos finitos, podemos sem perda de generalidade escolher nossa representação como sendo unitária. Isto finaliza a prova.

2.4 Análises de Representações; Redutibilidade; Representações Irredutíveis

Dada uma representação $\rho : G \to GL(V)$, será que é possível escrevê-la numa representação mais simples? Imagine que todas as matrizes da representação tridimensional ρ são da forma

$$\begin{bmatrix} a_i & b_i & e_i \\ c_i & d_i & f_i \\ 0 & 0 & g_i \end{bmatrix}, \tag{2.6}$$

então o produto terá a seguinte forma

$$\begin{bmatrix} a_1a_2 + b_1c_2 & a_1b_2 + b_1d_2 & a_1e_2 + b_1f_2 + e_1g_2 \\ c_1a_2 + d_1c_2 & c_1b_2 + d_1d_2 & c_1e_2 + d_1f_2 + f_1g_2 \\ 0 & 0 & g_1g_2 \end{bmatrix}. \tag{2.7}$$

Vemos que a matriz no canto superior esquerdo é oriunda da representação bi-dimensional:

$$\begin{bmatrix} a_i & b_i \\ c_i & d_i \end{bmatrix}, \tag{2.8}$$

enquanto o canto inferior direito vem da representação uni-dimensional:

$$\begin{bmatrix} g_i \end{bmatrix}. \tag{2.9}$$

Entretanto, as matrizes da representação podem não ter a forma (2.6), mas se pudermos achar uma transformação de base que trás todas as matrizes da representação para forma (equivalente) (2.6), dizemos que a representação é redutível. Em geral, se acharmos uma base em que todas as matrizes R_g (esta é a matriz correspondente a ρ_g para $g \in G$) da representação n-dimensional podem ser convertidas para a forma

$$R_g = \begin{bmatrix} R_g^{(1)} & S_g \\ 0 & R_g^{(2)} \end{bmatrix}, \tag{2.10}$$

onde $R_g^{(1)}$ é uma matriz $m \times m$, $R_g^{(2)}$ é $(n-m)\times(n-m)$, S_g é uma matriz retangular $m \times (n-m)$, e 0 denota uma matriz $(n-m)\times m$, então dizemos que a representação R_g é *redutível*.

Note que a matriz produto

$$R_{gh} = R_g R_h = \begin{bmatrix} R_g^{(1)} R_h^{(1)} & R_g^{(1)} S_h + S_g R_h^{(2)} \\ 0 & R_g^{(2)} R_h^{(2)} \end{bmatrix}$$

tem a mesma forma de (2.10), e portanto as matrizes $R_{gh}^{(1)} = R_g^{(1)} R_h^{(1)}$ fornecem uma

representação m-dimensional, e as matrizes $R^{(2)}_{gh} = R^{(2)}_g R^{(2)}_h$ dão uma representação $(n-m)$-dimensional.

Agora nós transformaremos a base num espaço m-dimensinal de $R^{(1)}$ e tentaremos converter todas as matrizes $R^{(1)}_g$ para a forma (2.10), i.e.,

$$R^{(1)}_g = \begin{bmatrix} R^{(3)}_g & S'_g \\ 0 & R^{(4)}_g \end{bmatrix}, \tag{2.11}$$

onde $R^{(3)}$ é p-dimensional e $R^{(4)}$ é $(m-p)$-dimensional, e aplicamos o mesmo procedimento para a matriz $R^{(2)}_g$. Este processo claramente chega a um fim, e então temos todas as matrizes da representação ρ expressas na forma

$$R_g = \begin{bmatrix} R^{(1)}_g & & & S^{(1)}_g & & \\ & R^{(2)}_g & & S^{(2)}_g & & \\ & & R^{(3)}_g & S^{(3)}_g & & \\ & & & & & \\ & & & & R^{(k-1)}_g & S^{(k-1)}_g \\ 0 & 0 & 0 & 0 & 0 & R^{(k)}_g \end{bmatrix},$$

onde o conjunto $R^{(1)}_g, \ldots, R^{(k)}_g$ são representações irredutíveis de G de dimensão m_i ($n = \sum_{i=1}^{k} m_i$).

2.4.1 Critério de Redutibilidade

Voltando a (2.6), e considerando todos os vetores que estão no subspaço bidimensional das 2 primeiras componentes, temos que se aplicarmos a matrix (2.6)

em qualquer um destes vetores obtemos

$$\begin{bmatrix} a & b & e \\ c & d & f \\ 0 & 0 & g \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ 0 \end{bmatrix} = \begin{bmatrix} ax_1 + bx_2 \\ cx_1 + dx_2 \\ 0 \end{bmatrix},$$

que ainda está no subspaço $x_3 = 0$. Em outras palavras, o subspaço bi-dimensional é invariante sob todas as transformações do grupo. Por outro lado, os vetores com as componentes $x_1 = x_2 = 0$ são transformados em

$$\begin{bmatrix} a & b & e \\ c & d & f \\ 0 & 0 & g \end{bmatrix} \begin{bmatrix} 0 \\ 0 \\ x_3 \end{bmatrix} = \begin{bmatrix} ex_3 \\ fx_3 \\ gx_3 \end{bmatrix},$$

então o espaço (complementar) uni-dimensional da terceira componente é variante.

No caso de (2.10), o subspaço das m primeiras componentes é invariante:

$$\begin{bmatrix} R_g^{(1)} & S_g \\ 0 & R_g^{(2)} \end{bmatrix} \begin{bmatrix} x \\ 0 \end{bmatrix} = \begin{bmatrix} R_g^{(1)} x \\ 0 \end{bmatrix},$$

enquanto o complemento (subspaço $(n-m)$-dimensional) é variante:

$$\begin{bmatrix} R_g^{(1)} & S_g \\ 0 & R_g^{(2)} \end{bmatrix} \begin{bmatrix} 0 \\ x \end{bmatrix} = \begin{bmatrix} S_g x \\ R_g^{(2)} x \end{bmatrix}.$$

Em geral, se existe um subspaço de dimensão $m < n$ que é invariante sob todas as tranformações do grupo, a representação é redutível. Podemos escolher m novos vetores base neste subspaço, e completar o conjunto com $(n-m)$ outros vetores

base, de modo que obtenhamos n vetores base para todo o espaço n-dimensional. Nesta base, as matrizes da representação assumirão a forma (2.6).

Se não existe um subspaço próprio que é invariante, a representação é *irredutível*. Vamos resumir toda essa noção de redutibilidade com a seguinte definição.

Definição 2.5 *Seja $\rho : G \to GL(V)$ uma representação de G. Dizemos que ρ é irredutível se não existe nenhum subspaço invariante por G além do espaço nulo e do próprio V.*

Agora, suponhamos que seja possível achar uma base onde todas as matrizes da representação assumem a forma (2.10), mas com $S_g = 0$, i.e.,

$$R_g = \begin{bmatrix} R_g^{(1)} & 0 \\ 0 & R_g^{(2)} \end{bmatrix}, \tag{2.12}$$

neste caso dizemos que a representação é *completamente redutível*. Note ainda, que ambos os subspaços m-dimensional de $R_g^{(1)}$ e $(n-m)$-dimensional de $R_g^{(2)}$ são invariantes.

O espaço V é *decomposto* numa *soma direta* de $W^{(1)}$ e $W^{(2)}$,

$$V = W^{(1)} \oplus W^{(2)},$$

e a representação R_g numa soma direta de $R_g^{(1)}$ e $R_g^{(2)}$,

$$R_g = R_g^{(1)} \oplus R_g^{(2)}. \tag{2.13}$$

Agora vamos verificar se as representações $R_g^{(1)}$ e $R_g^{(2)}$ na equação (2.13) também são redutíveis. Note que podemos estudar $R_g^{(1)}$ e $R_g^{(2)}$ separadamente, já que podemos

tratar os espaços independentemente um do outro. Assim, uma transformação de coordenadas da forma

$$M = \begin{bmatrix} M_1 & 0 \\ 0 & 1 \end{bmatrix} \begin{matrix} \} \ m \\ \} \ n-m \end{matrix}$$

transforma somente o subspaço da representação $R_g^{(1)}$ e permanece com as matrizes de $R_g^{(2)}$ inalteradas. Continuando com este processo, podemos finalmente exibir R_g na forma

$$R_g = \begin{bmatrix} R_g^{(1)} & 0 & & 0 \\ 0 & R_g^{(2)} & & 0 \\ & & \ddots & \\ 0 & 0 & & 0 \\ 0 & 0 & 0 & R_g^{(k)} \end{bmatrix},$$

isto é, $R_g = R_g^{(1)} \oplus R_g^{(2)} \oplus \ldots \oplus R_g^{(k)}$, onde todas as $R_g^{(\nu)}$ são representações irredutíveis.

Dentre todas as representações irredutíveis $R_g^{(1)}, R_g^{(2)}, \ldots, R_g^{(k)}$, podem existir representações que são equivalentes a uma determinada representação irredutível deste conjunto. Representações irredutíveis equivalentes não podem ser consideradas distintas (representações equivalentes possuem o mesmo caráter - veja corolário 2.7.2), logo é provável que uma certa representação R_g possa conter em sua decomposição uma dada representação irredutível $R_g^{(\nu)}$ inúmeras vezes. Desta forma, obtemos a

seguinte expressão

$$R_g = a_1 R_g^{(1)} \oplus a_2 R_g^{(2)} \oplus \ldots \oplus a_r R_g^{(r)},$$

onde os a_ν são inteiros positivos.

Na seção (2.4), nós mostramos que para grupos finitos, sem perda de generalidade, as representações serão assumidas unitárias, portanto normais. Então segue do teorema Espectral da Álgebra Linear, que estas representações são diagonalizáveis por bloco, e portanto, completamente redutíveis. Assim concluímos que para grupos finitos, sempre é possível decompor representações como uma soma de representações irredutíveis.

Podemos resumir o que tratamos nesta seção com o seguinte teorema.

Teorema 2.3 *Toda representação de G é uma soma direta de representações irredutíveis de G.*

Na próxima seção, introduziremos um conceito fundamental em teoria da representação, o conceito de caráter de uma representação. Caráteres são fundamentais, pois o estudo de uma representação pode ser completamente reduzido ao estudo de seus caráteres, como veremos a seguir.

2.5 Teoria de Caráter

Seja V um espaço vetorial dotado da base (e_i) de n elementos, e seja a uma aplicação linear de V em V, com representação matricial (a_{ij}). Definimos o *traço* de a como sendo

$$\mathrm{Tr}(a) = \sum_i a_{ii}.$$

Definição 2.6 *Seja $\rho : G \to GL(V)$ uma representação. Para cada $g \in G$, seja $\chi_\rho(g) = Tr(\rho_g)$. O valor da função complexa χ_ρ em G assim obtido é chamado de caráter da representação ρ.*

As próximas duas proposições nos fornecem alguns fatos básicos sobre caráteres.

Proposição 2.2 *Se χ é o caráter de uma representação ρ de grau n, então nós temos:*

(i) $\chi(e) = n$.

(ii) $\chi(g^{-1}) = \chi(g)^* \ \forall \ g \in G$.

(iii) $\chi(hgh^{-1}) = \chi(g) \ \forall \ g, h \in G$.

Prova. (i) é trivial, pois $\rho(e)$ é a matriz identidade. Para (ii), assumiremos sem perda de generalidade que ρ_g é uma matriz unitária, logo

$$\|\rho_g x\|^2 = \|x\|^2 \tag{2.14}$$

para todo vetor x pertencente ao espaço V.

Sejam $\lambda_1, \ldots, \lambda_m$ os autovalores da representação ρ_g com respectivos autovetores $x_1, \ldots, x_m$. Note que $\|\rho_g x_i\| = |\lambda_i| \|x_i\|$. Assim segue da equação (2.14) que $|\lambda_i|^2 = 1$, mas como $1 = |\lambda_i|^2 = \lambda_i \lambda_i^*$, segue que $\lambda_i^* = \lambda_i^{-1}$. Logo,

$$\chi(g)^* = \mathrm{Tr}(\rho_g)^* = \sum_{i=1}^{m} \lambda_i^* = \sum_{i=1}^{m} \lambda_i^{-1} = \mathrm{Tr}[(\rho_g)^{-1}] = \mathrm{Tr}(\rho_{g^{-1}}) = \chi(g^{-1}).$$

(*iii*) Sabemos que $\mathrm{Tr}(ab) = \mathrm{Tr}(ba)$ é válido para duas aplicações lineares a e b quaisquer no espaço V. Assim temos

$$\begin{aligned} \chi_\rho(hgh^{-1}) &= \mathrm{Tr}(\rho_{hgh^{-1}}) = \mathrm{Tr}(\rho_h \rho_{gh^{-1}}) \\ &= \mathrm{Tr}(\rho_{gh^{-1}} \rho_h) = \mathrm{Tr}(\rho_{gh^{-1}h}) \\ &= \mathrm{Tr}(\rho_g) = \chi_\rho(g). \end{aligned} \tag{2.15}$$

■

Note que isto implica que duas representações isomorfas possuem o mesmo caráter. De fato, para uma matriz unitária u qualquer, nós temos

$$\chi_{u^{-1}\rho u}(g) = \mathrm{Tr}(u^{-1}\rho(g)u) = \mathrm{Tr}(\rho(g)uu^{-1}) = \mathrm{Tr}(\rho(g)) = \chi_\rho(g).$$

Observação 2.1 *Uma função f em G satisfazendo (iii) é chamada função de classe.*

Proposição 2.3 *Sejam $\rho^1 : G \to GL(V_1)$ e $\rho^2 : G \to GL(V_2)$ duas representações de G, e sejam χ_1 e χ_2 os seus respectivos caráteres. Então o caráter χ da representação $V_1 \oplus V_2$ é igual a $\chi_1 + \chi_2$.*

Prova. Sejam R^1_g e R^2_g as representações matriciais de ρ^1 e ρ^2, respectivamente. A representação $V_1 \oplus V_2$ é dada por

$$R_g = \begin{pmatrix} R^1_g & 0 \\ 0 & R^2_g \end{pmatrix}.$$

Então $\mathrm{Tr}(R_g) = \mathrm{Tr}(R^1_g) + \mathrm{Tr}(R^2_g)$, isto é, $\chi(g) = \chi_1(g) + \chi_2(g)$.

■

Exemplo 2.5 *O Caráter da Representação Regular.*

O caráter r_G da representação regular é dado por

$$r_G(g) = \begin{cases} |G| & \text{se} \quad g = e \\ 0 & \text{se} \quad g \neq e. \end{cases}$$

De fato, se $g \in G$ é tal que $g \neq e$, então $gh \neq h \; \forall \; h \in G$. Isto mostra que os termos da diagonal da matriz $\text{reg}_G(g)$ são nulos, em particular temos $\text{Tr}(\text{reg}_G(g)) = 0$. Por outro lado, se $g = e$, temos

$$\text{Tr}(\text{reg}_G(e)) = \text{Tr}(I) = |G|.$$

■

O próximo teorema define um produto interno que é de extrema importância em teoria de caráteres. Várias relações importantes de caráteres que usaremos no decorrer do nosso trabalho seguem deste teorema.

Teorema 2.4 *Se ϕ e ψ são duas funções complexas em G, definimos $(\phi|\psi) = \frac{1}{|G|}\sum_{g\in G}\phi(g)\psi(g)^*$. Então $(.|.)$ é um produto interno.*

Prova. Temos que verificar as três propriedades de produto interno:

- $(.|.)$ é linear no primeiro argumento: $(c_1\phi_1 + c_2\phi_2, \psi) = \frac{1}{|G|}\sum_{g\in G}(c_1\phi_1 + c_2\phi_2(g))\psi(g)^* = \frac{1}{|G|}\sum_{g\in G} c_1\phi_1(g)\psi(g)^* + \frac{1}{|G|}\sum_{g\in G} c_2\phi_2(g)\psi(g)^* = c_1(\phi_1|\psi) + c_2(\phi_2|\psi)$.

- $(\phi|\psi)^* = (\psi|\phi)$, trivial.

- $(\phi|\phi) \geq 0$, com $(\phi|\phi) = 0$ se, e somente se, $\phi = 0$: note que $aa^* \geq 0$ para qualquer número complexo a, sendo $aa^* = 0$ se, e somente se, $a = 0$.

