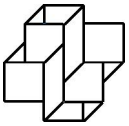


Laboratório Nacional de Computação Científica

Programa de Pós Graduação em Modelagem Computacional

Algoritmos Quânticos para o Problema do Subgrupo Oculto não Abeliano

Por

Carlos Magno Martins Cosme

PETRÓPOLIS, RJ - BRASIL

MARÇO DE 2008

ALGORITMOS QUÂNTICOS PARA O PROBLEMA DO SUBGRUPO OCULTO NÃO ABELIANO

Carlos Magno Martins Cosme

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

Aprovada por:

Prof. Renato Portugal, D.Sc
(Presidente)

Prof. Paulo César Marques Vieira, D.Sc.

Prof. Gilson Antonio Giraldi, D.Sc.

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

Prof. Carlile Lavor, D.Sc.

PETRÓPOLIS, RJ - BRASIL
MARÇO DE 2008

Cosme, Carlos Magno Martins

C384a Algoritmos quânticos para o problema do subgrupo oculto não abeliano / Carlos Magno Martins Cosme. Petrópolis, RJ. : Laboratório Nacional de Computação Científica, 2008.

xv, 98 p. : il.; 29 cm

Orientador: Renato Portugal

Tese (D.Sc.) – Laboratório Nacional de Computação Científica, 2008.

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

CDD 004.1

Não me perguntem o que eu farei de agora em diante. Ainda não decidi o que vou ser quando crescer.

À minha família: meu pai Caluca, minha mãe Helena e meus irmãos Gegê e Ulisses.

Os Amo.

Agradecimentos

A Deus, pois eu nada seria sem a força que dele recebo.

Aos meus pais, Carlos e Helena. É por causa deles que pude chegar aqui.

Aos amigos, que durante minha caminhada sempre me encorajaram nos momentos de dificuldade, me alegraram nos momentos de tristeza e dividiram comigo os muitos momentos de alegria.

A todos os professores com os quais tive o privilégio de trabalhar durante esses anos de minha vida acadêmica.

Por fim, gostaria de agradecer a Renato Portugal, que ao longo dos anos desse doutorado foi sempre mais que um orientador, foi sempre um grande amigo. Que soube cobrar o que deveria ser cobrado, reconhecer o meu esforço, valorizar as nossas conquistas e que depositou em mim a confiança que, em certos momentos, até mesmo eu não depositava.

A todos meu muito obrigado.

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

ALGORITMOS QUÂNTICOS PARA O PROBLEMA DO SUBGRUPO OCULTO NÃO ABELIANO

Carlos Magno Martins Cosme

Março , 2008

Orientador: Renato Portugal, D.Sc

Neste trabalho apresentamos um algoritmo quântico eficiente para o Problema do Subgrupos Oculto (PSO) no produto semidireto $\mathbb{Z}_{p^r} \rtimes_\phi \mathbb{Z}_{p^s}$, onde p é qualquer número primo ímpar, r e s são inteiros positivos e o homomorfismo ϕ é dado por uma raiz $tp^{r-s+l}+1$ para a qual $r \geq 2s-l$. Como conseqüência, podemos resolver eficientemente o PSO também no grupo $\mathbb{Z}_N \rtimes_\phi \mathbb{Z}_{p^s}$, onde o inteiro N possui uma especial fatoração prima.

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

QUANTUM ALGORITHMS FOR THE NON ABELIAN HIDDEN SUBGROUP PROBLEM

Carlos Magno Martins Cosme

March, 2008

Advisor: Renato Portugal, D.Sc

We present an efficient quantum algorithm for the Hidden Subgroup Problem (HSP) on the semidirect product of cyclic groups $\mathbb{Z}_{p^r} \rtimes_\phi \mathbb{Z}_{p^s}$, where p is any odd prime number, r and s are positives integers and the homomorphism ϕ is given by the root $tp^{r-s+l}+1$ such that $r \geq 2s-l$. As a consequence we can solve efficiently de HSP on the group $\mathbb{Z}_N \rtimes_\phi \mathbb{Z}_{p^s}$, where N has a special prime factorization.

Sumário

Lista de Figuras

Figura

Lista de Algoritmos

Algoritmo

Lista de Tabelas

Tabela

Lista de Símbolos e Abreviaturas

PSO : Problema do Subgrupo Oculto.

HSP : Hidden Subgroup Problem.

TFQ : Transformada de Fourier Quântica.

MAF : Método de Amostragem de Fourier.

ω_N : N-ésima raiz da unidade.

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

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

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

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

G' : Subgrupo dos comutadores de G.

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

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

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

$|G|$: Ordem do grupo G.

$|g|$: Ordem do elemento g.

$H \leq G$: H é subgrupo de G.

$H \lhd G$: H é subgrupo normal de G.

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

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

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

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

$j \oplus k$: Soma binária de j e k.

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

poli(n) : Polinômio na indeterminada n.

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

log : Logaritmo de base 2.

$a \mid b$: a divide b.

$a \nmid b$: a não divide b.

Capítulo 1

Introdução

No início da década de 80, quando Feynman (1982, 1985) perguntava à comunidade científica se seria possível construir um computador baseado nos princípios da mecânica quântica, eram lançadas as sementes da área do conhecimento hoje chamada Computação Quântica. Um tal computador poderia simular eficientemente os princípios da Mecânica Quântica? Esse era outro questionamento feito por Feynman, tendo em vista que os computadores clássicos não eram (nem são) capazes. Deutsch (1985) foi um pouco além e estendeu a questão: um computador quântico poderia resolver algum problema mais eficientemente que um computador clássico? A resposta a essa pergunta é afirmativa e dada pelo próprio Deutsch, quando demonstrou que em um computador quântico basta uma chamada a uma função $f : \{0,1\} \rightarrow \{0,1\}$ para decidir se esta é ou não balanceada[1] , enquanto em um computador clássico determinístico são necessárias duas chamadas. Foi também neste trabalho que Deutsch apresentou o primeiro modelo quântico completo de computação. Na seqüência, com os trabalhos de Deutsch (1989); Deutsch e Jozsa (1992) e Simon (1994, 1997) a Computação Quântica toma contornos cada vez mais formais e avança na solução de outros problemas, sempre apresentando ganho de eficiência em relação aos algoritmos clássicos conhecidos.

Mas o grande impulso da área surge com o Algoritmo de Shor para fatoração prima, Shor (1994, 1997). Este trabalho foi o divisor de águas para a Computação

[1] f é balanceada se $f(0) \neq f(1)$.

Quântica. Pesquisadores de várias áreas agora se juntavam para o desenvolvimento desse novo e promisor campo do conhecimento. De um lado buscava-se criar o hardware de um computador quântico que possibilitasse realizar a computação em si. Do outro, se tentava obter novos algoritmos quânticos que pudessem apresentar o mesmo, surpreendente, ganho de eficiência obtido pelo Algoritmo de Shor.

A busca pela construção do *hardware* do computador quântico tem se mostrado até hoje uma árdua tarefa e desafia, principalmente, os físicos. No tocante à busca de novos algoritmos, o desenvolvimento tem sido mais profícuo. Depois do Algoritmo de Shor, o Algoritmo de Grover obteve um ganho de eficiência quadrático sobre o melhor algoritmo clássico conhecido, Grover (1996, 1997). Neste impulso, pesquisadores de outras áreas buscaram se envolver com a pesquisa em Computação Quântica. A Criptografia é uma dessas áreas e neste caso há um claro apelo para seu envolvimento, pois um dos métodos de criptografia mais difundidos na atualidade é o método RSA, Rivest et al. (1978), que pode ser quebrado por um computador quântico. De fato, este método de criptografia está baseado na dificuldade de se resolver o problema da fatoração prima em um computador clássico. Mas esse dificuldade é pronta e eficientemente eliminada por um computador quântico através do Algoritmo de Shor, colocando em cheque a segurança do sistema criptográfico. Surge aí o ramo da Computação Quântica chamado Criptografia Quântica, que busca a construção de métodos criptográficos baseados nas leis da Mecânica Quântica.

Podemos citar ainda outras áreas como a Teoria de Jogos Quânticos, Abreu (2005), os Caminhos Aleatórios Quânticos, Oliveira (2007), Teoria da Informação Quântica, Souza (2007), Códigos Corretores de Erro, Nielsen e Chuang (2003), que têm se desenvolvido fortemente nos últimos anos. Vê-se que o campo de pesquisa em Computação Quântica se solidifica cada vez mais.

É nesse ambiente, na construção desse novo modelo de computação, principalmente no que diz respeito aos algoritmos quânticos, que temos dedicado esforço e tentado contribuir com nosso trabalho de tese. Compreendemos que, mesmo

nos restringindo ao problema que abordamos, trata-se de um grande desafio e que certamente ainda irá demandar de muito mais pesquisa e trabalho.

Tratando especificamente de algoritmos quânticos, ambiente onde se insere essa tese, há um formalismo unificador para muitos dos algoritmos conhecidos. De fato, muitos desses como o caso dos algoritmos de Shor e de Simon, podem ser vistos como casos particulares de algoritmos quânticos para a solução do Problema do Subgrupo Oculto - PSO (do inglês *Hidden Subgroup Problem - HSP*). Podemos descrever o PSO da seguinte maneira. Dados um grupo G, um conjunto X, ambos finitos, e uma função $f : G \to X$ tal que $f(a) = f(b)$ se, e somente se, a e b pertençam à mesma classe lateral de um subgrupo H de G, o PSO consiste em determinar um conjunto de geradores para H a partir de informações obtidas de f. Dizemos que H é oculto por f e a função f é chamada função separadora de classes laterais.

Um algoritmo para a solução do PSO será considerado eficiente se sua complexidade computacional for $O(\text{poli}(\log|G|))$, onde $\text{poli}(\log|G|)$ é um polinômio em $\log|G|$. Não é conhecido nenhum algoritmo clássico eficiente para a solução do PSO. Entretanto, por meio de algoritmos quânticos, tem-se conseguido resolver, eficientemente, o problema em classes de grupos particulares. O caso mais importante completamente resolvido até agora é o PSO abeliano, isto é, o PSO para um grupo G é abeliano. Neste caso, há um algoritmo quântico eficiente para sua solução, Mosca e Ekert (1999); Kitaev (1995); Lomont (2004).

Atualmente, a atenção está voltada para o PSO em grupos não abelianos, Ivanyos et al. (2003, 2007b,a); Bacon et al. (2005); Inui e Le Gall (2005); Chi et al. (2006); Cosme e Portugal (2007b,a), onde encontram-se os dois casos mais desafiadores e interessantes do PSO, a saber, o PSO no grupo simétrico, Moore et al. (2005), e no grupo diedral, Kuperberg (2005). O interesse nesses dois problemas explica-se pois, caso seja possível resolvê-los eficientemente, outros dois problemas de grande interesse, o Problema do Isomorfismo de Grafos e o Problema do Menor Vetor de um Reticulado, teriam soluções eficientes, Ettinger e Høyer (1999); Regev

(2004a). Infelizmente, embora grande esforço esteja sendo empregado na busca de suas soluções, estes casos do PSO continuam em aberto e desafiando os pesquisadores. Os sucessos que se tem obtido acontecem em grupos não abelianos que sejam, em certo sentido, "quase" abelianos. Nestes casos, muitas vezes, pode-se reduzir o PSO não abeliano a instâncias do PSO abeliano.

Se de início a relação entre o PSO e os problemas da fatoração prima, do isomorfismo de grafos e do menor vetor de um reticulado foi a principal responsável pelo grande interesse na busca de solução para o PSO, hoje, por si só, ele representa um dos problemas mais estudados e desafiadores da Computação Quântica, envolvendo físicos, matemáticos, cientistas da computação, dentre outros, num trabalho multidisciplinar que está longe de terminar.

Seguindo a linha dos resultados mais recentes da área, nessa tese apresentamos uma solução eficiente para o PSO no grupo não abeliano $\mathbb{Z}_{p^r} \rtimes_\phi \mathbb{Z}_{p^s}$, produto semidireto dos grupos cíclicos $\mathbb{Z}_{p^r}$ e $\mathbb{Z}_{p^s}$, onde p é qualquer número primo ímpar e r e s são inteiros positivos tais que $r \geq 2s - l$ e o inteiro l é dado pela raiz $tp^{r-s+l} + 1$ que define o homomorfismo ϕ, Teorema 4.4.1, sendo este o principal resultado da tese. Ele generaliza os resultados apresentados em Inui e Le Gall (2005) e Cosme e Portugal (2007b) e representa mais um avanço na busca do incremento do número de grupos onde o PSO é eficientemente resolvido. Em nossa abordagem do problema, o conhecimento da estrutura dos subgrupos é de fundamental importância para o algoritmo. Desta forma, parte do nosso esforço foi dedicado a obter uma completa classificação dos subgrupos (Teorema 3.2.1) e entender certas propriedades dos mesmos, como normalidade e o comportamento das suas classes laterais.

Há outros três componentes importantes em nossa análise, além da classificação dos subgrupos: (1) o algoritmo para o PSO abeliano, Mosca e Ekert (1999); Lomont (2004); (2) o algoritmo para o PSO quando o grupo é solúvel e o subgrupo oculto é normal, Ivanyos et al. (2003); (3) a transformada de Fourier abeliana, Kitaev (1995); Lomont (2004). Nosso método utiliza a estrutura dos

subgrupos, combinada a estes outros três elementos. De início, reduzindo parte do problema ao caso abeliano através de (1) e (2). Por fim, através de um algoritmo direto (Algoritmo 4.2.1), onde se emprega (3) e onde tais reduções não são mais possíveis.

A tese se desenvolve da seguinte maneira. No Capítulo 2, fazemos uma rápida revisão dos conceitos básicos da Computação Quântica que serão necessários para o desenvolvimento do trabalho. Também fazemos um apanhado histórico do problema através de uma revisão bibliográfica. Por fim, abordamos o formalismo quântico que envolve o PSO.

Nos Capítulos 3, 4, 5 e 6, apresentamos nossas contribuições. No primeiro deles é definido o grupo onde iremos atacar o problema, qual seja, o produto semidireto $\mathbb{Z}_{p^r} \rtimes_\phi \mathbb{Z}_{p^s}$ sob algumas restrições em r, s e ϕ. No Teorema 3.2.1, apresentamos a classificação dos subgrupos do grupo abordado, peça chave para a solução do PSO. Na seqüência, demonstramos uma série de propriedades de tais subgrupos visando a implementação do algoritmo quântico.

O algoritmo quântico para a solução do PSO em $\mathbb{Z}_{p^r} \rtimes_\phi \mathbb{Z}_{p^s}$ é apresentado no Capítulo 4. O algoritmo é composto por uma série de reduções à instâncias já resolvidas do PSO, combinadas ao Algoritmo 4.2.1 que deve ser utilizado pois somente as reduções não são suficientes para resolver o problema.

Como conseqüência da solução obtida para o PSO no grupo $\mathbb{Z}_{p^r} \rtimes_\phi \mathbb{Z}_{p^s}$ podemos atacar o PSO também no grupo $\mathbb{Z}_N \rtimes_\phi \mathbb{Z}_{p^s}$. Isso é apresentado no Capítulo 5.

Por fim, no Capítulo 6, apresentamos a estrutura geral do grupo $\mathbb{Z}_{p^r} \rtimes_\phi \mathbb{Z}_{p^s}$, conjecturando sobre a classificação de seus subgrupos, e fazemos alguns apontamentos de uma possível solução do PSO.

Capítulo 2

Computação Quântica e o Problema do Subgrupo Oculto

Pretendemos fazer na primeira parte deste capítulo um apanhado geral dos conceitos básicos sobre computação quântica que serão necessários para o desenvolvimento da tese. Portanto, não podemos escapar de falar dos postulados da mecânica quântica. Não nos ateremos aos detalhes dos conceitos aqui abordados, nos limitando a uma exposição bem sucinta dos mesmos. Julgamos que a literatura da área é suficientemente difundida e abrangente neste aspecto. Para uma descrição detalhada destes conceitos remetemos o leitor a referência Nielsen e Chuang (2003) e às inúmeras outras referências lá contidas. Para abordagens mais básicas sugerimos o trabalho de Lomont (2004), a dissertação de mestrado de Marquezino (2006) e o trabalho de Batty et al. (2003). A descrição que faremos segue basicamente essas quatro referências. Muitos conceitos de Álgebra Linear são necessários. Nielsen e Chuang (2003) fazem uma boa revisão destes conceitos. Uma outra referência para este assunto é o livro de Hoffman e Kunze (1971).

Na segunda seção discutiremos sucintamente os circuitos quânticos e as portas quânticas (operadores unitários), introduzindo as portas importantes para o nosso trabalho, caso das portas controladas e da Transformada de Fourier, bem como faremos uma breve discussão sobre implementação eficiente das portas quânticas.

Na Seção 2.3 nos empenhamos em descrever o Problema do Subgrupo Oculto,

apresentando-o formalmente situando-o historicamente no desenvolvimento da computação quântica, mostrando os casos onde ele já se encontra resolvido e apontando para onde caminha a pesquisa mais recente da área. Encerramos o capítulo com a apresentação de alguns resultados gerais, embora elementares, sobre o problema e o formalismo quântico para o PSO.

2.1 Os Postulados da Mecânica Quântica

Os quatro postulados da mecânica quântica nos fornecem um modelo para os sistemas quânticos isolados, eles são a abstração matemática de tais sistemas quânticos. Na seqüência os apresentaremos.

Postulado 1 (Espaço de Estados) Associado a qualquer sistema quântico isolado há um espaço vetorial complexo com produto interno, um espaço de Hilbert, chamado espaço de estados do sistema. O sistema é completamente descrito por um vetor unitário do espaço de estados que chamaremos vetor de estado.

Lidaremos apenas com espaços de estado de dimensão finita, logo podemos considerar que nosso espaço de estados é $\mathbb{C}^N$.

Assim como a computação clássica[1] tem no *bit* sua unidade básica de armazenamento de informação, na computação quântica há o *bit* quântico, abreviado aqui para *qbit*, como unidade básica de armazenamento de informação. Formalmente um *qbit* é um vetor de estado do espaço de estados $\mathbb{C}^2$. Para este espaço vetorial fixamos a base ortonormal canônica, aqui denotada por

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \text{ e } |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

onde o símbolo $|\cdot\rangle$, chamado *ket*, faz parte da notação de Dirac e denota sempre um vetor coluna. Os *qbits* $|0\rangle$ e $|1\rangle$ são os equivalentes quânticos dos *bits* clássicos 0 e 1. A grande diferença entre o *bit* e o *qbit* é que enquanto o primeiro sempre se encontra

[1] Convencionaremos chamar a computação atual de computação clássica.

ou no estado 0 ou no estado 1, o segundo pode assumir qualquer combinação do tipo $\alpha|0\rangle + \beta|1\rangle$, onde $\alpha, \beta \in \mathbb{C}$ e satisfazem a $|\alpha|^2 + |\beta|^2 = 1$. A base $\{|0\rangle, |1\rangle\}$ de $\mathbb{C}^2$ é chamada base computacional de $\mathbb{C}^2$. De maneira análoga, a base ortonormal canônica de $\mathbb{C}^N$ é chamada base computacional de $\mathbb{C}^N$. Na notação de Dirac esta base é denotada por

$$|0\rangle = (1, 0, \cdots, 0)^T,\ |1\rangle = (0, 1, 0 \cdots, 0)^T, \cdots, |N-1\rangle = (0, \cdots, 0, 1)^T.$$

Nesta base, um vetor de estado $|\psi\rangle$ do sistema é dado por $|\psi\rangle = \sum_{j=0}^{N-1} a_j |j\rangle$, onde $a_j \in \mathbb{C}$ para todo j. Os coeficientes a_i são chamados amplitudes e, sendo $|\psi\rangle$ um vetor de estado, satisfazem $\sum_{j=0}^{N-1} |a_j|^2 = 1$. Diz-se que o estado $|\psi\rangle$ está em uma superposição dos estados da base computacional.

Postulado 2 (Evolução dos Estados) A evolução de um sistema quântico fechado[2] é descrita por um operador unitário. Isto é, o estado $|\psi\rangle$ do sistema no instante t_1 está relacionado ao estado $|\psi'\rangle$ no instante t_2 por um operador unitário U que depende apenas de t_1 e t_2 e tal que

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

Como todo operador unitário é invertível, segue do Postulado 2 que é sempre possível recuperar o estado inicial do sistema quântico através do operador U^{-1}. Isso confere à computação quântica seu caráter de computação reversível, Toffoli (1980a,b). Além disso, os operadores unitários serão os elementos responsáveis pela computação em si, eles serão as portas lógicas da computação quântica. Na Seção 2.3 retomaremos essa discussão.

Da notação de Dirac temos que $\langle\psi|$ denota o vetor transposto conjugado de $|\psi\rangle$, onde o símbolo $\langle\cdot|$ é chamado *bra*. Dado um operador U que atua sobre um espaço vetorial V e vetores $|\psi\rangle, |\psi'\rangle \in V$, $\langle\psi|U|\psi'\rangle$ denota o produto interno de $|\psi\rangle$ por $U|\psi'\rangle$. $U^\dagger$ denota o operador adjunto de U.

[2] Um sistema quântico fechado é aquele que não iterage com nenhum outro sistema físico.

Postulado 3 (Medição dos Estados) Uma medição quântica é descrita por um operador Hermitiano M, chamado observável, agindo sobre o espaço de estados do sistema a ser medido. Por ser normal o observável possui uma decomposição espectral

$$M = \sum_m mP_m,$$

onde P_m é o projetor sobre o auto espaço de M cujo autovalor é m. Os possíveis resultados da medida são os autovalores de M. Se o estado do sistema é $|\psi\rangle$ imediatamente antes da medição, então a probabilidade que o resultado da medida seja m é dada por

$$p(m) = \langle\psi| P_m |\psi\rangle$$

e o estado do sistema após a medição é

$$|\psi'\rangle = \frac{P_m |\psi\rangle}{\sqrt{p(m)}}.$$

O tipo de medida definida no Postulado 3 é chamada de medida projetiva e é o tipo de medida que utilizaremos na tese. Devemos dizer que há outras maneiras de enunciarmos o Postulado da Medição de Estados que são equivalentes a esta, Nielsen e Chuang (2003).

Alternativamente à maneira como fora introduzido o processo de medição no Postulado 3, é comum na literatura simplesmente listar um conjunto completo de projetores ortogonais P_m satisfazendo as relações[3]

$$\sum_m mP_m \text{ e } P_m P_{m'} = \delta_{mm'} P_m.$$

O observável correspondente é dado por

$$M = \sum_m mP_m.$$

[3] $\delta_{mm'}$ denota a função delta de Dirac.

Um caso particular desta maneira de descrever uma medição é chamada de 'medida em uma base $\mathcal{B} = \{|m\rangle\}$'. Nesta medição os projetores da medida projetiva são definidos por $P_m = |m\rangle \langle m|$[4] . Quando $\mathcal{B}$ é a base computacional, esse processo de medida é chamado medida na base computacional. Se lidamos com um sistema quântico cuja base computacional é $\{|0\rangle, \cdots, |N-1\rangle\}$ e

$$|\psi\rangle = \sum_{i=0}^{N-1} a_i |i\rangle$$

é um vetor de estado desse sistema, ao medirmos $|\psi\rangle$ na base computacional produziremos o estado $|j\rangle$ com probabilidade $|a_j|^2$. Logo, o quadrado do módulo da amplitude de um vetor da base computacional representa a probabilidade desse mesmo vetor ser observado pela medida na base computacional.

Postulado 4 (Sistemas Compostos) O espaço de estados de um sistema quântico composto é o produto tensorial dos espaços de estados dos sub-sistemas quânticos que o compõem. Numerando de 1 até n tais sub-sistemas e supondo que o sub-sistema i esteja no estado $|\psi_i\rangle$, temos que o sistema composto está no estado

$$|\psi_1\rangle \otimes \cdots \otimes |\psi_n\rangle .$$

Geralmente nós utilizamos a notação abreviada $|\psi\psi'\rangle$ ou $|\psi\rangle |\psi'\rangle$ para o produto tensorial $|\psi\rangle \otimes |\psi'\rangle$, desta forma o estado do sistema composto passa a ser denotado por $|\psi_1 \cdots \psi_n\rangle$ ou ainda $|\psi_1\rangle \cdots |\psi_n\rangle$.

Este postulado nos permite concatenar *qbits*, como fazemos com *bits* clássicos, para obtenção de sistemas maiores. Considere o espaço composto por dois sub-sistemas de um *qbit*, um sistema quântico de dois *qbits*. Seu espaço de estados é $\mathbb{C}^2 \otimes \mathbb{C}^2$, um espaço complexo 4-dimensional cuja base computacional é formada pelos vetores $|00\rangle = |0\rangle \otimes |0\rangle = (1,0,0,0)^T$, $|01\rangle = |0\rangle \otimes |1\rangle = (0,1,0,0)^T$, $|10\rangle = |1\rangle \otimes |0\rangle = (0,0,1,0)^T$ e $|11\rangle = |1\rangle \otimes |1\rangle = (0,0,0,1)^T$. Identificando os rótu-

[4] Dados vetores $|\psi\rangle$ e $|\psi'\rangle$, $|\psi\rangle \langle\psi'|$ denota o produto da matriz coluna $|\psi\rangle$ pela matriz linha $\langle\psi'|$.

los 00, 01, 10 e 11 como números binários, é imediata a correspondência com seus equivalentes números decimais, e assim, temos $|00\rangle = |0\rangle$, $|01\rangle = |1\rangle$, $|10\rangle = |2\rangle$ e $|11\rangle = |3\rangle$, por onde recuperamos a notação fixada anteriormente para a base computacional. Pode-se generalizar essa idéia para n sistemas de um *qbit*, produzindo um sistema composto de n *qbits* cujo espaço de estados é $\underbrace{\mathbb{C}^2 \otimes \cdots \otimes \mathbb{C}^2}_{n \text{ vezes}}$, escrito abreviadamente como $\mathbb{C}^{2^{\otimes n}}$, um espaço 2^n-dimensional cuja base computacional é $\{|0\rangle = |0\cdots 0\rangle, \cdots, |2^n - 1\rangle = |1\cdots 1\rangle\}$.

2.2 Portas e Circuitos Quânticos

Um circuito quântico é um modelo teórico para a descrição do processo de computação. Assim como um circuito da computação clássica, é constituído por fios e portas lógicas, neste caso, portas lógicas quânticas. Os fios servem para carregar a informação durante o processo de computação. As portas servem para, efetivamente, realizar a computação. Os circuitos quânticos são acíclicos, isto é, não são permitidos laços.

Uma importante restrição sobre as portas lógicas quânticas é fornecida pelo Postulado da Evolução dos Estados. Por ele, qualquer porta deverá ser descrita como um operador unitário no espaço de estados do computador quântico. No que segue, iniciando com as portas de um *qbit*, faremos um apanhado das portas que utilizaremos no decorrer da tese. O que segue é baseado nas referências Nielsen e Chuang (2003); Portugal et al. (2006); Marquezino (2006).

A primeira porta de 1 *qbit* que apresentamos é a porta NOT quântica, denotada por X, equivalente quântica da porta NOT clássica. Sua atuação na base computacional é a seguinte: $|0\rangle \mapsto |1\rangle$ e $|1\rangle \mapsto |0\rangle$, ou seja, $|j\rangle \mapsto |1 \oplus j\rangle$, onde $\oplus$ denota a soma binária. Sua descrição como operador unitário é dada pela matriz

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

E sua descrição como um circuito quântico atuando num *qbit* geral $|\psi\rangle = a\,|0\rangle + b\,|1\rangle$

é[5]

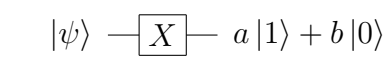


Figura 2.1: Circuito da porta X.

Três outras portas de um *qbit* muito importantes para a computação quântica são a porta Hadamard, denotada por H, a porta fase, denotada por S e a porta $\pi/8$, denotada por T. Suas matrizes são dadas abaixo.

