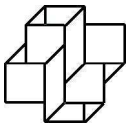


Laboratório Nacional de Computação Científica

Programa de Pós Graduação em Modelagem Computacional

Algoritmos Quânticos para Problemas em Teoria de Grupo Computacional

Por

Demerson Nunes Gonçalves

PETRÓPOLIS, RJ - BRASIL

AGOSTO DE 2009

ALGORITMOS QUÂNTICOS PARA PROBLEMAS EM TEORIA DE GRUPO COMPUTACIONAL

Demerson Nunes Gonçalves

TESE SUBMETIDA AO CORPO DOCENTE DO LABORATÓRIO NACIONAL DE COMPUTAÇÃO CIENTÍFICA COMO PARTE DOS REQUISITOS NECESSÁRIOS PARA A OBTENÇÃO DO GRAU DE DOUTOR EM MODELAGEM COMPUTACIONAL

Aprovada por:

Prof. Renato Portugal, D.Sc
(Presidente)

Prof. Gilson Antônio Giraldi, D.Sc.

Prof. Guilherme Augusto de La Rocque Leal, D.Sc.

Prof. Raul Jose Donangelo, PhD.

PETRÓPOLIS, RJ - BRASIL
AGOSTO DE 2009

Gonçalves, Demerson Nunes

G635a Algoritmos quânticos para problemas em teoria de grupo computacional / Demerson Nunes Gonçalves. Petrópolis, RJ. : Laboratório Nacional de Computação Científica, 2009.

xv, 134 : il.; 29 cm

Orientador: Renato Portugal

Tese (D.Sc.) – Laboratório Nacional de Computação Científica, 2009.

1. Computação Quântica. 2. Problema do Subgrupo Oculto. 3. Algoritmos Quânticos. 4. Teoria de Grupos. 5. Transformada de Fourier I. Portugal, Renato. II. LNCC/MCT. III. Título.

CDD 004.1

"Quando achamos a matemática e a física teórica muito difíceis, voltamo-nos para o misticismo." (Stephen Hawking)

Aos meus pais.

Agradecimentos

A Deus, o que seria de mim sem a fé que deposito nele.

Aos meus pais, Adalcina e Dinivaldo, minha amada esposa Polini e a toda minha família que, com muito carinho e apoio, não mediram esforços para que eu chegasse até aqui.

A todos os professores e funcionários do LNCC, que foram tão importantes na minha vida acadêmica e no desenvolvimento desta tese.

Aos meus amigos e a todos que me ajudaram com seu apoio e suas sugestões.

Finalmente, ao prof. Renato Portugal, pela sugestão do tema, e pela dedicação e incentivo demonstrados durante o desenvolvimento desta tese.

Agradeço a CAPES pelo apóio financeiro.

A todos meu muito obrigado.

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

ALGORITMOS QUÂNTICOS PARA PROBLEMAS EM TEORIA DE GRUPO COMPUTACIONAL

Demerson Nunes Gonçalves

Agosto , 2009

Orientador: Renato Portugal, D.Sc

Neste trabalho apresentamos um novo algoritmo quântico eficiente para o Problema do Subgrupo Oculto (PSO) sobre uma classe especial de grupos metacíclicos, $\mathbb{Z}_p \rtimes \mathbb{Z}_{q^s}$, com $q \mid (p-1)$ e $p/q = \text{poli}(\log p)$, onde p, q são números primos ímpares distintos e s um inteiro positivo qualquer. Em um contexto mais geral, sem impor uma relação entre p e q, obtemos um algoritmo quântico com complexidade de tempo $2^{O(\sqrt{\log p})}$. Em qualquer caso, esses resultados são melhores que qualquer algoritmo clássico para o mesmo fim, cuja complexidade é $\Omega(\sqrt{p})$. Apresentamos também, algoritmos quânticos para o PSO sobre grupos não abelianos de ordem 2^{n+1} que possuem subgrupos cíclicos de índice 2 e para certos produtos semidiretos de grupos $\mathbb{Z}_N^m \rtimes \mathbb{Z}_p$, com m, N inteiros positivos e N fatorado de forma especial.

Abstract of Thesis presented to LNCC/MCT as a partial fulfillment of the requirements for the degree of Doctor of Sciences (D.Sc.)

QUANTUM ALGORITHMS FOR PROBLEMS IN COMPUTATIONAL GROUP THEORY

Demerson Nunes Gonçalves

August, 2009

Advisor: Renato Portugal, D.Sc

We present a new polynomial-time quantum algorithm that solves the hidden subgroup problem (HSP) for a special class of metacyclic groups, namely $\mathbb{Z}_p \rtimes \mathbb{Z}_{q^s}$, with $q \mid (p-1)$ and $p/q = \text{poly}(\log p)$, where p, q are any odd prime numbers and s is any positive integer. This solution generalizes previous algorithms presented in the literature. In a more general setting, without imposing a relation between p and q, we obtain a quantum algorithm with time and query complexity $2^{O(\sqrt{\log p})}$. In any case, those results improve the classical algorithm, which needs $\Omega(\sqrt{p})$ queries. We also present quantum algorithms for the HSP over non-abelian groups of order 2^{n+1} which have a cyclic subgroup of index 2 and for some semidirect product $\mathbb{Z}_N^m \rtimes \mathbb{Z}_p$, where N has a special prime factorization.

Sumário

Lista de Figuras

Figura

Lista de Algoritmos

Algoritmo

Lista de Tabelas

Tabela

Lista de Símbolos e Abreviaturas

PSO : Problema do Subgrupo Oculto.

HSP : Hidden Subgroup Problem.

TFQ : Transformada de Fourier Quântica.

MAF : Método de Amostragem de Fourier.

ω_N : N-ésima raiz da unidade.

$\mathrm{mdc}\,(m,n)$: Máximo divisor comum de m e n.

$\mathbb{Z}_N$: Grupo aditivo dos inteiros módulo N.

$\mathbb{Z}_N^*$: Grupo multiplicativo dos inteiros módulo N invertíveis em relação à multiplicação.

$G \rtimes H$: Produto semidireto do grupos G por H.

$\ker(\phi)$: Núcleo do homomorfismo ϕ.

$\mathrm{Im}(\phi)$: Imagem do homomorfismo ϕ.

G' : Subgrupo dos comutadores de G.

$\mathcal{Z}\,(G)$: Centro do grupo G.

$\langle S \rangle$: Grupo gerado pelo conjunto S.

$\mathrm{Aut}\,(G)$: Grupo dos automorfismos do grupo G.

$|G|$: Ordem do grupo G.

$\mathrm{ord}(g)$: Ordem do elemento g.

$H \leq G$: H é subgrupo de G.

$H \lhd G$: H é subgrupo normal de G.

$\mathcal{N}(H)$: Subgrupo normalizador de H em G.

$|\cdot\rangle$: *Ket.*

$\langle\cdot|$: *Bra.*

$\mathbb{C}$: Corpo dos números complexos.

$|j\rangle \otimes |k\rangle$: Produto tensorial dos vetores $|j\rangle$ e $|k\rangle$.

$j \oplus k$: Soma binária de j e k.

$O(p(n))$: Classe de complexidade das funções limitadas superiormente por $p(n)$.

poli(n) : Polinômio na indeterminada n.

$\lceil N \rceil$: Menor número inteiro que seja maior que, ou igual a, N.

log : Logaritmo de base 2.

$a \mid b$: a divide b.

$a \nmid b$: a não divide b.

Capítulo 1

Introdução

A Computação Quântica é uma área de pesquisa nova, que está em ascensão, e que utiliza elementos de várias outras áreas do conhecimento, como Matemática, Física e Ciência da Computação. Um computador quântico é um dispositivo de computação que faz uso direto dos fenômenos da Mecânica Quântica, tais como sobreposição (ou superposição) de estados e emaranhamento, para realizar operações sobre dados.

O início da computação quântica deu-se nos anos 80 com os trabalhos de Benioff (1980) e Feynman (1982). Feynman foi o primeiro a propor a utilização de fenômenos quânticos para executar rotinas computacionais. Ele mostrou que um computador tradicional levaria um tempo extremamente longo para simular um simples experimento de física quântica. Isso deve ao fato de que a dimensão do espaço de Hilbert associado ao sistema cresce exponencialmente em função do número de partículas acrescentadas ao mesmo. Por outro lado, sistemas quânticos podem executar enormes quantidades de cálculos num curto espaço de tempo. É possível utilizar essa capacidade para se calcular algo útil?

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). Ele mostrou que da mesma forma que uma Máquina de Turing pode simular outra máquina de Turing eficientemente, um computador quântico universal é capaz de

simular o funcionamento de outro computador quântico com complexidade, no máximo, polinomial. Isso fez crescer a esperança de que um dispositivo simples seja capaz de executar muitos algoritmos quânticos diferentes. Posteriormente, o autor também generalizou o modelo de circuitos baseado em portas lógicas. Nesse novo contexto, operadores unitários tomaram o lugar das usuais portas lógicas AND, OR e NOT, Deutsch (1989).

O primeiro exemplo do uso de operações quânticas para realizar uma computação foi o algoritmo quântico conhecido como *algoritmo de Deutsch*, Deutsch (1985). O autor apresentou um algoritmo, utilizando apenas operações quânticas, capaz de resolver um determinado problema matemático de maneira mais eficiente que qualquer algoritmo clássico. Especificamente, Deutsch demonstrou que utilizando um computador quântico, basta fazer uma única chamada a uma função $f : \{0,1\} \to \{0,1\}$ para decidir se f é balanceada,[1] enquanto, em um computador clássico determinístico são necessárias duas chamadas. Mais tarde, Deutsch e Jozsa (1992) generalizaram o algoritmo de Deutsch para funções booleanas da forma $f : \{0,1\}^n \to \{0,1\}$.

É na década de 90 que a computação quântica ganha um forte impulso. Shor (1994, 1997), baseado no modelo de circuitos, apresentou um algoritmo quântico eficiente para cálculo de ordem de um número inteiro[2] . O autor mostrou que os problemas de fatoração de inteiros e de um caso particular do logaritmo discreto podem ser reduzidos ao problema de cálculo de ordem. Em outras palavras, Shor demonstrou que existem algoritmos de complexidade de tempo polinomial, que usam como sub-rotina o cálculo de ordem para fatorar um número composto e realizar cálculos de logaritmo discreto. Estes algoritmos são exponencialmente mais rápidos que qualquer algoritmo clássico conhecido. Eles permitem a quebra dos principais códigos de criptografia usados atualmente, como RSA, Diffie-Hellman e ElGamal, Koblitz (1998), caso um computador quântico de tamanho razoável esteja disponível.

[1] Uma função $f : \{0,1\} \to \{0,1\}$ é dita balanceada se $f(0) \neq f(1)$.

[2] A ordem de um inteiro y coprimo com N é o menor inteiro positivo r tal que $y^r \equiv 1 \bmod N$.

O algoritmo de Shor foi uma generalização do algoritmo de Simon (1994). Tal algoritmo resolve de forma eficiente e com probabilidade 1/2 o seguinte problema: dada uma função $f : \mathbb{Z}_2^n \to \mathbb{Z}_2^n$ tal que existe um elemento $s \in \mathbb{Z}_2^n$ satisfazendo

$$f(x) = f(y) \Leftrightarrow x = y \oplus s, \tag{1.1}$$

determinar o valor de s. Este problema é conhecido como o *problema de Simon*.

Por exemplo, para $n = 3$ e $s = 110$, a função a seguir é um exemplo de uma função que satisfaz a propriedade requerida pelo problema de Simon:

x	f(x)
000	101
001	010
010	000
011	110
100	000
101	110
110	101
111	010

Tabela 1.1: A função f satisfaz $f(x) = f(y) \Leftrightarrow x = y \oplus 110$, para todo $x, y \in \mathbb{Z}_2^3$.

Classicamente, o melhor algoritmo para o problema de Simon tem complexidade de tempo $\Omega(\sqrt{2^n})$. Quanticamente, o algoritmo de Simon resolve este problema fazendo apenas um número linear de consultas ao oráculo, isto é, $O(n)$.

Outro algoritmo quântico que também demonstra o poder da computação quântica é o algoritmo de Grover. Este algoritmo faz uma busca por um elemento marcado em uma lista não ordenada, Grover (1997); Lavor et al. (2003a). Apesar do algoritmo de Grover não apresentar um ganho exponencial, ele possui um ganho de eficiência quadrático sobre o melhor algoritmo clássico conhecido.

Da mesma forma que o número de algoritmos quânticos crescia, os esforços na tentativa de produzir o hardware do computador quântico também aumentavam. Técnicas como ressonância magnética nuclear (RMN) e armadilha de íons são usadas com sucesso no desenvolvimento de sistemas com 7 q-bits. Embora grande esforço esteja sendo feito nessa direção, a busca pela construção do hard-

ware quântico tem se mostrado cada vez mais, uma tarefa árdua e desafiadora.

No tocante a elaboração de algoritmos quânticos, nota-se que a maior parte dos algoritmos quânticos com ganho exponencial em relação aos seus equivalentes clássicos, tais como o algoritmo de Simon e o algoritmo de Shor, apresenta um determinado padrão em sua construção. Na realidade, os problemas que tais algoritmos resolvem podem ser vistos como instâncias de um problema mais geral, denominado Problema do Subgrupo Oculto (PSO). Podemos descrever o PSO da seguinte forma. Dado um grupo finito G e uma função f que é constante nas classes laterais de um subgrupo H de G e distinta em cada classe lateral, o problema do subgrupo oculto consiste em determinar um conjunto gerador para H, a partir de informações obtidas da função f. Dizemos que a função f oculta o subgrupo H em G, ou ainda que f separa as classes laterais de H em G. Assim, o subgrupo H é dito o subgrupo oculto em G por f.

Um algoritmo quântico para o PSO é dito eficiente (ou roda em tempo polinomial), quando a complexidade computacional do algoritmo é polilogaritmo na ordem do grupo, isto é, $O(\text{poli}(\log|G|))$. Para grupos finitos abelianos, o PSO pode ser resolvido eficientemente em um computador quântico. A solução é uma generalização do algoritmo de Shor, para fatoração de números inteiros e cálculo de logaritmo discreto, veja Kitaev (1995); Jozsa (2001); Lomont (2004). A principal ferramenta usada pelo algoritmo para o PSO abeliano é a transformada de Fourier em grupos.

A transformada de Fourier em grupos foi desenvolvida na década de 90 por Maslen e Rockmore (1997). A descrição matemática é dada em termos das representações irredutíveis da Teoria da Representação de Grupos Finitos, e é bem mais complexa que a transformada de Fourier de funções de várias variáveis complexas.

É natural perguntar se computadores quânticos podem resolver eficientemente o PSO em grupos arbitrários. Esta questão tem sido discutida regularmente pela comunidade científica devido à importantes aplicações, como por exemplo, no problema de isomorfismo de grafos, onde o grupo em questão é o grupo simétrico,

veja Ettinger et al. (2004); Beals (1997); Ahn (2002); Dalcumune (2008). Outro problema que vem ganhando destaque, principalmente por suas aplicações, é o PSO no grupo diedral, Kuperberg (2005). Regev (2004c) mostrou que uma solução eficiente do PSO no grupo Diedral implica um algoritmo eficiente para o problema de determinar o menor vetor em um reticulado, ou pelo menos para uma classe de reticulados para o qual nenhum algoritmo clássico eficiente é conhecido. Infelizmente, esses dois casos do PSO continuam em aberto, mostrando serem problemas bem desafiadores.

Embora não exista um algoritmo quântico eficiente (nem clássico) para o PSO sobre grupos arbitrários, alguns sucessos foram alcançados para algumas classes particulares de grupos, como podemos ver em Puschel et al. (1999); Hallgren et al. (2000); Grigni et al. (2004); Gavinsky (2004); Friedl et al. (2003); Ivanyos et al. (2003a); Moore et al. (2004); Inui e Le Gall (2007); Chi et al. (2006); Cosme e Portugal (2007a); Cosme (2008); Bacon et al. (2005); Radhakrishnan et al. (2005); Bacon (2007); Krovi e Rötteler (2008); Ivanyos et al. (2007a,b).

Nesta tese de doutorado apresentamos nossa contribuição no que diz respeito ao incremento do número de grupos onde o PSO pode ser resolvido eficientemente por um computador quântico. Apresentamos duas classes de algoritmos quânticos para o PSO, uma subexponencial[3] e outra polinomial. Resolvemos o PSO sobre 2-grupos de ordem 2^{n+1} que possuem subgrupos cíclicos de ordem 2^n e sobre grupos da forma $\mathbb{Z}_p \rtimes \mathbb{Z}_{q^s}$, onde p e q são números primos ímpares distintos e s um inteiro positivo qualquer. Em ambos os casos os algoritmos possuem complexidade subexponencial em relação aos dados de entrada do algoritmo. Mostramos também que o PSO pode ser resolvido eficientemente sobre grupos da forma $\mathbb{Z}_N^m \rtimes \mathbb{Z}_p$, onde N, m são inteiros positivos, N com uma fatoração especial e p primo ímpar. Mostramos que o grupo $\mathbb{Z}_N^m \rtimes \mathbb{Z}_p$ pertence a família dos grupos nilpotentes de classe 2, logo pode ser resolvido eficientemente utilizando as técnicas apresentadas

[3] Seja G um grupo finito e denotamos por $|G|$ o número de elementos do grupo. Dizemos que um algoritmo quântico para o PSO tem complexidade subexponencial, se o tempo de execução do algoritmo é $2^{O(\sqrt{\log |G|})}$.

em Ivanyos et al. (2007b). Por fim, apresentamos o resultado principal da tese, um algoritmo quântico eficiente para uma classe de produtos semidiretos de grupos da forma $\mathbb{Z}_p \rtimes \mathbb{Z}_{q^s}$, onde p e q são números primos ímpares distintos com $q \mid p-1$ e $p/q = \text{poli}(\log p)$.

A tese está organizada como segue. No Capítulo 2, apresentamos um apanhado histórico do PSO através de uma revisão bibliográfica. Definimos o PSO e tratamos o formalismo quântico que envolve o problema, analisando os casos abeliano e não abeliano.

No Capítulo 3, apresentamos algoritmos quânticos para o PSO sobre certos 2-grupos. Reunindo as idéias apresentadas em Kuperberg (2005), para o PSO no grupo diedral, com o conhecimento da estrutura dos subgrupos, exibimos um algoritmo quântico que resolve o PSO sobre esta classe de grupos em tempo subexponencial.

O Capítulo 4 inicia com uma breve revisão de alguns conceitos importantes sobre produtos semidiretos de grupos, homomorfismo de grupos e grupos de automorfismos. Mostramos que existe um algoritmo quântico em tempo polinomial para o PSO sobre o produto semidireto de grupos $\mathbb{Z}_N^m \rtimes_\phi \mathbb{Z}_p$, onde p é um número primo ímpar, m, N inteiros positivos, e N fatorado como $N = p_1^{r_1}...p_n^{r_n}$, com $1 \leq r_1 \leq \ldots \leq r_n$ onde $p \nmid p_i^k - 1$ para todo $i = 1, \ldots, n$ e $k = 1, \ldots, m$.

No Capítulo 5, estudamos os grupos metacíclicos[4] $\mathbb{Z}_p \rtimes \mathbb{Z}_{q^s}$. Apresentamos, no Teorema 5.2.2, a classificação dos subgrupos do grupo abordado. Esta classificação é fundamental na solução do PSO, pois, permite reduzir o PSO sobre $\mathbb{Z}_p \rtimes \mathbb{Z}_{q^s}$ ao problema de encontrar subgrupos cíclicos. No Capítulo 6, apresentamos nossos resultados principais. Exibimos um algoritmo quântico para o PSO no grupo em estudo, com complexidade de tempo $2^{O(\sqrt{\log p})}$. Esta classe de complexidade é subexponencial, mostrando ser melhor que qualquer algoritmo clássico para o mesmo fim, cuja classe de complexidade é $\Omega(\sqrt{p})$. Finalmente, apresentamos nosso resultado mais importante, um algoritmo quântico eficiente para o PSO so-

[4] Um grupo G é dito metacíclico se ele possui um subgrupo cíclico normal H tal que o grupo quociente G/H é também cíclico.

bre o grupo $\mathbb{Z}_p \rtimes \mathbb{Z}_{q^s}$, com $p/q = \text{poli}(\log p)$, onde p, q são números primos distintos ímpares e s um inteiro positivo qualquer.

Finalmente, no Capítulo 7, coligimos as conclusões obtidas neste trabalho e fazemos alguns apontamentos da solução do PSO em classes de produtos semidiretos de grupos mais gerais.

No Apêndice A, apresentamos uma breve revisão de alguns conceitos fundamentais sobre Teoria de Grupos e Teoria da Representação. No Apêndice B, apresentamos o algoritmo quântico que decompõe grupos abelianos em uma soma direta de grupos cíclicos com ordens potências de números primos. Este algoritmo é peça fundamental na solução do PSO abeliano, apresentado no Capítulo 2. Entretanto, gostaríamos de chamar à atenção do leitor ao fato de que a não leitura deste apêndice não implica no entendimento do algoritmo para o PSO abeliano e também no entendimento dos demais capítulos da tese. O motivo pelo qual inserimos tal apêndice é que acreditamos que a versão aqui apresentada é mais didática e compreensível do que a versão original descrita em Cheung e Mosca (2001). Finalmente, no Apêndice C apresentamos um apanhado geral sobre Computação Quântica.

Capítulo 2

O Problema do Subgrupo Oculto

Vários problemas em computação quântica podem ser descritos em termos da Teoria de Grupos Finitos. A teoria de grupos fornece uma estrutura simples para vários algoritmos quânticos, tornando mais fácil a tarefa de compreender a razão pela qual, em certas situações, os algoritmos quânticos são mais eficientes do que os melhores algoritmos clássicos conhecidos.

Um dos problemas mais importantes em teoria de grupos com vista ao desenvolvimento de algoritmos quânticos, é o chamado, Problema do Subgrupo Oculto (PSO). Este problema pode ser definido da seguinte forma.

Definição 2.0.1 Dado um grupo finito G e uma função f que é constante nas classes laterais de um subgrupo H de G e distinta em cada classe lateral, determinar um conjunto gerador para H, a partir de informações obtidas da função f. O problema de determinar H chama-se o *Problema do Subgrupo Oculto (PSO).*

Dizemos que a função f oculta o subgrupo H em G, ou ainda que f separa as classes laterais de H em G. Assim, o subgrupo H é dito o subgrupo oculto em G por f.

Um algoritmo ingênuo para o PSO em qualquer grupo finito G, consiste em chamar a função separadora de classes laterais várias vezes, cada vez, calculando $f(g)$ e verificando se $f(g) = f(e)$, para todo $g \in G$. Sempre que encontramos um elemento g com a propriedade $f(g) = f(e)$, nós acrescentamos este elemento ao

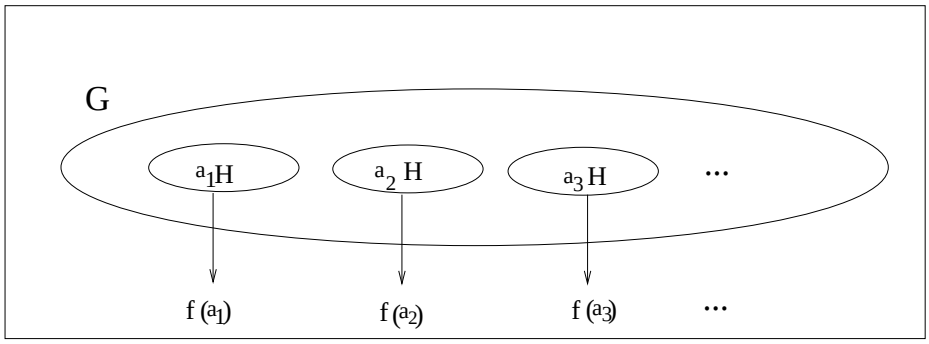


Figura 2.1: A função f é constante nas classes laterais de H e distinta em cada classe lateral.

conjunto H. Assim, após $|G|$ chamadas à função f seremos capazes de determinar o subgrupo H. Claramente este algoritmo é ineficiente, e sua complexidade é $O(|G|)$.

Definição 2.0.2 Um algoritmo quântico para o PSO é dito eficiente, quando a complexidade computacional do algoritmo é polilogaritmo na ordem do grupo, isto é, $O(\text{poli}(\log|G|))$.

São exemplos de algoritmos quânticos eficientes para o PSO, o algoritmo de Simon (1994) e o algoritmo de Shor (1997) para fatoração de números inteiros e cálculo de logaritmo discreto. No problema de Simon, temos $G = \mathbb{Z}_2^n$, com a promessa de que existe um elemento $y \in \mathbb{Z}_2^n$ tal que $f(x) = f(x+y)$ para todo $x \in \mathbb{Z}_2^n$; neste caso, o subgrupo oculto é dado por $H = \{0, y\}$, onde y é o parâmetro a ser determinado. No algoritmo de Shor, $G = \mathbb{Z}_N$, onde N é o número que desejamos fatorar, f é dada por $f(x) = y^x \bmod N$, com $y \in \mathbb{Z}_N^*$ satisfazendo $y^r \equiv 1 \bmod N$. Neste caso, H é o subgrupo de $\mathbb{Z}_N$ gerado pelo elemento r.

Observamos que em ambos os algoritmos de Shor e Simon os grupos em questão são abelianos. Como veremos na Seção 2.2, o PSO pode ser resolvido eficientemente por um computador quântico quando G é abeliano (veja também Høyer (1999)). Esta solução tem como principal ferramenta a transformada de Fourier em grupos além de um fato importante que vem da teoria de grupos que diz que qualquer grupo finito abeliano pode ser decomposto como uma soma direta de subgrupos cíclicos. Não é conhecido na literatura algoritmo clássico eficiente para decompor grupos abelianos, no entanto, Cheung e Mosca (2001) descobriram um

algoritmo quântico que faz essa decomposição em tempo polinomial. Para uma descrição mais detalhada do algoritmo para decompor grupos abelianos veja o Apêndice B. Veja também a referência Portugal et al. (2006).

Infelizmente, não é conhecida nenhuma solução geral para o caso de grupos não abelianos. Uma solução eficiente para o PSO em grupos arbitrários tem sido um tópico bastante estudado na última década devido à importantes aplicações, como no problema de isomorfismo de grafos.

Sejam $G_1 = (V_1, E_1)$ e $G_2 = (V_2, E_2)$ dois grafos, onde V_i e E_i denotam o conjunto de vértices e arestas, respectivamente, para todo $i = 1, 2$. Dizemos que G_1 e G_2 são isomorfos se existe uma permutação τ tal que $\tau G_1 = G_2$, ou seja, $(\tau(u), \tau(v)) \in E_2 \Leftrightarrow (u, v) \in E_1$. Neste caso, escrevemos $G_1 \simeq G_2$, e τ é chamado um isomorfismo de grafos entre G_1 e G_2. Então o problema de isomorfismo de grafos é o seguinte:

Definição 2.0.3 (Problema de Isomorfismo de Grafos) Dados dois grafos G_1 e G_2, com o mesmo número de vértices, determinar se G_1 e G_2 são isomorfos.

Um algoritmo eficiente para o PSO no grupo simétrico[1] implica um algoritmo eficiente para o problema de isomorfismo de grafos, Ettinger et al. (2004); Beals (1997); Ahn (2002); Dalcumune (2008).

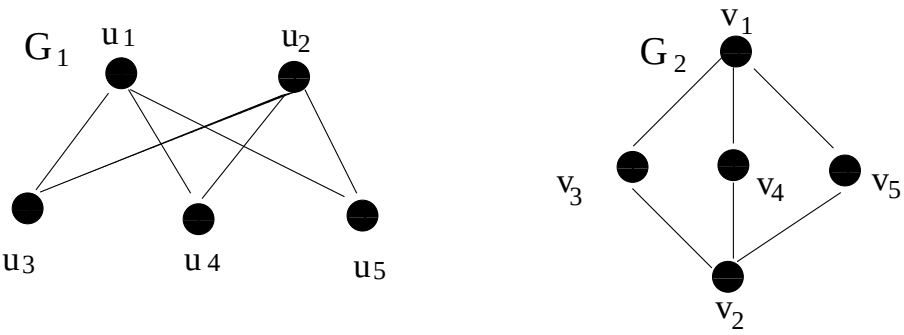


Figura 2.2: Os grafos G_1 e G_2 são isomorfos pois a função $\tau : G_1 \to G_2$ definida por $\tau(u_i) = v_i$, para todo $i = 1, \ldots, 5$ é um isomorfismo.

Outro problema importante é o PSO no grupo diedral, Kuperberg (2005). O grupo diedral, denotado por D_n, é o grupo formado pelas simetrias (rotações

[1] O grupo simétrico é o grupo das permutações de n elementos, e denotado por S_n.

e reflexões) de um polígono regular de n vértices. Uma solução eficiente para o PSO no grupo diedral implica um algoritmo eficiente para o Problema do Menor Vetor em um Reticulado[2] , Regev (2004c,a,b). Este problema possui aplicações importantes na área de criptografia, Ajtai (1996); Ajtai e Dwork (1997); Ajtai (1998).

Nas Seções 2.1 e 2.2 discutimos o problema do subgrupo oculto abeliano. Exibimos a transformada de Fourier em grupos e mostramos a sua importância na solução do PSO abeliano. Na Seção 2.3, apresentamos a transformada de Fourier em grupos não abelianos e discutimos a dificuldade no avanço de novos algoritmos quânticos eficientes para o PSO não abeliano.

2.1 Representações Irredutíveis de Grupos Abelianos

A principal ferramenta usada por algoritmos quânticos para o PSO é a transformada de Fourier em grupos. A transformada de Fourier em grupos foi desenvolvida na década de 90 com os trabalhos de Maslen e 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. Para uma breve revisão sobre Teoria da Representação veja o Apêndice A.2. Um estudo mais detalhado pode ser encontrado nas referências Serre (1997); Hamermesh (1962); Reiner e Curtis (1962); Gonçalves (2005).

O problema de achar representações irredutíveis para grupos abelianos é bastante simples. De fato, seja G um grupo abeliano, então não é difícil mostrar que cada classe de conjugação de G possui um único elemento[3] . Assim, o número de classes de conjugação em G é igual a ordem do grupo G. Segue dos Teoremas A.2.1 e A.2.5 (ver Apêndice A.2) que as representações irredutíveis de G são todas

[2] Um reticulado n-dimensional é um conjunto de vetores $R = \{\sum_{i=1}^{n} a_i b_i; a_i \in \mathbb{Z}\}$, onde $b_1, \ldots, b_n \in \mathbb{R}^m$ é um conjunto de vetores L.I., chamado uma base do reticulado, Khot (2005). O Problema do Menor Vetor em um Reticulado consiste em, dado um reticulado R, determinar o menor vetor pertencente a R.

[3] Veja o Apêndice A para uma rápida revisão sobre alguns tópicos da teoria de grupos.

unidimensionais. Então quando G é abeliano, as entradas da matriz representação coincidem com o caráteres de G e daí temos uma simples multiplicação de números complexos.

Um caráter de um elemento $g \in G$ é um homomorfismo $g \mapsto \chi(g) \in \mathbb{C}^*$. Note que $\chi(e) = 1$ e como G é finito, 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[4] . Se G for cíclico então existe um elemento $g \in G$ tal que $G = \langle g \rangle$. Assim $g^{|G|} = 1$, e então

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

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

Segue do Teorema Fundamental para grupos abelianos finitos (Teorema A.1.3) que G é isomorfo a uma soma direta de grupos cíclicos, de ordens $t_1, t_2, \ldots, t_N$,

$$G \simeq \mathbb{Z}_{t_1} \oplus \mathbb{Z}_{t_2} \oplus \ldots \oplus \mathbb{Z}_{t_N}. \tag{2.1}$$

Por simplicidade assumimos que G é igual a esta soma direta. Os elementos de G são n-uplas $(g_1, \ldots, g_n)$, onde cada $g_j \in \mathbb{Z}_{t_j}$. Pensando em G como um grupo aditivo, o elemento identidade de G será denotado por $e = (0, 0, \ldots, 0)$. Assim, para cada $g = (g_1, \ldots, g_n) \in G$ definimos o caráter do elemento g como sendo

$$\chi(g) = \chi(\sum_{j=1}^{N} g_j\beta_j) = \prod_{j=1}^{N} \chi(g_j\beta_j) = \prod_{j=1}^{N} \chi(\beta_j)^{g_j}, \tag{2.2}$$

onde $\beta_j \in G$ possui 1 na j-ésima entrada e 0 nas demais entradas.

Agora, note que para cada $j = 1, \ldots, n$, a ordem de β_j é t_j. Assim,

$$\chi(\beta_j) = \omega_{t_j}^{h_j}, \tag{2.3}$$

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

onde ω_{t_j} é a t_j-ésima raíz primitiva da unidade, $\omega_{t_j} = e^{\frac{2\pi i}{t_j}}$, com $h_j \in \mathbb{Z}_{t_j}$. Logo, podemos definir os caráteres de G fazendo corresponder cada elemento $g \in G$, um número complexo

$$\chi_g(h) = \prod_{j=1}^{n} \omega_{t_j}^{g_j h_j}, \ \forall\ h \in G. \tag{2.4}$$

Verifica-se facilmente que $\chi_g : G \to \mathbb{C}^*$ definido por (2.4) é de fato um homomorfismo de grupos.

Lema 2.1.1 Para quaisquer $g, h \in G$, $\chi_g(h) = \chi_h(g)$.

Demonstração: Trivial, pois G é abeliano.

■

Os caráteres de um grupo finito abeliano G podem ser organizados em uma tabela, como mostra a Tabela 2.1. As colunas na tabela 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	$\cdots$	$c_{\lvert G\rvert}$
χ_1	$\chi_1(c_1)$	$\chi_1(c_2)$	$\cdots$	$\chi_1(c_{\lvert G\rvert})$
χ_2	$\chi_2(c_1)$	$\chi_2(c_1)$	$\cdots$	$\chi_2(c_{\lvert G\rvert})$
$\vdots$	$\vdots$	$\vdots$	$\cdots$	$\vdots$
$\chi_{\lvert G\rvert}$	$\chi_{\lvert G\rvert}(c_1)$	$\chi_{\lvert G\rvert}(c_2)$	$\cdots$	$\chi_{\lvert G\rvert}(c_{\lvert G\rvert})$

Tabela 2.1: Tabela de caráteres de um grupo finito abeliano G.

2.2 O Problema do Subgrupo Oculto Abeliano

Sejam G um grupo finito (não necessariamente abeliano) e X um conjunto finito tal como na Definição 2.0.1. Definimos B_n e B_m como sendo os conjuntos de todas as palavras binárias de n e m dígitos, respectivamente, onde $n = \lceil \log |G| \rceil$ e $m = \lceil \log |X| \rceil$. Para cada elemento do grupo G associamos uma palavra binária em B_n. Analogamente, para cada elemento em X associamos uma palavra binária em B_m. Como exemplo de tal codificação, considere o grupo $\mathbb{Z}_N$, o grupo aditivo

dos inteiros módulo N. Para cada $g \in \mathbb{Z}_N$ associamos uma palavra binária que representa o inteiro g na base 2.

Uma vez estabelecida à associação entre G e B_n (analogamente, entre X e B_m), sejam $\mathcal{H}_n$ e $\mathcal{H}_m$ espaços de Hilbert gerados por bases ortonormais cujos elementos são indexados pelos elementos de B_n e B_m, respectivamente. O espaço de estados do computador quântico será $B_n \otimes B_m$. Note que, através da associação feita entre os elementos de G e X com elementos de B_n e B_m, podemos considerar os subespaços

$$\mathcal{H}_G = \langle |g\rangle \, ; g \in G\rangle \quad \text{e} \quad \mathcal{H}_X = \langle |z\rangle \, ; z \in X\rangle \, . \tag{2.5}$$

Se $|G| < 2^n$ e/ou $|X| < 2^m$, então o subespaço $\mathcal{H} = \mathcal{H}_G \otimes \mathcal{H}_X$ é um subespaço próprio de $B_n \otimes B_m$. Neste caso, ignoraremos o restante do espaço aplicando o operador identidade nos elementos que não pertencem ao subespaço $\mathcal{H}$[5] .

Agora que sabemos como os elementos do grupo são representados no computador quântico, vamos definir a principal ferramenta utilizada por algoritmos quânticos com ganho exponencial, a saber, a transformada de Fourier em grupos abelianos.

Seja G um grupo finito abeliano e seja F_G uma matriz quadrada de dimensão $|G| \times |G|$. As colunas de F_G são os vetores $|v_g\rangle$ tais que

$$|v_g\rangle = \frac{1}{\sqrt{|G|}} \begin{pmatrix} \chi_g(h_1) \\ \chi_g(h_2) \\ \vdots \\ \chi_g(h_{|G|}) \end{pmatrix} \tag{2.6}$$

onde $g \in G$, e $h_1, \ldots, h_{|G|}$ é uma lista completa dos elementos de G .

Segue das relações de ortogonalidade de caráteres (Teorema A.2.3) que a matriz F_G é unitária. Dizemos então que F_G é a *transformada de Fourier* em

[5] Note que se $|G| < 2^n$ então alguns vetores da base computacional não tem correspondência com os elementos do grupo de forma que um subespaço do espaço de Hilbert não é utilizado. Nesse subespaço assumimos que todos os operadores tem atuação trivial, isto é, atuam como operador identidade.

grupos abelianos. F_G também pode ser definida por sua atuação nos vetores da base como:

$$F_G |g\rangle = \frac{1}{\sqrt{|G|}} \sum_{h \in G} \chi_g(h) |h\rangle . \tag{2.7}$$

Definição 2.2.1 (Subgrupo Ortogonal) Para qualquer subgrupo H de um grupo finito abeliano G, definimos o subgrupo ortogonal $H^\perp$, como

$$H^\perp = \{g \in G \mid \chi_g(h) = 1 \, \forall \, h \in H\}. \tag{2.8}$$

Como G é finito, $H^\perp$ é um subgrupo de G, se e somente se, a operação do grupo é fechada em $H^\perp$. Assim, se $a, b \in H^\perp$ então para qualquer $h \in H$ nós temos $\chi_h(ab) = \chi_h(a)\chi_h(b) = 1$, isto é, $ab \in H^\perp$, logo $H^\perp \leq G$.