O teorema a seguir nos ajudará na demonstração das relações de ortogonalidade dadas no teorema 2.6.

Teorema 2.5 (Lema de Schur) .

1. Sejam R_g e R'_g duas representações irredutíveis de um grupo G nos espaços V e W de dimensões n, m respectivamente. Suponha que exista uma matriz retangular $P_{m\times n}$ satisfazendo

$$PR_g = R'_g P, \ \forall \ g \in G. \tag{2.16}$$

Então $P = 0$ ou $n = m$ e P é não singular.

2. Se uma representação P comuta com todas as representações irredutíveis R_g de G, então P é um múltiplo escalar λI da matriz identidade.

Prova. Veja o apêndice.

Teorema 2.6 (Relações de ortogonalidade de caráteres) .

1. Se χ é o caráter de uma representação irredutível, então $(\chi|\chi) = 1$.

2. Se χ e χ' são os caráteres de duas representações irredutíveis não isomorfas, então $(\chi|\chi') = 0$.

Prova. Veja também o apêndice.

Teorema 2.7 *Seja V uma representação de G com caráter ϕ, e suponha que V se decomponha como uma soma direta de representações irredutíveis, i.e., $V = W_1 \oplus \ldots \oplus W_k$. Então, se W é uma representação irredutível com caráter χ, o número de W_i isomorfos à W é igual a $(\phi|\chi)$.*

Prova. Seja χ_i o caráter de W_i. Pela proposição (2.3), nós temos que $\phi = \chi_1 + \ldots + \chi_k$. Logo, $(\phi|\chi) = (\chi_1|\chi) + \ldots + (\chi_k|\chi)$. Mas, de acordo com o teorema (2.6), temos

$$(\chi_i|\chi) = \begin{cases} 1, & \text{se } W_i \simeq W \\ 0 & \text{caso contrário.} \end{cases}$$

Isto prova o teorema.

■

Corolário 2.7.1 *O número de W_i isomorfos a W não depende da decomposição escolhida.*

Prova. De fato, $(\phi|\chi)$ só depende do grupo G e não da decomposição escolhida.

■

O próximo corolário mostra a correspondência fundamental entre representações e seus caráteres, isto é, o estudo de um pode ser completamente reduzido ao estudo do outro.

Corolário 2.7.2 *Duas representações com mesmo caráter são isomorfas.*

Prova. Vimos no corolário (2.7.1), que se duas representações possuem o mesmo caráter, então elas possuem a mesma decomposição em representações irredutíveis. Logo, se elas possuem a mesma decomposição então elas são iguais.

■

Agora nós voltaremos a representação regular e mostraremos que ela é uma representação interessante pois contém todas as representações irredutíveis de um grupo finito G.

Lema 2.1 *Toda representação W_i irredutível de G está contida na representação regular de G com multiplicidade igual ao próprio grau n_i.*

Prova. Seja W_i uma representação irredutível de G com caráter χ_i. Sabemos que a quantidade de vezes que W_i está contido na representação regular é dada por

$$(\chi_i|r_G) = \frac{1}{|G|}\sum_{g\in G} r_G(g)\chi_i(g^{-1}) = \frac{1}{|G|}|G|\chi_i(e) = n_i.$$

■

Teorema 2.8 *Sejam $W_1, W_2, \ldots, W_k$ todas as representações irredutíveis não isomorfas de G e $n_1, \ldots, n_k$ os seus respectivos graus. Então*

1. O grau n_i satisfaz a relação $\sum_{i=1}^{k} n_i^2 = |G|$.

2. Se $g \in G$ é diferente de e, então $\sum_{i=1}^{k} n_i\chi_i(g) = 0$.

Prova. Pelo lema (2.1), nós temos $r_G(g) = \sum_{g\in G} n_i\chi_i(g) \ \ \forall\ g \in G$. Tomando $g = e$ obtemos *1*, e tomando $g \neq e$, obtemos *2*.

■

Lembrando que uma função f em G é chamada *função de classe* se $f(ghg^{-1}) = f(h)\ \forall\ g, h \in G$, temos o seguinte teorema.

Teorema 2.9 *Seja $\mathbb{H}$ o espaço das funções de classes em G. Os caráteres $\chi_1, \ldots, \chi_k$ das representações irredutíveis de G formam uma base ortonormal de $\mathbb{H}$.*

Prova. Veja (SERRE, 1997).

O teorema a seguir faz uma interessante relação entre as classes de conjugação de um grupo G e seus caráteres irredutíveis.

Teorema 2.10 *O número de representações irredutíveis de G (a menos de isomorfismos) é igual ao número de classes de conjugação de G.*

Prova. Sejam $\mathcal{C}_1, \ldots, \mathcal{C}_k$ as distintas classes de conjugação de G. Se f é uma função de classe em G, então f é constante em cada classe de conjugação $C_1, \ldots, C_k$, de modo que f é determinada por um representante λ_i de $\mathcal{C}_i$ escolhido arbitrariamente. Temos então que a dimensão do espaço $\mathbb{H}$ das funções classes é igual a k. Mas pelo teorema (2.9), k é o número de representações irredutíveis de G (a menos dos isomorfismos), logo temos o resultado desejado.

■

2.6 Grupos Abelianos

O problema de achar representações irredutívies para grupos abelianos é simples. De fato, seja G um grupo abeliano, isto é, $\forall\ h, g \in G$ temos $hg = gh$. Isto implica que cada classe de conjugação de G possui um único elemento. Assim o número de classes em G é igual a ordem $|G|$, mas isto implica que as representações irredutíveis de G devem ser uni-dimensionais. Então quando G é abeliano, a matriz representação coincide com o caráter, e daí temos uma simples multiplicação de números complexos. Podemos definir os caráteres de G como um homomorfismo $\chi : G \to \mathbb{C}^*$, isto é, cada caráter de G satisfaz a condição $\chi(g_1 g_2) = \chi(g_1)\chi(g_2)$ para quaisquer elementos g_1 e $g_2 \in G$. Note que $\chi(e) = 1$ e como G é finito temos que qualquer elemento $g \in G$ satisfaz a condição $g^{|G|} = e$. Logo $\chi(g)^{|G|} = \chi(g^{|G|}) = \chi(e) = 1$, então qualquer caráter de G é uma raíz $|G|-$ésima da unidade[1]. Note que se G for

[1]Uma raíz $|G|-$ésima da unidade é um número complexo x satisfando $x^{|G|} = 1$.

cíclico, então algum elemento $g \in G$ gera todo o grupo, $g^{|G|} = 1$, logo

$$\chi_k(g) = e^{\frac{2\pi ik}{|G|}} \qquad (k = 1, \ldots, |G|),$$

e o caráter de qualquer outro elemento de G pode ser obtido tomando potências de $\chi(g)$. Por exemplo, $\chi_k(g^m) = e^{\frac{2\pi km}{|G|}}$.

Um fato que nos ajudará a encontrar os caráteres de um grupo abeliano finito genérico, é que qualquer grupo abeliano finito pode ser decomposto como uma soma direta de grupos cíclicos de ordens $t_1, t_2, \ldots, t_N$ (veja (LANG & ADISAN-WESLEY, 1993)), isto é,

$$G \simeq \mathbb{Z}_{t_1} \oplus \mathbb{Z}_{t_2} \oplus \ldots \mathbb{Z}_{t_N}.$$

Por simplicidade assumiremos que G é igual a esta soma direta.

Denotemos os elementos de G como N-uplas $g = (g_1, \ldots, g_N)$, onde podemos encarar os g_j ou como um inteiro módulo t_j ou como um inteiro no conjunto $\{0, 1, \ldots, t_j - 1\}$. Pensando na estrutura de G como sendo aditiva, e a estrutura de $\mathbb{C}^*$ multiplicativa, podemos denotar o elemento identidade de G por $e = (0, 0, \ldots, 0)$, e a identidade de $\mathbb{C}^*$ por 1. Assim se $\chi : G \to \mathbb{C}^*$ é um caráter de G e $\beta_1 = (1, 0, \ldots, 0)$, $\beta_2 = (0, 1, \ldots, 0), \ldots, \beta_N = (0, 0, \ldots, 1)$ são elementos de G. Então para qualquer elemento $g = (g_1, \ldots, g_N)$ de G nós temos

$$\chi(g) = \chi(\sum_{j=1}^{N} g_j \beta_j) = \prod_{j=1}^{N} \chi(g_j \beta_j) = \prod_{j=1}^{N} \chi(\beta_j)^{g_j}, \tag{2.17}$$

ou seja, χ é completamente determinado pelos valores em β_j. Como β_j tem ordem t_j, devemos ter

$$\chi(\beta_j) = \varepsilon_{t_j}^{h_j},$$

onde ε_{t_j} é t_j-ésima raíz primitiva da unidade, $\varepsilon_{t_j} = e^{\frac{2\pi i}{t_j}}$ e $h_j \in \{0, 1, \ldots, t_j - 1\}$. Assim qualquer caráter $\chi : G \to \mathbb{C}^*$ é determinado por uma N-upla $(h_1, h_2, \ldots, h_N)$, que pode ser vista como um elemento h de G. Logo podemos definir os caráteres de G pondo para cada $g \in G$ o caráter $\chi_g : G \to \mathbb{C}^*$ tal que

$$\chi_g(h) = \prod_{j=1}^{N} \varepsilon_{t_j}^{g_j h_j}, \ \forall\, h \in G. \tag{2.18}$$

Podemos verificar facilmente que $\chi_g : G \to \mathbb{C}^*$ definido por (2.18) é um homomorfismo. De fato,

$$\chi_g(h+h') = \prod_{i=1}^{N} \varepsilon_{t_i}^{g_i(h_i+h'_i)} = \prod_{i=1}^{N} \varepsilon_{t_i}^{g_i h_i + g_i h'_i} = \prod_{i=1}^{N} \varepsilon_{t_i}^{g_i h_i} \varepsilon_{t_i}^{g_i h'_i} = \prod_{i=1}^{N} \varepsilon_{t_i}^{g_i h_i} \prod_{i=1}^{N} \varepsilon_{t_i}^{g_i h'_i} = \chi_g(h)\chi_g(h').$$

Lema 2.2 *Para quaisquer* $g, h \in G$, $\chi_g(h) = \chi_h(g)$.

Prova. Trivial, pois G é Abeliano.

Terminamos este capítulo mostrando a tabela de caráteres de um grupo finito G de ordem N. A tabela pode ser organizada como segue. As colunas correspondem as classes de conjugação de G e as linhas correspondem aos caráteres χ_i das representações irredutíveis não equivalentes de G. A j-ésima classe de conjugação $\mathcal{C}_j$ é indicada mostrando um representante $c_j \in \mathcal{C}_j$. Na (i, j)-ésima entrada colocamos $\chi_i(c_j)$.

	c_1	c_2	$\ldots$	c_N
χ_1	$\chi_1(c_1)$	$\chi_1(c_2)$	$\ldots$	$\chi_1(c_N)$
χ_2	$\chi_2(c_1)$	$\chi_2(c_1)$	$\ldots$	$\chi_2(c_N)$
$\vdots$	$\vdots$	$\vdots$	$\ldots$	$\vdots$
χ_N	$\chi_N(c_1)$	$\chi_N(c_2)$	$\ldots$	$\chi_N(c_N)$

TABELA 2.1: Tabela de caráteres do grupo G.

Capítulo 3

Transformada de Fourier Quântica e o Problema do Subgrupo Escondido em Grupos Abelianos

Sejam $\mathbb{Z}_2^n$ a soma direta de $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \ldots \oplus \mathbb{Z}_2$ com n termos, onde $\mathbb{Z}_2 = \{0, 1\}$ é o grupo aditivo dos inteiros módulo 2 e $\mathcal{H}$ o espaço de Hilbert com base ortonormal $\{|x\rangle : x \in \mathbb{Z}_2^n\}$. Se $x = (x_1, \ldots, x_n)$ e $y = (y_1, \ldots, y_n) \in \mathbb{Z}_2^n$ então escrevemos

$$\begin{aligned} x \oplus y &= (x_1 \oplus y_1, \ldots, x_n \oplus y_n) \in \mathbb{Z}_2^n \\ x.y &= (x_1 y_1 \oplus \ldots \oplus x_n y_n) \in \mathbb{Z}_2, \end{aligned}$$

onde $\oplus : \mathbb{Z}_2^n \times \mathbb{Z}_2^n \to \mathbb{Z}_2^n$ também denota a adição em $\mathbb{Z}_2^n$.

Consideremos agora a porta de *Hadamard* de um q-bit como sendo uma matriz unitária 2×2 dada por

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

Pela aplicação direta do operador H nos estados $|0\rangle$ e $|1\rangle$ temos que

$$\begin{aligned} H|0\rangle &= \frac{|0\rangle + |1\rangle}{\sqrt{2}} \\ H|1\rangle &= \frac{|0\rangle - |1\rangle}{\sqrt{2}}. \end{aligned}$$

Se a entrada do computador quântico é $|0\rangle$, a porta de Hadamard cria uma superposição dos estados com a mesma amplitude. Esta é uma característica geral, válida para dois ou mais q-bits. Vamos analisar o caso com 2 q-bits. Devemos fazer o produto tensorial $H|0\rangle \otimes H|0\rangle$. Assim temos[1]

$$\begin{aligned} H^{\otimes 2}|0\rangle|0\rangle &= (H \otimes H)(|0\rangle \otimes |0\rangle) = H|0\rangle \otimes H|0\rangle \\ &= (\frac{|0\rangle + |1\rangle}{\sqrt{2}}) \otimes (\frac{|0\rangle + |1\rangle}{\sqrt{2}}) \\ &= \frac{1}{2}(|0\rangle|0\rangle + |0\rangle|1\rangle + |1\rangle|0\rangle + |1\rangle|1\rangle) \\ &= \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle) \\ &= \frac{1}{2}(|0\rangle + |1\rangle + |2\rangle + |3\rangle). \end{aligned} \tag{3.1}$$

O resultado é uma superposição de todos os estados com amplitudes iguais. De forma mais geral, o operador de Hadamard aplicado a n q-bits no estado $|0\rangle$ é

$$H^{\otimes n}|0\ldots 0\rangle = \frac{1}{\sqrt{2^n}} \sum_{y \in \mathbb{Z}_2^n} |y\rangle .$$

Assim o produto tensorial de n operadores de Hadamard produz uma superposição com amplitudes iguais para todos os estados da base computacional, quando a en-

[1]Usamos a base decimal para escrever os números dentro do $|\,\rangle$. Esta notação é um abuso de linguagem, porém bastante útil em computação quântica.

trada é o estado $|0\rangle$.

Para um elemento qualquer $x \in \mathbb{Z}_2^n$, o operador de Hadamard aplicado ao estado $|x\rangle$ é

$$H^{\otimes n} |x\rangle = \frac{1}{\sqrt{2^n}} \sum_{y \in \mathbb{Z}_2^n} (-1)^{x.y} |y\rangle .$$

3.1 Problema do Subgrupo Escondido

O problema do subgupo escondido (PSE) definido imediatamente abaixo, tem muitas aplicações úteis. Para grupos abelianos, uma solução eficiente para este problema implica em algoritmos eficientes para o cálculo de fatoração e logaritmo discreto. Já para grupos não abelianos, uma solução eficiente implicará num algoritmo polinomial para decidir se dois grafos são isomorfos ou não.

Definição 3.1 *: Dada uma função eficientemente computável $f : G \to X$, de um grupo finito G para um conjunto X, que é constante nas classes laterais (à esquerda) de algum subgrupo H de G e que toma valores distintos nas distintas classes laterais de G, o problema do subgrupo escondido é achar um conjunto gerador para H.*

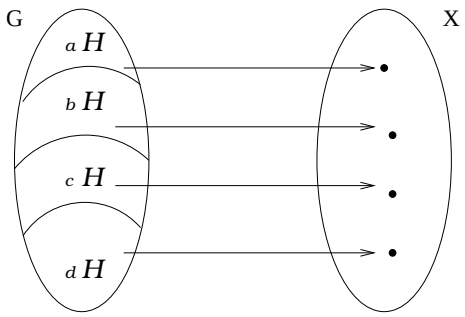

FIGURA 3.1: A função f é constante nas classes laterais de H e distinta em cada classe lateral.