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix},\ S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix},\ T = e^{\pi i/8} \begin{pmatrix} e^{-\pi i/8} & 0 \\ 0 & e^{\pi i/8} \end{pmatrix}$$

Passando a portas de mais de um *qbit*, devemos dedicar atenção à porta NOT quântica controlada, denotada por CNOT. Trata-se de uma porta de dois *qbits*, sendo um o *qbit* de controle e o outro o *qbit* alvo. Como uma porta controlada clássica, o *qbit* alvo só será afetado pela porta NOT se o *qbit* de controle estiver no estado $|1\rangle$. Sua atuação na base computacional é $|j_1\rangle\,|j_2\rangle \mapsto |j_1\rangle\,X^{j_1}\,|j_2\rangle = |j_1\rangle\,|j_1 \oplus j_2\rangle$. Na base computacional do espaço de estados $\mathbb{C}^4$, a sua matriz é dada por

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

Seu circuito é exibido na Figura 2.2

Avançando e generalizando a porta CNOT, suponha que U seja uma porta de n *qbits*, isto é, um operador unitário atuando em $\mathbb{C}^{2^{\otimes n}}$. A porta U controlada, denotada por $C(U)$, é a operação sobre $n+1$ *qbits* definida por sua atuação na base computacional: $|j_1\rangle\,|k\rangle \mapsto |j_1\rangle\,U^{j_1}\,|k\rangle$, onde $|j_1\rangle \in \{|0\rangle, |1\rangle\}$ e $|k\rangle \in \{|0\rangle, \cdots, |2^n - 1\rangle\}$. Seu circuito é mostrado na Figura 2.3.

[5] Qualquer circuito para computação de uma porta de um *qbit* será descrito de maneira similar ao circuito da Figura 2.1, por isso os omitiremos.

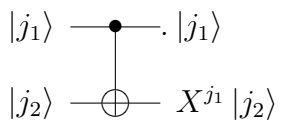


Figura 2.2: Circuito da porta CNOT. A linha de cima representa o *qbit* de controle e o de baixo o *qbit* alvo.

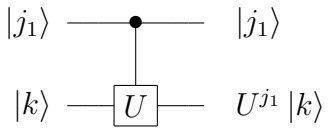
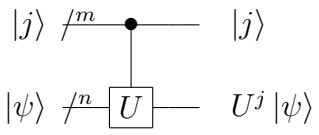


Figura 2.3: Circuito da porta U controlada.

Por fim, seja um operador unitário U de n *qbits* como anteriormente e considere um espaço de estados de m *qbits*. Podemos definir um operador $\tilde{C}(U)$ sobre $m+n$ *qbits* da seguinte forma: Dados $|j\rangle \in \{|0\rangle, \cdots, |2^m-1\rangle\}$ e $|k\rangle \in \{|0\rangle, \cdots, |2^n-1\rangle\}$, a atuação de $\tilde{C}(U)$ é dada por

$$|j\rangle|k\rangle \mapsto |j\rangle U^j |k\rangle . \tag{2.1}$$

Esta porta, pode ser vista como uma porta $C(U)$ generalizada, onde seu *qbit* de controle é substituído por um estado de controle. No circuito abaixo vemos sua representação esquemática.



A representação gráfica é a mesma de $C(U)$, porém não há perigo de confusão pois o primeiro registrador[6] tem mais do que um *qbit*. É interessante notar que a porta $\tilde{C}(U)$ pode ser decomposta como uma composição de portas $C(U)$. Para tanto, considere a representação binária do registrador de controle, digamos $|j\rangle =$

[6] A palavra registrador é usada como sinônimo para um vetor de estado.

$|j_1\rangle \cdots |j_m\rangle$. O circuito da Figura 2.4 mostra como fazer tal decomposição, Portugal et al. (2006).

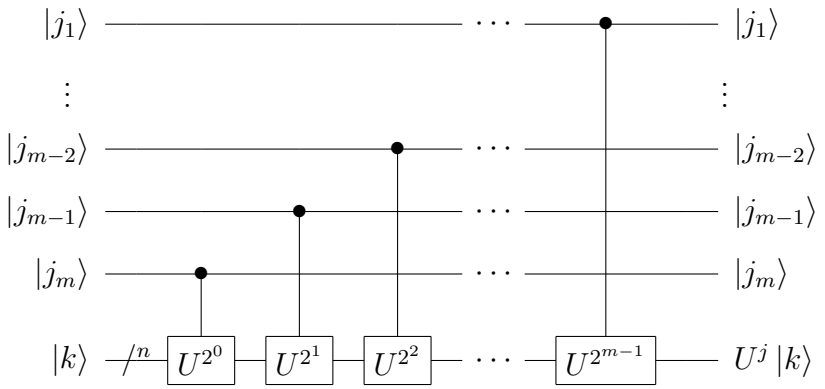


Figura 2.4: Circuito decompondo $\tilde{C}(U)$ através da porta controlada $C(U)$.

Encerrando nossa discussão sobre circuitos quânticos, apresentamos a representação esquemática de um operador de medida. Em qualquer caso, seja a medida efetuada na base computacional ou não, sua representação esquemática é a que segue abaixo.

A linha dupla que segue após o símbolo de medida significa que a informação depois de medida passa a ser conhecida, isto é, passa a ser informação clássica.

De acordo com o segundo postulado, operadores lineares unitários são potenciais algoritmos quânticos. No entanto, nem todo operador unitário pode ser imediatamente implementado através de um experimento físico no laboratório, sendo necessário antes expressá-lo através de operadores mais elementares. Para tanto, é necessário eleger um tal conjunto de operadores, assim como é feito na computação clássica[7] .

O primeiro conjunto universal de operadores que se pode utilizar para tal construção é composto pelo CNOT e pelas portas unitárias de um *qbit*. Qualquer operador unitário pode ser descrito como combinação desse conjunto elementar de portas. Entretanto, há um contínuo de portas de um *qbit*. Deseja-se um conjunto

[7] Por exemplo, os operadores NOT, AND e OR formam um conjunto universal de portas lógicas para a computação clássica, Nielsen e Chuang (2003).

universal menor, preferencialmente, finito. Infelizmente tal desejo não pode ser realizado. É impossível obter um conjunto universal finito para implementar todas as portas de um *qbit* exatamente. Mas pode-se obter um conjunto universal[8] finito de portas quânticas que aproxime qualquer operador. Este conjunto universal é constituído pelas portas CNOT, Hadamard, fase e $\pi/8$. Todos estes fatos que estamos apresentando aqui estão provados em Nielsen e Chuang (2003).

Um outro aspecto importante nesta discussão é se um operador unitário qualquer pode ser eficientemente implementável nesse conjunto universal de portas. Seja U um operador unitário de n *qbits*. Diremos que U é eficientemente implementável se existir um circuito de tamanho[9] polinomial em n para a computação de U. Nem todo operador U é eficientemente implementável. Na verdade, a maioria das transformações unitárias não são eficientemente implementáveis. Mas se um operador U é eficientemente implementável, então $C(U)$ e $\tilde{C}(U)$ também o são. Além dessas, uma importante porta lógica da computação quântica, a Transformada de Fourier, também é eficientemente implementável na maioria dos casos de interesse. Na próxima seção a apresentamos.

2.2.1 A Transformada de Fourier Quântica

Não há dúvida sobre a grande importância da Transformada de Fourier Quântica - TFQ, para os algoritmos quânticos. A maior parte, senão todos, dos algoritmos quânticos que apresentam ganho exponencial em relação aos seus equivalentes clássicos utilizam a TFQ. Desta forma, ela tem sido objeto de exaustivo estudo ao longo dos anos. Simon (1997); Shor (1997, 1994); Josza (1997); Kitaev (1995); Mosca e Ekert (1999) foram alguns trabalhos que lidaram inicialmente com a TFQ. No que segue definiremos a TFQ no grupo $\mathbb{Z}_N$ dos inteiros módulo N. Mas ressaltamos que a TFQ pode ser definida em um grupo finito qualquer, Lomont (2004); Gonçalves (2005).

[8] De fato, existe não só este conjunto universal, mas este é o mais importante.

[9] O tamanho de um circuito é definido como o menor número de portas lógicas elementares necessárias para o implementar.

Definição 2.2.1 (Transformada de Fourier Quântica em $\mathbb{Z}_N$) Considere o espaço de estados cuja base computacional é $\{|0\rangle, \cdots, |N-1\rangle\}$. A TFQ é o operador linear que atua sobre este espaço de estados definido na base computacional da seguinte maneira

$$FT_N |k\rangle = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} \omega_N^{jk} |j\rangle ,$$

onde ω_N é a N-ésima raiz da unidade.

O operador FT_N é unitário e eficientemente implementável, Coppersmith (1994); Kitaev (1995). Em Portugal et al. (2006) há uma descrição bastante didática de um circuito polinomial para sua implementação.

Finalizando, deixamos registrada uma importante relação envolvendo ω_N que nos será útil.

$$\frac{1}{N} \sum_{j=0}^{N-1} \omega_N^{jk} = \begin{cases} 1 & \text{se} \quad N \mid k \\ 0 & \text{se} \quad N \nmid k \end{cases} \tag{2.2}$$

2.3 O Problema do Subgrupo Oculto

Introduzimos agora o objeto central da tese, qual seja, o **Problema do Subgrupo Oculto - PSO**. Ao longo desta seção, definiremos formalmente o PSO, apresentaremos alguns importantes problemas que estão diretamente ligados a ele, como o Problema do Isomorfismo de Grafos e o Problema do Menor Vetor em um Reticulado, bem como discutiremos os principais casos onde o PSO já se encontra resolvido e qual a fronteira onde ele ainda continua não resolvido e tem sido atacado.

O apanhado histórico que faremos nesta seção é baseado nas discussões presentes em Lomont (2004); Batty et al. (2003); Nielsen e Chuang (2003).

2.3.1 Definição e Histórico

Historicamente, o PSO surge com o objetivo de unificar uma série de problemas que a computação quântica vinha obtendo êxito em resolver, frente o insucesso da computação clássica. Cronologicamente, podemos destacar os trabalhos

de Deutsch (1985) e Deutsch e Jozsa (1992) onde são apresentados algoritmos quânticos eficientes para determinar se uma dada função é ou não balanceada - $f : \{0,1\}^n \to \{0,1\}$ é balanceada se a cardinalidade de $f^{-1}(0)$ e $f^{-1}(1)$ são iguais a 2^{n-1}. Seguindo, surge o trabalho de Simon (1997) onde o autor mostra ser possível determinar eficientemente o período de uma função periódica através de um algoritmo quântico. Após isso, avançando nas idéias presentes no trabalho de Simon, Shor (1994, 1997) apresenta seu surpreendente algoritmo para decomposição de inteiros em fatores primos e para cálculo de logaritmo discreto. Então Josza (1997), observou que todos esses problemas poderiam ser visto como casos particulares de um problema mais geral, a saber, o PSO. Vamos à definição.

Definição 2.3.1 (Problema do Subgrupo Oculto) Considere um grupo G e um conjunto X, ambos finitos[10] , e uma função $f : G \to X$ tal que exista um subgrupo H de G, para o qual $f(a) = f(b)$ se, e somente se, $aH = bH$ quaisquer que sejam $a, b \in G$, isto é, f é constante em elementos da mesma classe lateral de H em G e distinta em classes laterais distintas. O problema de determinar um conjunto de geradores para H, a partir de informações obtidas de f, é chamado o Problema do Subgrupo Oculto.

Dizemos que a função f oculta H em G, ou ainda que f separa as classes laterais de H em G. É comum encontrarmos menção na literatura à função f como função oráculo, função *black box*, função separadora de classes, etc. O subgrupo H é dito o subgrupo oculto em G por f.

Uma óbvia solução para o PSO é mostrada no Algoritmo 2.3.1. Notamos que nesta solução a função separadora de classes é invocada $|G|$ vezes.

Nós diremos que um algoritmo resolve eficientemente o PSO no grupo G se o número de operações básicas realizadas por ele, aí incluídas as consultas à função separadora de classes, e a memória por ele requerida forem limitados por algum polinômio em $\log |G|$, isto é, se a complexidade computacional do algoritmo for $O(\text{poli}(\log |G|))$. Desta forma, vemos que o Algoritmo 2.3.1 é ineficiente.

[10] Em alguns casos, G é considerado finitamente gerado.

Algoritmo 2.3.1 Um algoritmo trivial para o PSO em um grupo qualquer.

Entrada: Um conjunto de geradores de G e a função f;
Saída: O subgrupo oculto H;

1: Inicialize H como $H = \emptyset$;
2: **para** $g \in G$ **faça**
3: **se** $f(g) = f(e)$ **então**
4: $H = H \cup g$;
5: **fim se**
6: **fim para**

Não se conhece nenhum algoritmo capaz de resolver eficientemente o PSO em seu caso geral, entretanto, no formalismo quântico tem-se avançado em importantes casos particulares do problema, sendo o mais significativo desses, a solução do PSO abeliano, isto é, a solução do PSO para um grupo abeliano G. Em Mosca e Ekert (1999); Mosca (1999), os autores apresentam uma descrição de tal solução utilizando-se das idéias já presentes no trabalho de Kitaev et al. (2002), sobre o problema do cálculo da fase do autovalor de um operador[11] .

Em ambos os trabalhos é utilizado o Método de Amostragem de Fourier - MAF. Em linhas muito gerais este método de ataque ao problema consiste em inicialmente, criar uma superposição nos elementos do grupo. Utiliza-se a função separadora de classes laterais para converter a superposição inicial em uma superposição em uma das classes laterais do subgrupo oculto. Aplica-se a TFQ ao estado resultante, para que o período da função separadora de classes possa ser evidenciado, obtendo-se a informação sobre o subgrupo oculto. Por fim, uma medida deve ser realizada para que se possa ter acesso à informação sobre o subgrupo oculto.

Vale ressaltar que não é conhecido algoritmo clássico eficiente para a solução do PSO abeliano, o que confere aos resultados anteriores importância ainda maior, principalmente se levamos em conta, por exemplo, que o Algoritmo de Shor é um caso particular do PSO abeliano. Para uma descrição minuciosa e didática da solução do PSO abeliano, bem como da TFQ e do MAF, sugerimos o trabalho de Lomont (2004) e os trabalhos de Kitaev (1995); Kitaev et al. (2002); Mosca e Ekert

[11] O problema do cálculo da fase consiste em dado um operador unitário U e um de seus autovetores $|v\rangle$, estimar o valor ϕ tal que $e^{2\pi i\phi}$ seja o autovalor associado a $|v\rangle$

(1999).

Por fim, o algoritmo para o PSO abeliano utiliza-se do fato de que qualquer grupo abeliano finito se decompõe como produto direto de grupos cíclicos, cujas ordens são potências de números primos. Desta forma, é necessário que tal decomposição seja obtida de maneira eficiente. Em Cheung e Mosca (2001) os autores apresentam um algoritmo quântico eficiente para tal problema (Veja também Portugal et al. (2006).).

No que segue, apresentaremos alguns importantes problemas que se reduzem ao PSO.

Seja A um grupo cíclico aditivo, S um conjunto qualquer e $f : A \to S$. Diremos que f é periódica de período $r \in A$ se para todo $x \in A$ e $n \in \mathbb{Z}$ tivermos $f(x) = f(x + nr)$. Se $A = \langle a \rangle$, observamos que uma função f de período r oculta $H = \langle ra \rangle$ em A. Logo, o problema de determinar o período de uma função periódica é um caso particular do PSO abeliano. Devemos notar que o problema de decompor um número inteiro em seus fatores primos, se reduz ao problema de determinar o período de uma função periódica, Batty et al. (2003); Lavor et al. (2003); Portugal et al. (2006). Desta forma, o Algoritmo de Shor para fatoração é um caso particular do PSO abeliano.

Novamente seja $A = \langle a \rangle$ um grupo cíclico e $n = |A|$. Dado um elemento $b \in A$, o logaritmo discreto de b é o menor inteiro r tal que $b = a^r$ (aqui estamos usando a notação multiplicativa para os elementos de A). O problema do logaritmo discreto consiste em determinar r. Pode-se formular esse problema em termos do PSO da seguinte maneira. Seja $f : \mathbb{Z}_n^2 \to A$ dada por $f(x, y) = a^x b^{-y}$. Esta função é um homomorfismo de grupos e, portanto, f oculta seu núcleo $K = \ker f$. Resolvendo o PSO no grupo abeliano $\mathbb{Z}_n^2$ determina-se geradores para K e a partir disso r.

Além desses problemas que citamos até agora, há vários outros que se reduzem ao PSO abeliano e que, portanto, possuem uma solução eficiente através de um algoritmo quântico. A descrição desses problemas como um PSO pode ser

encontrada em Nielsen e Chuang (2003) e Batty et al. (2003).

Depois de se ter resolvido completamente o PSO abeliano, naturalmente voltou-se a atenção para o PSO em grupos não abelianos. Neste ambiente, dois casos particulares do PSO merecem destaque. O PSO no grupo simétrico S_n e o PSO no grupo diedral D_n[12] . Estes dois problemas são os mais interessantes e desafiantes casos do PSO. Muitos pesquisadores até mesmo questionam se será possível construir um algoritmo eficiente para suas soluções. De fato, não se tem conseguido avançar muito na direção das soluções, embora grande esforço esteja sendo empregado nos últimos anos. Mas por qual razão esses problemas chamam tanto a atenção? Para responder a essa pergunta, vamos definir outros dois problemas.

Dado um grafo A denotamos por $V(A)$ o seu conjunto de vértices e $E(A)$ seu conjunto de arestas. Um isomorfismo entre grafos simples A e B é uma bijeção $\phi : V(A) \to V(B)$ tal que dados $u, v \in V(A)$ a aresta $uv \in E(A)$ se, e somente se, a aresta $\phi(u)\phi(v) \in E(B)$, Butler (1991). Posto isso, definimos

Definição 2.3.2 (Problema do Isomorfismo de Grafos) Dados dois grafos A e B, com mesmo número de vértices, determinar se A e B são isomorfos.

Este problema, pertencente à classe dos problemas NP, Kitaev (1995), tem aplicações nas mais diversas áreas da ciência, despertando interesse desde a computação teórica, passando por biologia, química, entre outras, Arvind e Kurur (2006); Johannes et al. (1993). Existe uma estreita ligação entre o Problema do Isomorfismo de Grafos e o PSO no grupo S_n. Como mostrado em Ettinger e Høyer (1999); Beals (1997); Lomont (2004), uma solução eficiente para o PSO em S_n implica em uma solução eficiente para o Problema do Isomorfismo de Grafos (Veja também Dalcumune (2008)).

O PSO em D_n se relaciona com o Problema do Menor Vetor em um Reticulado. Vamos defini-lo apropriadamente. Um reticulado n-dimensional é um conjunto de vetores $R = \{\sum_{i=1}^{n} a_i \mathbf{b}_i;\ a_i \in \mathbb{Z}\}$, onde $\mathbf{b}_1, \cdots, \mathbf{b}_n \in \mathbb{R}^m$ é um con-

[12] O grupo simétrico S_n é o grupo das permutações de n elementos. Enquanto o grupo D_n é o subgrupo de S_n dado por $D_n = \langle a, b \in S_n;\ a^2 = b^n = e,\ (n > 2),\ ab = b^{-1}a \rangle$ (veja Hernstein (1970))

junto linearmente independente de vetores, chamado uma base do reticulado, Khot (2005).

Definição 2.3.3 (Problema do Menor Vetor em um Reticulado) Dado um reticulado R como definido anteriormente, o Problema do Menor Vetor em um Reticulado consiste em se determinar o menor vetor pertencente a R.

Dada a dificuldade de resolver tal problema, Ajtai (1996, 1998); Khot (2005), vários sistemas criptográficos foram construídos de maneira que suas chaves criptográficas são obtidas através da solução do mesmo, Ajtai e Dwork (1997); Regev (2003), conferindo alta confiabilidade aos sistemas criptográficos assim obtidos. No artigo Regev (2004a) o autor demonstra que uma solução eficiente para o PSO no grupo D_n implica uma solução eficiente para o Problema do Menor Vetor em um Reticulado, selando a estreita relação entre os dois problemas.

Infelizmente nem o PSO em S_n nem o PSO em D_n possuem até agora soluções eficientes, quer clássica ou quântica. Mas certo avanço foi conseguido na solução do PSO em D_n. Ettinger e Høyer apresentaram uma interessante redução do problema, na qual estabelecem que basta procurar por subgrupos ocultos que sejam ou triviais ou tenham ordem 2, Ettinger e Høyer (2000). Posteriormente, Kuperberg atacou o problema. O algoritmo de Kuperberg (2005), é um algoritmo quântico subexponencial no tamanho, $O(\log n)$, da entrada. Sua complexidade computacional é $2^{O(\sqrt{\log n})}$. Posteriormente, Regev (2004b), apresentou uma versão melhorada do algoritmo de Kuperberg, onde o tempo de processamento do algoritmo ainda é subexponencial, $2^{O(\sqrt{\log n \log\log n})}$, mas a quantidade de memória utilizada é polinomial no tamanho da entrada.

Generalizando idéias desenvolvidas, a princípio, para o PSO em D_n Ettinger et al. (1999, 2004) apresentaram um algoritmo quântico para o PSO num grupo finito qualquer, no qual com um número polinomial de chamadas à função separadora de classes, obtém-se informação suficiente para determinar o subgrupo oculto. Entretanto, o pós-processamento (clássico) desta informação requer um tempo exponencial para obter os geradores do subgrupo oculto, tornando o algo-

ritmo ineficiente.

Embora o PSO em S_n e D_n tenha se mostrado bastante difícil de ser resolvido, Moore et al. (2005); Kuperberg (2005); Regev (2004b), a pesquisa avançou para vários outros grupos não abelianos com êxito. Assim como no caso abeliano, a Transformada de Fourier tem importante papel nestas soluções. O exemplo mais latente deste fato é a solução apresentada por Hallgren et al. (2000). Neste trabalho, os autores exibem um algoritmo quântico eficiente para a solução do PSO em um grupo qualquer desde que a TFQ seja eficientemente implementável no grupo e que o subgrupo oculto seja normal.

Mais recentemente, Ivanyos et al. (2003), demonstraram que em certos grupos é possível eliminar a hipótese de que a TFQ seja implementável, por exemplo, quando o grupo é solúvel ou em certos grupos de permutações. A estratégia dos autores combina algoritmos clássicos já consolidados na literatura para resolução de problemas da teoria de grupos computacionais, Babai e Szemerédi (1984); Babai et al. (1995), com algoritmos quânticos, a saber, o algoritmo de Shor para o cálculo de logaritmo discreto e o algoritmo de Kitaev para o cálculo da ordem de elementos de um grupo, Kitaev (1995); Portugal et al. (2006). Neste mesmo trabalho, os autores mostram ser possível resolver eficientemente o PSO em uma série de outros grupos não abelianos, onde a ordem do subgrupo de comutadores seja pequena em relação à ordem do grupo, no sentido de que $|G'|$ seja $O(\log |G|)$.

Provavelmente motivado pelo fato de o grupo diedral se escrever como o produto semidireto $\mathbb{Z}_n \rtimes \mathbb{Z}_2$, parte da pesquisa de novos algoritmos quânticos para o PSO foi voltada para grupos não abelianos que se escrevem como o produto semidireto de grupos cíclicos. Num dos primeiros trabalhos nesta linha Puschel et al. (1999) ataca o PSO no grupo produto wreath[13] $\mathbb{Z}_2^n \wr \mathbb{Z}_2$. No trabalho os autores mostram como implementar eficientemente a TFQ no grupo e utilizam o MAF na solução do problema, construindo um algoritmo quântico eficiente.

[13] O produto wreath pode ser visto como um produto semidireto, Robinson (1995).

Moore et al. (2004), resolveram eficientemente o PSO nos grupos q-edrais $\mathbb{Z}_p \rtimes \mathbb{Z}_q$, onde p e q são números primos tais que $q = (p-1)/\text{poli}(\log p)$, através de um algoritmo quântico. Os autores também utilizam o MAF para resolver o problema. No mesmo trabalho é demonstrado outro interessante resultado sobre o PSO. Suponha que o PSO seja eficientemente resolvido em um grupo H. Considere um grupo G e um subgrupo N normal em G. Se $|N| = \text{poli}(\log |H|)$ e $H \simeq G/N$, então o PSO é eficientemente resolvido em G.

Bacon et al. (2005) apresentam mais uma série de grupos não abelianos onde se pode resolver eficientemente o PSO através de um algoritmo quântico. A estratégia utilizada também é o MAF. Dentre os grupos atacados no trabalho, temos o produto semidireto $\mathbb{Z}_N \rtimes \mathbb{Z}_p$ onde p é um número primo e N um inteiro positivo tal que $N/p = \text{poli}(\log N)$ e o produto semidireto $\mathbb{Z}_p^2 \rtimes \mathbb{Z}_p$, o grupo de Heisemberg. Neste mesmo trabalho, os autores ainda atacam o PSO no grupo $\mathbb{Z}_p^r \rtimes \mathbb{Z}_p$, com condições bastante restritivas sobre o parâmetro r. Para atacar tais problemas, eles propõe uma redução do PSO para a busca de subgrupos ocultos que sejam ou triviais ou cíclicos de ordem p. Mas tal redução é válida num ambiente mais amplo. De fato, seja A um grupo abeliano e considere o produto semidireto $A \rtimes \mathbb{Z}_p$, p um número primo. Foi demonstrado pelos autores, de maneira similar ao resultado de Ettinger e Høyer (2000), que é suficiente resolver o PSO no produto semidireto $\tilde{A} \rtimes \mathbb{Z}_p$, onde $\tilde{A}$ é um subgrupo qualquer de A, sob a hipótese adicional de que ou o subgrupo oculto é trivial ou é cíclico de ordem p. Outro aspecto importante neste trabalho é a maneira como a informação é medida. Os autores empregam um processo de medida chamado *pretty good measurement*, diferente da medida projetiva realizada na maioria dos trabalhos da área. Este tipo de abordagem requer que tais operadores de medida sejam eficientemente implementados, o que neste caso é obtido pelos autores.

Uma das desvantagens da utilização do MAF é a necessidade de verificar que a TFQ é eficientemente implementável no grupo em questão. Quando o grupo é abeliano, já sabemos que a TFQ é eficientemente implementável. Entretanto,

no caso de grupos não abelianos não há uma implementação eficiente da TFQ no caso geral. Sendo assim, para cada grupo em que se ataque o problema com o MAF deve-se, de antemão, construir a TFQ. Esta tarefa pode não ser simples dependendo do grupo para o qual se quer realizá-la.

Inui e Le Gall (2005) apresentam uma interessante estratégia para contornar esse problema. Ao atacar o PSO no grupo $\mathbb{Z}_{p^r} \rtimes \mathbb{Z}_p$, p inteiro primo e r um inteiro positivo, os autores utilizam basicamente o MAF. Entretanto, recorrendo à estrutura dos subgrupos, os autores conseguem "fugir" da utilização da TFQ em $\mathbb{Z}_{p^r} \rtimes \mathbb{Z}_p$, utilizando em seu lugar a TFQ no grupo abeliano $\mathbb{Z}_p$. Peça central na estratégia empregada é a classificação de todos os subgrupos do grupo. É a partir desta classificação que os autores identificam as propriedades imprescindíveis para a construção do algoritmo. Devemos mencionar que a redução proposta por Bacon et al. (2005) reduz o PSO em $\mathbb{Z}_{p^r} \rtimes \mathbb{Z}_p$ ao PSO abeliano, no entanto, para utilizar tal redução ainda se faz necessário o conhecimento da classificação dos subgrupos. Desta forma, permanece interessante a principal virtude do trabalho.

