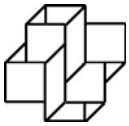

Laboratório Nacional de Computação Científica

Programa de Pós Graduação em Modelagem Computacional

Problema do subgrupo oculto em grupos nilpotentes

Por

Tharso Dominisini Fernandes

PETRÓPOLIS, RJ - BRASIL

ABRIL DE 2008

PROBLEMA DO SUBGRUPO OCULTO EM GRUPOS NILPOTENTES

Tharso Dominisini Fernandes

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

Aprovada por: _____

Prof. Renato Portugal, D.Sc
(Presidente)

_____

Prof. Eduardo Lúcio Mendes Garcia, D.Sc.

_____

Prof. Guilherme Leal, D.Sc.

_____

Prof. Maurício Vieira Kritz, D.Sc.

_____

Prof. Carlile Lavor, D.Sc.

PETRÓPOLIS, RJ - BRASIL
ABRIL DE 2008

FERNANDES, THARSO DOMINISINI

f363p Problema do subgrupo oculto nilpotentes / Tharso Dominisini Fernandes. Petropólis, RJ. : Laboratório Nacional de Computação Científica, 2008.

xv,63 p. : il.; 29 cm

Orientadore(s): Renato Portugal

Dissertação (M.Sc.) – Laboratório Nacional de Computação Científica, 2008.

1. Computação Quântica. 2. Problema do Subgrupo Oculto. 3. Algoritmos Quânticos. I. Renato Portugal II. LNCC/MCT III. Título

CDD 004.1

Imagination is more important than knowledge. *(Albert Einstein)*

A minha avó Joaquina

Agradecimentos

A minha família, pelo apoio.

A minha namorada *Sun*, pelo amor, carinho e compreensão.

A todos que me ajudaram com seu apoio e sugestões, dentre os quais, o meu orientador, pela dedicação e incentivo demonstrados durante o desenvolvimento desta dissertação; os colegas do LNCC, pelas sugestões e contribuições.

A FAPERJ e a CAPES, pelo apoio financeiro; ao LNCC, pela infraestrutura.

Principalmente sou muito agradecido a DEUS, por tudo.

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

PROBLEMA DO SUBGRUPO OCULTO EM GRUPOS NILPOTENTES

Tharso Dominisini Fernandes

Abril , 2008

Orientador: Renato Portugal, D.Sc

Computadores quânticos prometem resolver certos problemas assintoticamente mais rápido do que os computadores clássicos. Algoritmos quânticos, como o algoritmo de Shor, podem ser considerados casos particulares do chamado Problema do Subgrupo Oculto(PSO). O PSO consiste em encontrar um subgrupo H de um grupo G por meio de avaliações de uma função f que é constante em classes laterais de H e distinta em classes laterais diferentes. O PSO em grupos abelianos é resolvido eficientemente em um computador quântico, mas será que os computadores quânticos podem resolver o PSO em grupos não abelianos? Esta questão tem sido discutida regularmente pela comunidade científica devido a importantes aplicações, como é o caso do problema de isomorfismo de grafos e do problema do menor vetor em um reticulado.

Nesta dissertação é feita uma revisão do trabalho de Ivanyos et al. (2007a), o qual apresenta uma solução para o PSO em grupos nilpotentes de classe 2. Com esta finalidade, é elaborada uma breve revisão sobre a Computação Quântica; são mostradas algumas características dos grupos nilpotentes e dos grupos solúveis, dando uma atenção especial aos grupos nilpotentes de classe 2; é exposto o método padrão de solução do PSO em grupos abelianos; também são exibidas as principais características de seqüências policíclicas e reduções importantes do PSO em classes de grupos nilpotentes usando as propriedades de seqüências policíclicas; e por fim

é apresentado um algoritmo quântico eficiente para resolução do PSO em grupos nilpotentes de classe 2.

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

HIDDEN SUBGROUP PROBLEM IN NILPOTENT GROUPS

Tharso Dominisini Fernandes

April, 2008

Advisor: Renato Portugal, D.Sc

Quantum computers may solve certain problems asymptotically faster than the classical computers. Quantum algorithms, such as Shor's algorithm, may be considered as a particular case of the Hidden Subgroup Problem (HSP). The HSP consists in finding a subgroup H of a group G by evaluating a function f, which is constant in cosets of H and distinct for each coset. The HSP for Abelian groups is efficiently solved in a quantum computer, but is quantum computers can solve the HSP in non-Abelian groups efficiently? This question has been regularly discussed by the scientific community due to the importance of some applications, such as the graph isomorphism problem and the short vector in a lattice.

In this dissertation we review the Ivanyos et al. (2007a) that address HSP in nilpotent groups of class 2. We make a brief review on Quantum Computing; we address some characteristics of nilpotent groups and solvable groups, with special attention to nilpotent groups of class 2; we discuss the standard method of solution of the HSP in Abelian groups; we present the main characteristics of the polycyclic sequences and important reductions of the HSP in classes of nilpotent groups using the properties of polycyclic sequences. Finally, we present an efficient algorithm to solve the HSP in nilpotent groups of class 2.

Sumário

Lista de Figuras

Figura

Lista de Tabelas

Tabela

Símbolos e Abreviaturas

- $A_{m\times n}$: Matriz A qualquer, de dimensão $m \times n$
- a_{jk}: Elemento da linha j e coluna k de uma matriz A
- A^T: Transposta da matriz A
- $A^\dagger$: Transposta conjugada da matriz A
- A^*: Complexo conjugado da matriz A
- $A \otimes B$: Produto tensorial entre A e B
- $A^{\otimes n}$: Produto tensorial entre A de A com A repetido n vezes
- $|\psi\rangle$: Vetor, também chamado *ket*
- $\langle\psi|$: Vetor dual, também chamado *bra*
- $\langle\varphi|\psi\rangle$: Produto escalar entre $|\varphi\rangle$ e $|\psi\rangle$
- $||\,|\psi\rangle\,||$: Norma do vetor $|\psi\rangle$ definida por $||\,|\psi\rangle\,|| = \langle\psi|\psi\rangle^{1/2}$
- $|\varphi\rangle \otimes |\psi\rangle$: Produto tensorial entre $|\varphi\rangle$ e $|\psi\rangle$
- $|\varphi\rangle\,|\psi\rangle$: Produto tensorial entre $|\varphi\rangle$ e $|\psi\rangle$
- $\langle\varphi|\,A\,|\psi\rangle$: Produto escalar entre $|\varphi\rangle$ e $A\,|\psi\rangle$
- $\log(\cdot)$: logaritmo na base 2
- $\ln(\cdot)$: logaritmo Neperiano
- $O(\cdot)$: Complexidade computacional no pior caso, $f(x) = O(g(x))$ se existem C, x_0 tais que $f(x) < Cg(x), \forall x > x_0$
- $\mathbb{Z}$: Conjunto dos números inteiros
- $\mathbb{C}$: Conjunto dos números complexos
- $\mathbb{Z}_\mathbb{N}$: Conjunto dos inteiros $\{0, 1, \ldots, N-1\}$ com a soma módulo 2
- ω_N: Raiz principal da unidade, definida por $\omega_N \equiv \exp^{\frac{2\pi i}{N}}$

- $\lfloor \cdot \rfloor$: Maior número inteiro que seja menor ou igual a $\cdot$
- $\lceil \cdot \rceil$: Menor número inteiro que seja maior ou igual a $\cdot$

Capítulo 1

Introdução

A Computação Quântica, que nos últimos anos tem sido vista como uma área de pesquisa em grande crescimento, faz uso das propriedades da Mecânica Quântica na Teoria da Computação, permitindo o desenvolvimento de algoritmos exponencialmente mais rápidos do que os correspondentes clássicos existentes.

A Computação Quântica tem início na década de 80. Feynman (1982) mostra que a Mecânica Quântica pode ser usada para computar informações. Poucos anos depois, Deutsch (1985) mostra que a Computação Clássica pode ser vista como um caso particular da Computação Quântica em termos de computabilidade. E assim começam a surgir os primeiros algoritmos quânticos.

Deutsch e Jozsa (1992) apresentam um algoritmo quântico para determinar se uma dada função é balanceada ou não, enquanto Simon (1997) propõe um algoritmo quântico para determinar o período de uma função periódica. Mas a comunidade científica só passou a dar importância à Computação Quântica quando Shor (1994) apresentou um algoritmo quântico para fatoração de números inteiros, algoritmo esse que obteve ganho exponencial em relação à seus equivalentes clássicos. Jozsa (1997) apontou que esses algoritmos eram casos particulares de um problema maior, o Problema do Subgrupo Oculto (PSO)[1] . Há outros algoritmos quânticos que não são casos particulares do PSO, mas são importantes para a Computação Quântica,

[1] O PSO consiste em encontrar um subgrupo H de um grupo G por meio de avaliações de uma função f que é constante em classes laterais de H e distinta para classes laterais diferentes. No capítulo 4 é feita a definição formal do problema.

como o algoritmo de Grover (1996).

Vale ressaltar que as aplicações do PSO não se restringem às citadas acima, dentre outras aplicações pode-se destacar:(1) uma solução eficiente para o PSO no grupo simétrico implica em uma solução eficiente para o problema do isomorfismo de grafos, implicação que pode ser vista com detalhes em Dalcumune (2008); (2) uma solução eficiente para o PSO no grupo diedral implica em uma solução eficiente para o Problema do Menor Vetor em um Reticulado (Khot, 2005).

Um grande esforço tem sido feito com objetivo de resolver o PSO devido a sua grande importância. Encontrar uma solução para o PSO no caso geral é uma tarefa que ainda não teve êxito, uma alternativa que tem sido usada é buscar soluções em classes de grupos específicas. No caso de grupos abelianos o problema já está completamente resolvido (Mosca e Ekert, 1999).

A Transformada de Fourier Quântica desempenha um papel fundamental na solução do PSO em grupos abelianos, já em grupos não abelianos há duas técnicas que em geral são usadas: a primeira extende a solução do PSO abeliano à classes de grupos não abelianos usando a Transformada de Fourier Quântica não abeliana (Hales e Hallgren, 2000; Puschel et al., 1999; Moore et al., 2004; Grigni et al., 2001); a outra técnica reduz o PSO, mesmo que em grupos não abeliano, à instâncias de grupos abelianos para revolver o PSO (Ivanyos et al., 2007b, 2003; Friedl et al., 2003).

Nesta dissertação é feita uma revisão do trabalho de Ivanyos et al. (2007a), no qual é apresentado uma solução eficiente para PSO em grupos nilpotentes de classe 2. A solução proposta por Ivanyos et al. (2007a) faz uso da estrutura dos grupos nilpotentes de classe 2 para reduzir o PSO nesta classe de grupos ao PSO abeliano, generalizando o método usado em Ivanyos et al. (2007b) para resolução do PSO em grupos extra-especiais. Embora Ivanyos et al. (2007a) não solucionem o PSO em grupos nilpotentes gerais, eles fazem uma redução relevante, a qual supostamente contribuirá para futuros trabalhos que objetivam resolver o PSO em grupos nilpotentes.

No capítulo 2 é exposta uma revisão sobre a Computação Quântica, destacando-se o contexto histórico, a Mecânica Quântica e a estrutura dos algoritmos quânticos. No capítulo 3, algumas propriedades dos grupos nilpotentes são expostas, dando uma atenção especial aos grupos nilpotentes de classe 2. No capítulo 4 é apresentado o método de solução padrão do PSO em grupos abelianos, com a omissão de alguns detalhes. No capítulo 5 é visto como o PSO é resolvido em grupos nilpotentes de classe 2, e para esse fim são apresentadas algumas propriedades das seqüências policíclicas, além de reduções do PSO em grupos nilpotentes gerais, as quais são fundamentais não só para o PSO em grupos nilpotentes de classe 2, mas também para futuras investidas em busca de soluções para o PSO em toda classe de grupos nilpotentes.

1.1 Notação

A notação utilizada neste trabalho é a mesma da Mecânica Quântica, a notação de Dirac. Essa notação facilita a manipulação algébrica no uso das propriedades matemáticas dos Sistemas Quânticos.

Um vetor em um espaço Hilbert $\mathcal{H}$ é denotado por $|\psi\rangle$ e chamado de *ket*. O seu dual é representado por $\langle\psi|$.

O produto interno de dois vetores $|\psi\rangle, |\phi\rangle$ é dado por $\langle\psi|\,|\phi\rangle$, que é escrito de forma simplicada como $\langle\psi\,|\phi\rangle$.

Um produto que será utilizado nesta dissertação é o produto tensorial ou produto de Kronecker (Loan, 1992).

A definição de produto Kronecker em matrizes é suficiente para este trabalho, embora haja definições de produto tensorial muito mais gerais do que será apresentada aqui.

O produto tensorial entre duas matrizes $A_{m\times n}$ e $B_{p\times q}$,

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix}, \; B = \begin{pmatrix} b_{11} & b_{12} & \cdots & b_{1q} \\ b_{21} & b_{22} & \cdots & b_{2q} \\ \vdots & \vdots & \ddots & \vdots \\ b_{p1} & b_{p2} & \cdots & b_{pq} \end{pmatrix}, \tag{1.1}$$

é a matriz definida por

$$A \otimes B = \begin{pmatrix} a_{11}B & a_{12}B & \cdots & a_{1n}B \\ a_{21}B & a_{22}B & \cdots & a_{2n}B \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1}B & a_{m2}B & \cdots & a_{mn}B \end{pmatrix}, \tag{1.2}$$

denotada por $(A \otimes B)_{mp\times nq}$. Um caso particular do produto tensorial é o produto tensorial entre dois vetores que pode ser escrito de forma simplificada por $|\psi\rangle\,|\phi\rangle$. Sejam $|\mu_1\rangle, |\mu_2\rangle$ vetores de dimensão m, $|\nu_1\rangle, |\nu_2\rangle$ vetores de dimensão n e z um escalar. O produto tensorial satisfaz as seguintes propriedades:

(1) O vetor $|\mu_1\rangle \otimes |\nu_1\rangle$ é um vetor de dimensão mn.

(2) $z(|\mu_1\rangle \otimes |\nu_1\rangle) = (z\,|\mu_1\rangle) \otimes |\nu_1\rangle = |\mu_1\rangle \otimes (z\,|\nu_1\rangle)$.

(3) $(|\mu_1\rangle + |\mu_2\rangle) \otimes |\nu_1\rangle = |\mu_1\rangle \otimes |\nu_1\rangle + |\mu_2\rangle \otimes |\nu_1\rangle$.

(4) $|\mu_1\rangle \otimes (|\nu_1\rangle + |\nu_2\rangle) = |\mu_1\rangle \otimes |\nu_1\rangle + |\mu_1\rangle \otimes |\nu_2\rangle$.

Os ítens (2), (3) e (4) levam a concluir que o produto tensorial é bilinear.

A base computacional é formada por vetores ortonormais do espaço de Hilbert $\mathbb{C}^n$, descrita a seguir:

$$\{|0\rangle := \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, |1\rangle := \begin{pmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{pmatrix}, \ldots, |n-1\rangle := \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix}\}$$

Há uma maneira de representar operadores lineares com uso do produto interno. Representação essa conhecida como produto externo, sejam $|\mu\rangle$ um vetor de uma espaço vetorial M e $|\nu\rangle$ um vetor de um espaço vetorial N, o operador linear $|\mu\rangle\langle\nu| : N \to M$ cuja ação é dada por:

$$(|\mu\rangle\langle\nu|)(|v\rangle) \equiv |\mu\rangle\langle\nu|v\rangle = \langle\nu|v\rangle|\mu\rangle$$

é o produto externo de $|\mu\rangle$ e $|\nu\rangle$. Ele apresenta a seguinte propriedade

$$\sum_{i=0}^{n-1} |i\rangle\langle i| = I.$$

Capítulo 2

Computação Quântica

Com a criação dos primeiros algoritmos quânticos na década de 80, os quais obtiveram um ganho exponencial em relação aos algoritmos clássicos existentes, foi criada uma grande expectativa em relação à potencialidade da Computação Quântica. Nos dias atuais, a Computação Quântica é uma área de pesquisa muito explorada, tanto em relação à criação de dispositivos quânticos quanto em relação à criação de algoritmos quânticos. Neste capítulo é apresentado um histórico da Computação Quântica, os postulados da Mecânica Quântica e a composição dos algoritmos quânticos. Uma boa revisão sobre o assunto pode ser encontrada em Marquezino (2006).