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

Teorema 2.2.1 Temos $H^\perp \simeq G/H$, em particular $|H^\perp| = |G|/|H|$.

Demonstração: Ver Lomont (2004).

■

Lema 2.2.1 Para qualquer classe lateral H_i de H em G, temos

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

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

Demonstração: Aplicando a definição de F_G e invertendo a ordem da soma, obtemos

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

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

$$\begin{aligned}\frac{1}{\sqrt{|G||H|}}\sum_{h\in G}\sum_{g\in H_i}\chi_g(h)\,|h\rangle &= \frac{|H|}{\sqrt{|G||H|}}\sum_{h\in H^{\perp}}\chi_h(g_i)\,|h\rangle\\ &= \sqrt{\frac{|H|}{|G|}}\sum_{h\in H^{\perp}}\chi_h(g_i)\,|h\rangle\\ &= \frac{1}{\sqrt{|H^{\perp}|}}\sum_{h\in H^{\perp}}\chi_h(g_i)\,|h\rangle\,. \qquad (2.9)\end{aligned}$$

■

A seguir, apresentamos um algoritmo quântico eficiente para o PSO abeliano, chamado *Método Padrão de Solução*. A descrição do algoritmo é baseada nas referências Lomont (2004); Damgard (2004); Gonçalves (2005).

Antes, faremos algumas suposições necessárias à solução do PSO em G. Suponhamos que temos a nossa disposição dois registradores, um registrador com $n = \lceil \log|G| \rceil$ q-bits e outro com $m = \lceil \log|X| \rceil$ q-bits. Assumimos também que a operação dos elementos do grupo é feita de forma eficiente, ou seja, fixado $|g\rangle \in \mathcal{H}_G$, existe um operador unitário U_g, tal que

$$U_g\,|h\rangle = |gh\rangle\,, \qquad (2.10)$$

para todo $|h\rangle \in \mathcal{H}_G$. Por fim, assumimos a existência de um operador unitário V_f,

tal que, $|g\rangle \in \mathcal{H}_G$, $|z\rangle \in \mathcal{H}_X$, temos

$$V_f |g\rangle |z\rangle = |g\rangle |z \oplus f(g)\rangle , \tag{2.11}$$

onde $\oplus$ denota a soma binária em B_m, e f é a função separadora de classes laterais.

O algoritmo é o seguinte:

(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 o operador $F_G \otimes I$. O estado resultante é

$$|\Psi_0\rangle = \frac{1}{\sqrt{|G|}} \sum_{g \in G} |g\rangle |0^m\rangle . \tag{2.12}$$

(2) Aplique o operador unitário V_f ao estado $|\Psi_0\rangle$ e obtenha

$$|\Psi_1\rangle = \frac{1}{\sqrt{|G|}} \sum_{g \in G} |g\rangle |f(g)\rangle . \tag{2.13}$$

Este é um estado quântico notável. Como V_f é linear, ele atua em todos os estados $|g\rangle |0^m\rangle$, para todo $g \in G$, gerando todos os valores $f(g)$ simultaneamente. Este fenômeno é conhecido como *paralelismo quântico*.

(3) Meça o segundo registrador do estado $|\Psi_1\rangle$. Como a função f é constante nas classes laterais do subgrupo H, o estado após a medida fica

$$|\Psi_2\rangle = \frac{1}{\sqrt{|H|}} \sum_{g_0 \in H_i} |g_0\rangle |f(g_0)\rangle , \tag{2.14}$$

onde H_i é alguma classe lateral de H em G. Observe que a constante $\frac{1}{\sqrt{|G|}}$ foi renormalizada para $\frac{1}{\sqrt{|H|}}$. Isso acontece porque após a medida sobram apenas os elementos cuja imagem é $f(g_0)$.

(4) Aplique F_G ao primeiro registrador do estado $|\Psi_2\rangle$. Pelo Lema 2.2.1, o

estado resultante é uma superposição sobre os elementos em $H^{\perp}$, i.e.,

$$|\Psi_3\rangle = \frac{1}{\sqrt{|H^{\perp}|}} \sum_{h \in H^{\perp}} \chi_h(g_i) \, |h\rangle \, . \tag{2.15}$$

(5) Agora, meça o primeiro registrador do estado $|\Psi_3\rangle$. A medida produz um elemento randômico em $H^{\perp}$.

(6) Segue do Teorema A.1.1, que repetindo os passos (1) - (5), $O(\log |G|)$ vezes, obtemos um conjunto gerador para $H^{\perp}$. Usando as relações entre H e $H^{\perp}$ é possível achar um conjunto gerador para H com alta probabilidade, Damgard (2004); Gonçalves (2005).

2.3 O Problema do Subgrupo Oculto Não Abeliano

O problema do subgrupo oculto (PSO) é atualmente um dos maiores desafios para a computação quântica. Após a descoberta do algoritmo de Shor (1994) para fatoração e cálculo de logaritmo discreto (que resolve basicamente o PSO em grupos abelianos, Kitaev (1995)), tem-se focado a atenção na seguinte questão: quais problemas computacionais podem ser resolvidos eficientemente utilizando computadores quânticos? Em particular, gostaríamos de saber para quais classes de grupos não abelianos o PSO admite uma solução eficiente.

O ponto chave da maioria dos algoritmos quânticos conhecidos para o PSO é a transformada de Fourier em grupos. Em grupos genéricos, ela é definida em termos das representações irredutíveis da Teoria da Representação de Grupos Finitos. Para qualquer grupo finito G, denotamos por $\widehat{G}$, o conjunto de todas as representações irredutíveis de G. Seja $\mathcal{H}_G$ um espaço de Hilbert munido de duas bases ortonormais, uma base indexada pelos elementos de G (denotada por $|g\rangle$ para todo $g \in G$) e a outra dada pelos coeficientes matriciais das representações irredutíveis de G (denotado por $|\rho, i, j\rangle$, onde $\rho \in \widehat{G}$, e $i, j = 1, \ldots, d_\rho$, onde d_ρ denota

a dimensão de ρ). A transformada de Fourier sobre G, escrevemos F_G, é

$$F_G \left|g\right\rangle = \sum_{\rho \in \widehat{G}} \sqrt{\frac{d_\rho}{|G|}} \sum_{i,j=1}^{d_\rho} \rho_{ij}(g) \left|\rho, i, j\right\rangle . \tag{2.16}$$

Uma descrição mais completa da transformada de Fourier quântica em grupos pode ser encontrada em Grigni et al. (2004); Gonçalves (2005).

É conhecido que uma solução eficiente do PSO no grupo simétrico implica um algoritmo eficiente para o problema de isomorfismo de grafos, Ettinger et al. (2004); Beals (1997); Ahn (2002). Não é conhecido nenhum algoritmo eficiente para o problema de isomorfismo de grafos, embora grande esforço tenha sido feito para resolver este problema, tanto classicamente, veja Köbler et al. (1993), quanto quanticamente, Hallgren et al. (2006); Moore e Russel (2006).

Adicionando ainda mais interesse na busca por novos algoritmos quânticos para o PSO não abeliano, Regev (2004a,c) mostrou que um algoritmo quântico eficiente para o PSO no grupo diedral resolve instâncias do problema de determinar o menor vetor em um reticulado.

O grupo diedral foi o primeiro grupo não abeliano para o qual o PSO foi estudado. Em parte, essa iniciativa deu-se pela simplicidade da estrutura de seus subgrupos e pelo grande número de subgrupos de ordem 2. O grupo diedral de ordem $2n$ é formado pelas rotações e reflexões do plano que preservam um polígono regular com n vértices. Algebricamente, ele pode ser representado como o produto semidireto de grupos $D_n = \mathbb{Z}_n \rtimes_\phi \mathbb{Z}_2$, onde o homomorfismo $\phi : \mathbb{Z}_2 \to \mathrm{Aut}(\mathbb{Z}_n)$ é tal que $\phi(b)(a) = (-1)^b a$ para todo $b \in \mathbb{Z}_2$ e $a \in \mathbb{Z}_n$, e $\mathrm{Aut}(\mathbb{Z}_n)$ denota o grupo de automorfismos de $\mathbb{Z}_n$. Para resolver o PSO sobre D_n, Ettinger e Høyer (2000) mostraram que é suficiente resolver o caso onde o subgrupo oculto possui ordem 2. Ao invés de olhar para D_n como um grupo não abeliano, os autores aplicam a transformada de Fourier abeliana ao produto direto de grupos $\mathbb{Z}_n \times \mathbb{Z}_2$, e com isso eles conseguem obter informações sobre o subgrupo oculto, fazendo $O(\log n)$ chamadas à função separadora de classes laterais . Entretanto, o pós-

processamento do algoritmo, que consiste em obter um conjunto de geradores para o subgrupo oculto a partir das informações obtidas pela função separadora de classes laterais, toma tempo exponencial. Isto torna o algoritmo de Ettinger e Høyer (2000) ineficiente.

Embora não seja conhecida nenhuma solução eficiente para o PSO diedral, Kuperberg (2005) descobriu um algoritmo quântico com complexidade $2^{O(\sqrt{\log n})}$. Posteriormente, Regev (2004a) apresentou uma versão melhorada do algoritmo de Kuperberg, onde o tempo de processamento do algoritmo é ainda subexponencial, mas a quantidade de memória necessária para o processamento é apenas polinomial em $\log n$. Recentemente, Alagic et al. (2006) descobriram um algoritmo quântico em tempo subexponencial para o PSO sobre certos produtos diretos de grupos. Ainda nesta direção, Gonçalves et al. (2009) apresentaram um algoritmo quântico com complexidade de tempo $2^{O(\sqrt{\log p})}$ para resolver PSO sobre grupos metacíclicos da forma $\mathbb{Z}_p \rtimes \mathbb{Z}_{q^s}$, onde p e q são primos ímpares distintos e s um inteiro positivo. A classe de complexidade $2^{O(\sqrt{\log p})}$ é subexponencial, mostrando ser melhor que qualquer algoritmo clássico para o mesmo fim, cuja classe de complexidade é $\Omega(\sqrt{p})$. Este algoritmo está descrito no Capítulo 5.

Alguns sucessos foram alcançados na busca por novos algoritmos quânticos para o PSO não abeliano. Por exemplo, Puschel et al. (1999) apresentaram um algoritmo quântico eficiente para o PSO sobre o produto wreath $\mathbb{Z}_2^n \wr \mathbb{Z}_2$. Mais tarde, Hallgren et al. (2000) mostraram que existe um algoritmo quântico eficiente para o PSO em qualquer grupo finito G, desde que a transformada de Fourier seja implementada eficientemente no grupo e que o subgrupo oculto H seja normal. Em particular eles resolveram o PSO sobre grupos Hamiltonianos[6] . Em seguida, Grigni et al. (2004) descobriram uma solução eficiente para o PSO em grupos que são "quase Abelianos", no sentido de que a interseção dos normalizadores de todos os subgrupos do grupo é grande. Mais tarde, este resultado foi estendido por Gavinsky (2004), que resolveu o PSO de forma eficiente sobre grupos "quase Hamiltonianos".[7]

[6] Um grupo G é dito Hamiltoniano se ele possui apenas subgrupos normais.

Continuando a busca por novos algoritmos quânticos, Friedl et al. (2003) mostraram como resolver eficientemente o PSO sobre o produto semidireto de grupos $\mathbb{Z}_{p^k}^n \rtimes \mathbb{Z}_2$, onde a potência p^k, p primo e k inteiro positivo, é um número fixo. Os autores também mostraram que o PSO pode ser resolvido eficientemente em grupos solúveis de expoente limitado e séries derivadas limitadas. Um algoritmo quântico eficiente para o PSO sobre grupos cuja ordem do subgrupo de comutadores é pequena, isto é, $|G'| = \log|G|$, é apresentado por Ivanyos et al. (2003a).

Moore et al. (2004) deram um algoritmo quântico eficiente, baseado na transformada de Fourier não abeliana, para resolver o PSO sobre os grupos q-edrais $\mathbb{Z}_p \rtimes \mathbb{Z}_q$, onde p e q são primos distintos tais que $p/q = \text{poli}(\log p)$. Mais recentemente, Gonçalves et al. (2009) apresentaram um algoritmo quântico eficiente para o PSO sobre certos grupos metacíclicos da forma $\mathbb{Z}_p \rtimes \mathbb{Z}_{q^s}$, com $p/q = \text{poli}(\log p)$, onde p, q são números primos distintos ímpares e s um inteiro positivo qualquer. A partir da classificação dos subgrupos de $\mathbb{Z}_p \rtimes \mathbb{Z}_{q^s}$, os autores mostraram que o PSO se reduz ao problema de encontrar subgrupos cíclicos da forma $\langle x^a y\rangle$, onde $a \in \mathbb{Z}_p$, $x = (1,0)$ e $y = (0,1)$. Existem na verdade $\Omega(p)$ subgrupos da forma $\langle x^a y\rangle$. Isto implica que uma busca exaustiva pelo valor a é ineficiente. Por outro lado, preparando o computador quântico numa superposição de todos os elementos do grupo e em seguida aplicando a transformada de Fourier (abeliana), é possível construir um estado quântico $|\Psi\rangle$ tal que a *fidelidade*[8] quântica entre $|\Psi\rangle$ e o estado

$$|\tilde{a}\rangle = \frac{1}{\sqrt{p}} \sum_{j=0}^{p-1} \omega_p^{ja} |j\rangle , \tag{2.17}$$

onde $\omega_p = \exp(2\pi i/p)$, é $\sqrt{\frac{q}{p}}$. Medindo o estado $|\Psi\rangle$ na base computacional,

[7] Para qualquer subgrupo H de G, $\mathcal{N}(H) = \{g \in G; g^{-1}Hg = H\}$ é o normalizador de H. Definimos M_G como sendo a interseção de todos os normalizadores: $M_G = \bigcap_{H \leq G} \mathcal{N}(H)$. Definimos $k_G = [G : M_G]$ e $n = \log|G|$. Então G é:

- Quase abeliano (Grigni et al. (2004)) se $k_G \in \exp(O(\log^{1/2} n))$;
- Quase Hamiltoniano (Gavinsky (2004)) se $k_G \in \text{poli}(n)$.

[8] Na Teoria da Informação Quântica, *fidelidade* é uma medida que diz quão próximos são dois estados quânticos.

é possível encontrar o valor de a com probabilidade q/p. Rodando o algoritmo $O(\text{poli}(\log p))$ vezes, obtém-se o valor de a com probabilidade $1/2$. Isto generaliza um resultado de Moore et al. (2004) para grupos q-edrais, que requer $s = 1$. Este algoritmo está descrito no Capítulo 6.

Uma forma alternativa de tratar o PSO não abeliano, é investigar a estrutura de todos os subgrupos de um dado grupo, e então determinar um algoritmo quântico que se aplique a estes subgrupos utilizando a transformada de Fourier abeliana. Esta estratégia foi primeiramente adotada por Ettinger e Høyer (2000), que mostrou que o PSO no grupo diedral pode ser reduzido ao problema de encontrar subgrupos de ordem 2. Mais tarde, também fazendo uso da estrutura dos subgrupos, Inui e Le Gall (2007) apresentaram um algoritmo quântico eficiente para o PSO em grupos da forma $\mathbb{Z}_{p^r} \rtimes \mathbb{Z}_p$ com p primo. No mesmo trabalho, os autores estenderam seu resultado para grupos da forma $\mathbb{Z}_{p^r}^m \rtimes \mathbb{Z}_p$, onde m é qualquer inteiro positivo.

Baseado nos resultados de Inui e Le Gall (2007), Chi et al. (2006) apresentaram um algoritmo quântico eficiente para o PSO em $\mathbb{Z}_N \rtimes \mathbb{Z}_p$, onde N é fatorado como $N = p_1^{r_1} p_2^{r_2} \cdots p_n^{r_n}$ e p um primo ímpar que não divide cada $p_j - 1$. Seguindo esta direção, Cosme e Portugal (2007a) apresentaram um algoritmo quântico em tempo polinomial para o PSO sobre o produto semidireto $\mathbb{Z}_{p^r} \rtimes \mathbb{Z}_{p^s}$, com p um primo ímpar e r, s inteiros satisfazendo algumas restrições. Como consequência, os autores mostraram que é possível resolver eficientemente o PSO no grupo $\mathbb{Z}_N \rtimes \mathbb{Z}_{p^s}$, onde N é um inteiro positivo com uma fatoração especial (veja também Cosme e Portugal (2007b) e Cosme (2008)). Na mesma linha, Gonçalves et al. (2008) apresentaram um algoritmo quântico eficiente para o PSO no produto semidireto de grupos $\mathbb{Z}_N^m \rtimes \mathbb{Z}_p$, onde p é um número primo ímpar, m, N inteiros positivos, e N fatorado como $N = p_1^{r_1} ... p_n^{r_n}$, com $1 \leq r_1 \leq \ldots \leq r_n$ onde $p \nmid p_i^k - 1$ para todo $i = 1, \ldots, n$ e $k = 1, \ldots, m$. Este algoritmo está descrito no Capítulo 4.

Os métodos apresentados até aqui para solução do PSO fazem uso do Método Padrão de Solução (veja Seção 2.2). Em linhas gerais, o método consiste em aplicar

um operador unitário $V_f |g\rangle |z\rangle = |g\rangle |z \oplus f(g)\rangle$, onde $g \in G$ e $z \in X$ em uma superposição de todos os elementos do grupo, $\frac{1}{\sqrt{|G|}} \sum_{g \in G} |g, 0\rangle$. Esta aplicação produz um estado da forma $\frac{1}{\sqrt{|G|}} \sum_{g \in G} |g, f(g)\rangle$. Em seguida, um operador de medida é aplicado ao segundo registrador produzindo o estado $|gH\rangle := \frac{1}{\sqrt{|H|}} \sum_{h \in H} |gh\rangle$. Este estado é uma superposição uniforme sobre os elementos de uma classe lateral arbitrária do subgrupo oculto H. O desafio é determinar H a partir do estado $|gH\rangle$.

Quanta informação sobre o subgrupo oculto pode ser extraída do estado $|gH\rangle$? A forma mais comum de extrair informações clássicas de estados quânticos é através das medidas *POVM*, Nielsen e Chuang (2003)(Veja também o Apêndice C). Baseado nessas medidas, Bacon et al. (2005) encontraram um algoritmo quântico eficiente para o PSO sobre grupos da forma $A \rtimes \mathbb{Z}_p$, com A abeliano e p um número primo. O método utilizado pelos autores é fundamentalmente diferente daqueles apresentados até agora para o PSO: o método é baseado num tipo de medida emaranhada, chamada *pretty good measurement*. Enquanto o método padrão de solução usa uma medida projetiva no estado $|gH\rangle$ para obter informações sobre H, diferentemente, o método de Bacon et al. (2005), usa medidas POVM para identificar o subgrupo oculto a partir do estado $|gH\rangle^{\otimes k}$, onde k é um inteiro positivo. Os autores mostram que dado um POVM, é possível obter maior informação sobre o subgrupo oculto aplicando o POVM em k estados da forma $|gH\rangle$ de uma única vez, ao invés de aplicar o POVM em cada estado separadamente. Por exemplo, nenhuma medida que trata cada estado $|gH\rangle$ individualmente, é capaz de resolver eficientemente o PSO sobre o grupo S_n, Moore et al. (2005). Por outro lado, Hallgren et al. (2006) mostraram que utilizando medidas emaranhadas, é suficiente utilizar $k = O(n \log n)$ estados $|gH\rangle$, para obter informação suficiente para identificar o subgrupo oculto em S_n.

Duas questões surgem de forma bem natural. A primeira é, qual o menor valor de k necessário para identificar o subgrupo oculto H aplicando um POVM no estado $|gH\rangle^{\otimes k}$? A segunda questão diz respeito a implementação desses operadores

de medida, isto é, é sempre possível implementar esses POVMs eficientemente em um computador quântico? Ettinger et al. (2004) mostraram que é possível identificar o subgrupo oculto em qualquer grupo finito G aplicando um operador POVM no produto tensorial de estados $|gH\rangle^{\otimes k}$, onde $k = O(\log |G|)$. Infelizmente, não se sabe como implementar tal operador eficientemente em um computador quântico.

Em particular, considerando $k = 1$, Bacon et al. (2005) resolveram em tempo polinomial o PSO sobre grupos da forma $\mathbb{Z}_n \rtimes \mathbb{Z}_p$, para todo inteiro n e primo p tal que $n/p = \text{poli}(\log n)$, melhorando o resultado de Moore et al. (2004). Eles também apresentaram um algoritmo quântico eficiente para o PSO sobre o produto semidireto $\mathbb{Z}_p^r \rtimes \mathbb{Z}_p$, com r fixo e tomando $k = r$. Para o caso particular $r = 2$, os autores mostram que existe um algoritmo quântico eficiente que resolve PSO no grupo de Heisenberg, um problema cuja complexidade clássica é exponencial. Isto generaliza o resulto de Radhakrishnan et al. (2005).

Em um trabalho mais recente, Bacon (2007) mostrou que o PSO no grupo de Heisenberg também pode ser resolvido eficientemente utilizando uma nova estratégia, chamada *transformação de Clebsch-Gordan*. Mais tarde, também fazendo uso da transformação de Clebsch-Gordan, Krovi e Rötteler (2008) apresentaram um algoritmo quântico eficiente para o PSO sobre Weyl-Heisenberg grupos de ordem p^{2n+1}, com p primo e n inteiro positivo. Neste trabalho, os autores utilizam apenas $k = 2$ estados da forma $|gH\rangle$, mostrando ser melhor que um resultado em Ivanyos et al. (2007a), que requer no mínimo $k = 4$.

No trabalho de Ivanyos et al. (2007b), é apresentado um algoritmo quântico eficiente para o PSO sobre grupos nilpotentes de classe 2. Os autores utilizam a estrutura desses grupos para mostrar que o PSO nestas classes de grupos pode ser reduzido ao PSO abeliano. Isto generaliza o método apresentado em Ivanyos et al. (2007a), para o PSO em grupos extra-especiais. Para uma leitura mais detalhada sobre estes dois últimos problemas veja Fernandes (2008).

Esta revisão bibliográfica apesar de não cobrir todos os trabalhos realizados

nesta área, versa o que de mais importante e representativo tem sido feito até o momento para a solução do PSO. Entre os resultados mais expressivos, temos a existência de um algoritmo quântico eficiente para a solução do PSO em grupos abelianos arbitrários. O PSO abeliano foi uma generalização do algoritmo de Shor para fatoração de números inteiros e cálculo de logaritmo discreto, tendo como ponto chave o algoritmo padrão de solução. Este possui como um dos pontos principais a transformada de Fourier em grupos abelianos.

Também, nós apresentamos o PSO no contexto de grupos não abelianos e descrevemos a transformada de Fourier utilizando elementos da teoria da representação de grupos finitos. Surge então um grande desafio, a solução do PSO sobre grupos arbitrários. Apesar do problema no caso geral parecer bem mais complicado, alguns resultados parciais foram surgindo, dos quais muitos foram listados neste capítulo.

Discutimos problemas de enorme interesse prático, como o PSO no grupo S_n, que implica um algoritmo quântico eficiente para o problema de isomorfismo de grafos. Vimos também, que uma solução eficiente do PSO no grupo diedral implica uma solução eficiente para o problema de determinar o menor vetor em um reticulado. Estes dois problemas possuem implicações interessantes, como em problemas relacionados à biologia molecular e criptografia. Embora grande esforço tenha sido feito na tentativa de solucionar tais PSOs, os mesmos continuam em aberto e desafiando a comunidade científica.

Existem várias outras áreas onde algoritmos quânticos demonstram ser mais eficientes do que os seus equivalentes clássicos. Por exemplo, o algoritmo de busca de Grover (1997), que reduz a complexidade clássica da busca em uma lista não ordenada contendo N elementos, de $O(N)$ para $O(\sqrt{N})$, veja também Lavor et al. (2003a). Outro exemplo é o trabalho de Watrous (2001); neste trabalho o autor apresenta um algoritmo quântico eficiente para o cálculo de ordem de grupos solúveis. Como consequência, vários outros problemas em grupos solúveis, como teste de pertinência, teste de igualdade de subgrupos e teste de normalidade podem

ser resolvidos de forma eficiente em um computador quântico.

Por fim, referimo-nos aos algoritmos de busca baseados em caminhos aleatórios quânticos. Estes por sua vez têm demonstrado ter um ganho quadrático em relação aos seus equivalentes clássicos, Shenvi et al. (2003); Ambainis et al. (2005); Ambainis (2007).

Nesta tese de doutoramento trataremos apenas de algoritmos quânticos para o PSO não abeliano.

Capítulo 3

Algoritmos Quânticos para o PSO sobre 2-Grupos

Neste capítulo apresentamos algoritmos quânticos para o PSO sobre uma família de grupos não abelianos. Especificamente, estudamos 2-grupos[1] de ordem 2^{n+1} que possuem um subgrupo cíclico de ordem 2^n, para qualquer inteiro positivo n maior ou igual que 3.

O teorema a seguir nos diz que para qualquer inteiro positivo n maior ou igual que 3, existem exatamente quatro classes não isomorfas de grupos não abelianos de ordem 2^{n+1} que têm um subgrupo cíclico de ordem 2^n. Vamos ao teorema.

Teorema 3.0.1 Seja G um grupo tal que $|G| = 2^{n+1}$ onde $n \geq 3$ e tal que G possui um subgrupo cíclico maximal $\langle x \rangle$ (isto é, $|\langle x \rangle| = 2^n$). Então G é isomorfo a um dos seguintes grupos:

Classe 1. O grupo Q_{2^n} dos quatérnios generalizados:

$$Q_{2^n} = \left\langle x, y \mid x^{2^n} = 1,\ y^2 = x^{2^{n-1}},\ y^{-1}xy = x^{-1} \right\rangle.$$

Classe 2. O grupo diedral:

$$D_{2^n} = \left\langle x, y \ \mid x^{2^n} = y^2 = 1,\ y^{-1}xy = x^{-1} \right\rangle.$$

[1] Para qualquer número primo p, um grupo G (não necessariamente finito) é dito um *p-grupo* se todo elemento em G tem sua ordem uma potência de p.

Classe 3. O grupo quasi-diedral:

$$QD_{2^n} = \left\langle x, y \mid x^{2^n} = y^2 = 1,\ y^{-1}xy = x^{2^{n-1}-1} \right\rangle.$$

Classe 4.

$$P_{2,n} = \left\langle x, y \mid x^{2^n} = y^2 = 1,\ y^{-1}xy = x^{2^{n-1}+1} \right\rangle.$$

Demonstração: Veja ref. Kwak e Xu (2005).

■

Primeiro, começamos investigando os grupos $P_{2,n}$. Este grupo pode ser encarado como um produto semidireto da forma

$$P_{2,n} \simeq \mathbb{Z}_{2^n} \rtimes_\alpha \mathbb{Z}_2, \tag{3.1}$$

onde o homomorfismo α é definido por $\alpha = 2^{n-1} + 1$. O grupo $P_{2,n}$ é nilpotente de classe 2 (veja Sec. 4.3); assim, o PSO nesta classe de grupos pode ser resolvido eficientemente em um computador quântico, Ivanyos et al. (2007b).

Na classe 2, temos o grupo diedral, podendo também ser representado por um produto semidireto

$$D_{2^n} \simeq \mathbb{Z}_{2^n} \rtimes_\phi \mathbb{Z}_2, \tag{3.2}$$

onde $\phi = 2^n - 1$. Neste caso, o melhor algoritmo quântico conhecido para o PSO é devido à Kuperberg (2005), e possui complexidade subexponencial, $2^{O(\sqrt{n})}$.

Por fim, consideremos o PSO sobre os grupos das classes 1 e 3. Estes grupos são nilpotentes de classe n (veja Apêndice A, Exemplo A.1.1), logo não podemos aplicar os resultados de Ivanyos et al. (2007b), para grupos nilpotentes de classe de nilpotência constante, nestas classes de grupos.

Neste capítulo, apresentamos algoritmos quânticos com complexidade de tempo subexponencial para o PSO sobre os grupos das classes 1 e 3. Nossa abordagem reúne as idéias apresentadas por Kuperberg (2005), para o PSO diedral, com um critério de redução primeiramente utilizado por Ettinger e Høyer (2000).

Este critério consiste basicamente em conhecer a estrutura dos subgrupos de um determinado grupo e utilizar a transformada de Fourier abeliana para obter informações sobre o subgrupo oculto. Através do conhecimento da estrutura dos subgrupos, mostramos que o PSO pode ser reduzido ao problema de encontrar subgrupos cíclicos.

3.1 O Algoritmo Peneira

Em Regev (2004a), Regev apresenta uma versão simplificada do algoritmo de Kuperberg para o PSO diedral, com espaço de solução polinomial. O autor descreve um algoritmo clássico para um determinado problema de busca e mostra que este algoritmo corresponde exatamente ao algoritmo de Kuperberg. Nesta seção, nós descrevemos em detalhes este algoritmo, pois, o entendimento do mesmo será de extrema importância na compreensão dos algoritmos quânticos apresentados nas seções subsequentes.

Suponhamos que exista um procedimento (caixa preta) que cria objetos rotulados com números no conjunto $\{0, \ldots, N-1\}$, onde N é qualquer inteiro positivo. Por simplicidade, façamos $N = 2^n$, $n = k^2 + 1, k \in \mathbb{Z}$. Suponhamos que a saída do procedimento seja um objeto e seu rótulo. Nosso objetivo é obter um objeto com rótulo 2^{n-1} ou em binário $10\ldots0$. Esse problema pode ser facilmente resolvido chamando repetidas vezes o procedimento que cria os objetos até obtermos como saída um objeto com rótulo 2^{n-1}. Este algoritmo é simples e resolve nosso problema, contudo, é ineficiente, pois possui complexidade $\mathrm{O}(2^n)$. Nossa intenção é obter um algoritmo, cujo tempo de execução seja $2^{O(\sqrt{n})}$, isto é, um algoritmo com complexidade de tempo subexponencial.

Suponhamos que os objetos criados pela nossa caixa preta tenham a seguinte propriedade: dados dois objetos, com rótulos a e b, respectivamente, podemos *combinar* estes objetos de modo a obter um novo objeto com rótulo $a - b$. Então os dois objetos originais são descartados. Com probabilidade $1/2$ nós obtemos o novo objeto com rótulo $a - b$, e com probabilidade $1/2$ a operação falha, isto é,

ambos o novo objeto e os objetos originais são perdidos[2] .

A descrição geral do algoritmo, como mostra a Figura 3.1.1, é a seguinte. Imagine que temos um conjunto formado por k rotinas, tal que a entrada da rotina $i+1$ é a saída da rotina i. A entrada da rotina 1, são os objetos que acabaram de ser produzidos pela caixa preta. Os objetos que entram na rotina i, para todo $i = 1, \ldots, k$, são objetos cujos rótulos possuem os ik bits menos significativos todos iguais a zero. Os $n - ik$ bits restantes são bits aleatórios. A partir desse processo, a k-ésima rotina resulta com probabilidade $1/2$ o objeto com rótulo 2^{n-1}.

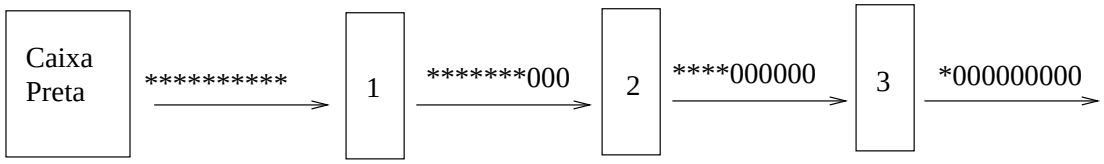


Figura 3.1: Caso particular com $n = 10$ e $k = 3$ do procedimento que produz ao final da k-ésima rotina o elemento procurado com probabilidade $1/2$.

Para entendermos como essas rotinas são de fato implementadas, fixe uma rotina i, para algum $i = 1, \ldots, k$. A rotina i mantém uma pilha objetos, que são produzidos pela caixa preta. Inicialmente esta pilha está vazia, contudo, novos objetos vão surgindo na pilha. Quando um novo objeto surge, a rotina compara os k bits do rótulo do objeto enviado, nas posições $(i-1)k+1, \ldots, ik$, com o mesmo conjunto de bits dos rótulos dos objetos armazenados na pilha. Quando um par de objetos, cujos rótulos possuem o mesmo conjunto de k bits, é encontrado, a rotina zera esse conjunto de bits. Esse procedimento resulta num novo objeto com probabilidade $1/2$. Caso a rotina não encontre um par de objetos com a propriedade descrita acima, um novo objeto é adicionado à pilha.

A seguir, mostraremos que a complexidade do algoritmo que acabamos de descrever é $2^{O(\sqrt{n})}$. Esse algoritmo é também chamado de algoritmo Peneira, devido a similaridade com a peneira de Eratóstenes, que é um algoritmo para formar uma tabela de números primos.

[2] O motivo pelo qual supomos os objetos produzidos pela caixa preta terem tal propriedade é explicado na Seção 3.2.2. Lá esses objetos são trocados por q-bits.

3.1.1 Análise do Algoritmo

Nesta seção, mostramos que, dado um conjunto com elementos rotulados com números de 0 a $2^n - 1$, o algoritmo Peneira determina em tempo $2^{O(\sqrt{n})}$ e com alta probabilidade, um elemento com rótulo 2^{n-1}.

Começamos observando que para cada $i = 1, \ldots, k$, a rotina i mantém uma pilha de objetos. Sempre que um novo objeto chega na rotina, ela procura em sua pilha um elemento que tenha o mesmo conjunto de k bits nas posições $(i-1)k + 1, \ldots, ik$. Quando a rotina encontra tal elemento dizemos que temos um *match*. Note que, se a pilha tiver poucos elementos armazenados esse match raramente ocorre. Por outro lado, se cada rotina tiver um total de 2^k objetos armazenados, um match ocorre com alta probabilidade. Com isso, fazemos a combinação entre os elementos que compõem o match e com probabilidade $1/2$ essa combinação gera um novo objeto. Esse novo objeto, agora com os k bits nas posições $(i-1)k+1, \ldots, ik$ zerados, é então enviado para próxima rotina.

Observe que cada rotina precisa em média de 4 objetos para produzir um novo objeto com alta probabilidade. De fato, suponha que um match seja encontrado. Com probabilidade $1/2$ a combinação falha e a pilha perde um objeto. Então um novo objeto é enviado para a rotina para completar o conjunto de 2^k objetos estocados. Outro match é encontrado; a probabilidade de falha de duas combinações sucessivas é $1/4$, portanto, a probabilidade de sucesso da segunda combinação é $3/4$, uma boa probabilidade em termos computacionais. Após a combinação (seja ela bem sucedida ou não) a rotina sempre perde um objeto. Assim, um último objeto é enviado à rotina para completar o conjunto de 2^k elementos guardados. Com isso, cada rotina precisa em média de 4 objetos para produzir um novo objeto de saída com alta probabilidade. Logo, o número total de objetos provenientes da caixa preta, necessários para que o algoritmo Peneira resulte o elemento desejado, é $4^k = 2^{O(\sqrt{n})}$.

Vamos repetir esse argumento de maneira mais formal. Para isso considere o seguinte teorema:

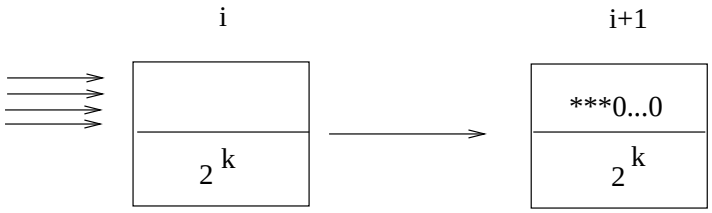


Figura 3.2: Número de objetos necessários para a rotina i produzir um objeto de saída com alta probabilidade.

Teorema 3.1.1 Suponha que uma rotina i receba $l2^k$ objetos, com $l \geq 8$. Então, com alta probabilidade, a rotina resulta pelo menos $\frac{l}{8}2^k$ objetos, para todo $i = 1, \ldots, k$.

Demonstração: De fato, suponha que $l2^k$ objetos sejam enviados para a rotina i, qualquer que seja $i = 1, \ldots, k$. Temos que $(l-1)2^k$ destes objetos são usados pela rotina para efeito de combinação, enquanto, os objetos restantes, cerca de 2^k, permanecem na pilha. Agora, para cada par de objetos combinados, defina a variável aleatória[3] χ_j, tal que, $\chi_j = 1$, se a combinação entre o par de objetos for bem sucedida, e $\chi_j = 0$, caso contrário. O número esperado de variáveis aleatórias que resultam sucesso é $\frac{l-1}{4}2^k$. Assim, aplicando o limite de Chernoff a este conjunto de variáveis aleatórias, obtemos

$$p\left(\sum_{j=1}^{\frac{l-1}{4}2^k} \chi_j \leq \frac{l-1}{8}2^k\right) \leq e^{-2\epsilon^2 \frac{l-1}{4}2^k}. \tag{3.3}$$

Isto mostra que com alta probabilidade, o número de objetos resultados da i-ésima rotina é, no mínimo $\frac{l}{8}2^k$.

■

Agora, segue do Teorema 3.1.1, que iniciando o algoritmo Peneira com

$$8^k.2^k = 2^{O(\sqrt{n})} \tag{3.4}$$

objetos, a k-ésima rotina resulta com alta probabilidade, pelo menos um objeto

[3] Uma variável aleatória χ representa um valor numérico associado a cada um dos resultados de um experimento probabilístico.

com rótulo 2^{n-1}.