Utilizando-se do resultado apresentado por Inui e Le Gall (2005), Chi et al. (2006) atacaram o PSO no produto semidireto $\mathbb{Z}_N \rtimes \mathbb{Z}_p$, onde p é um inteiro primo e N um inteiro tal que p não divide nenhum dos seus fatores primos. Em tais grupos é possível separar o PSO em dois subproblemas: o PSO abeliano em $\mathbb{Z}_{N/p^r}$ e o PSO em $\mathbb{Z}_{p^r} \rtimes \mathbb{Z}_p$ (veja Teorema 2.3.1). Como em ambos os casos o PSO é eficientemente resolvido, mostra-se que o PSO em $\mathbb{Z}_N \rtimes \mathbb{Z}_p$ é eficientemente resolvido por um algoritmo quântico. Embora os grupos atacados neste trabalho tenham a mesma definição daqueles atacados por Bacon et al. (2005), as restrições sobre N em cada caso mostram que mesmo havendo interseções, ambos os trabalhos resolvem o PSO em grupos distintos. Ainda assim não resolvem completamente o problema em $\mathbb{Z}_N \rtimes \mathbb{Z}_p$.

Retomando a estratégia de atacar o PSO em classes de grupos mais gerais, Ivanyos et al. (2007a) apresentam um algoritmo quântico eficiente para a classe dos grupos extra-especiais. Estes grupos, pertencentes à classe dos p-grupos para p

primo, são definidos como segue. Um p-group G é dito extra-especial se $G' = \mathcal{Z}(G)$ e $|G'| = p$, onde G' denota o subgrupo dos comutadores de G e $\mathcal{Z}(G)$ o centro de G[14] . Neste trabalho, os autores demonstram que determinar eficientemente o subgrupo H em um grupo G extra-especial é redutível a determinar eficientemente o subgrupo HG'[15] . Por fim, demonstram que o último problema é redutível ao PSO abeliano. O maior esforço no trabalho se dá para demonstrar que em cada redução a função separadora de classes do subgrupo H induz uma função separadora de classes nas novas instâncias do problema. A mesma estratégia utilizada aqui, é também utilizada num outro trabalho dos autores, Ivanyos et al. (2007b), no qual os autores atacam o PSO em uma classe de grupos nilpotentes. Voltaremos a tratar deste trabalho no Capítulo 6 .

Este apanhado histórico que acabamos de fazer certamente não cobre a totalidade dos trabalhos realizados nesta área de pesquisa, mas apresenta o que de mais importante e representativo foi desenvolvido até o presente momento. Pode-se concluir que o PSO não abeliano representa um dos grandes desafios da área de pesquisa de algoritmos quânticos, embora não seja o único problema atacado. Há outros problemas de teoria de grupos computacionais sendo abordados pelo formalismo quântico. Um exemplo muito interessante é o trabalho de Watrous (2001). Nele o autor apresenta um algoritmo quântico eficiente para o cálculo da ordem de um grupo solúvel. Uma série de outros problemas em grupos solúveis, como teste de pertinência, teste de igualdade de subgrupos e teste de normalidade de subgrupos, se reduzem ao problema do cálculo de ordem. Desta forma, como conseqüência do Algoritmo de Watrous, todos esses problemas são resolvidos eficientemente em grupos solúveis. O algoritmo opera no ambiente dos grupos *black-box*, Babai e Szemerédi (1984); Holt et al. (2005), e nenhum algoritmo clássico eficiente é conhecido para a solução de tal problema. Embora este resultado não esteja diretamente ligado ao PSO, vários algoritmos quânticos para o PSO foram desenvolvidos utilizando idéias nele presentes ou mesmo o próprio resultado, Ivanyos et al. (2003,

[14] Veja o Apêndice A.
[15] $HG' = \{hg;\ h \in H,\ g \in G'\}$.

2007a). Para uma apresentação mais detalhada do Algoritmo de Shor sugerimos ao leitor a leitura de Portugal et al. (2006).

Mencionamos ainda a existência de outras duas grandes vertentes na área de algoritmos quânticos, que podem ser caracterizadas como algoritmos para problemas de busca e otimização, que inclui o algoritmo de Grover, e algoritmos baseados em caminhos aleatórios quânticos. Nesse trabalho nos ateremos apenas aos algoritmos quânticos para o PSO.

2.3.2 Resultados Elementares

Nesta subseção demonstramos dois resultados gerais e simples sobre o PSO que nos serão úteis no desenvolvimento da tese e que, em geral, não são encontrados demonstrados na literatura.

Proposição 2.3.1 Seja G um grupo finito e $H \leq G$ oculto pela função $f : G \to X$. Para qualquer $\tilde{G} \leq G$ temos que $\tilde{f} = f\Big|_{\tilde{G}} : \tilde{G} \to X$ oculta $\tilde{H} = H \cap \tilde{G}$ em $\tilde{G}$.

Demonstração: Devemos mostrar que para todos $a, b \in \tilde{G}$ temos que $\tilde{f}(a) = \tilde{f}(b)$ se, e somente se, $a\tilde{H} = b\tilde{H}$. Suponhamos que $a, b \in \tilde{G}$ são tais que $\tilde{f}(a) = \tilde{f}(b)$. Então, como f oculta H em G, temos $aH = bH$. Assim, existe $h \in H$ tal que $a = bh$. Como $a, b \in \tilde{G}$, temos que $h = b^{-1}a \in \tilde{G}$ e, assim, $h \in \tilde{H}$. Isso prova que $a\tilde{H} = b\tilde{H}$. Reciprocamente, suponhamos que $a\tilde{H} = b\tilde{H}$. Como $a\tilde{H} \subset aH$ e $b\tilde{H} \subset bH$, temos $\emptyset \neq aH \cap bH$ o que implica que $aH = bH$. Mas isso é equivalente a $\tilde{f}(a) = \tilde{f}(b)$, o que encerra a prova.

■

Embora a Proposição 2.3.1 estabeleça um resultado bastante simples de ser verificado, ele tem grande aplicação para a solução do PSO. Suponha que o subgrupo H seja oculto em G e que o PSO não é eficientemente resolvido em G. Se existir um subgrupo $\tilde{G}$ de G onde o PSO seja resolvido eficientemente, pode-se determinar eficientemente o subgrupo $\tilde{H} = H \cap \tilde{G}$ e obter informação sobre o subgrupo oculto H. Caso $H \subset \tilde{G}$, teremos determinado completamente o subgrupo H. No Capítulo 4 utilizaremos este resultado várias vezes.

Um importante corolário da Proposição 2.3.1 segue abaixo.

Corolário 2.3.1 Sejam G_1 e G_2 grupos cujas ordens sejam coprimas e onde o PSO é eficientemente resolvido. Então o PSO em $G_1 \times G_2$ também é eficientemente resolvido.

Demonstração: Pela Proposição A.1.1 todo subgrupo de $G_1 \times G_2$ é da forma $H_1 \times H_2$ com $H_1 \leq G_1$ e $H_2 \leq G_2$. Suponha que um tal grupo seja oculto por uma função $f : G_1 \times G_2 \to X$. As restrições de f a G_1 e a G_2 ocultam, respectivamente, H_1 e H_2. Como nos grupos em questão o PSO é eficientemente resolvido, podemos determinar geradores para H_1 e H_2. Conseqüentemente, geradores para $H_1 \times H_2$, o que mostra que o PSO em $G_1 \times G_2$ é eficientemente resolvido. Encerrando a prova.

■

2.3.3 Formalismo Quântico para o PSO

Como lidar com o PSO no grupo G em um computador quântico? A primeira coisa a fazer é definir o espaço de estados do computador quântico. Uma pergunta relevante que devemos fazer é como os elementos do grupo G e do conjunto X serão registrados no computador. Como uma das premissas do problema, deve-se admitir que os elementos de G e X são, de alguma maneira, codificados no computador quântico. Nos principais casos onde o PSO vem sendo estudado, e aqui inclui-se o caso que trataremos na tese, podemos responder a isso da seguinte maneira. Sejam $n = \lceil \log |G| \rceil$[16] e $m = \lceil \log |X| \rceil$ e considere $\mathcal{B}_n$ e $\mathcal{B}_m$ o conjunto das palavras binárias de n e m dígitos, respectivamente. Associamos a cada elemento do grupo G uma palavra binária de $\mathcal{B}_n$ e a cada elemento de X associamos uma palavra de $\mathcal{B}_m$. Para ilustrar esse tipo de procedimento, considere o caso bastante simples do grupo cíclico $\mathbb{Z}_N$, onde a cada elemento $a \in \mathbb{Z}_N$ corresponde a palavra binária que representa o inteiro a na base 2. Isso induz uma óbvia codificação em grupos que se escrevam como produto direto ou semidireto de tais grupos.

[16] $\forall\, a \in \mathbb{R}$, $\lceil a \rceil$ = menor inteiro maior que ou igual a a.

Seja agora um espaço de Hilbert, $\mathcal{H}_n$, gerado por uma base ortonormal cujos elementos são indexados pelos elementos de $\mathcal{B}_n$ e, analogamente, seja um espaço de Hilbert, $\mathcal{H}_m$, gerado por uma base ortonormal cujos elementos são indexados pelos elementos de $\mathcal{B}_m$. O espaço de estados do computador quântico será o espaço $\mathcal{H}_n \otimes \mathcal{H}_m$. Pela associação feita entre os elementos de G e X aos elementos de $\mathcal{B}_n$ e $\mathcal{B}_m$, podemos considerar os subespaços $\mathcal{H}_G = \langle |g\rangle \,;\, g \in \mathcal{G}\rangle$ e $\mathcal{H}_X = \langle |z\rangle \,;\, z \in X\rangle$. Caso $|G| < 2^n$ e/ou $|X| < 2^m$ esses subespaços são próprios, assim como o subespaço $\mathcal{H} = \mathcal{H}_G \otimes \mathcal{H}_X$. Se este for o caso, assumiremos que os operadores unitários que farão a computação necessária para a solução do PSO, atuarão trivialmente sobre elementos não pertencentes ao espaço $\mathcal{H}$, isto é, atuarão como o operador identidade. Para uma discussão mais profunda sobre codificação dos elementos referenciamos os trabalhos de Babai et al. (1995).

Respondida a pergunta sobre a representação dos elementos no computador quântico, devemos nos preocupar com as operações fundamentais que deverão ser efetuadas sobre tais elementos, a saber, o produto do grupo G e a atuação da função separadora de classes, f. Também como premissas do problema, assumimos que existem operadores unitários que efetuam tais operações. Isto é, existe um operador unitário U tal que dados elementos $|g\rangle, |h\rangle \in \mathcal{H}_G$, $U|g\rangle|h\rangle = |g\rangle|gh\rangle$. É comum na literatura, pensar o operador U como um operador sobre um único registrador. Fixado um elemento $|g\rangle \in \mathcal{H}_G$ denotamos por U_g o operador unitário sobre um registrador dado por $U_g|h\rangle = |gh\rangle$. Obviamente este operador é induzido por U.

Por fim, assumimos a existência de um operador unitário V_f responsável pela aplicação da função separadora de classes laterais, que opera da seguinte maneira. Dados $|g\rangle \in \mathcal{H}_G$ e $|z\rangle \in \mathcal{H}_X$, $V_f|g\rangle|x\rangle = |g\rangle|z \oplus f(g)\rangle$, onde $\oplus$ denota a soma binária dos elementos de $\mathcal{B}_m$.

Encerramos este capítulo introdutório discutindo um outro importante aspecto do algoritmos quânticos. Todo algoritmo quântico é probabilístico, o que se deve ao fato de todo algoritmo ter que efetuar alguma medida. Sendo assim, eles podem em determinado momento nos fornecer uma resposta errada, ou falhar na

obtenção de uma tal resposta, isto é, não nos dar resposta alguma. Precisamos, de alguma forma, medir a confiabilidade de um algoritmo. Diremos que um algoritmo probabilístico é eficiente se sua complexidade computacional for polinomial e se sua probabilidade de sucesso for maior que 1/2. É importante notar que a palavra eficiente está sendo empregada em três ambientes distintos no nosso trabalho: (1) quando dizemos que uma transformação unitária de n *qbits* é implementada eficientemente, significando que o número de portas elementares empregadas em sua implementação é polinomial em n; (2) quando dizemos que um algoritmo para o PSO em um grupo G é eficiente, significando que sua complexidade computacional é $O(\text{poli}(\log |G|))$ e (3) quando um algoritmo probabilístico é eficiente, significando que sua probabilidade de sucesso seja maior que 1/2. Sempre que necessário for, enfatizaremos o caráter da palavra eficiência para que não haja risco de confusão. Para uma discussão mais profunda sobre este tema sugerimos a referência Kitaev et al. (2002).

Capítulo 3

O Grupo $\mathbb{Z}_{p^r} \rtimes \mathbb{Z}_{p^s}$

Neste capítulo, apresentamos o grupo $\mathbb{Z}_{p^r} \rtimes \mathbb{Z}_{p^s}$ onde iremos atacar o PSO. De fato, não se trata de um único grupo, mas de uma coleção de grupos, pois a cada homomorfismo $\phi : \mathbb{Z}_{p^s} \to \mathrm{Aut}(\mathbb{Z}_{p^r})$ fixado, temos um grupo distinto. Entretanto, como veremos, podemos separar esses grupos em sub-coleções de grupos isomorfos. Isso nos permitirá atacar o PSO em um reduzido número de grupos, um representante para cada sub-coleção, para os quais a abordagem será a mesma.

Ferramenta imprescindível para o entendimento do problema é a teoria de grupos. Não faremos na tese uma descrição dos aspectos básicos da teoria, reportando o leitor para as referências Garcia e Lequain (2002); Hernstein (1970). Entretanto, alguns elementos da teoria que são centrais no desenvolvimento do nosso trabalho, estão apresentados sucintamente no Apêndice A. Para esses tópicos, além das referências já mencionadas, sugerimos a leitura de Robinson (1995); Hall Jr. (1959) e Spindler (1994). Ao longo de toda a tese iremos nos ater a grupos finitos, exceto em menção contrária.

3.1 A Estrutura do Grupo $\mathbb{Z}_{p^r} \rtimes \mathbb{Z}_{p^s}$

Sejam p um número primo ímpar e $r, s \in \mathbb{N}$. Considere os grupos aditivos $\mathbb{Z}_{p^r}$ e $\mathbb{Z}_{p^s}$, e o produto semidireto $\mathbb{Z}_{p^r} \rtimes_\phi \mathbb{Z}_{p^s}$, onde $\phi : \mathbb{Z}_{p^s} \to \mathrm{Aut}(\mathbb{Z}_{p^r})$ é o homomorfismo de grupos que define o produto semidireto (ver Apêndice A, Definição A.1.1). Os elementos neste grupo são da forma (a, b), com $a \in \mathbb{Z}_{p^r}$ e $b \in \mathbb{Z}_{p^s}$, a

operação do grupo é dada pela regra $(a,b)(c,d) = (a + \phi(b)(c), b + d)$ e o elemento identidade é $e = (0,0)$. A fórmula de multiplicação do grupo atesta que se ϕ não for o homomorfismo trivial descrito no Exemplo A.1.1, então $\mathbb{Z}_{p^r} \rtimes_\phi \mathbb{Z}_{p^s}$ não é abeliano.

Do Teorema A.1.1, temos que $\mathrm{Aut}\,(\mathbb{Z}_{p^r}) \simeq \mathbb{Z}_{p^r}^*$ e em conseqüência, o homomorfismo ϕ é completamente determinado por $\alpha = \phi(1)(1) \in \mathbb{Z}_{p^r}^*$, sendo $\phi(b)(a) = a\alpha^b$, $\forall\, a \in \mathbb{Z}_{p^r}$, $b \in \mathbb{Z}_{p^s}$. Na definição de α, 1 representa tanto o elemento identidade de $\mathbb{Z}_{p^r}$ quanto o elemento identidade de $\mathbb{Z}_{p^s}$. Assim, a fórmula de multiplicação dos elementos do grupo se reescreve como $(a,b)(c,d) = (a + c\alpha^b, b + d)$.

A pergunta que devemos nos fazer agora é: quais são os elementos em $\mathbb{Z}_{p^r}^*$ que definem tais homomorfismos? Para responder, notamos que $\phi(0) = \phi(p^s) : \mathbb{Z}_{p^r} \to \mathbb{Z}_{p^r}$ é o elemento identidade de $\mathrm{Aut}\,(\mathbb{Z}_{p^r})$, assim temos que $\alpha^{p^s} = \phi(p^s)(1) = 1$. Desta forma, segue que um elemento $\alpha \in \mathbb{Z}_{p^r}^*$ que define um tal homomorfismo, deve satisfazer à equação de congruência

$$Y^{p^s} \equiv 1 \bmod p^r. \tag{3.1}$$

Nos interessa saber quais são as raízes de (3.1) em $\mathbb{Z}_{p^r}^*$. Notamos que as raízes da equação (3.1) possuem uma estreita relação com os parâmetros p, r e s que definem o grupo. De fato, caso seja $r \leq s$ note que para todo $0 \leq \tau < p^{r-1}$, tem-se que $\alpha_\tau = \tau p + 1 \in \mathbb{Z}_{p^r}^*$ é uma raiz da equação (3.1). Para verificar esse fato, basta expandir $(\tau p + 1)^{p^s}$ e tomar a congruência módulo p^r. Considere agora o polinômio $Y^{p^s} - 1$. Tem-se que

$$Y^{p^s} - 1 \equiv (x - \alpha_\tau)^{p^{s-r+1}} P(Y) \bmod p^r, \tag{3.2}$$

onde

$$P(Y) = \sum_{i=0}^{p^s - p^{s-r+1}} a_i \alpha_\tau^i Y^{p^s - p^{s-r+1} - i}$$

e os coeficientes a_i são definidos como o número binomial $\begin{pmatrix} i+p^{s-r+1}-1 \\ p^{s-r+1}-1 \end{pmatrix}$. Além disso, temos que

$$P(\alpha_\tau) = \begin{pmatrix} p^s - p^{s-r+1} \\ p^{s-r+1} \end{pmatrix} \alpha_\tau^{p^s - p^{s-r+1}} \not\equiv 0 \bmod p^r.$$

Portanto, concluímos que a multiplicidade de cada raíz é p^{s-r+1}. Contadas as raízes α_τ e suas multiplicidades, totalizamos p^s raízes de (3.1). Pelo Lema de Hensel, Gouvêa (1997), verifica-se que essas são todas as raízes em $\mathbb{Z}_{p^r}^*$. Se $p^l = \text{mdc}\,(\tau, p^{r-1})$, $0 \leq l < r-1$, podemos escrever $\tau = tp^l$, com $t \in \mathbb{Z}_{p^{r-1}}^* \cup \{0\}$ e $\alpha_\tau = tp^{l+1} + 1$. Para ressaltar a dependência das raízes aos parâmetros t e l, denotaremos a raiz α_τ por $\alpha_{t,l}$. É importante notar que quando $r = 1$ existe apenas a raiz trivial $\alpha = 1$, com multiplicidade p^s, e o grupo por ela definido é o produto direto $\mathbb{Z}_p \times \mathbb{Z}_{p^s}$. Este também é o caso, quando $\tau = t = 0$. Não abordaremos nessa primeira parte da tese o caso em que $r \leq s$. Ele será tratado no Capítulo 6.

Nos dedicaremos até o fim do Capítulo 5 ao caso em que $r > s$. Nestas circunstâncias, para todo $0 \leq \tau < p^s$ temos que $\alpha_\tau = \tau p^{r-s} + 1 \in \mathbb{Z}_{p^r}^*$ é uma raiz de (3.1). Para verificar este fato, basta expandir $(\tau p^{r-s}+1)^{p^s}$ e observar que todas as parcelas da soma, exceto a parcela igual a 1, são congruentes a 0 módulo p^r. Desta forma, temos p^s raízes distintas e o Lema de Hensel nos diz que estas são todas as raízes da equação. Considerando agora $p^l = \text{mdc}\,(\tau, p^s)$, temos $0 \leq l < s$ e podemos escrever $\tau = tp^l$ com $t \in \mathbb{Z}_{p^s}^* \cup \{0\}$. Logo, $\alpha_\tau = \tau p^{r-s} + 1 = tp^{r-s+l} + 1$. Por coerência na notação, passamos a denotar α_τ por $\alpha_{t,l}$. Usamos esta notação para ressaltar a dependência das raízes aos parâmetros t e l.

Cada raíz $\alpha_{t,l}$ define um homomorfismo $\phi_{t,l} : \mathbb{Z}_{p^s} \to \text{Aut}\,(\mathbb{Z}_{p^r})$, e portanto, um produto semidireto $\mathcal{G}^{t,l} = \mathbb{Z}_{p^r} \rtimes_{\phi_{t,l}} \mathbb{Z}_{p^s}$. Caso $t = 0$ temos o produto direto $\mathbb{Z}_{p^r} \times \mathbb{Z}_{p^s}$, para o qual o PSO já está resolvido, por tratar-se de um grupo abeliano. Assim, podemos considerar $t \in \mathbb{Z}_{p^s}^*$. Observamos que $x = (1, 0)$ e $y = (0, 1)$ geram $\mathcal{G}^{t,l}$. Logo, qualquer elemento $(a, b) \in \mathcal{G}^{t,l}$ pode ser reescrito como $(a, b) = x^a y^b$. Nesta notação, o produto de dois elementos $x^a y^b, x^c y^d \in \mathcal{G}^{t,l}$ é dado por

$\left(x^a y^b\right)\left(x^c y^d\right) = x^{a+c\alpha_{t,l}^b} y^{b+d}$.

Vamos lançar um olhar mais cuidadoso sobre a potência $\alpha_{t,l}^b$ que aparece nessa equação de produto. Se expandimos a mesma, obtemos:

$$\alpha_{t,l}^b = \left(tp^{r-s+l}\right)^b + b\left(tp^{r-s+l}\right)^{b-1} + \cdots + \frac{b(b-1)}{2}\left(tp^{r-s+l}\right)^2 + b\left(tp^{r-s+l}\right) + 1. \quad (3.3)$$

Caso o parâmetro l seja tal que $r \geq 2(s-l)$ a equação (3.3) assegura que

$$\alpha_{t,l}^b \equiv tbp^{(r-s+l)} + 1 \bmod p^r,$$

pois para qualquer $j \geq 2$, $j(r-s+l) \geq r$. Manteremos a suposição de que $r \geq 2(s-l)$ até a próxima seção, onde fixaremos definitivamente a hipótese sobre o parâmetro l. Desta maneira, a fórmula do produto do grupo passa a ser dada por,

$$\left(x^a y^b\right)\left(x^c y^d\right) = x^{a+c(tbp^{r-s+l}+1)} y^{b+d}, \quad (3.4)$$

quaisquer que sejam $a, c \in \mathbb{Z}_{p^r}$ e $b, d \in \mathbb{Z}_{p^s}$. Como conseqüência, para quaisquer $a \in \mathbb{Z}_{p^r}$ e $b \in \mathbb{Z}_{p^s}$ temos

$$y^b x^a = x^{a(tbp^{r-s+l}+1)} y^b. \quad (3.5)$$

De especial interesse para nós, são os grupos definidos por $\alpha_{1,l} = p^{r-s+l} + 1$. Denotaremos o produto semidireto definido por $\alpha_{1,l}$ por $\mathcal{G}^l$. O teorema seguinte nos diz por qual razão tais grupos serão tão especiais. Vamos a ele.

Teorema 3.1.1 Para qualquer par t, l que defina uma raíz $\alpha_{t,l}$ não trivial[1] da equação (3.1) tem-se, $\mathcal{G}^{t,l} \simeq \mathcal{G}^l$.

Demonstração: Fixemos as raízes $\alpha_{t,l}$ e $\alpha_{1,l}$ da equação (3.1) e os respectivos grupos $\mathcal{G}^{t,l}$ e $\mathcal{G}^l$, por elas definidos. Como $t \in \mathbb{Z}_{p^s}^*$, existe um único $t^{-1} \in \mathbb{Z}_{p^s}^*$ tal que $tt^{-1} \equiv 1 \bmod p^s$. Seja $\Psi_{t,l} : \mathcal{G}^l \to \mathcal{G}^{t,l}$ definida por $\Psi_{t,l}(x^a y^b) = x^a y^{t^{-1}b}$. Pela unicidade de t^{-1}, dado $x^a y^b \in \mathcal{G}^{t,l}$ temos que $x^a y^{tb}$ é o único elemento em $\mathcal{G}^l$, tal que $\Psi_{t,l}(x^a y^{tb}) = x^a y^b$, o que prova que $\Psi_{t,l}$ é uma aplicação bijetora. Além disso,

[1] Por raíz trivial entendemos a raiz $\alpha = 1$ da equação (3.1).

note que:

$$\begin{aligned}
\Psi_{t,l}\left(\left(x^a y^b\right)\left(x^c y^d\right)\right) &= \Psi_{t,l}\left(x^{a+c(bp^{r-s+l}+1)} y^{b+d}\right) \\
&= x^{a+c(bp^{r-s+l}+1)} y^{t^{-1}(b+d)} \\
&= x^a y^{t^{-1}b} y^{-t^{-1}b} x^{c(bp^{r-s+l}+1)} y^{t^{-1}(b+d)} \\
&= x^a y^{t^{-1}b} x^{c(bp^{r-s+l}+1)(-t^{-1}btp^{r-s+l}+1)} y^{-bt^{-1}} y^{t^{-1}(b+d)} \\
&= x^a y^{t^{-1}b} x^c y^{t^{-1}d} = \Psi_{t,l}\left(x^a y^b\right)\Psi_{t,l}\left(x^c y^d\right).
\end{aligned}$$

Concluímos que $\Psi_{t,l}$ é um homomorfismo bijetor, portanto, um isomorfismo.

■

Devido ao isomorfismo do Teorema 3.1.1, os grupos $\mathcal{G}^{t,l}$ são subdivididos em classes de subgrupos isomorfos. Desta forma, podemos nos concentrar no estudo de um único representante de cada uma dessas classes de grupos, a saber, o grupo $\mathcal{G}^l$. Por isso, no restante do trabalho nos ateremos aos grupos $\mathcal{G}^l$ com $0 \leq l < s$.

Encerramos esta seção com um último resultado sobre esses grupos.

Teorema 3.1.2 Para cada $1 \leq l < s$ temos que $\dfrac{\mathcal{G}^l}{\left\langle y^{p^l}\right\rangle} \simeq \mathbb{Z}_{p^r} \rtimes_{\phi_0} \mathbb{Z}_{p^{s-l}}$, onde $\phi_0(1)(1) = p^{r-s}+1$.

Demonstração: De fato, fixado l definimos $\Gamma_l : \mathcal{G}^l \to \mathbb{Z}_{p^r} \rtimes_{\phi_0} \mathbb{Z}_{p^{s-l}}$ por $\Gamma_l\left(x^a y^b\right) = x^a y^{r_b}$, onde r_b é o resto da divisão de b por p^{s-l}. Verifica-se que Γ_l é um homomorfismo sobrejetor, cujo núcleo é $\left\langle y^{p^l}\right\rangle$. Logo, segue o resultado.

■

3.2 A Estrutura dos Subgrupos de $\mathcal{G}^l$

Nesta seção iremos caracterizar os subgrupos de $\mathcal{G}^l$ em função dos geradores x e y. Deste ponto até o fim do Capítulo 6 restante da tese, seja $0 \leq l < s$ fixado arbitrariamente e consideremos o grupo $\mathcal{G}^l$, cuja operação é dada por

$$\left(x^a y^b\right)\left(x^c y^d\right) = x^{a+c(bp^{r-s+l}+1)} y^{b+d} \tag{3.6}$$

e que tem com conseqüência o fato abaixo:

$$y^b x^a = x^{a(bp^{r-s+l}+1)} y^b. \tag{3.7}$$

Dado $k \in \mathbb{N}$ e um elemento qualquer $x^a y^b \in \mathcal{G}^l$, segue de (3.7) que

$$\left(x^a y^b\right)^k = x^{a\left(k+\frac{k(k-1)}{2}bp^{r-s+l}\right)} y^{bk} = x^{a\frac{k(k-1)}{2}bp^{r-s+l}} x^{ak} y^{bk}. \tag{3.8}$$

Considere $p^i = \text{mdc}\,(a, p^r)$ e $p^j = \text{mdc}\,(b, p^s)$, onde $0 \leq i \leq r$ e $0 \leq j \leq s$. Decorre da equação anterior que

$$\begin{cases} (x^a y^b)^{p^{s-j}} = x^{ap^{s-j}}, & (x^a y^b)^{p^{r-i}} = e, & \text{se } r-i \geq s-j \\ (x^a y^b)^{p^{s-j}} = e, & (x^a y^b)^{p^{r-i}} = y^{bp^{r-i}}, & \text{se } r-i < s-j \end{cases}. \tag{3.9}$$

As identidades mostradas em (3.9) nos permitem concluir que a ordem do elemento $x^a y^b \in \mathcal{G}^l$, que denotamos por $\left|x^a y^b\right|$, é dada por

$$\left|x^a y^b\right| = \max\left\{p^{r-i}, p^{s-j}\right\}. \tag{3.10}$$

Desde a seção anterior, assumimos que o parâmetro l satisfaz à desigualdade $r \geq 2(s-l)$. Neste momento restringiremos essa hipótese, fixando o seguinte:

Hipótese 1 O parâmetro l que define o homomorfismo do grupo $\mathcal{G}^l$ satisfaz à desigualdade $r \geq 2s - l$.