3.2 O Problema de Simon

(SIMON, 1994) apresentou um algoritmo quântico em tempo polinomial para o seguinte problema.

Dada: Uma função $f : \mathbb{Z}_2^n \to \mathbb{Z}_2^n$ dois para um, ou seja, a cada par de valores distintos no domínio corresponde a uma única imagem no contradomínio e com periodicidade $\epsilon \in \mathbb{Z}_2^n$, i.e.,

$$f(x) = f(y) \Leftrightarrow y = x \oplus \epsilon, \ \forall \ x, y \in \mathbb{Z}_2^n.$$

Determine: ϵ eficientemente (isto é, com probabilidade maior que $\frac{1}{2}$ e com poucas chamadas ao oráculo[2]).

Vamos assumir que seja possível construir um operador linear unitário dependendo de f, U_f, tal que $U_f : |x\rangle |y\rangle \to |x\rangle |y \oplus f(x)\rangle$. U_f é chamado de *oráculo*. Este é o nosso primeiro exemplo de um problema de subgrupo escondido. A função f é definida no grupo $\mathbb{Z}_2^n$ e constante nas classes laterais de um subgrupo $H = \{0, \epsilon\}$ não conhecido. O objetivo é reconstruir este subgrupo. O algoritmo requer o uso de dois registradores, um com $n = \lceil \log_2 |\mathbb{Z}_2^n| \rceil$ q-bits e outro com $m \geq n$ q-bits. O algoritmo é o seguinte:

Passo 1. Inicialize o computador quântico no estado $|0^n\rangle |0^m\rangle$, e aplique $H^{\otimes n}$ no primeiro registrador para obter o estado

$$\frac{1}{\sqrt{2^n}} \sum_{x \in \mathbb{Z}_2^n} |x\rangle |0^m\rangle .$$

[2]Um oráculo é uma função que pode ser avaliada em qualquer número de pontos, porém a sua fórmula não é conhecida. Classicamente, o único jeito de revelar o oráculo é testar sequencialmente um grande número de pontos até que a fórmula fique evidente. Quanticamente, podemos fazer o uso do paralelismo quântico que permite a avaliação simultânea de um número exponencial de pontos com uma única consulta

Passo 2. Aplique U_f no estado final do passo 1 para obter

$$\frac{1}{\sqrt{2^n}} \sum_{x \in \mathbb{Z}_2^n} |x\rangle \, |f(x)\rangle \, .$$

Passo 3. Meça o segundo registrador e continue com o estado do primeiro registrador inalterado. Assim depois da medida o estado do primeiro registrador terá a forma:

$$\frac{1}{\sqrt{2}}(|x_0\rangle \oplus |x_0 + \epsilon\rangle) \, |y\rangle \tag{3.2}$$

onde $x_0 \in \mathbb{Z}_2^n$ foi escolhido equiprobabilisticamente (observe que depois da medida, a constante é renormalizada para $\frac{1}{\sqrt{2}}$ já que sobraram apenas dois termos na soma (3.2), i.e., os termos cuja imagem é um elemento randômico y do conjunto $Im(f)$). Podemos ainda escrever o estado do primeiro registrador na forma mais geral $\frac{1}{\sqrt{|H|}} \sum_{h \in H} |x_0 + h\rangle \, .$

Observação 3.1 *Note que agora temos um estado de superposição envolvendo* $|x_0\rangle$ *e* $|x_0 + \epsilon\rangle$. *Este estado contém a informação desejada* ϵ *junto com o número randômico* x_0. *Uma medida direta no primeiro registrador pode não trazer a informação desejada sobre* ϵ.

Passo 4. Aplique a transformação de Hadamard na superposição envolvendo o primeiro registrador do estado final do passo 3 para obter

$$\begin{aligned} H^{\otimes n} \frac{1}{\sqrt{2}}(|x_0\rangle + |x_0 \oplus \epsilon\rangle) \, |y\rangle &= \frac{1}{\sqrt{2}}(H^{\otimes n} \, |x_0\rangle + H^{\otimes n} \, |x_0 \oplus \epsilon\rangle) \, |y\rangle \\ &= \frac{1}{\sqrt{2^{n+1}}} \sum_{y \in \mathbb{Z}_2^n} ((-1)^{x_0 . y} + (-1)^{(x_0 \oplus \epsilon) . y}) \, |y\rangle \\ &= \frac{1}{\sqrt{2^{n-1}}} \sum_{y : y . \epsilon = 0} (-1)^{(x_0 . y)} \, |y\rangle \, , \text{ com } y, \epsilon \in \mathbb{Z}_2^n. \end{aligned}$$

Note que:

- Se $\epsilon.y = 1$ então

$$(-1)^{x_0.y} + (-1)^{(x_0 \oplus \epsilon).y} = (-1)^{x_0.y} + (-1)^{x_0.y \oplus \epsilon.y} = (-1)^{x_0.y} + (-1)^{x_0.y+1} = 0.$$

- Se $\epsilon.y = 0$ então

$$(-1)^{x_0.y} + (-1)^{(x_0 \oplus \epsilon)y} = (-1)^{x_0.y} + (-1)^{x_0.y} = 2(-1)^{x_0.y}.$$

Passo 5. Meça o primeiro registrador para achar um valor y_i tal que $\epsilon.y_i = 0$ (a probabilidade de se obter um y_i específico é $\frac{1}{2^{n-1}}$).

Passo 6. Repetir o processo acima para achar suficientes y_i´s tal que ϵ possa ser determinado resolvendo um sistema de equações lineares $y_1.\epsilon, \ldots, y_r.\epsilon = 0$. Veremos na seção (3.4) que a quantidade de y_i´s necessários para encontrar ϵ é no máximo $[\mathbb{Z}_2^n : H]$, onde $H = \{0, \epsilon\}$. O algoritmo de Simon consiste essencialmente de $O(n)$ repetições da sub-rotina descrita acima (SIMON, 1994). Já que o nosso valor procurado ϵ é uma cadeia de bits de tamanho n, serão necessários n y_i's para determinar ϵ resolvendo um sistema de equações lineares . O número de passos para resolver este sistema é $O(n^2)$. Portanto serão necessários $O(n + n^2) = O(n^2)$ repetições para determinar ϵ com probabilidade maior que $\frac{1}{2}$.

3.3 A Transformada de Fourier em Grupos Abelianos

Seja G um grupo abeliano finito e seja $\mathcal{H}$ o espaço de Hilbert com base ortonormal $\{|g\rangle : g \in G\}$ indexada pelos elementos de G. Suponhamos que temos um

computador quântico atuando em $\mathcal{H}$ (sabemos que quando o número de q-bits aumenta linearmente, a dimensão do espaço de Hilbert aumenta exponencialmente), logo para implementarmos isto fisicamente precisamos de $n = \lceil \log_2 |G| \rceil$ q-bits. O estado de um computador quântico com n q-bits é um vetor num espaço vetorial complexo de dimensão 2^n.

Agora vamos contruir uma matriz $|G| \times |G|$, cujas colunas são vetores $|v_g\rangle$ definidos como

$$|v_g\rangle = \frac{1}{\sqrt{|G|}} \begin{pmatrix} \chi_g(h_1) \\ \chi_g(h_2) \\ \vdots \\ \chi_g(h_{|G|}) \end{pmatrix}$$

onde $g \in G$, e $h_1, \ldots, h_{|G|}$ é uma lista completa dos elementos de G . Segue das relações de ortogonalidade (definidas no Capítulo 2) que esta matriz é unitária. Logo o operador definido por esta matriz que denotaremos por F_G é unitário. Dizemos então que F_G é a *transformada de Fourier* em grupos Abelianos. Podemos também definí-la por sua atuação nos vetores da base como:

$$F_G |g\rangle = \frac{1}{\sqrt{|G|}} \sum_{h \in G} \chi_g(h) |h\rangle . \tag{3.3}$$

Note que a saída de $F_G |g\rangle$ é o estado quântico correspondente ao vetor $|v_g\rangle$, que toma a forma acima quando escrito na notação usual para um estado. Já que o operador é unitário ele pode ser implementado em um computador quântico.

Exemplo 3.1 *Neste exemplo podemos verificar que a transformada de Fourier no grupo* $G = \underbrace{\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \ldots \oplus \mathbb{Z}_2}_{n \ vezes}$ *é a transformação de Hadamard* $H^{\otimes n}$ *utilizada no algoritmo de Simon.*

Vimos no início deste capítulo que este é o grupo cujos elementos são cadeias de bits de tamanho n e operação do grupo como sendo adição módulo 2 (essa operação é também conhecida como XOR na computação). Temos então que $t_1 = t_2 = \ldots = t_n = 2 \Rightarrow \varepsilon_{t_1} = \ldots = \varepsilon_{t_n} = -1$ (veja seção 2.6 do Capítulo 2). Os elementos $g, h \in G$ são n-uplas $g = (g_1, \ldots, g_n),\ h = (h_1, \ldots, h_n)$ com g_i, h_i tomando os valores 0 ou 1. Assim, temos que $\chi_g(h) = \prod_{i=1}^{n}(-1)^{g_i h_i}$. Substituindo isto na equação (3.3) acima, obtemos:

$$F_{\mathbb{Z}_2^n} |g\rangle = \frac{1}{\sqrt{2^n}} \sum_{h \in \mathbb{Z}_2^n} (\prod_{i=1}^{n} (-1)^{g_i h_i} |h\rangle = \frac{1}{\sqrt{2^n}} \sum_{h \in \mathbb{Z}_2^n} (-1)^{g.h} |h\rangle = H^{\otimes n} |g\rangle .$$

3.4 O Subgrupo Ortogonal

Para qualquer subgrupo H de um grupo finito G, podemos definir o subgrupo ortogonal $H^{\perp}$, como

$$H^{\perp} = \{g \in G \mid \chi_g(h) = 1 \,\forall\, h \in H\}.$$

Como G é finito, para mostrar que $H^{\perp}$ é um subgrupo de G, basta mostrarmos que a operação do grupo é fechada em $H^{\perp}$. De fato, se $a, b \in H^{\perp}$ então para qualquer $h \in H$ nós temos $\chi_h(ab) = \chi_h(a)\chi_h(b) = 1 \times 1 = 1$, isto é, $ab \in H^{\perp}$, logo $H^{\perp} \leq G$. No caso particular onde $G = \mathbb{Z}_2 \oplus \ldots \oplus \mathbb{Z}_2$, dizemos que $z \in H^{\perp}$ se $(-1)^{x.z} = 1$, i.e., $z.x = 0\ \forall\ x \in H$. Se olharmos para z, x como vetores num espaço n-dimensional sobre um corpo P qualquer com 2 elementos, então H é um subspaço e $H^{\perp}$ é o complemento de H. Esta é a motivação para a terminologia $H^{\perp}$. No entanto essa propriedade não é preservada no caso geral.

O teorema a seguir mostra uma importante relação entre H e $H^{\perp}$.

Teorema 3.1 *Temos $H^{\perp} \simeq G/H$, em particular $|H^{\perp}| = |G|/|H|$.*

Prova. Ver (LOMONT, 2004).

Voltando novamente ao caso particular $G = \mathbb{Z}_2 \oplus \ldots \oplus \mathbb{Z}_2$, e $H = \{0, \epsilon\}$, i.e., ao algoritmo de Simon, podemos enxergar o estado quântico depois do passo 3 como uma superposição sobre uma classe lateral de H. Então aplicamos F_G, e de fato esta produz uma superposição sobre todos os z's com $z.\epsilon = 0$, isto é, z's em $H^{\perp}$. Agora mostraremos que para um grupo Abeliano genérico (finito) G, F_G produz uma superposição sobre os elementos em $H^{\perp}$, qualquer que seja $H \leq G$.

Lema 3.1 *Para qualquer classe lateral H_i de H em G, temos*

$$F_G(\frac{1}{\sqrt{|H|}} \sum_{g \in H_i} |g\rangle) = \frac{1}{\sqrt{|H^{\perp}|}} \sum_{h \in H^{\perp}} \chi_h(g_i) \, |h\rangle$$

onde g_i é um elemento fixo representante da classe lateral H_i.

Prova. Aplicando a definição de F_G e invertendo a ordem da soma, obtemos

$$F_G(\frac{1}{\sqrt{|H|}} \sum_{g \in H_i} |g\rangle) = \frac{1}{\sqrt{|G||H|}} \sum_{h \in G} \sum_{g \in H_i} \chi_g(h) \, |h\rangle \, .$$

Seja g_i um representante para a classe lateral H_i, de modo que $g \in H_i$ pode ser escrito como $g = g_i\tau$ para algum $\tau \in H$. Para a soma interna acima, nós temos

$$\begin{aligned} \sum_{g \in H_i} \chi_g(h) &= \sum_{g \in H_i} \chi_h(g) \\ &= \sum_{\tau \in H} \chi_h(g_i\tau) \\ &= \chi_h(g_i) \sum_{\tau \in H} \chi_h(\tau). \end{aligned}$$

Se $h \in H^{\perp}$, então $\chi_h(\tau) = 1, \forall\, \tau \in H$. Então a soma interna resulta $\chi_h(g_i)|H|$. Assim

$$\begin{aligned} \frac{1}{\sqrt{|G||H|}} \sum_{h\in G} \sum_{g\in H_i} \chi_g(h)\,|h\rangle &= \frac{|H|}{\sqrt{|G||H|}} \sum_{h\in H^{\perp}} \chi_h(g_i)\,|h\rangle \\ &= \sum_{h\in H^{\perp}} \frac{\sqrt{|H|}}{\sqrt{|G|}} \chi_h(g_i)\,|h\rangle\,, \end{aligned} \tag{3.4}$$

o que nos dá a amplitude de $|h\rangle$ após aplicar F_G como sendo $\frac{\sqrt{|H|}}{\sqrt{|G|}}\chi_h(g_i)\,|h\rangle$. Portanto, cada h possui a probabilidade de medida $|\frac{\sqrt{|H|}}{\sqrt{|G|}}\chi_h(g_i)|^2 = \frac{|H|}{|G|}$. Pelo teorema (3.1) temos que $\frac{|H|}{|G|} = \frac{1}{|H^{\perp}|}$, e como existem $|H^{\perp}|$ elementos em $H^{\perp}$, qualquer outro elemento em G deve ter amplitude 0. Isso prova o lema (3.1).

■

Agora apresentaremos um algoritmo eficiente para o PSE, i.e., um algoritmo que rode em tempo polinomial em $\log_2 |G|$. Antes mostraremos que um algoritmo eficiente para o PSE implica num algoritmo eficiente para o problema de Simon.

De fato, seja $f : \mathbb{Z}_2^n \to \mathbb{Z}_2^n$ uma função 2 para 1 com periodicidade ϵ como no problema de Simon. Note que f é constante nas classes laterais do subgrupo $\{0, \epsilon\}$ de $\mathbb{Z}_2^n$ e distinta em cada classe lateral. O problema de Simon é achar ϵ, que é o único gerador de $\{0, \epsilon\}$. O problema de Simon, então, é justamente um PSE com $G = \mathbb{Z}_2^n$, $X = \mathbb{Z}_2^n$ e f como dada acima. Então, uma solução eficiente para o PSE produzirá f em tempo menor que $O(\log 2^n) = O(n)$ passos. Agora voltemos ao algoritmo para o PSE.

Como no algoritmo de Simon, assumiremos que temos dois registradores: um registrador com $n = \lceil \log_2 |G| \rceil$ q-bits e o segundo registrador com m q-bits, onde m

é um inteiro positivo maior ou igual que n. O algoritmo usa a seguinte sub-rotina:

Passo 1. Inicialize o computador quântico no estado $|0_G\rangle\,|0^m\rangle$, onde $|0_G\rangle$ é o estado base correspondente ao elemento neutro de G. Depois aplique F_G no primeiro registrador para obter

$$\frac{1}{\sqrt{|G|}}\sum_{g\in G}|g\rangle\,|0^m\rangle\,.$$

Passo 2. Aplique U_f no estado final do passo anterior e obtenha

$$\frac{1}{\sqrt{|G|}}\sum_{g\in G}|g\rangle\,|f(g)\rangle\,.$$

Este é um estado quântico notável. Como U_f é linear, ele atua em todos os $|g\rangle\,|0^m\rangle$ para $|G|$ valores de g, então isto gera todos os $f(g)$ simultaneamente. Este fenômeno é o que chamamos de *paralelismo quântico*.