3.2 O grupo QD_{2^n}

O grupo quasi-diedral, denotado por QD_{2^n}, possui 2^{n+1} elementos e tem a seguinte apresentação

$$QD_{2^n} = \left\langle x, y \mid x^{2^n} = y^2 = e,\ yx = x^{2^{n-1}-1}y \right\rangle. \tag{3.5}$$

O grupo QD_{2^n} também pode ser representando pelo produto semidireto

$$QD_{2^n} = \mathbb{Z}_{2^n} \rtimes_\phi \mathbb{Z}_2, \tag{3.6}$$

onde o homomorfismo $\phi : \mathbb{Z}_2 \to \mathrm{Aut}(\mathbb{Z}_{2^n})$ é tal que $\phi(1)(1) = 2^{n-1} - 1$. Denotamos por $x = (1, 0)$ e $y = (0, 1)$ os geradores do QD_{2^n} nesta nova notação. Assim, cada elemento $x^a y^b$ de QD_{2^n} pode ser representado como (a, b) com $a \in \mathbb{Z}_{2^n}$ e $b \in \mathbb{Z}_2$.

A proposição seguinte classifica todos os subgrupos de QD_n. Veremos na Seção 3.2.1 que o conhecimento da estrutura dos subgrupos de QD_n é fundamental na construção do algoritmo quântico para o PSO no grupo QD_n.

Proposição 3.2.1 Os subgrupos de QD_{2^n} são da forma $\left\langle x^{2^i} \right\rangle$ ou $\left\langle x^{2^i}, x^a y \right\rangle$ para todo $0 \leq i \leq n$ e $0 \leq a \leq 2^n - 1$.

Demonstração: Seja $H' = H \cap \langle x \rangle$, onde $\langle x \rangle$ é um subgrupo normal de QD_{2^n}. Então $H' = \left\langle x^{2^i} \right\rangle$ para algum $0 \leq i \leq n$. Vamos assumir que $H \neq H'$. Então é claro que $x^a y \in H$ para algum $0 \leq a \leq 2^n - 1$. Como $\left\langle x^{2^i} \right\rangle \subset H$ temos que $\left\langle x^{2^i}, x^a y \right\rangle \subset H$. Agora basta mostrar que $H \subset \left\langle x^{2^i}, x^a y \right\rangle$. Com efeito, seja $h \in H$ um elemento arbitrário. Então $h = x^s y^t$, para algum $0 \leq s \leq 2^n - 1$ e $t = 0, 1$. Se $t = 0$ então $h = x^{\alpha 2^i}$ e a inclusão é imediata. Considere então $t = 1$. Como $x^a y \in H$ temos que o inverso de $x^a y$, $yx^{-a} \in H$, logo $x^s yyx^{-a} \in H \Rightarrow x^{s-a} \in H \Rightarrow s - a = k2^i \Rightarrow s = k2^i + a \Rightarrow x^s y = x^{k2^i + a} y = x^{k2^i} x^a y \in \left\langle x^{2^i}, x^a y \right\rangle$ e portanto, $H \subset \left\langle x^{2^i}, x^a y \right\rangle$.

■

Proposição 3.2.2 Seja $H = \langle x^a y \rangle$ um subgrupo de QD_n. Então $|H| = 2$ se $2 \mid a$ ou $|H| = 4$ caso contrário.

Demonstração: Com efeito,

$$(x^a y)^2 = x^a y x^a y = x^a x^{a(2^{n-1}-1)} y^2 = x^{a2^{n-1}} \tag{3.7}$$

implica que $|H| = 2$ se $2 \mid a$. Suponha que $2 \nmid a$, então $(x^a y)^3 = x^{a(2^{n-1}+1)} y$ e $(x^a y)^4 = e$, portanto $|H| = 4$.

■

3.2.1 Algoritmo Quântico para o PSO no Grupo QD_{2^n}

Nesta seção apresentamos um algoritmo quântico que resolve o PSO no grupo QD_{2^n}, com complexidade de tempo $2^{O(\sqrt{n})}$, onde n é o parâmetro que especifica o grupo que estamos tratando. Nosso algoritmo combina as idéias apresentadas na Seção 3.1 junto com um procedimento de redução que daremos a seguir.

Seja f a função que oculta o subgrupo H em QD_n. De acordo com a Proposição 3.2.1 existem duas possibilidades para o subgrupo H, ou de forma equivalente, existem dois parâmetros a serem determinados i e a. O parâmetro a é o mais difícil de ser encontrado. Mostraremos como a pode ser determinado na próxima seção.

Agora, observe como o problema do subgrupo oculto em QD_{2^n} pode ser reduzido ao problema de encontrar subgrupos cíclicos. De fato, primeiro rodamos o algoritmo descrito na Seção 3.2.2. Se o algoritmo resulta o valor de a e se $f(x^a y) = f(e)$ (lembre-se que f é prometida ser constante nas classes laterais do subgrupo H) então $H = \left\langle x^{2^i}, x^a y \right\rangle$. Caso contrário, sabemos que $H = \left\langle x^{2^i} \right\rangle$. Podemos determinar i calculando $f(x^{2^i})$ para todo $i = 0, \ldots, n$. Quando encontramos um inteiro i com a propriedade $f(x^{2^i}) = f(e)$ então concluímos que x^{2^i} é um elemento gerador de H. Assim, o PSO em QD_{2^n} pode ser reduzido ao problema de determinar o gerador do subgrupo $\langle x^a y \rangle$, ou seja, determinar a, um número entre

0 e $2^n - 1$.

Antes de exibirmos o algoritmo que determina o parâmetro a, façamos uma última redução. Mostraremos que o problema de determinar a reduz-se ao problema de determinar a paridade r_0 de a. Com efeito, suponhamos que, dada uma função $f : QD_{2^n} \to X$ que oculta o subgrupo $H = \langle x^a y \rangle$ em QD_{2^n}, existe um procedimento quântico que determina r_0. Logo, podemos escrever

$$a = 2a_1 + r_0, \tag{3.8}$$

onde a_1 é um elemento arbitrário em $\mathbb{Z}_{2^{n-1}}$ e r_0 é conhecido. Observe que r_0 fornece o bit menos significativo de a.

Agora, defina a função $f^{(1)} : QD_{2^{n-1}} \to X$ tal que

$$f^{(1)}(x^s y^t) = f(x^{2s+tr_0} y^t). \tag{3.9}$$

Temos que $f^{(1)}$ oculta o subgrupo $H^{(1)} = \langle x^{a_1} y \rangle$ de $QD_{2^{n-1}}$. De fato, da Proposição 3.2.1 segue que uma classe lateral arbitrária de $H^{(1)}$ em $QD_{2^{n-1}}$ é

$$x^\alpha H^{(1)} = \left\{ x^{a_1+\alpha} y, x^{a_1 2^{n-1}+\alpha}, x^{a_1(2^{n-1}+1)+\alpha} y, x^\alpha \right\} \tag{3.10}$$

para algum $\alpha \in \mathbb{Z}_{2^{n-3}}$ se $|H| = 4$, ou

$$x^\alpha H^{(1)} = \{ x^{a_1+\alpha} y, x^\alpha \} \tag{3.11}$$

para algum $\alpha \in \mathbb{Z}_{2^{n-2}}$ se $|H| = 2$. Assim, aplicando a função $f^{(1)}$ aos elementos da classe lateral $x^\alpha H^{(1)}$, obtemos

$$f^{(1)}(x^{a_1+\alpha} y) = f^{(1)}(x^{a_1(2^{n-1}+1)+\alpha} y) = f(x^{a+2\alpha} y) \tag{3.12}$$

e

$$f^{(1)}(x^{a_1 2^{n-1}+\alpha}) = f^{(1)}(x^\alpha) = f(x^{2\alpha}). \tag{3.13}$$

Como f é constante na classe lateral $x^{2\alpha}H$ do subgrupo $H = \langle x^a y \rangle$ de QD_{2^n}, temos que $f^{(1)}$ é constante em $x^\alpha H^{(1)}$. Agora, basta verificarmos que $f^{(1)}$ assume valores distintos para diferentes classes laterais de $H^{(1)}$ em $QD_{2^{n-1}}$. De fato, sejam $x^\alpha H^{(1)}$ e $x^\beta H^{(1)}$ duas classes laterais distintas de $H^{(1)}$, então

$$f^{(1)}(x^\alpha H^{(1)}) = f^{(1)}(x^\beta H^{(1)}) \Leftrightarrow f^{(1)}(x^{a_1+\alpha}y) = f^{(1)}(x^{a_1+\beta}y) \quad (3.14)$$

$$\Leftrightarrow f(x^{a+2\alpha}y) = f(x^{a+2\beta}y) \quad (3.15)$$

$$\Leftrightarrow x^{a+2\beta} \in x^{2\alpha}H \quad (3.16)$$

$$\Leftrightarrow \alpha = \beta, \quad (3.17)$$

portanto, $f^{(1)}(x^\alpha H^{(1)}) \neq f^{(1)}(x^\beta H^{(1)})$, e concluímos que $f^{(1)}$ oculta o subgrupo $H^{(1)}$ em $QD_{2^{n-1}}$.

Assim, dada a função $f^{(1)}$ que oculta o subgrupo $H^{(1)} = \langle x^{a_1} y \rangle$ em $QD_{2^{n-1}}$, existe um procedimento quântico que determina a paridade r_1 de a_1, com alta probabilidade. Este procedimento acha o segundo bit menos significativo de a.

De forma geral, pondo $f^{(0)} := f$, e definindo $f^{(k)} : QD_{2^{n-k}} \to X$ tal que

$$f^{(k)}(x^s y^t) = f^{(k-1)}(x^{2s+tr_{k-1}} y^t), \quad (3.18)$$

para todo $1 \leq k \leq n-1$, onde r_{k-1} é o k-ésimo bit menos significativo de a, a função $f^{(k)}$ oculta o subgrupo $H^{(k)} = \langle x^{a_k} y \rangle$ em $QD_{2^{n-k}}$. Logo, existe um procedimento quântico que encontra o k-ésimo bit menos significativo de a. Isto implica que, rodando o procedimento que acabamos de descrever, $O(n)$ vezes, obtemos todos os bits de a, e consequentemente, a.

Na próxima seção, exibiremos o procedimento quântico que determina a paridade de a a partir da informações da função f que oculta o subgrupo $H = \langle x^a y \rangle$.

3.2.2 O Caso $\langle x^a y \rangle$

Dada uma função f que oculta o subgrupo $H = \langle x^a y \rangle$, o procedimento a seguir determina em tempo $2^{O(\sqrt{n})}$ e com alta probabilidade, a paridade de a. Este

procedimento, que está resumido no Algoritmo 3.2.1, utiliza a transformada de Fourier abeliana. Note que este é um fato interessante pois o grupo em questão é um grupo não abeliano. O procedimento é o seguinte:

(1) Prepare o computador quântico no estado inicial

$$|\Psi_1\rangle = \frac{1}{\sqrt{2^{n+1}}} \sum_{m=0}^{2^n-1} \sum_{n=0}^{1} |m\rangle\,|n\rangle\,|f(x^m y^n)\rangle \tag{3.19}$$

e defina $m_0 = m - na \bmod 2^n$. Então o estado acima pode ser reescrito usando m_0 no somatório ao invés de m como segue

$$|\Psi_1\rangle = \frac{1}{\sqrt{2^{n+1}}} \sum_{m_0=0}^{2^n-1} \sum_{n=0}^{1} |m_0 + na\rangle\,|n\rangle\,\left|f(x^{m_0+na} y^n)\right\rangle. \tag{3.20}$$

Note que para cada $n = 0, 1$, $x^{na}y^n$ é um elemento no subgrupo oculto H, assim, todos os elementos $x^{m_0}x^{na}y^n$ são levados num mesmo valor, isto é,

$$f(x^{m_0}x^{na}y^n) = f(x^{m_0}), \tag{3.21}$$

para todo $0 \leq m_0, a \leq 2^n - 1$. Novamente reescrevendo o estado em (6.10) obtemos

$$|\Psi_1\rangle = \frac{1}{\sqrt{2^{n+1}}} \sum_{m_0=0}^{2^n-1} \sum_{n=0}^{1} |m_0 + na\rangle\,|n\rangle\,|f(x^{m_0})\rangle. \tag{3.22}$$

(2) Meça o terceiro registrador na base computacional. Este, por não ter mais relevância na computação, será descartado. Assim, o resultado da medida é

$$|\Psi_2\rangle = \frac{1}{\sqrt{2}} \sum_{n=0}^{1} |m_0' + na\rangle\,|n\rangle, \tag{3.23}$$

onde $m_0' \in \mathbb{Z}_{2^n}$ é um número uniformemente randômico.

(3) Aplique a transformada de Fourier $F_{\mathbb{Z}_{2^n}} \otimes I$ ao estado $|\Psi_2\rangle$. O resultado é

$$\begin{aligned} |\Psi_3\rangle &= \frac{1}{\sqrt{2}} \sum_{n=0}^{1} \left(\frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} {\omega_{2^n}}^{(m_0'+na)k} |k\rangle \right) |n\rangle \\ &= \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} {\omega_{2^n}}^{m_0'k} |k\rangle \left(\frac{1}{\sqrt{2}} \sum_{n=0}^{1} {\omega_{2^n}}^{kna} |n\rangle \right), \end{aligned} \tag{3.24}$$

onde $\omega_{2^n} = e^{\frac{2\pi i}{2^n}}$.

(4) Meça o primeiro registrador do estado $|\Psi_3\rangle$. O resultado é

$$\frac{1}{\sqrt{2}} \left(|0\rangle + e^{\frac{2\pi i k_0 a}{2^n}} |1\rangle \right), \tag{3.25}$$

onde $k_0 \in \mathbb{Z}_{2^n}$ é um número uniformemente randômico.

A discussão acima pode ser sumarizada no seguinte algoritmo:

Algoritmo 3.2.1 Procedimento de Amostragem sobre QD_{2^n}

Entrada: um inteiro n e a função $f : QD_{2^n} \to X$, onde X é um conjunto finito.

Saída: um estado quântico de 1 q-bit.

1. Prepare o estado quântico

$$\frac{1}{\sqrt{2^{n+1}}} \sum_{t=0}^{2^n-1} \sum_{s=0}^{1} |t\rangle |s\rangle \left| f(x^t y^s) \right\rangle.$$

2. Meça o último registrador:

$$\frac{1}{\sqrt{2}} \sum_{n=0}^{1} |m_0' + na\rangle |n\rangle, \;\; m_0' \in \mathbb{Z}_{2^n}.$$

3. Aplique $F_{\mathbb{Z}_{2^n}}$ ao primeiro registrador.
4. Meça o primeiro registrador:

$$\frac{1}{\sqrt{2}} \left(|0\rangle + e^{2\pi i k \frac{a}{2^n}} |1\rangle \right).$$

A saída do Algoritmo 3.2.1 é um estado da forma

$$\left| \psi_k^{a,2^n} \right\rangle = \frac{1}{\sqrt{2}} \left(|0\rangle + e^{2\pi i k \frac{a}{2^n}} |1\rangle \right), \tag{3.26}$$

para algum k uniformemente distribuído em $\mathbb{Z}_{2^n}$. Nosso objetivo, é obter o estado

$$\left|\psi_{2^{n-1}}^{a,2^n}\right\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + e^{\pi i a}\,|1\rangle\right), \tag{3.27}$$

pois, uma única aplicação da transformada de Hadamard em $\left|\psi_{2^{n-1}}^{a,2^n}\right\rangle$ revela a paridade de a. De fato,

$$\begin{aligned} H\left|\psi_{2^{n-1}}^{a,2^n}\right\rangle &= \frac{1}{\sqrt{2}}\left(H\,|0\rangle + e^{\pi i a} H\,|1\rangle\right) \\ &= \frac{1}{\sqrt{2}}\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}} + e^{\pi i a}\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) \\ &= \frac{1}{2}\left((1+e^{\pi i a})\,|0\rangle + (1-e^{\pi i a})\,|1\rangle\right) \\ &= \begin{cases} |0\rangle, & \text{se } a \text{ for par} \\ |1\rangle, & \text{se } a \text{ for ímpar.} \end{cases} \end{aligned}$$

Quando obtemos o estado $\left|\psi_k^{a,2^n}\right\rangle$, o parâmetro k é um número uniformemente randômico no conjunto $\{0,1,\ldots,2^n-1\}$, logo a probabilidade de obtermos o estado $\left|\psi_{2^{n-1}}^{a,2^n}\right\rangle$ direto do Algoritmo 3.2.1 é $1/2^n$, que é exponencialmente pequena. Desta forma, vamos utilizar o algoritmo Peneira, descrito na Seção 3.1, para o obtermos o estado $\left|\psi_{2^{n-1}}^{a,2^n}\right\rangle$ em tempo subexponencial.

O procedimento é o seguinte: use o Algoritmo 3.2.1 para produzir $2^{O(\sqrt{n})}$ estados da forma $\left|\psi_k^{a,2^n}\right\rangle$, com k uniformemente distribuído em $\mathbb{Z}_{2^n}$. Vamos chamar o conjunto formado por estes estados de L_0. Aqui, o Algoritmo 3.2.1 funciona como a caixa preta descrita na Seção 3.1, e os objetos, são estados de um q-bit. Dois estados $\left|\psi_{k_1}^{a,2^n}\right\rangle$ e $\left|\psi_{k_2}^{a,2^n}\right\rangle$ são escolhidos no conjunto L_0 se k_1 e k_2 possuem o mesmo conjunto de $k = \lceil\sqrt{n-1}\rceil$ bits menos significativos. Agora, faça o produto tensorial $\left|\psi_{k_1}^{a,2^n}\right\rangle \otimes \left|\psi_{k_2}^{a,2^n}\right\rangle$. O resultado deste produto é

$$\frac{1}{2}(|00\rangle + e^{2\pi i\frac{k_2}{2^n}}\,|01\rangle + e^{2\pi i\frac{ak_1}{2^n}}\,|10\rangle + e^{2\pi i\frac{(k_1+k_2)a}{2^n}}\,|11\rangle). \tag{3.28}$$

Aplique a porta C-NOT ao estado dado pela expressão (3.28), usando o primeiro q-bit como q-bit de controle. O resultado desta aplicação é

$$\frac{1}{2}(|00\rangle + e^{2\pi i \frac{k_2 a}{2^n}} |01\rangle + e^{2\pi i \frac{k_1 a}{2^n}} |11\rangle + e^{2\pi i \frac{(k_1+k_2)a}{2^n}} |10\rangle). \tag{3.29}$$

Meça o segundo q-bit na base $\{|0\rangle, |1\rangle\}$. Então, obtemos com probabilidade 1/2, o estado

$$\left|\psi_{k_1+k_2}^{a,2^n}\right\rangle = \frac{1}{\sqrt{2}}(|0\rangle + e^{2\pi i \frac{(k_1+k_2)a}{2^n}} |1\rangle). \tag{3.30}$$

Também obtemos com probabilidade 1/2 o estado

$$\frac{1}{\sqrt{2}}(e^{\frac{2a\pi i k_2}{2^n}} |0\rangle + e^{\frac{2a\pi i k_1}{2^n}} |1\rangle). \tag{3.31}$$

Multiplicando o estado em (3.31) por um fator de fase global $e^{-2\pi k_2 a}$, obtemos

$$\left|\psi_{k_1-k_2}^{a,2^n}\right\rangle = \frac{1}{\sqrt{2}}(|0\rangle + e^{2\pi i \frac{(k_1-k_2)a}{2^n}} |1\rangle). \tag{3.32}$$

Note que podemos saber qual dos dois estados foi obtido após o processo de medida[4] . O estado quântico com rótulo $k_1 - k_2$, possui os k bits menos significativos iguais a zero. Agora, seja L_1 o conjunto formado por todos os estados $\left|\psi_{k_1-k_2}^{a,2^n}\right\rangle$ com esta propriedade. Repetindo esse procedimento k vezes, obtemos com alta probabilidade um conjunto L_k que possui pelo menos um estado da forma $\left|\psi_{2^{n-1}}^{a,2^n}\right\rangle$.

A análise de complexidade do nosso algoritmo é idêntica à análise do algoritmo Peneira, feita na Seção 3.1.1. Assim, temos o seguinte resultado:

Teorema 3.2.1 Existe um algoritmo quântico que resolve PSO em QD_{2^n}, com alta probabilidade e com complexidade de tempo $2^{O(\sqrt{n})}$.

[4] Os objetos produzidos pela caixa preta, descritos na Seção 3.1, aqui são trocados por q-bits, e o processo que combina dois objetos é representado pelo produto tensorial entre dois estados arbitrários $\left|\psi_{k_1}^{a,2^n}\right\rangle$ e $\left|\psi_{k_2}^{a,2^n}\right\rangle$, seguido de uma medição. Note que a probabilidade 1/2 da combinação entre dois objetos ser bem sucedida refere-se a probabilidade 1/2 de obtermos um estado de um q-bit $\left|\psi_{k_1-k_2}^{a,2^n}\right\rangle$.

3.3 O Grupo Q_{2^n}

Nesta seção, mostramos que o PSO sobre o grupo dos quatérnios generalizados, Q_{2^n}, pode ser resolvido em tempo subexponencial por um computador quântico. Iniciamos a seção apresentando a estrutura dos subgrupos de Q_{2^n} e a partir desta, indicaremos como o algoritmo Peneira pode ser usado para resolver o PSO nesta classe de grupos.

Como vimos no Teorema 3.0.1, o grupo Q_{2^n} de ordem 2^{n+1} é definido como

$$Q_{2^n} = \left\langle x, y \mid x^{2^n} = 1,\ y^2 = x^{2^{n-1}},\ y^{-1}xy = x^{-1} \right\rangle. \tag{3.33}$$

O grupo dos quatérnios generalizados não pode ser expresso como um produto semidireto de um grupo cíclico de ordem 2^n por um grupo de ordem 2. Contudo, existe uma bijeção entre Q_{2^n} e o produto direto de grupos $\mathbb{Z}_{2^n} \times \mathbb{Z}_2$. Essa bijeção fica evidente com a seguinte proposição:

Proposição 3.3.1 Os elementos de Q_{2^n} podem ser escritos da forma $x^a y^b$, com $0 \leq a \leq 2^n - 1$ e $b = 0, 1$.

Demonstração: Sabemos que $x^{2^{n-1}} = y^2$, daí obtemos $x^a y^2 = x^{a+2^{n-1}}$, $x^a y^3 = x^{a+2^{n-1}} y$, $x^a y^4 = x^a$ (pois a ordem de y é 4), $x^a y^5 = x^a y$ e assim sucessivamente. Desta forma, se $g \in Q_{2^n}$ então $g = x^a y^b$, $0 \leq a \leq 2^n - 1$ e $b = 0, 1$.

■

A proposição a seguir fornece a classificação de todos os subgrupos do grupo Q_{2^n}.

Proposição 3.3.2 Os subgrupos de Q_{2^n} são da forma $\left\langle x^{2^i} \right\rangle$ ou $\left\langle x^{2^i}, x^a y \right\rangle$ para todo $0 \leq i \leq n$ e $0 \leq a \leq 2^n - 1$.

Demonstração: Análoga à Proposição 3.2.1.

■

De forma inteiramente análoga à Seção 3.2.1, podemos verificar que o problema do subgrupo oculto no grupo Q_{2^n} se reduz ao problema de determinar um

subgrupo cíclico da forma $H = \langle x^a y \rangle$, onde a um número entre 0 e $2^n - 1$. Agora note que, como existe uma bijeção entre os elementos de Q_{2^n} e $\mathbb{Z}_{2^n} \times \mathbb{Z}_2$, podemos construir o estado quântico

$$\frac{1}{\sqrt{2^{n+1}}} \sum_{t=0}^{2^n-1} \sum_{s=0}^{1} |t\rangle \, |s\rangle \, \left| f(x^t y^s) \right\rangle . \tag{3.34}$$

O estado (3.34) corresponde ao estado inicial do Algoritmo 3.2.1.

Portanto, passando para o Algoritmo 3.2.1 a função $f : Q_{2^n} \to X$ que oculta o subgrupo $H = \langle x^a y \rangle$ em Q_{2^n} e seguindo como na seção anterior, resolvemos o PSO em Q_{2^n} em tempo subexponencial. Isto nos leva ao seguinte resultado:

Teorema 3.3.1 Existe um algoritmo quântico que resolve PSO em Q_{2^n}, com alta probabilidade e com complexidade de tempo $2^{O(\sqrt{n})}$.

Capítulo 4

Produtos Semidiretos de Grupos

O grupo diedral é um caso particular de um produto semidireto de grupos. Embora não seja conhecido algoritmos quânticos eficientes para o PSO no grupo diedral, existem algumas classes de produtos semidiretos de grupos onde o PSO pode ser resolvido eficientemente em um computador quântico.

Neste capítulo, mostramos que existe um algoritmo quântico eficiente para o PSO no produto semidireto de grupos $\mathbb{Z}_N^m \rtimes \mathbb{Z}_p$, onde p é um número primo ímpar, m, N inteiros positivos. Mostramos que, impondo algumas restrições sobre a fatoração prima de N, o grupo $\mathbb{Z}_N^m \rtimes \mathbb{Z}_p$ é isomorfo a um grupo G, que é um produto direto de um grupo abeliano por um grupo não abeliano. Então, nós resolvemos o PSO em G, determinando uma solução eficiente para o PSO em cada parte do produto direto grupos.

4.1 Preliminares

Iniciamos este capítulo com uma breve revisão de alguns conceitos importantes sobre produtos semidiretos de grupos e grupos de automorfismos que são fundamentais para o entendimento do trabalho. Para um estudo mais aprofundado desses tópicos sugerimos o leitor as referências Garcia e Lequain (2002); Hernstein (1970); Robinson (1995); Hall Jr. (1959).

Considere o produto direto de grupos $G_1 \times G_2$, onde G_1 e G_2 são dois grupos finitos. Note que, se $H_1 \leq G_1$ e $H_2 \leq G_2$ então $H_1 \times H_2$ é um subgrupo de $G_1 \times G_2$.

Entretanto, nem todo subgrupo de $G_1 \times G_2$ é da forma $H_1 \times H_2$. A proposição a seguir diz que a afirmação contrária é verdadeira sempre que G_1 e G_2 possuem ordens coprimas.

Proposição 4.1.1 Sejam G_1 e G_2 grupos finitos com ordens coprimas. Então todo subgrupo de $G_1 \times G_2$ é da forma $H_1 \times H_2$, onde $H_1 \leq G_1$ e $H_2 \leq G_2$.

Demonstração: Seja $\pi_i : G_1 \times G_2 \to G_i$ tal que $\pi_i(g_1, g_2) = g_i$, $i = 1, 2$. Para todo subgrupo H de $G_1 \times G_2$ defina $H_1 = \pi_1(H) \leq G_1$ e $H_2 = \pi_2(H) \leq G_2$, assim $H \leq H_1 \times H_2$. Vamos mostrar que $H = H_1 \times H_2$. De fato, se $(h_1, h_2) \in H_1 \times H_2$ então pela definição de H_1 e H_2, existem $h_1' \in G_1$ e $h_2' \in G_2$ tais que $(h_1, h_2'), (h_1', h_2) \in H$. Como $\text{mdc}\,(|G_1|, |G_2|) = 1$, segue do Teorema Chinês dos Restos que existem inteiros r_1 e r_2 tais que

$$\begin{cases} r_1 \equiv 1 \mod |G_1| \\ r_1 \equiv 0 \mod |G_2| \end{cases} \text{ e } \begin{cases} r_2 \equiv 0 \mod |G_1| \\ r_2 \equiv 1 \mod |G_2| \end{cases}. \tag{4.1}$$

Segue das equações em (4.1) que existem inteiros positivos k_1, k_2, k_3, k_4 tais que

$$\begin{cases} r_1 = k_1|G_1| + 1 \\ r_1 = k_2|G_2| \end{cases} \text{ e } \begin{cases} r_2 = k_3|G_1| \\ r_2 = k_4|G_2| + 1 \end{cases}.$$

Assim,

$$\begin{aligned} (h_1, h_2')^{r_1} &= (h_1^{r_1}, h_2'^{r_1}) = (h_1^{k_1|G_1|+1}, h_2'^{k_2|G_2|}) = (h_1, e_2) \in H \\ (h_1', h_2)^{r_2} &= (h_1'^{r_2}, h_2^{r_2}) = (h_1'^{k_3|G_1|}, h_2^{k_4|G_2|+1}) = (e_1, h_2) \in H \end{aligned}$$

onde e_1 e e_2 são os elementos identidade dos grupos G_1 e G_2, respectivamente. Logo, $(h_1, h_2) = (h_1, e_2)(e_1, h_2) \in H$.

■

Sejam G_1 e G_2 grupos. A aplicação $\phi : G_1 \to G_2$ tal que $\phi(g_1 g_2) = \phi(g_1)\phi(g_2)$ é chamada um *homomorfismo* de grupos. Quando o homomorfismo ϕ é bijetivo ele é chamado um *isomorfismo* de grupos e escrevemos $G_1 \simeq G_2$. Um isomorfismo

$\phi : G \to G$ é chamado um *automorfismo* do grupo G. Denotamos por $\mathrm{Aut}\,(G)$ o conjunto de todos os automorfismos de G. O conjunto $\mathrm{Aut}\,(G)$ com a operação de composição de funções é um grupo, cujo elemento identidade é a função identidade, Id.

Proposição 4.1.2 (Hillar e Rhea (2006)) Sejam H e K grupos finitos com ordens coprimas. Então $\mathrm{Aut}(H) \times \mathrm{Aut}(K) \simeq \mathrm{Aut}(H \times K)$.

Demonstração: Considere a aplicação $\phi : \mathrm{Aut}(H) \times \mathrm{Aut}(K) \to \mathrm{Aut}(H \times K)$ dada por

$$\phi(\alpha\beta)(h,k) = (\alpha(h), \beta(k))$$

onde $\alpha \in \mathrm{Aut}(H)$ e $\beta \in \mathrm{Aut}(K)$. Sejam, Id_H e Id_K os elementos identidades de $\mathrm{Aut}(H)$ e $\mathrm{Aut}(K)$, respectivamente. Para provar que ϕ é um homomorfismo, note que $\phi(Id_H, Id_K) = Id_{H\times K}$ e que

$$\phi(\alpha_1\alpha_2, \beta_1\beta_2)(h,k) = (\alpha_1\alpha_2(h), \beta_1\beta_2(k)) = \phi(\alpha_1, \beta_1)\phi(\alpha_2, \beta_2)(h,k),$$

para todo $\alpha_1, \alpha_2 \in \mathrm{Aut}(H)$, $\beta_1, \beta_2 \in \mathrm{Aut}(K)$, $h \in H$ e $k \in K$.

Agora, vamos mostrar que ϕ é um isomorfismo. De fato, claramente ϕ é injetiva. Sejam $n = |H|$, $m = |K|$ e $\pi_H : H \times K \to H$ tal que $\pi_H(h,k) = h$, $\pi_K : H \times K \to K$ tal que $\pi_K(h,k) = k$ os homomorfismos projeções canônicos. Fixe $\omega \in \mathrm{Aut}(H \times K)$ e considere o homomorfismo $\gamma : K \to H$ dado por $\gamma(k) = \pi_H(\omega(1_H, k)$, onde 1_H é o elemento identidade do grupo H. Note que

$$\gamma(k^n) = \pi_H(\omega(1_H, k^n)) = \pi_H(\omega(1_H, k)^n) = \pi_H(\omega(1_H, k))^n = 1_H,$$

o que implica $\{k^n; k \in K\} \subseteq \ker\gamma$. Como $\mathrm{mdc}(m,n) = 1$, o conjunto $\{k^n; k \in K\}$ possui exatamente m elementos. Consequentemente, $\ker\gamma = K$ e γ é o homomorfismo trivial. Analogamente, $\delta : H \to K$ tal que $\delta(h) = \pi_K(\omega(h), 1_K)$ é trivial.

Agora, defina $\omega_H(h) = \pi_H(\omega(h, 1_K))$ e $\omega_K(k) = \pi_K(\omega(1_H, k))$. Note que

$$\omega(h,k) = \omega(h,1_K)\omega(1_H,k) = (\omega_H(h), \omega_K(k)) = \phi(\omega_K, \omega_K)(h,k),$$

para todo $h \in H$ e $k \in K$. Agora falta mostrar que $\omega_H \in \mathrm{Aut}(H)$ e $\omega_K \in \mathrm{Aut}(K)$. Para isso, basta ver que ω_H e ω_K são injetivos (pois ambos H e K são finitos). Assim, suponha que $\omega_H(h) = 1_H$ para algum $h \in H$. Então $\omega(h, 1_K) = (\omega_H(h), \omega_K(1_K)) = (1_H, 1_K)$, logo $h = 1_H$ pela injetividade de ω. Um argumento similar mostra que $\omega_K \in \mathrm{Aut}(K)$, e isto completa a prova.

■

Definição 4.1.1 Considere grupos G_1 e G_2 e um homomorfismo $\phi : G_2 \to \mathrm{Aut}\,(G_1)$ tal que $g_2 \in G_2 \mapsto \phi(g_2) \in \mathrm{Aut}\,(G_1)$. Definimos sobre os elementos de $G_1 \times G_2$ a seguinte operação:

$$(g_1,\, g_2)(g_1',\, g_2') = (g_1\phi(g_2)(g_1'), g_2g_2').$$

O conjunto $G_1 \times G_2$ com a operação acima definida é chamado o *produto semidireto* de G_1 por G_2, denotado por $G_1 \rtimes_\phi G_2$ ou $G_2 \ltimes_\phi G_1$.

Observe que o produto direto dos grupos G_1 e G_2 é um caso especial do produto semidireto. Com efeito, seja $\phi : G_2 \to \mathrm{Aut}\,(G_1)$, $g_2 \in G_2 \mapsto \phi(g_2) = I_d \in \mathrm{Aut}\,(G_1)$. Então

$$(g_1,\, g_2)(g_1',\, g_2') = (g_1\phi(g_2)(g_1'), g_2g_2') = (g_1I_d(g_1'), g_2g_2') = (g_1g_1', g_2g_2'). \qquad (4.2)$$

Assim, $G_1 \rtimes_\phi G_2 = G_1 \times G_2$.

Exemplo 4.1.1 São exemplos de produtos semidiretos de grupos não triviais os seguintes grupos:

i) diedral: $D_{2^n} \simeq \mathbb{Z}_{2^n} \rtimes_{\phi_1} \mathbb{Z}_2$ com $\phi_1 = 2^n - 1$;

ii) quasi-diedral: $QD_{2^n} \simeq \mathbb{Z}_{2^n} \rtimes_{\phi_2} \mathbb{Z}_2$ com $\phi_2 = 2^{n-1} - 1$;

iii) $P_{2,n} \simeq \mathbb{Z}_{2^n} \rtimes_{\phi_3} \mathbb{Z}_2$ onde $\phi_3 = 2^{n-1} + 1$.

Demonstração: Para provarmos i) considere a aplicação $\Psi : \mathbb{Z}_{2^n} \rtimes_{\phi_1} \mathbb{Z}_2 \to D_{2^n}$ definida por $\Psi(a, b) = x^a y^b$. Temos que Ψ é um homomorfismo. De fato,

$$\begin{aligned}
\Psi((a,b)(a',b')) &= \Psi(a + \phi_1(b)(a'), b + b') = \Psi(a + (-1)^b a') \\
&= x^{a+(-1)^{b'}a'} y^{b+b'} = x^a x^{a'(-1)^b} y^{b+b'} \\
&= x^a y^b x^{a'} y^{b'} = \Psi(a,b)\Psi(a',b')
\end{aligned}$$

para todo $(a, b), (a', b') \in \mathbb{Z}_{2^n} \rtimes_{\phi_1} \mathbb{Z}_2$. Claramente Ψ é uma bijeção, portanto um isomorfismo de grupos.

As demonstrações de ii) e iii) seguem de forma análoga.

■

Seja o produto semidireto de grupos $G_1 \rtimes_\phi G_2$. O homomorfismo $\phi : G_2 \to \mathrm{Aut}\,(G_1)$ nem sempre é único. De fato, tome por exemplo, $G_1 = \mathbb{Z}_{p^r}$ e $G_2 = \mathbb{Z}_q$, onde p e q são números primos ímpares e r um inteiro positivo. Temos que $\mathbb{Z}_{p^r} \rtimes_\phi \mathbb{Z}_q$ é o grupo gerado pelos elementos $x = (1, 0)$ e $y = (0, 1)$, satisfazendo $x^{p^r} = y^q = 1_{\mathbb{Z}_{p^r} \rtimes_\phi \mathbb{Z}_q}$ e $yx = x^{\phi(1)(1)}y$. Neste caso, Inui e Gall (2007) classificaram o produto semidireto de grupos $\mathbb{Z}_{p^r} \rtimes_\phi \mathbb{Z}_q$ em cinco classes.

Teorema 4.1.1 (Inui e Gall (2007)) O produto semidireto de grupos $\mathbb{Z}_{p^r} \rtimes_\phi \mathbb{Z}_q$ para p e q primos e r um inteiro, está divido nas seguintes cinco classes de grupos.

Classe 1. O produto direto $\mathbb{Z}_{p^r} \times \mathbb{Z}_q$ (grupos abelianos).

Classe 2. Os grupos q-edrais definidos por p, q e r tal que $r \geq 1$ e $q \mid (p-1)$, que são os grupos G gerados por x e y satisfazendo $x^{p^r} = y^q = 1_G$ e $yx = x^\gamma y$ onde γ é tal que $\gamma^q \equiv 1 \mathrm{mod}\ p$.

Classe 3. O grupo diedral D_{2^r} para $r > 2$, que são os grupos gerados por x e y satisfazendo $x^{2^r} = y^2 = 1_{D_{2^r}}$ e $yx = x^{2^r-1}y$.

Classe 4. Os grupos quasi-diedrais, para $r > 2$ e x e y satisfazendo $x^{2^r} = y^2 = 1_{D_{2^r}}$ e $yx = x^{2^{r-1}-1}y$.

Classe 5. Os grupos $P_{p,r}$ para $r \geq 2$, que são os grupos gerados por x e y, satisfazendo $x^{p^r} = y^p = 1_{P_{p,r}}$ e $yx = x^{p^{r-1}+1}y$.

■

Moore et al. (2004) resolveram o PSO eficientemente sobre os grupos da Classe 2, com $r = 1$ e q suficientemente grande com relação a p. Os grupos da Classe 3 foram estudados no Capítulo 3, onde apresentamos um algoritmo quântico em tempo subexponencial para o PSO sobre estas classes de grupos. Inui e Gall (2007) resolveram o PSO sobre os grupos da Classe 5, com p primo ímpar.