Essa é a última restrição que faremos sobre esses parâmetros ao longo da tese. Assim como o caso em que $r \leq s$, os casos que violem esta hipótese serão abordados no Capítulo 6. Vale observar que quaisquer que sejam r e s, com $r > s$, é sempre possível escolher ao menos um l satisfazendo a esta hipótese, isto é, existe ao menos um grupo da forma $\mathcal{G}^l$ com l satisfazendo à Hipótese 1. Caso $r \geq 2s$ obviamente a hipótese será satisfeita para qualquer l. Por esta razão, os resultados que apresentaremos na tese irão generalizar os resultados apresentados em Cosme e Portugal (2007a,b), bem como os resultados apresentados em Inui e Le Gall (2005);

Chi et al. (2006).

Analisando a equação (3.8) à luz de (3.9), podemos mostrar que $x^{a\frac{k(k-1)}{2}bp^{r-s+l}} \in \langle x^a y^b \rangle$, logo $x^{ak}y^{bk} \in \langle x^a y^b \rangle \ \forall\, k \in \mathbb{N}$. De fato, sendo $r \geq 2s - l$, se $r - i \geq s - j$ temos

$$x^{a\frac{k(k-1)}{2}bp^{r-s+l}} = \left(x^{ap^{s-j}}\right)^{\frac{k(k-1)}{2}bp^{r-2s+l+j}} = \left(\left(x^a y^b\right)^{p^{s-j}}\right)^{\frac{k(k-1)}{2}bp^{r-2s+l+j}}.$$

Caso seja $r - i < s - j$, então $x^{a\frac{k(k-1)}{2}bp^{r-s+l}} = e$.

Levando em consideração a discussão precedente, temos o seguinte lema, que embora seja bastante simples, terá grande importância em nosso trabalho.

Lema 3.2.1 Dado $x^a y^b \in \mathcal{G}^l$ temos que $\langle x^a y^b \rangle = \left\{x^{ak}y^{bk}; 0 \leq k < \left|x^a y^b\right|\right\}$.

Demonstração: Seja $R = \left|x^a y^b\right|$ Como já mostramos que $x^{ak}y^{bk} \in \langle x^a y^b \rangle \ \forall\, k \in \mathbb{N}$, basta provar que se $0 < k \leq R$, então $(x^a y^b)^k = e$ se, e somente se, $k = R$. De (3.9) nota-se que se $k = R$, então $(x^a y^b)^k = e$. Se por outro lado, for $k < R$, então ou $ak < p^r$ ou $bk < p^s$, e por (3.8) tem-se que $(x^a y^b)^k \neq e$.

■

Seja $x^a y^b \in \mathcal{G}^l$, $a, b \neq 0$, e escrevamos $b = up^j$ onde, como antes, $p^j = \text{mdc}\,(b, p^s)$ com $0 \leq j < s$ e $u \in \mathbb{Z}_{p^s}^*$. Existe $u^{-1} \in \mathbb{Z}_{p^s}^*$ tal que $uu^{-1} \equiv 1 \bmod p^s$, assim $(x^a y^b)^{u^{-1}} = x^{a'}y^{bu^{-1}} = x^{a'}y^{p^j}$ onde $a' = a\left(u^{-1} + \frac{u^{-1}-1}{2}p^{r-s+j+l}\right)$. Como $u^{-1} \in \mathbb{Z}_{p^s}^*$, temos que $\text{mdc}\,(a, p^r) = \text{mdc}\,(a', p^r)$ e, portanto, segue deste fato que $\left|x^a y^b\right| = \left|x^{a'}y^{p^j}\right|$. Desta forma, $\langle x^a y^b \rangle = \left\langle x^{a'}y^{p^j} \right\rangle$. Seja $p^i = \text{mdc}\,(a', p^r)$ e $a' = t'p^i$. Se $r - i \geq s - j$ podemos tomar $t' \in \mathbb{Z}_{p^{s-j}}^*$. De fato, caso $t' \geq p^{s-j}$, escrevemos $t' = qp^{s-j} + t$ com $t \in \mathbb{Z}_{p^{s-j}}^*$. Então

$$x^{t'p^i}y^{p^j} = x^{qp^{i+s-j}}x^{tp^i}y^{p^j}. \tag{3.11}$$

Nos atenhamos ao termo $x^{qp^{i+s-j}}$. Por (3.9)

$$x^{qp^{i+s-j}} = \left(\left(x^{tp^i}\right)^{p^{s-j}}\right)^{qt^{-1}} = \left(x^{tp^i}y^{p^j}\right)^{qt^{-1}p^{s-j}}. \tag{3.12}$$

Segue de (3.11) e (3.12) que

$$x^{t'p^i}y^{p^j} = \left(x^{tp^i}y^{p^j}\right)^{1+qt^{-1}p^{s-j}} \Rightarrow \left\langle x^{t'p^i}y^{p^j}\right\rangle \leq \left\langle x^{tp^i}y^{p^j}\right\rangle$$

Como $\left|x^{t'p^i}y^{p^j}\right| = \left|x^{tp^i}y^{p^j}\right| = p^{r-i}$ temos

$$\left\langle x^a y^b\right\rangle = \left\langle x^{t'p^i}y^{p^j}\right\rangle = \left\langle x^{tp^i}y^{p^j}\right\rangle.$$

Por outro lado, sendo $r-i < s-j$ podemos tomar $t \in \mathbb{Z}^*_{p^{r-i}}$, sendo a análise análoga à do caso anterior.

Definição 3.2.1 Dados $i, j \in \mathbb{N}$ tais que $0 \leq i \leq r$ e $0 \leq j \leq s$, definimos $m' = \min\{r-i, s-j\}$.

O lema seguinte, de destacada importância, decorre da discussão precedente.

Lema 3.2.2 Os subgrupos cíclicos de $\mathcal{G}^l$ são da forma $\left\langle x^{tp^i}y^{p^j}\right\rangle$ onde $0 \leq i \leq r$, $0 \leq j \leq s$ e $t \in \mathbb{Z}^*_{p^{m'}}$ se $m' \neq 0$ ou $t = 1$ se $m' = 0$.

■

Definição 3.2.2 Dado $H \leq \mathcal{G}^l$, definimos $H_x, H_y \leq \mathcal{G}^l$ dados por $H_x = H \cap \langle x\rangle = \left\langle x^{p^m}\right\rangle$ e $H_y = H \cap \langle y\rangle = \left\langle y^{p^n}\right\rangle$, onde $0 \leq m \leq r$ e $0 \leq n \leq s$.

Tendo em vista a implementação de um algoritmo quântico para a solução do PSO em $\mathcal{G}^l$, é interessante entender a relação entre os coeficientes i, j e t que definem um subgrupo cíclico, $H = \left\langle x^{tp^i}y^{p^j}\right\rangle$, com os coeficientes m e n que definem os subgrupos H_x e H_y, respectivamente. Começamos observando que se $r-i \geq s-j$, então $H_y = \{y^{p^s}\} = \{e\}$ e $H_x = \left\langle x^{p^m}\right\rangle$ para algum m. Por outro lado, (3.9) nos diz que os elementos em H_x são da forma:

$$\left(x^{tp^i}y^{p^j}\right)^{kp^{s-j}} = \left(x^{p^{i+s-j}}\right)^{kt}.$$

Portanto, $m = i+s-j$ e podemos escrever $i = m-s+j$. Assim

$$H = \left\langle x^{tp^{m-s+j}}y^{p^j}\right\rangle. \tag{3.13}$$

Quando temos $r-i < s-j$, então $H_x = \{x^{p^r}\} = \{e\}$ e $H_y = \left\langle y^{p^n} \right\rangle$ para algum n. De maneira análoga concluímos que $n = j + r - i$. Assim, pondo $i = r - n + j$ temos

$$H = \left\langle x^{tp^{r-n+j}} y^{p^j} \right\rangle. \tag{3.14}$$

Neste caso, temos ainda que $t \in \mathbb{Z}^*_{p^{r-i}} = \mathbb{Z}^*_{p^{n-j}}$.

A definição seguinte nos será útil para dar melhor fluência ao texto da tese.

Definição 3.2.3 Seja $g \in \mathcal{G}^l$. Diremos que g satisfaz à hipótese cíclica, em alusão ao Lema 3.2.2, se $g = x^{tp^i} y^{p^j}$ com $0 \leq i \leq r$, $0 \leq j \leq s$ e $t \in \mathbb{Z}^*_{p^{m'}}$ se $m' \neq 0$ ou $t = 1$ se $m' = 0$.

Agora, voltamos nossa atenção para os subgrupos de $\mathcal{G}^l$ gerados por dois elementos. De imediato destacamos os subgrupos da forma $H = \left\langle x^{p^i}, y^{p^j} \right\rangle$, com $0 \leq i < r$ e $0 \leq j < 0$, todos distintos entre si. Obviamente, $H_x = \left\langle x^{p^i} \right\rangle$ e $H_y = \left\langle y^{p^j} \right\rangle$, com $m = i$ e $n = j$.

Vamos considerar outros dois casos de subgrupos gerados por dois elementos, $H = \left\langle x^{tp^i} y^{p^j}, x^{p^k} \right\rangle$ e $L = \left\langle x^{tp^i} y^{p^j}, y^{p^\lambda} \right\rangle$ onde $x^{tp^i} y^{p^j}$ satisfaz à hipótese cíclica, $0 \leq k < r$ e $0 \leq \lambda < s$. Vejamos primeiro o caso do subgrupo H. Se $k \leq i$, podemos escrever $i = k + i'$ e assim $x^{tp^i} y^{p^j} = \left(x^{p^k}\right)^{tp^{i'}} y^{p^j}$. Esta identidade assegura que $y^{p^j} \in H$ e que $x^{tp^i} y^{p^j} \in \left\langle x^{p^k}, y^{p^j} \right\rangle$. Logo, temos $H = \left\langle x^{p^k}, y^{p^j} \right\rangle$.

Suponhamos agora que $k \geq i + s - j$, o que implica que devemos ter $r - i \geq s - j$. Podemos escrever $k = i + s - j + k'$ e assim, por (3.9)

$$x^{p^k} = \left(x^{tp^{i+s-j}}\right)^{t^{-1}p^{k'}} = \left(x^{tp^i} y^{p^j}\right)^{t^{-1}p^{k'+s-j}}.$$

Logo $x^{p^k} \in \left\langle x^{tp^i} y^{p^j} \right\rangle$ e $H = \left\langle x^{tp^i} y^{p^j} \right\rangle$. Resta considerar o caso em que $i < k < \min\{i + s - j, r\}$ onde podemos escrever $k = i + k'$ com $0 < k' < m'$. Mas antes de prosseguirmos, vejamos o caso dos subgrupos da forma $L = \left\langle x^{tp^i} y^{p^j}, y^{p^\lambda} \right\rangle$. Pode-se verificar que este caso é inteiramente similar ao anterior, ressalvadas as particularidades. Se $\lambda \leq j$, então $L = \left\langle x^{p^i}, y^{p^j} \right\rangle$. Se $\lambda \geq j + r - i$, então $L = \left\langle x^{tp^i} y^{p^j} \right\rangle$ e aqui deve-se ter $r - i < s - j$. Resta o caso em que $j < \lambda <$

$\min\{j+r-i, s\}$, ou equivalentemente, onde $\lambda = j + \lambda'$ com $0 < \lambda' < m'$. Tendo em vista as restrições sobre k' e λ', deve-se ter $i < r-1$ e $j < s-1$ para que se tenha $m' > 1$ e, portanto, possam existir k' e λ'. O lema a seguir mostra a estreita relação entre os grupos H e L nesses casos restantes.

Lema 3.2.3 Dado $x^{tp^i}y^{p^j} \in \mathcal{G}^l$, com $0 \leq i < r-1$, $0 \leq j < s-1$ e $t \in \mathbb{Z}^*_{p^{m'}}$, sejam H e L os subgrupos definidos por $H = \left\langle x^{tp^i}y^{p^j}, x^{p^{i+k}} \right\rangle$ e $L = \left\langle x^{tp^i}y^{p^j}, y^{p^{j+k}} \right\rangle$ onde $0 < k < m'$. Então $H = L$ e pode-se tomar $t \in \mathbb{Z}^*_{p^k}$.

Demonstração: Calculando $\left(x^{tp^i}y^{p^j}\right)^{p^k}$ temos

$$\left(x^{tp^i}y^{p^j}\right)^{p^k} = \left(x^{p^{i+k}}\right)^{t\left(1+\frac{p^k-1}{2}p^{r-s+j}\right)} y^{p^{j+k}}.$$

Como $t\left(1+\frac{p^k-1}{2}p^{r-s+j}\right)$ é coprimo com p, a identidade anterior nos mostra que $x^{p^{i+k}} \in L$, $y^{p^{j+k}} \in H$ e, assim, $L = H$. Se agora escrevemos $t = qp^k + t'$ com $0 < t' < p^k$, temos que

$$x^{tp^i}y^{p^j} = \left(x^{p^{i+k}}\right)^q x^{t'p^i}y^{p^j} \Rightarrow H = \left\langle x^{t'p^i}y^{p^j}, x^{p^{i+k}} \right\rangle$$

e pode-se assumir $t \in \mathbb{Z}^*_{p^k}$, encerrando assim a prova.

■

Verifica-se que os subgrupos da forma $H = \left\langle x^{tp^i}y^{p^j}, x^{p^{i+k}} \right\rangle$ são todos distintos entre si, não são cíclicos e também distintos dos subgrupos da forma $\left\langle x^{p^i}, y^{p^j} \right\rangle$. Além disso, temos que

$$H_x = \left\langle x^{p^{i+k}} \right\rangle \text{ com } m = i+k \text{ e } H_y = \left\langle y^{p^{j+k}} \right\rangle \text{ com } n = j+k. \tag{3.15}$$

De fato, temos $\left\langle x^{p^{i+k}} \right\rangle \subset H_x$. Da discussão precedente a (3.13), temos $\left\langle x^{tp^i}y^{p^j} \right\rangle \cap \langle x \rangle = \left\langle x^{p^{i+s-j}} \right\rangle$ se $r-i \geq s-j$ e $\left\langle x^{tp^i}y^{p^j} \right\rangle \cap \langle x \rangle = \{e\}$ se $r-i < s-j$. No primeiro caso, como $0 < k < s-j$, segue que $i+s-j > i+k$ e, portanto, $\left\langle x^{p^{i+s-j}} \right\rangle \subset \left\langle x^{p^{i+k}} \right\rangle$. Conclui-se que $H_x = \left\langle x^{p^{i+k}} \right\rangle$. De forma análoga, conclui-se

a segunda parte da afirmação (3.15). Sendo assim, temos que

$$H = \left\langle x^{tp^{m-k}} y^{p^{n-k}}, x^{p^m} \right\rangle = \left\langle x^{tp^{m-k}} y^{p^{n-k}}, y^{p^n} \right\rangle. \tag{3.16}$$

Desejamos mostrar que as três classes de subgrupos que apresentamos até agora esgotam todos os possíveis subgrupos de $\mathcal{G}^l$. Para tanto, a discussão seguinte será útil. Sejam $g, h \in \mathcal{G}^l$, com $g = x^{tp^i} y^{p^j}$ e $h = x^{\tau p^\kappa} y^{p^\lambda}$ satisfazendo à hipótese cíclica. Nos interessa conhecer que tipo de relação é preservada entre os produtos gh e hg. Para tanto, começamos observando que a equação (3.7) implica que:

$$\begin{aligned} hg &= \left(x^{\tau p^\kappa} y^{p^\lambda}\right)\left(x^{tp^i} y^{p^j}\right) = x^{\tau p^\kappa}\left(x^{tp^{i+\lambda+r-s+l}} x^{tp^i} y^{p^\lambda}\right) y^{p^j} \\ &= x^{tp^{i+\lambda+r-s+l}} x^{tp^i}\left(x^{\tau p^\kappa} y^{p^j}\right) y^{p^\lambda} \\ &= x^{tp^{i+\lambda+r-s+l}} x^{tp^i}\left(x^{-\tau p^{\kappa+j+r-s+l}} y^{p^j} x^{\tau p^\kappa}\right) y^{p^\lambda} \\ &= x^{\left(tp^{i+\lambda} - \tau p^{\kappa+j}\right)p^{r-s+l}} gh, \\ \Rightarrow hg &= \gamma gh \end{aligned} \tag{3.17}$$

onde definimos γ como

$$\gamma = x^{\left(tp^{i+\lambda} - \tau p^{\kappa+j}\right)p^{r-s+l}}.$$

Vamos analisar o termo γ. Se $\min\{i+\lambda,\, \kappa+j\} \geq s-l$, então $gh = hg$ pois neste caso $\gamma = e$. Assim, suponhamos que $\min\{i+\lambda,\, \kappa+j\} < s-l$. Se $i+\lambda \leq \kappa+j$, reescrevemos γ como

$$\gamma = \left(x^{tp^{r-s+l+i+\lambda}}\right)^\beta,$$

com $\beta = 1 - t^{-1}\tau p^{\kappa+j-(i+\lambda)}$. Como $r-s+l \geq s$, temos que $i+\lambda+r-s+l \geq i+s-j$; temos ainda que $i+\lambda < s-l$, o que implica que $r-i > s-j$. Assim, podemos

mostrar, utilizando (3.9), que

$$\begin{aligned} x^{tp^{i+\lambda+r-s+l}} &= \left(x^{tp^i}y^{p^j}\right)^{p^{\lambda+r-s+l}} \\ \Rightarrow \gamma &= g^{\beta p^{\lambda+r-s+l}} \\ \Rightarrow hg &= g^{1+\beta p^{\lambda+r-s+l}}h \end{aligned} \tag{3.18}$$

Antes de tratar o caso em que $\kappa + j < i + \lambda$, observamos que a equação (3.7) nos permite demonstrar que $x^{p^{r-s+l}}y = yx^{p^{r-s+l}}$, o que implica que $x^{p^{r-s+l}}$ comuta com qualquer elemento de $\mathcal{G}^l$. Sendo assim, pela equação (3.17), temos que $hg = gh\gamma$. Suponhamos agora que $\kappa + j < i + \lambda$. Por um argumento semelhante ao anterior concluímos que

$$hg = gh^{1+\delta p^{j+r-s+l}}, \tag{3.19}$$

onde $\delta = \tau^{-1}tp^{i+\lambda-(\kappa+j)} - 1$.

As equações (3.18) e (3.19) continuam válidas se tomarmos quaisquer $g, h \in \mathcal{G}^l$, pois pelo Lema 3.2.1 podemos considerar $g = x^{\eta tp^i}y^{\eta p^j}$ e $h = x^{\mu\tau p^\kappa}y^{\mu p^\lambda}$ e a introdução dos parâmetros μ e η não interfere no algebrismo desenvolvido acima. Da discussão que acabamos de fazer segue o seguinte lema.

Lema 3.2.4 Sejam $g, h \in \mathcal{G}^l$, com $g = x^{\eta tp^i}y^{\eta p^j}$ e $h = x^{\mu\tau p^\kappa}y^{\mu p^\lambda}$, tais que $x^{tp^i}y^{p^j}, x^{\tau p^\kappa}y^{p^\lambda}$ satisfaçam à hipótese cíclica. Sob essas condições temos que

(i) Se $\min\{i + \lambda,\ \kappa + j\} \geq s - l$, então $gh = hg$.

(ii) Se $i + \lambda \leq \kappa + j$, então $hg = g^{1+\beta p^{\lambda+r-s+l}}h$, onde $\beta = 1 - t^{-1}\tau p^{\kappa+j-(i+\lambda)}$.

(iii) Se $\kappa + j < i + \lambda$, então $hg = gh^{1+\delta p^{j+r-s+l}}$, onde $\delta = \tau^{-1}tp^{i+\lambda-(\kappa+j)} - 1$.

(iv) $\langle g, h\rangle = \{g^n h^m;\ 0 \leq n < |g|,\ 0 \leq m < |h|\} = \langle g\rangle\langle h\rangle$.

■

Uma das possibilidades que o Lema 3.2.4 nos abre é o cálculo da ordem de um subgrupo gerado por dois elementos. De fato, se $H = \langle g, h\rangle$, então $|H| = |\langle g\rangle||\langle h\rangle|/|\langle g\rangle \cap \langle h\rangle|$. Como conhecemos $|g|$ para qualquer $g \in \mathcal{G}^l$, resta apenas

determinar a ordem de $\langle g\rangle \cap \langle h\rangle$. Esta interseção também é simples de ser calculada, pois conhecemos a completa caracterização dos subgrupos cíclicos de $\mathcal{G}^l$ dada nos Lemas 3.2.1 e 3.2.2.

A proposição seguinte mostra que qualquer subgrupo de $\mathcal{G}^l$ pode ser gerado por um conjunto com, no máximo, dois geradores. Este é o último obstáculo a transpormos antes de podermos caracterizar completamente os subgrupos de $\mathcal{G}^l$. Antes de a enunciarmos, vamos fazer algumas observações para tornar a sua demonstração mais *limpa*. Pelo Lema 3.2.1, temos que dado um elemento qualquer $g \in \mathcal{G}^l$, existe um elemento $x^{tp^i}y^{p^j} \in \mathcal{G}^l$ satisfazendo à hipótese cíclica, tal que $\langle g\rangle = \left\langle x^{tp^i}y^{p^j}\right\rangle$. Além disso, o item (iv) do Lema 3.2.4 nos assegura que $\langle g, h\rangle = \langle g\rangle\langle h\rangle$. Combinando esses dois resultados, ao tratarmos de subgrupos de $\mathcal{G}^l$ com dois geradores, podemos sempre considerar, sem perda de generalidade, que estes geradores satisfazem à hipótese cíclica. Vamos à proposição.

Proposição 3.2.1 Qualquer subgrupo de $\mathcal{G}^l$ pode ser gerado por um conjunto com, no máximo, dois geradores.

Demonstração: Para provarmos a proposição, basta mostrarmos que se um subgrupo de $\mathcal{G}^l$ é gerado por 3 elementos, então existem dois elementos no subgrupo que também o geram. De fato, suponhamos provada esta afirmação. Seja $H \leq \mathcal{G}^l$, com $H = \langle g_1, g_2, g_3, g_4\rangle$. Podemos tomar $H' = \langle g_1, g_2, g_3\rangle \leq H$. Pelo que estamos assumindo verdadeiro, existem $g_1', g_2' \in H'$ tais que $H' = \langle g_1', g_2'\rangle$. Desta forma, $H = \langle g_1', g_2', g_4\rangle$. Novamente aplicando o resultado, reduzimos o número de geradores de H para 2. Este argumento se aplica a subgrupos gerados por um número qualquer de geradores, o que comprova a afirmação inicial.

Sendo assim, seja $H = \langle g_1, g_2, g_3\rangle \leq \mathcal{G}^l$. Vamos demonstrar que existe um desses geradores que pertence ao subgrupo gerado pelos dois outros. Pelo discutido no parágrafo que antecede esta proposição, podemos assumir que $g_1 = x^{tp^i}y^{p^j}$, $g_2 = x^{\tau p^\kappa}y^{p^\lambda}$ e $g_3 = x^{up^m}y^{p^n}$ são distintos e satisfazem à hipótese cíclica. Podem ocorrer duas possibilidades em relação aos parâmetros i, κ, m e j, λ, n. Na primeira delas, consideramos que $i = \kappa = m$ e $j = \lambda = n$. Na segunda, pode-se escolher entre os

elementos i, κ, m e j, λ, n um elemento que é estritamente menor que os demais, por exemplo $i < \kappa, m$ ou $\lambda < j, n$.

No primeiro caso, os parâmetros t, τ e u desempenham papel fundamental. Como g_1, g_2, g_3 são distintos, certamente t, τ e u o são. Consideremos as diferenças $u-t$, $u-\tau$ e $t-\tau$. Se quaisquer duas dessas três diferenças forem divisíveis por p, então a terceira delas também o será. Equivalentemente, se uma delas for coprima com p, então deverá existir uma segunda diferença, também coprima. Para que um dos geradores, digamos g_3, pertença ao grupo gerado pelos demais, $\langle g_1, g_2 \rangle$, devemos ser capazes de mostrar que existem M, N inteiros tais que $g_3 = g_1^M g_2^N$. Pelo Lema 3.2.1, isso equivale a mostrar que M, N são tais que

$$x^{up^i} y^{p^j} = x^{\left(tM+\tau N\left(Mp^{r-s+l+j}+1\right)\right)p^i} y^{(M+N)p^j}.$$

Equivalentemente, temos o sistema de equações

$$\begin{cases} tM + \tau N + \tau NMp^{r-s+l+j} - u & \equiv & 0 \bmod p^{r-i} \\ M + N - 1 & \equiv & 0 \bmod p^{s-\lambda} \end{cases} \tag{3.20}$$

Este sistema de equações de congruência, é equivalente à equação abaixo

$$(\tau - t)N + (t - u) + tqp^{s-j} + \tau NMp^{r-s+l+j} \equiv 0 \bmod p^{r-i}. \tag{3.21}$$

Se p divide as diferenças $\tau - t$, $\tau - u$ e $t - u$, sejam $\tau - t = T_1 p^{\delta_1}$ e $t - u = T_2 p^{\delta_2}$ com $\text{mdc}\,(T_1, p) = \text{mdc}\,(T_2, p) = 1$. Suporemos que $\delta_1 \leq \delta_2$, o que podemos fazer sem perda de generalidade. Neste caso, a equação (3.21) se reescreve como

$$T_1 N p^{\delta_1} + T_2 p^{\delta_2} + tqp^{s-j} + \tau NMp^{r-s+l+j} - u \equiv 0 \bmod p^{r-i}.$$

Caso $\delta_1 < s - j$ a equação acima é equivalente a

$$T_1 N + T_2 p^{\delta_2 - \delta_1} + tqp^{s-j-\delta_1} + \tau NMp^{r-s+l+j-\delta_1} - u \equiv 0 \bmod p^{r-i-\delta_1}, \tag{3.22}$$

onde estamos assumindo que $r-i > s-j$ (o caso em que $r-i \leq s-j$, é análogo). Definindo $P(N) = T_1N + T_2p^{\delta_2-\delta_1} + tqp^{s-j-\delta_1} + \tau NMp^{r-s+l+j-\delta_1} - u$, temos que $P(N) \equiv T_1N + T_2 \bmod p$, se $\delta_1 = \delta_2$, ou $P(N) \equiv T_1N \bmod p$, se $\delta_1 > \delta_2$. Em qualquer caso, existe N_0 tal que $P(N_0) \equiv 0 \bmod p$, Hefes (2006). Além disso, se $P'(N)$ denota a derivada formal do polinômio $P(N)$, temos em ambos os casos que $P'(N) \equiv T_1 \bmod p$, portanto $P'(N) \not\equiv 0 \bmod p$. Desta forma, o Lema de Hensel, Gouvêa (1997); Eisenbud (1995), nos garante que existe solução para a equação (3.22), o que implica que existe solução para o sistema (3.20).

Se por outro lado, for $\delta_1 \geq s-j$, temos diretamente que $g_3 \in \langle g_1 \rangle$. De fato, $g_3 \in \langle g_1 \rangle$ se, e somente se, existir M tal que $x^{up^i}y^{p^j} = x^{tMp^i}y^{Mp^j}$. Equivalentemente, temos $t-u = qp^{\min(r-i,s-j)}$. Como $\delta_1 \leq \delta_2$, temos que $t-u = T_2p^{\delta_2}\tilde{T}_2p^{s-j}$ e, assim, segue que afirmação é verdadeira.