Passo 3. Meça o segundo registrador do estado final do passo 2. A medida, segundo um postulado da mecânica quântica, provoca um distúrbio no estado original. Este estado por sua vez é levado no estado

$$\frac{1}{\sqrt{|H|}}\sum_{g_0\in H_i}|g_0\rangle\,|f(g_0)\rangle$$

onde H_i é alguma classe lateral de H. Note que a constante foi renormalizada para $\frac{1}{\sqrt{|H|}}$ já que após a medida sobraram apenas $|H|$ elementos na soma. Estes elementos são aqueles cuja imagem é $f(g_0)$.

Passo 4. Aplique F_G no primeiro registrador e obtenha então uma superposição

sobre $H^{\perp}$. Pelo lema (3.1) teremos

$$\frac{1}{\sqrt{|H^{\perp}|}} \sum_{h \in H^{\perp}} \chi_h(g_i) \, |h\rangle \, .$$

Passo 5. Meça agora o primeiro registrador. A medida produz um elemento randômico em $H^{\perp}$.

Passo 6. Segue do teorema (2.1) que se repetirmos esta sub-rotina quântica um número de vezes logaritmico em $|G|$ (e portanto polinomial em n) obtemos um conjunto de geradores para $H^{\perp}$. Mostraremos agora que apartir desse conjunto gerador podemos calcular um elemento randômico em H em tempo polinomial (i.e., polinomial no tamanho da entrada). Em particular, podemos calcular um conjunto de elementos geradores em H em tempo polinomial (DAMGARD, 2004).

De fato, no caso geral onde $G = \mathbb{Z}_{t_1} \oplus \ldots \oplus \mathbb{Z}_{t_N}$, seja θ o menor múltiplo comum de todos os t_i's. Note que qualquer raíz da unidade ε_{t_i} pode ser escrita como uma potência de ε_{θ}. Realmente, $\varepsilon_{t_i} = e^{\frac{2\pi i}{t_i}} = \varepsilon_{\theta}^{\frac{\theta}{t_i}}$. Então temos que para quaisquer elementos $g = (g_1, \ldots, g_N)$, $h = (h_1, \ldots, h_N)$ e usando a fórmula (2.18) do Capítulo 2, temos o caráter $\chi_g(h) = \varepsilon_{\theta}^{\alpha_1^g h_1 + \ldots + \alpha_n^g h_N}$, onde os coeficientes α_i^g são tais que $\alpha_i^g = \theta \frac{g_i}{t_i}$. Portanto, assumamos que $\{g^{(1)}, \ldots, g^{(d)}\}$ seja um conjunto de geradores para $H^{\perp}$, assim sabemos que h está em H se, e somente se, forem satisfeitas as seguintes equações lineares

$$\alpha_1^{g^{(i)}} h_1 + \ldots + \alpha_n^{g^{(i)}} h_n = 0 \bmod \theta$$

para $i = 1, \ldots, d$. Assim um elemento randômico em H pode ser obtido selecionando uma solução qualquer deste sistema de equações lineares. Sabemos que isto pode ser

feito eficientemente desde que a solução exista. Usando novamente o teorema (2.1), vemos que se selecionarmos $\log_2 |G|$ soluções deste sistema de equações acharemos um conjunto gerador para H com probabilidade próxima de 1 (LOMONT, 2004).

Na última seção deste capítulo, mostraremos que o algoritmo de Shor para fatoração é um caso particular do PSE. Veja também em (AHN, 2002) que o problema do logaritmo discreto também resume-se ao PSE.

3.5 O Algoritmo de Shor

Queremos achar um fator de um número composto N. Classicamente só são conhecidos algoritmos ineficientes. Quanticamente, Peter Shor desenvolveu um algoritmo eficiente com características bastantes interessantes (SHOR, 1997).

Nesta seção mostraremos que o algoritmo de Shor é um caso particular do PSE, i.e., o problema de fatoração é um PSE. Para fazermos isto, basta mostrarmos que uma solução eficiente do PSE implica num algoritmo eficiente para achar a ordem de elementos em $\mathbb{Z}_N^*$ (onde $\mathbb{Z}_N^*$ é o grupo dos inteiros não nulos coprimos com N, com respeito a multiplicação de classes de $\mathbb{Z}_N$).

Definição 3.2 *Seja n um número natural e y coprimo com n. A ordem de y é o menor inteiro positivo r tal que $y^r = 1 \ mod \ n$.*

Seja $f : \mathbb{Z} \to \mathbb{Z}_n$ uma função definida por $f(x) = y^x \bmod n \ \ \forall \ \ x \in \mathbb{Z}$. Note que $\mathbb{Z}$ é finitamente gerado. Note também que f é constante em cada classe lateral do subgrupo $H = \{\ldots, -2r, -r, 0, r, 2r, \ldots\}$ de $\mathbb{Z}$ e distinta em cada classe lateral (aqui r é o menor inteiro positivo tal que $y^r = 1 \bmod n$). O problema de achar a ordem é achar r. Isto é equivalente a achar $-r$. Como r e $-r$ são os únicos geradores

de H em $\mathbb{Z}$, vemos que achar a ordem é justamente um PSE com $G = \mathbb{Z}$, $X = \mathbb{Z}_n$ e f como definida acima. Portanto, uma solução eficiente para o PSE produzirá uma solução eficiente para o problema de achar ordem, i.e., um algoritmo que rode em tempo polinomial em $\log_2 n$ passos (onde n é um limite superior do número de classes laterais de H em $\mathbb{Z}$, já que existem r classes laterais e temos sempre $r < n$).

Podemos conferir em (SHOR, 1997) que o problema de achar a ordem se reduz ao problema de fatoração e vice-versa, assim vemos facilmente que uma solução eficiente para o problema de achar a ordem implica num algoritmo eficiente para fatoração.

Capítulo 4

Representações Irredutíveis do Grupo Diedral

O grupo Simétrico pode ser definido como se segue.

Considere um conjunto não vazio S e seja $G = \{f : S \to S \mid f \text{ bijetiva}\}$. Se $\circ$ é a operação composição de funções, então $\{G, \circ\}$ é claramente um grupo tendo $I_s : S \to S$ definido por $I_s(x) = x,\ \forall\ x \in S$ como identidade. Se $S = \{1, 2, \ldots, N\}$ denotaremos esse grupo por S_N, e temos que o número de elementos de S_N é $N!$.

Agora veremos um subgrupo de S_N, não abeliano, contendo exatamente $2N$ elementos. Este subgrupo é formado pelas rotações e reflexões do plano que preservam um polígono regular com N vértices. Chamaremos este subgrupo de *grupo Diedral* ou *grupo de simetrias do polígono regular de N vértices* e o denotaremos por D_N. O conjunto formado pelas rotações formam um subgrupo abeliano de D_N que denotaremos por C_N.

Se denotarmos por r as rotações do ângulo $\frac{2\pi}{N}$ e por s qualquer uma das reflexões,

então temos

$$r^N = e,\ s^2 = e,\ srs = r^{-1}.$$

Note que cada elemento de D_N pode ser escrito unicamente, ou na forma r^k, com $0 \leq k \leq N-1$ (se o elemento pertence a C_N), ou na forma sr^k, com $0 \leq k \leq N-1$ (se o elemento não pertence a C_N). Temos ainda que a relação $srs = r^{-1}$ implica que $sr^k s = r^{-k}$. De fato, usando indução sobre k temos que para $k = 1$, $srs = r^{-1}$. Supondo que $sr^k s = r^{-k}$, vamos mostrar que $sr^{k+1}s = r^{-(k+1)}$. Com efeito,

$$sr^{k+1}s = sr^k rs = r^{-k}srs = r^{-k}r^{-1} = r^{-(k+1)}.$$

4.1 Representações Uni-Dimensionais do Grupo D_N

Nesta seção daremos todas as representações uni-dimensionais de D_N, e veremos que a quantidade de representações uni-dimensionais varia conforme N seja par ou ímpar. As duas representações uni-dimensionais de D_N que daremos a seguir são válidas tanto para N par como N ímpar.

1. Representação Trivial

$$\begin{array}{rccc} \rho^{(1)}: & D_N & \longrightarrow & GL(\mathbb{C}) \\ & g & \longmapsto & \rho_g^{(1)} = 1. \end{array}$$

2. Podemos definir uma segunda representação para D_N da seguinte forma

$$\rho^{(2)}: \quad D_N \longrightarrow GL(\mathbb{C})$$

$$g \longmapsto \rho_g^{(2)} = \begin{cases} 1 & \text{se} \quad g \in C_N \\ -1 & \text{se} \quad g \notin C_N. \end{cases}$$

Note que C_N é um subgrupo normal de D_N ($C_N \trianglelefteq D_n$), e sabemos da teoria de grupos que podemos olhar para C_N como sendo o núcleo de um homomorfismo com domínio D_N. Logo esta aplicação é um homomorfismo que define o grupo quociente D_N/C_N isomorfo a S_2.

3. A proposição a seguir é a peça chave para acharmos outra representação unidimensional para D_N, se considerarmos N como sendo par.

Proposição 4.1 *Seja D_N o grupo Diedral de ordem $2N$ e seja $C_N \trianglelefteq D_N$. Se N for par, então considere os subconjuntos de D_N,*

$$C_{\frac{N}{2}} \simeq \{r^{2i}\} \text{ e } sC_{\frac{N}{2}} = \{sr^{2i}\},$$

com $s \in \{D_N - C_N\}$ e $i = 0, \ldots, \frac{N}{2} - 1$. Seja $T_N = C_{\frac{N}{2}} \cup sC_{\frac{N}{2}}$. Então T_N é um subgrupo próprio normal de D_N.

Prova. Primeiro mostraremos que $T_N \leq D_N$. Para isso devemos mostrar que se $\alpha, \beta \in T_N$ então $\alpha\beta \in T_N$. De fato, sejam $\alpha = s^k r^{2i}$, $\beta = s^l r^{2j}$ com k, l tomados módulo 2 e $i, j = 0, \ldots, \frac{N}{2} - 1$. Então

$$\begin{aligned} \alpha\beta &= s^k r^{2i} s^l r^{2j} = s^{k-l}(s^l r^{2i} s^l) r^{2j} \\ &= s^{k-l} r^{(-1)^l 2i} r^{2j} = s^{k-l} r^{2(j+(-1)^l i)} \in T_N, \end{aligned} \tag{4.1}$$

onde $k-l$ são inteiros tais que $0 \leq k-l \leq 1$. Por construção temos que T_N é um subgrupo próprio de D_N. O fato de que $T_N \trianglelefteq D_N$ é trivial, pois, $|D_N| = |T_N| + |tT_N| = 2|T_N|,\ \forall\, t \in \{D_N - T_N\}$.

■

Então acabamos de mostrar que T_N é o núcleo de um homomorfismo com domínio D_N. Logo podemos definir uma terceira representação de grau 1 para D_N como sendo

$$\begin{array}{rccl} \rho^{(3)}: & D_N & \longrightarrow & GL(\mathbb{C}) \\ & g & \longmapsto & \rho_g^{(3)} = \begin{cases} 1 & \text{se} \quad g \in T_N \\ -1 & \text{se} \quad g \notin T_N. \end{cases} \end{array}$$

Note que este homomorfismo define o grupo quociente D_N/T_N isomorfo a S_2.

4. A forma como acharemos a quarta representação uni-dimensional para D_N é análoga ao do ítem 3. Aqui também consideraremos N sendo par.

Proposição 4.2 *Dados o grupo D_N, com N um inteiro positivo par, $C_N \trianglelefteq D_N$ e os subconjuntos de D_N,*

$$C_{\frac{N}{2}} \simeq \{r^{2i}\}\ e\ srC_{\frac{N}{2}} = \{sr^{2i+1}\},$$

com $sr \in \{D_N - C_N\}$ e $i = 0, \ldots, \frac{N}{2} - 1$. Seja $V_N = C_{\frac{N}{2}} \cup srC_{\frac{N}{2}}$. Então V_N é um subgrupo próprio normal de D_N.

Prova. Com efeito, os elementos de V_N são da forma r^{2i} ou sr^{2j+1} com $i, i = 0, \ldots, \frac{N}{2} - 1$. Assim, se $\alpha, \beta \in V_N$ então

- $\alpha = r^{2i},\ \beta = r^{2j} \ \Rightarrow\ \alpha\beta = r^{2(i+j)} \in V_N.$
- $\alpha = r^{2i},\ \beta = r^{2j+1} \ \Rightarrow\ \alpha\beta = r^{2i}sr^{2j+1} = sr^{-2i}r^{2j}r = sr^{2(j-i)+1} \in V_N.$
- $\alpha = sr^{2i+1},\ \beta = r^{2j} \ \Rightarrow\ \alpha\beta = sr^{2(i+j)+1} \in V_N.$
- $\alpha = sr^{2i+1},\ \beta = r^{2j+1} \ \Rightarrow\ \alpha\beta = sr^{2i+1}sr^{2j+1} = r^{2(j-i)} \in V_N.$

Portanto, $V_N \leq D_N$ e pelo mesmo argumento do caso anterior, temos que V_N é um subgrupo próprio normal de D_N.

■

Assim, obtemos uma quarta representação uni-dimensional para D_N dada por

$$\begin{array}{rccl} \rho^{(4)}: & D_N & \longrightarrow & GL(\mathbb{C}) \\ & g & \longmapsto & \rho_g^{(4)} = \begin{cases} 1 & \text{se} \quad g \in V_N \\ -1 & \text{se} \quad g \notin V_N. \end{cases} \end{array}$$

Claramente este homomorfismo define o grupo quociente D_N/V_N que também é isomorfo a S_2.

4.2 Representações Induzidas

Seja $\rho : G \to GL(V)$ uma representação de G, e seja ρ_H ($H \leqslant G$) a restrição para H (isto é, $\rho : H \to GL(V)$). Seja W uma subrepresentação de ρ_H, i.e., um subspaço de V invariante por ρ_t, $t \in H$. Denotemos por $\rho^W : H \to GL(W)$ a restrição de H em W. Seja s um elemento qualquer em G, assim o espaço vetorial $\rho_s W$ depende somente da classe lateral (à esquerda) sH de G. De fato, se substituírmos s por st, com $t \in H$, teremos que $\rho_{st}W = \rho_s\rho_t W = \rho_s W$, pois $\rho_t W = W$. Assim, se σ é uma

classe lateral (à esquerda) de H, podemos definir um subspaço W_σ de V como sendo $\rho_s W \quad \forall\, s \in \sigma$. Agora, tome $s' \in G = \cup_{i=1}^{k} \sigma_i$ tal que $s' \notin \sigma_j$, para algum $1 \leq j \leq k$, onde k é o número de classes laterais de H em G. Então temos

$$\rho_{s'} W_{\sigma_j} = \rho_{s'} \rho_s W = \rho_{s's} W = W_{\sigma_i},$$

$\forall\, s \in \sigma_j$ e $1 \leq i \leq k$. Em outras palavras, os subspaços W_σ são permutados entre si, por ρ_s. Portanto, o subspaço formado pela soma $\sum_{\sigma \in G/H} W_\sigma$ é invariante por ρ_g, com $g \in G$. Logo a soma $\sum_{\sigma \in G/H} W_\sigma$ é uma subrepresentação de V.

Definição 4.1 *Dizemos que a representação ρ de G em V é induzida pela representação ρ^W de H em W se $V = \oplus_{\sigma \in G/H} W_\sigma$.*

Exemplo 4.1 *Mostre que a representação permutação $\rho : S_3 \to GL(V)$ é induzida pela representação permutação $\rho^W : S_2 \to GL(W)$.*

Para fins de visualização façamos $V = \mathbb{R}^3$. Na notação cíclica[1] temos $S_3 = \{(), (12), (13), (23), (123), (132)\}$ e $S_2 = \{(), (12)\}$. Seja $\{e_1, e_2, e_3\}$ uma base para $\mathbb{R}^3$ e $\sigma_1 = S_2,\ \sigma_2 = (23)S_2,\ \sigma_3 = (13)S_2$ as classes laterais de S_2 em S_3. Note que o subspaço $W = Ke_3$, com K constante arbitrária é invariante por $\rho_g^W,\ g \in S_2$. De fato, $\rho_{()}^W e_3 = e_{()3} = e_3,\ \rho_{(12)}^W e_3 = e_{(12)3} = e_3$. Logo,

- $W_{\sigma_1} = \rho_{(12)} W = K\rho_{(12)} e_3 = Ke_3,$
- $W_{\sigma_2} = \rho_{(23)} W = K\rho_{(23)} e_3 = Ke_2,$
- $W_{\sigma_3} = \rho_{(13)} W = K\rho_{(13)} e_3 = Ke_1.$

[1]Maiores detalhes sobre a notação cíclica para permutação veja (GARCIA & LEAQUAIN, 1998).