Uma solução eficiente do PSO sobre os grupos das Classes 1 a 5, representa um avanço considerável na solução do PSO em produtos semidiretos de grupos. Além disso, o estudo dessas classes de grupos ajuda na solução do PSO sobre produtos semidiretos mais gerais, como veremos a seguir.

4.2 O PSO sobre o Grupo $\mathbb{Z}_N^m \rtimes \mathbb{Z}_p$

Nesta seção mostramos que existe um algoritmo quântico eficiente para o PSO sobre o produto semidireto de grupos $\mathbb{Z}_N^m \rtimes_\phi \mathbb{Z}_p$, onde p é um número primo ímpar, m, N inteiros positivos, e N fatorado como $N = p_1^{r_1}...p_n^{r_n}$, com $1 \leq r_1 \leq \ldots \leq r_n$ onde $p \nmid p_i^k - 1$ para todo $i = 1, \ldots, n$ e $k = 1, \ldots, m$. Mostramos que o grupo $\mathbb{Z}_N^m \rtimes \mathbb{Z}_p$ é isomorfo ao produto direto $\mathbb{Z}_{\frac{N}{p_n^{r_n}}}^m \times (\mathbb{Z}_{p_n{}^{r_n}}^m \rtimes_\varphi \mathbb{Z}_{p_n})$. Então, determinamos os geradores do subgrupo oculto resolvendo o PSO em cada parte do produto direto de grupos.

Considere o seguinte lema:

Lema 4.2.1 Seja o homomorfismo de grupos $\phi : \mathbb{Z}_p \to \mathrm{Aut}(\mathbb{Z}_{q^s}^m \times \mathbb{Z}_{p^r}^m)$ onde p, q são primos ímpares distintos e r, s, m inteiros positivos. Dados $a \in \mathbb{Z}_{q^s}^m$, $b \in \mathbb{Z}_{p^r}^m$ e $\alpha \in \mathbb{Z}_p$, existem $a' \in \mathbb{Z}_{q^s}^m$ e $b' \in \mathbb{Z}_{p^r}^m$ tais que $\phi(\alpha)(a, 0) = (a', 0)$ e $\phi(\alpha)(0, b) = (0, b')$.

Demonstração: De fato, seja e_i um elemento de $\mathbb{Z}_{q^s}^m$ cuja i-ésima coordenada é 1 e as demais são iguais a zero. Suponha que $\phi(\alpha)(e_i, 0) = (c, d)$ para algum $c \in \mathbb{Z}_{q^s}^m$

e $d \in \mathbb{Z}_{p^r}^m$. Como $\phi(\alpha)$ é um homomorfismo note que

$$\begin{aligned}(0,0) &= \phi(\alpha)(0,0) = \phi(\alpha)(q^s,0) = \phi(\alpha)(q^s e_i,0) = \phi(\alpha)(e_i + \ldots + e_i,0) \\ &= \phi(\alpha)((e_i,0) + \ldots + (e_i,0)) = \phi(\alpha)(e_i,0) + \phi(\alpha)(e_i,0) + \ldots + \phi(\alpha)(e_i,0) \\ &= q^s\phi(\alpha)(e_i,0) = q^s(c,d) = (q^s c, q^s d). \end{aligned} \tag{4.3}$$

Isto implica que $q^s d \equiv 0 \bmod p^r$, mas p e q são primos distintos, logo $d \equiv 0 \bmod p^r$, e portanto $\phi(\alpha)(e_i,0) = (c,0)$. Agora, considere $a \in \mathbb{Z}_{p^r}^m$ um elemento qualquer, então

$$\begin{aligned}\phi(\alpha)(a,0) &= \phi(\alpha)((a_1,\ldots,a_m),0) = \phi(\alpha)(\sum_i a_i e_i,0) \\ &= \sum_i a_i\phi(\alpha)(e_i,0) = \sum_i a_i(c,0) = (a',0). \end{aligned} \tag{4.4}$$

Analogamente, podemos mostrar que para qualquer $b \in \mathbb{Z}_{p^r}^m$, existe um $b' \in \mathbb{Z}_{p^r}^m$ tal que $\phi(\alpha)(0,b) = (0,b')$.

■

Teorema 4.2.1 Sejam os grupos $\mathbb{Z}_{q^s}^m \times \mathbb{Z}_{p^r}^m$ e $\mathbb{Z}_p$ com $r,s,m \in \mathbb{N}$ e q,p primos ímpares distintos satisfazendo $p \nmid (q^k - 1)$ para todo $1 \leq k \leq m$. Então

$$(\mathbb{Z}_{q^s}^m \times \mathbb{Z}_{p^r}^m) \rtimes_\phi \mathbb{Z}_p \simeq \mathbb{Z}_{q^s}^m \times (\mathbb{Z}_{p^r}^m \rtimes_\varphi \mathbb{Z}_p),$$

para algum $\phi \in \mathrm{Hom}(\mathbb{Z}_p, \mathrm{Aut}(\mathbb{Z}_{q^s}^m \times \mathbb{Z}_{p^r}^m))$ e $\varphi \in \mathrm{Hom}(\mathbb{Z}_p, \mathrm{Aut}(\mathbb{Z}_{p^r}^m))$.

Demonstração: Com efeito, para cada $c \in \mathbb{Z}_p$, existem elementos $a, a' \in \mathbb{Z}_{q^s}^m$ (Lema 4.1.2) tais que

$$\phi(c)(a,0) = (a',0). \tag{4.5}$$

Isso nos permite definir o seguinte homomorfismo

$$\begin{aligned} \Psi: \ & \mathbb{Z}_p \to \mathrm{Aut}(\mathbb{Z}_{q^s}^m) \\ & c \mapsto \Psi(c) = \phi(c)\Big|_{\mathbb{Z}_{q^s}^m} : \ \mathbb{Z}_{q^s}^m \to \mathbb{Z}_{q^s}^m \\ & \qquad\qquad\qquad\qquad a \mapsto \Psi(c)(a) = \phi(c)(a) = a'. \end{aligned} \tag{4.6}$$

Note que Ψ é de fato um homomorfismo, pois ϕ o é. Além disso, sendo $\phi(c)$ um automorfismo, a' é único tal que $\phi(c)(a,0) = a'$.

Agora consideremos o $\ker(\Psi)$. Como p é primo e $\ker(\Psi)$ é um subgrupo de $\mathbb{Z}_p$, temos que $\ker(\Psi) = \{e\}$ ou $\ker(\Psi) = \mathbb{Z}_p$. Suponhamos $\ker(\Psi) = \{e\}$ então Ψ é injetiva, e portanto, $\mathrm{Im}(\Psi)$ é um subgrupo de $\mathrm{Aut}(\mathbb{Z}_{q^s}^m)$ de ordem p. Então, p divide $|\mathrm{Aut}(\mathbb{Z}_{q^s}^m)|$. Mas

$$|\mathrm{Aut}(\mathbb{Z}_{q^s}^m)| = q^{m^2(s-1)+\frac{m(m-1)}{2}} \prod_{k=1}^{m} (q^k - 1), \tag{4.7}$$

logo, como p e q são primos distintos, temos que $p \mid q^k - 1$ para algum k, contrariando nossa hipótese. Assim, $\ker(\Psi) = \mathbb{Z}_p$ e então $\Psi(c) = Id$, para todo $c \in \mathbb{Z}_p$, ou seja, ϕ age trivialmente em $\mathbb{Z}_{q^s}^m$. Assim, ϕ é tal que

$$\phi(c)(a,b) = (a, \varphi(c)(b)), \tag{4.8}$$

para algum homomorfismo $\varphi : \mathbb{Z}_p \to \mathrm{Aut}(\mathbb{Z}_{p^r})$ tal que $\varphi(c) = \phi(c)\Big|_{\mathbb{Z}_{p^r}^m}$. Logo, se $((a,b),c), ((a',b'),c') \in (\mathbb{Z}_{q^s}^m \times \mathbb{Z}_{p^r}^m) \rtimes_\phi \mathbb{Z}_p$ então:

$$\begin{aligned} ((a,b),c)._\phi((a',b'),c') &= ((a,b) + \phi(c)(a',b'), c + c') && (4.9) \\ &= ((a,b) + (a', \varphi(c)(b')), c + c') && (4.10) \\ &= (a + a', b + \varphi(c)(b'), c + c') && (4.11) \\ &= (a, (b,c)._\varphi(a', (b', c'))). && (4.12) \end{aligned}$$

Portanto,

$$(\mathbb{Z}_{q^s}^m \times \mathbb{Z}_{p^r}^m) \rtimes_\phi \mathbb{Z}_p \simeq \mathbb{Z}_{q^s}^m \times (\mathbb{Z}_{p^r}^m \rtimes_\varphi \mathbb{Z}_p),$$

como queríamos demonstrar.

■

De maneira mais geral, seja $N \in \mathbb{N}$ com decomposição em fatores primos $N = p_1^{r_1}...p_n^{r_n}$, com $1 \leq r_1 \leq \ldots \leq r_n$. Assim, $\mathbb{Z}_N \simeq \mathbb{Z}_{p_1^{r_1}} \times \ldots \times \mathbb{Z}_{p_n^{r_n}}$ e dado $m \in \mathbb{N}$ temos

$$\mathbb{Z}_N^m \simeq \mathbb{Z}_{p_1^{r_1}}^m \times \ldots \times \mathbb{Z}_{p_n^{r_n}}^m. \tag{4.13}$$

Pela Proposição 4.1.2

$$\mathrm{Aut}(\mathbb{Z}_N^m) \simeq \mathrm{Aut}(\mathbb{Z}_{p_1^{r_1}}^m) \times \ldots \times \mathrm{Aut}(\mathbb{Z}_{p_n^{r_n}}^m). \tag{4.14}$$

Seja p um número primo ímpar tal que $p \nmid p_i^k - 1$ para todo $i = 1, \ldots, n$ e $k = 1, \ldots, m$. Seja também $\phi : \mathbb{Z}_p \to \mathrm{Aut}(\mathbb{Z}_N^m) \simeq \mathrm{Aut}(\mathbb{Z}_{p_1^{r_1}}^m) \times \ldots \times \mathrm{Aut}(\mathbb{Z}_{p_n^{r_n}}^m)$ um homomorfismo de grupos não trivial. Como p é primo, $\ker(\phi) = \{e\}$, o que implica que ϕ é um homomorfismo injetor. Assim, $\phi(\mathbb{Z}_p)$ é um subgrupo de $\mathrm{Aut}(\mathbb{Z}_N^m)$ cuja ordem é p, logo, $p \mid |\mathrm{Aut}(\mathbb{Z}_N^m)|$. Mas

$$\begin{aligned} |\mathrm{Aut}(\mathbb{Z}_N^m)| &= |\mathrm{Aut}(\mathbb{Z}_{p_1^{r_1}}^m)| \ldots |\mathrm{Aut}(\mathbb{Z}_{p_n^{r_n}}^m)| && (4.15)\\ &= p_1^{m^2(r_1-1)+\frac{m(m-1)}{2}} \prod_{k_1=1}^{m} (p_1^{k_1} - 1) \ldots && (4.16)\\ &\ldots \quad p_n^{m^2(r_n-1)+\frac{m(m-1)}{2}} \prod_{k_n=1}^{m} (p_n^{k_n} - 1). && (4.17) \end{aligned}$$

Como supomos $p \nmid p_i^k - 1$ para todo $i = 1, \ldots, n$ e $k = 1, \ldots, m$, segue que $p = p_i$ para algum i. Sem perda de generalidade podemos supor $p = p_n$ e por um argumento análogo ao do Teorema 4.2.1, segue que para todo $c \in \mathbb{Z}_p$, $\phi(c)$ age trivialmente sobre $\mathbb{Z}_{p_1^{r_1}}^m, \ldots, \mathbb{Z}_{p_{n-1}^{r_{n-1}}}^m$. Assim,

$$\mathbb{Z}_N^m \rtimes_\phi \mathbb{Z}_p \simeq (\mathbb{Z}_{p_1^{r_1}}^m \times \ldots \times \mathbb{Z}_{p_{n-1}^{r_{n-1}}}^m) \times (\mathbb{Z}_{p_n^{r_n}}^m \rtimes_\varphi \mathbb{Z}_{p_n}) \tag{4.18}$$

para algum $\varphi \in \mathrm{Hom}(\mathbb{Z}_{p_n}, \mathrm{Aut}(\mathbb{Z}_{p_n^{r_n}}^m))$. Além disso, como

$$\mathbb{Z}_{p_1^{r_1}}^m \times \ldots \times \mathbb{Z}_{p_{n-1}^{r_{n-1}}}^m \simeq \mathbb{Z}_{\frac{N}{p_n^{r_n}}}^m, \tag{4.19}$$

temos

$$\mathbb{Z}_N^m \rtimes_\phi \mathbb{Z}_p \simeq \mathbb{Z}_{\frac{N}{p_n^{r_n}}}^m \times (\mathbb{Z}_{p_n^{r_n}}^m \rtimes_\varphi \mathbb{Z}_{p_n}). \tag{4.20}$$

Note também que

$$\mathrm{mdc}\left(\left|\mathbb{Z}_{\frac{N}{p_n^{r_n}}}^m\right|, \left|\mathbb{Z}_{p_n^{r_n}}^m \rtimes_\psi \mathbb{Z}_{p_n}\right|\right) = 1, \tag{4.21}$$

logo, pela Proposição 4.1.1, se H é um subgrupo de $\mathbb{Z}_N^m \rtimes_\phi \mathbb{Z}_p$, então

$$H \simeq H_0 \times H_1, \tag{4.22}$$

onde H_0 é um subgrupo de $\mathbb{Z}_{\frac{N}{p_n^{r_n}}}^m$ e H_1 um subgrupo de $\mathbb{Z}_{p_n^{r_n}}^m \rtimes_\varphi \mathbb{Z}_{p_n}$.

Agora, resolvendo o PSO no grupo abeliano $\mathbb{Z}_{N/p_n^{r_n}}^m$, encontramos os geradores de H_0 de forma eficiente, Shor (1997). O grupo $\mathbb{Z}_{p_n^{r_n}}^m \rtimes_\varphi \mathbb{Z}_{p_n}$ é uma generalização dos grupos da Classe 5, descrita no Teorema 4.1.1, logo os geradores de H_1 podem ser encontrados de forma eficiente utilizando as técnicas apresentadas em Inui e Gall (2007). Uma vez conhecidos os geradores de H_0 e H_1 obtemos facilmente os geradores de H. Com isso, estabelecemos o seguinte resultado:

Teorema 4.2.2 Existe um algoritmo quântico eficiente para o PSO sobre o produto semidireto de grupos $\mathbb{Z}_N^m \rtimes_\phi \mathbb{Z}_p$, onde $N = p_1^{r_1}...p_n^{r_n}$, p é um número primo ímpar satisfazendo $p \nmid p_i^k - 1$ para todo $i = 1, \ldots, n$ e $k = 1, \ldots, m$.

■

4.3 Sobre a Nilpotência de $\mathbb{Z}_N^m \rtimes_\phi \mathbb{Z}_p$

Nesta seção, mostramos que o grupo $\mathbb{Z}_N^m \rtimes \mathbb{Z}_p$ é nilpotente de classe 2. Para isso, considere o grupo

$$P_{p,r}^m = \mathbb{Z}_{p^r}^m \rtimes_\alpha \mathbb{Z}_p = \left\langle x_1, \ldots, x_m, y;\ y^p = 1,\ yx_i = x_i^{p^{r-1}+1} y,\ x_i^{p^r} = 1, \forall i \right\rangle \tag{4.23}$$

onde o homomorfismo α é definido por $\alpha = p^{r-1} + 1$ (Inui e Gall (2007)). Este grupo é gerado pelos elementos $x_1 = (1, \ldots, 0, 0), x_2 = (0, 1, \ldots, 0, 0), \ldots, x_m = (0, \ldots, 1, 0)$ e $y = (0, \ldots, 0, 1)$. Seja também o seguinte conjunto

$$\left\{ g \in P_{p,r}^m \; ; \; gx_i = x_i g \; \forall \; i = 1, \ldots, m \text{ e } gy = yg \right\}. \tag{4.24}$$

É fácil ver que este conjunto corresponde exatamente ao centro de $P_{p,r}^m$, ou seja,

$$\mathcal{Z}(P_{p,r}^m) = \{ g \in P_{p,r}^m \; ; \; gx_i = x_i g \; \forall \; i = 1, \ldots, m \text{ e } gy = yg \}. \tag{4.25}$$

Proposição 4.3.1 $\mathcal{Z}(P_{p,r}^m) = \langle x_1^p, \ldots, x_m^p \rangle$.

Demonstração: Primeiro, observe que para todo $i = 1, \ldots, m$, $\langle x_i \rangle \lhd P_{p,r}^m$. Desta forma, $\langle x_1, \ldots, x_m \rangle \lhd P_{p,r}^m$ e podemos escrever $P_{p,r}^m = \langle x_1, \ldots, x_m \rangle \langle y \rangle$. Assim, todo elemento $g \in P_{p,r}^m$ pode ser escrito como

$$g = x_1^{a_1} \ldots x_m^{a_m} y^b, \tag{4.26}$$

para algum $a_1, \ldots, a_m \in \mathbb{Z}_{p^r}$ e $b \in \mathbb{Z}_p$.

Seja $g \in \mathcal{Z}(P_{p,r}^m)$ um elemento arbitrário, então

$$\begin{aligned} gx_i &= (x_1^{a_1} \ldots x_m^{a_m} y^b) x_i && (4.27) \\ &= x_i^{\alpha^b} (x_1^{a_1} \ldots x_m^{a_m} y^b) && (4.28) \\ &= x_i^{\alpha^b} g = x_i g && (4.29) \\ &\Leftrightarrow \; b \equiv 0 \bmod p. && (4.30) \end{aligned}$$

Seja também

$$\begin{aligned} yg &= y(x_1^{a_1}\dots x_m^{a_m}y^b) && (4.31)\\ &= \left(x_1^{a_1(p^{r-1}+1)}x_2^{a_2(p^{r-1}+1)}\dots x_m^{a_m(p^{r-1}+1)}y^b\right)y && (4.32)\\ &= gy && (4.33)\\ &\Leftrightarrow\ p \mid a_i\ \forall\ i=1,\dots,m. && (4.34)\end{aligned}$$

Logo, se $g \in \mathcal{Z}(P_{p,r}^m)$ então podemos escrever $g = x_1^{k_1p}x_2^{k_2p}\dots x_m^{k_mp} \in \langle x_1^p,\dots,x_m^p\rangle$ com $k_1,\dots,k_n \in \mathbb{Z}_{p^{r-1}}$, isto implica que $\mathcal{Z}(P_{p,r}^m) \subset \langle x_1^p,\dots,x_m^p\rangle$. Para a inclusão inversa, note que se $g \in \langle x_1^p,\dots,x_m^p\rangle$ então (como $\langle x_i\rangle \lhd P_{p,r}^m$)

$$g = x_1^{k_1p}x_2^{k_2p}\dots x_m^{k_mp} \tag{4.35}$$

com $k_1,\dots,k_n \in \mathbb{Z}_{p^{r-1}}$. Agora note que

$$\begin{aligned} yg = yx_1^{k_1p}\dots x_m^{k_mp} &= x_1^{k_1p(p^{r-1}+1)}\dots x_m^{k_mp(p^{r-1}+1)}y && (4.36)\\ &= x_1^{k_1p}\dots x_m^{k_mp}y && (4.37)\\ &= gy, && (4.38)\end{aligned}$$

logo $g \in \mathcal{Z}(P_{p,r}^m)$ e portanto, temos a igualdade desejada.

■

Seja $P_{p,r}^{m\,\prime} = [P_{p,r}^m, P_{p,r}^m]$ o subgrupo dos comutadores de $P_{p,r}^m$. Então

Lema 4.3.1 $P_{p,r}^{m\,\prime} \subseteq \mathcal{Z}(P_{p,r}^m)$.

Demonstração: Seja g' um elemento arbitrário de $P_{p,r}^{m\,\prime}$, então, $g' = ghg^{-1}h^{-1}$ para algum $g = x_1^{a_1}\dots x_m^{a_m}y^b, h = x_1^{a_1\prime}\dots x_m^{a_m\prime}y^{b'} \in P_{p,r}^m$, logo

$$\begin{aligned} g' = ghg^{-1}h^{-1} &= \left(x_1^{a_1}\dots x_m^{a_m}y^b\right)\left(x_1^{a_1\prime}\dots x_m^{a_m\prime}y^{b'}\right)\\ &\quad \left(y^{-b}x_m^{-a_m}\dots x_1^{-a_1}\right)\left(y^{-b'}x_m^{-a_m\prime}\dots x_1^{-a_1\prime}\right)\\ &= x_1^{(a_1\prime b - a_1b')p^{r-1}}\dots x_m^{(a_m\prime b - a_mb')p^{r-1}}. && (4.39)\end{aligned}$$

Assim $g' \in \left\langle x_1^{p^{r-1}}, \ldots, x_m^{p^{r-1}} \right\rangle$ e portanto,

$$P_{p,r}^{m\,\prime} \subset \left\langle x_1^{p^{r-1}}, \ldots, x_m^{p^{r-1}} \right\rangle \subset \mathcal{Z}(P_{p,r}^m), \tag{4.40}$$

como queríamos demonstrar.

■

Teorema 4.3.1 O grupo $\mathbb{Z}_N^m \rtimes \mathbb{Z}_p$ é nilpotente de classe 2.

Demonstração: O grupo $\mathbb{Z}_{\frac{N}{p^{rn}}}^m$ é nilpotente de classe de 1, pois é um grupo abeliano. Como $P_{p,r}^{m\,\prime} \subseteq \mathcal{Z}(P_{p,r}^m)$ (Lema 4.3.1), segue do Teorema A.1.4 que $P_{p,r}^m$ é nilpotente de classe 2. A conclusão segue do isomorfismo $\mathbb{Z}_N^m \rtimes \mathbb{Z}_p \simeq \mathbb{Z}_{\frac{N}{p^{rn}}}^m \times P_{p,r}^m$.

■

Agora, aplicando as ferramentas apresentadas por Ivanyos et al. (2007b), para grupos nilpotentes de classe 2, resolvemos o PSO de forma eficiente sobre o grupo $\mathbb{Z}_N^m \rtimes \mathbb{Z}_p$.

Capítulo 5

O Grupo $\mathbb{Z}_p \rtimes \mathbb{Z}_{q^s}$

Neste capítulo estudamos os grupos $\mathbb{Z}_p \rtimes_\phi \mathbb{Z}_{q^s}$, com p, q primos ímpares distintos e s um inteiro positivo qualquer. Cada homomorfismo $\phi : \mathbb{Z}_{q^s} \to \mathrm{Aut}(\mathbb{Z}_p)$ define um produto semidireto de grupos distinto. O objetivo deste capítulo é entender a estrutura desses grupos e seus subgrupos.

5.1 Conceitos Básicos

O que segue é uma apresentação de alguns teoremas básicos da teoria de grupos que são pertinentes ao trabalho. Um breve apanhado sobre a teoria geral de grupos encontra-se no Apêndice A. Para uma leitura mais profunda, recomendamos o leitor as referências Garcia e Lequain (2002); Hernstein (1970); Robinson (1995); Hall Jr. (1959) e Spindler (1994).

Seja o grupo $\mathbb{Z}_N^*$, o grupo multiplicativo dos inteiros módulo N e coprimos com N. O teorema a seguir apresenta uma relação entre os grupos $\mathbb{Z}_N^*$ e $\mathrm{Aut}(\mathbb{Z}_N)$.

Teorema 5.1.1 Seja $N \in \mathbb{Z}$. Então a aplicação $\Psi : \mathrm{Aut}(\mathbb{Z}_N) \to \mathbb{Z}_N^*$ definida por $\Psi(f) = f(1)$ é um isomorfismo de grupos.

Demonstração: Note primeiro que Ψ está bem definida, pois, como 1 gera $\mathbb{Z}_N$, temos que $f(1)$ também gera $\mathbb{Z}_N$ para toda $f \in \mathrm{Aut}(\mathbb{Z}_N)$, assim, $f(1) \in \mathbb{Z}_N^*$. É fácil ver que Ψ é um homomorfismo. Além disso, se $f \in \mathrm{Ker}(\Psi)$ temos que $f(1) = \Psi(f) = 1$, então $f(a) = f(\underbrace{1+1+\ldots+1}_{a \text{ vezes}}) = \underbrace{f(1)+\ldots+f(1)}_{a \text{ vezes}} = \underbrace{1+1+\ldots+1}_{a \text{ vezes}} =$

a. Mas isto implica que f é a função identidade, logo $\mathrm{Ker}(\Psi)$ possui apenas o elemento identidade, e portanto Ψ é injetora. Agora suponha $a \in \mathbb{Z}_N^*$ e seja $f : \mathbb{Z}_N \to \mathbb{Z}_N$ definida por $f(b) = ab$. Observe que f é um homomorfismo, $f(1) = a \in \mathbb{Z}_N^*$. Note que f é injetora, pois, $0 = f(b) = ab \Rightarrow b = 0 \Rightarrow \mathrm{Ker}(f) = \{0\}$. Ela é também sobrejetiva, pois, se $b \in \mathbb{Z}_N$ então $b = a(a^{-1}b) = f(a^{-1}b)$. Assim, f é um isomorfismo tal que $\Psi(f) = f(1) = a$. Logo Ψ é sobrejetiva e, portanto, um isomorfismo.

■

Segue do Teorema 5.1.1 que para toda $f \in \mathrm{Aut}(\mathbb{Z}_N)$ existe um único $f(1) \in \mathbb{Z}_N^*$ tal que $f(a) = af(1)$. Desta forma, podemos mostrar usando indução sobre k que

$$f^k(a) = af(1)^k \tag{5.1}$$

para todo $k \in \mathbb{N}$.

Agora considere $M \in \mathbb{N}$ e $\phi : \mathbb{Z}_M \to \mathrm{Aut}(\mathbb{Z}_N)$ um homomorfismo de grupos. Como ϕ é um homomorfismo, para todo $b \in \mathbb{Z}_M$ temos

$$\phi(b) = \phi(\underbrace{1 + \ldots + 1}_{b \text{ vezes}}) = \underbrace{\phi(1) \circ \ldots \circ \phi(1)}_{b \text{ vezes}} = \phi(1)^b. \tag{5.2}$$

Assim, não é difícil ver que

$$\phi(b)(a) = \phi(1)^b(a) = a\phi(1)(1)^b. \tag{5.3}$$

Portanto, ϕ fica completamente determinada por $\phi(1)(1) \in \mathbb{Z}_N^*$. Com isso temos o seguinte resultado.

Teorema 5.1.2 A aplicação $\Gamma : \mathrm{Hom}(\mathbb{Z}_M, \mathrm{Aut}(\mathbb{Z}_N)) \to \mathbb{Z}_N^*$ definida por $\Gamma(\phi) = \phi(1)(1)$ é uma bijeção.

Demonstração: Pelo discutido anteriormente, a aplicação Γ está bem definida, pois dado $\phi \in \mathrm{Hom}(\mathbb{Z}_M, \mathrm{Aut}(Z_N))$ existe um único $\phi(1)(1) \in \mathbb{Z}_N^*$ tal que $\Gamma(\phi) = \phi(1)(1)$.

Seja então $r \in \mathbb{Z}_N^*$ e $\phi : \mathbb{Z}_M \to \mathrm{Aut}(\mathbb{Z}_N)$ tal que para todo $b \in \mathbb{Z}_M$, $\phi(b) : \mathbb{Z}_N \to \mathbb{Z}_N$ é definida por

$$\phi(b)(a) = ar^b. \tag{5.4}$$

Primeiro mostraremos que a aplicação ϕ está bem definida. De fato, para quaisquer elementos $b, b' \in \mathbb{Z}_M$ temos que

$$r^b = \phi(b)(1) = \phi(b')(1) = r^{b'}. \tag{5.5}$$

Como $r \in \mathbb{Z}_N^*$, segue que $r^{b-b'} \equiv 1 \bmod N$. Assim, $b - b' \equiv 0 \bmod M$ implicando em $b = b'$. Agora mostraremos que qualquer que seja $b \in \mathbb{Z}_M$, $\phi(b) \in \mathrm{Aut}(\mathbb{Z}_N)$. De fato, $\phi(b)$ é um homomorfismo, pois,

$$\phi(b)(a + c) = (a + c)r^b = ar^b + cr^b = \phi(b)(a) + \phi(b)(c). \tag{5.6}$$

Note também que $\phi(b)$ é bijetiva. Com efeito, se $a \in \mathbb{Z}_N$ então $a = a(r^{-b}r^b) = (ar^{-b})r^b = \phi(b)(ar^{-b})$. Como r^{-b} é único, dado $a \in \mathbb{Z}_N$ existe um único $a' \in \mathbb{Z}_N$, $a' = ar^{-b}$, tal que $\phi(b)(a') = a$, logo, $\phi(b)$ é bijetiva e, portanto, $\phi(b) \in \mathrm{Aut}(\mathbb{Z}_N)$.

Por fim, ϕ é um homomorfismo. De fato, para todo $b, b' \in \mathbb{Z}_M$ e $a \in \mathbb{Z}_N$ temos que

$$\begin{aligned} \phi(b) \circ \phi(b')(a) &= \phi(b)(\phi(b')(a)) = \phi(b)(ar^{b'}) && (5.7)\\ &= (ar^{b'})r^b = ar^{b+b'} && (5.8)\\ &= \phi(b + b')(a). && (5.9) \end{aligned}$$

Portanto, $\phi(b + b') = \phi(b) \circ \phi(b')$.

Finalmente, note que $\Gamma(\phi) = \phi(1)(1) = r$. Assim, dado $r \in \mathbb{Z}_N^*$, temos que ϕ definida em (5.4) é o único elemento em $\mathrm{Hom}(\mathbb{Z}_M, \mathrm{Aut}(\mathbb{Z}_N))$ tal que $\Gamma(\phi) = r$, com isso demonstramos o teorema.

■

5.2 A Estrutura do Grupo $\mathbb{Z}_p \rtimes \mathbb{Z}_{q^s}$

Sejam p e q números primos e s um inteiro positivo qualquer. Considere os grupos cíclicos $\mathbb{Z}_p$ e $\mathbb{Z}_{q^s}$, e o produto semidireto $\mathbb{Z}_p \rtimes_\phi \mathbb{Z}_{q^s}$, onde $\phi : \mathbb{Z}_{q^s} \to \mathrm{Aut}(\mathbb{Z}_p)$ é o homomorfismo de grupos que define o produto semidireto. Os elementos neste grupo são da forma (a, b), com $a \in \mathbb{Z}_p$ e $b \in \mathbb{Z}_{q^s}$ e a operação entre seus elementos definida pela regra $(a, b)(c, d) = (a+\phi(b)(c), b+d)$. Note que os elementos $x = (1, 0)$ e $y = (0, 1)$ geram o grupo.

Segue do Teorema 5.1.1, que os grupos $\mathrm{Aut}(\mathbb{Z}_p)$ e $\mathbb{Z}_p^*$ são isomorfos. Pelo Teorema 5.1.2, cada homomorfismo ϕ que define o grupo $\mathbb{Z}_p \rtimes \mathbb{Z}_{q^s}$ é completamente determinado por um elemento

$$\alpha = \phi(1)(1) \in \mathbb{Z}_p^*, \tag{5.10}$$

e ainda, $\phi(b)(a) = a\alpha^b$, para todo $a \in \mathbb{Z}_p$ e $b \in \mathbb{Z}_{q^s}$. Desta forma, a operação do grupo fica

$$(a, b)(c, d) = (a + c\alpha^b, b + d). \tag{5.11}$$

Além disso, valem as seguintes regras operacionais:

i) $x^a y^b = (a, b)$;

ii) $y^b x^a = x^{a\alpha^b} y^b$.

Demonstração: De fato, $x^a y^b = (1, 0)^a (0, 1)^b = (a, 0)(0, b) = (a+\phi(0)(0), 0+b) = (a, b)$, assim provamos i). Para ii) note que $y^b x^a = (0, 1)^b (1, 0)^a = (0, b)(a, 0) = (0 + \phi(b)(a), b) = (a\alpha^b, b) = x^{a\alpha^b} y^b$.

■

Agora note que $\phi(0) = \phi(q^s) : \mathbb{Z}_p \to \mathbb{Z}_p$ é o elemento identidade do grupo $\mathrm{Aut}(\mathbb{Z}_p)$, logo

$$\alpha^{q^s} = \phi(q^s)(1) = 1. \tag{5.12}$$

Então, um elemento $\alpha \in \mathbb{Z}_p^*$ define o produto semidireto de grupos $\mathbb{Z}_p \rtimes_\alpha \mathbb{Z}_{q^s}$ se

satisfaz a seguinte equação de congruência

$$X^{q^s} \equiv 1 \bmod p. \tag{5.13}$$

Neste caso, devemos ter

$$\mathrm{ord}(\alpha) = q^t \tag{5.14}$$

para algum $t = 0, \ldots, s$. O caso $t = 0$ nos conduz ao produto direto de grupos $\mathbb{Z}_p \times \mathbb{Z}_{q^s}$, que é um grupo abeliano. Neste caso, uma solução eficiente para o PSO é conhecida. Daqui para frente consideraremos $1 \leq t \leq s$.

Para todo primo p, o grupo $\mathbb{Z}_p^*$ é cíclico e seja $u \in \mathbb{Z}_p^*$ um gerador arbitrário. Então $\mathrm{ord}(u) = p - 1$. Logo podemos escrever $\alpha = u^k$, para algum $1 \leq k < p - 1$. Assim,

$$\alpha^{q^t} = u^{kq^t} \equiv 1 \bmod p \Rightarrow p - 1 \mid kq^t. \tag{5.15}$$

Mas p e q são primos distintos, logo devemos ter $q^t \mid p - 1$. Desta forma temos

$$k = \frac{l(p-1)}{q^t}, \tag{5.16}$$

para algum $l \in \mathbb{Z}_{q^t}^*$. Assim, para cada $1 \leq t \leq s$ e $l \in \mathbb{Z}_{q^t}^*$, o número

$$\alpha := u^{\frac{l(p-1)}{q^t}}, \tag{5.17}$$

define um produto semidireto de grupos, que será denotado por

$$G_{t,l} = \mathbb{Z}_p \rtimes_\alpha \mathbb{Z}_{q^s}. \tag{5.18}$$

Nós podemos eliminar o parâmetro l na Eq. (5.17), pois, o grupo $G_{t,l}$ é isomorfo ao grupo $G_{t,1}$, para todo valor de l. O Teorema a seguir mostra esse fato.

Teorema 5.2.1 Para todo $l \in \mathbb{Z}_{q^t}^*$, tem-se $G_{t,l} \simeq G_{t,1}$.

Demonstração: De fato, considere a aplicação $\Phi_{t,l} : G_{t,1} \to G_{t,l}$ definida por

$$\Phi_{t,l}(x^a y^b) = x^a y^{l^{-1}b}. \tag{5.19}$$

Note que existe l^{-1}, pois, $l \in \mathbb{Z}_{q^t}^*$, além disso, l^{-1} é único tal que $l^{-1}l = 1$. Assim, dado $x^a y^b \in G_{t,l}$ existe um único $x^a y^{lb} \in G_{t,1}$ tal que $\Phi_{t,l}(x^a y^{lb}) = x^a y^b$, logo $\Phi_{t,l}$ é bijetiva. Pode ser facilmente verificado que $\Phi_{t,l}(x^a y^b x^c y^d) = \Phi_{t,l}(x^a y^b)\Phi_{t,l}(x^c y^d)$, portanto, $\Phi_{t,l}$ é um isomorfismo de grupos.

■

Por simplicidade denotemos o grupo $G_{t,l}$ por G_t, com o homomorfismo α dado pela Eq. (5.17) com $l = 1$.

5.2.1 A Estrutura dos Grupos G_t

Usando a relação $y^b x^a = x^{a\alpha^b} y^b$ e indução sobre k, podemos verificar facilmente que

$$(x^a y^b)^k = \begin{cases} x^{ak} y^{bk} & , \text{se } q^t \mid b \\ x^{\frac{a(\alpha^{bk}-1)}{\alpha^b - 1}} y^{bk} & \text{caso contrário} \end{cases} \tag{5.20}$$

onde $q^t = \text{ord}(\alpha)$.

O lema a seguir tem um papel fundamental na caracterização dos subgrupos cíclicos de G_t.

Lema 5.2.1 Para todo $i = 0, 1$ e $j = t, \ldots, s$ onde t é tal que $\text{ord}(\alpha) = q^t$, temos que

$$\left\langle x^{p^i}, y^{q^j} \right\rangle = \left\langle x^{p^i} y^{q^j} \right\rangle.$$

Demonstração: De fato, se $j = s$ ou $i = 1$, a igualdade é imediata. Então vamos considerar $t \leq j < s$ e $i = 0$. Assim $(xy^{q^j})^{q^{s-j}} = x^{q^{s-j}} \in \left\langle xy^{q^j} \right\rangle$. Além disso, como $\text{mdc}(p, q^{s-j}) = 1$, podemos encontrar inteiros positivos m e n tais que $mp + nq^{s-j} = 1$. Logo, $x = x^{mp+nq^{s-j}} = (x^{q^{s-j}})^n \in \left\langle xy^{q^j} \right\rangle$, o que implica $y^{q^j} \in \left\langle xy^{q^j} \right\rangle$, e portanto $\left\langle x, y^{q^j} \right\rangle \subset \left\langle xy^{q^j} \right\rangle$. A continência $\left\langle xy^{q^j} \right\rangle \subset \left\langle x, y^{q^j} \right\rangle$ é imediata. Assim, $\left\langle xy^{q^j} \right\rangle = \left\langle x, y^{q^j} \right\rangle$.

■

O próximo lema caracteriza todos os subgrupos cíclicos de G_t.

Lema 5.2.2 Os subgrupos cíclicos de G_t são da forma

i) $\left\langle x^a y^{q^j} \right\rangle$, $a \in \mathbb{Z}_p$ e $0 \leq j < t$.

ii) $\left\langle x^{p^i} y^{q^j} \right\rangle$, $i = 0, 1$ e $j = t, \ldots, s$.