Devemos tratar agora, o caso em que existam duas das diferenças $\tau-t$, $\tau-u$ e $t-u$, coprimas com p, que suporemos ser $\tau-t$ e $t-u$. Definindo

$$P(N) = (\tau-t)N + (t-u) + tqp^{s-j} + \tau NMp^{r-s+l+j}$$

temos que $P(N) \equiv (\tau-t)N+(t-u) \bmod p$. Desta forma, a equação de congruência $P(N_0) \equiv 0 \bmod p$ tem uma solução N_0 Hefes (2006) e como $P'(N) \equiv \tau-t \bmod p$, temos que $P'(N) \not\equiv 0 \bmod p$. Pelo Lema de Hensel, garantimos solução para o sistema de equações (3.20). Fica assim estabelecido que se $i = \kappa = m$ e $j = \lambda = n$, então um dos três geradores de H pertence ao grupo gerado pelos outros dois.

Na seqüência da prova, podemos supor que entre i, κ, m e j, λ, n pode-se escolher um elemento que é estritamente menor que os demais. Há um número bastante grande de possibilidades, por exemplo: $i < \kappa, m$ e $j = \lambda = n$; ou $i < \kappa, m$ e $j < \lambda, n$; ou $i = \kappa = m$ e $j < \lambda, n$; etc. O argumento da prova, em qualquer caso, será sempre o mesmo, mostrar que a partir do sistema de equações de congruências inicial, recaímos numa equação de congruência que satisfaz às hipóteses do Lema de Hensel. Desta forma, apresentaremos a prova apenas no caso em que $i < \kappa, m$ e que $\lambda \leq j, n$. Sob essas hipóteses, afirmamos que $g_3 \in \langle g_1, g_2 \rangle$. Para que a afirmação

seja verdadeira, devemos mostrar que existem $M, N \in \mathbb{N}$ tais que $g_3 = g_1^M g_2^N$. Esta identidade é equivalente ao sistema de equações de congruência abaixo, que devemos garantir ter solução.

$$\begin{cases} tM + \tau N p^{\kappa-i} + \tau MN p^{r-s+l+j+\kappa-i} - up^{m-i} & \equiv & 0 \mod p^{r-i} \\ Mp^{j-\lambda} + N - p^{n-\lambda} & \equiv & 0 \mod p^{s-\lambda} \end{cases} . \tag{3.23}$$

O sistema (3.23) é equivalente à equação

$$tM + \tau\left(qp^{s-\lambda} - Mp^{j-\lambda} - N + p^{n-\lambda}\right)p^{\kappa-i} + \tau MN p^{r-s+l+j+\kappa-i} - up^{m-i} \equiv 0 \mod p^{r-i}.$$

Pondo

$$P(M) = tM + \tau\left(qp^{s-\lambda} - Mp^{j-\lambda} - N + p^{n-\lambda}\right)p^{\kappa-i} + \tau MN p^{r-s+l+j+\kappa-i} - up^{m-i},$$

podemos verificar que $P(M)$ é tal que $P(0) \equiv 0 \mod p$ e $P'(0) \not\equiv 0 \mod p$. Desta forma, novamente aplicamos o Lema de Hensel para garantir que existe um inteiro M_0 tal que $P(M_0) \equiv 0 \mod p^{r-i}$. Assim, existe solução para o sistema de equações de congruência (3.23). Portanto, existem M e N tais que $g_3 = g_1^M g_2^N$. Fica assim demonstrada a proposição.

■

Na verdade, demonstramos um pouco mais do que enunciamos na proposição. De fato, mostramos que qualquer subgrupo gerado por um conjunto de geradores com mais de dois elementos, pode ser gerado por um subconjunto desse conjunto de geradores, com apenas dois elementos, ou equivalentemente, que dados três elementos quaisquer de $\mathcal{G}^l$, um deles pertence ao subgrupo gerado pelos outros dois. Observe que este conjunto de geradores, pode ainda ser redundante, pois existem os subgrupos cíclicos.

Neste ponto, podemos caracterizar completamente os subgrupos de $\mathcal{G}^l$, exibindo seus geradores em função de x e y. Faremos isso no

Teorema 3.2.1 Os subgrupos de $\mathcal{G}^l$ são classificados da seguinte forma:

(i) $\left\langle x^{tp^i}y^{p^j}\right\rangle$ onde $x^{tp^i}y^{p^j}$ satisfaz a hipótese cíclica.

(ii) $\left\langle x^{p^i}, y^{p^j}\right\rangle$, $0 \leq i < r$, $0 \leq j < s$;

(iii) $\left\langle x^{tp^i}y^{p^j}, x^{p^{i+k}}\right\rangle = \left\langle x^{tp^i}y^{p^j}, y^{p^{j+k}}\right\rangle$, $0 \leq i < r-1$, $0 \leq j < s-1$, $0 < k < m'$ e $t \in \mathbb{Z}_{p^k}^*$.

Demonstração: Se H é um subgrupo de $\mathcal{G}^l$ com um único gerador, o Lema 3.2.2 nos garante que H pertence à classe (i). Assim, tendo em vista a Proposição 3.2.1, suponhamos que H seja gerado por dois elementos $g = x^{tp^i}y^{p^j}$, $h = x^{\tau p^\kappa}y^{p^\lambda} \in \mathcal{G}^l$ satisfazendo à hipótese cíclica. Demonstraremos que H pertence a uma das três classes descritas no teorema. Suponhamos inicialmente que $\kappa \geq i$ e $\lambda \leq j$. Escrevendo $\kappa = i + \kappa'$ e $j = \lambda + j'$, temos

$$g = x^{tp^i}y^{p^j} = \left(x^{p^i}\right)^t \left(y^{p^\lambda}\right)^{p^{j'}},\ h = x^{\tau p^\kappa}y^{p^\lambda} = \left(x^{p^i}\right)^{tp^{\kappa'}} y^{p^\lambda},$$

o que implica $g, h \in \left\langle x^{p^i}, y^{p^j}\right\rangle$, logo $H \leq \left\langle x^{p^i}, y^{p^\lambda}\right\rangle$. Mostraremos que $H = \left\langle x^{p^i}, y^{p^\lambda}\right\rangle$ e, portanto, pertence à classe (ii). Para tanto, calcularemos a ordem do subgrupo H que é dada por $|H| = |g||h|/|\langle g\rangle \cap \langle h\rangle|$, mostrando que ela é igual à $\left|\left\langle x^{p^i}, y^{p^\lambda}\right\rangle\right| = p^{r+s-(i+\lambda)}$.

Se $r-\kappa \geq s-\lambda$ necessariamente $r-i \geq s-j$ e, assim, $|g| = p^{r-i}$, $|h| = p^{r-\kappa}$. Além disso, $\langle g\rangle \cap \langle h\rangle = \left\langle x^{p^{\kappa+s-\lambda}}\right\rangle$. De fato, como $\kappa + s - \lambda \geq i + s - j$, segue que $\left\langle x^{p^{\kappa+s-\lambda}}\right\rangle = (\langle g\rangle \cap \langle h\rangle) \cap \langle x\rangle$, portanto, $\left\langle x^{p^{\kappa+s-\lambda}}\right\rangle \leq \langle g\rangle \cap \langle h\rangle$. Se existirem $0 < \eta, \eta' < p^{s-\lambda}$ tais que $x^{t\eta p^i}y^{\eta p^j} = x^{\tau\eta' p^\kappa}y^{\eta' p^\lambda}$, $(y^{\eta p^j} \neq e \neq y^{\eta' p^\lambda})$, então

$$\begin{cases} t\eta p^i \equiv \tau\eta' p^\kappa \mod p^r \\ \eta p^j \equiv \eta' p^\lambda \mod p^s \end{cases} \Leftrightarrow \begin{cases} \eta \equiv u\eta' p^{\kappa-i} \mod p^{r-i} \\ \eta p^{j-\lambda} \equiv \eta' \mod p^{s-\lambda} \end{cases}.$$

onde $u = t^{-1}\tau$. Como $r - i \geq r - \kappa \geq s - \lambda$, temos

$$\begin{cases} \eta \equiv u\eta' p^{\kappa-i} \mod p^{s-\lambda} \\ \eta p^{j-\lambda} \equiv \eta' \mod p^{s-\lambda} \end{cases} \Rightarrow \begin{cases} \eta - u\eta' p^{\kappa-i} = q_1 p^{s-\lambda} \\ \eta p^{j-\lambda} - \eta' = q_2 p^{s-\lambda} \end{cases}$$

O último sistema nos dá a equação $\eta'\left(up^{\kappa+j-(i+\lambda)}-1\right)=\left(q_2-q_1p^{j-\lambda}\right)p^{s-\lambda}$, que nos conduz a um absurdo, pois $p^{s-\lambda}\nmid\eta'$ e $p^{s-\lambda}\nmid\left(up^{\kappa+j-(i+\lambda)}-1\right)$. Logo, não existem tais η e η',$\langle g\rangle\cap\langle h\rangle=\left\langle x^{p^{\kappa+s-\lambda}}\right\rangle$ e, portanto, $|H|=p^{r+s-(i+\lambda)}$ o que implica $H=\left\langle x^{p^i},y^{p^\lambda}\right\rangle$.

Há outras duas possibilidades a serem consideradas, ainda sob a suposição que $\kappa\geq i$ e $\lambda\leq j$: (1) $r-\kappa<s-\lambda$ e $r-i<s-j$; (2) $r-\kappa\geq s-\lambda$ e $r-i<s-j$. Em ambos os casos, temos $|H|=p^{r+s-(i+\lambda)}$ e, portanto, $H=\left\langle x^{p^i},y^{p^\lambda}\right\rangle$. As provas são análogas ao caso tratado anteriormente.

Podemos supor, agora, que $\kappa>i$ e $\lambda>j$. Se $r-i\geq s-j$ e $\kappa\geq i+s-j$ podemos escrever $\kappa=i+s-j+\kappa'$ e

$$h=x^{\tau p^\kappa}y^{p^\lambda}=\left(\left(x^{tp^i}\right)^{p^{s-j}}\right)^{t^{-1}\tau p^{\kappa'}}y^{p^\lambda}=\left(x^{tp^i}y^{p^j}\right)^{t^{-1}\tau p^{s-j+\kappa'}}y^{p^\lambda},$$

o que implica $h\in\left\langle g,y^{p^\lambda}\right\rangle$, $y^{p^\lambda}\in H$ e, desta forma, $H=\left\langle g,y^{p^j}\right\rangle$. Pelo Lema 3.2.3 e pela discussão que o precede, temos que H pertence a uma das três classes de subgrupos do teorema.

Se agora for $r-i\geq s-j$ e $i<\kappa<i+s-j$, note que deve ser $s-j>1$, podemos escrever $\kappa=i+\kappa'$ com $0<\kappa'<s-j$. Como $j<\lambda$, também podemos escrever $\lambda=j+\lambda'$. Pondo $k=\min\{\kappa',\lambda'\}$, afirmamos que $H=\left\langle g,x^{p^{i+k}}\right\rangle=\left\langle g,y^{p^{j+k}}\right\rangle$ e, portanto, pertence à classe (iii). Vamos provar esta afirmação. Como $k\leq\kappa'$ e $k\leq\lambda'$, podemos escrever $\kappa=i+k+\delta_\kappa$ e $\lambda=j+k+\delta_\lambda$, onde $\delta_\kappa=\kappa'-\lambda'$, $\delta_\lambda=0$ se $\kappa'\geq\lambda'$ e $\delta_\kappa=0$, $\delta_\lambda=\lambda'-\kappa'$ se $\kappa'<\lambda'$. Assim

$$h=\left(x^{p^{i+k}}\right)^{tp^{\delta_\kappa}}\left(p^{j+k}\right)^{p^{\delta_\lambda}}\in\left\langle g,x^{p^{i+k}}\right\rangle.$$

Logo, $H\leq\left\langle g,x^{p^{i+k}}\right\rangle$. Voltamos nossa atenção para a ordem de H que é dada por $|H|=p^{r-i}|h|/|\langle g\rangle\cap\langle h\rangle|$. Se $r-\kappa\geq s-\lambda$, então $|h|=p^{r-\kappa}$ e $\kappa+s-\lambda=i+s+j+(\delta_\kappa-\delta_\lambda)$. Assim, $\kappa+s-\lambda\geq i+s+j$ se $\kappa'\geq\lambda'$ e $\kappa+s-\lambda<i+s+j$ se $\kappa'<\lambda'$, o que implica que $\langle g\rangle\cap\langle h\rangle=\left\langle x^{p^{\kappa+s-\lambda}}\right\rangle$ se $\kappa'\geq\lambda'$ e $\langle g\rangle\cap\langle h\rangle=\left\langle x^{p^{i+s-j}}\right\rangle$ se $\kappa'<\lambda'$. Logo, $|H|=p^{r+s-(i+\lambda)}$ se $\kappa'\geq\lambda'$ e $|H|=p^{r+s-(\kappa+j)}$ se $\kappa'<\lambda'$. Porém,

se $\kappa' \geq \lambda'$ temos $\lambda = j + k$ e se $\kappa' < \lambda'$ temos $\kappa = i + k$. Em qualquer caso, $|H| = p^{r+s-(i+j+k)} = \left|\left\langle g, x^{p^{i+k}} \right\rangle\right|$, provando que $H = \left\langle g, x^{p^{i+k}} \right\rangle$ caso $r - \kappa \geq s - \lambda$. Caso seja $r - \kappa < s - \lambda$, $\langle g \rangle \cap \langle h \rangle = \{e\}$ e $|h| = p^{s-\lambda}$. Assim, $|H| = p^{r+s-(i+\lambda)}$. Mas

$$s - j - \lambda' = s - \lambda > r - \kappa = r - i - \kappa' \geq s - j - \kappa' \Rightarrow \kappa' > \lambda' \Rightarrow \delta_\lambda = 0.$$

Logo, $\lambda = j+k+\delta_\lambda = j+k$ e, assim, $|H| = p^{r+s-(i+j+k)}$. Portanto, $H = \left\langle g, x^{p^{i+k}} \right\rangle$. O caso em que $r - i < s - j$ é análogo ao caso $r - i \geq s - j$. Encerramos, assim, a prova do teorema.

■

Note que a classificação dos subgrupos de $\mathcal{G}^l$ não depende do particular valor de l. Isso significa que, como conjunto de elementos, esses subgrupos são os mesmos, qualquer que seja l. A classificação do Teorema 3.2.1 será a ferramenta fundamental para a solução do PSO em $\mathcal{G}^l$. De fato, veremos que ela nos permitirá reduzir, na maioria dos casos, o PSO em $\mathcal{G}^l$ para instâncias do PSO abeliano. Quando isso não for possível, o conhecimento da estrutura dos subgrupos irá nos permitir construir um algoritmo capaz de obter os parâmetros que determinam o subgrupo oculto.

Um outro aspecto importante que decorre do Teorema 3.2.1 é o domínio de variação dos parâmetros que definem os subgrupos. Os parâmetros i, j e k variam entre 0 e no máximo r, ao passo que o parâmetro t pode variar, num pior caso, entre 0 e p^s. Desta forma, vemos que enquanto i, j e k estão em um domínio da ordem de $(r+s)\log p = \log\left|\mathcal{G}^l\right|$, t está em um domínio que é da ordem de $O\left(\left|\mathcal{G}^l\right|\right)$. Este fato, t estar em um domínio muito grande, inviabiliza uma tentativa direta de solução do PSO em $\mathcal{G}^l$, por uma estratégia de busca de todas as possibilidades, testando um a um todos os possíveis subgrupos de $\mathcal{G}^l$, pois neste caso o número de chamadas à função separadora de classes seria da ordem de $\left|\mathcal{G}^l\right|$, portanto um método ineficiente.

3.3 Propriedades dos Subgrupos de $\mathcal{G}^l$

Reunimos nesta seção algumas propriedades importantes dos subgrupos de $\mathcal{G}^l$ que nos serão úteis no decorrer do trabalho. Começamos observando que somos capazes de decidir quando um subgrupo de $\mathcal{G}^l$ é ou não cíclico. Na observação seguinte, mostramos como fazer esta distinção.

Observação 3.3.1 Dado $H \leq \mathcal{G}^l$, considere $H_x = \left\langle x^{p^m} \right\rangle$ e $H_y = \left\langle y^{p^n} \right\rangle$, como definidos na Definição 3.2.2. Pela análise que fizemos a respeito dos subgrupos com dois geradores, em especial nas equações (3.15) e (3.16), decorre que se $m < r$ e $n < s$, então H é gerado por dois elementos e: ou $H = \left\langle x^{p^m}, y^{p^n} \right\rangle$ ou $H = \left\langle x^{tp^{m-k}} y^{p^{n-k}}, y^{p^n} \right\rangle = \left\langle x^{tp^{m-k}} y^{p^{n-k}}, x^{p^m} \right\rangle$ com $0 < k \leq \min\{m, n\}$ e $t \in \mathbb{Z}^*_{p^k}$. Note que caso $m = 0$ ou $n = 0$, podemos assegurar que $H = \left\langle x^{p^m}, y^{p^n} \right\rangle$, pois neste caso $\min\{m, n\} = 0$.

Das equações (3.13) e (3.14), temos que se $m < r$ e $n = s$, então $H = \left\langle x^{tp^{m-s+j}} y^{p^j} \right\rangle$ com $0 \leq j \leq s$, $t \in \mathbb{Z}^*_{p^{s-j}}$ se $j \neq s$ ou $t = 1$ se $j = s$ e $s - j \leq m$. Caso $m = r$ e $n < s$, então $H = \left\langle x^{tp^{r-n+j}} y^{p^j} \right\rangle$, $0 \leq j \leq n$ e $t \in \mathbb{Z}^*_{p^{n-j}}$ se $j \neq n$ ou $t = 1$ se $j = n$. Por fim, se $m = r$ e $n = s$, então $H = \left\langle x^{tp^{r-s+j}} y^{p^j} \right\rangle$ com $0 \leq j < s$ e $t \in \mathbb{Z}^*_{p^{s-j}}$ ou $H = \{e\}$. ∎

Do ponto de vista computacional, os parâmetros m e n representam uma grande vantagem, pois como $\mathbb{Z}_{p^r} \simeq \langle x \rangle$ e $\mathbb{Z}_{p^s} \simeq \langle y \rangle$ são grupos abelianos, m e n podem ser determinados eficientemente, supondo que $\left\langle x^{p^m} \right\rangle$ seja oculto em $\mathbb{Z}_{p^r}$ e que $\left\langle y^{p^n} \right\rangle$ seja oculto em $\mathbb{Z}_{p^s}$. A Observação 3.3.1 mostra que o conhecimento de m e n permite que alguns dos parâmetros que definem o subgrupo sejam eliminados. De fato, caso H seja cíclico, o parâmetro i é eliminado, enquanto no caso dos grupos não cíclicos, os parâmetros i e j o são. Em qualquer caso, restarão sempre dois parâmetros a serem determinados.

Na seqüência do trabalho, vamos caracterizar os subgrupos normais de $\mathcal{G}^l$. Relembrando, um subgrupo N de G é normal se para todo $g \in G$, $gN = Ng$. Começamos pelos subgrupos da classe (i). Seja $H = \left\langle x^{tp^i} y^{p^j} \right\rangle$. Como x e y

geram o grupo $\mathcal{G}^l$, temos que o subgrupo H será normal se, e somente se, existirem $g, h \in H$ tais que $x\left(x^{tp^i}y^{p^j}\right) = gx$ e $y\left(x^{tp^i}y^{p^j}\right) = hy$. Segue que

$$x\left(x^{tp^i}y^{p^j}\right) = x^{tp^i}y^{p^j}x^{-p^{r-s+l+j}}x.$$

Se definimos $g = x^{tp^i}y^{p^j}x^{-p^{r-s+l+j}}$, temos que $g \in H$ se, e somente se, $x^{-p^{r-s+l+j}} \in H$. Caso $r-i < s-j$, $x^{-p^{r-s+l+j}} \notin H$ e, assim, H não é normal. Se for $r-i \geq s-j$, devemos ter $r-s+l+j \geq i+s-j$ o que é equivalente a $r-i \geq 2(s-j)-l$. Além disso,

$$y\left(x^{tp^i}y^{p^j}\right) = x^{tp^{r-s+l+i}}x^{tp^i}y^{p^j}y.$$

Se definimos $h = x^{tp^{r-s+l+i}}x^{tp^i}y^{p^j}$, então $h \in H$ se, somente se, $x^{p^{r-s+l+i}} \in H$. Desta forma, devemos ter $r-s+l+i \geq i+s-j$ o que é equivalente a $r-s+l \geq s-j$. Mas como $r \geq 2s-l$, temos $r-s+l \geq s \geq s-j$, portanto, $h \in H$ em qualquer caso. Concluímos que

$$H = \left\langle x^{tp^i}y^{p^j} \right\rangle \text{ é normal } \Leftrightarrow r-i \geq \max\{2(s-j)-l, s-j\}. \tag{3.24}$$

Vejamos agora os subgrupos da classe (ii). Considere $H = \left\langle x^{p^i}, y^{p^j} \right\rangle$. O subgrupo H será normal se, e somente se, existirem $g, h \in H$ tais que $yx^{p^i} = gy$ e $xy^{p^j} = hx$. Temos que $yx^{p^i} = x^{p^i(p^{r-s+l}+1)}y$ e, obviamente, $x^{p^i(p^{r-s+l}+1)} \in H$. Observe agora que $xy^{p^j} = x^{-(p^{r-s+l}+1)}y^{p^j}$. Sendo $\text{mdc}\left(p^{r-s+l}+1, p\right) = 1$, segue que $x^{-(p^{r-s+l}+1)} \in H$ se, e somente se, $i = 0$. Logo:

$$H = \left\langle x^{p^i}, y^{p^j} \right\rangle \text{ é normal } \Leftrightarrow i = 0. \tag{3.25}$$

Por fim, para os subgrupos da classe (iii), se $H = \left\langle x^{tp^i}y^{p^j}, x^{p^{i+k}} \right\rangle$, verifica-se que

$$H \text{ é normal } \Leftrightarrow r-s+l \geq i+k-j. \tag{3.26}$$

Os lemas seguintes descrevem o comportamento das classes laterais de subgrupos de $\mathcal{G}^l$, quando calculamos sua interseção com certos subconjuntos de $\mathcal{G}^l$. Suponhamos que exista m tal que $r-s+l<m<2s-l$. Esta suposição, que por hora pode parecer sem propósito, ficará clara quando utilizarmos os resultados dos lemas mais à frente. Sejam os subgrupos K_j^t definidos por

$$K_j^t = \left\langle x^{tp^{m-s+j}} y^{p^j} \right\rangle \tag{3.27}$$

onde $0 \leq j \leq s$ e $t \in \mathbb{Z}^*_{p^{s-j}}$ se $j \neq s$ ou $t = 1$ se $j = s$. Caso H seja um subgrupo cíclico de $\mathcal{G}^l$ tal que $H_x = \left\langle x^{p^m} \right\rangle$, temos que $H = K_j^t$ para algum par j, t. Considere agora

$$T_j = \left\{ x^a y^b;\ 0 \leq a < p^m,\ 0 \leq b < p^j \right\}. \tag{3.28}$$

Temos que T_j é uma transversal[2] de K_j^t para qualquer t e em virtude do Lema 3.2.1, para qualquer $x^a y^b \in T_j$ segue que

$$x^a y^b K_j^t = \left\{ x^{a+t\kappa p^{m-s+j}\left(bp^{r-s+l}+1\right)} y^{b+\kappa p^j};\ 0 \leq \kappa < p^{r+s-m-j} \right\}. \tag{3.29}$$

Sob essas condições, prova-se o seguinte lema

Lema 3.3.1 Seja $L = \{x^a y^b;\ 0 \leq a < p^m, 0 \leq b < p^s\}$. Dado $x^a y^b \in T_j$, considere o conjunto $N = \left\{ x^{\left(a+t\kappa p^{m-s+j}\right) \bmod p^m} y^{b+\kappa p^j};\ 0 \leq \kappa < p^{s-j} \right\}$. Então $\left(x^a y^b K_j^t\right) \cap L = N$ quaisquer que sejam j e t.

Demonstração: Sejam $x^a y^b \in T_j$ e $g \in \left(x^a y^b K_j^t\right) \cap L$. Como $g \in x^a y^b K_j^t$, temos $g = x^{a+t\kappa' p^{m-s+j}\left(bp^{r-s+l}+1\right)} y^{b+\kappa' p^j}$ com $0 \leq \kappa' < p^{r+s-m-j}$. Por outro lado, como $g \in L$, temos $g = x^{a'} y^{b'}$ com $0 \leq a' < p^m$ e $0 \leq b' < p^s$. Podemos escrever $\kappa' = qp^{s-j} + \kappa$, com $0 \leq \kappa < p^{s-j}$. Assim, podemos reescrever $g = x^{a+t\kappa p^{m-s+j}+\gamma p^m} y^{b+\kappa p^j}$,

[2] Um conjunto completo de representantes das classes laterais de um dado subgrupo no grupo.

onde $\gamma = t\left(q\left(bp^{r-s+l}+1\right)+\kappa p^{r-2s+l+j}\right)$. Desta forma,

$$\begin{cases} a + t\kappa p^{m-s+j} + \gamma p^m \equiv a' \bmod p^r \\ b + \kappa p^j \equiv b' \bmod p^s \end{cases} \Rightarrow \begin{cases} a + t\kappa p^{m-s+j} \equiv a' \bmod p^m \\ b + \kappa p^j \equiv b' \bmod p^s \end{cases}.$$

Como $a' < p^m$ e $b', b+\kappa p^j < p^s$ segue que $a' = (a + t\kappa p^{m-s+j}) \mod p^m$ e $b' = b+\kappa p^j$ com $0 \leq \kappa < p^{s-j}$. Logo, $g \in N \Rightarrow \left(x^a y^b K_j^t\right) \cap L \subset N$.

Para a inclusão inversa, começamos notando que $N \subset L$. Seja, agora, $g = x^{\left(a+t\kappa p^{m-s+j}\right) \bmod p^m} y^{b+\kappa p^j} \in N$. Podemos escrever $(a + t\kappa p^{m-s+j}) \mod p^m = a + t\kappa p^{m-s+j} + qp^m$, para algum q. Assim

$$\begin{aligned} g &= x^{a+t\kappa p^{m-s+j}+qp^m} y^{b+\kappa p^j} \\ &= x^{a+t\kappa p^{m-s+j}} x^{t\kappa b p^{m-s+j} p^{r-s+l}} x^{-t\kappa b p^{m-s+j} p^{r-s+l}} x^{qp^m} y^{b+\kappa p^j} \\ &= x^{a+t\kappa p^{m-s+j}\left(bp^{r-s+l}+1\right)} x^{\gamma p^m} y^{b+\kappa p^j} \\ &= x^{a+t\kappa p^{m-s+j}\left(bp^{r-s+l}+1\right)} y^{b+\kappa p^j} x^{\gamma p^m\left(-\left(b+\kappa p^j\right)p^{r-s+l}+1\right)} \\ &= \left(x^a y^b\right)\left(x^{t\kappa p^{m-s+j}} y^{\kappa p^j}\right)\left(x^{p^m}\right)^{\gamma\left(-\left(b+\kappa p^j\right)p^{r-s+l}+1\right)} \end{aligned}$$

onde $\gamma = q - t\kappa b p^{r-2s+l+j}$. Temos $x^{t\kappa p^{m-s+j}} y^{\kappa p^j} \in K_j^t$ e

$$x^{p^m} = \left(x^{tp^{m-s+j}}\right)^{t^{-1}p^{s-j}} = \left(x^{tp^{m-s+j}} y^{p^j}\right)^{t^{-1}p^{s-j}},$$

assim, $x^{p^m} \in K_j^t$. Portanto, $g \in x^a y^b K_j^t$ o que implica que $N \subset x^a y^b K_j^t$ e nos permite concluir que $N \subset \left(x^a y^b K_j^t\right) \cap L$, encerrando a prova.