Portanto, $W_{\sigma_1} \oplus W_{\sigma_2} \oplus W_{\sigma_3} = \mathbb{R}^3$, ou seja, a representação permutação ρ de S_3 em V é induzida pela representação permutação ρ^W de S_2 em W.

4.3 Representações Bi-Dimensionais para D_N Induzidas por C_N

Nesta seção construiremos representações para D_N de grau 2.

Sabemos que o grupo C_N de ordem N consiste das potências $r^1, r^2, \ldots, r^N$ de um elemento r de ordem N, $r^N = e$. Como C_N é abeliano, as representações irredutíveis são de grau 1. De acordo com a seção (2.6) do Capítulo 2, os caráteres de C_N são raízes N-ésimas da unidade, dadas por

$$\chi_h(r^k) = e^{\frac{2\pi i h k}{N}}, \text{ com } h = 0, 1, \ldots, N-1.$$

Fazendo $\varepsilon = e^{\frac{2\pi i}{N}}$, podemos organizar os caráteres de C_N na tabela (4.1).

	e	r	r^2	$\ldots$	r^{N-1}
χ_0	1	1	1	$\ldots$	1
χ_1	1	ε	ε^2	$\ldots$	ε^{N-1}
χ_2	1	ε^2	ε^4	$\ldots$	$\varepsilon^{2(N-1)}$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ldots$	$\vdots$
χ_{N-1}	1	ε^{N-1}	$\varepsilon^{2(N-1)}$	$\ldots$	$\varepsilon^{(N-1)(N-1)}$

Tabela 4.1: Tabela de caráteres do grupo C_N.

Seja $\rho : D_N \to GL(V)$ uma representação bi-dimensional para D_N. Vamos mostrar que ρ é induzida pela representação $\theta : C_N \to GL(W)$, onde W é um subspaço de V. De fato, como a representação W de C_N é uni-dimensional, temos que W é gerado por um único vetor w. Tome $w = (1, 0)$ e considere a seguinte base

para V dada pelos vetores $w = (1, 0)$ e $v = (0, 1)$. Tomamos esses valores particulares para obtermos adiante uma representação matricial explicita para $GL(V)$.

Agora nós calculamos a ação $\theta_g,\ g \in C_N$ em W. Pela tabela (4.1), vemos que existem N representações de C_N dadas por $\theta_g^{(h)} = \chi_h(g)$, com $0 \leq h \leq N-1$. Assim

$$\theta_{r^k}^{(h)} w = e^{\frac{2\pi i k h}{N}} w, \ \ 0 \leq k, h \leq N-1.$$

Como C_N possui a metade dos elementos de D_N, as classes laterais são duas, a saber

$$\sigma_1 = \{e, r, r^2, \ldots, r^{N-1}\}, \sigma_2 = \{s, sr, sr^2, \ldots, sr^{N-1}\}.$$

Sabemos que

$$W_{\sigma_1} = \theta_{r^k}^{(h)} w = e^{\frac{2\pi i k h}{N}} w, \ \ \text{com } 0 \leq k, h \leq N-1.$$

Por outro lado,

$$W_{\sigma_2} = \rho_{sr^k}^{(h)} w = \rho_s^{(h)} \rho_{r^k}^{(h)} w = e^{\frac{2\pi i k h}{N}} \rho_s^{(h)} w.$$

Note que $\rho_s^{(h)} w = v$. Com efeito, W é invariante somente por $\rho_g,\ \forall\ g \in \sigma_1$, mas neste caso $g = s \in \sigma_2$, logo a igualdade segue. Portanto, $W_{\sigma_2} = e^{\frac{2\pi i k h}{N}} v$, e consequentemente

$$V = W_{\sigma_1} \oplus W_{\sigma_2}.$$

O nosso objetivo agora é obter representações matriciais para ρ. Podemos fazer isso atuando o grupo D_N nos elementos da base de V. Como já fizemos D_N atuar em w, então basta fazermos D_N atuar em v. Desta forma temos

- $\rho_{r^k}^{(h)} v = \rho_{r^k}^{(h)} \rho_s^{(h)} w = \rho_{r^k s}^{(h)} w = \rho_{sr^{-k}}^{(h)} w = \rho_s^{(h)} \rho_{r^{-k}}^{(h)} w = \varepsilon^{-kh} \rho_s^{(h)} w = \varepsilon^{-kh} v.$

- $\rho^{(h)}_{sr^k} v = \rho^{(h)}_{sr^k}\rho^{(h)}_{s} w = \rho^{(h)}_{sr^k s} w = \rho^{(h)}_{r^{-k}} w = \varepsilon^{-kh} w.$

Assim, as matrizes do operador $\rho^{(h)}_g$, com $g \in D_N$ na base $\{w, v\}$ de V são dadas por

$$\rho^{(h)}_{r^k} = \begin{pmatrix} \varepsilon^{hk} & 0 \\ 0 & \varepsilon^{-hk} \end{pmatrix}, \qquad \rho^{(h)}_{sr^k} = \begin{pmatrix} 0 & \varepsilon^{-hk} \\ \varepsilon^{hk} & 0 \end{pmatrix}.$$

Estas matrizes definem uma representação $\rho^{(h)}$ de D_N. De fato, para elementos $\alpha = r^m$ e $\beta = sr^p$ de D_N, com $m, p = 0, \ldots, N-1$, temos

$$\begin{aligned} \rho^{(h)}_{\alpha\beta} &= \rho^{(h)}_{r^m sr^p} = \rho^{(h)}_{sr^{p-m}} = \begin{pmatrix} 0 & \varepsilon^{-h(p-m)} \\ \varepsilon^{h(p-m)} & 0 \end{pmatrix} = \begin{pmatrix} \varepsilon^{hm} & 0 \\ 0 & \varepsilon^{-hm} \end{pmatrix}\begin{pmatrix} 0 & \varepsilon^{-hp} \\ \varepsilon^{hp} & 0 \end{pmatrix} \\ &= \rho^{(h)}_{r^m}\rho^{(h)}_{sr^p} = \rho^{(h)}_{\alpha}\rho^{(h)}_{\beta}. \end{aligned}$$

Um cálculo análogo, mostra que $\rho^{(h)}_{\alpha\beta} = \rho^{(h)}_{\alpha}\rho^{(h)}\beta$ para todo $\alpha, \beta \in D_N$.

O próximo passo é mostrar que as representações de graus 1 e 2 definidas para D_N são as únicas representações irredutíveis de D_N a menos de isomorfismos. Recordemos que $g \overset{D_N}{\sim} h$ se os elementos de g, h de D_N estão na mesma classe de conjugação.

Proposição 4.3 *Se D_N é o grupo Diedral de ordem $2N$, $N \geq 2$ um inteiro, então para $i, j = 0, \ldots, N-1$ nós temos:*

(i) $r^i \overset{D_N}{\sim} r^{N-i}$,

(ii) $s \overset{D_N}{\sim} sr^{2i}$,

(iii) $sr \overset{D_N}{\sim} sr^{2i+1}$,

(iv) $r^i \overset{D_N}{\nsim} sr^j$.

Prova. Para provarmos (i), (ii) e (iii) basta tomarmos $g = r^i \in D_N$. Assim para

(i) temos $r^i = gr^{N-i}g^{-1}$. Para (ii), temos $g(sr^{2i})g^{-1} = r^i(sr^{2i})r^{-i} = r^isr^i = s$. Para (iii), $g(sr^{2i+1})g^{-1} = r^i(sr^{2i+1})r^{-i} = r^isr^{i+1} = sr$.

(iv) Suponha que existam inteiros $0 \leq m \leq 1$, e $p = 0, \ldots, N-1$ tais que $r^i = s^m r^p (sr^j) r^{-p} s^m$. Assim,

$$s^m r^p sr^j r^{-p} s^m = ss^m r^{-p} r^j r^{-p} s^m = ss^m r^{j-2p} s^m = \begin{cases} sr^{j-2p} & \text{se} \quad m = 0 \\ sr^{2p-j} & \text{se} \quad m = 1 \end{cases} . \quad (4.2)$$

Logo, é um absurdo termos $r^i = sr^{j-2p}$ ou $r^i = sr^{2p-j}$. Portanto, r^i não é conjugado com sr^j.

■

Desta proposição temos o seguinte corolário.

Corolário 4.0.1 *O grupo D_N, para um dado inteiro $N \geq 2$, possui $\frac{N}{2} + 3$ classes de conjugação se N for par, e $\frac{N+3}{2}$ se N for ímpar.*

Prova. De fato, para N par, segue da proposição (4.3) que as classes de conjugação de D_N são:

$$\{e\}, \{r, r^{N-1}\}, \ldots, \{r^{\frac{N}{2}-1}, r^{\frac{N}{2}+1}\}, \{r^{\frac{N}{2}}\}, \{sr^{2i},\ i = 0, \ldots, \frac{N}{2}-1\}, \{sr^{2i+1},\ i = 0, \ldots, \frac{N}{2}-1\}.$$

E para N ímpar, temos

$$\{e\}, \{r, r^{N-1}\}, \ldots, \{r^{\frac{N-1}{2}}, r^{\frac{N+1}{2}}\}, \{sr^j,\ j = 0, \ldots, N-1\}.$$

■

Voltando a representação $\rho^{(h)}$ de D_N, note que $\rho^{(h)}$ depende somente da classe de resíduos de N módulo h. Considerando ainda N par, podemos assumir $0 \leq h \leq \frac{N}{2}$, já que $\rho^{(h)} \simeq \rho^{(N-h)}$. Os casos extremos $h = 0$ e $h = \frac{N}{2}$ são descartados, pois as representações correspondentes são redutíveis, com caráteres $\Psi_1 + \Psi_2$ e $\Psi_3 + \Psi_4$, respectivamente[2]. Por outro lado, para todo h satisfazendo $0 < h < \frac{N}{2}$, a representação $\rho^{(h)}$ é irredutível. De fato, como $\varepsilon^h \neq \varepsilon^{-h}$, os únicos subspaços invariantes por $\rho_r^{(h)}$ são os subspaços da forma $\begin{pmatrix} x \\ 0 \end{pmatrix}$ ou $\begin{pmatrix} 0 \\ x \end{pmatrix}$ $\forall\, x \in \mathbb{C}$, mas estes subspaços não são invariantes por $\rho_s^{(h)}$. Logo as representações $\rho^{(h)}$ são irredutíveis. Os caráteres das representações irredutíveis de D_N são dados por

$$\chi_h(r^k) = \varepsilon^{hk} + \varepsilon^{-hk} = 2\cos\frac{2\pi hk}{N}, \quad \chi_h(sr^k) = 0.$$

Corolário 4.0.2 *As representações $\rho^{(h)}$, com $0 < h < \frac{N}{2}$ são duas a duas não isomorfas.*

Prova. Suponhamos por absurdo, que $\rho^{(h)} \simeq \rho^{(p)}$, com $h \neq p$ e tal que $h + p < N$, logo estas representações possuem o mesmo caráter, i.e.,

$$\chi_h(r^k) = \chi_p(r^k) \Rightarrow \cos(\frac{2\pi hk}{N}) = \cos(\frac{2\pi pk}{N}) \Rightarrow h = p \text{ ou } h = N - p,$$

mas isto é um absurdo, portanto $\chi_h(r^k) \neq \chi_p(r^k)$ e as representações $\rho^{(h)}$ e $\rho^{(p)}$ são não isomorfas.

■

Agora nós mostraremos que as representações irredutíveis que definimos neste capítulo são as únicas representações irredutíveis (a menos de isomorfismos) de D_N.

[2]Veja tabela 4.2.

De fato, segue do corolário (4.0.1) que para N par, D_N possui $\frac{N}{2}+3$ classes de conjugação (ou representações irredutíveis). Se D_N possui quatro representações uni-dimensionais[3], então a soma dos quadrados dos seus graus deve ser igual a $2N$ (teorema 2.8). De fato, $4\times 1^2+(\frac{N}{2}-1)\times 2^2=2N$, que é a ordem de D_N. Isto mostra que para N par, D_N possui 4 representações de grau 1 e $\frac{N}{2}-1$ representações de grau 2.

Podemos visualizar os caráteres de D_N na tabela abaixo.

	r^k	sr^k
Ψ_1	1	1
Ψ_2	1	-1
Ψ_3	$(-1)^k$	$(-1)^k$
Ψ_4	$(-1)^k$	$(-1)^{k+1}$
Ψ_5^h	$2\cos(\frac{2\pi hk}{N})$	0

TABELA 4.2: Tabela de caráteres do grupo D_N para N par, $0\leq k<N$, $0<h<\frac{N}{2}$.

Agora, analisaremos as representações irredutíveis de D_N para N ímpar.

Segue do corolário (4.0.1) que para N ímpar, D_N possui $\frac{N+3}{2}$ representações irredutíveis, assim existem apenas duas representações de grau 1, a saber Ψ_1 e Ψ_2 dada pela tabela (4.3), e $\frac{N-1}{2}$ representações de grau 2 dadas como no caso de N par. Estas representações são as únicas representações irredutíveis de D_N. De fato,a soma dos quadrados dos seus graus é igual a $2\times 1+\frac{1}{2}(n-1)\times 4=2N$, que é a ordem de D_N.

[3]Note que $(\frac{N}{2}+3)-4=\frac{N}{2}-1$ é o número de representações de grau 2 de D_N.

	r^k	sr^k
Ψ_1	1	1
Ψ_2	1	-1
Ψ_3^h	$2\cos(\frac{2\pi hk}{N})$	0

TABELA 4.3: Tabela de caráteres do grupo D_N para N ímpar, $0 \leq k < N$, $0 < h \leq \frac{N-1}{2}$.

Capítulo 5

Transformada de Fourier no Grupo Diedral

5.1 Transformada de Fourier em Grupos Genéricos

Agora consideraremos o problema do subgrupo escondido numa situação em que tanto o grupo G quanto o seu subgrupo H podem não ser abelianos.

Sabemos que para grupos abelianos as representações irredutíveis são sempre uni-dimensionais, mas para grupos não abelianos as representações irredutíveis são homomorfismos $\rho : G \to GL(V)$ tomando valores no conjunto $GL(V)$ das matrizes unitárias de dimensão d_ρ. Considere $\widehat{G} = \{\rho_1, \ldots, \rho_k\}$ como sendo o conjunto de todas as representações irredutíveis de G, a menos de isomorfismo. Assim podemos definir a transformada de Fourier sobre G da seguinte forma.

Definição 5.1 (Transformada de Fourier sobre Grupos Finitos) *Seja G um grupo finito, $f : G \to \mathbb{C}$ uma aplicação qualquer entre os conjuntos G e $\mathbb{C}$. Para*

uma representação irredutível ρ de G de dimensão d_ρ, definimos a transformada de Fourier de f na representação ρ como sendo

$$\widehat{f}(\rho) = \sqrt{\frac{d_\rho}{|G|}} \sum_{g \in G} f(g)\rho(g).$$

Nos referimos a coleção $\langle \widehat{f}(\rho) \rangle_{\rho \in \widehat{G}}$ como a transformada de Fourier de f.

Esta definição nos diz que f é mapeada em $|\widehat{G}|$ matrizes podendo ter diferentes dimensões. O número total de entradas nestas matrizes é $\sum_{i=1}^{k} d_i^2 = |G|$ (teorema 2.8).