Demonstração:

De fato, seja H um subgrupo cíclico de G_t. Então $H = \langle x^a y^b \rangle$ para algum $a \in \mathbb{Z}_p$ e $b \in \mathbb{Z}_{q^s}$. Os casos $a = 0$ ou $b = 0$ nos conduzem aos subgrupos $\left\langle y^{q^j} \right\rangle$ e $\langle x \rangle$ respectivamente, onde $q^j = \text{mdc}(b, q^s)$. Em ambos os casos temos que ou H pertence a classe i) ou a classe ii). Quando $a = b = 0$ obtemos o subgrupo trivial $H = \{e\}$. Suponhamos então a e b inteiros não nulos. Note que se $q^j = \text{mdc}(b, q^s)$ então podemos escrever $b = vq^j$ para algum $v \in \mathbb{Z}_{q^s}^*$. Assim, temos duas possibilidades para o parâmetro j, a saber $j < t$ ou $j \geq t$. No primeiro caso temos

$$(x^a y^{vq^j})^{v^{-1}} = x^{\frac{a(\alpha^{q^j}-1)}{\alpha^b-1}} y^{q^j} \in \left\langle x^a y^b \right\rangle. \tag{5.21}$$

Note que existe v^{-1} tal que $vv^{-1} = 1$, pois $v \in \mathbb{Z}_{q^s}^*$. Fazendo,

$$a' = \frac{a(\alpha^{q^j} - 1)}{\alpha^b - 1} \tag{5.22}$$

temos que $x^{a'} y^{q^j} \in \left\langle x^a y^b \right\rangle$. Como $\text{ord}(x^a y^b) = \text{ord}(x^{a'} y^{q^j}) = q^{s-j}$, temos

$$\left\langle x^{a'} y^{q^j} \right\rangle = \left\langle x^a y^b \right\rangle, \tag{5.23}$$

sempre que $q^j \nmid b$, para todo $0 \leq j < t$ e portanto, H pertence a classe i).

Agora, suponha $j \geq t$. Como $a \neq 0$ e $b \neq 0$ temos

$$(x^a y^b)^k = (x^a y^{vq^j})^k = x^{ak} y^{vq^j k} = e \Leftrightarrow k = pq^{s-j}. \tag{5.24}$$

Além disso, segue do Lema 5.2.1 que $x, y^{q^j} \in \left\langle xy^{q^j} \right\rangle$, logo, $\left\langle x^a y^{vq^j} \right\rangle \subset \left\langle xy^{q^j} \right\rangle$. Como $\left| \left\langle xy^{q^j} \right\rangle \right| = \left| \left\langle x^a y^{vq^j} \right\rangle \right| = pq^{s-j}$, temos que

$$\left\langle x^a y^b \right\rangle = \left\langle x^a y^{vq^j} \right\rangle = \left\langle xy^{q^j} \right\rangle. \tag{5.25}$$

Logo aprendemos que H pertence a classe ii).

■

Agora, consideremos os subgrupos de G_t gerados por um conjunto com n elementos distintos, para algum $n \in \mathbb{N}$. Na verdade, mostramos que qualquer subgrupo de G_t pode ser gerado por um conjunto com no máximo dois elementos. De fato, sejam $g_1, \ldots, g_n$ elementos no grupo G_t. Como $\langle x \rangle$ é um subgrupo normal de G_t (Proposição 5.3.1), podemos escrever

$$g_1 = x^{a_1} y^{b_1}, \ldots, g_n = x^{a_n} y^{b_n}, \tag{5.26}$$

com $a_1, \ldots, a_n \in \mathbb{Z}_p$ e $b_1, \ldots, b_n \in \mathbb{Z}_{q^s}$. Seja H um subgrupo de G_t gerado pelos elementos $g_1, \ldots, g_n \in G_t$. Então, para todo $1 \leq t \leq s$, temos os seguintes casos a considerar:

Caso 1. $q^t \mid b_1, \ldots, q^t \mid b_n$;

Caso 2. $q^t \nmid b_1, \ldots, q^t \nmid b_n$;

Caso 3. $q^t \mid b_i$ para algum $i = 1, \ldots, n$.

No Caso 1, podemos escrever o subgrupo H da forma

$$H = \left\langle x^{a_1} y^{v_1 q^{j_1}}, \ldots, x^{a_n} y^{v_n q^{j_n}} \right\rangle, \tag{5.27}$$

onde $q^{j_k} = \text{mdc}(b_j, q^s)$, $t \leq j_k \leq s$ e $v_k \in \mathbb{Z}_{q^s}^* \bigcup \{0\}$ para todo $1 \leq k \leq n$. Seja $j = \min\{j_1, \ldots, j_n\}$. Se tivermos $a_k = 0$ para todo $k = 1, \ldots, n$ e se existe algum inteiro $1 \leq k \leq n$ tal que $b_k \neq 0$, temos facilmente que $H = \left\langle y^{q^j} \right\rangle$. Por outro lado, se $b_1 = b_2 = \ldots = b_n = 0$ e existe algum $1 \leq k \leq n$ tal que $a_k \neq 0$ então

$H = \langle x \rangle$. Se $a_k = b_k = 0$, para todo $k = 1, \ldots, n$, então é fácil ver que $H = \{e\}$. Em qualquer outro caso, mostramos que $H = \left\langle x, y^{q^j} \right\rangle$, onde $j = \min\{j_1, \ldots, j_n\}$. De fato, para cada a_k e b_k não nulos, com $k = 1, \ldots, n$, temos

$$(x^{a_k} y^{v_k q^{j_k}})^{q^{s-j_k} a_k^{-1}} = x^{q^{s-j_k}} \in H \tag{5.28}$$

o que implica $x \in H$, pois $\text{mdc}(p, q^{s-j_k}) = 1$. Como $x \in H$ temos que $y^{v_k q^{j_k}} \in H$, o que nos leva $y^{q^{j_k}} \in H$. Sendo $j = \min\{j_1, \ldots, j_n\}$ temos $y^{q^j} \in H$ e consequentemente $\left\langle x, y^{q^j} \right\rangle \subset H$. Note também que

$$x^{a_k} y^{q^{j_k}} = x^{a_k} y^{q^{j+j'_k}} = x^{a_k} (y^{q^j})^{q^{j'_k}} \in \left\langle x, y^{q^j} \right\rangle, \tag{5.29}$$

assim $H \subset \left\langle x, y^{q^j} \right\rangle$, e portanto, $H = \left\langle x, y^{q^j} \right\rangle$. Logo, podemos escrever o subgrupo H na forma $H = \left\langle x^{p^i}, y^{q^j} \right\rangle$, para algum $0 \leq i \leq 1$ e $t \leq j \leq s$.

Segue do Lema 5.2.1 que $\left\langle x^{p^i}, y^{q^j} \right\rangle = \left\langle x^{p^i} y^{q^j} \right\rangle$, logo, se H é um subgrupo de G_t com os geradores satisfazendo as condições do Caso 1, então H é da forma

$$H = \left\langle x^{p^i} y^{q^j} \right\rangle \tag{5.30}$$

para algum $0 \leq i \leq 1$ e algum $t \leq j \leq s$.

Agora vamos tratar o Caso 2, isto é,

$$H = \left\langle x^{a_1} y^{b_1}, \ldots, x^{a_n} y^{b_n} \right\rangle \text{ onde } q^t \nmid b_1, \ldots, q^t \nmid b_n. \tag{5.31}$$

Sejam $q^{j_1} = \text{mdc}(b_1, q^s), \ldots, q^{j_n} = \text{mdc}(b_n, q^s)$ e $j = \min\{j_1, \ldots, j_n\}$, onde $0 \leq j < t$. Se $a_k = 0$ para todo $k = 1, \ldots, n$ então

$$H = \left\langle y^{q^j} \right\rangle = \left\langle x^p, y^{q^j} \right\rangle. \tag{5.32}$$

Suponhamos que nem todos os a_k sejam nulos e que existam geradores $x^{a_i} y^{b_i}, x^{a_j} y^{b_j}$ em H que não comutam entre si. Vamos mostrar que $H = \left\langle x, y^{q^j} \right\rangle$. De fato, note

que

$$x^{a_i}y^{b_i}x^{a_j}y^{b_j}(x^{a_i}y^{b_i})^{-1}(x^{a_j}y^{b_j})^{-1} = x^{a_i+a_j\alpha^{b_i}-a_i\alpha^{b_j}-a_j} \in H. \tag{5.33}$$

Da Eq. (5.33) segue que $x \in H$, pois, $a_i + a_j\alpha^{b_i} - a_i\alpha^{b_j} - a_j \neq 0 \bmod p$. Como conseqüência, $y^{q^j} \in H$, logo $\left\langle x, y^{q^j} \right\rangle \subset H$. Não é difícil ver que $H \subset \left\langle x, y^{q^j} \right\rangle$, portanto, temos a igualdade

$$H = \left\langle x, y^{q^j} \right\rangle. \tag{5.34}$$

Suponhamos então que todos os geradores do subgrupo H comutam entre si. Seja $b_j = \min\{b_1, \ldots, b_n\}$, logo podemos escrever $b_k = b_j + v_k$, $v_k \in \mathbb{Z}_{q^s}$ para todo $k = 1, \ldots, n$. Assim, o subgrupo H pode ser descrito da forma

$$H = \left\langle x^{a_1}y^{b_j+v_1}, \ldots, x^{a_j}y^{b_j}, \ldots, x^{a_n}y^{b_j+v_n} \right\rangle. \tag{5.35}$$

Afirmamos que $H = \left\langle x^{a_j}y^{b_j} \right\rangle$. De fato, para todo $k = 1, \ldots, n$ temos que

$$x^{a_j}y^{b_j}x^{a_k}y^{b_j+v_k} = x^{a_k}y^{b_j+v_k}x^{a_j}y^{b_j} \Leftrightarrow \tag{5.36}$$

$$x^{a_j+a_k\alpha^{b_j}-a_j\alpha^{b_j+v_k}}y^{b_j+v_k} = x^{a_k}y^{b_j+v_k}. \tag{5.37}$$

Assim, um elemento $x^{a_k}y^{b_j+v_k}$ pertence ao subgrupo $\left\langle x^{a_j}y^{b_j} \right\rangle$ se, e somente se, existe um inteiro m tal que

$$\begin{aligned} x^{a_k}y^{b_j+v_k} &= (x^{a_j}y^{b_j})^m & (5.38)\\ &= x^{a_j\frac{\alpha^{mb_j}-1}{\alpha^{b_j}-1}}y^{mb_j}, & (5.39) \end{aligned}$$

ou equivalente,

$$\begin{cases} a_k \equiv a_j\frac{\alpha^{mb_j}-1}{\alpha^{b_j}-1} \bmod p \\ b_j + v_k \equiv mb_j \bmod q^s. \end{cases} \tag{5.40}$$

Do Sistema (5.40) temos a equação de congruência

$$a_k \equiv a_j + a_k\alpha^{b_j} - a_j\alpha^{b_j+v_k} \bmod p \tag{5.41}$$

que é verdadeira segundo a Equação (5.36). Com isso concluímos que $H \subset \left\langle x^{a_j} y^{b_j} \right\rangle$. A inclusão inversa é trivial, logo obtemos $H = \left\langle x^{a_j} y^{b_j} \right\rangle$. Mas pelo Lema 5.2.2, podemos escrever

$$H = \left\langle x^{a} y^{q^j} \right\rangle, \tag{5.42}$$

para algum $a \in \mathbb{Z}_p$ e $0 \leq j < t$. Portanto, se H é um subgrupo de G_t onde os geradores satisfazem as condições do Caso 2, então ou H é da forma

$$H = \left\langle x^{p^i}, y^{q^j} \right\rangle, \tag{5.43}$$

para algum $0 \leq i \leq 1$ e $0 \leq j < t$ ou da forma

$$H = \left\langle x^{a} y^{q^j} \right\rangle \tag{5.44}$$

para algum $a \in \mathbb{Z}_p$ e $0 \leq j < t$.

Por fim, consideremos o Caso 3. Este é uma mera consequência dos casos 1 e 2 já estudados. Com efeito, suponhamos que o subgrupo H possa ser escrito da forma $H = \left\langle x^{a_1} y^{b_1}, \ldots, x^{a_n} y^{b_n} \right\rangle$ para algum $n \in \mathbb{N}$ e tal que existam índices $1 \leq j_1 < j_2 < \ldots < j_k \leq n$ tais que $q^t \nmid b_{j_1}, \ldots, q^t \nmid b_{j_k}$. Por simplicidade suponhamos $j_1 = 1, \ldots, j_k = k$. Logo, podemos escrever o subgrupo H da seguinte forma

$$\begin{aligned} H &= \left\langle x^{a_1} y^{b_1}, \ldots, x^{a_k} y^{b_k}, x^{a_{k+1}} y^{v_{k+1} q^{j_{k+1}}}, \ldots, x^{a_n} y^{v_n q^{j_n}} \right\rangle && (5.45) \\ &= \left\langle \left\langle x^{a_1} y^{b_1}, \ldots, x^{a_k} y^{b_k} \right\rangle, \left\langle x^{a_{k+1}} y^{v_{k+1} q^{j_{k+1}}}, \ldots, x^{a_n} y^{v_n q^{j_n}} \right\rangle \right\rangle && (5.46) \\ &= \left\langle \left\langle x^{a_1} y^{b_1}, \ldots, x^{a_k} y^{b_k} \right\rangle, x^{p^\kappa} y^{q^\gamma} \right\rangle, && (5.47) \end{aligned}$$

pois, $\left\langle x^{a_{k+1}} y^{v_{k+1} q^{j_{k+1}}}, \ldots, x^{a_n} y^{v_n q^{j_n}} \right\rangle = \left\langle x^{p^\kappa} y^{q^\gamma} \right\rangle$ (Caso 1) para algum $0 \leq \kappa \leq 1$ e $t \leq \gamma \leq s$. Além disso, como discutido no Caso 2, podemos ter

$$\left\langle x^{a_1} y^{b_1}, \ldots, x^{a_k} y^{b_k} \right\rangle = \left\langle x^{p^i}, y^{q^j} \right\rangle, \tag{5.48}$$

para algum $0 \leq i \leq 1$ e $0 \leq j < t$ ou ainda

$$\left\langle x^{a_1}y^{b_1}, \ldots, x^{a_k}y^{b_k} \right\rangle = \left\langle x^a y^{q^j} \right\rangle, \tag{5.49}$$

para algum $a \in \mathbb{Z}_p$ e $0 \leq j < t$. Sendo assim, o subgrupo H pode ser escrito da forma

$$H = \left\langle x^{p^i}, y^{q^j}, x^{p^\kappa}y^{q^\gamma} \right\rangle = \left\langle x^{p^m}, y^{q^j} \right\rangle, \tag{5.50}$$

onde $m = \min\{i, \kappa\}$, ou da forma

$$H = \left\langle x^a y^{q^j}, x^{p^\kappa}y^{q^\gamma} \right\rangle. \tag{5.51}$$

Neste último caso, não é difícil verificar que $H = \left\langle x, y^{q^j} \right\rangle$ se $\kappa = 0$ ou $H = \left\langle x^a y^{q^j} \right\rangle$ se $\kappa = 1$, já que $y^{q^\gamma} \in \left\langle x^a y^{q^j} \right\rangle$. Portanto, se H é um subgrupo de G_t onde os geradores satisfazem as condições do Caso 3, então ou H é da forma

$$H = \left\langle x^{p^i}, y^{q^j} \right\rangle, \tag{5.52}$$

para algum $0 \leq i \leq 1$ e $0 \leq j < t$, ou da forma

$$H = \left\langle x^a y^{q^j} \right\rangle, \tag{5.53}$$

para algum $a \in \mathbb{Z}_p$ e $0 \leq j < t$.

Da discussão que tivemos ao longo desta seção segue o seguinte resultado.

Teorema 5.2.2 Os subgrupos de G_t possuem a forma descrita abaixo

i) $\left\langle x^a y^{q^j} \right\rangle$ para todo $a \in \mathbb{Z}_p$, $0 \leq j < t$;

ii) $\left\langle x^{p^i} y^{q^j} \right\rangle$ para todo $0 \leq i \leq 1$ e $t \leq j \leq s$;

iii) $\left\langle x^{p^i}, y^{q^j} \right\rangle$ para todo $0 \leq i \leq 1$ e $0 \leq j < t$.

■

5.3 Propriedades dos Subgrupos de G_t

Nesta seção, estudamos algumas propriedades do grupo G_t e seus subgrupos, como subgrupos normais, subgrupos de comutadores e nilpotência.

Um subgrupo H de G_t é dito normal se para todo $g \in G_t$, $gHg^{-1} = H$. Assim, seja H um subgrupo de G_t. Suponha que H pertença a classe ii), então $H = \left\langle x^{p^i} y^{q^j} \right\rangle$, para algum $0 \leq i \leq 1$ e $t \leq j \leq s$. Como x e y geram G_t, temos que H será normal em G_t, se e somente se, existirem elementos $g, h \in H$ tais que $x(x^{p^i} y^{q^j}) = gx$ e $y(x^{p^i} y^{q^j}) = hy$. Como x^{p^i} e y^{q^j} comutam para todo $t \leq j \leq s$, temos que $x(x^{p^i} y^{q^j}) = (x^{p^i} y^{q^j})x$. Definindo $g = x^{p^i} y^{q^j}$ temos claramente $g \in H$. Agora observe que

$$y(x^{p^i} y^{q^j}) = x^{\alpha p^i} y^{q^j} y. \tag{5.54}$$

Pelo Lema 5.2.1, temos que $x^{p^i}, y^{q^j} \in \left\langle x^{p^i} y^{q^j} \right\rangle$, logo $x^{\alpha p^i} y^{q^j} \in \left\langle x^{p^i} y^{q^j} \right\rangle$. Assim, definindo $h = x^{\alpha p^i} y^{q^j}$ temos $h \in H$, logo H é normal em G_t.

Por outro lado, se H for da classe i), então $H = \left\langle x^a y^{q^j} \right\rangle$ para algum $a \in \mathbb{Z}_p$ e $0 \leq j < t$. Suponhamos que existam $g, h \in H$ tais que

$$x(x^a y^{q^j}) = gx = (x^a y^{q^j})^k x \tag{5.55}$$

para algum $k \in \mathbb{Z}_{q^s}$ e

$$y(x^a y^{q^j}) = hy = (x^a y^{q^j})^{k'} y \tag{5.56}$$

para algum $k' \in \mathbb{Z}_{q^s}$. Da Eq. (5.55) temos o seguinte sistema de equações modulares

$$\begin{cases} a\frac{\alpha^{kq^j}-1}{\alpha^{q^j}-1} + \alpha^{kq^j} \equiv a+1 \bmod p \\ q^j k \equiv q^j \bmod q^s, \end{cases} \tag{5.57}$$

ou de forma equivalente,

$$a + 1 \equiv a + \alpha^{q^j} \bmod p. \tag{5.58}$$

Da Eq. (5.58) temos $q^t \mid q^j$, um absurdo, pois $j < t$. Logo, o subgrupo H não é normal em G_t. Observe que não precisamos verificar a existência de um elemento

$h \in H$ satisfazendo a Eq. (5.56), pois já sabemos que H não é normal.

Por fim, suponhamos que H seja da forma $\left\langle x^{p^i}, y^{q^j} \right\rangle$ para algum $0 \leq j < t$. Se $H = \left\langle x^p, y^{q^j} \right\rangle = \left\langle y^{q^j} \right\rangle$, então H pertence a classe i), logo não é normal. Assim, suponhamos $H = \left\langle x, y^{q^j} \right\rangle$, para todo $0 \leq j < t$. Se $j = 0$ então é óbvio que H é normal. Seja então $0 < j < t$; neste caso, o subgrupo H será normal em G_t se, e somente se, existirem $g, h \in H$ tais que $yx = gy$ e $xy^{q^j} = hx$. Temos que $yx = x^\alpha y$ e claramente $x^\alpha \in H$, pois $x \in H$. De $xy^{q^j} = hx$ temos $h = x^{1-\alpha^{q^j}} y^{q^j} \in H$, portanto, $H = \left\langle x, y^{q^j} \right\rangle$ é normal.

Assim, podemos resumir essa discussão com a seguinte proposição.

Proposição 5.3.1 Os subgrupos normais de G_t são da forma $\left\langle x, y^{q^j} \right\rangle$ para todo $j = 0, \ldots, t-1$ e $\left\langle x^{p^i} y^{q^j} \right\rangle$ para todo $i = 0, 1$ e $j = t, \ldots, s$.

■

A proposição a seguir mostra que G_t não é um grupo nilpotente.

Proposição 5.3.2 O grupo G_t é não nilpotente.

Demonstração: Note que $\left| \langle x^a y \rangle \right| = q^s$. Pelo Teorema 5.2.2, não existe um subgrupo próprio K de G_t tal que $\langle x^a y \rangle \leq K \leq G_t$, logo $\langle x^a y \rangle$ é maximal. Mas pela Proposição 5.3.1, $\langle x^a y \rangle$ não é normal, logo o grupo G_t é não nilpotente[1] .

■

Proposição 5.3.3 Seja $\mathcal{Z}(G_t)$ o centro de G_t. Então $\mathcal{Z}(G_t) = \left\langle y^{q^t} \right\rangle$.

Demonstração: Note que os elementos y^{q^t} e x comutam, logo $\left\langle y^{q^t} \right\rangle \subset \mathcal{Z}(G_t)$. Agora vamos mostrar que $\mathcal{Z}(G_t) \subset \left\langle y^{q^t} \right\rangle$. De fato, um elemento arbitrário $x^a y^b \in G_t$ está em $\mathcal{Z}(G_t)$ se e somente se,

$$(x^a y^b)x = x(x^a y^b) \tag{5.59}$$

e

$$(x^a y^b)y = y(x^a y^b). \tag{5.60}$$

[1] Aqui usamos um resultado da teoria de grupos nilpotentes que diz que um grupo G é nilpotente se, e somente se, todo subgrupo maximal de G é normal.

De (5.59) e (5.60) temos

$$\begin{cases} \alpha^b \equiv 1 \bmod p \\ a \equiv a\alpha \bmod p. \end{cases} \tag{5.61}$$

Como $\alpha \neq 1$, temos que um par (a, b) é uma solução de (5.61) se e somente se, $a = 0$ e $b = q^j$ para algum $t \leq j \leq s$. Assim, $\mathcal{Z}(G_t) \subset \left\langle y^{q^j} \right\rangle \subset \left\langle y^{q^t} \right\rangle$ e portanto, a igualdade $\mathcal{Z}(G_t) = \left\langle y^{q^t} \right\rangle$.

■

O subgrupo dos comutadores de G_t é denotado por G_t'. Então

Proposição 5.3.4 $G_t' = \langle x \rangle$.

Demonstração: Relembrando, o subgrupo de comutadores de G_t é definido como

$$G_t' = \{[g, h] = ghg^{-1}h^{-1} |\, g, h \in G_t\}.$$

Assim, se g é um elemento arbitrário de G_t então $g = x^{a(1-\alpha^d)+c(\alpha^b-1)}$, com $a, c \in \mathbb{Z}_p$ e $b, d \in \mathbb{Z}_{q^s}$. Mas isto implica que $G_t' \subset \langle x \rangle$. Agora note que $[y^{-1}, x] = x^{\alpha-1} \Rightarrow \langle x \rangle \subset G_t'$, e portanto, $G_t' = \langle x \rangle$.

■

Segue do Teorema 5.2.2, que o grupo G_t possui $\Omega(p)$ subgrupos. Desta forma, o PSO não pode ser resolvido eficientemente por um computador clássico fazendo consultas a todos os subgrupos de G_t. Além disso, o subgrupo de comutadores de G_t é o grupo $\langle x \rangle$ (Proposição 5.3.4). Logo, o algoritmo quântico dado por Ivanyos et al. (2003b), para o PSO sobre grupos cuja ordem do subgrupo de comutadores é polinomial no tamanho da entrada, não pode ser aplicado. Temos ainda que G_t não é um grupo nilpotente (Proposição 5.3.2), então, a estratégia dada por Ivanyos et al. (2007b), para grupos nilpotentes de classe 2, também não pode ser aplicada aqui.

No capítulo seguinte, apresentamos dois algoritmos quânticos para o PSO sobre os grupos G_t. Tomando $t = 1$, exibimos um algoritmo quântico exponencialmente mais rápido que qualquer algoritmo clássico para o PSO sobre G_t. Num

contexto mais geral, apresentamos um algoritmo em tempo subexponencial, que também apresenta um ganho sobre qualquer algoritmo clássico para o mesmo fim.

Capítulo 6

Algoritmos Quânticos para o PSO sobre o Grupo $\mathbb{Z}_p \rtimes \mathbb{Z}_{q^s}$

Neste capítulo apresentamos dois novos algoritmos quânticos que resolvem o PSO sobre o grupo $\mathbb{Z}_p \rtimes \mathbb{Z}_{q^s}$, onde p, q são números primos ímpares distintos e s um inteiro positivo qualquer. Esses algoritmos representam um avanço na busca de novos algoritmos quânticos para o PSO em grupos não abelianos.

Na Seção 6.2, descrevemos um algoritmo quântico em tempo subexponencial para $1 \leq t \leq s$. Este algoritmo tem como um dos pontos principais a utilização do algoritmo Peneira, apresentado no Capítulo 3. Na Seção 6.3, apresentamos um algoritmo quântico em tempo polinomial para o caso $t = 1$. Este algoritmo generaliza um resultado de Moore et al. (2004), para grupos q-edrais, que requer $s = 1$. Em alguns aspectos, esse resultado também generaliza o algoritmo apresentado por Bacon et al. (2005), que também requer $s = 1$.

6.1 Determinando Subgrupos Cíclicos

Nesta seção, mostraremos que o PSO em $\mathbb{Z}_p \rtimes \mathbb{Z}_{q^s}$ pode ser reduzido ao problema de encontrar subgrupos cíclicos da forma $\left\langle x^a y^{q^j} \right\rangle$, onde a é um elemento no grupo cíclico $\mathbb{Z}_p$ e $0 \leq j < t$.

Seja f a função oráculo que oculta o subgrupo H em $\mathbb{Z}_p \rtimes \mathbb{Z}_{q^s}$. Segue do Teorema 5.2.2 que existem três possibilidades para H:

1) H pertence a Classe 1 e temos que determinar os parâmetros a e j;

2) H pertence a Classe 2 e precisamos determinar os parâmetros i e j;

3) H pertence a Classe 3 e temos que determinar os parâmetros i and j.

O parâmetro a é o mais difícil de ser encontrado. Nós descrevemos o algoritmo que determina a na próxima seção.

A idéia geral do algoritmo para o PSO em $\mathbb{Z}_p \rtimes \mathbb{Z}_{q^s}$ é a seguinte. Seja

$$H_x = H \cap \langle x \rangle \quad \text{e} \quad H_y = H \cap \langle y \rangle \,. \tag{6.1}$$

Considere a função f_x definida por $f_x(a) = f(a, 0)$, que oculta o subgrupo H_x in $\mathbb{Z}_p$. Analogamente, seja f_y a função definida por $f_y(b) = f(0, b)$, que oculta o subgrupo H_y em $\mathbb{Z}_{q^s}$. A solução do PSO sobre o grupos abelianos $\mathbb{Z}_p$ e $\mathbb{Z}_{q^s}$ com funções oráculos f_x and f_y respectivamente, determina geradores para os subgrupos H_x and H_y. Estes subgrupos são da forma $H_x = \left\langle x^{p^i} \right\rangle$ e $H_y = \left\langle y^{q^j} \right\rangle$, para algum $0 \leq i \leq 1$ e $0 \leq j \leq s$. Assim, podemos supor os valores de i e j conhecidos. Se $j \geq t$, aprendemos que (Teorema 5.2.2),

$$H = \left\langle x^{p^i} y^{q^j} \right\rangle, \tag{6.2}$$

caso contrário, rodamos o algoritmo descrito na Seção 6.2 (Sec. 6.3 para $t = 1$). Se o número a correspondente a saída do algoritmo satisfaz $f(x^a y^{q^j}) = f(e)$, então sabemos que

$$H = \left\langle x^a y^{q^j} \right\rangle. \tag{6.3}$$

Se o algoritmo da Seção 6.2 (Sec. 6.3 para $t = 1$) retorna um valor de a tal que $f(x^a y^{q^j}) \neq f(e)$, então concluímos que

$$H = \left\langle x^{p^i}, y^{q^j} \right\rangle. \tag{6.4}$$

Vimos que se o subgrupo oculto H for da forma $\left\langle x^{p^i} y^{q^j} \right\rangle$ ou $\left\langle x^{p^i}, y^{q^j} \right\rangle$, os

parâmetros i e j podem ser facilmente determinados através de reduções ao PSO abeliano. O caso mais difícil é quando H envolve o parâmetro $a \in \mathbb{Z}_p$. Neste caso, exibimos dois algoritmos quânticos (Sec. 6.2 e Sec. 6.3) para determinar o valor de a. Desta forma, podemos assumir que o PSO sobre $\mathbb{Z}_p \rtimes \mathbb{Z}_{q^s}$ se reduz ao problema de encontrar o gerador do subgrupo cíclico $H = \left\langle x^a y^{q^j} \right\rangle$.

Finalizamos esta seção com uma análise da complexidade do algoritmo *clássico* para o PSO sobre $\mathbb{Z}_p \rtimes \mathbb{Z}_{q^s}$. Segue do Teorema 5.2.2, que $\mathbb{Z}_p \rtimes \mathbb{Z}_{q^s}$ possui $\Omega(p)$ subgrupos. Portanto, o PSO não pode ser resolvido eficientemente por um computador clássico fazendo uma busca exaustiva aos subgrupos de $\mathbb{Z}_p \rtimes \mathbb{Z}_{q^s}$. Outros métodos, tais como aqueles apresentados em Ivanyos et al. (2003b, 2007b), para grupos com subgrupos de comutadores de tamanho polinomial e para grupos nilpotentes de classe 2, não podem ser aplicados aqui.

O PSO em $\mathbb{Z}_p \rtimes \mathbb{Z}_{q^s}$ pode ser resolvido classicamente, encontrando, dois elementos distintos g_1 e g_2 em $\mathbb{Z}_p \rtimes \mathbb{Z}_{q^s}$, tais que $f(g_1) = f(g_2)$. De fato, achar tal colisão é suficiente para resolver o PSO. Para cada $0 \leq j \leq s$, a função f é prometida ocultar o subgrupo $H = \left\langle x^a y^{q^j} \right\rangle$. Então, se conhecemos elementos g_1 e g_2 tais que $f(g_1) = f(g_2)$ obtemos $g_2^{-1} g_1 \in H$. Escrevendo $g_2^{-1} g_1 = x^u y^v$ para algum $u \in \mathbb{Z}_p$ e $v \in \mathbb{Z}_{q^s}$, temos que $g_2^{-1} g_1 \in H$ se e somente se,

$$\begin{cases} u \equiv a \frac{\alpha^{kq^j}-1}{\alpha^{q^j}-1} \bmod p \\ v \equiv kq^j \bmod q^s, \end{cases} \tag{6.5}$$

para algum $k = 0, \ldots, q^{s-j} - 1$. Do sistema (6.5) segue que

$$a \equiv u \frac{\alpha^{q^j}-1}{\alpha^v - 1} \bmod p \Leftrightarrow q^t \nmid v. \tag{6.6}$$

Como $\mathrm{ord}(\alpha) = q^t$, a Eq. (6.6) só faz sentido se $q^t \nmid v$. Neste caso, obtemos o valor de a resolvendo o lado direito da Eq. (6.6). Mas qual a probabilidade de $q^t \nmid v$? Suponha que v seja um múltiplo de q^t, isto é, $q^t \mid v$. Como $v \in \mathbb{Z}_{q^s}$, existem q^{s-t}

múltiplos de v em $\mathbb{Z}_{q^s}$. Logo, a probabilidade de $v \in \mathbb{Z}_{q^s}$ e ser um múltiplo de q^t é

$$\frac{q^{s-t}}{q^s} = \frac{1}{q^t}, \tag{6.7}$$

e portanto, a probabilidade de $v \in \mathbb{Z}_{q^s}$ e não ser um múltiplo de q^t é

$$1 - \frac{1}{q^t}. \tag{6.8}$$

Assim, com probabilidade $1 - \frac{1}{q^t} \approx 1$ (estamos interessados em valores de q muito grandes), o PSO em $\mathbb{Z}_p \rtimes \mathbb{Z}_{q^s}$, reduz-se ao problema de encontrar elementos $g_1 \neq g_2$ tais que $f(g_1) = f(g_2)$. Este problema é conhecido na literatura como *problema de colisão*. Neste caso, a função f é dita q^{s-j}-para-um[1] e a complexidade clássica deste problema é $\Theta(\sqrt{pq^j})$, veja Kutin (2005). Portanto, o limite inferior do algoritmo clássico para o PSO em $\mathbb{Z}_p \rtimes \mathbb{Z}_{q^s}$ é $\Omega(\sqrt{p})$.

6.2 O Algoritmo Peneira para o PSO sobre $\mathbb{Z}_p \rtimes \mathbb{Z}_{q^s}$

Dada uma função f que oculta o subgrupo $H = \left\langle x^a y^{q^j} \right\rangle$ em $\mathbb{Z}_p \rtimes \mathbb{Z}_{q^s}$, nosso objetivo é achar o valor de a. Mostraremos como determinar a em tempo subexponencial e com alta probabilidade, utilizando o algoritmo Peneira, apresentado no Capítulo 3. A descrição do algoritmo é idêntica ao do algoritmo para o PSO sobre o grupo QD_n, visto na Seção 3.2.2. Vamos ao algoritmo:

(1) Prepare o estado quântico

$$|\Psi_1\rangle = \frac{1}{\sqrt{2p}} \sum_{m=0}^{p-1} \sum_{n=0}^{1} |m\rangle\,|n\rangle \left| f(x^m y^{nq^j}) \right\rangle. \tag{6.9}$$

Geralmente, os algoritmos quânticos para o PSO iniciam numa superposição sobre todos os elementos do grupo. Aqui, diferentemente, nós iniciamos o computador quântico num estado que é uma superposição sobre uma parte do grupo.

[1] Uma função $f : X \to Y$ é dita ser r-para-um, quando existem r elementos em X que são levados no mesmo elemento em Y.

Agora, defina $m = m_0 + na \bmod p$, logo reescrevendo o estado $|\Psi_1\rangle$ temos

$$|\Psi_1\rangle = \frac{1}{\sqrt{2p}} \sum_{m_0=0}^{p-1} \sum_{n=0}^{1} |m_0 + na\rangle \, |n\rangle \left| f(x^{m_0+na} y^{nq^j}) \right\rangle . \tag{6.10}$$

Observe que $x^{na} y^{nq^j} \in H$ para todo $n = 0, 1$, portanto,

$$f(x^{m_0} x^{na} y^{nq^j}) = f(x^{m_0}).$$

Assim, $|\Psi_1\rangle$ fica

$$|\Psi_1\rangle = \frac{1}{\sqrt{2p}} \sum_{m_0=0}^{p-1} \sum_{n=0}^{1} |m_0 + na\rangle \, |n\rangle \, |f(x^{m_0})\rangle . \tag{6.11}$$

(2) Meça o terceiro registrador do estado $|\Psi_1\rangle$. O resultado da medida é

$$|\Psi_2\rangle = \frac{1}{\sqrt{2}} \sum_{n=0}^{1} |m_0' + na\rangle \, |n\rangle , \tag{6.12}$$

para algum m_0' uniformemente distribuído sobre $\mathbb{Z}_p$.

(3) Aplique a transformada de Fourier, $F_{\mathbb{Z}_p}$, ao primeiro registrador do estado $|\Psi_2\rangle$. O resultado é

$$\begin{aligned} |\Psi_3\rangle &= \frac{1}{\sqrt{2}} \sum_{n=0}^{1} \left(\frac{1}{\sqrt{p}} \sum_{k=0}^{p-1} \omega_p^{(m_0'+na)k} \, |k\rangle \right) |b\rangle \\ &= \frac{1}{\sqrt{p}} \sum_{k=0}^{p-1} {\omega_p}^{m_0' k} \, |k\rangle \left(\frac{1}{\sqrt{2}} \sum_{n=0}^{1} {\omega_p}^{kna} \, |n\rangle \right), \end{aligned} \tag{6.13}$$

onde $\omega_p = e^{\frac{2\pi i}{p}}$ é a p-ésima raíz primitiva da unidade.

(4) Meça o primeiro registrador do estado $|\Psi_3\rangle$. O resultado é o estado

$$|\Psi_4\rangle = \frac{1}{\sqrt{2}} \left(|0\rangle + \omega_p^{k_0 a} \, |1\rangle \right), \tag{6.14}$$

onde $k_0 \in \mathbb{Z}_p$ é um número uniformemente randômico.

A discussão acima está sintetizada no Algoritmo 6.2.1 descrito abaixo:

Algoritmo 6.2.1

Entrada: Inteiros p, q, s, j e uma função $f : \mathbb{Z}_p \rtimes \mathbb{Z}_{q^s} \to X$, onde X é um conjunto finito qualquer.

Saída: Um estado de um q-bit.

1. Prepare o estado

$$\frac{1}{\sqrt{2p}} \sum_{m=0}^{p-1} \sum_{n=0}^{1} |m\rangle |n\rangle \left| f(x^m y^{nq^j}) \right\rangle .$$

2. Meça o terceiro registrador.
3. Aplique a transformada de Fourier $F_{\mathbb{Z}_p}$ ao primeiro registrador.
4. Meça o primeiro registrador.