■

Sejam agora m e n tais que $0 < m < 2s - l$ e $0 < n < s$. Considere os subgrupos K_k^t dados por

$$K_k^t = \left\langle x^{tp^{m-k}} y^{p^{n-k}}, x^{p^m} \right\rangle \tag{3.30}$$

onde $0 < k \leq \min\{m, n\}$ e $t \in \mathbb{Z}_{p^k}^*$. Novamente, se H é um subgrupo de $\mathcal{G}^l$ tal que $H_x = \langle x^{p^m} \rangle$ e $H_y = \langle x^{p^n} \rangle$, então $H = K_k^t$ para algum par k, t ou $H = \langle x^{p^m}, y^{p^n} \rangle$. Uma transversal para K_k^t é dada por

$$T_k = \{x^a y^b;\ 0 \leq a < p^m, 0 \leq b < p^{n-k}\}, \tag{3.31}$$

qualquer que seja t. Agora, pelos Lemas 3.2.3 e 3.2.1 temos que

$$x^a y^b K_k^t = \left\{ x^{a+t\kappa p^{m-k}\left(bp^{r-s+l}+1\right)} y^{b+\kappa p^{n-k}+\lambda p^n};\ 0 \leq \kappa < p^{r-m+k}, 0 \leq \lambda < p^{s-n} \right\}. \tag{3.32}$$

Sob essas condições, temos o lema

Lema 3.3.2 Seja $L = \{x^a y^b;\ 0 \leq a < p^m, 0 \leq b < p^n\}$. Dado $x^a y^b \in T_k$, considere o conjunto $N = \left\{ x^{(a+t\kappa p^{m-k}) \bmod p^m} y^{b+\kappa p^{n-k}};\ 0 \leq \kappa < p^k \right\}$. Então $\left(x^a y^b K_k^t\right) \cap L = N$ para todo par k, t.

Demonstração: É análoga à demonstração do Lema 3.3.1.

■

Note que o conjunto L definido no Lema 3.3.2 é uma transversal para o subgrupo $\langle x^{p^m}, y^{p^n} \rangle$, assim $\left(x^a y^b \langle x^{p^m}, y^{p^n} \rangle\right) \cap L = \{x^a y^b\}$ para todo $x^a y^b \in L$. Além disso, os lemas precedentes trazem a luz uma extraordinária propriedade do conjunto L. Pelos lemas, vemos que o conjunto L é subdividido em subconjuntos de mesma cardinalidade quando intersectado com as classes laterais dos subgrupos K_j^t no Lema 3.3.1 e K_k^t no Lema 3.3.2. Além disso, a caracterização das interseções nos possibilitará extrair a informação necessária para determinarmos o subgrupo oculto H no algoritmo que apresentaremos no Capítulo 4.

Capítulo 4

Algoritmo Quântico para o PSO em $\mathcal{G}^l$

Neste capítulo, apresentaremos um algoritmo eficiente para a solução do PSO em $\mathcal{G}^l$. Dado que conhecemos a estrutura dos subgrupos de $\mathcal{G}^l$, nosso algoritmo deve ser capaz de decidir a que classe de subgrupos, as classes descritas no Teorema 3.2.1, pertence o subgrupo oculto, bem como obter os coeficientes que o determinam.

Numa descrição geral e superficial, o algoritmo opera da seguinte maneira. Dada a função f, separadora de classes laterais do subgrupo oculto H, calculamos geradores para H_x e H_y através do PSO abeliano, restringindo f à $\mathbb{Z}_{p^r}$ e $\mathbb{Z}_{p^s}$, respectivamente. Com isso, saberemos se o subgrupo oculto é cíclico ou não e teremos eliminado de nossa busca, alguns dos parâmetros que definem H. O parâmetro i, caso H seja cíclico. Os parâmetros i e j, caso H não seja cíclico.

Separamos o problema em dois subproblemas, o PSO para o caso cíclico e o PSO para o caso não cíclico, cujas abordagens são similares. Primeiro, observamos que para certos valores dos parâmetros que definem H_x e H_y o subgrupo oculto está contido no subgrupo abeliano $\mathcal{A} = \left\langle x^{p^{s-l}}, y \right\rangle$ e, sendo assim, podemos calcular seus geradores através do PSO abeliano. Depois, observamos que para outros valores dos parâmetros que definem H_x e H_y, distintos dos anteriores, o subgrupo oculto é normal. Como $\mathcal{G}^l$ é um p-grupo e todo p-grupo é solúvel, Garcia e Lequain (2002), podemos aplicar os resultados de Ivanyos et al. (2003) para determinar seus geradores.

Por fim, para os parâmetros que não se enquadrem nos casos anteriores,

aplicamos um algoritmo direto para a solução do PSO em $\mathcal{G}^l$. Esta descrição é certamente muito imprecisa, mas nos dá uma visão geral de como iremos proceder. No que segue, detalharemos todo o processo.

4.1 Primeira Redução

Sejam X um conjunto finito e $f : \mathcal{G}^l \to X$ a função separadora de classes laterais que oculta o subgrupo H de $\mathcal{G}^l$. Considere os subgrupos H_x oculto em $\mathbb{Z}_{p^r}$ por $f_x = f\Big|_{\mathbb{Z}_{p^r}} : \mathbb{Z}_{p^r} \to X$, $f_x(a) = f(a,0)$ e H_y oculto em $\mathbb{Z}_{p^s}$ por $f_y = f\Big|_{\mathbb{Z}_{p^s}} : \mathbb{Z}_{p^s} \to X$, $f_x(b) = f(0,b)$. Usando o algoritmo para a solução do PSO abeliano, determinamos eficientemente geradores para H_x e H_y. Assim, temos em mãos m e n, $0 \leq m \leq r$ e $0 \leq n \leq s$, tais que $H_x = \left\langle x^{p^m} \right\rangle$ e $H_y = \left\langle y^{p^n} \right\rangle$. Da Observação 3.3.1 segue que se $m = r$ ou $n = s$, então H é cíclico. Sendo assim, podemos resolver o PSO em $\mathcal{G}^l$, considerando o caso cíclico e o não cíclico separadamente.

4.2 O Caso Cíclico

Suponhamos que $m = r$ ou $n = s$. Aqui há duas possibilidades a serem consideradas:

(a) $m = r$ e $n \leq s$.

(b) $m < r$ e $n = s$.

Pela Observação 3.3.1, em (a) temos que $H = \left\langle x^{tp^{r-n+j}} y^{p^j} \right\rangle$ para algum par j, t tal que $0 \leq j \leq n$ e $t \in \mathbb{Z}^*_{p^{n-j}}$ se $j \neq n$ ou $t = 1$ se $j = n$. Desta maneira, afim de resolver o PSO, devemos determinar os parâmetros t e j que definem o subgrupo oculto H. Seja o subgrupo

$$\mathcal{A} = \left\langle x^{p^{s-l}}, y \right\rangle. \tag{4.1}$$

Como $x^{p^{s-l}} y = y x^{p^{s-l}}$, segue que $\mathcal{A}$ é abeliano. Além disso, como $r \geq 2s - l$, observamos que $r - n + j \geq s - l$ e, portanto, $x^{tp^{r-n+j}} y^{p^j} \in \mathcal{A}$ quaisquer que sejam j e t. Sendo assim, $H \leq \mathcal{A}$ e restringindo f ao subgrupo abeliano $\mathcal{A}$, determinamos

os parâmetros j e t que definem H através do PSO abeliano. Resolvemos, assim, o PSO em $\mathcal{G}^l$ para o caso (a).

Em (b), pela Observação 3.3.1, segue que $H = \left\langle x^{tp^{m-s+j}} y^{p^j} \right\rangle$ para algum par j, t com $0 \leq j \leq s$ e $t \in \mathbb{Z}^*_{p^{s-j}}$ se $j \neq s$ ou $t = 1$ se $j = s$.

Se $m \geq 2s-l$, então $m-s+j \geq s-l$ para qualquer j e temos $x^{tp^{m-s+j}} y^{p^j} \in \mathcal{A}$ quaisquer que sejam j e t. Logo, se $m \geq 2s - l$, $H \leq \mathcal{A}$ e podemos determinar os parâmetros j e t que definem H através do PSO abeliano, como fizemos em (a).

Se por outro lado $m \leq r - s + l$, então $r - (m - s + j) \geq 2(s - j) - l$ o que implica, pela equação (3.24), que o subgrupo $\left\langle x^{tp^{m-s+j}} y^{p^j} \right\rangle$ é normal, quaisquer que sejam j e t. Desta forma, H é normal e podemos determinar eficientemente os parâmetros j e t através da abordagem de Ivanyos et al. (2003)(ver Teorema 7), pois $\mathcal{G}^l$ é solúvel e o subgrupo oculto é normal. Desta forma, resta-nos tratar o caso em que $r - s + l < m < 2s - l$, caso ele exista.

De fato, para que exista um tal m, deve-se ter $r - s + l + 1 < 2s - l \Leftrightarrow r < 3s - 2l - 1$. Caso r, s e l sejam tais que a última desigualdade não seja satisfeita, teremos encerrado a análise do PSO em $\mathcal{G}^l$ no caso cíclico. Vale observar que se $r \geq 3s - 1$ a referida desigualdade não é válida para qualquer valor de l.

Desta forma, suponhamos $r < 3s - 2l - 1$. Sabemos que existe pelo menos um m tal que $r - s + l < m < 2s - l$. O Algoritmo 4.2.1, a seguir, resolve o PSO nestes casos. Ele é uma variação do conhecido e já mencionado MAF utilizado, por exemplo, na solução do PSO abeliano, dentre outras aplicações, Kitaev (1995); Kuperberg (2005); Gonçalves (2005); Lomont (2004); Moore et al. (2005); Inui e Le Gall (2005). As principais diferenças residem em dois fatos. O primeiro deles é não superpormos todos os elementos do grupo, mas apenas um subconjunto especial do grupo. O segundo, nós utilizaremos a Transformada de Fourier abeliana em nosso algoritmo, embora $\mathcal{G}^l$ seja um grupo não abeliano. Em geral, o MAF utiliza a Transformada de Fourier do grupo em questão.

Sejam $\mathcal{H}_{\mathcal{G}^l} = \langle |g\rangle \,;\, g \in \mathcal{G}\rangle$ e $\mathcal{H}_X = \langle |z\rangle \,;\, z \in X\rangle$ os espaços de Hilbert associados à $\mathcal{G}^l$ e X, respectivamente. Considere ainda as transformações unitárias

U, que efetua a operação do grupo, e V_f, que atua como a função separadora de classes do subgrupo oculto, como discutido na Seção 2.3.3.

Além destes elementos que acabamos de descrever, introduzimos dois espaços de Hilbert auxiliares, de grande importância para o algoritmo, cujos elementos da base ortonormal são indexados pelos elementos dos grupos $\mathbb{Z}_{p^\kappa}$ e $\mathbb{Z}_{p^\eta}$, respectivamente. São eles $\mathcal{H}_{p^\kappa} = \langle |a\rangle \,;\, a \in \mathbb{Z}_{p^\kappa} \rangle$ e $\mathcal{H}_{p^\eta} = \langle |b\rangle \,;\, b \in \mathbb{Z}_{p^\eta} \rangle$, onde κ e η são parâmetros de entrada do algoritmo.

O espaço onde o algoritmo irá operar é $\mathcal{H} = \mathcal{H}_{p^\kappa} \otimes \mathcal{H}_{p^\eta} \otimes \mathcal{H}_{\mathcal{G}^l} \otimes \mathcal{H}_X$. Uma pergunta importante a ser feita em relação a esse espaço é em relação à quantidade de *qbits* necessários para codificar cada um dos seus vetores. É fundamental que esse número seja $O(\text{poli}(\log |\mathcal{G}^l|))$. Asseguramos que este é o caso. De fato, na Tabela 4.1 listamos a quantidade necessária de *qbits* para codificar os elementos de cada espaço. Como veremos κ e η são menores que $r + s$. Desta fora, o número de *qbits* necessários é $O((r + s) \log p) = O(\log |\mathcal{G}^l|)$.

Espaço	$\mathcal{H}_{\mathcal{G}^l}$	$\mathcal{H}_X$	$\mathcal{H}_{p^\kappa}$	$\mathcal{H}_{p^\eta}$	$\mathcal{H}$
nº de *qbits*	$(r + s) \log p$	$\leq (r + s) \log p$	$\kappa \log p$	$\eta \log p$	$\leq (2(r + s) + \kappa + \eta) \log p$

Tabela 4.1: Número de *qbits* para codificação dos espaços da computação.

Vamos ao algoritmo. Ele pode ser visualizado esquematicamente no circuito

Algoritmo 4.2.1 Subrotina para a solução do PSO em $\mathcal{G}^l$.

Entrada: κ e η;
Saída: $a \in \mathbb{Z}_{p^\kappa}$ e $b \in \mathbb{Z}_{p^\eta}$;

1: Inicialize o computador quântico no estado $|\psi_0\rangle = |0\rangle\,|0\rangle\,|e\rangle\,|0\rangle$;
2: Aplique $F = FT_{p^\kappa} \otimes FT_{p^\eta}$ nos dois primeiros registradores;
3: Controlada pelo segundo registrador, aplique a porta $\tilde{C}(U_y)$ no terceiro registrador;
4: Controlada pelo primeiro registrador, aplique a porta $\tilde{C}(U_x)$ no terceiro registrador;
5: Aplique a porta V_f aos dois últimos registradores;
6: Meça o terceiro registrador e o descarte;
7: Aplique $F = FT_{p^\kappa} \otimes FT_{p^\eta}$ nos dois primeiros registradores;
8: Meça os dois primeiros registradores;

da Figura 4.1.

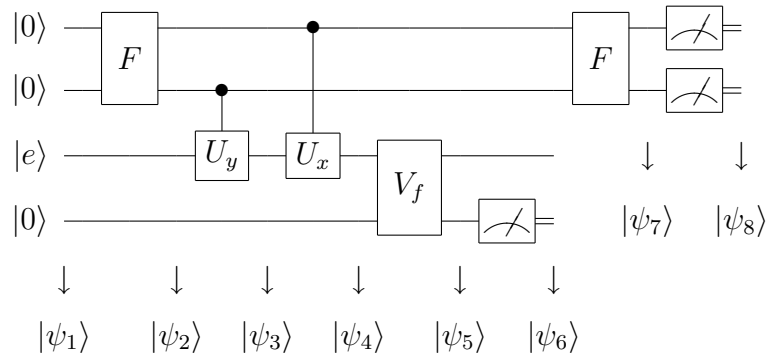


Figura 4.1: Circuito para a computação do Algoritmo 4.2.1.

Devemos nos assegurar que o Algoritmo 4.2.1 determina eficientemente os geradores do subgrupo oculto H. Inicializamos o algoritmo fazendo $\kappa = m$, $\eta = s$ e colocando o computador quântico no estado inicial $|\psi_1\rangle = |0\rangle\,|0\rangle\,|e\rangle\,|0\rangle$. Este estado, quando submetido à ação da Transformada de Fourier $F = FT_{p^m} \otimes FT_{p^s}$ no segundo passo do algoritmo, cria a seguinte superposição de estados:

$$|\psi_2\rangle = \frac{1}{\sqrt{p^{m+s}}} \sum_{a=0}^{p^m-1} \sum_{b=0}^{p^s-1} |a\rangle\,|b\rangle\,|e\rangle\,|0\rangle\,.$$

Quando o estado $|\psi_2\rangle$ é operado por $\tilde{C}(U_y)$ e $\tilde{C}(U_x)$ na seqüência do algoritmo, nós criamos uma superposição de estados que pode ser interpretada como a superposição dos elementos do conjunto L do Lema 3.3.1. De fato, os estados resultantes das computações de $\tilde{C}(U_y)$ e $\tilde{C}(U_x)$ são, respectivamente:

$$|\psi_3\rangle = \frac{1}{\sqrt{p^{m+s}}} \sum_{a=0}^{p^m-1} \sum_{b=0}^{p^s-1} |a\rangle\,|b\rangle\,\left|y^b\right\rangle\,|0\rangle$$

e

$$|\psi_4\rangle = \frac{1}{\sqrt{p^{m+s}}} \sum_{a=0}^{p^m-1} \sum_{b=0}^{p^s-1} |a\rangle\,|b\rangle\,\left|x^a y^b\right\rangle\,|0\rangle\,.$$

Pelo Lema 3.3.1, após o passo 5 do Algoritmo 4.2.1, quando aplicamos a transformação unitária separadora das classes laterais do subgrupo oculto, o estado

resultante é

$$
\begin{aligned}
|\psi_5\rangle &= \frac{1}{\sqrt{p^{m+s}}} \sum_{a=0}^{p^m-1} \sum_{b=0}^{p^s-1} |a\rangle\,|b\rangle\,\left|x^a y^b\right\rangle \left|f\left(x^a y^b\right)\right\rangle \\
&= \frac{1}{\sqrt{p^{m+j}}} \sum_{x^a y^b \in T_j} \left(\frac{1}{\sqrt{p^{s-j}}} \sum_{\lambda=0}^{p^{s-j}-1} \left|\left(a + t\lambda p^{m-s+j}\right) \bmod p^m\right\rangle \left|b + \lambda p^j\right\rangle \right. \\
&\quad \left. \left|x^{\left(a+t\lambda p^{m-s+j}\right) \bmod p^m} y^{b+\lambda p^j}\right\rangle \right) \left|f\left(x^a y^b\right)\right\rangle .
\end{aligned}
$$

Do Lema 3.3.1 sabemos que $H = K_j^t$ para algum par j, t, onde K_j^t está definido em (3.27). Embora esse par esteja presente implicitamente na descrição do estado $|\psi_5\rangle$, não significa que o conheçamos. Significa, simplesmente, que a informação que desejamos obter, já está presente no estado. Entretanto, neste ponto não dispomos de meios para obtê-lo. Na descrição acima, T_j representa a transversal do subgrupo oculto H definida em (3.28).

De alguma maneira, devemos extrair do estado $|\psi_5\rangle$ a informação que nos permita determinar j e t. Caminhamos nesta direção, efetuando a medida do quarto registrador. Ao fazermos isso, colapsamos o estado $|\psi_5\rangle$ para o estado

$$
\begin{aligned}
|\psi_6\rangle &= \left(\frac{1}{\sqrt{p^{s-j}}} \sum_{\lambda=0}^{p^{s-j}-1} \left|\left(a_0 + t\lambda p^{m-s+j}\right) \bmod p^m\right\rangle \left|b_0 + \lambda p^j\right\rangle \right. \\
&\quad \left. \left|x^{\left(a_0+t\lambda p^{m-s+j}\right) \bmod p^m} y^{b_0+\lambda p^j}\right\rangle \right) \left|f\left(x^{a_0} y^{b_0}\right)\right\rangle
\end{aligned}
$$

para $a_0 \in \mathbb{Z}_{p^m}$ e $b_0 \in \mathbb{Z}_{p^j}$ uniformemente distribuídos ($x^{a_0} y^{b_0} \in T_j$). Podemos entender o estado $|\psi_6\rangle$ como uma superposição dos elementos do subconjunto $L \cap x^{a_0} y^{b_0} H = L \cap x^{a_0} y^{b_0} K_j^t$. Por simplicidade de notação, desconsideraremos os registradores 3 e 4, passando a trabalhar apenas com os dois primeiros. Isso, não implica em erro no procedimento, tendo em vista que o terceiro registrador não será alterado no restante do processo e nem será utilizado, explicitamente, para a extração da informação desejada. O quarto registrador, foi medido e portanto pode ser desconsiderado sem maiores problemas. Desta maneira, o estado $|\psi_6\rangle$

pode ser reescrito como:

$$|\psi_6\rangle \;=\; \frac{1}{\sqrt{p^{s-j}}}\sum_{\lambda=0}^{p^{s-j}-1}\left|\left(a_0+t\lambda p^{m-s+j}\right)\bmod p^m\right\rangle\left|b_0+\lambda p^j\right\rangle.$$

A aplicação da Transformada de Fourier $F = FT_{p^m}\otimes FT_{p^s}$ ao estado $|\psi_6\rangle$ nos possibilitará extrair informação suficiente para o cálculo efetivo dos parâmetros j e t que definem o subgrupo oculto H. O estado resultante da aplicação de F é descrito abaixo.

$$\begin{aligned}|\psi_7\rangle &= \frac{1}{\sqrt{p^{s-j}}}\sum_{\lambda=0}^{p^{s-j}-1}\left(\frac{1}{\sqrt{p^{m+s}}}\sum_{a=0}^{p^m-1}\sum_{b=0}^{p^s-1}\omega_{p^m}^{a\left(\left(a_0+t\lambda p^{m-s+j}\right)\bmod p^m\right)}\omega_{p^s}^{b\left(b_0+\lambda p^j\right)}|a\rangle\,|b\rangle\right)\\ &= \frac{1}{\sqrt{p^{m+2s-j}}}\sum_{a=0}^{p^m-1}\sum_{b=0}^{p^s-1}\omega_{p^m}^{aa_0}\omega_{p^s}^{bb_0}\left(\sum_{\lambda=0}^{p^{s-j}-1}\omega_{p^m}^{at\lambda p^{m-s+j}}\omega_{p^s}^{b\lambda p^j}\right)|a\rangle\,|b\rangle\end{aligned}$$

Mas,

$$\omega_{p^m}^{at\lambda p^{m-s+j}} \;=\; \exp\left(\frac{2\pi i}{p^m}at\lambda p^{m-s+j}\right)=\exp\left(\frac{2\pi i}{p^{s-j}}at\lambda\right)=\omega_{p^{s-j}}^{at\lambda},$$

$$\omega_{p^s}^{b\lambda p^j} \;=\; \exp\left(\frac{2\pi i}{p^s}b\lambda p^j\right)=\exp\left(\frac{2\pi i}{p^{s-j}}b\lambda\right)=\omega_{p^{s-j}}^{b\lambda}.$$

Desta forma,

$$|\psi_7\rangle \;=\; \frac{1}{\sqrt{p^{m+j}}}\sum_{a=0}^{p^m-1}\sum_{b=0}^{p^s-1}\omega_{p^m}^{aa_0}\omega_{p^s}^{bb_0}\left(\frac{1}{p^{s-j}}\sum_{\lambda=0}^{p^{s-j}-1}\omega_{p^{s-j}}^{(at+b)\lambda}\right)|a\rangle\,|b\rangle.$$

Seja $\gamma=\left(\frac{1}{p^{s-j}}\sum_{\lambda=0}^{p^{s-j}-1}\omega_{p^{s-j}}^{(at+b)\lambda}\right)$. Pela equação (2.2) temos que $\gamma=0$ se $at+b\not\equiv 0 \bmod p^{s-j}$ e $\gamma=1$ se $at+b\equiv 0 \bmod p^{s-j}$. Sendo assim, o estado resultante da aplicação da Transformada de Fourier F é dado por

$$|\psi_7\rangle \;=\; \frac{1}{\sqrt{p^{m+j}}}\underbrace{\sum_{a=0}^{p^m-1}\sum_{b=0}^{p^s-1}}_{at+b\equiv 0 \bmod p^{s-j}}\omega_{p^m}^{aa_0}\omega_{p^s}^{bb_0}|a\rangle\,|b\rangle.$$

Se, agora, medimos o estado $|\psi_7\rangle$, obtemos a e b tais que $a \in \mathbb{Z}_{p^m}$ e $b \in \mathbb{Z}_{p^s}$ estão uniformemente distribuídos e satisfazem à equação de congruência $at + b \equiv 0 \bmod p^{s-j}$. Caso $H = \left\langle x^{p^m} \right\rangle$, também obtemos a e b tais que $a \in \mathbb{Z}_{p^m}$ e $b \in \mathbb{Z}_{p^s}$ estejam uniformemente distribuídos, entretanto, não satisfazendo a qualquer restrição, pois neste caso, temos que L é uma transversal para H. De qualquer forma, já somos capazes de determinar o subgrupo oculto.

A chave para determinarmos os parâmetros j e t é resolvermos a equação de congruência satisfeita pelos parâmetros a e b. Se $a \not\equiv 0 \bmod p$, então a equação possui solução, Hefes (2006). Nos casos em que o resultado da medida nos fornece $a \equiv 0 \bmod p$, nosso algoritmo falha na determinação do subgrupo oculto H, pois não podemos garantir que a equação de congruência $at + b \equiv 0 \bmod p^{s-j}$ possua solução. Mas a probabilidade que isso ocorra é pequena. De fato, esta probabilidade é $1/p < 1/2$. Na Seção 4.4, analisamos o quão pequena é essa probabilidade de erro e veremos que é possível tornar esse erro tão pequeno quanto queiramos.

Suponhamos então que $a \not\equiv 0 \bmod p$. Para cada j, $0 \leq j < s$, resolvemos a equação de congruência $at + b \equiv 0 \bmod p^{s-j}$, determinando $t_j = -ba^{-1} \bmod p^{s-j}$. Seja $J = \left\{ j;\, f\left(x^{t_j p^{m-s+j}} y^{p^j}\right) = f(e) \right\}$. Os elementos $x^{t_j p^{m-s+j}} y^{p^j} \in \mathcal{G}^l$ para os quais $j \in J$, acrescidos de x^{p^m}, são os possíveis geradores do subgrupo oculto H. Se $J = \emptyset$, então $j = s$ e $t = 1$ e temos $H = \left\langle x^{p^m} \right\rangle$. Caso contrário, pondo $j' = \min\{J\}$, temos $H = \left\langle x^{t_{j'} p^{m-s+j'}} y^{p^{j'}} \right\rangle$. De fato, basta uma comparação das ordens dos elementos $x^{t_j p^{m-s+j}} y^{p^j} \in H$ para confirmar tal afirmação.

Como a probabilidade de erro do algoritmo é $1/p$, sua probabilidade de determinar corretamente o subgrupo oculto, ou seja, sua probabilidade de sucesso é $1 - 1/p > 1/2$, pois p é um número primo ímpar. Na Seção 4.4, analisamos mais detalhadamente essa probabilidade de acerto, bem como a complexidade computacional do algoritmo. Demonstramos, assim, que se o subgrupo oculto H for cíclico, conseguimos resolver eficientemente o PSO em $\mathcal{G}^l$.

4.3 O Caso Não Cíclico

Suponhamos, agora, que $0 \leq m < r$ e $0 \leq n < s$, isto é, o subgrupo oculto H possui dois geradores e devemos decidir se $H = \left\langle x^{p^m}, y^{p^n} \right\rangle$ ou $H = \left\langle x^{tp^{m-k}} y^{p^{n-k}}, y^{p^n} \right\rangle = \left\langle x^{tp^{m-k}} y^{p^{n-k}}, x^{p^m} \right\rangle$ com $0 < k \leq \min\{m, n\}$ e $t \in \mathbb{Z}_{p^k}^*$. No segundo caso, devemos determinar os parâmetros k e t. Caso $m = 0$ ou $n = 0$ a Observação 3.3.1 assegura que $H = \left\langle x^{p^m}, y^{p^n} \right\rangle$, pois neste caso não existe $0 < k \leq \min\{m, n\}$. Assim, podemos considerar $0 < m < r$ e $0 < n < s$.

Observamos que se $m \geq 2s - l$, $m - k \geq s - l$ qualquer que seja k. Desta forma, $\left\langle x^{p^m}, y^{p^n} \right\rangle, \left\langle x^{tp^{m-k}} y^{p^{n-k}}, y^{p^n} \right\rangle \leq \mathcal{A}$ e, portanto, $H \leq \mathcal{A}$. Restringindo f ao subgrupo abeliano $\mathcal{A}$ determinamos os geradores de H. Como os subgrupos da classe (ii) do Teorema 3.2.1, $\left\langle x^{p^i}, y^{p^j} \right\rangle$, só são normais quando $i = 0$ (ver (3.25)), aqui nós não poderemos utilizar a abordagem de Ivanyos et al. (2003), como fizemos no caso cíclico. Neste caso empregaremos diretamente o Algoritmo 4.2.1.