Podemos enxergar a transformada de Fourier como um mapeamento de $\mathbb{C}[G]$ ($\mathbb{C}[G]$ é o espaço das combinações lineares complexas de G) em $\mathbb{C}^{|G|}$, de modo que, para cada $g \in G$ temos um vetor $\sqrt{\frac{d_\rho}{|G|}}\rho_{ij}(g)$ de tamanho $|G|$ ($\rho_{ij}(g)$ indica a ij-ésima entrada de $\rho(g)$). Agora se F é a matriz deste mapeamento, então é fácil mostrar que F é uma matriz unitária. De fato, se cada coluna de F corresponde aos valores $\sqrt{\frac{d_\rho}{|G|}}\rho_{ij}(g)$ de um único elemento $g \in G$, e se c_g, c_h são duas colunas distintas de F, então nós temos

$$\begin{aligned}
c_g c_h^* &= \frac{1}{|G|} \sum_{\rho,i,j} d_\rho \rho_{ij}(g)\rho_{ij}(h)^* \\
&= \frac{1}{|G|} \sum_{\rho} d_\rho \sum_{i} \sum_{j} \rho_{ij}(g)\rho_{ij}(h)^* \\
&= \frac{1}{|G|} \sum_{\rho} d_\rho \sum_{i} \rho_{ii}(gh^{-1}) \\
&= \frac{1}{|G|} \sum_{\rho} d_\rho \chi_\rho(gh^{-1}) \\
&= \frac{r_G(gh^{-1})}{|G|} = 0 \qquad (5.1)
\end{aligned}$$

Analogamente temos, $c_g c_g^* = 1$.

Outra propriedade da transformada de Fourier é a linearidade em f. Realmente,

$$\begin{aligned}\widehat{\sum_{i=1}^{k} f_i}(\rho) &= \sqrt{\frac{d_\rho}{|G|}}\sum_{g\in G}(\sum_{i=1}^{k} f_i(g))\rho(g) = \sqrt{\frac{d_\rho}{|G|}}\sum_{g\in G}(\sum_{i=1}^{k} f_i(g)\rho(g)) \\ &= \sum_{i=1}^{k}(\sqrt{\frac{d_\rho}{|G|}}\sum_{g\in G} f_i(g)\rho(g)) = \sum_{i=1}^{k}\widehat{f_i}(\rho).\end{aligned}$$

Agora consideremos o seguinte exemplo.

Exemplo 5.1 *Calcularemos a seguir a transformada de Fourier no grupo D_4 e explicitaremos a matriz desta transformação.*

Sabemos que D_4 é o grupo Diedral de ordem 8, e os seus elementos são dados por $D_4 = \{e, r, r^2, r^3, s, sr, sr^2, sr^3\}$. De acordo com o capítulo 4 as representações irredutíveis de D_4 são as seguintes:

$$\begin{aligned}\Psi_1 &= \{1,1,1,1,1,1,1,1\} \\ \Psi_2 &= \{1,1,1,1,-1,-1,-1,-1\} \\ \Psi_3 &= \{1,-1,1,-1,1,-1,1,-1\} \\ \Psi_4 &= \{1,-1,1,-1,-1,1,-1,1\} \\ \Psi_5 &= \{\rho(e) = \left(\begin{smallmatrix}1 & 0\\ 0 & 1\end{smallmatrix}\right),\ \rho(r) = \left(\begin{smallmatrix}\varepsilon & 0\\ 0 & \varepsilon^{-1}\end{smallmatrix}\right),\ \rho(r^2) = \left(\begin{smallmatrix}\varepsilon^2 & 0\\ 0 & \varepsilon^{-2}\end{smallmatrix}\right),\ \rho(r^3) = \left(\begin{smallmatrix}\varepsilon^3 & 0\\ 0 & \varepsilon^{-3}\end{smallmatrix}\right), \\ &\quad \rho(s) = \left(\begin{smallmatrix}0 & 1\\ 1 & 0\end{smallmatrix}\right),\ \rho(sr) = \left(\begin{smallmatrix}0 & \varepsilon^{-1}\\ \varepsilon & 0\end{smallmatrix}\right),\ \rho(sr^2) = \left(\begin{smallmatrix}0 & \varepsilon^{-2}\\ \varepsilon^2 & 0\end{smallmatrix}\right),\ \rho(sr^2) = \left(\begin{smallmatrix}0 & \varepsilon^{-3}\\ \varepsilon^3 & 0\end{smallmatrix}\right)\},\end{aligned}$$

onde $\varepsilon = e^{\frac{\pi i}{2}} = i$. Aplicando a transformada de Fourier definida em (5.1) no conjunto das representações irredutíveis de D_4, obtemos

$$
\begin{aligned}
\widehat{f}(\Psi_1) &= \frac{\sqrt{s}}{4}[f(e)+f(r)+f(r^2)+f(r^3)+f(2)+f(sr)+f(sr^2)+f(sr^3)]\\
\widehat{f}(\Psi_2) &= \frac{\sqrt{s}}{4}[f(e)+f(r)+f(r^2)+f(r^3)-f(2)-f(sr)-f(sr^2)-f(sr^3)]\\
\widehat{f}(\Psi_3) &= \frac{\sqrt{s}}{4}[f(e)-f(r)+f(r^2)-f(r^3)+f(2)-f(sr)+f(sr^2)-f(sr^3)]\\
\widehat{f}(\Psi_4) &= \frac{\sqrt{s}}{4}[f(e)-f(r)+f(r^2)-f(r^3)-f(2)+f(sr)-f(sr^2)+f(sr^3)]\\
\widehat{f}(\Psi_5) &= \frac{1}{2}[f(e)\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)+f(r)\left(\begin{smallmatrix}i&0\\0&i^{-1}\end{smallmatrix}\right)+f(r^2)\left(\begin{smallmatrix}i^2&0\\0&i^{-2}\end{smallmatrix}\right)+f(r^3)\left(\begin{smallmatrix}i^3&0\\0&i^{-3}\end{smallmatrix}\right)+\\
&\quad f(s)\left(\begin{smallmatrix}0&1\\1&0\end{smallmatrix}\right)+f(sr)\left(\begin{smallmatrix}0&i^{-1}\\i&0\end{smallmatrix}\right)+f(sr^2)\left(\begin{smallmatrix}0&i^{-2}\\i^2&0\end{smallmatrix}\right)+f(sr^2)\left(\begin{smallmatrix}0&i^{-3}\\i^3&0\end{smallmatrix}\right)].
\end{aligned}
$$

Logo a matriz da transformada de Fourier no grupo D_4 é dada por

$$
F=\begin{bmatrix}
\frac{\sqrt{2}}{4} & \frac{\sqrt{2}}{4} & \frac{\sqrt{2}}{4} & \frac{\sqrt{2}}{4} & \frac{\sqrt{2}}{4} & \frac{\sqrt{2}}{4} & \frac{\sqrt{2}}{4} & \frac{\sqrt{2}}{4}\\
\frac{\sqrt{2}}{4} & \frac{\sqrt{2}}{4} & \frac{\sqrt{2}}{4} & \frac{\sqrt{2}}{4} & -\frac{\sqrt{2}}{4} & -\frac{\sqrt{2}}{4} & -\frac{\sqrt{2}}{4} & -\frac{\sqrt{2}}{4}\\
\frac{\sqrt{2}}{4} & -\frac{\sqrt{2}}{4} & \frac{\sqrt{2}}{4} & -\frac{\sqrt{2}}{4} & \frac{\sqrt{2}}{4} & -\frac{\sqrt{2}}{4} & \frac{\sqrt{2}}{4} & -\frac{\sqrt{2}}{4}\\
\frac{\sqrt{2}}{4} & -\frac{\sqrt{2}}{4} & \frac{\sqrt{2}}{4} & -\frac{\sqrt{2}}{4} & -\frac{\sqrt{2}}{4} & \frac{\sqrt{2}}{4} & -\frac{\sqrt{2}}{4} & \frac{\sqrt{2}}{4}\\
\frac{1}{2} & \frac{i}{2} & \frac{-1}{2} & \frac{-i}{2} & 0 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & \frac{1}{2} & \frac{1}{2i} & \frac{-1}{2} & \frac{-1}{2i}\\
0 & 0 & 0 & 0 & \frac{1}{2} & \frac{i}{2} & \frac{-1}{2} & \frac{-i}{2}\\
\frac{1}{2} & \frac{1}{2i} & \frac{-1}{2} & \frac{-i}{2} & 0 & 0 & 0 & 0
\end{bmatrix}. \tag{5.2}
$$

Definição 5.2 *Seja $f: G \to \mathbb{C}$ uma função. A transformada de Fourier inversa de $\widehat{f}$ é definida por*

$$
f(g)=\sqrt{\frac{1}{|G|}}\sum_{\rho\in\widehat{G}}\sqrt{d_\rho}\,Tr(\widehat{f}(\rho)\rho(g^{-1})).
$$

Note que esta definição realmente faz sentido. Com efeito, se substituirmos a definição de $\widehat{f}$ na definição para a inversa, lembrando que o caráter da representação

regular de G é

$$r_G(g) = \sum_{\rho \in \widehat{G}} d_\rho \chi_\rho(g) = \begin{cases} 0 & \text{se } g \neq e \\ |G| & \text{se } g = e \end{cases} \quad \text{(lema 2.1)},$$

e trocando a ordem da soma, obtemos

$$\frac{1}{|G|} \sum_{g' \in G} f(g') \sum_{\rho \in G} d_\rho \mathrm{Tr}(\rho(g'g^{-1})) = \begin{cases} 0 & \text{se } g \neq g' \\ f(g) & \text{se } g = g' \end{cases}.$$

Assim a igualdade segue para $g = g'$.

A transformada de Fourier pode ser aplicada tanto numa função quanto num estado da base computacional. Como a transformada de Fourier é um operador linear unitário, então sabemos como ela atua num estado genérico da base computacional

$$\sum_{g \in G} f(g) \left| g \right\rangle . \tag{5.3}$$

Assim aplicando a transformada de Fourier no estado dado pela expressão (5.3) temos

$$\sum_{\rho \in \widehat{G}} \sum_{1 \leq i,j \leq d_\rho} \widehat{f}(\rho)_{ij} \left| \rho, i, j \right\rangle .$$

Esta é a definição da transformada de Fourier quântica para grupos finitos.

5.2 O Método Padrão de Solução

Muitos algoritmos quânticos, incluindo o algoritmo de Shor para fatoração e logaritmo discreto reduzem-se ao PSE, onde um subgrupo H de um grupo G deve ser determinado de um estado quântico $|\psi\rangle$, sendo este uma superposição numa

classe lateral (à esquerda) de H. Estes $\mathrm{PSE_S}$ são resolvidos pela amostragem de Fourier: a transformada de Fourier do estado $|\psi\rangle$ é calculada e medida. Quando o grupo for não abeliano duas importantes variações da amostragem de Foureir são identificadas: o método padrão *fraco*, onde somente o "nome" da representação é medido deixando os índices matriciais inobserváveis, e o método padrão *forte*, onde a medida é completa, i.e., tanto a representação quanto os índices matricias são medidos. Usaremos no nosso trabalho as duas versões do método padrão de solução.

O algoritmo que apresentaremos agora, o qual chamaremos de algoritmo padrão, é uma generalização do PSE em grupos Abelianos. Este foi primeiramente introduzido por (HALLGREN *et al*, 2003).

O algoritmo é o seguinte:

Passo 1. Inicialize o computador quântico numa superposição uniforme sobre os elementos do grupo:

$$\frac{1}{\sqrt{|G|}} \sum_{g \in G} |g, 0\rangle \, .$$

Passo 2. Calcule f sobre esta superposição para obter: $\frac{1}{\sqrt{|G|}} \sum_{g \in G} |g, f(g)\rangle \, .$

Passo 3. Meça o segundo registrador. Como f assume valores distintos nas classes laterais (à esquerda) de H, o estado resultante será a superposição

$$\frac{1}{\sqrt{|H|}} \sum_{h \in H} |ch, f(ch)\rangle \, ,$$

para alguma classe lateral cH de H. Além disso, c está uniformemente distribuído sobre G.

Passo 4. Aplique a transformada de Fourier no primeiro registrador do estado do passo 3 e desconsidere o segundo registrador que tem o mesmo valor para todos os

termos da soma, para obter

$$\sum_{\rho\in\widehat{G}}\sum_{1\leq i,j\leq d_\rho}\sqrt{\frac{d_\rho}{|G|}}\sqrt{\frac{1}{|H|}}(\sum_{h\in H}\rho(ch))_{i,j}\,|\rho,i,j\rangle=\sum_{\rho\in\widehat{G}}\sum_{1\leq i,j\leq d_\rho}\widehat{f}(\rho)_{i,j}\,|\rho,i,j\rangle\,,$$

lembrando que $\widehat{f}(\rho)_{i,j}$ é um número complexo.

Passo 5. Meça o primeiro registrador e observe uma representação ρ.

Agora usaremos a versão fraca do método padrão para observar a representação ρ.

Começamos medindo a primeira parte da tripla $|\rho,i,j\rangle$. Assim, nós observamos $\rho\in\widehat{G}$ com probabilidade

$$\sum_{1\leq i,j\leq d_\rho}|\widehat{f}(\rho)_{i,j}|^2=\|\widehat{f}(\rho)\|^2,$$

onde $\|M\|$ denota a norma matricial Euclidiana dada por $\|M\|^2=\sum_{i,j}|M_{i,j}|^2$.

Agora seja f uma *função indicadora* de uma classe lateral (à esquerda) de H, i.e., para algum $c\in G$,

$$f(g)=\begin{cases}\frac{1}{\sqrt{|H|}} & \text{se } g\in cH, \text{ e}\\ 0 & \text{caso contrário.}\end{cases}\tag{5.4}$$

Nosso objetivo é encontrar a transformada de Fourier de f e mostrar que isto equivale a calcular a transformada de Fourier do estado $\frac{1}{\sqrt{|H|}}\sum_{h\in H}|ch\rangle$, dado no final do passo 3 do algoritmo padrão. De fato, a transformada de Fourier de f é dada por

$$\widehat{f}(\rho)=\sqrt{\frac{d_\rho}{|G|}}\sqrt{\frac{1}{|H|}}\sum_{h\in H}\rho(ch).$$

Como vimos no final da seção anterior, se aplicarmos a transformada de Fourier num estado quântico genérico $\sum_{g\in G} f(g)\,|g\rangle$, nós obtemos

$$\sum_{\rho\in\widehat{G}}\sum_{1\leq i,j\leq d_\rho}\widehat{f}(\rho)_{i,j}\,|\rho,i,j\rangle=\sum_{\rho\in\widehat{G}}\sum_{1\leq i,j\leq d_\rho}\sqrt{\frac{d_\rho}{|G|}}\sqrt{\frac{1}{|H|}}(\sum_{h\in H}\rho(ch))_{i,j}\,|\rho,i,j\rangle\,,$$

que é a transformada de Fourier do estado $\frac{1}{\sqrt{|H|}}\sum_{h\in H}|ch,f(ch)\rangle$, visto no passo 4 do algoritmo padrão.

Agora abriremos um parêntese na nossa discussão para introduzirmos uma notação que será útil na próxima seção.

Considere um subconjunto S de G, e defina $|S\rangle=\frac{1}{\sqrt{|S|}}\sum_{g\in S}|g\rangle$ e $\rho(S)=\rho(|S\rangle)=\frac{1}{\sqrt{|S|}}\sum_{g\in S}\rho(g)$. Sendo 1_G a representação trivial, temos que

$$\begin{aligned}1_G(G) &= \frac{1}{\sqrt{|G|}}\sum_{g\in G}1_G(g)=\frac{1}{\sqrt{|G|}}\sum_{g\in G}1\\ &= \frac{|G|}{\sqrt{|G|}}=\sqrt{|G|}.\end{aligned}$$

Como a representação trivial é irredutível, nós temos que para qualquer outra representação ρ, $\rho(G)=0$. De fato, $\rho(G)=\frac{1}{\sqrt{|G|}}\sum_{g\in G}\rho(g)=(\rho|1_G)=0$.

Como vimos anteriormente, a probabilidade de observar ρ é $\sum_{1\leq i,j\leq d_\rho}|\widehat{f}(\rho)_{i,j}|^2=\|\widehat{f}(\rho)\|^2$. A vantagem de observar somente a representação ρ deixando de lado os índices matriciais vem do seguinte fato chave sobre a transformada de Fourier.