A saída do Algoritmo 6.2.1 (a menos de um fator de fase global) é o estado

$$|\psi_k^{a,p}\rangle = \frac{1}{\sqrt{2}} \Big(|0\rangle + e^{\frac{2\pi i a k}{p}} |1\rangle \Big), \tag{6.15}$$

para algum $0 \leq k < p$ randomicamente distribuído. Note que, quando o estado $|\psi_k^{a,p}\rangle$ é obtido, aprendemos sobre os valores de p e k, mas não sabemos nada sobre o parâmetro a, que determina o subgrupo oculto $\left\langle x^a y^{q^j} \right\rangle$. Então, para cada $0 \leq \gamma \leq \lceil \log p \rceil$, defina a função $f^{(\gamma)} : \mathbb{Z}_p \rtimes \mathbb{Z}_{q^s} \to X$ como

$$f^{(\gamma)}(x^a y^b) = f(x^{a2^{-\gamma}} y^b). \tag{6.16}$$

Não é difícil verificar que $f^{(\gamma)}$ oculta o subgrupo

$$H_\gamma = \left\{ x^{a2^\gamma S(k)} y^{kq^j} : k = 0, \ldots, q^{s-j} - 1 \right\}, \tag{6.17}$$

onde

$$S(k) = \frac{\alpha^{kq^j} - 1}{\alpha^{q^j} - 1}. \tag{6.18}$$

Então, para cada $0 \leq \gamma \leq \lceil \log p \rceil$, use a função $f^{(\gamma)}$ como entrada para o Algoritmo 6.2.1. Desta vez, a saída do Algoritmo 6.2.1 é um estado da forma $\left| \psi_k^{2^\gamma a,p} \right\rangle$, onde k está uniformemente distribuído sobre $\mathbb{Z}_p$. Nosso objetivo é obter o estado $\left| \psi_1^{2^\gamma a,p} \right\rangle$,

pois, o valor de a pode ser obtido com alta probabilidade, a partir do conjunto

$$\left\{ \left| \psi_1^{2^\gamma a,p} \right\rangle, \gamma = 0, \ldots, n = \lceil \log p \rceil \right\}, \tag{6.19}$$

pela aplicação da transformada de Fourier. De fato, aplicando a transformada de Fourier inversa ao produto tensorial

$$\begin{aligned} |\psi\rangle &= \left| \psi_1^{2^0 a,p} \right\rangle \otimes \left| \psi_1^{2^1 a,p} \right\rangle \otimes \ldots \otimes \left| \psi_1^{2^n a,p} \right\rangle \\ &= \frac{1}{\sqrt{2}} \Big(|0\rangle + e^{\frac{2\pi i a}{p}} |1\rangle \Big) \otimes \frac{1}{\sqrt{2}} \Big(|0\rangle + e^{\frac{2\pi i 2a}{p}} |1\rangle \Big) \otimes \ldots \otimes \frac{1}{\sqrt{2}} \Big(|0\rangle + e^{\frac{2\pi i 2^n a}{p}} |1\rangle \Big) \\ &= \frac{1}{2^{\frac{n+1}{2}}} \sum_{k=0}^{2^n} e^{\frac{2\pi i a k}{p}} |k\rangle, \end{aligned}$$

obtemos o valor de a com alta probabilidade.

Acontece que, a probabilidade de obter o estado $\left| \psi_1^{2^\gamma a,p} \right\rangle$ direto do Algoritmo 6.2.1 é $1/p$, que é exponencialmente pequena. Vamos mostrar como obter o estado $\left| \psi_1^{2^\gamma a,p} \right\rangle$, em tempo subexponencial, usando um computador quântico.

Primeiro, para duas amostras $\left| \psi_{k_1}^{2^\gamma a,p} \right\rangle$ e $\left| \psi_{k_2}^{2^\gamma a,p} \right\rangle$ do Algoritmo 6.2.1, aplicamos a porta CNOT ao produto tensorial $\left| \psi_{k_1}^{2^\gamma a,p} \right\rangle \otimes \left| \psi_{k_2}^{2^\gamma a,p} \right\rangle$ usando o primeiro q-bit como q-bit de controle. O resultado é o seguinte estado

$$\frac{1}{2} \big(|00\rangle + e^{2\pi i \frac{k_2 2^\gamma a}{p}} |01\rangle + e^{2\pi i \frac{k_1 2^\gamma a}{p}} |11\rangle + e^{2\pi i \frac{(k_1+k_2) 2^\gamma a}{p}} |10\rangle \big). \tag{6.20}$$

Medindo o segundo q-bit na base computacional, a menos de um fator de fase global, obtemos o estado $\left| \psi_{k_1-k_2}^{2^\gamma a,p} \right\rangle$, com probabilidade 1/2. Esse procedimento, que envolve produto tensorial de estados quânticos e medida na base computacional, damos o nome de *combine-and-measure*.

Agora, chamamos o Algoritmo 6.2.1, $2^{O(\sqrt{\log p})}$ vezes, tomando a função $f^{(\gamma)}$ como entrada do algoritmo, e cada vez produzindo um estado quântico de um q-bit, $\left| \psi_k^{2^\gamma a,p} \right\rangle$. Seja L_0 o conjunto formado por todos esses estados. Como na Seção 3.2.2, o Algoritmo Peneira acha pares $\left| \psi_{k_1}^{2^\gamma a,p} \right\rangle$ e $\left| \psi_{k_2}^{2^\gamma a,p} \right\rangle$ no conjunto L_0 tais que os primeiros $m = \left\lceil \sqrt{\log p - 1} \right\rceil$ bits de k_1 e k_2 são idênticos. Então, para

cada par, aplicamos o procedimento combine-and-measure, descrito no parágrafo anterior, para produzir, com probabilidade 1/2, o estado $\left|\psi_{k_1-k_2}^{2^\gamma a,p}\right\rangle$. O conjunto L_1 consiste dos estados da forma $\left|\psi_{k}^{2^\gamma a,p}\right\rangle$, tais que os m bits mais significativos de k são todos iguais a zero. Repetindo esse procedimento m vezes, obtemos com alta probabilidade, um conjunto L_m, que possui pelo menos um estado da forma $\left|\psi_{1}^{2^\gamma a,p}\right\rangle$. A análise de complexidade do nosso algoritmo é idêntica à análise do algoritmo Peneira, feita na Seção 3.1.1. Assim, podemos enunciar o

Teorema 6.2.1 O PSO sobre o grupo $\mathbb{Z}_p \rtimes \mathbb{Z}_{q^s}$, onde p, q são números primos ímpares distintos e s um inteiro positivo qualquer, tem um algoritmo quântico com complexidade de tempo $2^{O(\sqrt{\log p})}$.

6.3 O Caso $H = \langle x^a y \rangle$

Nesta seção, apresentamos um algoritmo quântico eficiente que resolve o PSO no grupo $\mathbb{Z}_p \rtimes \mathbb{Z}_{q^s}$, com $q \mid p-1$ e $p/q = \text{poli}(\log p)$. Esta classe de grupos é obtida escolhendo $t = 1$ na Eq. (5.17).

De acordo com a Seção 6.1, o PSO em $\mathbb{Z}_p \rtimes \mathbb{Z}_{q^s}$ se reduz ao problema de encontrar subgrupos cíclicos de ordem potência de primo, da forma $H = \langle x^a y \rangle$. A partir dessa redução, exibimos um procedimento que, dada uma função f que oculta o subgrupo $H = \langle x^a y \rangle$ em $\mathbb{Z}_p \rtimes \mathbb{Z}_{q^s}$, determina de forma eficiente e com alta probabilidade, o valor de a, quando $q \mid p-1$ e $p/q = \text{poli}(\log p)$. Note que neste caso, a ordem de H é q^s. O procedimento é o seguinte:

(1) Inicie o computador quântico no estado

$$|\Psi_1\rangle = \frac{1}{\sqrt{qp}} \sum_{m=0}^{p-1} \sum_{n=0}^{q-1} |m\rangle\,|n\rangle\,|f(x^m y^n)\rangle\,. \tag{6.21}$$

As operações aritméticas no primeiro(segundo) ket são feitas módulo $p(q)$. Observe que as classes laterais à esquerda de H são da forma

$$x^{m_0} H = \left\{ x^{m_0 + aS(n)} y^n, n = 0, \ldots, q^s - 1 \right\}, \tag{6.22}$$

onde $m_0 \in \mathbb{Z}_p$ e

$$S(n) = \frac{\alpha^n - 1}{\alpha - 1} \bmod p. \tag{6.23}$$

Além disso, a função $S(n)$ definida em (6.23) é injetiva em $\mathbb{Z}_q$. De fato, sejam $n, m \in \mathbb{Z}_q$ então

$$\begin{aligned} S(n) = S(m) &\Rightarrow S(n) - S(m) = \frac{\alpha^{n-m} - 1}{\alpha - 1} = 0 && (6.24)\\ &\Rightarrow \alpha^{n-m} = 1 \bmod p && (6.25)\\ &\Rightarrow q \mid n - m && (6.26)\\ &\Rightarrow m \equiv n \bmod q. && (6.27) \end{aligned}$$

Logo, $S(n)$ é injetiva, para todo $n \in \mathbb{Z}_q$.

(2) Meça o terceiro registrador do estado $|\Psi_1\rangle$ na base computacional. O resultado da medida é

$$|\Psi_2\rangle = \frac{1}{\sqrt{q}} \sum_{n=0}^{q-1} |m_0 + aS(n)\rangle \, |n\rangle \,, \tag{6.28}$$

para algum $0 \leq m_0 < p$ randomicamente distribuído. Note que nós descartamos o terceiro registrador, pois, o mesmo não será relevante na computação a seguir.

(3) Aplique a transformada de Fourier, $F_{\mathbb{Z}_p} \otimes I$, ao estado $|\Psi_2\rangle$. O resultado é

$$|\Psi_3\rangle = \frac{1}{\sqrt{qp}} \sum_{k=0}^{p-1} \sum_{n=0}^{q-1} \omega_p^{k(m_0 + aS(n))} \, |k\rangle \, |n\rangle \,, \tag{6.29}$$

onde ω_p é a p-ésima raíz primitiva da unidade.

(4) Meça o primeiro registrador na base computacional. Assuma que o resultado da medida seja algum elemento $k_0 \in \mathbb{Z}_p^*$. Então, tem-se o estado

$$|\Psi_4\rangle = \frac{1}{\sqrt{q}} \sum_{n=0}^{q-1} \omega_p^{k_0(m_0 + aS(n))} \, |k_0\rangle \, |n\rangle \,. \tag{6.30}$$

A probabilidade de obter o estado $|\Psi_4\rangle$ é $1 - \frac{1}{p}$.

(5) Aplique o operador unitário U, definido por

$$U|m\rangle|n\rangle = |mS(n)\rangle \left| n - S^{-1}\left(\frac{mS(n)}{k_0}\right)\right\rangle, \tag{6.31}$$

ao estado $|\Psi_4\rangle$. Esta aplicação produz o estado

$$|\Psi_5\rangle = \frac{1}{\sqrt{q}} \sum_{n=0}^{q-1} \omega_p^{k_0(m_0+aS(n))} |k_0 S(n)\rangle |0\rangle . \tag{6.32}$$

Mostraremos a seguir como determinar o valor de a a partir do estado $|\Psi_5\rangle$. Antes, mostraremos que o operador U definido em (6.31) é de fato um operador unitário. Para isso, considere o operador U_1 definido por

$$U_1|m\rangle|n\rangle = |mS(n) \bmod p\rangle |n\rangle . \tag{6.33}$$

Temos que U_1 é unitário. De fato, note

$$(U|m\rangle|n\rangle)^\dagger = (|mS(n)\rangle|n\rangle)^\dagger = \langle n|\langle mS(n)| . \tag{6.34}$$

Assim, o produto interno

$$\begin{aligned} \langle n|\langle mS(n)|U_1|m'\rangle|n'\rangle &= \langle n|\langle mS(n)|m'S(n')\rangle|n'\rangle \\ &= \langle n|n'\rangle\langle mS(n)|m'S(n')\rangle \\ &= \delta_{n,n'}\delta_{m,m'}, \end{aligned}$$

para todo $m, m' \in \mathbb{Z}_p$ e $n, n' \in \mathbb{Z}_q$. Logo U_1 preserva o produto interno entre dois vetores quaisquer, portanto, é unitário. Analogamente, podemos mostrar que o operador U_2 definido por

$$U_2|m\rangle|n\rangle = |n\rangle \left| n - S^{-1}\left(\frac{m}{k_0}\right)\right\rangle \tag{6.35}$$

também é unitário.

Observe que a unitariedade dos operadores U_1 e U_2, definidos acima, segue do fato da função $S(n)$ ser injetiva em $\mathbb{Z}_q$. Note também que $S^{-1}(n)$ pode ser calculada eficientemente utilizando o algoritmo de Shor para cálculo de logaritmo discreto. As potências de α podem ser calculadas eficientemente pelo método do quadrado repetido[2] . Assim, os operadores unitários U_1 e U_2 podem ser implementados eficientemente num computador quântico.

Por fim, fazendo $U = U_2U_1$ temos claramente que U é unitário, pois, U_1 e U_2 os são.

Nosso objetivo agora é obter o parâmetro a, a partir do estado $|\Psi_5\rangle$. Para isso, usaremos o seguinte argumento, presente em Bacon et al. (2005). Considere o estado

$$|\tilde{a}\rangle = \frac{1}{\sqrt{p}} \sum_{j=0}^{p-1} \omega_p^{ja} |j\rangle . \tag{6.36}$$

Aplicando a transformada de Fourier inversa, $F_{\mathbb{Z}_p}^{\dagger}$, ao estado $|\tilde{a}\rangle$, obtemos um novo estado da forma

$$\begin{aligned} |\Psi\rangle &= \frac{1}{p} \sum_{j\in\mathbb{Z}_p} \omega_p^{ja} \sum_{k\in\mathbb{Z}_p} \omega_p^{-kj} |k\rangle & (6.37)\\ &= \frac{1}{p} \sum_{j\in\mathbb{Z}_p} \sum_{k\in\mathbb{Z}_p} \omega_p^{j(a-k)} |k\rangle & (6.38)\\ &= \sum_{k\in\mathbb{Z}_{p^r}} \left(\frac{1}{p} \sum_{j\in\mathbb{Z}_p} \omega_p^{j(a-k)} \right) |k\rangle . & (6.39) \end{aligned}$$

O termo dentro do parêntese é uma soma geométrica, onde

$$\frac{1}{p} \sum_{j\in\mathbb{Z}_p} \omega_p^{j(a-k)} = \begin{cases} 1 & \text{se } p \mid a-k \\ 0 & \text{caso contrário.} \end{cases} \tag{6.40}$$

[2] O método do quadrado repetido consiste em calcular a congruência de $b^r \bmod n$, sendo b, r e n inteiros positivos grandes. Por exemplo, podemos calcular eficientemente $10^{135} \bmod 7$ da seguinte forma: $10^{135} \equiv (10^6)^{22}10^3 \equiv 1^{22}10^3 \equiv 6 \bmod 7$. Logo, o resto da divisão de 10^{135} por 7 é 6.

Assim temos

$$|\Psi\rangle = \sum_{k\in\mathbb{Z}_p} |k\rangle\,, \tag{6.41}$$

onde k é tal que

$$k \equiv a \bmod p. \tag{6.42}$$

Então, medindo o primeiro registrador, obtemos o valor desejado a com probabilidade 1.

Vimos que o estado $|\tilde{a}\rangle$ guarda toda a informação a cerca do parâmetro a. O que aprendemos sobre a medindo o estado $|\Psi_5\rangle$? Existe alguma relação entre os estados $|\tilde{a}\rangle$ e $|\Psi_5\rangle$? Esta pergunta pode ser respondida através do conceito de *Fidelidade Quântica* [3] .

A fidelidade entre os estados quânticos $|\tilde{a}\rangle$ e $|\Psi_5\rangle$ (descartando o ket $|0\rangle$ de $|\Psi_5\rangle$) é dada por

$$\begin{aligned} |\langle\tilde{a}\,|\Psi_5\rangle| &= \left|\frac{1}{\sqrt{pq}}\sum_{m=0}^{p-1}\sum_{n=0}^{q-1}\omega_p^{-am+m_0k_0+aS(n)k_0}\langle m\,|k_0S(n)\rangle\right| && (6.43)\\ &= \left|\frac{1}{\sqrt{pq}}q\omega_p^{m_0k_0}\right| && (6.44)\\ &= \sqrt{\frac{q}{p}}. && (6.45)\end{aligned}$$

Então, aplicando a transformada de Fourier inversa, $F^{\dagger}_{\mathbb{Z}_p}$, no estado $|\Psi_5\rangle$ e depois medindo o resultado na base computacional, obtemos com probabilidade

$$|\langle\tilde{a}\,|\Psi_5\rangle|^2 = \frac{q}{p}, \tag{6.46}$$

o valor de a.

Como a probabilidade de obtermos o estado $|\Psi_4\rangle$ é $1-\frac{1}{p}$, temos que a pro-

[3] Na Teoria da Informação Quântica, Fidelidade Quântica, ou simplesmente Fidelidade, é uma medida que diz quão próximos são dois estados quânticos. Para dois estados puros $\rho = |\phi\rangle\langle\phi|$ e $\sigma = |\psi\rangle\langle\psi|$, sua fidelidade é definida como

$$F(\rho,\sigma) = \mathrm{Tr}(\rho\sigma\rho)^{1/2} = \mathrm{Tr}(|\phi\rangle\langle\phi|\psi\rangle\langle\psi|\phi\rangle\langle\phi|)^{1/2} = |\langle\phi|\psi\rangle|.$$

Se $|\phi\rangle$ é um auto-estado de um observável, e o sistema é preparado no estado $|\psi\rangle$, então $F(\rho,\sigma)^2$ é a probabilidade do sistema estar no estado $|\phi\rangle$ após a medida.

babilidade total de sucesso de obtermos o valor de a é

$$\left(1-\frac{1}{p}\right)\frac{q}{p}=\frac{(p-1)q}{p^2}. \tag{6.47}$$

Todo o procedimento desenvolvido nesta seção pode ser reunido no Algoritmo 6.3.1 descrito a seguir:

Algoritmo 6.3.1 Algoritmo para o PSO no grupo $\mathbb{Z}_p \rtimes \mathbb{Z}_{q^s}$.

Entrada: Inteiros p, q, s e uma função f que oculta o subgrupo $H = \langle x^a y \rangle$.
Saída: Os geradores do subgrupo oculto H.

1. Prepare o estado

$$\frac{1}{\sqrt{qp}}\sum_{m=0}^{p-1}\sum_{n=0}^{q-1}|m\rangle\,|n\rangle\,|f(x^m y^n)\rangle$$

2. Meça o terceiro registrador na base computacional e em seguida descarte-o:

$$\frac{1}{\sqrt{q}}\sum_{n=0}^{q-1}|m_0+aS(n)\rangle\,|n\rangle\,,\ \text{onde } S(n)=\frac{\alpha^n-1}{\alpha-1}.$$

3. Aplique $F_{\mathbb{Z}_p}$ ao primeiro registrador e em seguida meça-o:

$$\frac{1}{\sqrt{q}}\sum_{n=0}^{q-1}\omega_p^{k_0(m_0+aS(n))}\,|k_0\rangle\,|n\rangle\,.$$

4. Aplique o operador unitário $U\,|m\rangle\,|n\rangle = |mS(n)\rangle\,\left|n - S^{-1}\left(\frac{mS(n)}{k_0}\right)\right\rangle$:
5. Aplique $F^{\dagger}_{\mathbb{Z}_p}$ e meça o resultado.

6.3.1 Análise da Complexidade Computacional do Algoritmo

Na seção anterior exibimos um algoritmo quântico (Algoritmo 6.3.1) para o PSO sobre $\mathbb{Z}_p \rtimes \mathbb{Z}_{q^s}$. Nesta seção, mostramos que a complexidade computacional de tal algoritmo é polilogarítmica na ordem do grupo.

O Algoritmo 6.3.1 faz uso da transformada de Fourier sobre o grupo abeliano $\mathbb{Z}_p$, que pode ser implementada eficientemente em um computador quântico, Lomont (2004). Desta forma, podemos supor sua complexidade sendo $O(1)$, por não representar danos ao algoritmo. Assim, podemos nos preocupar apenas com o número de consultas à função separadora de classes laterais f. Este número é da ordem

$O(\text{poli}(\log p))$, como veremos a seguir.

Vimos que a probabilidade total de sucesso de obtermos o parâmetro a rodando o Algoritmo 6.3.1 é $\frac{(p-1)q}{p^2}$. Esta é uma boa probabilidade se fixarmos $q = p/\text{poli}(\log p)$. De fato, rode o Algoritmo 6.3.1, l vezes. A probabilidade de obtermos o valor de a, pelo menos uma vez, é

$$1 - \left(1 - \frac{(p-1)q}{p^2}\right)^l, \tag{6.48}$$

onde $\left(1 - \frac{(p-1)q}{p^2}\right)^l$ representa a probabilidade de não obtermos o valor de a todas as l vezes que rodamos o algoritmo. Além disso, o termo $\frac{(p-1)q}{p^2}$ é sempre menor que 1, logo podemos usar a expansão binomial para obtermos a seguinte aproximação

$$\left(1 - \frac{(p-1)q}{p^2}\right)^l \approx 1 - l\frac{(p-1)q}{p^2}. \tag{6.49}$$

Assim, para que o Algoritmo 6.3.1 retorne o valor de a, após l repetições e com probabilidade maior ou igual que $1/2$, devemos ter

$$1 - \left(1 - l\frac{(p-1)q}{p^2}\right) \geq \frac{1}{2}, \tag{6.50}$$

ou equivalente,

$$\begin{aligned} l \geq \frac{p^2}{2(p-1)q} &= \frac{p}{2(p-1)}\frac{p}{q} && (6.51)\\ &= \frac{p}{2(p-1)}\text{poli}(\log p) && (6.52)\\ &= O(\text{poli}(\log p)). && (6.53) \end{aligned}$$

Observe que assumimos uma probabilidade de sucesso $1/2$, pois, a aplicação do Limite de Chernoff amplifica essa probabilidade para próxima de 1 com poucas repetições do algoritmo, Kitaev et al. (2002); Chuang e Nielsen (2000).

Com isso, podemos enunciar o nosso resultado principal.

Teorema 6.3.1 Existe um algoritmo quântico que resolve em tempo polinomial e

com probabilidade de sucesso maior que $1/2$, o PSO sobre o grupo $\mathbb{Z}_p \rtimes \mathbb{Z}_{q^s}$, com $q \mid (p-1)$ e $p/q = \text{poli}(\log p)$, onde p, q são números primos ímpares distintos e s um inteiro positivo qualquer.

Capítulo 7

Conclusão

O principal objetivo desta tese foi encontrar algoritmos quânticos para o PSO em certas classes de grupos não abelianos. Para grupos finitos abelianos, o PSO pode ser resolvido eficientemente em um computador quântico, enquanto, nenhuma solução geral é conhecida para o caso de grupos não abelianos. Nesta tese de doutorado apresentamos nossa contribuição, no que diz respeito ao incremento do número de grupos onde o PSO pode ser resolvido eficientemente por um computador quântico.

No Capítulo 3, apresentamos algoritmos quânticos para o PSO sobre uma família de grupos não abelianos, de ordem 2^{n+1}, que possuem subgrupos normais de ordem 2^n. Conhecendo a estrutura dos subgrupos do grupo em estudo, nós mostramos que o PSO se reduz ao problema de encontrar subgrupos cíclicos. Então, adaptamos os resultados apresentados em Kuperberg (2005), para o PSO no grupo diedral, e exibimos um algoritmo quântico com complexidade de tempo subexponencial.

No Capítulo 4, mostramos que existe um algoritmo quântico eficiente para o PSO sobre o produto semidireto de grupos $\mathbb{Z}_N^m \rtimes_\phi \mathbb{Z}_p$, onde p é um número primo ímpar, m, N inteiros positivos, e N fatorado como $N = p_1^{r_1}...p_n^{r_n}$, com $1 \leq r_1 \leq \ldots \leq r_n$ onde $p \nmid p_i^k - 1$ para todo $i = 1, \ldots, n$ e $k = 1, \ldots, m$. Usando um ferramental de teoria de grupos, mostramos que o grupo $\mathbb{Z}_N^m \rtimes \mathbb{Z}_p$ é isomorfo a um grupo G, que é um produto direto de um grupo abeliano por um grupo não

abeliano. Então, nós resolvemos o PSO em G, determinando uma solução eficiente para o PSO em cada parte do produto direto grupos. Mais tarde, verificamos que o grupo $\mathbb{Z}_N^m \rtimes_\phi \mathbb{Z}_p$ é nilpotente de classe 2, recaindo numa classe de grupos onde o PSO pode ser revolvido eficientemente por um computador quântico.

No Capítulo 6, apresentamos dois algoritmos quânticos para o PSO sobre os grupos $\mathbb{Z}_p \rtimes \mathbb{Z}_{q^s}$, onde p, q são números primos ímpares distintos e s um inteiro positivo qualquer, utilizando a transformada de Fourier abeliana. Usando a classificação dos subgrupos de $\mathbb{Z}_p \rtimes \mathbb{Z}_{q^s}$, Teorema 5.2.2, nós simplificamos o PSO ao problema de encontrar subgrupos cíclicos com ordem potência de número primo. O primeiro algoritmo possui complexidade de tempo subexponencial e trabalha com qualquer homomorfismo que define o produto semidireto de grupos. O segundo, é um algoritmo em tempo polinomial para uma classe especial de grupos metacíclicos com $q \mid (p-1)$ e $p/q = \text{poli}(\log p)$. Ambos os algoritmos são probabilísticos, com probabilidade de sucesso maior que $1/2$.

Os resultados apresentados no Capítulo 6 generalizam o trabalho de Moore et al. (2004), para grupos q-edrais, que requer $s = 1$. Em alguns aspectos, este trabalho também generaliza a Ref. Bacon et al. (2005), que também requer $s = 1$. Em Moore et al. (2004), os autores utilizam a transformada de Fourier não abeliana para resolver o PSO sobre $\mathbb{Z}_p \rtimes \mathbb{Z}_q$ $(s = 1)$. Seria interessante analisar a possibilidade de obter resultados equivalentes para $\mathbb{Z}_p \rtimes \mathbb{Z}_{q^s}$ usando a transformada de Fourier não abeliana.

A maior parte dos algoritmos quânticos apresentados neste trabalho faz uso da classificação dos subgrupos. Esta tem se mostrado uma boa ferramenta na busca de novos algoritmos quânticos para o PSO. Desta forma, o próximo passo seria generalizar a solução do PSO para grupos da forma $\mathbb{Z}_{p^r} \rtimes \mathbb{Z}_{q^s}$. Acreditamos que a classificação dos subgrupos neste caso seja uma generalização do que fizemos aqui. Para um homomorfismo particular $(t = 1)$, mostramos que existe um algoritmo quântico eficiente para o PSO sobre $\mathbb{Z}_p \rtimes \mathbb{Z}_{q^s}$. Como sugestão de trabalhos futuros, seria interessante analisar o caso $t > 1$. Essa tarefa não parece ser uma simples

generalização dos resultados obtidos para o caso $t = 1$.

Esperamos que as idéias apresentadas nesta tese possam contribuir no desenvolvimento de novos algoritmos quânticos para outras instâncias do PSO não abeliano.

Referências Bibliográficas

L. V. Ahn. Survey: Quantum Computation and The Hidden Subgroup Problem. Relatório técnico, Dept. of Science Computer, Carnegie Mellon University, Pittsburgh, 2002.

M. Ajtai. Generating hard instances of lattice problems. In **Proc. of the 28th ACM Symp. on the Theory of Computing**, páginas 99–108, New York, 1996. ACM.

M. Ajtai. The shortest vector problem in l_2 is np-hard for randomized reductions. In **Proc. of the 30th ACM Symp. on Theory of Computing**, páginas 10–19, New York, 1998. ACM.

M. Ajtai e C. Dwork. A public-key cryptosystem with worst-case/average-case equivalence. In **Proc. of the 29th ACM Symp. on the Theory of Computing**, páginas 284–293, New York, 1997. ACM.

G. Alagic, C. Moore, e A. Russel. Subexponential-time algorithms for hidden subgroup problems over product groups. In **Proc. 18th ACM-SIAM Symp. on Discrete Algorithms**, 2006.

A. Ambainis. Quantum walk algorithm for element distinctness. **SIAM J. Comput.**, 37(1):210–239, 2007.

A. Ambainis, J. Kempe, e A. Rivosh. Coins make quantum walks faster. In **SODA '05: Proceedings of the sixteenth annual ACM-SIAM symposium on Discrete algorithms**, páginas 1099–1108, Philadelphia, PA, USA, 2005. Society for Industrial and Applied Mathematics. ISBN 0-89871-585-7.

D. Bacon. How a Clebsch-Gordan Transform Helps to Solve the Heisenberg Hidden Subgroup Problem. **ArXiv:quant-ph/0612107v2**, 2007.

D. Bacon, A. M. Childs, e W. van Dam. From optimal measurement to efficient quantum algorithms for the hidden subgroup problem over semi-direct product groups. In **Proc. of 46th Ann. IEEE Symp. on Foundations of Computer Science - FOCS 2005**, páginas 469–478, 2005.

M. Batty, S. L. Braunstein, A. J. Duncan, e S. Rees. Quantum algorithm in group theory. **ArXiv:quant-ph/0310133 v2**, 2003.

R. Beals. Quantum computation of Fourier transforms over symmetric groups. In **Proc. 29th ACM Symp. on Theory of Computing**, páginas 48–53, New York, 1997. ACM.

P. Benioff(1980). The Computer as a Physical System: A Microscopic Quantum Mechanical Hamiltonian Model of Computers as Represented by Turing Machines. **Journal of Statistical Physics**, 22.

K. K. H. Cheung e M. Mosca. Decomposing finite abelian groups. **Quantum Information and Computation**, 1(3):26–32, 2001.

D. P. Chi, J. S. Kim, e S. Lee. Notes on the hidden subgroup problem on some semi-direct product group. **arXiv:quant-ph/0604172.**, 1, 2006.

I. L. Chuang e M. A. Nielsen. **Quantum Computation and Quantum Information**. Cambridge Univesity Press, Cambridge, 2000.

C. M. M. Cosme. **Algoritmos Quânticos para o Problema do Subgrupo Oculto não Abeliano**. Tese de Doutorado, Laboratório Nacional de Computação Cientícia - LNCC, 2008.

C. M. M. Cosme e R. Portugal. O problema do subgrupo oculto em uma classe de produto semidireto de grupos. In **2º Workshop-Escola de Computação e**

Informação Quântica - Anais, páginas 80–89, Campina Grande, PB, 2007a. EDUFCG.

C. M. M. Cosme e R. Portugal. Quantum algorithms for the hidden subgroup problem on a class of semidirect product groups. **ArXiv:quant-ph/0703223v2**, 2007b.

E. Dalcumune. Algoritmos Quânticos para o Problema do Isomorfismo de Grafos. Dissertação de Mestrado, Laboratório Nacional de Computação Científica - LNCC, 2008.

I. Damgard. QIP Note: On the Quantum Fourier Transform and Applications. Relatório técnico, computer science department of Aarhus University, 2004.

D. Deutsch. Quantum Theory, the Church-Turing Principle and the Universal Quantum Computer. **Proceedings of the Royal Society of London**, A 400: 97–117, 1985.

D. Deutsch. Quantum Computational Networks. **Proceedings of the Royal Society of London. Series A, Mathematical and Physical Sciences**, 425 (1868):73–90, 1989. URL `http://www.jstor.org/stable/2398494`.

D. Deutsch e R. Jozsa. Rapid solution of problems by quantum computation. **Proceedings of the Royal Society of London**, A 439(1907):553–558, 1992.

M. Ettinger e P. Høyer. On quantum algorithms for noncommutative hidden subgroups. **Adv. in Appl. Math.**, (25):239–251, 2000.

M. Ettinger, P. Høyer, e M. Knill. The quantum query complexity of the hidden subgroup problem is polynomial. **Inform. Process. Lett.**, (91):43–48, 2004.

T. D. Fernandes. Problema do Subgrupo Oculto em Grupos Nilpotentes. Dissertação de Mestrado, Laboratório Nacional de Computação Científica - LNCC, 2008.

R. Feynman. Simulating Physics with Computers. **International Journal of Theoretical Physics**, 21:467–488, 1982.

K. Friedl, G. Ivanyous, F. Magniez, M. Santha, e P. Sean. Hidden translation and orbit coset in quantum computing. In **Proc. of 35th Annual ACM Symposium on Theory of Computing**, 2003.

A. Garcia e Y. Lequain. **Elementos de Álgebra**. IMPA, 2002.

D. Gavinsky. Quantum solution to the hidden subgroup problem for poly-near-hamiltonian groups. **Quantum Information and Computation**, (4):229–235, 2004.

D. N. Gonçalves. Transformada de Fourier Quântica no Grupo Diedral. Dissertação de Mestrado, Laboratório Nacional de Computação Cientícia - LNCC, 2005.

D. N. Gonçalves, R. Portugal, e C. M. M. Cosme. Algoritmos Quânticos para uma Classe de produtos Semidiretos de Grupos. In **Anais do XXXI CNMAC**, Belém, Pará, 2008.

D. N. Gonçalves, R. Portugal, e C. M. M. Cosme. Solutions to the hidden subgroup problem on some metacylic groups. In **Proc. 4th Worshop on Theory of Quantum Computation, Communication and Cryptography**. LNCS, Springer-Verlag (to apper), 2009.

M. Grigni, L. Schulman, M. Vazirani, e U. Vazirani. Quantum mechanical algorithms for the nonabilian hidden subgrou problem. **Combinatoria**, páginas 137–154, 2004.

L. K. Grover. Quantum mechanics helps in searching for a needle in a Haystack. **Physical Review Letters**, 79:325–328, 1997.

M. Hall Jr. **The Theory of Groups**. The Macmillan Company, 1959.

S. Hallgren, C. Moore, M. Rötteler, A. Russell, e P. Sen. Limitations of quantum coset states for graph isomorphism. In **Proceedings 38th ACM Symposium on Theory of Computing (STOC'06)**, páginas 604–617, 2006.

S. Hallgren, A. Russel, e A. Ta-Shma. Normal subgroup recontruction and quantum computing using group representation. In **Proceedings 32nd Annual ACM Symposium on Theory of Computing (STOC'06)**, páginas 627–635, 2000.

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

I. N. Hernstein. **Tópicos em Álgebra**. Polígono, 1970.

C. J. Hillar e D. L. Rhea. Automorphism of finite abelian groups. **arXiv:math/0605185**, 1, 2006.

Peter Høyer. Conjugated operators in quantum algorithms. **Phys. Rev. A**, 59 (5):3280–3289, May 1999.

Y. Inui e F. Le Gall. Efficient Quantum Algorithms for the Hidden Subgroup Problem over Semi-direct Product Groups. **arXiv:quant-ph/0604172**, 2007.

Y. Inui e F. Le Gall. An efficient quantum algorithm for the hidden subgroup problem over a class of semi-direct product groups. **Quantum Information and Computation**, (5):559–570, 2007.

G. Ivanyos, F. Magniez, e M. Santha. Efficient Quantum Algorithms for some Instances of the Non-Abelian Hidden Subgroup Problem. **Internation Journal of Foudations of Computer Science.**, 14(5):723–740, 2003a.

G. Ivanyos, F. Magniez, e M. Santha. Efficient Quantum Algorithms for some Instances of the Non-Abelian Hidden Subgroup Problem. **Internation Journal of Foudations of Computer Science**, 14(5):723–740, 2003b.

G. Ivanyos, L. Sanselme, e M. Santha. An efficient quantum algorithm for the hidden subgroup problem in extraspecial groups. In **In Proc. of STACS**, 2007a.

G. Ivanyos, L. Sanselme, e M. Santha. An efficient quantum algorithm for the hidden subgroup problem in nil-2 groups. **Proc. of 8th Latin American Theoretical Informatics, LATIN'08**, 2007b.

R. Jozsa. Quantum factoring, discrete logarithms and the hidden subgroup problem. **Computing in Science and Engineering**, 03(2):34–43, 2001. ISSN 1521-9615.

R. Kannan e A. Bachem. Historical notes on the Fast Fourier Transform. **SIAM Journal on Computing**.

J. Köbler, U. Schöning, e J. Torán. **The Graph Isomorphism Problem: Its Structural Complexity**. Birkhauser, 1993.

S. Khot. Hardness of approximating the shortest vector problem in lattices. **Journal of the ACM**, 52(5):789–808, 2005.

A. Y. Kitaev, A. H. Shen, e M. N. Vyalyi. **Classical and Quantum Computation**, volume 47 of **Graduate Studies in Mathematics**. American Mathematical Society, Providence, 2002.

A. Yu. Kitaev. Quantum measurements and and the abelian stabilizer problem. **ArqXiv preprint quant-ph/9511026**, 1995.

N. Koblitz. **Algebraic aspects of cryptography**. Berlin ; New York : Springer-Verlag, Rio de Janeiro, 1998.

H. Krovi e M. Rötteler. An Efficient Quantum Algorithm for the Hidden Subgroup Problem over Weyl-Heisenberg Groups. **ArXiv:quant-ph/08103695v1**, 2008.

G. Kuperberg. A Subexponential-Time Quantum Algorithm for the Dihedral Hidden Subgroup Problem. **SIAM J. Comput.**, 35(1):170–188, 2005. ISSN 0097-5397.

S. Kutin. Quantum lower bound for the collision problem with small range. **Theory of Computing**, 1(1):29–36, 2005. URL `http://www.theoryofcomputing.org/articles/v001a002`.

J. H. Kwak e M. Y. Xu. **Finite Group Theory for Combinatorists**, volume 1. Postech, 2005.

C. Lavor, L.R.Y. Mansur, e R. Portugal. Grover's Algorithm: Quantum Data Search. **Quantum Physics, abstract quant-ph/0301079**, 1, June 2003a.

C. Lavor, L.R.Y. Mansur, e R. Portugal. Shor's Algorithm for Factoring Large Integers. **Quantum Physics, Abstract quant-ph/0303175**, 1, March 2003b.

C. Lomont. The Hidden Subgroup Problem - Review and Open Problems. **Quantum Physics, Abstract quant-ph/0411037**, November 2004.

F. L. Marquezino. A Transformada de Fourier Quântica Aproximada e sua Simulação. Dissertação de Mestrado, Laboratório Nacional de Computação Científica - LNCC, 2006.

D. K. Maslen. The Efficient Computation of Fourier Transform on the Symmetric Group. **American Mathematical Society**, 67:1121–1147, 1998.