2.1 Histórico da Computação Quântica

Para se falar da história da Computação Quântica, é necessário mencionar dois triunfos intelectuais do século XX: a Mecânica Quântica e o desenvolvimento da Teoria da Ciência da Computação.

A Mecânica Quântica surge na virada do século XX, momento em que começa a surgir uma série de *problemas* com a física clássica. Os sistemas físicos previam absurdos como *catástrofe ultravioleta* e energias infinitas. A princípio, esses problemas foram resolvidos com a inclusão de hipóteses adicionais à física atual da época, mas a crise tornou-se mais agravante, pois as tentativas de explicação tornavam-se cada vez mais insustentáveis. Foi então que no início da década de 20 criou-se a

teoria da Mecânica Quântica, teoria esta que contribuiu para a explicação de vários fenômenos físicos e foi consolidando-se com passar do tempo.

Contudo, o que vem a ser Mecânica Quântica? Mecânica Quântica nada mais é do que uma estrutura matemática ou conjunto de regras para a construção de teorias físicas (Nielsen e Chuang, 2003).

A outra grande conquista intelectual do século XX foi o desenvolvimento da Teoria da Computação. Alan Turing (1936) desenvolveu em detalhes uma máquina capaz de executar algoritmos, a famosa Máquina de Turing, que é uma máquina teórica composta de um programa; uma unidade de controle de estados finitos, constituído de um conjunto finito de estados internos; uma fita, desempenhando o papel de memória do computador; e uma cabeça de leitura e gravação (Nielsen e Chuang, 2003). Turing mostrou que existe uma Máquina de Turing Universal, de forma que ela pode ser usada para simular qualquer outra Máquina de Turing. E foi ainda mais além ao argumentar que existe uma Máquina de Turing Universal a qual representa toda tarefa realizada por meio de algoritmos, ou seja, todo processo algorítmico que possa ser realizado na natureza pode ser descrito por uma Máquina de Turing. Tal afirmativa ficou conhecida como tese de Church-Turing.

A criação dos transistores, em 1948, foi um grande progresso no desenvolvimento dos computadores. A evolução tecnológica nessa área foi muito rápida, os transistores tornavam-se cada vez mais rápidos e menores (Tanenbaum, 2001).

Gordon Moore (1965) fez uma predição na qual afirmava que o número de transistores por unidade de área e, conseqüentemente, o poder de processamento dos computadores dobrariam a cada 18 meses. Predicação essa que ficou conhecida como a famosa lei de Moore. Essa lei conseguiu prever, de forma razoável, a evolução dos computadores até os dias atuais. Mas há um limite para a lei de Moore, visto que com a miniaturização dos componentes do computador, os efeitos quânticos começam a surgir e as leis da física clássica passam a não valer mais. A partir da ordem de 25 nanometros, os efeitos quânticos começam a interferir no processamento de informações (Ellenbogen, 1998). Uma alternativa para esse problema

seria passar a usar os efeitos quânticos como aliados, com o propósito de aumentar a eficiência de computação.

A partir da década de 80 começam a aparecer os primeiros trabalhos importantes para o desenvolvimento da Computação Quântica. Feynman (1982) mostrou que a Mecânica Quântica pode ser usada para a computação. Um pouco depois, Deutsch publicou um artigo, no qual provava que toda Computação Clássica poderia ser computada pela Computação Quântica, o que levou a se imaginar que a Computação Quântica teria poderes maiores que a Computação Clássica. Após essa publicação começou-se a criar aplicações para a máquina quântica proposta por Feynman.

Shor (1994) propõe um algoritmo quântico para a solução de importante problema da Teoria dos Números, o problema de fatoração. Ele mostrou que usando a Computação Quântica o problema seria resolvido em tempo polinomial nos dados de entrada, enquanto que os métodos atuais de Computação Clássica só o resolvem em um tempo de computação exponencial. Com esse avanço, a Computação Quântica passa de um mero interesse acadêmico a um interesse mundial. No ano seguinte, Kitaev (1995) desenvolve um algoritmo quântico para calcular a ordem dos elementos de um grupo.

Simon (1997) desenvolveu o primeiro algoritmo para resolução do Problema do Subgrupo Oculto em grupos da forma $\mathbb{Z}_2^n$. Posteriormente, vários trabalhos foram feitos, buscando uma solução para esse problema, como o trabalho de Hallgren et al. (2000), o qual apresenta uma solução para o problema com a hipótese de que o grupo oculto é normal. Já os trabalhos de Mosca (1999), Watrous (2001), Nielsen e Chuang (2003), e de Ivanyos et al. (2003) analisam problemas como decomposição de grupos Abelianos e cálculo de ordem de grupos solúveis.

2.2 Mecânica Quântica

Nesta seção são descritos os quatro postulados da Mecânica Quântica, postulados que, foram introduzidos após um longo processo de tentativa e erro, como é comum na criação de novas teorias. O primeiro postulado faz a descrição matemática de um sistema quântico isolado, o segundo descreve como os sistemas quânticos evoluem, já o terceiro descreve a forma como pode-se extrair informações de um sistema quântico através do processo de medição, e o quarto descreve a forma como sistemas quânticos diferentes podem ser combinados.
Um sistema quântico isolado é associado a um espaço linear complexo $\mathbb{C}^n$ com produto interno, num espaço de Hilbert, que é chamado de espaço de estados.

Postulado 2.2.1 A qualquer sistema físico isolado existe associado um espaço vetorial de Hilbert complexo, conhecido como espaço de estado do sistema. O sistema é completamente descrito pelo seu vetor de estado, um vetor unitário no espaço de estados.

Por analogia a um sistema físico clássico de dois níveis capaz de representar um bit, pode-se pensar em um sistema físico quântico de dois níveis capaz de representar um *bit* quântico, o que se define por *q-bit (quantum bit)*. Um bit clássico assume o valor "0" ou "1", já o *q-bit* pode assumir os valores "0", "1" ou qualquer superposição deles, o que é visto como combinação linear.

Definição 2.2.1 Um *q-bit* é um vetor unitário de $\mathbb{C}^2$

Um *q-bit* $|\psi\rangle \in \mathbb{C}^2$ pode ser visto como combinação dos elementos da base computacional $|\psi\rangle = a|0\rangle + b|1\rangle$. Onde $a, b \in \mathbb{C}$ são chamados de amplitudes e obedecem à equação $|a|^2 + |b|^2 = 1$. Diz-se que $|\psi\rangle$ está em superposição de $|0\rangle$ e $|1\rangle$.
O próximo postulado diz como ocorre a evolução temporal de um sistema. A evolução temporal nos sistemas quânticos é dada por uma transformação no espaço de Hilbert em questão. Como o vetor que representa o sistema deve ser sempre um vetor unitário, a transformação também deve ser sempre unitária, ou seja, a transformação deve levar vetores unitários a vetores unitários.

Postulado 2.2.2 A evolução de um sistema quântico fechado é descrita por uma transformação unitária. Ou seja, o estado $|\psi\rangle$ de um sistema em um tempo t_1 está relacionado ao estado $|\psi'\rangle$ do sistema em t_2 por um operador unitário que depende somente de t_1 e t_2:

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

Exemplo 2.2.3 Um operador unitário muito usado é a *porta de Hadamard*, sendo denotado por H.

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

A porta de Hadamard atua sobre os vetores da base computacional da seguinte forma:

$$H|0\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \text{ e } H|1\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle.$$

Já foi visto em qual estrutura matemática está o espaço de estados e também já foi descrito como o estado evolui. A evolução dos estados na Mecânica Quântica é um processo determinístico, porém não foi mostrado como extrair informações de um sistema quântico, o que introduz um caráter probabilístico à Mecânica Quântica. No próximo postulado, o postulado da medida, é visto como extrair informações de um sistema quântico.

Postulado 2.2.4 As medidas quânticas são descritas por determinados operadores de medida M_m, os quais atuam sobre os estados do sistema. O índice m refere-se aos possíveis resultados da medida, onde $m \in \mathbb{N}$. Se o estado quântico for $|\psi\rangle$, imediatamente antes da medida, a probabilidade de um resultado ocorrer é dada por:

$$p(m) = \langle\psi|M_m^\dagger M_m|\psi\rangle,$$

e o estado do sistema após a medida será:

$$\frac{M_m|\psi\rangle}{\sqrt{\langle\psi|M_m^\dagger M_m|\psi\rangle}},$$

Os operadores de medida satisfazem a relação de completude:

$$\sum_m M_m^\dagger M_m = I.$$

Onde $M^\dagger$ é a matriz transposta conjugada da matriz M.

A relação de completude deve-se ao fato de que a soma das probabilidades deve ser igual a 1, para todo estado $|\psi\rangle$.

Exemplo 2.2.5 Um exemplo de medida é a medida de um estado na base computacional, que é um tipo de medida muito utilizada na Computação Quântica. Defini-se $M_0 := |0\rangle\langle 0|$, $M_1 := |1\rangle\langle 1|$, seja $M = \{M_0, M_1\}$ os operadores de medida, observe que $M_0^2 = M_0 M_0 = (|0\rangle\langle 0|)(|0\rangle\langle 0|) = |0\rangle\langle 0| = M_0$, o mesmo acontecendo a $M_1^2 = M_1$, também observe que $M_0^\dagger = M_0$ e $M_1^\dagger = M_1$. Com isso $M_0^\dagger M_0 + M_1^\dagger M_1 = M_0 M_0 + M_1 M_1 = I$, portanto a relação de completude é satisfeita.
Dado um estado $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, a probabilidade de se ter o resultado 0 é dada por:

$$p(0) = \langle\psi|M_0^\dagger M_0|\psi\rangle = \langle\psi|M_0|\psi\rangle = |\alpha|^2$$

A probabilidade de se ter o resultado 1 é dada por:

$$p(1) = \langle\psi|M_1^\dagger M_1|\psi\rangle = \langle\psi|M_1|\psi\rangle = |\beta|^2$$

O estado do sistema após a medida será:

$\frac{M_0|\psi\rangle}{|\alpha|} = \frac{\alpha|0\rangle}{|\alpha|}$, se o resultado da medida foi 0.
$\frac{M_1|\psi\rangle}{|\beta|} = \frac{\beta|1\rangle}{|\beta|}$, se o resultado da medida foi 1.

Exemplo 2.2.6 Pode-se generalizar esses operadores de medida para um espaço de dimensão n. Com $M_i := |i\rangle\langle i|$, com $i = 0, 1, \ldots n-1$ e o conjunto de operadores de medida $M = \{M_i\}$.

$$M_i = [m^i_{jk}], m^i_{jk} = \begin{cases} 1 & \text{se } j = k = i \\ 0 & \text{caso contrário} \end{cases}$$

Pode-se ver que $M_i^\dagger = M_i$ e que $M_i^2 = M_i$, com isso a relação de completude é satisfeita.

$$\sum_i M_i^\dagger M_i = \sum_i M_i^2 = \sum_i M_i = I$$

No estado $|\psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle + \cdots + \alpha_{n-1}|n-1\rangle$. A probabilidade de se medir e obter o resultado i é:

$$p(i) = \langle\psi|M_i^\dagger M_i|\psi\rangle = |\alpha_i|^2$$

E o estado do sistema após a medida será:

$$\frac{M_i|\psi\rangle}{|\alpha_i|} = \frac{\alpha_i}{|\alpha_i|}|i\rangle$$

Agora é mostrado como se constrói um estado composto por dois ou mais sistemas distintos. Um estado composto por mais de um estado é formado pelo produto tensorial de seus sistemas individuais, como será visto a seguir.

Postulado 2.2.7 O espaço de um sistema físico composto é produto tensorial dos espaços de estados dos sistemas físicos individuais. Se os sistemas forem de 1 até n, e o sistema i estiver no estado $|\psi_i\rangle$, o estado do sistema composto será $|\psi_1\rangle \otimes |\psi_2\rangle \otimes \cdots \otimes |\psi_1\rangle$

2.3 Algoritmos Quânticos

Na Computação Clássica, a unidade básica para armazenar informação é o *bit*, já no contexto da Computação Quântica a unidade básica para armazenar uma informação é o *q-bit*. Mas além de armazenar informação também há o interesse

em manipular informações.

As operações mais básicas da Computação Quântica são as operações que atuam sobre um *q-bit*, que são representadas pelas matrizes unitárias 2×2. E as principais operações lógicas que atuam sobre um *q-bit* são as apresentadas na tabela a seguir.

Nome	Representação	Matriz
Identidade	I	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$
Hadamard	H	$H \equiv \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$
Pauli-X (NOT)	X ou σ_x	$\sigma_X \equiv X \equiv \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$
Pauli-Y	Y ou σ_y	$\sigma_Y \equiv Y \equiv \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$
Pauli-Z	Z ou σ_z	$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$
Fase	S	$\begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$
$\pi/8$	T	$\begin{pmatrix} 1 & 0 \\ 0 & e^{2\pi i/8} \end{pmatrix}$

Tabela 2.1: Principais operações lógicas sobre um *q-bit*

As operações lógicas básicas, tanto em sistemas clássicos quanto em sistemas quânticos, são chamadas de portas lógicas.

Os sistemas de computação clássicos são formados por circuitos, os quais são feitos de portas e fios. Os circuitos manipulam informações e podem ser vistos como uma função $f : \{0,1\}^k \longrightarrow \{0,1\}^l$ que tem como entrada informações codificadas em k *bits* e como saída informações codificadas em l *bits*.

Existe um conjunto elementar de portas lógicas que são universais para computação clássica, universais uma vez que todo circuito pode se decompor em uma combinação de portas elementares. Esse conjunto de portas elementares é formado pelas portas E(AND), OU-EXCLUSIVO(XOR), NÃO(NOT).

Semelhantemente à Computação Clássica, na Computação Quântica tem-se os circuitos quânticos, os quais funcionam como operadores unitários e são compostos por fios e portas quânticas. A figura 2.1 mostra um circuito quântico. No final do circuito quântico é comum ser feita uma medida para extrair informações do processamento.

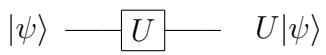

Figura 2.1: Circuito quântico.

A Computação Quântica também possui um conjunto elementar de portas lógicas universais, formado pelas portas Hadamard, de fase, $\pi/8$, CNOT e Toffoli[1] . Nielsen e Chuang (2003) provam que todas transformações unitárias podem ser decompostas em termos dessas portas. Exemplificando, a seguir será visto o primeiro algoritmo quântico proposto por Deutsch (1985), apesar de não ter aplicação prática é usado para fins didáticos.

O algoritmo de Deutsch resolve o problema, dada a função $f : \{0,1\} \rightarrow \{0,1\}$, descobrir se a função f é balanceada, $f(0) = f(1)$, ou se a função é constante, ou

[1] As portas CNOT e Toffoli são transformações unitárias 2 e 3 q-bits respectivamente e podem ser vistas em Nielsen e Chuang (2003)

seja, $f(0) \neq f(1)$.

Deutsch propôs o algoritmo baseado no circuito da figura 2.2.

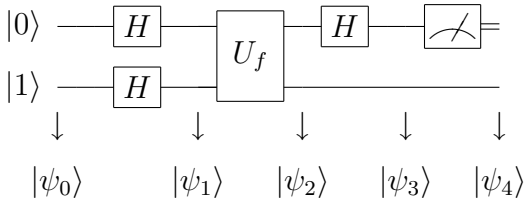

Figura 2.2: Circuito quântico do algoritmo de Deutsch.

Passo a passo,

$$
\begin{aligned}
|\psi_0\rangle &= |0\rangle \otimes |1\rangle \\
|\psi_1\rangle &= \frac{1}{2}[(|0\rangle + |1\rangle) \otimes (|0\rangle - |1\rangle)] = \frac{1}{2}(|00\rangle - |01\rangle + |10\rangle - |11\rangle) \\
|\psi_2\rangle &= \frac{1}{2}(|0f(0)\rangle - |0(\oplus f(0))\rangle + |1f(1))\rangle - |1(1 \oplus f(1))\rangle) \\
&= \frac{1}{2}[|0\rangle \otimes (|f(0)\rangle - |1 \oplus f(0)\rangle) + |1\rangle \otimes (|f(1)\rangle - |1 \oplus f(1)\rangle)] \\
|\psi_3\rangle &= \pm\frac{1}{\sqrt{2}}|f(0) \oplus f(1)\rangle \otimes (|0\rangle - |1\rangle) \\
|\psi_4\rangle &= |f(0) \oplus f(1)\rangle
\end{aligned}
$$

Onde $\oplus$ representa a soma módulo 2 e $|ij\rangle = |i\rangle\,|j\rangle$.