Lema 5.1 *A probabilidade de observar ρ é a mesma para uma superposição uniforme sobre uma classe lateral cH ou (Hc), como para uma superposição em H.*

Prova. $\widehat{f}(\rho)=\sqrt{\frac{d_\rho}{|G||H|}}\sum_{h\in H}\rho(ch)=\sqrt{\frac{d_\rho}{|G||H|}}\rho(c)\sum_{h\in H}\rho(h)$, e como $\rho(c)$ é uma

matriz unitária,

$$\|\widehat{f}(\rho)\|^2 = \|\rho(c)\sum_{h\in H}\rho(h)\|^2 = \|\sum_{h\in H}\rho(h)\|^2.$$

■

Dado este lema, podemos assumir, sem perda de generalidade, que nossa função f é $\frac{1}{\sqrt{|H|}}$ no subgrupo H, e zero caso contrário.

5.2.1 A Probabilidade de Medir ρ

Vimos na demonstração do lema (5.1) que a probabilidade de observar ρ depende apenas da soma $\sum_{h\in H}\rho(h)$. Esta soma é um operador linear, pois, trata-se de uma soma de transformações lineares. Iniciaremos esta seção mostrando que $\frac{1}{\sqrt{|H|}}\sum_{h\in H}\rho(h)$ é uma projeção.

Lema 5.2 *Seja ρ uma representação irredutível de G. Para qualquer subgrupo $H \leq G$, $\rho(H) = \frac{1}{\sqrt{|H|}}\sum_{h\in H}\rho(h)$ é $\sqrt{|H|}$ vezes uma matriz projeção, e o posto$(\rho(H)) = (\chi_\rho|\chi_{1_H})_H$.*

Prova. Considere a restrição $\mathrm{Res}_H\rho$. Esta pode ser decomposta numa soma direta de representações irredutíveis $\sigma_1, \ldots, \sigma_k$, e escrevemos $\mathrm{Res}_H\rho = \sigma_1 \oplus \ldots \oplus \sigma_k$. Assim, considerando uma base apropriada, temos que $\frac{1}{\sqrt{|H|}}\sum_{h\in H}\rho(h)$ é composta por blocos, cada bloco correspondendo a cada σ_i. Em particular, a matriz $\frac{1}{\sqrt{|H|}}\sum_{h\in H}\rho(h)$ é

$$U\begin{bmatrix} \frac{1}{\sqrt{|H|}}\sum_{h\in H}\sigma_1(h) & 0 & \ldots & 0 \\ 0 & \frac{1}{\sqrt{|H|}}\sum_{h\in H}\sigma_2(h) & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & \frac{1}{\sqrt{|H|}}\sum_{h\in H}\sigma_k(h) \end{bmatrix}U^\dagger$$

para alguma transformação unitária U e representações irredutíveis σ_i de H (com possíveis repetições). Sabemos que a soma $\frac{1}{\sqrt{|H|}}\sum_{g\in H}\sigma_i(g)$ é diferente de zero somente quando a representação irredutível for a representação trivial, neste caso, a soma é $\sqrt{|H|}$. Assim obtemos uma matriz onde cada autovalor ou é 0 ou é 1. Note que só aparece 1 na matriz quando a representação é trivial. Portanto, a quantidade de colunas linearmente independentes na matriz é igual ao número de representações triviais contidas em $\mathrm{Res}_\rho H$, i.e., $(\chi_\rho|\chi_{1_H})_H$.

■

Portanto, considerando $f : G \to \mathbb{C}$ uma função tal que

$$f(g) = \begin{cases} \frac{1}{\sqrt{|H|}} & \text{se } g \in H, \text{ e} \\ 0 & \text{caso contrário,} \end{cases}$$

temos que a probabilidade de medir ρ no passo 4 do algoritmo padrão é

$$\begin{aligned} \|\widehat{f}(\rho)\|^2 = \|\sqrt{\frac{d_\rho}{|G|}}\sqrt{\frac{1}{|H|}}\sum_{h\in H}\rho(h)\|^2 &= \frac{d_\rho}{|G||H|}(|\sum_{h\in H}\sigma_1(h)|^2 + \ldots + |\sum_{h\in H}\sigma_k(h)|^2)) \\ &= \frac{d_\rho}{|G||H|}|H|^2(\chi_\rho|\chi_{1_H})_H \\ &= \frac{|H|}{|G|}\, d_\rho(\chi_\rho|\chi_{1_H})_H. \end{aligned}$$

Assim finalizamos esta seção com o seguinte teorema.

Teorema 5.1 *Para qualquer subgrupo $H \leq G$, a probabilidade de medir ρ no passo 4 do algoritmo padrão, com subgrupo escondido H, é*

$$\|\widehat{f}(\rho)\|^2 = \frac{|H|}{|G|}\, d_\rho(\chi_\rho|\chi_{1_H})_H.$$

5.3 O Método Padrão de Solução (MPS) Aplicado ao Grupo Diedral

O objetivo principal do nosso trabalho é obter um algoritmo quântico para o PSE Diedral. Para isso faremos uma restrição do MPS para o grupo Diedral, isto é, verificaremos se existe uma solução eficiente para o PSE no grupo Diedral usando este método. (HALLGREN *et al*, 2003) mostraram que existe um algoritmo quântico eficiente para o PSE quando o subgrupo escondido é normal. Os autores fazem uso do método padrão de solução. O primeiro algoritmo quântico para o PSE num grupo não Abeliano foi apresentado por (ETTINGER & HØYER, 2000). O principal resultado do trabalho deles é que existe um algoritmo quântico que resolve o problema do subgrupo Diedral usando apenas um número linear de consultas ao oráculo. Entretanto, o algoritmo não roda em tempo polinomial, mesmo usando poucas avaliações do oráculo. A ineficiência do algoritmo dado por (ETTINGER & HØYER, 2000) é devido ao fato de que o algoritmo aplica um certo número linear de vezes uma subrotina quântica, cada vez produzindo algum dado de saída, e cada vez usando uma única aplicação do oráculo. A coleção de todos os dados de saída determinam o subgrupo escondido com alta probabilidade. Os autores sabem como achar o subgrupo deste conjunto de dados em tempo exponencial, mas não se sabe se existe um algoritmo em tempo polinomial (quântico ou clássico) que faz o pós-processamento dos dados de saída provenientes da subrotina quântica. (ETTINGER & HØYER, 2000) mostraram também, que sem perda de generalidade, o problema de achar o subgrupo escondido no grupo Diedral pode ser reduzido ao caso especial de achar subgrupos escondidos triviais ou gerados por uma reflexão.

Sabemos que o grupo Diedral de ordem $2N$, denotado por D_N, é o grupo das simetrias de um polígono regular de N lados (ver capítulo 4) consistindo de N rotações e N reflexões. Assumiremos no algoritmo descrito logo abaixo para o problema do subgrupo Diedral, que o subgrupo escondido $H = \{e, s\}$ é gerado por uma reflexão s.

De forma suscinta, o nosso problema é o seguinte:

Dado uma função $f : D_N \to R$ do grupo Diedral para um conjunto arbitrário R. A função f é constante nas classes laterais do subgrupo $H = \{e, s\}$ de D_N e distinta em cada classe lateral. O nosso objetivo é reconstruir o subgrupo H, ou seja, achar s.

O algoritmo é o seguinte:

Passo 1. Inicialize o computador quântico numa superposição uniforme sobre os elementos de D_N:

$$\frac{1}{\sqrt{2N}} \sum_{g \in D_N} |g, 0\rangle .$$

Passo 2. Calcule f sobre esta superposição para obter: $\frac{1}{\sqrt{2N}} \sum_{g \in D_N} |g, f(g)\rangle$.

Passo 3. Meça o segundo registrador. O estado resultante será a superposição

$$\frac{1}{\sqrt{2}} \sum_{h \in H} |ch, f(ch)\rangle ,$$

para alguma classe lateral cH de H. Além disso, c está uniformemente distribuído sobre D_N.

Passo 4. Aplique a transformada de Fourier no primeiro registrador do estado do passo 3 para obter

$$\sum_{\rho \in \widehat{D}_N} \sum_{1 \leq i,j \leq d_\rho} \widehat{f}(\rho)_{i,j} |\rho, i, j\rangle .$$

Passo 5. Meça o primeiro registrador e observe uma representação ρ.

Vimos na seção anterior que a probabilidade de observar ρ utilizando o método padrão fraco é

$$\begin{aligned} \|\widehat{f}(\rho)\|^2 &= \frac{2}{2N}\, d_\rho(\chi_\rho|\chi_{1_H})_H \\ &= \frac{d_\rho}{2N}\sum_{h\in H}\chi_\rho(h)\chi_{1_H}(h^{-1}) \\ &= \frac{d_\rho}{2N}\sum_{h\in H}\chi_\rho(h). \end{aligned}$$

De acordo com a tabela de caráteres do grupo Diedral dada no Capítulo 4, temos

- Se $d_\rho = 1$ então

$$\begin{aligned} \|\widehat{f}(\rho)\|^2 &= \frac{1}{2N}(\chi_\rho(e)+\chi_\rho(s)) \\ &= \frac{1}{2N}(1\pm 1) \leq \frac{1}{N} \leq \frac{1}{2}. \end{aligned}$$

- Se $d_\rho = 2$ então

$$\|\widehat{f}(\rho)\|^2 = \frac{1}{N}(\chi_\rho(e)+\chi_\rho(s)) = \frac{2}{N} \leq \frac{1}{2}.$$

Para sabermos se nosso algoritmo é eficiente, teremos que calcular o número de vezes que devemos repetir o algoritmo acima para obter ρ com probabilidade maior que $\frac{1}{2}$.

Suponhamos que executamos o nosso algoritmo um número X de vezes. A probabilidade de obter ρ na primeira rodada do algoritmo é $\frac{2}{N}$. Assim temos que

após X rodadas, a probabilidade de obter ρ pelo menos uma vez é

$$1 - (1 - \frac{2}{N})^X, \tag{5.5}$$

onde $(1 - \frac{2}{N})^X$ é a probabilidade de não obter ρ todas as X vezes que rodamos o algoritmo.

Agora, usando o binômio de Newton, nós aproximamos o termo $(1 - \frac{2}{N})^X$ da expressão (5.5) por $1 - \frac{2X}{N}$ com erro de aproximação da ordem $O(\frac{1}{N^2})$. Suponhamos então que $1-(1-\frac{2X}{N}) = \frac{1}{2} \Rightarrow X = \frac{N}{4}$. Isto quer dizer que após $\frac{N}{4}$ repetições do nosso algoritmo obtemos ρ com probabilidade em torno de $\frac{1}{2}$. Sabemos que um algoritmo eficiente para o PSE faz $\log_2 |G|$ chamadas ao oráculo, quando o grupo em questão é G. Para maiores detalhes veja (ETTINGER *et al*, 1999). Note que o nosso algoritmo não é eficiente, pois ele usa $\frac{N}{4}$ chamadas do oráculo, que é exponencialmente maior que $\log_2 |D_N| = \log_2 2N$.

De acordo com os trabalhos de (ROTTELER & BETH, 1998), a complexidade do cálculo da transformada de Fourier em D_N é $O(\log^2 N)$. Assim a complexidade de tempo total do nosso algoritmo para reconstruir o subgrupo H com probabilidade em torno de $\frac{1}{2}$ é $O(N \log^2 N)$. Note que precisamos de um algoritmo que reconstrua o subgrupo escondido H com probabilidade maior ou igual que $\frac{1}{2}$, para aplicarmos o *limite de Chernoff* (CHUANG & NIELSEN, 2000).

Como não obtivemos sucesso usando a versão fraca do método padrão de solução, voltaremos então ao passo 5 do algoritmo padrão para o grupo Diedral. Desta vez, faremos uma medida completa, i.e., vamos medir uma representação ρ juntamente com os índices matriciais (este é o método padrão forte). Assim, a probabilidade de medir um dado estado $|\rho, i, j\rangle$ depois do passo 4 do algoritmo padrão (assumindo

que o elemento escolhido aleatoriamente no passo 3 foi c) é:

$$\Pr_c(|\rho, i, j\rangle) = \frac{d_\rho}{|D_N||H|} |\sum_{h\in H} \rho_{ij}(ch)|^2.$$

Como c está uniformemente distribuído sobre D_N no passo 3, temos que a probabilidade de medir estado qualquer $|\rho, i, j\rangle$ é:

$$\Pr(|\rho, i, j\rangle) = \frac{1}{|D_N|} \sum_{g\in D_N} \Pr_g(|\rho, i, j\rangle).$$

Portanto, assumindo $H = \{e, s\}$ como no caso anterior, e levando em conta o grau da representação ρ, nós temos

- Se $d_\rho = 1$ então

$$\Pr_g(|\rho, i, j\rangle) = \frac{1}{4N}|\rho_{ij}(g) + \rho_{ij}(gs)|^2 = \frac{1}{4N}|\pm 1 \pm 1|^2 \leq \frac{1}{N}$$

  logo,

$$\Pr(|\rho, i, j\rangle) = \frac{1}{2N} \sum_{g\in D_N} Pr_g(|\rho, i, j\rangle) \leq \frac{1}{2N}(2N\frac{1}{N}) = \frac{1}{N}.$$

- Se $d_\rho = 2$ então

$$\Pr_g(|\rho, i, j\rangle) = \frac{1}{2N}|\rho_{ij}(g) + \rho_{ij}(gs)|^2$$

  Neste caso ainda temos duas possibilidades:

  1. Se $g = r^k$ então

$$\Pr_g(|\rho, i, j\rangle) = \begin{cases} \frac{1}{2N}|\varepsilon^{hk}|^2 & = & \frac{1}{2N}, \text{ ou} \\ \frac{1}{2N}|\varepsilon^{-hk}|^2 & = & \frac{1}{2N} \end{cases}$$

2. Se $g = sr^k$ então

$$\Pr_g(|\rho, i, j\rangle) = \begin{cases} \frac{1}{2N}|\varepsilon^{hk}|^2 & = & \frac{1}{2N}, \text{ ou} \\ \frac{1}{2N}|\varepsilon^{-hk}|^2 & = & \frac{1}{2N} \end{cases}$$

portanto,

$$\Pr(|\rho, i, j\rangle) = \frac{1}{2N}(2N\frac{1}{2N}) = \frac{1}{2N}.$$

Note então que no caso do grupo Diedral, a probabilidade de observar ρ usando o método padrão forte é tão pequena quanto a probabilidade de observar ρ usando o método anterior. Este resultado vem descartar todas as possibilidades de obter um algoritmo quântico eficiente para o problema do subgrupo Diedral usando este método.

Muitas tentativas têm sido feitas para achar um algoritmo eficiente para o PSE no grupo Diedral. Uma razão para isto é que o grupo Diedral é o mais simples dos grupos não abelianos, e portanto, mais fácil de ser estudado. Outra razão para resolver o PSE Diedral é a aplicação em sistemas de criptografia, como pode ser visto em (REGEV, 2004b). Agora daremos uma visão geral dos resultados conhecidos sobre o PSE no grupo Diedral.

(ETTINGER & HØYER, 2000) mostraram um algoritmo quântico que produz dados suficientes para encontrar qualquer subgrupo escondido H no grupo Diedral D_N, contudo não se sabe se estes dados podem ser pós-processados em tempo $O(\text{poly}(\log N))$ para reconstruir o subgrupo H. Resumidamente, o algoritmo deles explora a simplicidade do grupo cíclico $\mathbb{Z}_N \leq D_N$, e usa a transformada de Fourier para grupos abelianos para coletar informações que serão usadas para reconstruir o subgrupo H. Ettinger e Hoyer reduziram o problema original para o caso particular

de achar um subgrupo H gerado por uma reflexão. O principal resultado deles está no seguinte teorema.

Teorema 5.2 *Seja $f : D_N \rightarrow R$ uma função constante nas classes laterais do subgrupo H e distinta em cada classe lateral. Existe um algoritmo quântico que dado f, usa $O(\log N)$ avaliações de f e resulta um subconjunto $X \subseteq H$ tal que X é um conjunto gerador para H com probabilidade no mínimo $1 - \frac{2}{N}$.*

Mais tarde, (KUPERBERG, 2003) deu o primeiro algoritmo quântico em tempo subexponencial para o PSE Diedral, com tempo e complexidade de consulta $O(\exp(C\sqrt{\log N}))$. Isto é bem melhor do que $O(\sqrt{N})$ que é a complexidade clássica para o PSE Diedral. Este é atualmente o melhor algoritmo quântico conhecido para este problema. Contudo, este algoritmo requer um espaço de solução superpolinomial.