D. K. Maslen e D. N. Rockmore. Separation of Variable and Computation of Fourier Transforms on Finite Group. **American Mathematical Society**, 10: 169–214, 1997.

C. Moore, D. Rockmore, A. Russell, e L. J. Schulman. The power of basis selection in fourier sampling: hidden subgroup problems in affine groups. In **SODA '04: Proceedings of the fifteenth annual ACM-SIAM symposium on Discrete algorithms**, páginas 1113–1122, 2004.

C. Moore e A. Russel. On the Impossibility of a Quantum Sieve Algorithm for Graph Isomorphis. **ArqXiv preprint quant-ph/0609138**, 1, 2006.

C. Moore, A. Russel, e L. Schulman. The symmetric group defies Fourier sampling. In **Proc. of the 46th Symposium on Foundations of Computer Science**, páginas 479–488, 2005.

M. A. Nielsen e I. L. Chuang. **Quantum Computation and Quantum Information**. Cambridge University Press, 2003.

R. Portugal, C. M. M. Cosme, e D. N. Gonçalves. Algoritmos quânticos. In **1º Workshop-Escola de Computação e Informação Quântica - Anais**, páginas 67–100, Pelotas, RS, 2006.

M. Puschel, M. Rötteler, e T. Beth. Fast quantum Fourier transforms for a class of non-abelian groups. In **Proc. of the 13th AAECC**, volume 1719, páginas 148–159, 1999.

J. Radhakrishnan, M. R'oteller, e P. Sen. On the power of random bases in fourier sampling: Hidden subgroup problem in the heisenberg group. In **Proc. of the 32nd Internation Colloquium on Automata, Langueges and Programming**, páginas 1399–1412, 2005.

O. Regev. A Subexponential Time Algorithm for the Dihedral Hidden Subgroup Problem with Polynomial Space. **quant-ph/0406151**, 2004a.

O. Regev. New Lattice-Based Cryptographic. **J. ACM**, 51(6):899–942, 2004b.

O. Regev. Quantum Computation and Lattice Problems. **SIAM Journal on Computing**, 33(3):738–760, 2004c.

I. Reiner e C. W. Curtis. **Representation Theory of Finite Groups and Associative Algebras**. John Wiley and Sons, Lnc., London, 1962.

D. J. S. Robinson. **A Course in Theory of Groups**. Number 80 in Graduate Text in Mathematics. Springer-Verlag, New York, 1995.

J. P. Serre. **Linear Representation of Finite Group**. Springer-Verlag, Nova York, 1997.

N. Shenvi, J. Kempe, e K. B. Whaley. Quantum random-walk search algorithm. **Phys. Rev. A**, 67(5):052307, May 2003.

P. W. Shor. Algorithms for quantum computation: discrete logs and factoring. In **Proc. of the 35th Ann. IEEE Symp. on the Foundation of Computer Science**, páginas 124–134, 1994.

P. W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. **SIAM J. Comput.**, 26(5):1484–1509, 1997. ISSN 0097-5397.

D. R. Simon. On the Power of Quantum Computation. In **Proceedings of the 35th Annual Symposium on Foundations of Computer Science**, páginas 116–123, Los Alamitos, CA, 1994. Institute of Electrical and Electronic Engineers Computer Society Press.

K. Spindler. **Abstract Algebra with Aplications**, volume 1. Marcel Dekker, INC, New York, 1994.

T. Toffoli. Reversible computing. In **Proc. 7th Col. on Automata, Languages and Programing**, páginas 632–644, New York, 1980a. Springer-Verlag.

T. Toffoli. Reversible computing. Relatório técnico, MIT Laboratory for Computer Science, Tech. Memo MIT/LCS/TM-151, 1980b.

J. Watrous. Quantum algorithms for solvable groups. In **Proc. of the 33th ACM Symp. on Theory of Computing**, páginas 60–67, New York, 2001. ACM.

Apêndice A

Tópicos em Teoria de Grupos e Teoria da Representação

O presente apêndice apresenta uma breve revisão de alguns conceitos básicos sobre teoria de grupos finitos e teoria da representação que são importantes para o trabalho. Seguimos uma abordagem clássica baseada nas referências Garcia e Lequain (2002); Hernstein (1970); Robinson (1995); Hall Jr. (1959) e Spindler (1994)(teoria de grupos) e Serre (1997); Reiner e Curtis (1962); Gonçalves (2005)(teoria da representação).

A.1 Teoria de Grupos

Iniciamos a seção com uma série de definições:

Definição A.1.1 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: se $a, b, c \in G$ então $a * (b * c) = (a * b) * c$.

(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 denotamos $a * b$ por ab para todo $a, b \in G$.

Definição A.1.2 Dizemos que G é um grupo *abeliano* se $ab = ba$ para todo $a, b \in G$.

Definição A.1.3 Seja G um grupo.

(1) A ordem de G (denotamos por $|G|$) é a cardinalidade do conjunto G.

(2) Se $a \in G$, então a ordem do elemento a (denotamos $\text{ord}(a)$ ou $|a|$) é o menor inteiro positivo n tal que $a^n = e$.

(3) O expoente de G (denotamos $\exp(G)$) é o menor inteiro positivo m tal que $a^m = e$ para todo $a \in G$.

Definição A.1.4 Seja G um grupo. Um subconjunto não-vazio H de G é um *subgrupo* de G (denotamos $H \leq G$), quando, com a operação de G, o conjunto H é um grupo.

Definição A.1.5 Seja G um grupo e H um subgrupo de G. Uma *classe lateral à esquerda* de H em G é um conjunto da forma $gH = \{gh : h \in H\}$, com $g \in G$. Analogamente, definimos uma *classe lateral à direita* de H em G como sendo o conjunto $Hg = \{hg : h \in H\}$.

Seja G um grupo é H um subgrupo de G. Então para todo $g \in G$ temos $|H| = |gH| = |Hg|$. De fato, basta notar que a aplicação $h \mapsto gh$ (ou $h \mapsto hg$) é uma bijeção.

Agora, observe que duas classes laterais à esquerda (direita) de H em G são disjuntas ou são iguais. Com efeito, sejam g_1H e g_2H duas classes laterais à esquerda de H em G (os elementos $g_1, g_2 \in G$ são chamados *representantes* de classes laterais). Então, suponha que existam elementos $x, y \in H$ tais que $g_1x = g_2y$ (isto é, g_1H e g_2H possuem pelo menos um elemento em comum). Daí vem $g_1 = g_2yx^{-1}$, onde $yx^{-1} \in H$. Seja g um elemento arbitrário de g_1H, então $g = g_1x'$, $x' \in H$. Assim, $g = g_1x' = g_2yx^{-1}x' = g_2h$, $h \in H$ implica que

$g \in g_2H$, portanto $g_1H \subset g_2H$. Analogamente, podemos mostrar que $g_2H \subset g_1H$, e portanto, $g_1H = g_2H$.

Em particular, para qualquer subgrupo H de G podemos decompor G como uma união disjunta de classes laterais de H, isto é, $G = g_1H \cup g_2H \cup \ldots \cup g_nH$.

Segue do Teorema de Lagrange, que o número total de classes laterais distintas de H em G, denotado por $[G : H]$, é

$$[G : H] = \frac{|G|}{|H|}. \tag{A.1}$$

Para $g \in G$ e H um subgrupo de G, usamos o símbolo gHg^{-1} para denotar o conjunto $gHg^{-1} = \{ghg^{-1} \ : h \in H\}$. Um subgrupo H de G é dito *normal* (denotamos $H \lhd G$) se $H = gHg^{-1}$ para todo $g \in G$. Neste caso, as classes laterais à esquerda e a direita de H são iguais.

Seja H um subgrupo normal de um grupo G. Então o conjunto formado pelas classes laterais de H em G forma um grupo, com respeito a operação em G. Este grupo, denotado por G/H, é chamado de grupo *quociente*.

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 indicamos por $G = \langle S \rangle$. Também, dados elementos $g_1, \ldots, g_k$ de um grupo G, denotamos 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.

Um grupo G dado por um único gerador, isto é, $G = \langle g \rangle$, é dito *cíclico*.

Teorema A.1.1 Todo grupo G de tamanho $|G| > 1$ tem um conjunto gerador de tamanho no máximo $\lfloor \log_2 |G| \rfloor$.

Demonstração: 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 procedimento vemos que $|\langle g_1, \ldots, g_{\log_2 |G|}\rangle| \geq 2^{\log_2 |G|} = |G|$. Assim concluímos nossa prova.

■

Definição A.1.6 Sejam $G_1, \ldots, G_n$ grupos, definimos o *produto direto* de $G_1, \ldots, G_n$ como sendo o produto cartesiano $G_1 \times \ldots \times G_n$ com a operação

$$(x_1, \ldots, x_n).(y_1, \ldots, y_n) = (x_1 y_1, \ldots, x_n y_n).$$

O teorema a seguir fornece condições para que um grupo G seja isomorfo a um produto direto de grupos $G_1, \ldots, G_n$.

Teorema A.1.2 Sejam $G, G_1, \ldots, G_n$ grupos. Então o grupo G é isomorfo ao grupo $G_1 \times \ldots \times G_n$ se e somente se G possui subgrupos $H_1 \simeq G_1, \ldots, H_n \simeq G_n$ tais que:

(1) $G = H_1 \ldots H_n$.

(2) $H_i \lhd G_i$, para todo $i = 1, \ldots, n$.

(3) $H_i \cap (H_1 \ldots H_{i-1} H_{i+1} \ldots H_n) = \{e\}$.

Demonstração: Ver Garcia e Lequain (2002).

■

Quando um grupo G e subgrupos $H_1, \ldots, H_n$, munidos com à operação aditiva, satisfazem as condições do Teorema A.1.2, dizemos que G é uma *soma direta* de seus subgrupos, e escrevemos

$$G = H_1 \oplus \ldots \oplus H_n.$$

O teorema a seguir é importante pelas suas aplicações em algoritmos quânticos.

Teorema A.1.3 (Teorema Fundamental dos Grupos Abelianos Finitos) Todo grupo abeliano finito é uma soma direta de grupos cíclicos de ordens potências de números primos.

Demonstração: Ver Reiner e Curtis (1962).

■

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:

$$x, y \in G,\ x \overset{G}{\sim} y \Leftrightarrow \exists\ g \in G \text{ tal que } y = g^{-1}xg. \tag{A.2}$$

Assim temos a

Proposição A.1.1 Seja G um grupo. A relação $\overset{G}{\sim}$ define uma relação de equivalência em G.

Demonstração: De fato, para todo $x \in G$ temos $x = e^{-1}xe$, logo $x \overset{G}{\sim} x$. Agora, se $x \overset{G}{\sim} y$ então existe $g \in G$ tal que $y = g^{-1}xg$. Pondo $u = g^{-1}$ segue que $x = u^{-1}yu$, ou seja, $y \overset{G}{\sim} x$. Por fim, suponhamos que $x \overset{G}{\sim} y$ e $y \overset{G}{\sim} z$ então existem $g, h \in G$ tais que $y = g^{-1}xg$ e $z = h^{-1}yh$. Pondo $u = gh$ temos que $u^{-1}xu = z$, logo $x \overset{G}{\sim} z$ e isto demonstra a proposição.

■

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

$$\mathcal{C}_x = \{y : x \overset{G}{\sim} y\}. \tag{A.3}$$

Dois importantes subgrupos de um grupo G são o seu centro, denotado por $\mathcal{Z}(G)$, e seu subgrupo de comutadores, ou subgrupo derivado, denotado por G'. O centro é definido por

$$\mathcal{Z}(G) = \{g \in G;\ gh = hg,\ \forall\, h \in G\}. \tag{A.4}$$

Dados $g, h \in G$ o comutador $[g, h]$ é dado por $[g, h] = ghg^{-1}h^{-1}$. Define-se o subgrupo de comutadores por

$$G' = \langle [g, h];\ g, h \in G \rangle . \tag{A.5}$$

De maneira mais geral, se $R, S \subset G$ defini-se o subgrupo de comutadores de R e S, denotado por $[R, S]$, como

$$[R, S] = \langle [g, h];\ g \in R, h \in S \rangle .$$

Observe que $G' = [G, G]$.

Utilizando os subgrupos de comutadores podemos definir a seguinte série de subgrupos de G, à qual chamamos *série central inferior* do grupo G. Tal série de subgrupos é dada por

$$G = \gamma_1(G) \geq \gamma_2(G) \geq \cdots \tag{A.6}$$

onde $\gamma_{k+1}(G) = [\gamma_k(G), G]$. Observe que $\gamma_2(G) = G'$.

Definição A.1.7 Um grupo G é dito nilpotente se possuir uma série central inferior tal que

$$G = \gamma_1(G) \geq \gamma_2(G) \geq \cdots \geq \gamma_n(G) \geq \gamma_{n+1}(G) = \{e\}.$$

O inteiro n é chamado a *classe de nilpotência* do grupo G.

Teorema A.1.4 Um grupo G é nilpotente de classe n se, e somente se, $\gamma_n(G) \leq \mathcal{Z}(G)$.

Demonstração: De fato, se G é nilpotente de índice n, pela Definição A.1.7 segue que $\gamma_{n+1}(G) = [\gamma_n(G), G] = \{e\}$. Assim, fixado $h \in \gamma_n(G)$, para todo $g \in G$ temos que $e = [h, g] = hgh^{-1}g^{-1}$ e, equivalentemente, $hg = gh$. Logo $h \in \mathcal{Z}(G)$. O que mostra que $\gamma_n(G) \leq \mathcal{Z}(G)$. Reciprocamente, se $\gamma_n(G) \leq \mathcal{Z}(G)$ obviamente

$\gamma_{n+1}(G) = \{e\}$. O que encerra a prova.

■

Exemplo A.1.1 São exemplos de grupos nilpotentes de classe n os grupos D_{2^n}, Q_{2^n} e QD_{2^n} de ordem 2^{n+1}.

Demonstração: Sejam g, h elementos arbitrários em D_{2^n}, então não há dificuldade em verificar que

$$[g,h] = ghg^{-1}h^{-1} = \begin{cases} e & \text{se} \quad g = x^r \text{ e } h = x^s; \\ x^{2r} & \text{se} \quad g = x^r \text{ e } h = x^s y; \\ x^{-2r} & \text{se} \quad g = x^r y \text{ e } h = x^s; \\ x^{2r} & \text{se} \quad g = x^r y \text{ e } h = x^s y. \end{cases} \tag{A.7}$$

Isso mostra que

$$D'_{2^n} = [D_{2^n}, D_{2^n}] = \left\langle x^2 \right\rangle. \tag{A.8}$$

Vamos mostrar que D_{2^n} possui a seguinte série central inferior:

$$D_{2^n} \supseteq \left\langle x^2 \right\rangle \supseteq \left\langle x^4 \right\rangle \supseteq \ldots \supseteq \left\langle x^{2^n} \right\rangle = \{e\}. \tag{A.9}$$

De fato, note que $\gamma_2(D_{2^n}) = D'_{2^n} = \langle x^2 \rangle$. Usando indução sobre n é fácil ver que

$$\gamma_{n+1}(D_{2^n}) = [\gamma_n(D_{2^n}), D_{2^n}] = \left\langle x^{2^n} \right\rangle = \{e\}. \tag{A.10}$$

Assim, a série central inferior (A.9) tem comprimento n, o que implica D_{2^n} ter classe de nilpotência n.

A demonstração de que os grupos Q_{2^n} e QD_{2^n} possuem classe de nilpotência n é análoga.

■

Existe uma relação interessante entre os grupos nilpotentes e p-grupos, p primo. Esta relação é mostrada pelos teoremas a seguir, cujas demonstrações podem ser encontradas em Robinson (1995).

Teorema A.1.5 Todo p-grupo finito é nilpotente. ∎

Seja G um grupo e p um número primo. Seja $H \leq G$. Então H é dito um *p-subgrupo de Sylow* de G se $|H| = p^\alpha$ para algum $\alpha \in \mathbb{N}$ tal que p^α divide $|G|$ mas $p^{\alpha+1}$ não divide. Mostra-se que tais subgrupos sempre existem. Além disso, eles fornecem a seguinte decomposição dos grupos nilpotentes finitos.

Teorema A.1.6 Um grupo finito G é nilpotente se, e somente se, é o produto direto de seus subgrupos de Sylow. ∎

A.2 Teoria da Representação

A teoria da representação de grupos finitos desempenha um papel importante na construção de algoritmos quânticos para o PSO não abeliano. Essa figuração deve-se ao fato da transformada de Fourier em grupos ser descrita em termos das representações irredutíveis do grupo. Como vimos no Capítulo 2, a maioria dos algoritmos quânticos com ganho exponencial para o PSO tem a transformada de Fourier como um dos seus ingredientes principais.

Definição A.2.1 Uma representação ρ de um grupo finito G é um homomorfismo $\rho : G \to U(V)$, onde $U(V)$ denota o grupo dos operadores lineares unitários sobre um espaço de dimensão finita V, cuja dimensão denotamos por d_ρ.

Se fixarmos uma base para V, podemos olhar para cada $\rho(g)$ como uma matriz unitária $d_\rho \times d_\rho$, à qual chamamos de matriz representação de G.

Exemplo A.2.1 Seja G um grupo e seja $\mathbb{C}^*$ o grupo multiplicativo dos números complexos não nulos. É fácil verificar que a aplicação $\rho : G \to \mathbb{C}^*$ tal que $\rho(g) = 1$ é um homomorfismo, e portanto, uma representação do grupo G. A representação ρ é chamada *representação trivial* e geralmente denotada por 1_G.

Exemplo A.2.2 Seja G um grupo e $X = \{1, 2, \ldots, n\}$. Considere a ação do grupo G no conjunto X dada pela seguinte regra: para cada elemento $g \in G$ tem-se uma

permutação no conjunto X fazendo

$$i^g = j, \ \text{ com } 1 \leq i, j \leq n. \tag{A.11}$$

Seja V um espaço de dimensão finita com base $B = \{e_1, \ldots, e_n\}$. Para cada $g \in G$ definimos a aplicação $\rho(g)$ 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 $\rho(g)$ é uma representação de G. Com efeito,

$$e_i\rho(gh) = e_{i^{gh}} = e_{(i^g)^h} = e_{i^g}\rho(h) = e_i\rho(g)\rho(h), \tag{A.12}$$

logo $\rho(g)$ é um homomorfismo e portanto, uma representação do grupo G. Não é difícil verificar que $\rho(g)$ é um isomorfismo. Neste caso, a representação $\rho(g)$ é chamada *representação permutação*.

Definição A.2.2 Dizemos que uma representação ρ é *irredutível* se não existe nenhum subespaço invariante por G além do espaço nulo e do próprio V. Caso contrário, a representação é dita *redutível*.

Agora introduzimos o conceito de isomorfismo de representações.

Definição A.2.3 Dizemos que duas representações são isomorfas se elas diferem apenas por uma mudança de base, isto é, $\rho_1 \simeq \rho_2$ se existe uma matriz unitária U tal que $\rho_1(g) = U^\dagger\rho_2(g)U$.

O teorema a seguir mostra uma estreita relação entre o número de representações irredutíveis de um grupo finito G e suas classes de conjugação. A demonstração deste teorema, bem como as provas dos demais teoremas enunciados a longo deste apêndice, poderá ser encontrada em Serre (1997).

Teorema A.2.1 Seja G um grupo finito. O número de representações irredutíveis de G (a menos de isomorfismo) é igual ao número de classes de conjugação de G. ■

Denotamos por $\widehat{G}$ o conjunto formado por todas as representações irredutíveis de G.

Definição A.2.4 Seja G um grupo e ρ uma representação irredutível de G. O homomorfismo $\chi : G \to \mathbb{C}^*$ definido por $\chi_\rho(g) = \mathrm{tr}\rho(g)$ é chamado *caráter* da representação ρ.

Teorema A.2.2 Sejam ϕ e ψ duas funções complexas em G. Então, a função definida por $(\phi|\psi) = \frac{1}{|G|}\sum_{g\in G}\phi(g)\psi(g)^*$ é um produto interno.

Demonstração: Basta verificar as propriedades de produto interno.

■

Teorema A.2.3 (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 $(\chi|\chi') = 0$. ■

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

Teorema A.2.4 Duas representações com mesmo caráter são isomorfas. ■

Teorema A.2.5 Sejam $\rho_1, \rho_2, \ldots, \rho_k$ 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 $\sum_{i=1}^{k} n_i\chi_i(g) = 0$. ■

Se ρ é uma representação redutível de G, então ρ pode ser decomposta como uma soma direta de representações irredutíveis de G. Neste caso escrevemos $\rho \cong \oplus_i \rho_i$, lembrando que uma mesma representação $\tau \in \widehat{G}$ pode aparecer mais de uma vez na decomposição de ρ.

Se ρ e σ são duas representações de um grupo G podemos definir a representação $\rho \otimes \sigma$ nos espaços $V_\rho \otimes V_\sigma$ como sendo $(\rho \otimes \sigma)(g) = \rho(g) \otimes \sigma(g)$. Se as

representações ρ e σ são irredutíveis, pode acontecer da representação $\rho \otimes \sigma$ ser redutível. O problema de decompor $\rho \otimes \sigma$ em representações irredutíveis é conhecido na literatura como problema de *Clebsch- Gordan*.

Apêndice B

Algoritmo para Decompor Grupos Abelianos

O Teorema Fundamental de Grupos Finitos Abelianos (Teorema A.1.3) diz que qualquer grupo finito abeliano pode ser decomposto como uma soma direta de subgrupos cíclicos cujas ordens são potências de primos. Entretanto, não é conhecido nenhum algoritmo clássico que explicite este isomorfismo eficientemente. Neste apêndice, apresentamos um algoritmo quântico que faz essa decomposição em tempo polinomial.

Uma matriz quadrada U é dita *unimodular* se suas entradas são números inteiros e se $\det(U) = \pm 1$.

Teorema B.0.6 Para qualquer matriz com entradas inteiras A, pode-se determinar em tempo polinomial usando operações elementares sobre as linhas e colunas de A, matrizes unimodulares U e V tais que $UAV = \begin{bmatrix} D & 0 \\ 0 & 0 \end{bmatrix}$, onde $D = \mathrm{diag}(d_1, \ldots, d_k)$ é uma matriz diagonal com entradas inteiras $d_1, \ldots, d_k$ tais que $d_1 | d_2 | \ldots | d_k$, e para cada i, o produto $d_1, \ldots, d_i$ é igual ao mdc dos subdeterminantes de A de ordem i.

Demonstração: Veja ref. Kannan e Bachem. ■

A matriz $\begin{bmatrix} D & 0 \\ 0 & 0 \end{bmatrix}$ é chamada de forma normal de Smith de A.

O teorema que vamos enunciar logo abaixo é parte fundamental do algoritmo de decomposição de grupos abelianos.

Teorema B.0.7 Sejam $G = \langle a_1, \ldots, a_k \rangle$ um grupo finito abeliano e M uma matriz tal que $a_1^{x_1} \ldots a_k^{x_k} = e$ se, e somente se, $\mathbf{x} = (x_1, \ldots, x_k)^T \in \text{intcol}(M)$, onde $\text{intcol}(M)$ denota o conjunto dos valores obtidos tomando combinações lineares inteiras das colunas de M. Então, podemos determinar em tempo polinomial (no tamanho de M) elementos $g_1, \ldots, g_l$, com $l \leq k$ tais que, $G = \langle g_1 \rangle \oplus \ldots \oplus \langle g_l \rangle$.

Demonstração: Pelo Teorema B.0.6, podemos achar em tempo polinomial matrizes unimodulares $U_{k\times k}$ e $V_{n\times n}$ tais que $U_{k\times k}^{-1} M_{k\times n} V_{n\times n} = \underbrace{\begin{bmatrix} D & 0 \\ 0 & 0 \end{bmatrix}}_{D'}$, onde $D = \text{diag}(d_1, \ldots, d_m)$ é uma matriz diagonal com entradas inteiras $d_1, \ldots, d_m$. Como V é unimodular, segue da Observação B.0.1 que

$$\text{intcol}(MV) = \text{intcol}(M). \tag{B.1}$$

Assim,

$$a_1^{x_1} \ldots a_k^{x_k} = e \Leftrightarrow \mathbf{x} = (x_1, \ldots, x_k)^T \in \text{intcol}(MV).$$

Agora para cada $i, j = 1, \ldots, k$, seja r_i a ordem de $a_i^{'}$, onde $a_i^{'} = a_1^{u_{1i}} \ldots a_k^{u_{ki}}$ e u_{ji} são as entradas da matriz U. Pela Proposição B.0.1 $a_1'^{r_1} \ldots a_k'^{r_k} = e$ se, e somente se, $d_i | r_i$, logo $d_i = r_i$ pela minimalidade de r_i. Observe também que devemos ter $m = k$. De fato, suponhamos por absurdo que $m = k - j$, para algum $1 \leq j \leq k-1$, então invocando novamente a Proposição B.0.1 temos

$$\left(a_1'^{x_1} \ldots a_{k-j}'^{x_{k-j}}\right) a_{k-j+1}'^{x_{k-j+1}} \ldots a_k'^{x_k} = e \quad \Leftrightarrow \tag{B.2}$$

$$a_{k-j+1}'^{x_{k-j+1}} \ldots a_k'^{x_k} = e \quad \Leftrightarrow \tag{B.3}$$

$$x_{k-j+1} = \ldots = x_k = 0. \tag{B.4}$$

Mas isso é um absurdo, pois, como G é finito, existem inteiros positivos $r_{k-j+1}, \ldots, r_k$,

tais que

$$a'^{r_{k-j+1}}_{k-j+1} \dots a'^{r_k}_{k} = e, \tag{B.5}$$

onde $r_{k-j+1}, \dots, r_k$ são as ordens dos elementos $a'_{k-j+1}, \dots, a'_k$, respectivamente. Portanto, $m = k$.

Agora, seja j o menor índice tal que $d_j > 1$. Considere o conjunto formado pelos elementos $g_i = a'_{i+j-1}$, $i = 1, \dots, l$, onde $l = m - j + 1$. Pela Observação B.0.2, $G = \langle a'_1, \dots, a'_k \rangle$. Então, o conjunto $\{g_1, \dots, g_l\}$ também gera G e a ordem de cada g_i é d_{i+j-1}. Com efeito, suponhamos que $d_1 = \dots = d_{j-1} = 1$. Daí temos que $a'_1 = \dots = a'_{j-1} = e$ (pois d_i é a ordem de a'_i). Assim, se retirarmos as identidades do conjunto de geradores, ainda continuaremos com um conjunto de geradores para G. Ainda, da Observação B.0.3, o grupo G satisfaz as seguintes relações:

(1) $G = \langle g_1, \dots, g_l \rangle = \langle g_1 \rangle \dots \langle g_l \rangle$;

(2) Para todo $g \in G$, existem elementos unicamente determinados $x_1 \in \langle g_1 \rangle, \dots, x_l \in \langle g_l \rangle$ tais que $g = x_1 \dots x_l$;

(3) $\langle g_i \rangle \cap (\langle g_1 \rangle \dots \langle g_{i-1} \rangle \langle g_{i+1} \rangle \dots \langle g_l \rangle) = \{e\}$, $\forall\, i = 1, \dots, l$.

Segue dessas relações que $G = \langle g_1 \rangle \oplus \dots \oplus \langle g_l \rangle$ e com isso provamos o Teorema B.0.7.

■

Observação B.0.1 A Equação (B.1) está correta.

Demonstração: De fato,

$$M = U \begin{bmatrix} d_1 & & \dots & & 0 \\ & \ddots & & & \\ \vdots & & d_m & & \vdots \\ & & & \ddots & \\ 0 & & \dots & & 0 \end{bmatrix} V^{-1}$$

$$= \begin{bmatrix} u_{11} & \dots & u_{1k} \\ & \ddots & \\ \vdots & u_{jj} & \vdots \\ & & \\ u_{k1} & \dots & u_{kk} \end{bmatrix} \begin{bmatrix} d_1 & \dots & 0 \\ & \ddots & \\ \vdots & d_m & \vdots \\ & & \\ 0 & \dots & 0 \end{bmatrix} \begin{bmatrix} v'_{11} & \dots & v'_{1n} \\ & \ddots & \\ \vdots & v'_{jj} & \vdots \\ & & \\ v'_{n1} & \dots & v'_{nn} \end{bmatrix}$$

$$= \begin{bmatrix} u_{11}v'_{11}d_1 + \ldots + u_{1m}v'_{m1}d_m & \dots & u_{11}v'_{1n}d_1 + \ldots + u_{1m}v'_{mn}d_m \\ u_{21}v'_{11}d_1 + \ldots + u_{2m}v'_{m1}d_m & \dots & u_{21}v'_{1n}d_1 + \ldots + u_{2m}v'_{mn}d_m \\ \vdots & & \vdots \\ u_{k1}v'_{11}d_1 + \ldots + u_{km}v'_{m1}d_m & \dots & u_{k1}v'_{1n}d_1 + \ldots + u_{km}v'_{mn}d_m \end{bmatrix}.$$

Assim $\mathbf{x} \in \text{intcol}(M) \Leftrightarrow \mathbf{x} = \alpha_1 c_1 + \ldots + \alpha_n c_n$, onde $\mathbf{c}_i$ com $i = 1, \ldots, n$ representam as colunas de M e α_i são inteiros positivos. Logo, se

$$\mathbf{x} = (x_1, \ldots, x_k) = \alpha_1 c_1 + \ldots + \alpha_n c_n, \tag{B.6}$$

então

$$\begin{array}{lll} x_1 = (\alpha_1 v'_{11} + \ldots + \alpha_n v'_{1n}) u_{11} d_1 + & \dots & + (\alpha_1 v'_{m1} + \ldots + \alpha_n v'_{mn}) u_{1m} d_m \\ x_2 = (\alpha_1 v'_{11} + \ldots + \alpha_n v'_{1n}) u_{21} d_1 + & \dots & + (\alpha_1 v'_{m1} + \ldots + \alpha_n v'_{mn}) u_{2m} d_m \\ \vdots & \vdots & \\ x_k = (\alpha_1 v'_{11} + \ldots + \alpha_n v'_{1n}) u_{k1} d_1 + & \dots & + (\alpha_1 v'_{m1} + \ldots + \alpha_n v'_{mn}) u_{km} d_m. \end{array} \tag{B.7}$$

Renomeando os termos dentro dos parênteses em (B.7), obtemos:

$$\begin{array}{rcl} x_1 &=& \overline{\alpha}_1 u_{11} d_1 + \ldots + \overline{\alpha}_m u_{1m} d_m \\ x_2 &=& \overline{\alpha}_1 u_{21} d_1 + \ldots + \overline{\alpha}_m u_{2m} d_m \\ & \vdots & \\ x_k &=& \overline{\alpha}_1 u_{k1} d_1 + \ldots + \overline{\alpha}_m u_{km} d_m. \end{array} \tag{B.8}$$

Logo, segue de (B.8) que

$$\mathbf{x} = \overline{\alpha}_1 d_1 \begin{bmatrix} u_{11} \\ u_{21} \\ \vdots \\ u_{k1} \end{bmatrix} + \ldots + \overline{\alpha}_m d_m \begin{bmatrix} u_{1m} \\ u_{2m} \\ \vdots \\ u_{km} \end{bmatrix} \tag{B.9}$$

é uma combinação linear das colunas de $UD' = MV$, isto é, $\mathbf{x} \in \text{intcol}(UD') = \text{intcol}(MV)$.

Agora note que

$$MV = \begin{bmatrix} u_{11}d_1 & \ldots & u_{1m}d_m & \ldots & 0 \\ u_{21}d_1 & \ldots & u_{2m}d_m & \ldots & 0 \\ \vdots & & \vdots & \vdots & \\ u_{k1}d_1 & \ldots & u_{km}d_m & \ldots & 0 \end{bmatrix}, \tag{B.10}$$

portanto, $\mathbf{y} \in \text{intcol}(MV) \Leftrightarrow$

$$\mathbf{y} = \begin{bmatrix} y_1 \\ y_2 \\ \vdots \\ y_k \end{bmatrix} = \beta_1 d_1 \begin{bmatrix} u_{11} \\ u_{21} \\ \vdots \\ u_{k1} \end{bmatrix} + \ldots + \beta_m d_m \begin{bmatrix} u_{1m} \\ u_{2m} \\ \vdots \\ u_{km} \end{bmatrix} + \beta_{m+1} \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix} + \ldots + \beta_n \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix},$$

com $\beta_1, \ldots, \beta_n$ inteiros positivos, logo, $\mathbf{y} \in \text{intcol}(M)$, e portanto, $\text{intcol}(M) = \text{intcol}(MV)$, como queríamos demonstrar.

■

Observação B.0.2 Os elementos $a_1^{'}, \ldots, a_k^{'}$ geram o grupo G.

Demonstração: De fato, que $\langle a_1', \ldots, a_k' \rangle \subset G$ é trivial. Seja $a_i \in \{a_1, \ldots, a_k\}$

um gerador arbitrário de G. Vamos mostrar que $a_i = a_1^{'\alpha_1} \dots a_k^{'\alpha_k}$. Com efeito,

$$\begin{aligned} a_1^{'\alpha_1} \dots a_k^{'\alpha_k} &= (a_1^{u_{11}\alpha_1} \dots a_k^{u_{k1}\alpha_1}) \dots (a_1^{u_{1k}\alpha_k} \dots a_k^{u_{kk}\alpha_k}) \\ &= a_1^{u_{11}\alpha_1+\dots+u_{1k}\alpha_k} \dots a_k^{u_{k1}\alpha_1+\dots+u_{kk}\alpha_k} \\ &= a_1^{U_1\alpha} \dots a_i^{U_i\alpha} \dots a_k^{U_k\alpha}, \end{aligned} \tag{B.11}$$

onde U_i é a i-ésima linha da matriz U e $\alpha = (\alpha_1, \dots, \alpha_k)^T$. Afirmamos que existe um vetor de inteiros positivos $\alpha = (\alpha_1, \dots, \alpha_k)^T$, tal que a_i pode ser escrito na forma

$$a_i = a_1^0 \dots a_i^1 \dots a_k^0 = a_1^{U_1\alpha} \dots a_i^{U_i\alpha} \dots a_k^{U_k\alpha}.$$

Realmente, note que o sistema

$$= \begin{bmatrix} U_{11} & U_{12} & \dots & U_{1k} \\ \vdots & \vdots & & \\ U_{i1} & U_{i2} & \dots & U_{2k} \\ \vdots & \vdots & & \vdots \\ U_{k1} & U_{k2} & \dots & U_{kk} \end{bmatrix} \begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_i \\ \vdots \\ \alpha_n \end{bmatrix} = \begin{bmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{bmatrix}$$

possui solução inteira, pois, U é unimodular. Com isto mostramos que $G \subset \langle a_1', \dots, a_k' \rangle$, e portanto, $G = \langle a_1', \dots, a_k' \rangle$.

■

Observação B.0.3 O grupo G satisfaz as propriedades (1), (2), e (3) na demonstração do teorema B.0.7.

Demonstração: Observe que (1) segue simplesmente do fato de G ser abeliano. Para mostrarmos (2) note que por (1) temos que se $g \in G$ então $g = g_1^{\alpha_1} \dots g_l^{\alpha_l}$, com $g_i^{\alpha_i} \in \langle g_i \rangle$ e α_i para $i = 1, \dots, l$, inteiros positivos. Suponhamos que existam inteiros positivos $\beta_1, \dots, \beta_l$, tais que $g_i^{\beta_i} \in \langle g_i \rangle$, $g_i^{\alpha_i} \neq g_i^{\beta_i} \pmod{\text{ord}(g_i)}$ $\forall\ i =$

$1, \ldots, l$ e $g = g_1^{\alpha_1} \ldots g_l^{\alpha_l} = g_1^{\beta_1} \ldots g_l^{\beta_l}$. Então segue Proposição B.0.1 que

$$g_1^{\alpha_1 - \beta_1} \ldots g_l^{\alpha_l - \beta_l} = e \Leftrightarrow \alpha_i = \beta_i, \ \forall \ i = 1, \ldots, l. \tag{B.12}$$

Isto mostra a afirmação (2).

Agora seja $g \in \langle g_i \rangle \cap (\langle g_1 \rangle \ldots \langle g_{i-1} \rangle \langle g_{i+1} \rangle \ldots \langle g_l \rangle)$. Como $g \in \langle g_i \rangle$, podemos escrever $g = x_1 \ldots x_l$, com $x_1 = \ldots = x_{i-1} = x_{i+1} = \ldots = x_l = e$ e $x_i = g$; como $g \in (\langle g_1 \rangle \ldots \langle g_{i-1} \rangle \langle g_{i+1} \rangle \ldots \langle g_l \rangle)$, podemos escrever $g = x_1 \ldots x_l$, com $x_j \in \langle g_j \rangle \ \forall \ j = 1 \ldots, i-1, i+1, \ldots, l$ e $x_i = e$. Da unicidade do item (2), concluímos que $g = e$, com isso fica provado (3).

■

Proposição B.0.1 Seja $a_i' = a_1^{u_{1i}} \ldots a_k^{u_{ki}}, \ \forall \ i = 1, \ldots, k$. Então as seguintes condições são equivalentes:

(i) $a_1^{'x_1} \ldots a_k^{'x_k} = e$

(ii) $(x_1, \ldots, x_k)^T \in \text{intcol}(D')$

(iii) $d_i | x_i$ para $i = 1, \ldots, m$ e $x_i = 0$ para $i = m+1, \ldots, k$.