Se $|\psi_4\rangle$ for igual a 0, significa que $f(0) = f(1)$ e se $|\psi_4\rangle$ for igual a 1, então $f(0) \neq f(1)$.

Esse algoritmo ilustra a capacidade do paralelismo quântico, uma vez que a aplicação do operador unitário U_f permite a avaliação da função f em pontos distintos simultaneamente [2] . Isso também pode ser visto de forma mais clara usando somente o operador U_f. Aplicando U_f ao estado $1/\sqrt{2}[(|0\rangle + |1\rangle) \otimes |0\rangle]$, obtém-se:

$$U_f(1/2(|0\rangle + |1\rangle) \otimes |0\rangle) = \frac{|0f(0)\rangle + |1f(1)\rangle}{\sqrt{2}}$$

Observe que o estado final contém informações de $f(0)$ e $f(1)$ usando apenas uma

[2] O operador unitário U_f é definido $|x, y\rangle \mapsto |x, y \oplus f(x)\rangle$. Pode se demonstrar facilmente que U_f é um operador unitário.

avaliação de f.

Capítulo 3

p-Grupos Nil-2 de Expoente p

Neste capítulo são apresentadas algumas propriedades de p-grupos nil-2 de expoente p que são fundamentais no desenvolvimento do trabalho. Primeiramente é feita uma breve introdução a teoria de grupos, em seguida são vistas as principais características dos grupos solúveis e nilpotentes e posteriormente é apresentada uma caracterização dos p-grupos nil-2 de expoente p. Maiores detalhes sobre grupos solúveis e nilpotentes grupos podem ser encontrados em Spindler (1994). Em especial na seção 3.3 são apresentadas algumas características dos grupos nil-2 que não são comuns em literaturas.

3.1 Breve introdução a Teoria de Grupos

Nesta seção serão vistas algumas definições e propriedades da teoria de grupos que fundamentais para o desenvolvimento desta dissertação.

Um conjunto G não vazio com uma operação binária $*$ é um grupo se a operação for associativa, ou seja, $\forall x, y, z \in G$, $(x * y) * z = x * (y * z)$, se em G existe um elemento neutro e, tal que $x * e = e * x = x$, e existir $x' \in G$, tal que $x * x' = e$. Para facilitar a notação, é omitido $*$, substituindo $a * b$ por ab.

Se a operação definida em G for comutativa, isto é $xy = yx, \forall x, y \in G$, o grupo é dito abeliano. Quando $xy = yx$ é dito que x e y comutam.

O grupo G é finito se G possui uma quantidade finita de elementos, e denota-se por $|G|$ esta quantidade.

Um grupo G pode conter vários grupos, chamados de subgrupos de G, como é visto a seguir. Um subconjunto H de G é dito subgrupo de G, denota-se $H < G$, se H é um grupo com a operação definida em G.

Exemplo 3.1.1 O subconjunto de um grupo G formado por elementos G que comutam com todos os elementos de G, é um subgrupo de G, chamado de centro de G e é denotado por $Z(G)$.

A partir de um subgrupo de G pode-se criar novos grupos, chamados de grupos quociente. A seguir são apresentadas algumas propriedades dos subgrupos que permitem a definição dos grupos quociente.

Uma classe lateral (à esquerda) de H em G é um conjunto da forma $gH = \{gh; h \in H\}$, onde $g \in G$, semelhantemente define-se classe lateral à direita de H. Se $g_1, g_2 \in G$, então só há duas alternativas, ou as classes laterais de g_1, g_2 são distintas ou são idênticas, em particular pode-se decompor G como união disjunta de em classes laterais, a figura 3.1 ilustra essa afirmação.

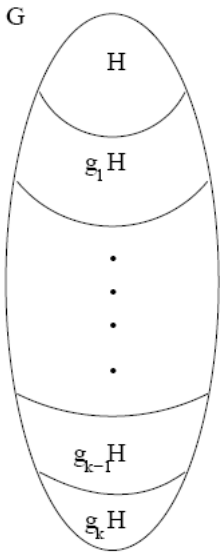

Figura 3.1: G decomposto como união disjunta de classes laterais. Fonte: apud (Gonçalves, 2005)

A cardinalidade do conjunto das classes laterais à esquerda é chamado de índice de H em G, e é denotado por $(G : H)$. Um teorema elementar porém importante da teoria de grupos é o Teorema de Lagrange enunciado a seguir.

Teorema 3.1.1 (Teorema de Lagrange) Sejam G um grupo finito e H um subgrupo de G. Então $|G| = |H|(G : H)$.

Seja $H < G$, se $gH = Hg, \forall g \in G$, o subgrupo H de G é dito normal em G. Quando H é um subgrupo normal de G, a operação induzida $\overline{*}$, onde $g_1 H \overline{*} g_2 H = g_1 g_2 H$ é bem definida e o conjunto formado por todas as classes laterais de H é um grupo, chamado de grupo quociente G/H. Em algumas literaturas o grupo quociente G/H é chamado de grupo fator G/H.

Um conceito importante, principalmente para teoria de grupos computacional, é o de conjunto de geradores. Seja S um subconjunto de um grupo G, o subgrupo de G gerado por S, representado por $\langle S \rangle$, é o conjunto de todos os elementos de G se escrevem como produto de elementos de S e dos seus inversos munido das mesmas operações que G. Diz que S é um conjunto gerador de $\langle S \rangle$.

Seja G um grupo e g um elemento de G, se existir um inteiro n tal que $g^n \equiv \underbrace{gg...g}_{n} = e$, então $\langle g \rangle = \{e, g, g^2, ..., g^{n-1}\}$ e é chamado grupo cíclico gerado por g. Caso n seja o menor inteiro tal que $g^n = e$, n chamado ordem de g. Quando os elementos de um grupo G tem como ordem um número primo p ou 1, G é um grupo de expoente p. E quando a ordem dos elementos do grupo forem potências de p, G é um p-grupo.

Seja G um grupo finito de ordem $|G| = p^n m$ onde p não divide m. Um subgrupo de G de ordem p^n chama-se um p-subgrupo de Sylow de G.

Sejam M, N dois grupos, uma função $f : M \longrightarrow N$ que preserva a operação definida no grupo, isto é, $f(ab) = f(a)f(b), \forall a, b \in G$, recebe um nome especial, f é chamada de homomorfismo. Em particular quando f é uma bijeção diz que f é um isomorfismo.

A seguir é apresentado um teorema importante para análise da complexidade dos algoritmos quânticos.

Teorema 3.1.2 Seja G um grupo com $|G| > 1$. Existe um conjunto gerador para G com no máximo $\lceil \log_2 |G| \rceil$ elementos.

Prova. Pelo fato de que $|G| > 1$, existe $g_1 \neq e \in G$, com isso $|\langle g_1 \rangle| \geq 2$, pois $g_1, g_2^2 \in \langle g_1 \rangle$. Se $G = \langle g_1 \rangle$ o processo termina e a afirmação do teorema é válida, caso contrário, existe $g_2 \in G \setminus \langle g_1 \rangle$. Segue que $|\langle g_1, g_2 \rangle| \geq 2^2$, pois $g_1, g_1^2, g_1 g_2$ e $g_1^2 g_2$ são distintos. Se $G = \langle g_1, g_2 \rangle$ o processo termina e a afirmação do teorema é válida, caso contrário existe $g_3 \in G \setminus \langle g_1, g_2 \rangle$ e usando um argumento semelhante ao anterior, $|\langle g_1, g_2, g_3 \rangle| \geq 2^3$. Continuando esse processo até que se tenha $|\langle g_1, g_2, \ldots, g_{\lceil \log_2 |G| \rceil} \rangle| \geq 2^{\lceil \log_2 |G| \rceil}$, mas $2^{\lceil \log_2 |G| \rceil} \geq |G|$, portanto $\langle g_1, g_2, \ldots, g_{\lceil \log_2 |G| \rceil} \rangle = G$. ■

3.2 Grupos Nilpotentes e Grupos Solúveis

Definição 3.2.1 Dado G um grupo. O comutador de dois elementos $x, y \in G$ é definido com $[x, y] = x^{-1}y^{-1}xy$. O comutador de dois subgrupos $X, Y \leq G$ é o subgrupo de G gerado por todos os comutadores $[x, y]$ onde $x \in X, y \in Y$, ou seja $[X, Y] = \langle \{x^{-1}y^{-1}xy; x \in X, y \in Y\} \rangle$.

Observe que $[x, y] = e$ se e somente se $xy = yx$. E similarmente $[X, Y] = \{e\}$ se e somente se quaisquer dos elementos $x \in X$ e $y \in Y$ comutam.
É apresentado a seguir as definições de série de comutadores e série central decrescente, que caracterizam os grupos solúveis e os grupos nilpotentes respectivamente.

Definição 3.2.2 (Série de Comutadores) Dado G um grupo, defini-se a série $G^0 \supseteq G^1 \supseteq G^2 \supseteq \cdots \supseteq G^{(k)} \supseteq \ldots$ de G indutivamente por

$$G^{(0)} = G,\ G^{(k+1)} = [G^{(k)}, G^{(k)}]$$

chamada série de comutadores de G.

O subgrupo $G^{(1)}$ de G é chamado de subgrupo dos comutadores de G e é denotado por G'.

Definição 3.2.3 (Série central decrescente) Dado G um grupo, defini-se a série $G \supseteq G^{[1]} \supseteq G^{[2]} \supseteq \cdots \supseteq G^{[k]} \supseteq \ldots$ de G indutivamente por

$$G^{[0]} = G,\ G^{[k+1]} = [G, G^{[k]}]$$

chamada série central de G.

Definição 3.2.4 Um grupo G é dito solúvel se a sua série de comutadores termina em $\{e\}$. E um grupo G é nilpotente se a série central decrescente termina em $\{e\}$. Diz que G é um grupo solúvel classe n se $G^{(n)} = \{e\}$ e $G^{(n-1)} \neq \{e\}$ analogamente diz que G é um grupo nilpotente classe n se $G^{[n]} = \{e\}$ e $G^{[n-1]} \neq \{e\}$

Proposição 3.2.1 Dados os grupos G, H.

(1) Se $U < G$ então $U^{(k)} \subset G^{(k)}$ e $U^{[k]} \subset G^{[k]}$.

(2) Se $f : G \to H$ é um homomorfismo então $f(G^{(k)}) \subseteq H^{(k)}$ e $f(G^{[k]}) \subseteq H^{[k]}$ $\forall k \geq 0$.

(3) $G^{(k)} \subseteq G^{[k]}, \forall k \geq 0$.

(4) Se $G = \prod_{i=1}^{n} G_i$ então $G^{(k)} = \prod_{i=1}^{n} G_i^{(k)}$ e $G^{[k]} = \prod_{i=1}^{n} G_i^{[k]}$.

Prova.

(1) É facilmente provada por indução sobre k.

(2) $\forall x, y \in G$, se tem $f([x, y]) = f(x^{-1}y^{-1}xy) = f(x)^{-1}f(y)^{-1}f(x)f(y) = [f(x), f(y)]$, com essa propriedade, a afirmação é facilmente provada por indução.

(3) Será provado por indução sobre k, o caso de $k = 0$ é trivial. Agora suponha que $G^{(k)} \subseteq G^{[k]}$, então

$$G^{(k+1)} = [G^{(k)}, G^{(k)}] \subseteq [G, G^{[k]}] = G^{[k+1]}.$$

(4) Dado $x = (x_i)_{i=1,\ldots,n}, y = (y_i)_{i=1,\ldots,n} \in G$, então $[x, y] = (x_i^{-1}y_i^{-1}x_iy_i)_{i=1,\ldots,n} = ([x_i, y_i])_{i=1,\ldots,n}$

■

Observe que o item (3) da proposição 3.2.1 é equivalente a afirmação, todo grupo nilpotente é um grupo solúvel.

Teorema 3.2.1 (1) A imagem homomorfica de um grupo solúvel (nilpotente) é solúvel (nilpotente).

(2) Um subgrupo de um grupo solúvel (nilpotente) é também solúvel(nilpotente).

(3) O produto direto de grupos solúveis (nilpotentes) é solúvel (nilpotente).

Prova. Conseqüência imediata da proposição 3.2.1. ■

O teorema a seguir caracteriza os grupos solúveis e os grupos nilpotentes.

Teorema 3.2.2 Dado um grupo G.

(1) Se N é um subgrupo normal de G. Então G é solúvel se e somente se N e G/N são solúveis.

(2) G é um grupo solúvel finito, se e somente se, existe uma série

$$G := M_0 \triangleright M_1 \triangleright \cdots \triangleright M_s = \{e\}$$

de subgrupo de G, tais que todos os grupos fatores M_k/M_{k+1} são cíclicos de ordem prima.

(3) O grupo G é nilpotente se e somente se G é isomorfo ao produto direto de seus subgrupos de Sylow.

Prova. Ver (Spindler, 1994). ■

3.3 p-Grupos de expoente p Nil-2

Será definido primeiramente o que é uma classe de grupos *nil-n* para posteriormente particularizar para o caso *nil*-2.

Definição 3.3.1 Chama-se *nil-n* a classe de grupos formada por grupos nilpotentes de classe menor ou iguais a n.

Proposição 3.3.1 Seja G um grupo *nil-c*, então todo subgrupo e grupo fator de G é *nil-c*.

Prova. Seja H um subgrupo de G, pelo item (1) da proposição 3.2.1 sabe-se que $H^{[c]} \subseteq G^{[c]} = \{e\}$, logo H também é *nil-c*.

Um subgrupo fator é imagem homomorfica de G, usando o item (2) da proposição 3.2.1 pode-se concluir que o grupo fator de um grupo *nil-c* também é *nil-c*. ■

Sendo assim a classe *nil*-2 abrange os grupos abelianos e os grupos nilpotentes de classe 2 em ambos os casos é fácil ver que G é um grupos que esta em *nil*-2 se $G' \leq Z(G)$. Onde $Z(G)$ é o subgrupo de G que contém os elementos que comutam com todos de G, e é chamado centro de G.

A proposição a seguir mostra que o comutador, nos grupos *nil*-2 tem a propriedade de ser bilinear.

Proposição 3.3.2 Dado G um grupo *nil*-2. Então para todo $g_1, g_2, g_3, g_4 \in G$, $[g_1g_2, g_3g_4] = [g_1, g_3][g_1, g_4][g_2, g_3][g_2, g_4]$

Prova. Será provado inicialmente que o comutador é linear no primeiro argumento, pela definição:

$$[g_1g_2, g_3] = (g_1g_2)^{-1}{g_3}^{-1}g_1g_2g_3 = g_2^{-1}g_1^{-1}g_3^{-1}g_1g_2g_3,$$

adicionando o elemento $g_3g_3^{-1}$ entre os elementos,

$$[g_1g_2, g_3] = g_2^{-1}g_1^{-1}g_3^{-1}g_1g_3{g_3}^{-1}g_2g_3 = g_2^{-1}[g_1, g_3]{g_3}^{-1}g_2g_3,$$

Lembrando que $G' \subseteq Z(G)$,

$$[g_1g_2, g_3] = [g_1, g_3]g_2^{-1}{g_3}^{-1}g_2g_3 = [g_1, g_3][g_2, g_3].$$

Analogamente tem-se que $[g_1, g_3g_4] = [g_1, g_3][g_1, g_4]$. E com isso,

$$[g_1g_2, g_3g_4] = [g_1, g_3][g_1, g_4][g_2, g_3][g_2, g_4]$$

■

A estrutura dos grupos *nil*-2 é expressa a seguir na proposição 3.3.3, do fato 3 de Ivanyos et al. (2007b).

Proposição 3.3.3 Dado G um p-grupo de expoente p nilpotente de classe 2. Então existem naturais m e d, e um conjunto de elementos $x_1, \ldots, x_m \in G$ e $z_1, \ldots, z_d \in G'$, tais que:

(1) $G/G' \simeq \mathbb{Z}_p^m$ e $G' \simeq \mathbb{Z}_p^d$.