O principal resultado do trabalho de Kuperberg está no seguinte teorema.

Teorema 5.3 *Existe um algoritmo quântico que determina uma reflexão escondida no grupo Diedral com tempo e complexidade de consulta $O(exp(C\sqrt{\log N}))$.*

Num trabalho ainda mais recente, (REGEV, 2004a) descreveu uma versão do algoritmo de Kuperberg para resolver o PSE Diedral. O algoritmo de Regev também roda em tempo superpolinomial, mas a novidade é que o espaço requerido pelo algoritmo é apenas polinomial, isto é, polinomial na ordem $O(\log N)$.

Capítulo 6

Conclusão

Nós mostramos no Capítulo 3, omitindo alguns detalhes, que para qualquer grupo finito abeliano G, o problema do subgrupo escondido pode ser resolvido eficientemente usando um computador quântico. Vimos também que uma solução eficiente do PSE abeliano é a base do algoritmo de Shor para fatoração. O ponto chave na resolução do PSE abeliano é a amostragem de Fourier, isto é, a transformada de Fourier é calculada nos estados que contém alguma informação sobre o subgrupo escondido, e então os estados resultantes são medidos afim de obter informações suficientes para determinar os geradores do subgrupo escondido.

Nós descrevemos no Capítulo 5 o caso não abeliano, usando a teoria da representação para definir a transformada de Fourier em grupos arbitrários. Então, particularizamos o PSE para o grupo Diedral e propusemos um algoritmo quântico para este problema, cujo ingrediente básico foi a amostragem de Fourier. Concluímos que nosso algoritmo é ineficiente pois ele reconstrói o subgrupo escondido com complexidade exponencial no tempo $O(N \log^2 N)$.

No final do Capítulo 5, nós descrevemos os resultados atuais sobre o PSE Diedral

e constatamos que nenhuma solução eficiente para este problema é conhecida.

São as aplicações práticas que nos incentivam a continuar nesta área tão interessante. Vimos que já existem algoritmos quânticos para fatoração e logaritmo discreto, e que estes algoritmos permitem a quebra dos principais códigos de criptografia usados atualmente.

Como proposta para trabalhos futuros, investigaremos em quais famílias de grupos a transformada de Fourier pode ser calculada eficientemente, e a partir daí analizaremos a extensão para grupos mais complexos, com vista na construção de algoritmos quânticos para o PSE.

Referências Bibliográficas

AHN, L. V., 2002. Survey: Quantum computation and the hidden subgroup problem. Technical report, Dept. of Science Computer, Carnegie Mellon University, Pittsburgh.

BENIOFF, P., 1985. "the computer as a physical system: A microscopicquantum mechanical hamiltonian model of computers as represented by turing machines". *Proc Roy Soc Lond A 400*, pp. 97–117.

CHUANG, I. L. & NIELSEN, M. A., 2000. Quantum Computation and Quantum Information. *Cambridge Univesity Press*.

DAMGARD, I., 2004. QIP Note: On the Quantum Fourier Transform and Applications. Technical report, computer science department of Aarhus University.

DEUTSCH, D., 1985. "quantum theory, the church-turing principle and the universal quantum computer". *Proceedings of the Royal Society*, vol. A425, pp. 73–90.

ETTINGER, M. & HØYER, P., 2000. "on quantum algorithms for noncommutative hidden subgroups". *Adv. Appl. Math.*, vol. 25, n. 3, pp. 239–251.

ETTINGER, M., HØYER, P., & KNILL, E., 1999. "hidden subgroup states are almost orthogonal". *quant-ph/9901034*.

FEYNMAN, R., 1982. "simulating physics with computers". *International Journal of Theoretical Physics*, vol. 21, pp. 467–488.

GARCIA, A. & LEAQUAIN, Y., 1998. Álgebra: um curso de introdução. *Projeto Euclides*.

HALLGREN, S., RUSSEL, A., & TA-SHMA, A., 2003. "the hidden subgroup problem and quantum computation using group representation". *Siam J. Computation*, vol. 32, n. 4, pp. 916–934.

HAMERMESH, M., 1962. Group Theory And Its Application To Physical. *Dover Publication New York Lnc*.

JOZSA, R., 1998. "quantum algorithms and the fourier transform". *Proc Roy Soc Lond A*, pp. 323–337.

KOBLITZ, N., 1998. Algebraic aspects of cryptography. *Berlin ; New York : Springer-Verlag*.

KUPERBERG, G., 2003. "a subexponential-time quantum algorithm for the dihedral hidden subgroup problem". *arXiv:quant-ph/0302112.*, vol. 1.

LANG, S. & ADISAN-WESLEY, 1993. Algebra. *Springer-Verlag New York Lnc.*

LAVOR, C., MANSUR, L., & PORTUGAL, R., 2003a. "grover's algorithm: Quantum data search". *Quantum Physics, abstract quant-ph/0301079*, vol. 1.

LAVOR, C., MANSUR, L., & PORTUGAL, R., 2003b. "shor's algorithm for factoring large integers". *Quantum Physics, Abstract quant-ph/0303175*, vol. 1.

LOMONT, C., 2004. "the hidden subgroup problem - review and open problems". *Quantum Physics, Abstract quant-ph/0411037*.

MASLEN, D. K., 1998. "the efficient computation of fourier transform on the symmetric group". *American Mathematical Society*, vol. 67, pp. 1121–1147.

MASLEN, D. K. & ROCKMORE, D. N., 1997. "separation of variable and computation of fourier transforms on finite group". *American Mathematical Society*, vol. 10, pp. 169–214.

REGEV, O., 2004a. "a subexponential time algorithm for the dihedral hidden subgroup problem with polynomial space".

REGEV, O., 2004b. "quantum computation and lattice problems". *SIAM Journal on Computing*, vol. 33, n. 3, pp. 738–760.

ROTTELER, M. & BETH, T., 1998. "polynomial-time solution to the hidden subgroup problem for a class of non-abelian groups". *quant-ph/9812070*.

SERRE, J.-P., 1997. Linear Representation of Finite Group. *Springer-Verlag*.

SHOR, P. W., 1997. "polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer". *SIAM J. Comput.*, vol. 26, n. 5, pp. 1484–1509.

SIMON, D. R., 1994. "on the power of quantum computation". In *Proceedings of the 35th Annual Symposium on Foundations of Computer Science*, pp. 116–123, Los Alamitos, CA. Institute of Electrical and Electronic Engineers Computer Society Press.

Apêndice A

Demonstrações do Lema de Schur e das Relações de Ortogonalidade de Caráteres

Teorema A.1 (Lema de Schur) .

1. Sejam R_g e R'_g duas representações irredutíveis de um grupo G nos espaços V e W de dimensões n, m respectivamente. Suponha que exista uma matriz retangular $P_{m\times n}$ satisfazendo

$$PR_g = R'_g P,\ \forall\ g \in G. \tag{A.1}$$

Então $P = 0$ ou P é não singular .

2. Se uma representação P comuta com todas as representações irredutíveis R_g de G, então P é um múltiplo escalar λI da matriz identidade.

Prova. Para provarmos *1*, considere γ como sendo o posto de P. A imagem $Px,\ x \in V$ forma um subspaço w de W de dimensão γ. Fixemos as bases $\{v_1, \ldots, v_n\}$ e $\{w_1, \ldots, w_m\}$ correspondentes aos espaços V e W respectivamente, e suponhamos

que os γ primeiros vetores da base de W ($\gamma < m$) forme uma base para w. Como $Px \in w$ podemos escrever $Px = \sum_{i=1}^{\gamma} \alpha_i w_i,\ \alpha_i \in \mathbb{C}$. Então segue da equação (A.1) que

$$R'_g Px = PR_g x = P(\sum_{j=1}^{n} \alpha'_j v_j) = \sum_{j=1}^{n} \alpha'_j Pv_j,\ \ \alpha'_j \in \mathbb{C}. \tag{A.2}$$

Note que a última igualdade da equação (A.2) é um elemento de w. Isto implica que w é invariante por R'_g. Mas como R'_g é irredutível temos ou $w = 0$ ($\gamma = 0$ e $P = 0$) ou $w = W$ ($\gamma = m$ e $m \leq n$).

Agora considere todos os vetores $x \in V$ tais que $Px = 0$. Isto constitui um subspaço v de V (núcleo de P) de dimensão $n - \gamma$, e como $PR_g x = R'_g Px = 0$ temos que v é invariante por R_g. Como R_g é irredútível, ou $v = V$ (e neste caso $\gamma = 0$ e $P = 0$) ou $v = 0$ ($\gamma = n$ e $n \leq m$). Assim temos, ou $P = 0$ ou $\gamma = n = m$ e P é não singular.

Para *2*, temos que a matriz identidade I comuta com todas as matrizes R_g de G, assim também todos os múltiplos λI, e portanto, todas as matrizes $(P - \lambda I)$. De acordo com a parte 1 do teorema (A.2), temos que para cada λ, ou $(P - \lambda I) = 0$ ou $\det(P - \lambda I) \neq 0$. Como o corpo de escalares é o corpo dos números complexos (e sendo este algebricamente fechado) sempre existirá uma solução para a equação algébrica $\det(P - \lambda I) = 0$, logo devemos ter $(P - \lambda I) = 0$, ou seja, $P = \lambda I$.

■

Teorema A.2 (Relações de Ortogonalidade de Caráteres) .

1. Se χ é o caráter de uma representação irredutível, então $(\chi|\chi) = 1$.

2. Se χ e χ' são os caráteres de duas representações irredutíveis não isomorfas, então $(\chi|\chi') = 0$.

Observação A.1 *Para um melhor entendimento da prova do teorema (A.2) acima, distinguiremos diferentes representações usando superscripts, para maiores detalhes da prova consulte (HAMERMESH, 1962).*

Prova. Seja $\widehat{G}$ o conjunto de todas as representações irredutíveis de um grupo finito G. Para uma dada matriz X arbitrária e um elemento qualquer $R \in \widehat{G}$ de dimensão n, construímos a matriz

$$A = \sum_{g \in G} R(g) X R(g^{-1}). \tag{A.3}$$

Temos claramente que A satisfaz as condições da parte 2 do teorema A.1. De fato,

$$\begin{aligned} R(h)A &= \sum_{g \in G} R(h)R(g)XR(g^{-1}) \\ &= \sum_{g \in G} R(h)R(g)XR(g)^{-1}(R(h^{-1})R(h)) \\ &= [\sum_{g \in G} R(hg)XR(\{hg\}^{-1})]R(h). \end{aligned} \tag{A.4}$$

Do fato de que G é finito, e lembrando da tabela de multiplicação de G, temos

$$\sum_{g \in G} R(hg)XR(\{hg\}^{-1}) = \sum_{g \in G} R(g)XR(g^{-1}), \tag{A.5}$$

e portanto, $R(h)A = AR(h)$ para todo $h \in G$. Logo, pela parte 2 do teorema A.1, temos $A = \lambda I$, onde o valor da constante λ dependerá da nossa escolha da matriz arbitrária X.

Suponhamos que escolhemos a matrix X tendo todos os seus elementos nulos, exceto $X_{lm} = 1$, e a constante λ como sendo λ_{lm}. Então da equação (A.3) temos

$$
\begin{aligned}
A_{ij} &= (\sum_{g\in G} R(g)XR(g^{-1}))_{ij} = \sum_{g\in G} R_{il}(g)X_{lm}R_{mj}(g^{-1}) \\
&= \sum_{g\in G} R_{il}(g)R_{mj}(g^{-1}) = \lambda_{lm}\delta_{ij}, \text{ para todo } 1 \leq i,j,l,m \leq n, \qquad \text{(A.6)}
\end{aligned}
$$

onde o símbolo δ_{ij} é chamado *delta de Kronecker*, e é definido por

$$
\delta_{ij} = \begin{cases} 1 & \text{se } i = j \\ 0 & \text{se } i \neq j \end{cases}.
$$

No caso de R ser unitária temos,

$$
\sum_{g\in G} R_{il}(g)R^{*}_{jm}(g) = \lambda_{lm}\delta_{ij}.
$$

Afim de avaliarmos λ_{lm}, façamos $i = j$, e somamos sobre i:

$$
\sum_{g\in G}\sum_{i=1}^{n} R_{il}(g)R_{mi}(g^{-1}) = n\lambda_{lm}. \qquad \text{(A.7)}
$$

Por outro lado, temos

$$
\sum_{g\in G}\sum_{i=1}^{n} R_{il}(g)R_{mi}(g^{-1}) = \sum_{g\in G}\sum_{i=1}^{n} R_{mi}(g^{-1})R_{il}(g) = \sum_{g\in G} R_{ml}(g^{-1}g) = \sum_{g\in G} R_{ml}(e). \qquad \text{(A.8)}
$$

Logo, das equações (A.7) e (A.8) temos

$$
n\lambda_{lm} = \sum_{g\in G} R_{ml}(e) = \sum_{g\in G} \delta_{ml} = |G|\delta_{ml}. \qquad \text{(A.9)}
$$

Então,

$$\lambda_{lm} = \frac{|G|}{n}\delta_{lm}, \tag{A.10}$$

e

$$\sum_{g\in G} R_{il}(g)R_{mj}(g^{-1}) = \frac{|G|}{n}\delta_{lm}\delta_{ij}, \tag{A.11}$$

ou, se R for unitária,

$$\sum_{g\in G} R_{il}(g)R^{*}_{mj}(g) = \frac{|G|}{n}\delta_{lm}\delta_{ij}. \tag{A.12}$$

Agora vamos construir de forma similar uma matriz A que satisfaça a parte 1 do teorema A.1. Sejam $R^{(1)}$ e $R^{(2)}$ duas representações arbitrárias em $\widehat{G}$ de dimensões n_1 e n_2, respectivamente. Então façamos

$$A = \sum_{g\in G} R^{(2)}(g)XR^{(1)}(g^{-1}), \tag{A.13}$$

onde X é uma matriz arbitrária. Assim

$$\begin{aligned} R^{(2)}(h)A &= \sum_{g\in G} R^{(2)}(h)R^{(2)}(g)XR^{(1)}(g^{-1}) \\ &= \sum_{g\in G} R^{(2)}(h)R^{(2)}(g)XR^{(1)}(g^{-1})(R^{(1)}(h^{-1})R^{(1)}(h)) \\ &= [\sum_{g\in G} R^{(2)}(hg)XR^{(1)}(\{hg\}^{-1})]R^{(1)}(h) = AR^{(1)}(h). \end{aligned} \tag{A.14}$$

Portanto, de acordo com a parte 1 do teorema A.1, temos $A = 0$.

Escolhendo X como antes, temos

$$\sum_{g\in G} R^{(2)}_{il}(g)R^{(1)}_{mj}(g^{-1}) = 0, \tag{A.15}$$

ou, se $R^{(1)}$ e $R^{(2)}$ forem unitárias,

$$\sum_{g\in G} R^{(2)}_{il}(g) R^{(1)*}_{mj}(g) = 0. \tag{A.16}$$

Agora consideremos duas representações genéricas $R^{(\mu)}$ e $R^{(\nu)}$ em $\widehat{G}$. Partindo das duas últimas equações dada acima, e fazendo $i = l$ e $j = m$ em (A.15), obtemos

$$\frac{1}{|G|} \sum_{g\in G} R^{(\mu)}_{ii}(g) R^{(\nu)}_{jj}(g^{-1}) = \frac{1}{n_\mu} \delta_{\mu\nu}\delta_{ij}. \tag{A.17}$$

Agora somando sobre i e j:

$$\frac{1}{|G|} \sum_{g\in G} \chi^{(\mu)}(g) \chi^{(\nu)}(g^{-1}) = \delta_{\mu\nu}, \tag{A.18}$$

ou, se $R^{(\mu)}$ e $R^{(\nu)}$ forem unitárias

$$\frac{1}{|G|} \sum_{g\in G} \chi^{(\mu)}(g) \chi^{(\nu)*}(g) = \delta_{\mu\nu} = (\chi^{(\mu)}|\chi^{(\nu)}). \tag{A.19}$$

■