Demonstração: De fato, para provarmos que (i) $\Rightarrow$ (ii), observe que

$$a_1^{'x_1} \ldots a_k^{'x_k} = a_1^{\underbrace{x_1 u_{11} + \ldots + x_k u_{1k}}_{z_1}} \ldots a_k^{\underbrace{x_1 u_{k1} + \ldots + x_k u_{kk}}_{z_k}} = e$$

$$\Leftrightarrow z = (z_1, \ldots, z_k)^T \in \text{intcol}(M) = \text{intcol}(MV) = \text{intcol}(UD').$$

Logo,

$$\begin{aligned}
z_1 &= \overline{\alpha}_1 u_{11} d_1 + \ldots + \overline{\alpha}_m u_{1m} d_m + \overline{\alpha}_{m+1} u_{1m+1}.0 + \ldots + \overline{\alpha}_n u_{1k}.0 \\
z_2 &= \overline{\alpha}_1 u_{21} d_1 + \ldots + \overline{\alpha}_m u_{2m} d_m + \overline{\alpha}_{m+1} u_{2m+1}.0 + \ldots + \overline{\alpha}_n u_{2k}.0 \\
&\vdots \\
z_k &= \overline{\alpha}_1 u_{k1} d_1 + \ldots + \overline{\alpha}_m u_{km} d_m + \overline{\alpha}_{m+1} u_{km+1}.0 + \ldots + \overline{\alpha}_n u_{kk}.0.
\end{aligned} \tag{B.13}$$

Substituindo $z_i = x_1u_{i1} + \ldots + x_ku_{ik}$ nas equações em (B.13) para todo $i = 1, \ldots, k$, obtemos

$$\begin{aligned}
(x_1 - \overline{\alpha}_1 d_1)u_{11} + \ldots + (x_m - \overline{\alpha}_m d_m)u_{1m} + x_{m+1}u_{1m+1} + \ldots + x_k u_{1k} = 0 \\
(x_1 - \overline{\alpha}_1 d_1)u_{21} + \ldots + (x_m - \overline{\alpha}_m d_m)u_{2m} + x_{m+1}u_{2m+1} + \ldots + x_k u_{2k} = 0 \\
(x_1 - \overline{\alpha}_1 d_1)u_{k1} + \ldots + (x_m - \overline{\alpha}_m d_m)u_{km} + x_{m+1}u_{km+1} + \ldots + x_k u_{kk} = 0
\end{aligned}$$

ou equivalente,

$$(x_1 - \overline{\alpha}_1 d_1)\begin{bmatrix} u_{11} \\ u_{21} \\ \vdots \\ u_{k1} \end{bmatrix} + \ldots + (x_m - \overline{\alpha}_m d_m)\begin{bmatrix} u_{1m} \\ u_{2m} \\ \vdots \\ u_{km} \end{bmatrix} + \ldots + x_k \begin{bmatrix} u_{1k} \\ u_{2k} \\ \vdots \\ u_{kk} \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}$$

$\Leftrightarrow x_1 = \overline{\alpha}_1 d_1, \ldots, x_m = \overline{\alpha}_m d_m$, com $x_i = 0 \; \forall \; i = m+1, \ldots, k$, pois, U é invertível. Logo, $(x_1, \ldots, x_k)^T \in \text{intcol}(D')$.

Que (ii) $\Rightarrow$ (iii), segue imediatamente da definição de intcol(D'). Finalmente, vamos mostrar que (iii) $\Rightarrow$ (i). Com efeito, segue de (iii) que existem inteiros positivos $\alpha_1, \ldots, \alpha_m$ tais que

$$\begin{aligned}
a_1'^{x_1} \ldots a_k'^{x_m} &= a_1^{x_1u_{11}+\ldots+x_mu_{1m}} \ldots a_k^{x_1u_{k1}+\ldots+x_mu_{km}} \\
&= a_1^{\alpha_1 d_1 u_{11}+\ldots+\alpha_m d_m u_{1m}} \ldots a_k^{\alpha_1 d_1 u_{k1}+\ldots+\alpha_m d_m u_{km}} \\
&= a_1^{y_1} \ldots a_k^{y_k},
\end{aligned}$$

onde

$$\mathbf{y} = (y_1, \ldots, y_k)^T \in \text{intcol}(UD') = \text{intcol}(M). \tag{B.14}$$

Mas por hipótese $a_1^{y_1} \ldots a_k^{y} = e$, portanto, $a_1'^{x_1} \ldots a_k'^{x_k} = e$, e com isto terminamos a prova.

■

Antes de apresentarmos o algoritmo que fatora o grupo G numa soma direta de grupos cíclicos de ordens potências de primos, façamos algumas suposições sobre G:

(1) Temos uma única representação binária para cada elemento de G e podemos reconhecer eficientemente se uma palavra binária representa um elemento de G ou não.

(2) Usando a representação binária, para qualquer $a \in G$, podemos construir um operador linear unitário eficiente U_a, tal que, $U_a : |y\rangle \rightarrow |ay\rangle$.

(3) Podemos achar um conjunto gerador para G eficientemente.

(4) As ordens dos geradores são potências de primos.

Para a suposição 3 veja o teorema abaixo.

Teorema B.0.8 Seja G um grupo finito. Para qualquer inteiro $t \geq 0$, a probabilidade que $t + \lceil \log |G| \rceil$ elementos escolhidos aleatoriamente de G gerem G é dada por

$$\text{prob}\{\langle g_1, g_2, \ldots, g_{t+\lceil \log |G| \rceil} \rangle = G\} \geq 1 - \frac{1}{2^t} \text{ para } t \geq 0.$$

Demonstração: Veja Lomont (2004).

■

Para entendermos a suposição 4, seja a um elemento no conjunto gerador de G de ordem pq, onde $\text{mdc}(p, q) = 1,\ p \neq 1$ e $q \neq 1$. Note que podemos encontrar p e q eficientemente utilizando o algoritmo de Shor. Então pelo algoritmo Euclidiano, podemos encontrar inteiros r e s, tais que, $rp + sp = 1$. Assim, temos que

$$a = a^{rp+sq} = a^{rp} a^{sq}, \tag{B.15}$$

e é fácil verificar que a ordem de a^{rp} é q e a ordem de sq é p. Se p e q são potências de primos, basta substituirmos a por a^{rp} e a^{sq}, que continuamos com um conjunto

gerador, caso contrário, repetimos este procedimento, agora utilizando as ordens p e q. Façamos isto até que cada elemento no conjunto de geradores tenha ordem potência de primo.

Para a suposição 2, já que conhecemos a ordem pq de a, podemos calcular eficientemente $a^{-1} = a^{pq-1}$, e portanto, calcular U_a^{-1}.

Sabemos que se G é um grupo finito abeliano então G pode ser escrito como uma soma direta de seus p-subgrupos de Sylow[1] . Estes p-subgrupos de Sylow podem ser determinados eficientemente, uma vez que conhecemos a decomposição da ordem do grupo em seus fatores primos utilizando o algoritmo de Shor. Seja então $G = G_{p_1} \oplus \ldots \oplus G_{p_l}$ onde G_{p_i} é um p_i-subgrupo de Sylow de G com p_i primos distintos, para todo $i = 1, \ldots, l$. Considere o conjunto S_j formado por todos os elementos no conjunto gerador de G cujas ordens são potências do primo p_j. Veremos na proposição a seguir, a importância de termos definido o conjunto S_j desta forma .

Proposição B.0.2 Se $G = G_{p_1} \oplus \ldots \oplus G_{p_l}$ onde G_{p_i} é um p_i-subgrupo de Sylow de G para todo $i = 1, \ldots, l$ e $p_1, \ldots, p_l$ são primos distintos, então $G_{p_j} = \langle S_j \rangle$.

Demonstração: Para cada $a \in S_j$, seja $K_a = \langle a \rangle$. Como as ordens G_{p_i} são coprimas podemos ter $K_a = K_{p_1} \oplus \ldots \oplus K_{p_l}$ onde $K_{p_i} \leq G_{p_i}$ para todo $i = 1, \ldots, l$. Como K_a é um p_j-grupo, devemos ter $K_a \leq G_{p_j}$, o que implica que $S_j \subset G_{p_j}$, portanto,$\langle S_j \rangle \subset G_{p_j}$. Agora vamos mostrar que $G_{p_j} \subset \langle S_j \rangle$. De fato, se $g \in G_{p_j}$ então $\text{ord}(g) = p_j^{\alpha}$ para algum inteiro positivo α. Por outro lado, $g \in G$, então $g = a_1^{\alpha_1} \ldots a_k^{\alpha_k}$ com a_i no conjunto de geradores de G para todo $i = 1, \ldots, k$. Como $\text{ord}(g) = p_j^{\alpha}$, devemos ter $\text{ord}(a_i^{\alpha_i}) = p_j^{\alpha_i}$ $\forall$ $i = 1, \ldots, k$. Mas isto implica que $g \in S_j$, logo, $G_{p_j} \subset \langle S_j \rangle$ e isto demonstra a proposição B.0.2.

■

A Proposição B.0.2 nos diz como achar um conjunto de geradores para cada p-subgrupo de Sylow de G. Então, podemos obter uma decomposição para G

[1] Para verificar este fato basta notar que todo p-subgrupo de G é normal em G e as ordens dos p-subgrupos são coprimas.

tomando o produto das decomposições dos p-subgrupos de Sylow de G. Desta forma, o problema de achar uma decomposição para G reduz-se ao problema de achar a decomposição para cada p-subgrupo de Sylow de G.

O Algoritmo DecomporSylow, descrito a seguir, determina a decomposição de cada p-subgrupo de Sylow de G, uma vez dado o seu conjunto de geradores.

Algoritmo B.0.1 DecomporSylow

1: **ENTRADA**:
2: Um conjunto gerador $\{a_1, \ldots, a_k\}$ de um p-subgrupo de Sylow de G.
3: $q = \max\{p^{r_i},$ onde $\text{ord}(a_i) = p^{r_i}\ \forall\ i = 1, \ldots, k\}$.
4: **SAÍDA**:
5: Um conjunto de elementos $g_1, g_2, \ldots, g_l,\ l \leq k$, de G_p.
6: **PROCEDIMENTO**:
7: Defina $\rho : \mathbb{Z}_q^k \to G$ tal que $(x_1, \ldots, x_k) \mapsto a_1^{x_1} \ldots a_k^{x_k}$. Determine os geradores para o subgrupo oculto K de $\mathbb{Z}_q^k$ definido pela função ρ.
8: Determine elementos $y_1, \ldots, y_k \in \mathbb{Z}_q^k/K$ tais que ${\mathbb{Z}_q}^k/K = \langle y_1, \ldots, y_k \rangle$.
9: Saída é o conjunto $\{\rho(y_1), \ldots, \rho(y_l)\}$.

O subgrupo oculto K de $\mathbb{Z}_q^k$ é o conjunto

$$\begin{aligned} K &= \{\mathbf{x} \in \mathbb{Z}_q^k \mid \rho(\mathbf{y}) = \rho(\mathbf{x} + \mathbf{y}),\ \forall\, \mathbf{y} \in \mathbb{Z}_q^k\} \\ &= \{\mathbf{x} \in \mathbb{Z}_q^k \mid \rho(\mathbf{x}) = a_1^{x_1} \ldots a_k^{x_k} = e\} \\ &= \ker(\rho). \end{aligned} \tag{B.16}$$

É fácil ver que a função ρ é um homomorfismo sobrejetivo de $\mathbb{Z}_q^k$ em G, logo, temos um isomorfismo entre $\mathbb{Z}_q^k/K$ e G. Assim, se o conjunto $\{y_1, \ldots,\ y_l\}$ gera $\mathbb{Z}_q^k/K$, então $\{\rho(y_1), \ldots, \rho(y_l)\}$ gera G.

Vejamos agora como podemos determinar os geradores de $\mathbb{Z}_q^k/K$ eficientemente. Observe que $e_1, \ldots, e_k$ geram $\mathbb{Z}_q^k$, onde e_i é um $0,1$-vetor com 1 na i-ésima coordenada. Agora note que, como $K \leq \mathbb{Z}_q^k$ e $\{e_1, \ldots, e_k\}$ gera $\mathbb{Z}_q^k$, temos que $\{e_1 + K, \ldots, e_k + K\}$ gera o grupo $\mathbb{Z}_q^k/K$. Note que os geradores de K podem ser determinados de forma eficiente resolvendo o PSO no grupo $\mathbb{Z}_q^k$.

Proposição B.0.3 Seja A a matriz cujas colunas são os geradores do subgrupo

oculto K. Então $\mathbb{I}\mathbf{v} \in K$ se, e somente se, $\mathbf{v} \in \text{intcol}([M|A])$, onde $M = q\mathbb{I}$ e

$$[M|A] = \left[\begin{array}{ccc|c} q & \cdots & 0 & \\ \vdots & \ddots & \vdots & A \\ 0 & \cdots & q & \end{array}\right].$$

Demonstração: Note que, $\mathbb{I}\mathbf{v} \in K$ se, e somente se, existe um vetor $\mathbf{x}$ tal que

$$\begin{aligned} \mathbb{I}\mathbf{v} = A\mathbf{x} &\Leftrightarrow \mathbb{I}\mathbf{v} = \mathbb{I}A\mathbf{x} \Leftrightarrow \mathbb{I}(\mathbf{v} - A\mathbf{x}) = 0 \\ &\Leftrightarrow \mathbf{v} - A\mathbf{x} \in \text{intcol}(M) \\ &\Leftrightarrow \mathbf{v} - A\mathbf{x} = \alpha_1 q e_1 + \ldots + \alpha_k q e_k \\ &\Leftrightarrow \mathbf{v} = \alpha_1 q e_1 + \ldots + \alpha_k q e_k + A\mathbf{x} \\ &\Leftrightarrow \mathbf{v} \in \text{intcol}([M|A]). \end{aligned}$$

■

Aplicando o teorema B.0.7 ao conjunto de geradores

$$\{e_i + K \mid i = 1, \ldots, k\} \tag{B.17}$$

de $\mathbb{Z}_q^k/K$ e fazendo $M' = [M|A]$, nós obtemos elementos $y_1,\ldots,y_l \in \mathbb{Z}_q^k/K$ tais que

$$\mathbb{Z}_q^k/K = \langle y_1 \rangle \oplus \ldots \oplus \langle y_l \rangle, \tag{B.18}$$

como desejado.

Veremos agora uma aplicação do algoritmo DecomporSylow.

Exemplo B.0.3 Use o algoritmo DecomporSylow para encontrar uma decomposição do grupo $\mathbb{Z}_{35}^*$.

Demonstração: Note que $\mathbb{Z}_{35}^* = \langle 8, 16 \rangle$ onde $\text{ord}(8) = 2^2$ e $\text{ord}(26) = 2 \times 3$. Como o $\text{mdc}(2, 3) = 1$, pelo algoritmo de Euclides, podemos encontrar inteiros r e

s tais que $2r + 3s = 1$. Assim, temos que

$$26 = 26^{2r+3s} = (26^2)^r (26^3)^s. \tag{B.19}$$

Note que $\text{ord}(26^2) = 3$ e $\text{ord}(26^3) = 2$, logo, se substituírmos 26 por $26^2 \equiv 11 \mod 35$ e $26^3 \equiv 6 \mod 35$, obtemos um novo conjunto gerador para $\mathbb{Z}_{35}^*$ dado por

$$\mathbb{Z}_{35}^* = \langle 6, 8, 11 \rangle, \tag{B.20}$$

onde as ordens dos elementos são todas potências de primos.

Agora, vejamos quantos subgrupos de Sylow existem em $\mathbb{Z}_{35}^*$ a menos de subgrupos conjugados. Como $\phi(35) = 24 = 2^3 \times 3$, os subgrupos de Sylow de $\mathbb{Z}_{35}^*$ devem ter ordens 2^3 e 3 apenas. Vamos denominar os subgrupos de Sylow de $\mathbb{Z}_{35}^*$ de ordens 2^3 e 3 por G_2 e G_3, respectivamente. Sejam $S_2 = \{6, 8\}$ e $S_3 = \{11\}$ os conjuntos formados pelos geradores de $\mathbb{Z}_{35}^*$ cujas ordens são potências de 2 e 3, respectivamente. Segue da Proposição B.0.2 que

$$G_2 = \langle S_2 \rangle \text{ e } G_3 = \langle S_3 \rangle. \tag{B.21}$$

Como o grupo G_3 é cíclico de ordem potência de primo, basta aplicarmos o algoritmo DecomporSylow ao grupo G_2, e depois tomarmos a soma direta com G_3 para obtermos a decomposição desejada.

Para aplicarmos o algoritmo DecomporSylow ao grupo G_2, devemos passar como entrada para o algoritmo o conjunto de geradores $\{6, 8\}$ e $q = \max\{\text{ord}(6), \text{ord}(8)\} = 4$. Considere então a função $\rho : \mathbb{Z}_q^2 \to G_2$ tal que $\rho((x_1, x_2)) = 6^{x_1} \times 8^{x_2} \mod 35$. Segue da expressão (B.16) que o subgrupo oculto K de $\mathbb{Z}_4^2$ é o conjunto

$$K = \{\mathbf{x} \in \mathbb{Z}_4^2 \mid \rho(\mathbf{x}) = 6^{x_1} \times 8^{x_2} = 1\}. \tag{B.22}$$

Após alguns cálculos, vemos que $K = \langle (2, 0) \rangle$.

Agora, seja $[M|A] = \left[\begin{array}{cc|c} 4 & 0 & 2 \\ 0 & 4 & 0 \end{array}\right]$ dada como na Proposição B.0.3. Então, basta aplicar o Teorema B.0.7 ao conjunto de geradores $\underbrace{e_1 + K}_{a_1}$, $\underbrace{e_2 + K}_{a_2}$ de $\mathbb{Z}_4^2$ e $M' = [M|A]$.

Sejam

$$D = \begin{bmatrix} 2 & 0 & 0 \\ 0 & 4 & 0 \end{bmatrix} \tag{B.23}$$

a forma normal de Smith da matriz M',

$$U = \begin{bmatrix} 1 & 0 \\ 33 & 1 \end{bmatrix} \text{ e } V = \begin{bmatrix} 0 & 0 & 34 \\ 1 & 1 & 0 \\ 1 & 0 & 2 \end{bmatrix} \tag{B.24}$$

matrizes unimodulares tais que $UM'V = D$. Observe que $g_i = a_i^{'} \; \forall \; i = 1, 2$. Logo o conjunto $\{g_1, g_2\}$ dado por

$$g_1 = a_1^{'} = a_1 + a_2^0 = (1, 0) + K, \tag{B.25}$$

$$g_2 = a_2^{'} = a_1^{33} + a_2 = (3, 1) + K \tag{B.26}$$

é tal que

$$\mathbb{Z}_4^2/K = \langle g_1 \rangle \oplus \langle g_2 \rangle \, . \tag{B.27}$$

Como a função $\rho : \mathbb{Z}_4^2/K \to G_2$ é um isomorfismo, temos

$$G_2 = \langle \rho(g_1) \rangle \oplus \langle \rho(g_2) \rangle \, . \tag{B.28}$$

Então,

$$\begin{aligned} \rho(g_1) &= \rho((1, 0)) = 6^1 \times 8^0 \bmod 35 = 6, \\ \rho(g_2) &= \rho((3, 1)) = 6^3 \times 8^1 \bmod 35 = 13 \end{aligned} \tag{B.29}$$

e

$$G_2 = \langle 6 \rangle \oplus \langle 13 \rangle \,. \tag{B.30}$$

Portanto,

$$\mathbb{Z}_{35}^{*} = \langle 11 \rangle \oplus \langle 6 \rangle \oplus \langle 13 \rangle \,. \tag{B.31}$$

■

Apêndice C

Tópicos em Computação Quântica

Neste apêndice faremos um apanhado geral dos conceitos básicos sobre computação quântica, necessários para o entendimento da tese. Descrevemos os quatro postulados fundamentais da Mecânica Quântica e as portas lógicas quânticas mais usadas. Para uma descrição mais detalhada destes conceitos, sugerimos o leitor a excelente referência Nielsen e Chuang (2003). Para abordagens mais básicas sugerimos as referências Lavor et al. (2003a,b); Marquezino (2006); Lomont (2004); Batty et al. (2003).

C.1 Os Postulados da Mecânica Quântica

O primeiro postulado trata da descrição matemática de um sistema quântico isolado[1] .

Postulado 1 (Espaço de Estados) Associado a qualquer sistema quântico isolado, existe um espaço vetorial complexo com produto interno, um espaço de Hilbert, chamado espaço de estados do sistema. O sistema é completamente descrito por um vetor unitário do espaço de estados que chamaremos vetor de estado.

■

Aqui, trataremos apenas de espaços vetoriais de dimensão finita, logo podemos assumir nosso espaço de estados como sendo $\mathbb{C}^n$, o espaço vetorial complexo de dimensão n.

[1] Um sistema quântico isolado é aquele que não interage com nenhum outro sistema físico.

Na computação clássica, o *bit* é a unidade básica de armazenamento de informação, e pode armazenar uma de duas posições, 0 ou 1. Na computação quântica, a unidade básica de armazenamento de informação é o *q-bit*[2] , uma abstração de uma partícula quântica de dois níveis. Enquanto um dispositivo clássico armazena sempre ou na posição 0 ou na posição 1, uma partícula quântica pode assumir uma "superposição"dos dois níveis. Matematicamente, esta superposição pode ser descrita por um vetor unitário no espaço $\mathbb{C}^2$, isto é,

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

Os estados $|0\rangle$ e $|1\rangle$ estão descritos na notação de Dirac e é a notação padrão para representar estados em computação quântica. As amplitudes α e β são números complexos satisfazendo

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

O estado $|\psi\rangle$ é um vetor em $\mathbb{C}^2$, onde os estados $|0\rangle$ e $|1\rangle$ formam uma base ortonormal, chamada *base computacional*. Além disso, o estado $|0\rangle$ é diferente do vetor nulo $0 = (0,0) \in \mathbb{C}^2$; ele representa o primeiro vetor da base. As representações matriciais dos vetores $|0\rangle$ e $|1\rangle$ são dadas por

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \quad \text{e} \quad |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}. \tag{C.3}$$

Para considerarmos múltiplos q-bits precisamos do conceito de produto tensorial. Suponha V e W dois espaços vetoriais complexos de dimensões m e n, respectivamente. O produto tensorial $V \otimes W$ é um espaço vetorial mn-dimensional. Os elementos de $V \otimes W$ são combinações lineares de produtos tensoriais $|v\rangle \otimes |w\rangle$ satisfazendo as seguintes propriedades: para todo $z \in \mathbb{C}$, $|v\rangle, |v_1\rangle, |v_2\rangle \in V$ e $|w\rangle, |w_1\rangle, |w_2\rangle \in W$ temos

(1) $z(|v\rangle \otimes |w\rangle) = (z\,|v\rangle \otimes |w\rangle) = (|v\rangle \otimes z\,|w\rangle)$;

[2] Q-bit é a abreviação de quantum bit.

(2) $(|v_1\rangle \otimes |v_2\rangle) \otimes |w\rangle = (|v_1\rangle \otimes |w\rangle) + (|v_2\rangle \otimes |w\rangle)$;

(3) $|n\rangle \otimes (|w_1\rangle + |w_2\rangle) = (|v\rangle \otimes |w_1\rangle) + (|v\rangle \otimes |w_2\rangle)$.

Podemos também representar o produto tensorial $|v\rangle \otimes |w\rangle$ como $|v\rangle |w\rangle, |v, w\rangle$ ou $|vw\rangle$.

Sejam A e B operadores lineares definidos nos espaços V e W, respectivamente. Definimos o operador $A \otimes B$ em $V \otimes W$ como sendo

$$(A \otimes B)(|v\rangle \otimes |w\rangle) = A|v\rangle \otimes B|w\rangle, \tag{C.4}$$

onde $|v\rangle \in V$ e $|w\rangle \in W$. Sua representação matricial é dada por[3]

$$A \otimes B = \begin{bmatrix} A_{11}B & \dots & A_{1m}B \\ \vdots & \ddots & \vdots \\ A_{m1}B & \dots & A_{mm}B \end{bmatrix}. \tag{C.5}$$

Por exemplo, o produto tensorial $|0\rangle |1\rangle$ é dado por[4]

$$|0\rangle \otimes |1\rangle = |01\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \otimes \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} \in \mathbb{C}^4. \tag{C.6}$$

O estado geral $|\psi\rangle$ de dois q-bits é uma superposição dos estados $|00\rangle, |01\rangle, |10\rangle$ e $|11\rangle$:

$$|\psi\rangle = \alpha_0 |00\rangle + \alpha_1 |01\rangle + \alpha_2 |10\rangle + \alpha_3 |11\rangle, \tag{C.7}$$

com $\sum_{i=0}^{3} |\alpha_i|^2 = 1$. O estado $|\psi\rangle$ é um vetor num espaço vetorial complexo de dimensão 4.

[3] Estamos usando a mesma notação para o operador e sua representação matricial.

[4] A notação $|\psi\rangle^{\otimes n}$ significa $\underbrace{|\psi\rangle \otimes |\psi\rangle \otimes \dots \otimes |\psi\rangle}_{n \text{ vezes}}$.

Olhando para os rótulos $00, 01, 10, 11$ como sendo números binários, podemos fazer a seguinte relação com sua representação na base decimal: $|00\rangle = |0\rangle, |01\rangle = |1\rangle, |10\rangle = |2\rangle$ e $|11\rangle = |3\rangle$. Assim, um estado geral de um vetor $|\psi\rangle$ de n q-bits é uma superposição de 2^n estados da forma $|0\rangle, |1\rangle, \ldots, |2^n - 1\rangle$:

$$|\psi\rangle = \sum_{i=0}^{2^n-1} \alpha_i |i\rangle, \tag{C.8}$$

com as amplitudes α_i satisfazendo $\sum_{i=0}^{2^n-1} |\alpha_i|^2 = 1$. A base $\{|0\rangle, |1\rangle, \ldots, |2^n - 1\rangle\}$ é chamada de *base computacional* e é uma base ortonormal.

Segue da notação de Dirac que $\langle\psi|$ representa o vetor transposto conjugado de $|\psi\rangle$. O símbolo $\langle .|$ é chamado *bra*. Assim, dados dois vetores $|\psi\rangle$ e $|\psi'\rangle$ em um espaço vetorial V, $\langle\psi|\psi'\rangle$ define um produto interno em V. O produto $|\psi\rangle\langle\psi'|$ definido por $(|\psi\rangle\langle\psi'|)|v\rangle = |\psi\rangle\langle\psi'|v\rangle$ é chamado *produto externo* de $|\psi\rangle$ e $|\psi'\rangle$.

A seguir, apresentamos o segundo postulado fundamental da mecânica quântica. Este postulado trata da evolução dos sistemas físicos quânticos.

Postulado 2 (Evolução dos Estados) A evolução de um sistema quântico isolado é descrita por um operador unitário. Isto é, o estado $|\psi\rangle$ do sistema no instante t_1 está relacionado ao estado $|\psi'\rangle$ no instante t_2 por um operador unitário U que depende apenas de t_1 e t_2 e tal que $|\psi'\rangle = U|\psi\rangle$.

■

Como todo operador unitário é invertível, segue do Postulado 2 que é sempre possível recuperar o estado inicial do sistema quântico através do operador U^{-1}. Assim, podemos dizer que a computação quântico é um tipo de computação reversível, Toffoli (1980a,b).

C.1.1 Medidas Quânticas

Uma medida quântica é um procedimento físico que extrai informações sobre um sistema quântico. O postulado a seguir, também intitulado, *Postulado da*

Medida, fornece a maneira como as medidas em um sistema quântico devem ser efetuadas.

Postulado 3 As medidas quânticas são descritas por determinados operadores de medida $\{M_m\}$. Esses operadores atuam sobre o espaço de estados do sistema. O índice m refere-se aos possíveis resultados da medida. Se o estado de um sistema for $|\psi\rangle$, imediatamente antes da medida, a probabilidade de um resultado m ocorrer é dada por

$$p(m) = \langle\psi| M_m^\dagger M_m |\psi\rangle , \tag{C.9}$$

e o estado do sistema após a medida será

$$\frac{M_m |\psi\rangle}{\sqrt{p(m)}}. \tag{C.10}$$

Os operadores de medida satisfazem a relação de completude

$$\sum_m M_m^\dagger M_m = I. \tag{C.11}$$

■

Descreveremos agora um caso especial das medidas descritas no Postulado 3, o postulado geral das medidas. Essa classe especial de medidas é conhecida como *medidas projetivas* é o tipo de medida que utilizamos na tese.

Definição C.1.1 (Medidas Projetivas) Uma medida projetiva é descrita por um observável M, um operador no espaço de estados do sistema a ser observado. O observável tem uma decomposição espectral

$$M = \sum_m m P_m, \tag{C.12}$$

onde P_m é o projetor sobre o auto espaço de M cujo autovalor é m. Os possíveis resultados da medida são os autovalores de M. Se o estado do sistema imediatamente antes da medida é $|\psi\rangle$, então a probabilidade que o resultado da medida

seja m é dada por

$$p(m) = \langle\psi| P_m |\psi\rangle . \tag{C.13}$$

Obtido o resultado m, o estado do sistema logo após a medida é

$$|\psi'\rangle = \frac{P_m |\psi\rangle}{\sqrt{p(m)}}. \tag{C.14}$$

■

O Postulado 3 se reduz ao postulado das medidas projetivas quando os operadores de medida satisfazem a relação de completude $\sum_m M_m^\dagger M_m = I$ e além disso são também projetores.

É comum na literatura uma descrição alternativa para as medidas projetivas. Geralmente, ao invés de fornecer um observável $M = \sum_m mP_m$, uma medida projetiva é descrita por uma lista de projetores ortogonais P_m satisfazendo as condições $\sum_m P_m = I$ e $P_m P_{m'} = \delta_{m,m'} P_m$. Neste caso, o observável correspondente é $M = \sum_m mP_m$.

Como um exemplo de medida projetiva, considere um estado quântico de n q-bits escrito na base computacional,

$$|\psi\rangle = \sum_{i=0}^{2^n-1} a_i |i\rangle .$$

Seja também os projetores $P_j = |j\rangle \langle j|$, para todo $j = 0, \ldots, 2^n - 1$. Se medirmos $|\psi\rangle$ utilizando esses projetores, obtemos o estado $|j\rangle$ com probabilidade $|a_j|^2$. Isso quer dizer que o quadrado do módulo da amplitude de um vetor da base computacional representa a probabilidade desse mesmo vetor ser observado nesta base. Esse tipo de medida é conhecida como *medida na base computacional*.

Outro tipo de medida que também pode ser considerada como um caso especial do Postulado 3 são as medidas POVM[5] .

Definição C.1.2 (Medidas POVM) Seja $\{E_m\}$ um conjunto qualquer de ope-

[5] A sigla POVM significa Positive Operator-Valued Measure.

radores satisfazendo as seguintes condições:

(a) Os operadores E_m são positivos[6] para todo m.

(b) Vale a relação de completude $\sum_m E_m = I$.

A probabilidade de um resultado m ocorrer em uma medida POVM é

$$p(m) = \langle\psi| E_m |\psi\rangle . \tag{C.15}$$

■

As medidas POVM são mais utilizadas quando estamos interessados apenas na estatística da medida, isto é, nas diversas possibilidades dos diferentes resultados, e não no estado do sistema imediatamente após a medida.

Postulado 4 (Sistemas Compostos) O espaço de estados de um sistema quântico composto é o produto tensorial dos espaços de estados dos sub-sistemas quânticos que o compõem. Numerando de 1 até n tais sub-sistemas e supondo que o sub-sistema i esteja no estado $|\psi_i\rangle$, temos que o sistema composto está no estado

$$|\psi_1\rangle \otimes \cdots \otimes |\psi_n\rangle .$$

■

Esse último postulado nos mostra como espaços de estados de sistemas quânticos diferentes devem ser combinados para formar sistemas compostos. Por exemplo, considere o espaço composto por dois sub-sistemas de um q-bit, um sistema quântico de dois q-bits. Seu espaço de estados é $\mathbb{C}^2 \otimes \mathbb{C}^2$, um espaço complexo 4-dimensional cuja base computacional é formada pelos vetores $|00\rangle = |0\rangle \otimes |0\rangle = (1,0,0,0)^T$, $|01\rangle = |0\rangle \otimes |1\rangle = (0,1,0,0)^T$, $|10\rangle = |1\rangle \otimes |0\rangle = (0,0,1,0)^T$ e $|11\rangle = |1\rangle \otimes |1\rangle = (0,0,0,1)^T$.

[6] Seja $A : V \to V$ um operador linear num espaço vetorial de dimensão finita V. Dizemos que A é positivo se para todo $|v\rangle \in V$ temos $\langle v|Av\rangle \geq 0$.

C.2 Portas Lógicas e Circuitos Quânticos

De forma bem geral, a computação quântica pode ser vista como um conjunto de estados quânticos que são transformados por aplicações de operadores unitários. Esses operadores desempenham um papel semelhante às portas lógicas clássicas, eles são responsáveis pela manipulação da informação. Aqui, faremos uma breve revisão das portas lógicas quânticas mais utilizadas na computação quântica.

Começamos com a porta X. Esta é a versão quântica da porta NOT clássica. Sua atuação na base computacional é a seguinte: $|0\rangle \mapsto |1\rangle$ e $|1\rangle \mapsto |0\rangle$, ou seja, $|j\rangle \mapsto |1 \oplus j\rangle$, onde $\oplus$ denota a soma binária. Sua descrição como operador unitário é dada pela matriz

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

Sua descrição como um circuito quântico atuando num q-bit arbitrário $|\psi\rangle = a\,|0\rangle + b\,|1\rangle$ é

$$|\psi\rangle \;\text{—}\boxed{X}\text{—}\; a\,|1\rangle + b\,|0\rangle$$

Figura C.1: Circuito da porta X.

Outras portas de um q-bit importantes para a computação quântica são a porta Hadamard, denotada por H, a porta fase, denotada por S e a porta $\pi/8$, denotada por T. Suas representações matriciais estão listadas abaixo.

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix},\ S = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix},\ T = e^{\pi i/8} \begin{bmatrix} e^{-\pi i/8} & 0 \\ 0 & e^{\pi i/8} \end{bmatrix}$$

A porta H é muito usada em algoritmos para criar um estado de superposição de todos os vetores da base computacional[7] . A forma usual de gerar essa

[7] A maioria dos algoritmos quânticos descritos nesta tese para o PSO utilizam a porta H para gerar uma superposição inicial sobre todos os elementos do grupo.

superposição é aplicar $H^{\otimes n}$ ao estado $|0\rangle^{\otimes n}$:

$$(H|0\rangle)^{\otimes n} = \frac{1}{\sqrt{2^n}} \sum_{j=0}^{2^n-1} |j\rangle . \tag{C.16}$$

Vamos agora às portas de 2 q-bits. A porta CNOT é uma porta quântica controlada e é uma das principais portas usadas em algoritmos. Ela trabalha com dois q-bits, um q-bit de controle e o outro o q-bit alvo. Como uma porta controlada clássica, o q-bit alvo só será afetado pela porta NOT se o q-bit de controle estiver no estado $|1\rangle$. Sua atuação na base computacional é

$$|j_1\rangle |j_2\rangle \mapsto |j_1\rangle X^{j_1} |j_2\rangle = |j_1\rangle |j_1 \oplus j_2\rangle . \tag{C.17}$$

Sua representação matricial é dada por

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

O circuito da porta CNOT é exibido na Figura C.2

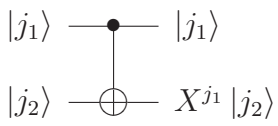


Figura C.2: Circuito da porta CNOT. A linha de cima representa o q-bit de controle e a de baixo o q-bit alvo.

De forma mais geral, seja U uma porta quântica de n q-bits. Denotamos por $C(U)$, a porta U-controlada, que é uma operação sobre $n+1$ q-bits definida por sua atuação na base computacional: $|j_1\rangle |k\rangle \mapsto |j_1\rangle U^{j_1} |k\rangle$, onde $|j_1\rangle \in \{|0\rangle, |1\rangle\}$ e $|k\rangle \in \{|0\rangle, \cdots, |2^n - 1\rangle\}$. Seu circuito é mostrado na Figura C.3.

Podemos também definir um operador $\tilde{C}(U)$ sobre $m+n$ q-bits da seguinte

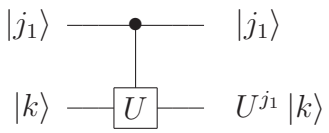
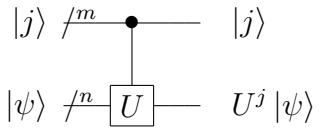


Figura C.3: Circuito da porta U controlada.

forma: Dados $|j\rangle \in \{|0\rangle, \cdots, |2^m - 1\rangle\}$ e $|k\rangle \in \{|0\rangle, \cdots, |2^n - 1\rangle\}$, a atuação de $\tilde{C}(U)$ é dada por $|j\rangle|k\rangle \mapsto |j\rangle U^j |k\rangle$. Esta porta, pode ser vista como uma porta $C(U)$ generalizada, onde seu q-bit de controle é substituído por um estado de controle. No circuito abaixo vemos sua representação esquemática.



A representação gráfica é a mesma de $C(U)$, porém não há perigo de confusão pois o primeiro registrador[8] tem mais do que um q-bit. É interessante notar que a porta $\tilde{C}(U)$ pode ser decomposta como uma composição de portas $C(U)$. Para tanto, considere a representação binária do registrador de controle, digamos $|j\rangle = |j_1\rangle \cdots |j_m\rangle$. O circuito da Figura C.4 mostra como fazer tal decomposição, Portugal et al. (2006).

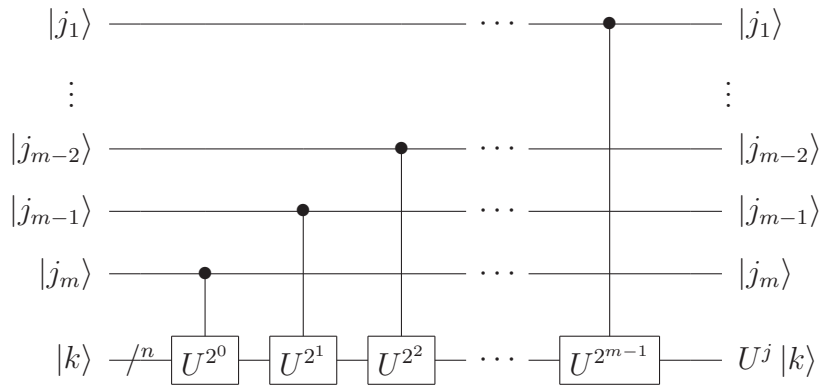


Figura C.4: Circuito decompondo $\tilde{C}(U)$ através da porta controlada $C(U)$.

[8] A palavra registrador é usada como sinônimo para um vetor de estado.