(2) Dado $g \in G$ existe um único elemento $(e_1, \ldots, e_m, f_1, \ldots, f_d) \in \mathbb{Z}_p^{m+d}$ tal que g se escreve de forma $g = x_1^{e_1} \ldots x_m^{e_m} z_1^{f_1} \ldots z_d^{f_d}$.

(3) $G = \langle x_1, \ldots, x_m \rangle$ e $G' = \langle z_1, \ldots, z_d \rangle$.

Quando G for um p-grupo *nil*-2 de expoente p, $G/G' \simeq \mathbb{Z}_p^m$ e $G' \simeq \mathbb{Z}_p^d$, G será identificado pelos parâmetros (m, d).

Agora é definido um automorfismo nos p-grupos nilpotentes de classe 2 de expoente p.

Seja G um p-grupo nilpotente de classe 2 de expoente p, para $j = 1, 2, \ldots, p-1$, defini-se $\phi_j : G \longrightarrow G$ nos geradores de G como sendo $\phi_j(x_i) = {x_i}^j$ e faz uma extensão homomorfica de ϕ_j a todos os elementos de G da seguinte forma, dado $g \in G$, sabe-se que $g = {x_{k_1}}^{e_{k_1}} \ldots {x_{k_m}}^{e_{k_m}}$, observe que esta sendo usado somente o fato de que $G = \langle x_1, \ldots, x_m \rangle$, sendo assim $\phi_j(g) = (\phi_j(x_{k_1}))^{e_{k_1}} \ldots (\phi_j(x_{k_m}))^{e_{k_m}} = {x_{k_1}}^{je_{k_1}} \ldots {x_{k_m}}^{je_{k_m}}$.

Proposição 3.3.4 ϕ_j é um automorfismo $\forall j \in \{1, 2, \ldots, p-1\}$

Prova. A função ϕ_j é construída homormoficamente, mas ainda falta provar que ϕ_j é uma bijeção. Esta sendo considerando G um grupo finito, por isso basta provar que ϕ_j é uma função injetora. Por isso será provado que ϕ_j é injetora, dados $g_1, g_2 \in G$, suponha que $\phi_j(g_1) = \phi_j(g_2)$. Existem $(e_{k_1}^1, \ldots, e_{k_m}^1)$, $(e_{l_1}^1, \ldots, e_{l_m}^2) \in \mathbb{Z}_p^m$ tais que $g_1 = {x_{k_1}}^{e_{k_1}^1} \ldots {x_{k_m}}^{e_{k_m}^1}$ e $g_2 = {x_{l_1}}^{e_{l_1}^1} \ldots {x_{l_m}}^{e_{l_m}^1}$, aplicando ϕ_j, te-se

$\phi(g_1) = \phi({x_{k_1}}^{e^1_{k_1}} \dots {x_{k_m}}^{e^1_{k_m}}) = {x_{k_1}}^{je^1_{k_1}} \dots {x_{k_m}}^{je^1_{k_m}}$ e $\phi(g_2) = \phi({x_{l_1}}^{e^2_{l_1}} \dots {x_{l_m}}^{e^2_{l_m}}) = {x_{l_1}}^{je^2_{l_1}} \dots {x_{l_m}}^{je^2_{l_m}}$. Pela hipótese inicial, tem-se:

$$ {x_{k_1}}^{je^1_{k_1}} \dots {x_{k_m}}^{je^1_{k_m}} = {x_{l_1}}^{je^2_{l_1}} \dots {x_{l_m}}^{je^2_{l_m}} \tag{3.1} $$

G não é necessariamente um grupo abeliano mas pode-se comutar os elementos de G da seguinte forma, $v, w \in G$, $vw = wvv^{-1}w^{-1}wv = wv[v, w]$. Usando este fato e o fato de que $G' \subseteq Z(G)$, pode-se reordenar ambos os lados da igualdade (5.4) de forma que ao final tem-se:

$$ {x_1}^{je^1_1} \dots {x_m}^{je^1_m} z' = {x_1}^{je^2_1} \dots {x_m}^{je^2_m} z'', z', z'' \in G' \tag{3.2} $$

Como z', $z'' \in G'$, existem $(f^1_1, \dots, f^1_d), (f^2_1, \dots, f^2_d) \in \mathbb{Z}^d_p$ tais que $z' = z_1^{f^1_1} \dots z_d^{f^1_d}$ e $z'' = z_1^{f^2_1} \dots z_d^{f^2_d}$, logo:

$$ {x_1}^{je^1_1} \dots {x_m}^{je^1_m} z_1^{f^1_1} \dots z_d^{f^1_d} = {x_1}^{je^2_1} \dots {x_m}^{je^2_m} z_1^{f^2_1} \dots z_d^{f^2_d} \tag{3.3} $$

Usando o segundo fato da proposição (3.3.3), pode-se concluir que:

$$ (je^1_1, \dots, je^1_m, f^1_1, \dots, f^1_d) = (je^2_1, \dots, je^2_m, f^2_1, \dots, f^2_d) $$

$$ (e^1_1, \dots, e^1_m, f^1_1, \dots, f^1_d) = (e^2_1, \dots, e^2_m, f^2_1, \dots, f^2_d) \tag{3.4} $$

Logo $z' = z''$ e $g_1 = g_2$. Portanto ϕ_j é um isomorfismo. ■

ϕ_j esta definida para $j = 1, \dots, p-1$, defini-se ϕ_0, como sendo $\phi_0(g) = e, \forall g \in G$, ϕ_0 não é um automorfismo, mas será útil no desenvolvimento do capítulo 5.
Na proposição a seguir são vistas algumas propriedades do automorfismo ϕ_j.

Proposição 3.3.5 Dado G um p-grupo de expoente p nilpotente de classe 2. Então ϕ_j apresenta as seguintes propriedades:

(1) $\forall j \in \mathbb{Z}_p, \forall z \in G', \phi_j(z) = z^{j^2}$.

(2) $\forall g \in G, \exists z_g \in G', \phi_j(g) = g^j {z_g}^{j-j^2}$.

Prova.

(1) Para $j = 0$, a prova é trivial. Agora dado $j \neq 0$, pelo fato de que dados $v, w \in G$, $vw = wvv^{-1}w^{-1}wv = wv[v, w]$, dado $g \in G$, existe $z \in G'$ tal que $\phi_j(g) = g^j z$. Seja $z = [g_1, g_2]$, então existe $z_1, z_2 \in G'$ tais que $\phi_j(z) = \phi_j([g_1, g_2]) = [\phi_j(g_1), \phi_j(g_2)] = [g_1^j z_1, g_2^j z_2] = [g_1^j, g_2^j][g_1^j, z_2][z_1, g_2^j][z_1, z_2] = [g_1^j, g_2^j] = [g_1, g_2]^{j^2}$.

(2) Para provar este item, tome inicialmente j_0 um elemento fixo raiz primitiva da unidade em $\mathbb{Z}_p^*$. Então $\phi_j(g) = g^j s$, para algum $s \in G'$ como j_0 é uma raiz primitiva da unidade existe um inverso para $j_0 - j_0^2$. definise $z_g = s^{(j_0 - j_0^2)^{-1}}$, sendo assim $\phi_{j_0}(g) = g^j z_g^{j_0 - j_0^2}$. Tome $k = gz_g$, então $\phi_{j_0}(k) = \phi_{j_0}(g)\phi_{j_0}(z_g) = g^{j_0} z_g^{j_0 - j_0^2} z^{j_0^2} = k^{j_0}$. Agora se $j \in \mathbb{Z}_p$, $\phi_j(k) = k^j$ logo $\phi_j(g) = \phi_j(k)\phi_j(z_g^{-1}) = g^j z_g^j z_g^{-j^2} = g^j {z_g}^{j-j^2}$

■

Capítulo 4

Problema do Subgrupo Escondido em Grupos Abelianos

Uma solução eficiente para o Problema do Subgrupo Oculto (PSO) tem como conseqüência algoritmos eficientes para alguns problemas como cálculo de fatoração, logaritmo discreto, isomorfismo de grafos e Problema do Menor Vetor em um Reticulado. Em relação ao algoritmo eficiente para o PSO abeliano, os problemas de cálculo de fatoração e logaritmo discreto apresentam soluções eficientes.

4.1 Preliminares

Dado um grupo finito G, é considerado que os elementos de G são codificados por *strings* binárias. Se $N = |G|$ precisa-se de *strings* binárias de tamanho $\lceil \log N \rceil$ para decodificar os elementos de G. Sendo assim, é levado em conta que um algoritmo é eficiente se a quantidade de operações do algoritmo é de ordem polinomial no tamanho da entrada. Quando a entrada de um algoritmo é composta de elementos de um grupo G, é necessário que o algoritmo seja de ordem $O(poli(\log N))$ para que este seja eficiente.

É considerado que existe um algoritmo eficiente para codificar os elementos G em *strings* binárias, as quais representam os vetores da base computacional, vetores estes definidos no capítulo 2, do espaço de Hilbert $\mathcal{H}$.

Seja $g' \in G$. É suposto que a transformação $U_{g'}$, a qual atua nos elementos da

base $U_{g'}(|g\rangle) = |gg'\rangle, \forall g \in G$, onde gg' representa o produto em G, pode ser implementada eficientemente, ou seja, U_h é decomposta em um número de ordem $O(poli(\log N))$ de portas básicas.

Se H for um subgrupo de G, denota-se por $|H\rangle$ o estado $\frac{1}{\sqrt{|H|}} \sum_{h \in H} |h\rangle$. E defini-se a ação de um elemento $g \in G$ no estado $|H\rangle$, como sendo $U_g|H\rangle = \frac{1}{\sqrt{|H|}} \sum_{h \in H} |hg\rangle$ e indica-se por $|H \cdot g\rangle$.

Especificamente neste capítulo é considerado, a menos de uma menção anterior, grupos abelianos finitos. O Teorema Fundamental dos Grupos Abelianos Finitos indica que cada grupo abeliano finito pode ser expresso como a soma direta de subgrupos cíclicos e Mosca (1999) prova que essa decomposição pode ser computada eficientemente, fato que também é levado em conta neste capítulo.

4.2 Problema do Subgrupo Oculto

O PSO consiste em encontrar geradores de um subgrupo H de um determinado grupo finito G com uma função oráculo f definida em G tal que $f(a) = f(b)$ se e somente se $aH = bH$ para todo $a, b \in G$. Mais formalmente veja a definição a seguir.

Definição 4.2.1 (PSO) Sejam G um grupo finito, X um conjunto finito e $f : G \longrightarrow X$ uma função tal que existe um subgrupo H de G tal que $\forall g_1, g_2 \in G$, $f(g_1) = f(g_2)$ se e somente se $g_1H = g_2H$. O Problema do Subgrupo Oculto baseia-se em utilizar avaliações da função f para determinar um conjunto gerador para H.

A função f é chamada função separadora de classes de H ou função que oculta H em G.

Pode-se imaginar um algoritmo clássico para o problema com procedimento que avalia $f(g)$ para todo $g \in G$ e determina o subgrupo oculto H em G com $|G|$ avaliações da função f, mas como a entrada do algoritmo é $\log |G|$, este algoritmo pode ser considerado de ordem exponencial nos dados de entrada, portanto não é eficiente.

4.3 Transformada de Fourier Abeliana

Uma das mais importantes ferramentas da Computação Quântica é a Transformada de Fourier, a qual é usada como elemento principal na fatoração de inteiros e em boa parte dos algoritmos quânticos.

Antes de definir a Transformada de Fourier Quântica, são apresentadas propriedades da teoria do caráter que contribuem para um melhor compreensão de tal Transformada. Maiores detalhes sobre teoria de caráter podem ser encontrados em Lomont (2004).

4.3.1 Caráter

Definição 4.3.1 O caráter de um grupo G é um homomorfismo $\chi : G \longrightarrow \mathbb{C}^*$. Onde $\mathbb{C}^*$ é o grupo multiplicativo dos complexo.

Se o grupo G for um grupo abeliano finito $\chi(G) \simeq G$ e quando $G = \mathbb{Z}_{N_1} \times \cdots \times \mathbb{Z}_{N_k}$ o caráter de G é definido por

$$\chi_g(h) = \prod_{i=1}^{k} \omega_{N_i}^{g_i h_i} \tag{4.1}$$

onde $g = (g_1, \ldots, g_k), h = (h_1, \ldots, h_k) \in \mathbb{Z}_{N_1} \times \cdots \times \mathbb{Z}_{N_k}, \omega_{N_i}$ é a N_i-ésima raiz da unidade (Lomont, 2004).

Proposição 4.3.1 Seja G um grupo abeliano, então:

(1) Para $g, h \in G$, $\chi_g(h) = \chi_h(g)$.

(2) Seja $N = |G|$, $N = N_1 \ldots N_k$. Considere o vetor

$$|v_g\rangle = \frac{1}{\sqrt{N}} \begin{pmatrix} \chi_g(h_1) \\ \vdots \\ \chi_g(h_N) \end{pmatrix}$$

para $g \in G$, onde $h_1, \ldots, h_N$ representam todos os elementos de G. Os vetores assim definidos são unitários e ortogonais dois a dois.

Prova.

(1) Direto da equação 4.1.

(2) O fato de que os vetores são unitários é uma conseqüência de que suas entradas são números complexos com normas iguais a 1.

É provado inicialmente para o caso $G = \mathbb{Z}_{N_i}$. Sejam $g_1 \neq g_2 \in G$.

$$\langle v_g | v_h \rangle = \frac{1}{N_i} \sum_{i=0}^{N_i-1} \chi_{g_1}(i)^* \chi_{g_2}(i) = \frac{1}{N_i} \sum_{i=0}^{N_i-1} (\omega_{N_i}^{g_1 i})^* \omega_{N_i}^{g_2 i} = \sum_{i=0}^{N_i-1} ((\omega_{N_i}^{g_1})^* \omega_{N_i}^{g_2})^i.$$

Como $g_1 \neq g_2$, $(\omega_{N_i}^{g_1})^* \omega_{N_i}^{g_2}$ é uma raiz da unidade não trivial e portanto $\sum_{i=0}^{N_i-1} ((\omega_{N_i}^{g_1})^* \omega_{N_i}^{g_2})^i = 0$.

O caso geral segue da generalização do argumento acima juntamente com a equação 4.1.

■

Um conjunto de caracteres de um grupo G com a multiplicação em $\mathbb{C}^*$ formam um grupo e é fácil verificar que $\chi_{g_1+g_2} = \chi_{g_1}\chi_{g_2}$. Seja F_G a matriz $|G| \times |G|$ cujas colunas são os vetores $|v_{g_i}\rangle$, onde os elementos g_i formam uma lista completa de elementos de G.

$$F_G = \frac{1}{\sqrt{N}} \begin{pmatrix} \chi_{g_1}(h_1) & \chi_{g_2}(h_1) & \dots & \chi_{g_N}(h_1) \\ \chi_{g_1}(h_2) & \chi_{g_2}(h_2) & \dots & \chi_{g_N}(h_2) \\ \vdots & \vdots & \ddots & \vdots \\ \chi_{g_1}(h_N) & \chi_{g_2}(h_N) & \dots & \chi_{g_N}(h_N) \end{pmatrix}$$

A matriz F_G é uma matriz unitária e simétrica, denominada Transformada de Fourier Quântica. A atuação de F_G nos vetores da base é dada por:

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

Observe que se $G = \mathbb{Z}_2^n$, com a operação XOR bit-a-bit, tem-se:

$$F_G = \frac{1}{\sqrt{N}} \sum_{h \in G} \prod_{i=1}^{n} (-1)^{g_i h_i} |h\rangle = \frac{1}{\sqrt{N}} \sum_{h \in G} (-1)^{<g,h>} |h\rangle .$$

que é a aplicação da transformada de Hadamard nos vetores da base, ou seja, $F_G = H^{\otimes n}$.

Nielsen e Chuang (2003) provam que se F_G é uma matriz $2^n \times 2^n$ a transformada é facilmente decomposta em portas universais que a simulam exatamente; caso contrário, a transformada também pode ser decomposta em portas universais, porém a sua simulação é feita de forma aproximada.

4.4 Subgrupo Ortogonal

Seja H um subgrupo de G defini-se o seguinte conjunto,

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

Como G é um grupo finito e $\chi_{g_1+g_2} = \chi_{g_1}\chi_{g_1}$, $H^{\perp}$ com a operação definida em G é um grupo, portanto um subgrupo de G. $H^{\perp}$ é chamado subgrupo ortogonal de H. A analogia com espaços vetoriais nem sempre é válida, mas no caso em que $G = \mathbb{Z}_2^n$ $z \in H^{\perp}$ se e somente se $(-1)^{<z,h>} = 1, \forall h \in H$ logo $< z, h >= 0, \forall h \in H$, por isso a terminologia.