Resta-nos analisar o caso em que $0 < m < 2s - l$. Neste caso, inicializamos o Algoritmo 4.2.1 fazendo $\kappa = m$ e $\eta = n$. A análise do algoritmo é similar ao caso cíclico. Por esta razão, seremos mais econômicos nos detalhes.

Após o 4º passo do algoritmo, o estado $|\psi_4\rangle$ resultante é dado por

$$|\psi_4\rangle = \frac{1}{\sqrt{p^{m+n}}} \sum_{a=0}^{p^m-1} \sum_{b=0}^{p^n-1} |a\rangle |b\rangle \left|x^a y^b\right\rangle |0\rangle .$$

Este estado pode ser interpretado, como uma superposição dos elementos do conjunto L definido no Lema 3.3.2. Quando, no passo 5 do algoritmo, aplicamos a operação separadora de classes laterais, V_f, resulta que esta superposição do conjunto L é separada em superposições sobre as intersecções das classes laterais do subgrupo oculto H com o conjunto L já mencionado, produzindo o estado

$$\begin{aligned} |\psi_5\rangle \;=\; & \frac{1}{\sqrt{p^{m+n-k}}} \sum_{x^a y^b \in T_k} \left(\frac{1}{\sqrt{p^k}} \sum_{\lambda=0}^{p^k-1} \left|\left(a + t\lambda p^{m-k}\right) \bmod p^m\right\rangle \left|b + \lambda p^{n-k}\right\rangle \right. \\ & \left. \left|x^{\left(a+t\lambda p^{m-k}\right) \bmod p^m} y^{b+\lambda p^{n-k}}\right\rangle \right) \left|f\left(x^a y^b\right)\right\rangle . \end{aligned}$$

Pela discussão precedente ao Lema 3.3.2, sabemos que $H = K_k^t$ para algum par k, t. Assim, no estado acima, T_k representa uma transversal do subgrupo oculto H.

Como resultado da medida efetuada no passo 6, obtemos o estado $|\psi_6\rangle$, mostrado abaixo. Podemos interpretá-lo como a superposição dos elementos na interseção $\left(x^{a_0}y^{b_0}H\right) \cap L$, onde $x^{a_0}y^{b_0} \in T_k$. Por simplicidade de notação já descartamos os *kets* referentes ao 3º e 4º registradores, como havíamos feito no caso cíclico.

$$|\psi_6\rangle \;=\; \frac{1}{\sqrt{p^k}} \sum_{\lambda=0}^{p^k-1} \left|\left(a_0 + t\lambda p^{m-k}\right) \mod p^m\right\rangle \left|b_0 + \lambda p^{n-k}\right\rangle .$$

A Transformada de Fourier F produz o estado

$$\begin{aligned} |\psi_7\rangle \;&=\; \frac{1}{\sqrt{p^{m+n-k}}} \sum_{a=0}^{p^m-1} \sum_{b=0}^{p^n-1} \omega_{p^m}^{aa_0} \omega_{p^n}^{bb_0} \left(\frac{1}{p^k} \sum_{\lambda=0}^{p^k-1} \omega_{p^k}^{(at+b)\lambda} \right) |a\rangle \, |b\rangle \\ &=\; \frac{1}{\sqrt{p^{m+n-k}}} \underbrace{\sum_{a=0}^{p^m-1} \sum_{b=0}^{p^n-1}}_{at+b \equiv 0 \mod p^k} \omega_{p^m}^{aa_0} \omega_{p^n}^{bb_0} \, |a\rangle \, |b\rangle . \end{aligned}$$

Se, agora, medimos o estado $|\psi_7\rangle$, obtemos a e b tais que $a \in \mathbb{Z}_{p^m}$ e $b \in \mathbb{Z}_{p^s}$ estão uniformemente distribuídos e satisfazem à equação de congruência $at + b \equiv 0 \mod p^k$. Caso $H = \left\langle x^{p^m}, y^{p^n} \right\rangle$, também obtemos a e b tais que $a \in \mathbb{Z}_{p^m}$ e $b \in \mathbb{Z}_{p^s}$ estejam uniformemente distribuídos, entretanto, não satisfazendo a qualquer restrição, pois neste caso, temos que L é uma transversal de H.

Como no caso cíclico, para determinarmos os parâmetros k e t, devemos resolver a equação de congruência satisfeita pelos parâmetros a e b. Entretanto, essa equação só possui solução se $a \not\equiv 0 \mod p$. Nos casos em que o resultado da medida nos fornece $a \equiv 0 \mod p$, nosso algoritmo falha na determinação do subgrupo oculto H. A probabilidade do algoritmo falhar é $1/p < 1/2$. Na Seção 4.4 discutiremos com mais detalhes esse fato.

Suponhamos que $a \not\equiv 0 \mod p$. Para cada $0 \leq k \leq \min\{m, n\}$, resolvemos

Algoritmo 4.3.1 Algoritmo para encontrar o subgrupo oculto H no grupo $\mathcal{G}^l$.

Entrada: Os geradores do grupo $\mathcal{G}^l$ e a função separadora de classes f;
Saída: Os geradores para o subgrupo oculto H;

Restringindo f à $\mathbb{Z}_{p^r}$ e à $\mathbb{Z}_{p^s}$ determine m e n tais que $H_x = \left\langle x^{p^m} \right\rangle$ e $H_y = \left\langle y^{p^n} \right\rangle$;
se $m = r$ ou $n = s$ **então**
  se $m = r$ **então**
    Restringindo f à $\mathcal{A}$ determine os geradores de H.
  senão
    se $m \geq 2s - l$ **então**
      Restringindo f ao subgrupo abeliano $\mathcal{A}$ determine os geradores de H.
    senão
      se $m \leq r - s + l$ **então**
        Determine os geradores de H através do PSO solúvel,
        sob a hipótese de H ser normal.
      senão
        Aplique o Algoritmo 4.2.1 para determinar os geradores de H.
      fim se
    fim se
  fim se
senão
  se $m \geq 2s - l$ **então**
    Restringindo f ao subgrupo abeliano $\mathcal{A}$ determine os geradores de H.
  senão
    Aplique o Algoritmo 4.2.1 para determinar os geradores de H.
  fim se
fim se

a equação de congruência $at + b \equiv 0 \bmod p^k$, determinando $t_k = -ba^{-1} \bmod p^k$. Seja $K = \left\{k;\ f\left(x^{t_k p^{m-k}} y^{p^{n-k}}\right) = f(e)\right\}$. Caso $K = \emptyset$ temos $k = 0$, $t = 1$ e $H = \left\langle x^{p^m}, y^{p^n} \right\rangle$. Caso contrário, pondo $k' = \max\{K\}$, temos $H = \left\langle x^{t_{k'} p^{m-k'}} y^{p^{n-k'}} \right\rangle$. Desta maneira, encerramos a solução do PSO em $\mathcal{G}^l$ para o caso dos subgrupos não cíclicos e, portanto, a solução do PSO em $\mathcal{G}^l$.

Para encerrar esta seção, reunimos no Algoritmo 4.3.1 todo o procedimento desenvolvido neste capítulo, para a solução do PSO em $\mathcal{G}^l$. Frisamos, porém, que nosso intuito é apenas reunir em uma figura todo o processo, não estando preocupados com, por exemplo, a optimalidade do algoritmo apresentado. Certamente ele poderia ser melhorado, diminuindo significativamente a quantidade de condicionantes "**se**", entretanto, isso significaria nos afastarmos da seqüência seguida no desenvolvimento anterior, fato que não desejamos.

4.4 Análise da Complexidade Computacional do Algoritmo

A complexidade computacional do Algoritmo 4.3.1 apresentado na seção anterior, pode ser analisada levando-se em consideração a complexidade computacional do algoritmo para o PSO abeliano, Kitaev (1995); Mosca (1999); Lomont (2004), a complexidade computacional do algoritmo para o PSO em grupos solú-

veis, admitido que o subgrupo oculto é normal, Ivanyos et al. (2003), e a complexidade computacional do Algoritmo 4.2.1. Nos dois primeiros casos, a complexidade do algoritmo é $O(\text{poli}((r+s)\log(p)))$, $\log|\mathcal{G}^l| = (r+s)\log(p)$

Resta fazermos a análise do Algoritmo 4.2.1. Começamos observando que a Transformada de Fourier sobre o grupo $\mathbb{Z}_N$ é eficientemente implementável qualquer que seja N, Lomont (2004). Desta forma ela não representa problemas para o nosso algoritmo. O que devemos garantir é que o número de consultas à função separadora de classes, f, seja polinomial no logaritmo da ordem do grupo $\mathcal{G}^l$. Garantimos que este número de consultas é menor que, ou igual a, $s+1$ vezes. De fato, no passo 5 do Algoritmo 4.2.1 fazemos uma chamada à função f. Depois disso, na parte de pós-processamento do algoritmo, quando criamos o conjunto J, para o caso cíclico, ou o conjunto K, para o caso não cíclico, invocamos a função f no máximo mais s vezes. Portanto, a quantidade de vezes que o Algoritmo 4.2.1 consulta a função separadora de classes é menor que o limite máximo $O(\text{poli}((r+s)\log(p)))$. Além disso, a equação de congruência $at + b \equiv 0 \bmod p^j$ deve ser resolvida $s-1$ vezes. Desta forma, o Algoritmo 4.2.1 é $O(\text{poli}((r+s)\log(p)))$.

Observando o Algoritmo 4.3.1, vemos que se trata de um algoritmo seqüencial sem laços e que, portanto, a sua complexidade de computação será a maior complexidade de computação dos procedimentos envolvidos. Desta forma, como todos os procedimentos envolvidos apresentam complexidade $O(\text{poli}((r+s)\log(p)))$, vemos que a complexidade computacional do algoritmo quântico que apresentamos para a solução do PSO em $\mathcal{G}^l$ é $O(\text{poli}((r+s)\log(p)))$, portanto, eficiente.

Um outro aspecto importante do Algoritmo 4.3.1 é o fato de ser um algoritmo probabilístico. De fato, o algoritmo para o PSO abeliano é probabilístico e a sua probabilidade de sucesso é $1-1/|G|$, onde G é o grupo abeliano onde se está resolvendo o problema, Lomont (2004). O algoritmo para a solução do PSO em grupos solúveis, trata-se de um algoritmo que combina algoritmos quânticos probabilísticos com um algoritmo clássico de Las Vegas, também probabilístico, Babai e Szemerédi (1984); Babai et al. (1995); Ivanyos et al. (2003); Holt et al. (2005). Neste caso

podemos assumir que a probabilidade de sucesso é, pelo menos, $1 - 1/|G|$, onde G é o grupo onde se está resolvendo o problema. Para o Algoritmo 4.2.1, sabemos que a probabilidade de sucesso, com uma única rodada é $1 - 1/p$. Se o repetimos r vezes, a probabilidade de sucesso aumenta para $1 - 1/p^r$, sem que isso interfira no fato do Algoritmo 4.3.1 ser $O(\text{poli}((r+s)\log(p)))$.

Para o cálculo da probabilidade de sucesso do Algoritmo 4.3.1, devemos levar em conta que sempre resolveremos o PSO em $\mathbb{Z}_{p^r}$ e $\mathbb{Z}_{p^s}$. Além disso, vamos ou resolver o PSO em $\mathcal{A}$, ou resolver o PSO em $\mathcal{G}^l$ utilizando a estratégia para grupos solúveis, ou utilizar o Algoritmo 4.2.1. Elegendo a pior probabilidade de sucesso entre esses três últimos procedimentos, $1 - 1/p^r$, asseguramos que a probabilidade de sucesso do Algoritmo 4.3.1 é de, pelo menos,

$$\left(1 - \frac{1}{p^r}\right)\left(1 - \frac{1}{p^s}\right)\left(1 - \frac{1}{p^r}\right) = 1 - \frac{p^{2r} + 2p^{r+s} - 2p^r + p^s - 1}{p^{2r+s}}.$$

Pode-se verificar que esta probabilidade é sempre maior que $1/2$. Portanto, o algoritmo também é eficiente do ponto de vista probabilístico, Kitaev et al. (2002). Na Figura 4.2 exibimos os gráficos da probabilidade de erro do Algoritmo 4.3.1 em casos particulares dos parâmetros r e s. No gráfico à esquerda temos $r = 2s$ e no gráfico à direita, temos $r = s + 2$. As figuras nos mostram claramente que o erro do algoritmo decresce rapidamente, se aproximando de 0.

Pode ser que a probabilidade de sucesso do algoritmo seja muito próxima de $1/2$ e isso possa causar dúvidas em relação ao resultado que o mesmo irá produzir. Entretanto, nos interessa resolver o PSO nos casos em que o grupo $\mathcal{G}^l$ é dado por parâmetros p, r e s suficientemente grandes. Sendo a probabilidade do algoritmo da ordem de $1 - 1/p^s$ e $r > s$, vemos que no limite assintótico, a probabilidade de nosso algoritmo tende para 1, o que se traduz em uma maior confiabilidade no resultado produzido.

Ainda sobre a probabilidade de sucesso do Algoritmo 4.3.1, temos da teoria dos algoritmos probabilísticos, Kitaev et al. (2002), que se um algoritmo eficiente (do ponto de vista da complexidade computacional) tem probabilidade de sucesso

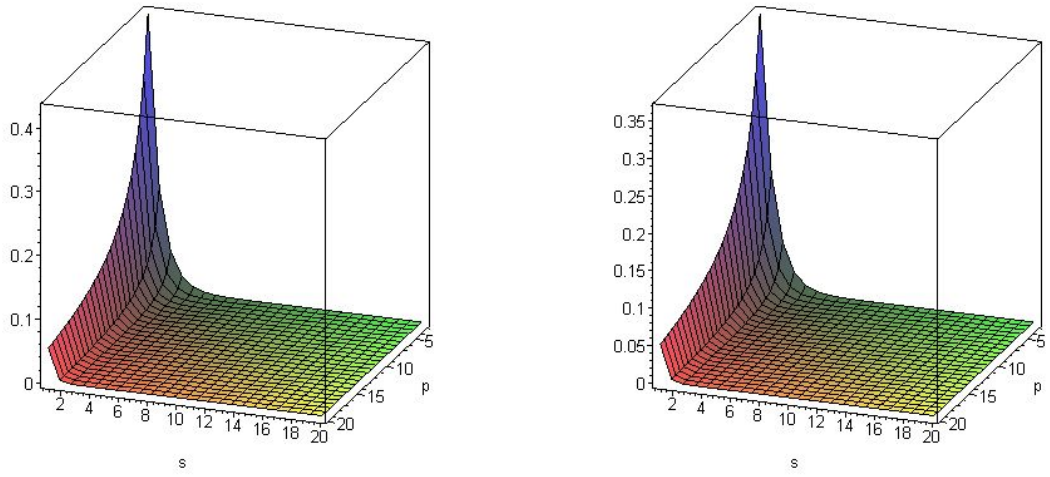


Figura 4.2: Probabilidade de erro do Algoritmo 4.3.1.

maior que 1/2, invocando o Limite de Chernoff, Kitaev et al. (2002); Nielsen e Chuang (2003), essa probabilidade pode ser amplificada, aproximando-se de 1, com poucas repetições do algoritmo e sem prejuízo na eficiência computacional final do mesmo.

Como conseqüência de tudo o que foi exposto neste capítulo, podemos enunciar o principal resultado da tese: um algoritmo quântico eficiente para a solução do Problema do Subgrupo Oculto nos grupos não abelianos $\mathcal{G}^l$.

Teorema 4.4.1 Sejam p um número primo ímpar, r e s inteiros positivos. Para todo grupo $\mathcal{G}^l = \mathbb{Z}_{p^r} \rtimes_\phi \mathbb{Z}_{p^s}$, onde $0 \leq l < s$ e $r \geq 2s - l$, existe um algoritmo quântico eficiente para a solução do Problema do Subgrupo Oculto em $\mathcal{G}^l$.

■

Como já mencionamos, os resultados que apresentamos em Cosme e Portugal (2007b,a) são casos particulares do Teorema 4.4.1. Esse resultado também generaliza o trabalho de Inui e Le Gall (2005).

Capítulo 5

O PSO no Grupo $\mathbb{Z}_N \rtimes \mathbb{Z}_{p^s}$

Como conseqüência do Teorema 4.4.1, podemos atacar o PSO no grupo não abeliano $\mathbb{Z}_N \rtimes \mathbb{Z}_{p^s}$. Dependendo da fatoração prima de N, nosso resultado implica um algoritmo eficiente para o PSO neste grupo. De fato, mostraremos que para uma especial fatoração de N, temos $\mathbb{Z}_N \rtimes \mathbb{Z}_{p^s} \simeq \mathbb{Z}_{N/p^r} \times (\mathbb{Z}_{p^r} \rtimes_\psi \mathbb{Z}_{p^s})$ e combinando os Teoremas 2.3.1 e 4.4.1 apresentaremos a solução do PSO.

5.1 O Grupo $\mathbb{Z}_N \rtimes \mathbb{Z}_{p^s}$

Considere o grupo produto semidireto $\mathbb{Z}_N \rtimes_\phi \mathbb{Z}_{p^s}$ onde $N, s \in \mathbb{N}$, $s \geq 1$, p um número primo ímpar e $\phi : \mathbb{Z}_{p^s} \to \mathrm{Aut}(\mathbb{Z}_N)$ é o homomorfismo de grupos que define o produto semidireto. Vamos assumir que f não é o homomorfismo trivial, portanto, o grupo não é abeliano. Este homomorfismo é completamente determinado por $\alpha = \phi(1)(1) \in \mathbb{Z}_N^*$ e para quaisquer $a \in \mathbb{Z}_N$ e $b \in \mathbb{Z}_{p^s}$, $\phi(b)(a) = a\alpha^b$. Observe ainda que $\phi(p^s) = Id \in \mathrm{Aut}(\mathbb{Z}_N)$, assim:

$$1 = \phi(p^s)(1) = \alpha^{p^s} \Rightarrow |\alpha| \mid p^s \Rightarrow |\alpha| = p^{r_0} \tag{5.1}$$

para algum r_0 tal que $0 \leq r_0 \leq s$. Como $\alpha \in \mathbb{Z}_N^*$, $p^{r_0} \mid |\mathbb{Z}_N^*| = \Phi(N)$ onde Φ é a função *phi* de Euler, Hefes (2006).

Suponhamos que a fatoração prima de N seja $N = p_1^{r_1} \cdots p_k^{r_k}$ e que $p \nmid p_j - 1$ para todo $0 \leq j \leq k$. Temos que $\mathbb{Z}_N \simeq \mathbb{Z}_{p_1^{r_1}} \times \cdots \times \mathbb{Z}_{p_k^{r_k}}$, e $\mathbb{Z}_N \rtimes \mathbb{Z}_{p^s} \simeq \left(\mathbb{Z}_{p_1^{r_1}} \times \cdots \times \mathbb{Z}_{p_k^{r_k}}\right) \rtimes \mathbb{Z}_{p^s}$. Além disso, $\Phi(N) = p_1^{r_1-1} \cdots p_k^{r_k-1}(p_1 - 1) \cdots (p_k - 1)$.

Como $|\alpha|$ divide $\Phi(N)$, a equação (5.1) implica que $p_j = p$ para algum j. Sem perda de generalidade, podemos supor que $p_k = p$. Para não carregar a notação, continuaremos utilizando p_k. Denotaremos o grupo $\left(\mathbb{Z}_{p_1^{r_1}} \times \cdots \times \mathbb{Z}_{p_k^{r_k}}\right) \rtimes \mathbb{Z}_{p^s}$ por $\mathcal{G}$ e seus elementos por $((a_1, \cdots, a_k), b)$ onde $(a_1, \cdots, a_k) \in \mathbb{Z}_{p_1^{r_1}} \times \cdots \times \mathbb{Z}_{p_k^{r_k}}$ e $b \in \mathbb{Z}_{p^s}$.

Para qualquer $1 \leq i \leq k$, identificaremos o grupo $\mathbb{Z}_{p_i^{r_i}}$ com o subgrupo de $\mathbb{Z}_{p_1^{r_1}} \times \cdots \times \mathbb{Z}_{p_k^{r_k}}$ a ele isomorfo. Com esta notação, afirmamos que qualquer que seja $b \in \mathbb{Z}_{p^s}$ tem-se $\phi(b)\left(\mathbb{Z}_{p_i^{r_i}}\right) = \mathbb{Z}_{p_i^{r_i}}$. Para provarmos esta afirmação, considere os elementos $\mathbf{e}_1, \cdots, \mathbf{e}_k \in \mathbb{Z}_{p_1^{r_1}} \times \cdots \times \mathbb{Z}_{p_k^{r_k}}$ definidos por

$$\mathbf{e}_1 = (1, 0, \cdots, 0),\ \mathbf{e}_2 = (0, 1, 0, \cdots, 0),\ \cdots, \mathbf{e}_k = (0, \cdots, 0, 1).$$

Se $\phi(b)\mathbf{e}_i \in \mathbb{Z}_{p_i^{r_i}}$, a teremos provado. Assim, seja $\phi(b)\mathbf{e}_i = (a_1, \cdots, a_k)$. Temos que

$$\begin{aligned}(0, \cdots, 0) &= \phi(b)(0, \cdots, 0) = \phi(b)(0, \cdots, 0, p_i^{r_i}, 0, \cdots, 0) = p_i^{r_i}\phi(b)\mathbf{e}_i \\ &= (p_i^{r_i}a_1, \cdots, p_i^{r_i}a_k).\end{aligned}$$

Segue que para todo $1 \leq j \leq k$ temos $p_i^{r_i}a_j \equiv 0 \bmod p_j^{r_j}$. Logo, para todo $j \neq i$ temos $a_j \equiv 0 \bmod p_j^{r_j}$, portanto, $\phi(b)\mathbf{e}_i = (0, \cdots, 0, a_i, 0, \cdots, 0) \in \mathbb{Z}_{p_i^{r_i}}$, como desejávamos. Vamos agora provar a seguinte proposição.

Proposição 5.1.1

$$\mathbb{Z}_N \rtimes \mathbb{Z}_{p^s} \simeq \mathcal{G} \simeq \left(\mathbb{Z}_{p_1^{r_1}} \times \cdots \times \mathbb{Z}_{p_{k-1}^{r_{k-1}}}\right) \times \left(\mathbb{Z}_{p^r} \rtimes_\psi \mathbb{Z}_{p^s}\right),$$

onde ψ é o homomorfismo induzido por ϕ e $r = r_k$.

Demonstração: Seja $1 \leq i < k$. Decorre do que foi exposto antes da proposição que se $\phi(1)\mathbf{e}_i = (0, \cdots, 0, a_i, 0, \cdots, 0)$, pelas propriedades do homomorfismo ϕ temos que $\phi(b)\mathbf{e}_i = (0, \cdots, 0, a_i^b, 0, \cdots, 0)$ para qualquer b. Logo, $\mathbf{e}_i = \phi(p^s)\mathbf{e}_i = (0, \cdots, 0, a_i^{p^s}, 0, \cdots, 0)$ e, assim, $a_i^{p^s} \equiv 1 \bmod p_i^{r_i}$. Logo, $a_i \in \mathbb{Z}^*_{p_i^{r_i}}$. Devemos ter $a_i = 1$, pois caso contrário, a sua ordem em $\mathbb{Z}^*_{p_i^{r_i}}$ seria $|a_i| = p^j$, para algum

$0 < j \leq s$. Como $|a_i|$ divide $\left|\mathbb{Z}^*_{p_i^{r_i}}\right| = p_i^{r_i-1}(p_i - 1)$, teríamos um absurdo pois $p \nmid p_i$ e $p \nmid p_i - 1$. Desta forma, $a_i = 1$ e $\phi(1)\mathbf{e}_i = \mathbf{e}_i$ para todo $1 \leq i < k$, o que implica que $\phi(b)\mathbf{e}_i = \mathbf{e}_i$ para todo $b \in \mathbb{Z}_{p^s}$. Sendo assim, concluímos que existe um homomorfismo $\psi : \mathbb{Z}_{p^s} \to \mathrm{Aut}\,(\mathbb{Z}_{p^r})$, ($p_k = p$ e $r_k = r$), tal que para todo $b \in \mathbb{Z}_{p^s}$ e todo $(a_1, \cdots, a_k) \in \mathbb{Z}_{p_1^{r_1}} \times \cdots \times \mathbb{Z}_{p_k^{r_k}}$, tenhamos

$$\phi(b)(a_1, \cdots, a_k) = (a_1, \cdots, a_{k-1}, \psi(b)(a_k)). \tag{5.2}$$

Sejam $g = ((a_1, \cdots, a_k), b), h = ((c_1, \cdots, c_k), d) \in \mathcal{G}$. Como conseqüência de (5.2) temos

$$\begin{aligned} gh &= ((a_1, \cdots, a_k) + \phi(b)(c_1, \cdots, c_k), b + d) \\ &= ((a_1 + c_1, \cdots, a_{k-1} + c_{k-1}, a_k + \psi(b)(c_k)), b + d). \end{aligned} \tag{5.3}$$

Definindo $\Gamma : \mathcal{G} \to \left(\mathbb{Z}_{p_1^{r_1}} \times \cdots \times \mathbb{Z}_{p_{k-1}^{r_{k-1}}}\right) \times \left(\mathbb{Z}_{p_k^{r_k}} \rtimes_\psi \mathbb{Z}_{p^s}\right)$ por

$$\Gamma(((a_1, \cdots, a_k), b)) = ((a_1, \cdots, a_{k-1}), (a_k, b)),$$

a equação (A.1) nos permite mostrar que Γ é o isomorfismo procurado, pois $p_k = p$. Encerramos assim a prova da proposição.

■

Se definimos N' como $N' = N/p^r$, temos que $Z_{p_1^{r_1}} \times \cdots \times \mathbb{Z}_{p_{k-1}^{r_{k-1}}} \simeq \mathbb{Z}_{N'}$. Decorre da Proposição 5.1.1 que $\mathbb{Z}_N \rtimes_\phi \mathbb{Z}_{p^s} \simeq \mathbb{Z}_{N'} \times (\mathbb{Z}_{p^r} \rtimes_\psi \mathbb{Z}_{p^s})$.

5.2 A solução do PSO em $\mathbb{Z}_N \rtimes_\phi \mathbb{Z}_{p^s}$

Sejam N e N' como dados na seção anterior. Como $\mathrm{mdc}\,(N', p^{r+s}) = 1$, a Proposição 5.1.1 e o Teorema 2.3.1 nos asseguram que para resolvermos o PSO em $\mathbb{Z}_N \rtimes_\phi \mathbb{Z}_{p^s}$ basta que saibamos resolver o PSO em $\mathbb{Z}_{N'}$ e em $\mathbb{Z}_{p^r} \rtimes_\psi \mathbb{Z}_{p^s}$. No primeiro caso, temos o PSO abeliano, eficientemente resolvível. No segundo caso, basta que o grupo $\mathbb{Z}_{p^r} \rtimes_\psi \mathbb{Z}_{p^s}$ satisfaça às hipóteses do Teorema 4.4.1 para que possamos

resolver eficientemente o PSO. Sendo assim, devemos ter $s < r$ e o homomorfismo ψ deve ser definido por uma raíz $tp^{r-s+l} + 1 \in \mathbb{Z}_{p^r}^*$, onde o parâmetro l satisfaça a $r \geq 2s - l$. Sob essas hipóteses, temos

Teorema 5.2.1 Existe um algoritmo quântico eficiente para a solução do PSO sobre o grupo não abeliano $\mathbb{Z}_N \rtimes_\phi \mathbb{Z}_{p^s}$, desde que o grupo satisfaça às hipóteses apresentadas anteriormente.

■

Este resultado generaliza o resultado apresentado em Chi et al. (2006), no qual os autores apresentam um algoritmo quântico eficiente para a solução do PSO nos grupos $\mathbb{Z}_N \rtimes \mathbb{Z}_p$, onde N satisfaz às mesmas hipóteses presentes aqui.