A seguir são apresentadas algumas propriedades que evolvem subgrupos ortogonais.

Lema 4.4.1 $H^{\perp} \simeq G/H$. Em particular $|H^{\perp}| = |G|/|H|$.

Prova. Ver Lomont (2004). ■

Proposição 4.4.1 $(H^{\perp})^{\perp} = H$.

Prova. Segue do fato que $\chi_g(h) = \chi_h(g)$. ■

Lema 4.4.2 Dado um conjunto de geradores de $H^{\perp}$, pode-se computar um elemento aleatório de H eficientemente.

Prova. Ver Lomont (2004). ■

Uma conseqüência imediata do lema anterior é que um conjunto de geradores de um subgrupo H de G pode ser obtido eficientemente a partir de um conjunto de geradores de $H^{\perp}$.

4.5 Algoritmo Quântico para Solução do PSO em Grupos Abelianos

Sejam G um grupo abeliano finito e f uma função que oculta um subgrupo H em G, nesta seção é visto um algoritmo quântico para gerar elementos do subgrupo ortogonal de H.

Lema 4.5.1 Para qualquer classe lateral H_i de H em G, tem-se

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

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

Prova. Pela definição de F_G, alterando a ordem da soma,

$$F_G(\frac{1}{\sqrt{|H|}}\sum_{g\in H_i}|g\rangle) = \frac{1}{\sqrt{|H||G|}}\sum_{h\in G}\sum_{g\in H_i}\chi_g(h)\,|h\rangle\,. \tag{4.2}$$

Seja g_i um representante de H_i, um elemento qualquer $g \in H_i$ pode ser escrito na forma $g = g_i\tau$, para algum $\tau \in H$. Analisando somente o somatório interno da segunda parte da igualdade 4.2,

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

Se $h \in H^{\perp}$, então $\chi_h(\tau) = 1$, pois $\tau \in H$. Logo,

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

Retornando a igualdade 4.2 e usando o lema 4.4.1,

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

■

A seguir é visto o algoritmo quântico para encontrar elementos do subgrupo ortogonal de um grupo oculto.

Lema 4.5.2 Sejam G um grupo abeliano e f uma função que oculta um subgrupo H de G, existe um algoritmo quântico para gerar elementos do subgrupo $H^{\perp}$.

Prova. Aqui será considerado que existe um circuito quântico U_f que computa a função f, e atua sobre os vetores da base da seguinte forma $U_f \left|g\right\rangle \left|0\right\rangle = \left|g\right\rangle \left|f(g)\right\rangle$. Como U_f só permuta os elementos da base, levando vetores unitários em vetores unitários, U_f será uma operação linear unitária.

Algoritmo 1 Algoritmo para encontrar elementos do subgrupo ortogonal

Entrada: G, circuito quântico que calcula $f : G \longrightarrow \{0,1\}^m$ e circuito quântico para cálculo de F_G
Saída: $h \in H$
1: Inicialize o computador com os estados $\left|e_G\right\rangle \left|0^m\right\rangle$.
2: Aplique F_G ao primeiro registrador.
3: Aplique U_f no estado.
4: Meça o segundo registrador.
5: Aplique F_G ao primeiro registrador.
6: Meça o primeiro registrador.

A figura 4.1 ilustra o circuito quântico do algoritmo.

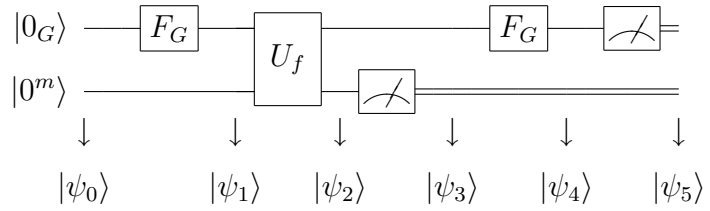

Figura 4.1: Circuito Quântico para encontrar elementos do subgrupo ortogonal.

Desta forma,

$$\begin{aligned}
|\psi_0\rangle &= |0_G\rangle|0^m\rangle \\
|\psi_1\rangle &= \frac{1}{\sqrt{|G|}} \sum_{g\in G} |g\rangle\,|0^m\rangle \\
|\psi_2\rangle &= \frac{1}{\sqrt{|G|}} \sum_{g\in G} |g\rangle\,|f(g)\rangle \\
|\psi_3\rangle &= \frac{1}{\sqrt{|H|}} \sum_{g\in H_i} |g\rangle\,|y\rangle \\
|\psi_4\rangle &= \frac{1}{\sqrt{|H^{\perp}|}} \sum_{\overline{g}\in H^{\perp}} |\overline{g}\rangle\,|\overline{y}\rangle \\
|\psi_5\rangle &= |h'\rangle
\end{aligned}$$

Onde $h' \in H^{\perp}$. ■

Seja G um grupo abeliano e f uma função que oculta um subgrupo H de G. De acordo com o teorema 3.1.2, repetindo o algoritmo do lema 3.1.2 ordem de $log|H^{\perp}|$ vezes se tem um conjunto de geradores para $H^{\perp}$, e a partir daí pode-se repetir o algoritmo do lema 4.4.2 ordem $log|H|$ vezes para se obter um conjunto de geradores de H. Com isso tem-se o teorema a seguir.

Teorema 4.5.1 Se G é um grupo abeliano, então existe um algoritmo quântico eficiente para resolução do PSO em G.

Capítulo 5

Resolução do PSO em Grupos Nilpotentes de Classe 2

Neste capítulo é apresentado um algoritmo eficiente para o PSO em grupos nilpotentes de classe 2 (Ivanyos et al., 2007a). Na primeira seção é exibida uma introdução sobre Seqüência Policíclica; na segunda, são realizadas algumas considerações em relação às Apresentações Policíclicas; na terceira seção são apresentadas reduções clássicas, as quais trazem o problema de grupos nilpotentes de classe 2 à *p-grupos nil*-2 de expoente p, onde o grupo oculto é considerado trivial ou de ordem p; já na quarta seção é mostrado o algoritmo quântico para a resolução do problema; e por último demonstramos um algoritmo eficiente para resolver a equação que surgi com o algoritmo quântico.

5.1 Seqüência Policíclica

Nesta seção são apresentadas algumas propriedades das seqüências policíclicas que serão úteis na definição da Apresentação policíclica de um grupo.
Seja G um grupo. Diz-se que G é um grupo policíclico se existe uma série de subgrupos de G, chamada série policíclica, $G = G_1 \geq G_2 \geq \cdots \geq G_{n+1} = \{e\}$, onde G_{i+1} é normal em G_i e o quociente G_i/G_{i+1} é cíclico.

Definição 5.1.1 Seja G um grupo policíclico. A seqüência de elementos de G, $X = [x_1, x_2, \ldots, x_n]$ tal que $x_i G_{i+1}$ gera o quociente G_i/G_{i+1}, ou seja, $\langle x_i G_{i+1} \rangle =$

G_i/G_{i+1} é chamada seqüência policíclica de G.

Não é difícil ver que G pode ser descrito por sua Série Policíclica, ou seja, $G = \langle x_1, x_2, \ldots, x_n \rangle$. Mais adiante é visto que além da seqüência policíclica de G gerar o grupo G, G pode ser unicamente definido por X.

Definição 5.1.2 Seja X uma seqüência policíclica de G. A seqüência $R(X) := (r_1, r_2, \ldots, r_n)$, definida por $r_i := |(G_i : G_{i+1})|$ é chamada de seqüência de ordens relativas de X.

O nome seqüência de ordens de X é bem apropriado, uma vez que r_i é a ordem de $x_i G_{i+1}$ em G_i/G_{i+1}.
Agora é apresentado uma importante característica da seqüência policíclica, a forma de apresentação única de um grupo em relação à sua seqüência policíclica.

Proposição 5.1.1 Seja G um grupo policíclico. Dada $X = [x_1, x_2, \ldots, x_n]$ uma seqüência policíclica de G, com as ordens relativas $R(X) = (r_1, r_2, \ldots, r_n)$. Então, para todo $g \in G$ há uma única seqüência $[e_1, e_2, \ldots, e_n]$, com $e_i \in \mathbb{Z}_{r_i}$ tal que $g = x_1^{e_1} x_2^{e_2} \ldots x_n^{e_n}$.

Prova. Seja $g \in G$, sabe-se que $\langle x_1 G_2 \rangle = G_1/G_2$. Sendo assim, há um único $e_1 \in \mathbb{Z}_{r_1}$ tal que $gG_2 = x_1^{e_1} G_2$, logo existe $z_2 \in G_2$ de forma que $g = x_1^{e_1} z_2$. A seqüência $X_1 = [x_2, \ldots, x_n]$ é uma seqüência policíclica de G_2, e como $z \in G_2$ pode-se usar os mesmos argumentos para provar que existem $e_2 \in \mathbb{Z}_{r_2}$, $z_3 \in G_3$ tais que $g = x_1^{e_1} x_2^{e_2} z_3$ e e_2 é único. E seguindo indutivamente, há uma única seqüência $[e_1, e_2, \ldots, e_n]$, onde $e_i \in \mathbb{Z}_{r_i}$ tal que $g = x_1^{e_1} x_2^{e_2} \ldots x_n^{e_n}$. ■

Definição 5.1.3 A expressão $g = x_1^{e_1} x_2^{e_2} \ldots x_n^{e_n}$ da proposição 5.1.1 é chamada forma normal de G em relação à X. E a seqüência $(e_1, e_2, \ldots, e_n)$ é o vetor expoente de g em relação à X e escreve-se $exp_X(g) = (e_1, e_2, \ldots, e_n)$.

Os vetores de expoentes dos elementos em grupos policíclicos podem ser usados para descrever as relações de G nos geradores X. A seguir é vista essas relações.

Proposição 5.1.2 Seja $X = [x_1, x_2, \ldots, x_n]$ seqüência policíclica de G com as ordens relativas $R(X) = (r_1, r_2, \ldots, r_n)$. Então:

(1) $\forall i \in 1, 2, \ldots, n$, a forma normal da potência $x_i^{r_i}$ é

$$x_i^{r_i} = x_{i+1}^{a_{i,i+1}} x_{i+2}^{a_{i,i+2}} \ldots x_n^{a_{i,n}},$$

onde $a_{i,k} \in \{0, 1, \ldots, r_k - 1\}$, para $k = i+1, \ldots, n$.

(2) Dados $1 \leq j \leq i \leq n$ a forma normal do conjugado $x_j^{-1} x_i x_j$ é da forma

$$x_j^{-1} x_i x_j = x_{j+1}^{b_{i,j,j+1}} x_{j+2}^{b_{i,j,j+2}} \ldots x_n^{b_{i,j,n}},$$

onde $b_{i,j,k} \in \{0, 1, \ldots, r_k - 1\}$, para $k = j+1, \ldots, n$.

(3) Dados $1 \leq j \leq i \leq n$ a forma normal do conjugado $x_j x_i x_j^{-1}$ é da forma

$$x_j x_i x_j^{-1} = x_{j+1}^{c_{i,j,j+1}} x_{j+2}^{c_{i,j,j+2}} \ldots x_n^{c_{i,j,n}},$$

onde $c_{i,j,k} \in \{0, 1, \ldots, r_k - 1\}$, para $k = j+1, \ldots, n$.

Prova.

(1) $r_i := |(G_i : G_{i+1})|$, com isso tem-se que $x_i^{r_i} G_{i+1} = G_{i+1}$, logo $x_i^{r_i} \in G_{i+1}$. A seqüência $[x_{i+1}, x_{i+2}, \ldots, x_n]$ é uma seqüência policíclica de G_{i+1}. Portanto, tem-se $x_i^{r_i}$ que apresenta a forma normal $x_i^{r_i} = x_{i+1}^{a_{i,i+1}} x_{i+2}^{a_{i,i+2}} \ldots x_n^{a_{i,n}}$.

(2) Dados $1 \leq j \leq i \leq n$, como $j \leq i$, G_{j+1} é normal em G_j, com isso $x_j^{-1} x_i x_j \in G_{j+1}$, pois $x_i \in G_{j+1}$. A seqüência $[x_{i+1}, x_{i+2}, \ldots, x_n]$ é uma seqüência policíclica de G_{i+1}, por isso $x_j^{-1} x_i x_j = x_{j+1}^{b_{i,j,j+1}} x_{j+1}^{b_{i,j,j+2}} \ldots x_{j+1}^{b_{i,j,n}}$.

(3) Análogo ao item anterior

■

5.2 Apresentações Policíclicas

Nesta seção é demonstrado como um grupo solúvel pode ser apresentado por sua seqüência policíclica. Maiores detalhes sobre Apresentações Policíclicas podem ser encontradas em Holt et al. (2005).

Definição 5.2.1 A apresentação de um grupo é definida por $[x_1, x_2, \ldots, x_n|R]$, onde $x_1, x_2, \ldots, x_n$, são os geradores do grupo e R as relações entre os geradores. Existem inteiros $a_{i,k}, b_{i,j,k}, c_{i,j,k}$ de forma que R consista em:

(1) $x_i^{r_i} = x_{i+1}^{a_{i,i+1}} x_{i+2}^{a_{i,i+2}} \ldots x_n^{a_{i,n}}$, para $i \in 1, 2, \ldots, n$.

(2) $x_j^{-1} x_i x_j = x_{j+1}^{b_{i,j,j+1}} x_{j+1}^{b_{i,j,j+2}} \ldots x_{j+1}^{b_{i,j,n}}$ para $1 \leq j \leq i \leq n$.

(3) $x_j x_i x_j^{-1} = x_{j+1}^{c_{i,j,j+1}} x_{j+1}^{c_{i,j,j+2}} \ldots x_{j+1}^{c_{i,j,n}}$, para $1 \leq j \leq i \leq n$

As relações da apresentação policíclica são chamadas de relações policíclicas. E dado o grupo $Pc[x_1, x_2, \ldots, x_n|R]$, definido e representado por uma apresentação policíclica, é chamado de PC−Grupo.

Todo grupo policíclico possui uma seqüência policíclica X e toda seqüência policíclica induz a um conjunto completo de relações policíclicas, pela proposição 5.1.2. Os expoentes S da apresentação policíclica são iguais às ordens relativas $R(X)$ neste caso.

Um caso de Apresentação Policíclica é quando tem-se uma Série Policíclica Refinada em que os grupos fatores da série policíclica são grupos cíclicos de ordem prima. O que se leva a definir:

Definição 5.2.2 Seja $[X|R]$ uma Apresentação Policíclica. Se os expoentes S da apresentação forem todos elementos primos, essa apresentação é denominada de Apresentação Policíclica Refinada.

Um grupo nilpotente é um grupo policíclico e pode ser representado por uma Apresentação Policíclica Refinada. Na seção seguinte o problema é reduzido fazendo o uso do conceito de Apresentação Policíclica Refinada.

5.3 Reduções Clássicas

Resolver o PSO diretamente nos grupos nilpotentes não tem sido considerado uma tarefa fácil. Para facilitar a resolução de tal problema, aqui é apresentada uma série de reduções em classes de grupos *nil-c*, uma classe fechada para subgrupos e grupos fatores.

É considerado na presente seção que um grupo nilpotente é representado por sua Apresentação Policíclica Refinada.

Também são utilizados, nesta seção, vários resultados que podem ser encontrados em diferentes literaturas, como as citadas a seguir. Usando a implementação quântica de Ivanyos et al. (2003) do algoritmo de Beals e Babai (1993), uma Apresentação Policíclica Refinada para um grupo solúvel pode ser computada eficientemente. Segundo Höfling (2007), há um algoritmo clássico eficiente para calcular a forma normal dos elementos de um grupo nilpotente, o qual denomina-se procedimento de coleta. E se há um procedimento de coleta, uma Apresentação Policíclica Refinada pode ser obtida eficientemente para subgrupos e grupos fatores por Holt et al. (2005), de forma clássica. Holt et al. (2005) também mostra que subgrupos de Sylow, centro e grupo de comutadores podem ser calculados de forma clássica e de maneira eficiente, caso haja um procedimento de coleta. Um outro resultado também usado é que em *p-grupos*, com Apresentação Policíclica Refinada, o normalizador de subgrupos pode ser computado em tempo polinomial usando a técnica clássica de Eick (2002) com algoritmo de estabilizador de subespaço de Luks (1992).

Lema 5.3.1 Seja G um grupo *nil-c*. O resolver o PSO em G reduz-se a resolver PSO em *p-grupos nil-c*.

Prova. Este resultado é uma conseqüência imediata de que um grupo é nilpotente se e somente se o grupo é isomorfo a soma direta de seus subgrupos de Sylow, os quais são *p-grupos*. Como a ordem dos subgrupos de Sylow são primas duas a duas, qualquer subgrupo H de G é intercessão de H com os subgrupos de Sylow

de G (Chi et al., 2006). ■

Lema 5.3.2 Seja G um *p-grupo nil-c*. Resolver o PSO G pode ser reduzido a encontrar subgrupos ocultos em *nil-c* com a hipótese adicional de que o subgrupo oculto tem ordem 1 ou p.

Prova. Aqui é assumido que há um procedimento $\mathcal{P}$, o qual encontra subgrupos ocultos em *nil-c* com a hipótese adicional de que o subgrupo oculto tem ordem 1 ou p. O problema já foi reduzido a *p-grupos*, seja G um *p-grupo* de C, e f a função separadora de classe, a qual oculta um subgrupo H de G.

Primeiramente é calculada uma seqüência refinada de G, $G = G_1 \triangleright G_2 \triangleright \cdots \triangleright G_s$. Observe que $|G_s| = p$, pois $G_s/\{e\} \simeq G_s$ tem ordem p daí que $|G_{s-1}| = p^2$ pelo teorema de Lagrange, da mesma forma $|G_{s-i}| = p^{i+1}$, para $0 \leq i \leq s-1$.

Agora percorre a seqüência refinada de G até encontrar um grupo de ordem p, começando por G_s. G_s tem ordem p, se não é encontrado em G_s um subgrupo de ordem p, é procurado em G_{s-1} por um subgrupo de ordem p, pois se $H \cap G_s = \{e\}$. Suponha que $|H \cap G| = p^2$, então $G_{s-1} = H$, mas $G_s \cap G_{s-1} = G_s \cap H$ que é um absurdo. Agora imagine que $H \cap G_{s-i} = \{e\}$ para $0 \leq i \leq s-2$ e provado que ou $|H \cap G_{s-i+1}| = p$ ou $|H \cap G_{s-i+1}| = 1$. Suponha que $|H \cap G_{s-i+1}| = p^k$, com $1 < k$, mas a cardinalidade de $G_{s-i+1} \setminus G_{s-i+1}$ é p, como $H \cap G_{s-i} = \{e\}$, $H \subset G_{s-i+1} \setminus G_{s-i+1}$, o que é um absurdo, logo $|H \cap G_{s-i+1}| = p$.

Quando encontrar um subgrupo de ordem $p, \langle h \rangle$ na seqüência policíclica de G, o processo é reiniciado em $G/\langle h \rangle$, mas $\langle h \rangle$ não necessariamente é um subgrupo normal de G, por isso o processo é reiniciado em $N_G(\langle h \rangle)$.

Mas como pode-se encontrar subgrupos de H em um grupo fator? Seja f a função que oculta H em G, dado $\tilde{H}$ um subgrupo de H, então f oculta $N_G(\tilde{H}) \cap H$ em $N_G(\tilde{H})$ e vai ocultar $(N_G(\tilde{H}) \cap H)$ em $(N_G(\tilde{H}) \cap H)/\tilde{H}$, se h é um representante de classe em $(N_G(\tilde{H}) \cap H)/\tilde{H}$, $h \in (N_G(\tilde{H}) \cap H)$, logo h também é um gerador de H.

Considere o seguinte algoritmo:

Algoritmo 2 EncotrarGruposdeOrdemp

Entrada: $\mathcal{P}, G$
Saída: Geradores de H

```
1: Sucesso:= V, H̃ := {e}
2: enquanto Sucesso = V faça
3:     se G ≠ H então
4:         compute (N_G(H̃) ∩ H) = G_1 ▷ G_2 ▷ ··· ▷ G_s, i := s
5:         enquanto i > 0 faça
6:             Chame P em G_i
7:             se P retornar ⟨h⟩ então
8:                 H̃ := ⟨H̃ ∪ {h}⟩, i := 0
9:             senão
10:                i := i − 1
11:                se i = 0 então
12:                    Sucesso:=F
13:                fim se
14:            fim se
15:        fim enquanto
16:    senão
17:        Sucesso:=F
18:    fim se
19: fim enquanto
```

O algoritmo 2 termina quando $(N_G(\tilde{H}) \cap H)/\tilde{H} = \{e\}$, e isso ocorre quando $G_1 = N_G(\tilde{H}) \cap H = \tilde{H}$. Suponha que $\tilde{H}$ é um subgrupo próprio de H, pelo fato de G ser nilpotente, $\tilde{H}$ é um subgrupo próprio de $N_H(\tilde{H}) = N_G(\tilde{H}) \cap H$ o que é um absurdo. Portanto $\tilde{H} = H$. No algoritmo a chamada do procedimento $\mathcal{P}$ está dentro de 2 loops que tem tamanho máximo s, com isso o algoritmo executa $O(\log_p^2 |G|)$ chamadas de $\mathcal{P}$. ■

Lema 5.3.3 Seja G um p-grupo *nil-c*. Resolver o PSO em G, em que o subgrupo oculto é trivial ou tem ordem p, pode ser reduzido ao PSO em grupos *nil-c* de expoente p.

Prova. Uma vez que o objetivo é encontrar grupos de ordens menores ou iguais a p, define-se G^* o subgrupo de G formado pelos elementos de ordem menor ou igual a p. O fato que G^* ser o subgrupo de G pode ser visto em Hall Jr. (1959). Cria-se um algoritmo por indução no tamanho da Apresentação Policíclica Refinada de G, se $|G| = p, G^* = G$. Caso contrário seja $G = G_1 \geq G_2 \geq \cdots \geq G_s \geq G_{s+1} = \{e\}$ a Série Policíclica de G, com $s > 1$. A série é construída a partir de G_s e por isso não é difícil criar a Série Policíclica começando com um elemento do centro. E suponha, daqui em diante, que $G_s \subset Z(G)$. Para facilitar a notação, seja $M = G_2, N = G_s$. Será descrito o passo de indução em um caso mais simples para posteriormente generalizar. Adicionando a hipótese $(G/N)^* = (G/N)$, o grupo quociente existe

pois é considerado que $N \subset Z(G)$. Veja que essa hipótese adicional é o mesmo que afirmar que todos os elementos de G/N têm ordem p, o que é equivalente a dizer que função $\phi : x \mapsto x^p$ leva todo elemento de G em N. Se a hipótese é satisfeita para G, a hipótese continua sendo verdade para M, ou seja, $(M/N)^* = M/N$. O teorema 12.4.4 de Hall Jr. (1959) afirma que ϕ é uma função separadora de classes de C^* em G, e com isso percebe-se que ou $C^* = G$ ou o índice de p. Se $C^* = G$ não há nada para prova, mas caso contrário, vai-se computar M^*. E se $M^* = M$ então $G^* = M$ senão M^* tem índice p em M e terá índice p^2 em G. Sejam $u \in M \setminus M^*$ e $y \in G \setminus M$, como $u^p \in G_s$ $y^p \in G_s$ e , existem $j_u, j_y \in \mathbb{Z}_p^*$ de forma que $u^p = g_s^{j_u}$ e $y^p = g_s^{j_y}$. Lembrando que com uma Apresentação Policíclica Refinada as formas normais de u^p e y^p podem ser computadas. Definindo $x := u^{j_y j_u}$ potências podem ser computadas usando exponenciação, $x^p = y^p$ mas portanto $xy^{-1} \in G^*$, da forma a qual xy^{-1} foi definido, $xy^{-1} \in G^* \setminus M^*$. Sendo assim, $G^* = \langle M^*, xy^{-1} \rangle$. No caso geral, $(G/N)^*$ é computado indutivamente, e se $(G/N)^* = G/N$ aplica-se o método anterior para computar G^*, caso contrário defini-se o conjunto $K = (G/N)^* N$.

Afirma-se que $G^* = K^*$, e prova-se que $G^* \subset K$.

Seja $x \in G^*$, $x = yz$ onde y é um representante de alguma classe lateral de N e $z \in N$, então $y^p = y^p z^p = (yz)^p = (x)^p = 1$, pois $|N| = p$, $N \leq Z(G)$ e $x \in G^*$. Logo $x \in K^*$ Observe que $K/N = (G/N)^*$ implica em $(K/N)^* = K/N$. Portanto pode-se determinar K^* indutivamente usando o caso simplificado.

Seja $c(s)$ o número de chamadas recursivas em função de s, em que s é o tamanho da Série Policíclica. No caso simplificado faz-se $s - 1$ cálculos. E no caso geral tem-se $c(s) = c(s-1) + s - 2$ e com isso $c(s) = O(s^2)$. ■

Essa seqüência de lemas tem como conseqüência o teorema a seguir.

Teorema 5.3.1 O problema do subgrupo oculto em grupos *nil-c* é reduzido ao PSO em *p-grupos* de expoente p *nil-c* onde o subgrupo oculto tem ordem 1 ou p.

E particularizando para os grupos *nil*-2.

Corolário 5.3.1 O problema do subgrupo oculto em grupos *nil*-2 é reduzido ao PSO em *p-grupos* de expoente p *nil*-2 onde o subgrupo oculto tem ordem 1 ou p.

5.4 Algoritmo Quântico

Nesta seção é construído algoritmo quântico para resolução do PSO em grupos *nil*-2. Na classe de grupos *nil*-2 o PSO foi reduzido ao PSO em *p-grupos nil*-2 de expoente p, com a hipótese de que o grupo procurado tem ordem p ou 1.
Em Algoritmos Quânticos Abelianos, geralmente repete-se várias vezes a aplicação da Transformada de Fourier de uma mesma função que *oculta* o grupo, como a cada interação usa-se diferentes funções que ocultam o grupo em questão, lança-se mão de uma técnica já usada por Ivanyos et al. (2003), na qual usa-se um procedimento que oculta o subgrupo em questão. É visto a seguir como se defini este procedimento e como ele será usado na resolução do PSO em grupos abelianos.

Definição 5.4.1 Um conjunto de vetores $\{|\Psi_g\rangle : g \in G\}$ de um espaço de Hilbert $\mathcal{H}$ é um conjunto que oculta o subgrupo H em G, se

- $|\Psi_g\rangle$ é um vetor unitário para todo $g \in G$.
- Se g, g' pertencem a mesma classe lateral de H, então $|\Psi_g\rangle = |\Psi_{g'}\rangle$.
- Se g, g' pertencem à classes laterais diferentes, então $|\Psi_g\rangle$ é ortogonal a $|\Psi_{g'}\rangle$.

Agora defini-se o que é o procedimento quântico que oculta o subgrupo H de G.

Definição 5.4.2 Dados $g_1, g_2, \ldots, g_N \in G$ um procedimento quântico que oculta um subgrupo H de G, um procedimento quântico que tem como entrada os estados $|g_1\rangle|g_2\rangle \ldots |g_N\rangle|0\rangle$ e como saída os estados $|g_1\rangle|g_2\rangle \ldots |g_N\rangle|\Psi^1_{g_1}\rangle|\Psi^2_{g_2}\rangle \ldots |\Psi^N_{g_N}\rangle$, onde $\{|\Psi^i_g\rangle : g \in G\}$ é um conjunto que oculta H em G.

A proposição a seguir mostra como usar o procedimento quântico para substituir a aplicação da Transformada de Fourier no PSO abeliano.

Proposição 5.4.1 Dado G um grupo abeliano. Se existe um procedimento quântico eficiente que oculta o subgrupo H em G, então existe um procedimento quântico eficiente para encontrar H em G.

Prova. Usa-se aqui o algoritmo quântico para resolução do PSO abeliano com uma pequena variação.

Algoritmo 3 PSEAbelianoPQE

1: Prepare a superposição inicial $|1_G\rangle|0^m\rangle$.
2: Aplique a transformada de Fourier abeliana no primeiro registrador:

$$\sum_{g\in G}|g\rangle|0^m\rangle$$

3: Chame o procedimento quântico que oculta H em G:

$$\sum_{g\in G}|g\rangle|\Psi_g^i\rangle$$

4: Aplique novamente a transformada de Fourier abeliana:

$$\sum_{g\in G/H,h\in H^\perp}\chi_h(g)|h\rangle|\Psi_g^i\rangle$$

5: Meça o primeiro registrador.

Depois da execução do algoritmo terá um elementos de $H^\perp$. Empregando os mesmos procedimentos que foram utilizados na resolução PSO abeliano, obtém-se os elementos geradores de H com probabilidade maior que $\frac{1}{2}$. ■

Não se trabalha com um procedimento quântico para ocultar H e sim é criado um procedimento quântico que oculta HG'. No teorema a seguir mostra-se como encontrar H tendo um procedimento quântico eficiente que oculta HG'.

Teorema 5.4.1 Dado G um p-grupo nil-2 de expoente p. Dada uma função oráculo f que oculta um subgrupo H de G, com a promessa de que H tem cardinalidade 1 ou p. Se existe um procedimento quântico eficiente que oculta HG' em G, então H pode ser encontrado eficientemente.

Prova. Primeiramente veja como encontrar H pode ser reduzido a encontrar HG'. H é um grupo abeliano, pois H tem ordem p ou 1, e $G' \subseteq Z(G)$, portanto HG' é um grupo abeliano.

A função f que oculta H em G também oculta H em HG', então basta usar o algoritmo para resolução do PSO abeliano em HG' para encontrar H.

Observe-se que G não é necessariamente um grupo abeliano e por isso não se pode aplicar diretamente a proposição anterior para encontrar HG' tendo um

procedimento quântico que oculta HG' em G, mas agora o problema é levado a um grupo abeliano para encontrar HG'.

G é um grupo nil-2 de parâmetros (m, d). Dado um elemento $g \in G$, g se escreve de forma única $g = x_1^{e_1}x_2^{e_2}\dots x_m^{e_m}\dots z_1^{f_1}z_2^{f_2}\dots z_d^{f_d}$, denota-se por $\overline{g}$, o elemento $\overline{g} = x_1^{e_1}x_2^{e_2}\dots x_m^{e_m}$ e seja o conjunto $\overline{G} = \{\overline{g} : g \in G\}$ e em $\overline{G}$ defini-se a operação $* : \overline{G} \to \overline{G}$ com sendo dados $\overline{g_1}, \overline{g_2} \in G$, $\overline{g_1} * \overline{g_2} = \overline{g_2 g_1}$. A operação $*$ está bem definida e verifica-se que $(*, \overline{G})$ é um grupo. Defini-se:

$$f : \overline{G} \to G/G'$$
$$\overline{g} \mapsto gG'$$

f é um homomorfismo. Veja que f também é um isomorfismo. f é injetora, pois dados $g_1, g_2 \in G$, tais que $f(\overline{g_1}) = f(\overline{g_2})$, escrevendo g_1, g_2 pelos geradores, $g_1 = x_1^{e_1^1}\dots x_m^{e_m^1}z_1^{f_1^1}\dots z_d^{f_d^1}$, $g_2 = x_1^{e_1^2}\dots x_m^{e_m^2}z_1^{f_1^2}\dots z_d^{f_d^2}$. Pelo fato de que $f(\overline{g_1}) = f(\overline{g2})$, existe $z \in G'$ tal que $x_1^{e_1^1}\dots x_m^{e_m^1} = x_1^{e_1^2}\dots x_m^{e_m^2}z$, mas pela escrita única, $z = e$ e $e_1^1 = e_1^2, \cdots, e_1^m = e_1^m$. A f é sobrejetiva, pois dado $gG' \in G/G'$, escrevendo g como produto de geradores, $g = x_1^{e_1}x_2^{e_2}\dots x_m^{e_m}\dots z_1^{f_1}z_2^{f_2}\dots z_d^{f_d}$, $\overline{g} = g = x_1^{e_1}x_2^{e_2}\dots x_m^{e_m}$, aplicando f a $\overline{g}$, $f(\overline{g}) = \overline{g} = g = x_1^{e_1}x_2^{e_2}\dots x_m^{e_m}G' = g = x_1^{e_1}x_2^{e_2}\dots x_m^{e_m}\dots z_1^{f_1}z_2^{f_2}\dots z_d^{f_d}G'$. Portanto f é isomorfismo.

$\overline{G}$ é isomorfo a G/G' que é isomorfo a $\mathbb{Z}_p^m$ logo $\overline{G}$ é isomorfo a $\mathbb{Z}_p^m$.

Observe que HG'/G' é um subgrupo de G/G', pois HG' é um subgrupo de G. Com isso, $HG' \cap \overline{G}$ é um subgrupo de $(\overline{G}, *)$. Agora pode-se tratar do problema em um grupo abeliano e o procedimento que oculta HG' em G também oculta $HG' \cap \overline{G}$ em $\overline{G}$. Ainda resta um problema, pois foi encontrado apenas $HG' \cap \overline{G}$, mas afirma-se o seguinte, $HG' = (HG' \cap \overline{G})G'$. O subgrupo G' é um subgrupo conhecido, logo HG' pode ser conhecido também. ■

Deve-se, contudo, criar um procedimento quântico eficiente que oculta o subgrupo HG' em G.

Seja $|G'_u\rangle = \frac{1}{\sqrt{|G'|}}\sum_{z\in\mathbb{Z}_p^m}\omega^{-<u,z>}|z\rangle$. Se multiplicar o vetor pelo elemento $\omega^{<u,z'>}$,

tem-se:

$$\omega^{<u,z'>}|G'_u\rangle = \omega^{<u,z'>}\frac{1}{\sqrt{|G'|}}\sum_{z\in\mathbb{Z}_p^m}\omega^{-<u,z>}|z\rangle = \frac{1}{\sqrt{|G'|}}\sum_{z\in\mathbb{Z}_p^m}\omega^{<u,z'-z>}|z\rangle =$$

$$\sum_{z\in\mathbb{Z}_p^m}\omega^{-<u,z>}|zz'\rangle = |G'_u\cdot z'\rangle.$$

Daí,

$$|G'_u\cdot z'\rangle = \omega^{<u,z'>}|G'_u\rangle. \tag{5.1}$$

Já a ação de h em $|aHG'_u\rangle$ será

$$|aHG'_u\cdot h\rangle = |aHG'_u\rangle \tag{5.2}$$

Não é difícil notar que o conjunto $\{|aHG'\cdot g\rangle, g\in G\}$ é um conjunto que oculta HG' em G. Mas criar o estado $|aHG'\rangle$ é eficiente somente para p, d constantes. Usando a Transformada de Fourier, pode-se criar eficientemente o estado $|aHG'_u\rangle$, para algum $a\in G$ e para algum $z\in G'$, embora não é permitido criar diretamente um conjunto que oculta HG' em G devido a uma fase que é adicionada ao estado. Porém, mais adiante será visto como anular essa fase criada.

Lema 5.4.1 Existe um algoritmo quântico eficiente para criar o estado

$$\frac{1}{\sqrt{p^d}}\sum_{u\in\mathbb{Z}_p^m}|u\rangle|aHG'_u\rangle$$

Prova.

Algoritmo 4 CriarEstado$|aHG'\rangle$

1: Prepare a superposição inicial $|0_{\mathbb{Z}_p^d}\rangle|0_G\rangle|0\rangle$.

2: Use o paralelismo quântico para criar a superposição:

$$\sum_{g\in G}|0_{\mathbb{Z}_p^d}\rangle|g\rangle|f(g)\rangle$$

3: Mede o terceiro registrador:

$$|0_{\mathbb{Z}_p^d}\rangle|aH\rangle$$

para algum $a \in G$

4: Aplique a transformada de Fourier no primeiro registrador:

$$|\mathbb{Z}_p^d\rangle|aH\rangle$$

para algum $a \in G$.

5: Multiplique o segundo registrador pelo inverso do primeiro:

$$\sum_{z\in\mathbb{Z}_p^d}|-z\rangle|aHz\rangle$$

6: Aplique novamente a transformada de Fourier ao primeiro registrador:

$$\sum_{u\in\mathbb{Z}_p^d}\omega^{-<u,z>}|u\rangle|aHG'_u\rangle$$

■

Medindo o primeiro registrador do estado $\sum_{u\in\mathbb{Z}_p^d}\omega^{-<u,z>}|u\rangle|aHG'_u\rangle$, tem-se o estado $|aHG'_u\rangle$. No próximo lema é visto que os estados $|aHG'_u\rangle$ são autovalores da ação de $\phi_j(g)$, com $g\in HG'$, ou seja, $|aHG'_u\rangle$ é um autovetor da transformação $U_{\phi_j(g)}$, em que $g\in HG'$. E os autovalores são potências de raízes da unidade.

Lema 5.4.2 Tem-se que

(1) $\forall z\in\mathbb{Z}_p^d,\forall a\in G,\forall u\in\mathbb{Z}_p^d,\forall j\in\mathbb{Z}_p^d,$

$$|aHG'_u\cdot\phi_j(z)\rangle=\omega^{<u,z>j^2}|aHG'_u\cdot\phi_j(z)\rangle$$

(2) $\forall h\in H,\forall z\in\mathbb{Z}_p^d,\forall a\in G,\forall u\in\mathbb{Z}_p^d,\forall j\in\mathbb{Z}_p^d,$

$$|aHG'_u\cdot\phi_j(h)\rangle=\omega^{<u,z_h>(j-j_2)}|aHG'_u\cdot\phi_j(z)\rangle$$

Prova. Segue diretamente da proposição 3.3.5 e das identidades 5.1, 5.2. ■

Veja que os autovalores dependem somente de u,j, onde u é um elemento aleatório de $\mathbb{Z}_p^d$, já j é escolhido. Se o autovalor associado a $|aHG'_u\rangle$ for igual a 1, o conjunto $\{|aHG'_u\cdot\phi_j(g)\rangle,g\in G\}$ é um conjunto que oculta HG' em G, como é visto mais adiante. Porém dados um vetor $u\in\mathbb{Z}_p^d$, $h\in H$ e $z\in G'$, o $|aHG'_u\cdot\phi_j(hz)\rangle=\omega^{<u,z_h>(j-j^2)+<u,z>j^2}|aHG'_u\rangle$. Encontrar $j\neq$ tal que a equação

$$<u,z_h>(j-j^2)+<u,z>j^2=0^d \tag{5.3}$$

seja satisfeita não é uma tarefa fácil e não se tem solução garantida, mas criando outros estados da forma $|aHG'_u\rangle$ pode-se chegar a uma equação que pode ser resolvida eficientemente.

Seja o inteiro $n=n(d)$ a quantidade de estados que será criado, em função de d que será determinado mais tarde.

Com isso para $\overline{a}=(a_1,\ldots,a_n)\in G^n$, $\overline{u}=(u_1,\ldots,u_n)\in\left(\mathbb{Z}_p^d\right)^n$ e $\overline{j}=(j_1,\ldots,j_n)\in\left(\mathbb{Z}_p\right)^n\setminus 0^n$ e $g\in G$, defini-se o estado:

$$|\psi_g^{\overline{a},\overline{u},\overline{j}}\rangle = \otimes_{i=1}^{n} |a_i HG'_{u_i} \cdot \phi_{j_i}(g)\rangle$$

Deve-se encontrar $\overline{j} \in (\mathbb{Z}_p)^n \setminus 0^n$ de forma que o conjunto $\{|\psi_g^{\overline{a},\overline{u},\overline{j}}\rangle; g \in G\}$ oculta HG' em G.

Diz-se que a tripla $(\overline{a}, \overline{u}, \overline{j})$ é uma tripla perfeita se o autovalor do vetor $|\psi_h^{\overline{a},\overline{u},\overline{j}}\rangle$ sobre a ação de $\phi_{j_i}(h)$ é $1, \forall h \in HG'$, ou seja, $|\psi_h^{\overline{a},\overline{u},\overline{j}}\rangle = \otimes_{i=1}^{n} |a_i HG'_{u_i}\rangle, \forall h \in HG'$. Será visto no próximo lema que quando a tripla $(\overline{a}, \overline{u}, \overline{j})$ é perfeita, o conjunto $\{|\psi_g^{\overline{a},\overline{u},\overline{j}}\rangle; g \in G\}$ oculta HG' em G.

Lema 5.4.3 Se $(\overline{a}, \overline{u}, \overline{j})$ é uma tripla perfeita, então $\{|\psi_g^{\overline{a},\overline{u},\overline{j}}\rangle; g \in G\}$ oculta HG' em G

Prova. Observe que HG' é um subgrupo normal de G, pois dados $g \in G, h \in H, z \in G'$, $gh = hg[g,h]$, como $G' \subseteq Z(G)$, multiplicando ambos os lados da igualdade anterior por z, $ghz = hz[g,h]g$, portanto $gHG' = HG'g$.

Dados $g_1, g_2 \in G$ elementos que pertencem às classes laterais distintas. Como há pelo menos um $j_i \neq 0, 0 \leq i \leq n$, ϕ_{j_i} é um automorfismo, logo leva elementos de classes laterais distintas à classes laterais distintas. E com isso $\phi_{j_i}(g_1)$ pertence a uma classe lateral distinta de $\phi_{j_i}(g_2)$. Tem-se que $supp|aHG'_u\rangle = supp|aHG'\rangle$, com isso o conjunto $supp(|aHG'_u \cdot \phi_{j_i}(g_1)\rangle)$ pertence a uma classe lateral distinta, da qual pertence o conjunto $supp(|aHG'_u \cdot \phi_{j_i}(g_2)\rangle)$. Portanto, os vetores $|\psi_{g_1}^{\overline{a},\overline{u},\overline{j}}\rangle$ e $|\psi_{g_2}^{\overline{a},\overline{u},\overline{j}}\rangle$ são ortonormais.

Agora imagine que g_1, g_2 pertencem a mesma classe lateral. Sendo assim, existe $g \in HG'$, tal que $g_1 = gg_2$, e $\phi_{j_i}(g_1) = \phi_{j_i}(g)\phi_{j_i}(g_2), \forall i \in \{0, \ldots, n\}$. Daí $|\psi_{g_1}^{\overline{a},\overline{u},\overline{j}}\rangle = |\psi_{gg_2}^{\overline{a},\overline{u},\overline{j}}\rangle$, usando o fato de que $\phi_{j_i}(g) \in HG'$ e $\otimes_{i=1}^{n} |a_i HG'_{u_i}\rangle$ é um autovetor da ação de $\phi_{j_i}(g)$ com autovalor 1, $|\psi_{g_1}^{\overline{a},\overline{u},\overline{j}}\rangle = |\psi_{g_2}^{\overline{a},\overline{u},\overline{j}}\rangle$. ■

Uma questão ainda pendente é como encontrar $\overline{j}$ de forma que o conjunto $\{|\psi_g^{\overline{a},\overline{u},\overline{j}}\rangle; g \in G\}$ oculta HG' em G. Dado hz em HG' e $(\overline{a}, \overline{u}, \overline{j}) \in G$.

$$|\psi_{hz}^{\overline{a},\overline{u},\overline{j}}\rangle = \omega^{\sum_{i=1}^{n} <u_i, z_h>(j_i - j_i^2) + <u_i, z> j_i^2} \otimes_{i=1}^{n} |a_i HG'_u\rangle \tag{5.4}$$

Como a o autovalor do estado acima dever ser 1, $\forall z_h, z \in G'$, na equação que depende somente de $\overline{j}$ e $\overline{u}$.

$$\begin{cases} \sum_{i=1}^{n} u_i(j_i - j_i^2) &= 0^d. \\ \sum_{i=1}^{n} u_i j_i &= 0^d. \end{cases} \tag{5.5}$$

O teorema A.0.4 do apêndice A mostra que quando $n = (d+1)^2(d+2)/2$ o sistema 5.5 admite solução e pode ser encontrada eficientemente. Assim é criado o procedimento quântico que oculta HG' em G.

Teorema 5.4.2 Dado G um p-grupo *nil*-2 de expoente p. Dada uma função f que oculta um subgrupo H de G, com a promessa de que H tem ordem 1 ou p. Existe um procedimento quântico eficiente que oculta HG' em G.

Agora usado o teorema 5.4.1 e as reduções que foram feitas na seção anterior chegamos ao principal teorema desse capítulo que é enunciado a seguir.

Teorema 5.4.3 Seja G um *nil*-2. O PSO pode ser resolvido de forma eficiente em G.

Capítulo 6

Conclusões

Esta dissertação iniciou-se com uma revisão dos conceitos da Computação Quântica. Em seguida foi elaborada uma breve revisão sobre grupos Solúveis e Nilpotentes, dando ênfase aos grupos nilpotentes de classe 2. Também foram apresentadas algumas propriedades de grupos nilpotentes de classe 2 não muito comuns em literaturas; e, omitindo alguns detalhes, foi mostrado o algoritmo quântico padrão para solução do PSO em grupos abelianos, que tem como um dos pontos principais a aplicação da transformada de Fourier abeliana.

No principal capítulo desta dissertação, o capítulo 5, foram exibidas as principais características de Cadeias Policíclicas. Em seguida, foram expostas reduções importantíssimas na resolução do PSO em grupos Nilpotentes e apresentado o algoritmo quântico para resolução do PSO em grupos nilpotentes de classe 2, uma importante classe de grupos na Teoria de Grupos.

Um resultado importante que foi indicado nesta dissertação é o fato de que o PSO em grupos de nilpotência constante - classe de grupos fechada para subgrupos e para grupos fatores - são reduzidos à *p-grupos* de expoente p, onde o subgrupo oculto tem ordem 1 ou p.

Uma perspectiva para trabalhos futuros é usar "ferramentas" apresentadas por (Ivanyos et al., 2007a) na solução do PSO em grupos Nilpotentes de classe 2 para a extensão da solução em grupos Nilpotentes de classe 3.

Apêndice A

Resolvendo o sistema de equações

Este apêndice é integralmente destinado a mostrar que o sistema de equação 5.5 admite solução e pode ser computada eficientemente. Baseado no teorema 5 de (Ivanyos et al., 2007a).

Teorema A.0.4 Considere a equação:

$$\begin{cases} \sum_{i=1}^{n} u_i(j_i - j_i^2) &= 0^d. \\ \sum_{i=1}^{n} u_i j_i &= 0^d. \end{cases} \tag{A.1}$$

Onde $\overline{u} = (u_1, \ldots, u_n) \in (\mathbb{Z}_p^d)^n$. Se $n = (d+1)^2(d+2)/2$ o sistema A.1 admite solução e é encontrada eficientemente.

Prova. Se $p = 2$ o sistema coincide com um sistema linear e pode ser computado eficientemente, por isso é considerado $p > 2$.

O teorema de Chevalley-Warning de (Chevalley, 1936; Warning, 1936) garante que o sistema A.1 admite solução e é equivalente ao sistema,

$$\begin{cases} \sum_{i=1}^{n} u_i j_i^2 &= 0^d \\ \sum_{i=1}^{n} u_i j_i &= 0^d, \end{cases} \tag{A.2}$$

segundo (Ivanyos et al., 2007a).

Seja $u_i = (u_{1,i}, u_{2,i}, \ldots, u_{d,i})$, com isso tem-se o sistema:

$$\begin{cases} \forall l \in [|1,d|], & \sum_{i=1}^{n} u_{l,i} j_i^2 = 0^d \\ \forall l \in [|1,d|], & \sum_{i=1}^{n} u_{l,i} j_i = 0^d. \end{cases} \tag{A.3}$$

Considere primeiramente a seguinte soma do sistema:

$$\begin{cases} \forall l \in [|1,d|], & \sum_{i=1}^{n} u_{l,i} j_i^2 = 0^d. \end{cases} \tag{A.4}$$

Sendo assim, o sistema é representado pela matrix $d \times n$:

$$M = \begin{pmatrix} u_{1,1} & \ldots & u_{1,n} \\ \vdots & \ddots & \vdots \\ u_{d,1} & \ldots & u_{d,n} \end{pmatrix}$$

O algoritmo que será apresentado é um algoritmo recursivo. Se $d = 1$, tem-se uma única equação quadrática da forma $u_{1,1} j_1^2 + u_{1,2} j_2^2 + u_{1,3} j_3^2 = 0$, que é um caso particular do Teorema A3 de (v. de Woestijne, 2005) e uma solução pode ser encontrada eficientemente.

É considerado que tem-se d equações com $n = (d+1)(d+2)/2$ incógnitas. Pode-se fazer operações elementares (subtraindo linhas e multiplicando por constantes) em M, criando um sistema equivalente, com objetivo de reduzir o sistema a um sistema de $d-1$ equações com $d(d+1)/2$ incógnitas para usar a recursividade. Se o posto de M for menor que d, pode-se esquecer uma equação e ficar com um sistema de $d-1$ equações com o mesmo número de incógnitas, mas se o posto de M for d, fazendo operações elementares na matriz M, obtém-se um sistema:

$$M_1 = \begin{pmatrix} 1 & 0 & 0 & \dots & 0 & u^{(1)}_{1,d+1} & \dots & u^{(1)}_{1,n} \\ 0 & 1 & 0 & \dots & 0 & u^{(1)}_{2,d+1} & \dots & u^{(1)}_{2,n} \\ \vdots & \vdots & \ddots & \dots & \vdots & \vdots & \ddots & \vdots \\ 0 & \dots & 0 & 1 & 0 & u^{(1)}_{d-1,d+1} & \dots & u^{(1)}_{d-1,n} \\ 0 & \dots & 0 & 0 & 1 & u^{(1)}_{d,d+1} & \dots & u^{(1)}_{d,n} \end{pmatrix}$$

Uma questão simples de ser verificada é que metade dos elementos de $\mathbb{Z}_p^*$ possui raiz, considerando o grupo $\mathbb{Z}_p$. Com isso um elemento λ que não possui raiz pode ser computado facilmente, e um elemento qualquer de $\mathbb{Z}_p$ que não possui raiz é múltiplo de uma raiz por λ. Agora observe a coluna $d+1$ do sistema. Se essa coluna for toda nula, então $j_{d+1} = 1$ e $j_i = 0, \forall i \neq d+1$ é uma solução não trivial para o sistema. Caso contrário, separa-se os elementos da coluna $d+1$, considerando $(k_1, k_2) \neq (0,0)$ tais que os k_1 primeiros elementos e os k_2 elementos seguintes não possuem raízes, já os restantes dos elementos da coluna $d+1$ de M_1 são nulos. Existem $v_1, v_2, \dots, v_{k_1+k_2}$ diferentes de 0, tais que $u^{(1)}_{i,d+1} = v_i^2$, para $1 \leq i \leq k_1$ e $u^{(1)}_{i,d+1} = \lambda v_i^2$, para $k_1 + 1 \leq i \leq k_1 + k_2$. Os elementos v_i $\forall 1 \leq i \leq k_1 + k_2$ podem ser determinados eficientemente de acordo com o algoritmo de Shanks-Tonelli em (Shanks, 1972). Agora define-se as incógnitas $j_{k_1+k_2+1}, \dots, j_d$ todas iguais a 0, eliminando as colunas $k_1 + k_2 + 1, \dots, d$ de M_1. Dividindo a linha i por $v_i, \forall 1 = 1, \dots, k_1 + k_2$. Introduzindo as novas variáveis $j_i^{'} = j_i v_i^{-1}, \forall 1 = 1, \dots, k_1 + k_2$ tem-se um sistema equivalente a M_1 com $n - d + k_1 + k_2$ variáveis com as incógnitas $j_1^{'}, \dots, j_{k_1+k_2}^{'}, j_{d+1}, \dots, j_n$.

$$M_2 = \begin{pmatrix} 1 & 0 & \dots & \dots & \dots & 0 & 1 & u^{(2)}_{1,d+2} & \dots & u^{(2)}_{1,n} \\ 0 & \ddots & \dots & \dots & \dots & \vdots & \vdots & \vdots & \dots & \vdots \\ 0 & \dots & 1 & \vdots & \dots & \vdots & 1 & u^{(2)}_{k_1,d+2} & \dots & u^{(2)}_{k_1,n} \\ \vdots & \dots & \ddots & 1 & \dots & \dots & \lambda & u^{(2)}_{k_1+1,d+2} & \dots & u^{(2)}_{k_1+1,n} \\ \vdots & \dots & \ddots & \dots & \vdots & 0 & \dots & \vdots & \dots & \vdots \\ 0 & \dots & \ddots & \dots & 0 & 1 & \lambda & u^{(2)}_{k_1+k_2,d+2} & \dots & u^{(2)}_{k_1+k_2,n} \\ 0 & \dots & \ddots & \dots & 0 & 0 & 0 & u^{(2)}_{k_1+k_2+1,d+2} & \dots & u^{(2)}_{k_1+k_2+1,n} \\ \vdots & \dots & \ddots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & \dots & \ddots & \dots & \vdots & \ddots & 0 & u^{(2)}_{d,d+2} & \dots & u^{(2)}_{d,n} \end{pmatrix}$$

Agora subtrai a primeira linha das linhas $2, \ldots, k_1$ e a linha 2 da s linhas $k_1 + 1, \ldots, k_2 + k_1$. E substitui as variáveis $j_2^{'}, \ldots, j_{k_1}^{'}$ por $j_1^{'}$ e as variáveis $j_{k_1+1}^{'}, \ldots, j_{k_1+k_2}^{'}$ por $j_{k_1}^{'}$, lembrando que se está buscando uma única solução não trivial para o sistema. Efetuando as mudanças na matriz M_2:

$$M_3 = \begin{pmatrix} 1 & 0 & 1 & u_{1,d+2}^{(3)} & \ldots & u_{1,n}^{(3)} \\ 0 & 1 & \lambda & u_{2,d+2}^{(3)} & \ldots & u_{2,n}^{(3)} \\ 0 & 0 & 0 & u_{3,d+2}^{(3)} & \ldots & u_{3,n}^{(3)} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \\ 0 & 0 & 0 & u_{d,d+2}^{(3)} & \ldots & u_{d,n}^{(3)} \end{pmatrix}$$

A parte final da redução distingue-se em 2 casos, dependendo da congruência de p módulo 4. Se p é côngruo a 1 módulo 4, então -1 possui raiz e uma raiz s de -1 pode ser computado eficientemente. Sendo assim, define-se $j_1^{'} = sj_{d+1}$ e elimina-se a coluna 1 da matriz M_3, definindo como 0 o elemento da linha 1 coluna $d+1$ e alterando a linha 1 e linha 2. Quando p é côngruo a 3 módulo 4 o elemento -1 não possui raíz e portanto defini-se $\lambda = -1$. Defini-se $j_{k_1+1}^{'} = j_{d+1}$, eliminando a coluna 2 e nomeando como sendo 0 o elemento da linha 2 coluna $d+1$. Obtendo uma matriz da forma:

$$M_4 = \begin{pmatrix} 1 & \alpha & u_{1,d+2}^{(3)} & \ldots & u_{1,n}^{(3)} \\ 0 & 0 & u_{2,d+2}^{(3)} & \ldots & u_{2,n}^{(3)} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & u_{d,d+2}^{(3)} & \ldots & u_{d,n}^{(3)} \end{pmatrix},$$

nas variáveis $j^{'}, j_{d+1}, \ldots, j_n$, onde $\alpha = \lambda$, $j^{'} = j_{k_1+1}$ quando p é côngruo a 1 módulo p, e caso contrário, $\alpha = 1$ e $j^{'} = j_1$. Com isso chegou-se a um sistema com $d-1$ equações e $d(d+1)/2$ incógnitas. Usando o processo recursivo, faz-se a mesma redução que foi feita na matriz M na matriz M_4. Até chegar ao sistema $j'^2 + \alpha j_{d+2}^2 + \sum_{k=d+2}^{n} u_{1,k}^{(3)} j_k = 0$, definindo $b = \sum_{k=d+2}^{n} u_{1,k}^{(3)} j_k$, tem-se o sistema $j'^2 + \alpha j_{d+2}^2 + b = 0$, que novamente é um caso particular do Teorema A3 de (v. de Woestijne, 2005) e pode ser determinada eficientemente.

As operações realizadas para resolver o sistema são todas de ordem $O(poli(d \log p))$.

Como o sistema é resolvido recursivamente, pode acontecer de aumentar o grau do polinômio, mas a ordem do algoritmo continuará sendo $O(poli(d \log p))$.
Novamente volta-se ao sistema A.3. Sejam $n' = n(d+1)$ e $1 \leq k \leq d$, considere o sistema quadrático d equações com n variáveis:

$$\left\{ \forall l \in [|1, d|], \quad \sum_{i=kn+1}^{(k+1)n} u_{l,i} j_i^2 \quad = \quad 0^d. \right. \tag{A.5}$$

Como foi visto, o sistema de equações acima possui solução e pode ser computada eficientemente. Para um k qualquer, dado $(j_{kn+1}, \ldots, j_{(k+1)n})$ uma solução do k-ésimo sistema quadrático. Então o conjunto:

$$\{(\lambda_0 j_1, \ldots, \lambda_0 j_n, \lambda_1 j_{n+1}, \ldots, \lambda_1 j_{2n}, \ldots, \lambda_d j_{dn+1}, \ldots, \lambda_d j_{(d+1)n}) : (\lambda_0, \lambda_d) \in \mathbb{Z}_p^{d+1}\}$$

é um subespaço de $\mathbb{Z}_n^{d+1}$, cujos elementos são soluções da equação quadrática de A.2. Então pode-se computar um elementos não diferente de $(0, \ldots, 0)$ tal que,

$$\{(\lambda_0 j_1, \ldots, \lambda_0 j_n, \lambda_1 j_{n+1}, \ldots, \lambda_1 j_{2n}, \ldots, \lambda_d j_{dn+1}, \ldots, \lambda_d j_{(d+1)n}) : (\lambda_0, \lambda_d) \in \mathbb{Z}_p^{d+1}\}$$

seja uma solução não trivial do sistema linear de A.2. Concluindo assim a prova do teorema.

■

Referências Bibliográficas

R. Beals e L. Babai. Las vegas algorithms for matrix groups. In **FOCS**, páginas 427–436, 1993.

C. Chevalley. Demonstration d'une hypothese de m. artin. In **Abhand. Math. Sem. Univ. Hamburg**, páginas 11:73–76, 1936.

D.P. Chi, J.S. Kim, e S. Lee. Quantum algorithms for the hidden subgroup problem on some semi-direct product groups by reduction to abelian cases. **Physics Letters A**, 359(2):114–116, 2006.

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

D. Deutsch. Quantum theory, the church-turing principle and the universal quantum computer. In **Proceedings of the Royal Society of London. Series A**, volume 400, páginas 97–117, 1985.

D. Deutsch e R. Jozsa. Rapid solution of problems by quantum computation. In **Proc: Mathematical and Physical Sciences (Royal Society of London)**, volume 439, páginas 553–558, 1992.

B. Eick. Orbit-stabilizer problems and computing normalizers for polycyclic groups. **J. Symb. Comput.**, 34(1):1–19, 2002. ISSN 0747-7171.

J. C. Ellenbogen. A brief overview of nanoelectronic devices. In **McLean, VA 22102**. The MITRE Corporation, 1998.

R. P. Feynman. Simulating physics with computers. **International Journal of Theoretical Physics**, 21(6-7):467–488, 1982.

K. Friedl, G. Ivanyos, F. Magniez, M. Santha, e P. Sen. Hidden translation and orbit coset in quantum computing, 2003. URL `citeseer.ist.psu.edu/friedl03hidden.html`.

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

M. Grigni, L. J. Schulman, M. Vazirani, e U. V. Vazirani. Quantum mechanical algorithms for the nonabelian hidden subgroup problem. In **ACM Symposium on Theory of Computing**, páginas 68–74, 2001. URL `citeseer.ist.psu.edu/grigni00quantum.html`.

Lov K. Grover. A fast quantum mechanical algorithm for database search. páginas 212–219, 1996. URL `citeseer.ist.psu.edu/grover96fast.html`.

L. Hales e S. Hallgren. An improved quantum fourier transform algorithm and aplications. In **Proc. 41st Ann. IEEE Symp. on Foundation of Computer Science - FOCS 2000**, páginas 515–525, 2000.

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

S. Hallgren, A. Russell, e A. Ta-Shma. Normal subgroup reconstruction and quantum computing using group representations. In **Proc. 32nd ACM Symp. on Theory of Computing**, páginas 627–635. ACM, 2000.

B. Höfling. Efficient multiplication algorithms for finite polycyclic groups, 2007. Submitted. `www-public.tu-bs.de/ bhoeflin/preprints/collect.pdf`.

D. F. Holt, B. Eick, e E. A. O'Brien. **Handbook of Group Computational Theory**. Discret Mathematics and Its Applications. Chapman&Hall/CRC, Boca Raton, 2005.

G. Ivanyos, F. Magniez, e M. Santha. Efficient quantum algorithms for some instances of the non-abelian hidden subgroup problem. **International Journal of Foundations of Computer Science**, 14(5):723–739, 2003.

G. Ivanyos, F. Magniez, e M. Santha. An efficient quantum algorithm for the hidden subgroup problem in nil-2 groups. **arXiv:quant-ph/0707.1260v1**, 2007a.

G. Ivanyos, L. Sanselme, e M. Santha. An efficient quantum algorithm for the hidden subgroup problem in extraspecial groups. In **Proc. of STACS'07**, 2007b.

R. Jozsa. Quantum algorithms and the fourier transform. **ArXiv:quant-ph/9707033**, 1997.

S. Khot. Hardness of approximating the shortest vector problem in lattices. **Journal of the ACM**, 52(5):789–808, 2005.

A. Y. Kitaev. Quantum measurements and the abelian stabilizer problem. **ArXiv:quant-ph/9511026**, 1995.

Charles Van Loan. **Computational frameworks for the fast Fourier transform**. Society for Industrial and Applied Mathematics, Philadelphia, PA, USA, 1992. ISBN 0-89871-285-8.

C. Lomont. The hidden subgroup problem - review and open problems. **ArXiv:quant-ph/0411037**, 2004.

E. M. Luks. Computing in solvable matrix groups. In **IEEE Symposium on Foundations of Computer Science**, páginas 111–120, 1992. URL `citeseer.ist.psu.edu/luks92computing.html`.

F. L. Marquezino. A transformada de fourier quântica aproximada e sua simulação. Dissertação de Mestrado, Laboratório Nacional de Computação Científica - LNCC, 2006.

C. Moore, D. N. Rockmore A. Russell, e L. J. Shulman. The power of basis selection in Fourier sampling: hidden subgroup problems in affine groups. In

Proc. of the 15th Ann ACM-SIAM Symp. on Discrete Algorithms, páginas 1113–1122, 2004.

G. E. Moore. Cramming more components onto integrated circuits. **Electronics**, 38(8), April 1965.

M. Mosca. **Quantum Computer Algorithms**. Tese de Doutorado, University of Oxford, 1999.

M. Mosca e A. Ekert. The hidden subgroup problem and eigenvalue estimation on a quantum computer. In **Proc. of the 1st NASA International Conference on Quantum Computing and Quantum Communication**, number 1509, Palm Springs, 1999. Lecture Notes in Computer Science.

M. A. Nielsen e I. L. Chuang. **Quantum Computation and Quantum Information**. Cambridge University Press, 2003.

M. Puschel, M. Rotteler, e T. Beth. Fast quantum Fourier transforms for a class of non-abelian groups. In **Proc. 13th AAECC**, volume 1719, páginas 148–159, 1999.

D. Shanks. Five number-theoretic algorithms. In **Proc. 2nd Manitoba Conference on Numerical Math ematics**, páginas 51–70, 1972.

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.

D. R. Simon. On the power of quantum computation. **SIAM Journal on Computing**, 26(5):1474–1483, 1997.

K. Spindler. **Abstract Algebra with Aplications**, volume 1. Marcel Dekker, INC, New York, 1994.

A. S. Tanenbaum. **Modern operating systems**. Segunda edição, 2001. ISBN 0-13-031358-0.

A. M. Turing. On computable number with an application to the **Entscheidugsproblem**. **Proc. Amer. Math. Soc.**, 42(2):230–265, 1936. URL `http://www.abelard.org/turpap2/tp2-ie.asp`.

C. v. de Woestijne. Deterministic equation solving over finite fields. In **ISSAC '05: Proceedings of the 2005 international symposium on Symbolic and algebraic computation**, páginas 348–353, New York, NY, USA, 2005. ACM. ISBN 1-59593-095-7.

E. Warning. Bemerkung zur vorstehenden arbeit von herr chevalley. In **Abhand. Math. Sem. Univ. Hamburg**, páginas 11:76–83, 1936.

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.