Capítulo 6

O Caso Geral do PSO em $\mathbb{Z}_{p^r} \rtimes \mathbb{Z}_{p^s}$

Até o presente momento, apresentamos um algoritmo quântico eficiente para resolver o PSO nos grupos $\mathcal{G}^l$ onde os parâmetros r, s e l estavam sujeitos à restrição $r \geq 2s - l$. A pergunta mais natural a ser feita é se o Algoritmo 4.3.1 não seria capaz de tratar o caso geral do problema. Infelizmente, pudemos constatar que não. De fato, quando r, s e l deixam de satisfazer à desigualdade acima, o grupo $\mathbb{Z}_{p^r} \rtimes \mathbb{Z}_{p^s}$ deixa de satisfazer certas propriedades, Lemas 3.2.1, 3.3.1, 3.3.2, e isso causa algumas dificuldades para o ataque do PSO utilizando a estratégia que mostramos nos capítulos anteriores. A principal delas é que a Transformada de Fourier abeliana que empregamos no Algoritmo 4.2.1 não é mais capaz de trazer à tona a informação necessária para a obtenção dos parâmetros que determinam o subgrupo oculto.

Entretanto, acreditamos que a estratégia de classificação dos subgrupos possa ainda nos ser útil. De fato, caminharemos nessa direção ao longo deste capítulo. Embora ainda não tenhamos uma prova definitiva de que, no caso geral dos grupos $\mathbb{Z}_{p^r} \rtimes \mathbb{Z}_{p^s}$, a classificação dos subgrupos seja a mesma apresentada no Teorema 3.2.1, temos evidencias numéricas e alguns apontamentos promissores para a prova de que isso seja verdade. Assumiremos esta conjectura, Conjectura 6.1.1, e avançaremos na direção da solução do PSO em $\mathbb{Z}_{p^r} \rtimes \mathbb{Z}_{p^s}$.

Faremos alguns apontamentos na direção de um possível ataque ao caso geral do PSO em $\mathbb{Z}_{p^r} \rtimes \mathbb{Z}_{p^s}$, representando uma pesquisa ainda em desenvolvimento e

que certamente é garantia de muito trabalho futuro. Nesta estratégia que apresentaremos, vamos combinar a Conjectura 6.1.1 com uma redução do problema, apresentada por Ivanyos et al. (2007b). Esta redução, que será discutida em maiores detalhes à frente, Teorema 6.3.1, assegura que para a eficiente solução do PSO em certas classes de grupos nilpotentes[1] , basta que saibamos como determinar os subgrupos ocultos em p-grupos de expoente p e sob a hipótese adicional que o subgrupo oculto ou é trivial ou tem ordem p. Essa redução é, de certa forma, similar às reduções existentes para o PSO no grupo diedral, Ettinger et al. (1999), e em grupos do tipo $A \rtimes \mathbb{Z}_p$, onde A é um grupo abeliano, Bacon et al. (2005).

Afim de utilizarmos esta redução, construiremos uma classe de grupos na qual estarão incluídos os grupos $\mathbb{Z}_{p^r} \rtimes \mathbb{Z}_{p^s}$. Se a conjectura sobre a classificação dos subgrupos for verdadeira, os grupos de expoente p pertencentes à classe mencionada serão todos abelianos. Desta forma, teremos reduzido o PSO nos grupos $\mathbb{Z}_{p^r} \rtimes \mathbb{Z}_{p^s}$ ao PSO abeliano e o teremos resolvido completamente, sem qualquer restrição sobre os parâmetros r, s e l.

No decorrer deste capítulo, denotaremos um grupo geral $\mathbb{Z}_{p^r} \rtimes_\phi \mathbb{Z}_{p^s}$ por $\mathcal{G}$, fazendo as devidas observações sobre os parâmetros que o definem quando for necessário.

6.1 A Estrutura do Grupo $\mathbb{Z}_{p^r} \rtimes \mathbb{Z}_{p^s}$

Retomaremos o estudo da estrutura do grupo $\mathcal{G} = \mathbb{Z}_{p^r} \rtimes_f \mathbb{Z}_{p^s}$ iniciado no Capítulo 3. Conduziremos tal estudo de forma muito parecida àquele realizado na Seção 3.1, por isso seremos mais econômicos nos detalhes menos importantes.

Pela discussão feita na Seção 3.1 sabemos que o homomorfismo que define o grupo é dado por $\phi(b)(a) = a\alpha^b$, $\forall\, a \in \mathbb{Z}_{p^r}$, $b \in \mathbb{Z}_{p^s}$, onde α é uma das raízes da equação (3.1). Portanto, se $s < r$, temos $\alpha = tp^{r-s+l} + 1$ com $0 \leq l < s$, $t \in \mathbb{Z}^*_{p^s}$ e $tp^l < p^s$. Caso $1 < r \leq s$ temos $\alpha = tp^{l+1} + 1$ onde $0 \leq l < r-1$, $t \in \mathbb{Z}^*_{p^{r-1}}$ e $tp^l < p^{r-1}$. Embora haja diferença entre as raízes que definem o grupo em cada

[1] Veja Apêndice A

caso, as diferenças no desenvolvimento do estudo são mínimas. Por esta razão optamos por fazê-lo sem distinguir entre um caso ou outro. Para tanto, definimos:

Definição 6.1.1

$$\eta = \eta(r,s,l) = \begin{cases} r-s+l & \text{se} \quad s<r \\ l+1 & \text{se} \quad 1<r\leq s \end{cases}.$$

Assim, as raízes α se reescrevem como $\alpha = tp^{r-s+l}+1$ com $t \in \mathbb{Z}_{p^s}^*$ ou $t \in \mathbb{Z}_{p^{r-1}}^*$. Note que em qualquer caso, $\eta + s \geq r$.

Dados $x^a y^b, x^c y^d \in \mathcal{G}$, o produto desses elementos é dado por

$$\left(x^a y^b\right)\left(x^c y^d\right) = x^{a+c\alpha^b} y^{b+d}. \tag{6.1}$$

Expandindo a potência α^b podemos escrever $\alpha^b = \varphi(b)tp^\eta + 1$, onde

$$\varphi(b) = \frac{\alpha^b - 1}{tp^\eta} = (tp^\eta)^{(b-1)} + b\,(tp^\eta)^{b-2} + \cdots + \frac{b(b-1)}{2}tp^\eta + b.$$

Na Seção 3.1, a hipótese de que $r \geq 2(s-l)$ garantia que $\varphi(b) \equiv b \bmod p^r$. Como não temos mais essa hipótese, nossa fórmula de produto se reescreve como

$$\left(x^a y^b\right)\left(x^c y^d\right) = x^{a+c(t\varphi(b)p^\eta+1)} y^{b+d}. \tag{6.2}$$

Decorre diretamente que

$$y^b x^a = x^{a((\varphi(b)p^\eta+1)} y^b. \tag{6.3}$$

Podemos verificar sem maiores dificuldades que $\operatorname{mdc}(\varphi(b), p^s) = \operatorname{mdc}(b, p^s)$. Assim, se $p^j = \operatorname{mdc}(b, p^s)$, escreveremos

$$\varphi(b) = \tilde{\varphi}(b)p^j, \tag{6.4}$$

com $\operatorname{mdc}(\tilde{\varphi}(b), p) = 1$. Note também que $\varphi(0) = 0$ e $\varphi(1) = 1$.

Consideremos agora $x^a y^b \in \mathcal{G}$ e seja k um inteiro maior que 1. Tem-se em

decorrência de (6.3) que

$$\left(x^a y^b\right)^k = x^{a\sum_{j=0}^{k-1}\left(\alpha^b\right)^j} y^{bk}. \tag{6.5}$$

Analisando o somatório $\sum_{j=0}^{k-1}\left(\alpha^b\right)^j$ temos

$$\begin{aligned}\sum_{j=0}^{k-1}\left(\alpha^b\right)^j &= \frac{\alpha^{bk}-1}{\alpha^b-1} = \frac{(\varphi(b)tp^\eta+1)^k-1}{(\varphi(b)tp^\eta+1)-1} \\ &= (\varphi(b)tp^\eta)^{k-1} + k\,(\varphi(b)tp^\eta)^{k-2} + \cdots + \frac{k(k-1)}{2}\varphi(b)tp^\eta + k.\end{aligned}$$

Definindo $\Sigma(b,k)$ como

$$\begin{aligned}\Sigma(b,k) = (\varphi(b)tp^\eta)^{k-2} + k\,(\varphi(b)tp^\eta)^{k-3} + \cdots + \tfrac{k(k-1)}{2}, &\quad \text{se } k \geq 2 \\ \Sigma(b,k) = 0, &\quad \text{se } k = 0,1\end{aligned}. \tag{6.6}$$

temos que $\sum_{j=0}^{k-1}\left(\alpha^b\right)^j = \Sigma(b,k)\varphi(b)tp^\eta + k$. Vale notar que se $k = p^i$ com $i > 0$, então $p^i \mid \Sigma(b,p^i)$ e, assim, podemos escrever

$$\Sigma(b,p^i) = \tilde{\Sigma}(b,p^i)p^i. \tag{6.7}$$

Podemos reescrever a equação (6.5) como segue

$$\left(x^a y^b\right)^k = x^{a(\Sigma(b,k)\varphi(b)tp^\eta+k)}y^{bk} = x^{a\Sigma(b,k)\varphi(b)tp^\eta}x^{ak}y^{bk}. \tag{6.8}$$

Considerando ainda $x^a y^b \in \mathcal{G}$, mas supondo que $a \neq 0$ e $b \neq 0$, sejam $p^i = \text{mdc}\,(a,p^r)$ e $p^j = \text{mdc}\,(b,p^s)$, onde devemos ter $0 \leq i < r$ e $0 \leq j < s$. Sejam também $a = a'p^i$, $b = b'p^j$ e $\varphi(b) = \tilde{\varphi}(b)p^j$. Se $r-i \geq s-j$, como $\eta+s \geq r$, temos que

$$\begin{aligned}\left(x^a y^b\right)^{p^{s-j}} &= x^{a\Sigma(b,p^{s-j})\varphi(b)tp^\eta}x^{ap^{s-j}}y^{bp^{s-j}} \\ &= x^{a\tilde{\Sigma}(b,p^{s-j})\tilde{\varphi}(b)tp^{\eta+s}}x^{ap^{s-j}} = x^{ap^{s-j}}, \\ \left(x^a y^b\right)^{p^{r-i}} &= x^{a\Sigma(b,p^{r-i})\varphi(b)tp^\eta}x^{ap^{r-i}}y^{bp^{r-i}} \\ &= x^{a'\tilde{\Sigma}(b,p^{r-i})\varphi(b)tp^{\eta+r}} = e\end{aligned}$$

De maneira análoga, se $r-i<s-j$ mostra-se que $\left(x^a y^b\right)^{p^{s-j}}=e$ e $\left(x^a y^b\right)^{p^{r-i}}=y^{bp^{r-i}}$. Assim obtemos a mesma relação dada pela equação (3.9)

$$\begin{cases} (x^a y^b)^{p^{s-j}}=x^{ap^{s-j}}, & (x^a y^b)^{p^{r-i}}=e, & \text{se } r-i\geq s-j \\ (x^a y^b)^{p^{s-j}}=e, & (x^a y^b)^{p^{r-i}}=y^{bp^{r-i}}, & \text{se } r-i<s-j \end{cases}. \tag{6.9}$$

Como na Seção 3.1, segue de (6.9) que

$$\left|x^a y^b\right|=\max\left\{p^{r-i},p^{s-j}\right\}. \tag{6.10}$$

Uma diferença crucial entre o estudo que fazemos agora e o que fora feito no Capítulo 3 é que o resultado do Lema 3.2.1 não é válido aqui. De fato, analisando o termo $x^{a\Sigma(b,k)\varphi(b)tp^{\eta}}$ da equação (6.8), nem sempre é possível mostrar que ele pertence ao subgrupo gerado por $x^a y^b$, basta tomar por exemplo $a=b=1$. Assim, não é possível mostrar que $x^{ak}y^{bk}\in\left\langle x^a y^b\right\rangle$ para todo k, portanto, não vale o resultado análogo ao lema supra citado.

Uma breve recapitulação das discussões feitas ao fim da Seção 3.3 nos mostra que a propriedade do Lema 3.2.1 é fundamental para que possamos caracterizar as classes laterais dos subgrupos K_j^t e K_k^t, equações (3.29) e (3.32), bem como para que possamos estabelecer os Lemas 3.3.1 e 3.3.2. Por sua vez, são estes lemas que permitem que a Transformada de Fourier abeliana, quando utilizada no Algoritmo 4.2.1, extraia a informação necessária para obtermos os parâmetros que determinam o subgrupo oculto. Sendo assim, a ausência de um resultado análogo ao Lema 3.2.1 inviabiliza a utilização da estratégia empregada na solução do PSO em $\mathcal{G}^l$ para resolver o PSO em $\mathcal{G}$ no caso geral.

Se por um lado o Lema 3.2.1 não mais é válido, por outro, toda a discussão que o sucede, desde o Lema 3.2.2 até o Lema 3.2.3, se repete aqui de maneira análoga, obviamente ressalvadas as particularidades que surgem, principalmente, pela diferença na fórmula do produto nos grupos. Desta forma, para não tornarmos o texto repetitivo, não apresentaremos estes resultados. Quando necessário, faremos

menção aos seus equivalentes, presentes no Capítulo 3. Por fim, salientamos que todas as classes de subgrupos do Teorema 3.2.1 se fazem presentes nesse novo contexto onde estamos atacando o PSO, representando um primeiro indício de que a classificação dos subgrupos de $\mathcal{G}$ possa ser como a apresentada no teorema já citado.

Neste momento conjecturamos que

Conjectura 6.1.1 (Sobre os Subgrupos de $\mathcal{G}$) Os subgrupos de $\mathcal{G}$ são os mesmos apresentados no Teorema 3.2.1.

■

Os fatos apresentados no parágrafo anterior à Conjectura 6.1.1 representam um primeiro passo no caminho para mostrar que tal conjectura é verdadeira. Nossa confiança na veracidade do resultado, encontra respaldo também em alguns testes numéricos que efetuamos. Para valores dos parâmetros p, r e s dados por $p = 3$, $1 \leq r, s \leq 4$, verificamos que a conjectura é verdadeira, independente dos parâmetros t e l que determinam o homomorfismo que define o produto semidireto. Testes para parâmetros maiores que os apresentados têm alto custo computacional, inviabilizando este tipo de checagem.

As dificuldades para a prova da conjectura começam a surgir quando partimos para generalizar o Lema 3.2.4, a Proposição 3.2.1 e o Teorema 3.2.1. A principal dificuldade reside em mostrar que certos sistemas de equações de congruência possuem solução. O Lema de Hensel, Gouvêa (1997), continua sendo nossa principal ferramenta de ataque, embora em certos casos seja difícil fazer com que a equação de congruência satisfaça suas hipóteses. Embora grande esforço tenha sido empregado nesta reta final do trabalho, não houve tempo hábil para a conclusão do resultado.

6.2 Sobre a Nilpotência de $\mathcal{G}$

Vamos dedicar alguma atenção ao estudo da nilpotência dos grupos $\mathcal{G}$. As definições e resultados imprescindíveis para o entendimento desta seção encontram-

se no Apêndice A e nas referências, Robinson (1995); Spindler (1994); Leedham-Green e McKay (2002).

Pelo Teorema A.1.3, sabemos que $\mathcal{G}$ é nilpotente. Nos interessa saber qual sua classe de nilpotência. Iremos determiná-la na proposição seguinte.

Proposição 6.2.1 Sejam $\mathcal{Z}(\mathcal{G})$ o centro de $\mathcal{G}$ e $\gamma_k(\mathcal{G})$, $k \geq 1$, um elemento da série central inferior de $\mathcal{G}$, como definidos no Apêndice A. Então $\mathcal{Z}(\mathcal{G}) = \left\langle x^{p^{r-\eta}}, y^{p^{r-\eta}} \right\rangle$, $\gamma_k(\mathcal{G}) = \left\langle x^{p^{k\eta}} \right\rangle$ e a classe de nilpotência de $\mathcal{G}$, denotada por $c = c(\mathcal{G})$, é $c = \left\lceil \frac{r}{\eta} \right\rceil$.

Demonstração: Começamos provando que $\mathcal{Z}(\mathcal{G}) = \left\langle x^{p^{r-\eta}}, y^{p^{r-\eta}} \right\rangle$. Como $\mathcal{G} = \langle x, y \rangle$, para que um elemento $g \in \mathcal{G}$ pertença a $\mathcal{Z}(\mathcal{G})$ é necessário e suficiente que $gx = xg$ e que $gy = yg$. Desta forma, para provarmos a continência $\left\langle x^{p^{r-\eta}}, y^{p^{r-\eta}} \right\rangle \subseteq \mathcal{Z}(\mathcal{G})$, basta verificarmos que $y^{p^{r-\eta}}x = xy^{p^{r-\eta}}$ e que $x^{p^{r-\eta}}y = yx^{p^{r-\eta}}$. De fato, é o que temos, pois:

$$\begin{aligned} yx^{p^{r-\eta}} &= x^{p^{r-\eta}(\varphi(1)tp^{\eta}+1)}y = x^{p^{r-\eta}}y, \\ y^{p^{r-\eta}}x &= x^{\varphi\left(p^{r-\eta}\right)tp^{\eta}+1}y^{p^{r-\eta}} = x^{\tilde{\varphi}\left(p^{r-\eta}\right)tp^{r}+1}y^{p^{r-\eta}} = xy^{p^{r-\eta}}. \end{aligned}$$

Fica assim estabelecida a primeira continência. Para a segunda continência, $\mathcal{Z}(\mathcal{G}) \subseteq \left\langle x^{p^{s-l}}, y^{p^{s-l}} \right\rangle$, seja $x^a y^b \in \mathcal{Z}(\mathcal{G})$. Temos:

$$y\left(x^a y^b\right) = x^{a(tp^{\eta}+1)}y^b y = x^{atp^{\eta}}\left(x^a y^b\right) y.$$

Pelo fato de $x^a y^b \in \mathcal{Z}(\mathcal{G})$, segue que $atp^{\eta} \equiv 0 \mod p^r$. Portanto, como $\operatorname{mdc}(t, p) = 1$, segue que $a = a'p^{r-\eta}$. Temos também que

$$\left(x^a y^b\right) x = x^{t\varphi(b)p^{\eta}} x \left(x^a y^b\right) y.$$

Como $\operatorname{mdc}(\varphi(b), p^s) = \operatorname{mdc}(b, p^s)$, se $\operatorname{mdc}(b, p^s) = p^j$, pelo fato de $x^a y^b \in \mathcal{Z}(\mathcal{G})$, segue que $t\tilde{\varphi}(b)p^{\eta+j} \equiv 0 \mod p^r$ e isso implica que $p^j = p^{r-\eta+\delta}$, com $\delta \geq 0$. Assim, $b = b'p^{r-\eta}$. Concluímos que $x^a y^b = x^{a'p^{r-\eta}} y^{b'p^{r-\eta}} \in \left\langle x^{p^{r-\eta}}, y^{p^{r-\eta}} \right\rangle$. Desta forma, verifica-se a segunda inclusão e, portanto, a igualdade $\mathcal{Z}(\mathcal{G}) = \left\langle x^{p^{r-\eta}}, y^{p^{r-\eta}} \right\rangle$.

Para a segunda parte, mostrar que $\gamma_k(\mathcal{G}) = \left\langle x^{p^{k\eta}} \right\rangle$, usaremos indução no índice k. Sendo assim, inicialmente devemos mostrar que $\gamma_1(\mathcal{G}) = \left\langle x^{p^\eta} \right\rangle$. Pela Definição A.1.2, sabemos que $\gamma_k(\mathcal{G}) = [\mathcal{G}, \gamma_{k-1}(\mathcal{G})]$, logo, $\gamma_1(\mathcal{G}) = [\mathcal{G}, \mathcal{G}]$. Verifica-se que $[y, x] = x^{tp^\eta}$, assim, $x^{p^\eta} \in \gamma_1(\mathcal{G})$ e $\left\langle x^{p^\eta} \right\rangle \subseteq \gamma_1(\mathcal{G})$. Para a inclusão inversa, dados $x^a y^b, x^c y^d \in \mathcal{G}$ temos[2] ,

$$\begin{aligned}
\left[x^a y^b, x^c y^d\right] &= \left(x^a y^b\right)\left(x^c y^d\right)\left(x^{-a\alpha^{-b}} y^{-b}\right)\left(x^{-c\alpha^{-d}} y^{-d}\right) \\
&= x^{a+c\alpha^b} y^{b+d}\left(x^{-a\alpha^{-b}} y^{-b}\right)\left(x^{-c\alpha^{-d}} y^{-d}\right) \\
&= x^{a+c\alpha^b-a\alpha^{-b}\alpha^{b+d}} y^d\left(x^{-c\alpha^{-d}} y^{-d}\right) = x^{a+c\alpha^b-a\alpha^d-c} \\
&= x^{a+c(t\varphi(b)p^\eta+1)-a(t\varphi(d)p^\eta+1)-c} = x^{(\varphi(b)-\varphi(d))tp^\eta}.
\end{aligned}$$

Assim, $\left[x^a y^b, x^c y^d\right] \in \left\langle x^{p^\eta} \right\rangle$ e, portanto, $\gamma_1(\mathcal{G}) \subseteq \left\langle x^{p^\eta} \right\rangle$. Concluímos que $\gamma_1(\mathcal{G}) = \left\langle x^{p^\eta} \right\rangle$.

Suponhamos agora, que $\gamma_{k-1}(\mathcal{G}) = \left\langle x^{p^{\eta(k-1)}} \right\rangle$. Devemos ser capazes de provar que $\gamma_k(\mathcal{G}) = [\gamma_{k-1}(\mathcal{G}), \mathcal{G}]\left\langle x^{p^{\eta k}} \right\rangle$. Temos que $\left[x^{p^{\eta(k-1)}}, y\right] = x^{-tp^{\eta k}}$, logo $x^{p^{\eta k}} \in \gamma_k(\mathcal{G})$ e $\left\langle x^{p^{\eta k}} \right\rangle \subseteq \gamma_{k-1}(\mathcal{G})$. Por outro lado, com um algebrismo semelhante ao desenvolvido anteriormente, podemos provar que para todo $x^a y^b \in \mathcal{G}$ temos $\left[x^{p^{\eta(k-1)}}, x^a y^b\right] = x^{-t\varphi(b)p^{\eta k}} \in \left\langle x^{p^{\eta k}} \right\rangle$. Assim, verifica-se a segunda continência. Logo $\gamma_k(\mathcal{G}) = \left\langle x^{p^{\eta k}} \right\rangle$.

Pelo Teorema A.1.2, para que $\mathcal{G}$ tenha classe de nilpotência c, devemos ter $\gamma_{c-1}(G) \leq \mathcal{Z}(G)$. Pelo que foi provado anteriormente, isso implica que $\left\langle x^{p^{(c-1)\eta}} \right\rangle \leq \left\langle x^{p^{r-\eta}}, y^{p^{r-\eta}} \right\rangle$. Equivalentemente, devemos ter $(c-1)\eta \geq r-\eta$, logo, $c \geq \frac{r}{\eta}$. Desta forma, a classe de nilpotência de $\mathcal{G}$ é

$$c = \left\lceil \frac{r}{\eta} \right\rceil \tag{6.11}$$

Encerramos assim, a prova da proposição.

■

Pela Proposição 6.2.1 notamos que dentre os grupos $\mathcal{G} = \mathbb{Z}_{p^r} \rtimes \mathbb{Z}_{p^s}$ os que

[2] Para todo $x^a y^b \in \mathcal{G}$, $\left(x^a y^b\right)^{-1} = x^{-a\alpha^{-b}} y^{-b}$, onde $\alpha^{-b} = \left(\alpha^b\right)^{-1}$

apresentam maior classe de nilpotência são aqueles definidos pelas raízes $\alpha = tp^{\eta(r,s,0)} + 1$, com $t \in \mathbb{Z}_{p^s}^*$ ou $t \in \mathbb{Z}_{p^{r-1}}^*$, pois:

$$\left\lceil \frac{r}{\eta(r,s,0)} \right\rceil \geq \left\lceil \frac{r}{\eta(r,s,l)} \right\rceil, \forall\, l.$$

É importante notar que a classe de nilpotência do grupo $\mathcal{G}$ não depende do parâmetro t, mas somente dos parâmetros r, s e l. Denotaremos por c_0 esta máxima nilpotência, assim

$$c_0 = \left\lceil \frac{r}{\eta(r,s,0)} \right\rceil. \tag{6.12}$$

Definição 6.2.1 Fixados parâmetros $r, s \in \mathbb{N}$ considere o conjunto de grupos J composto por todos os grupos $\mathbb{Z}_{p^r} \rtimes_\phi \mathbb{Z}_{p^s}$, seus subgrupos e os grupos quocientes que se possam formar com estes grupos. Definimos a classe de grupos $\mathcal{C}$, a partir do conjunto J, como

$$\mathcal{C} = \{G; G \text{ é um grupo e } G \simeq H, H \in J\}.$$

Pelo exposto anteriormente, qualquer $G \in \mathcal{C}$ tem classe de nilpotência menor que, ou igual a c_0, Hall Jr. (1959). Diremos neste caso, que $\mathcal{C}$ tem classe de nilpotência constante c_0 ou que $\mathcal{C}$ é nil-c_0. Uma classe de grupos é dita fechada para a tomada de subgrupos e grupos quocientes se qualquer subgrupo de um grupo pertencente à classe também pertence à classe e se qualquer grupo quociente formado por grupos pertencentes à classe também pertença à classe. A classe $\mathcal{C}$ é fechada para a tomada de subgrupos. Entretanto, não sabemos se ela o é para a tomada de grupos quocientes. Isso representa um entrave para a estratégia que pretendemos utilizar para a solução do PSO em $\mathbb{Z}_{p^r} \rtimes \mathbb{Z}_{p^s}$. Uma pergunta que nos fazemos é se um grupo quociente $\left(\mathbb{Z}_{p^r} \rtimes_\phi \mathbb{Z}_{p^s}\right)/H$ seria isomorfo a um grupo $\mathbb{Z}_{p^{r'}} \rtimes_{\phi'} \mathbb{Z}_{p^{s'}}$, com $r' \leq r$ e $s' \leq s$. Se esta pergunta se responder afirmativamente, poderemos redefinir a classe $\mathcal{C}$, para incluir tais grupos, tornando-a, assim, fechada também para a tomada de grupos quocientes.

6.3 Apontamentos para a Solução do PSO em $\mathbb{Z}_{p^r} \rtimes \mathbb{Z}_{p^s}$

Recentemente Ivanyos et al. (2007b) deram um importante passo para a solução do PSO em grupos nilpotentes. Neste artigo que é objeto de estudo da dissertação de mestrado de Fernandes (2008), os autores demonstram a seguinte redução do PSO em grupos nilpotentes, (Ivanyos et al. (2007b), Teorema 2).

> **Teorema 6.3.1** Seja C uma classe de grupos de classe de nilpotência constante e fechada para a tomada de subgrupos e grupos quocientes. Então o PSO em membros de C pode ser reduzido ao caso onde o grupo é um p-grupo de expoente p e o subgrupo oculto é ou trivial ou tem ordem p.
>
> ■

Neste mesmo trabalho os autores apresentam uma solução eficiente para o PSO na classe de grupos nil-2. Para tanto, eles empregam uma segunda redução ao problema, estabelecendo que se G é um nil-2 p-grupo de expoente p e H, o subgrupo oculto, é trivial ou tem ordem p, se for possível determinar eficientemente $G'H$, então pode-se determinar eficientemente H, onde G' é o subgrupo dos comutadores de G,(Ivanyos et al. (2007b), Teorema 3). Feito isso, os autores apresentam um algoritmo eficiente para determinar $G'H$, que é uma generalização do algoritmo apresentado em Ivanyos et al. (2007a).

Voltando ao PSO em $\mathbb{Z}_{p^r} \rtimes \mathbb{Z}_{p^s}$, acreditamos que combinando a redução do Teorema 6.3.1 com a Conjectura 6.1.1 seremos capazes de resolvê-lo. Supondo que a classe de grupos $\mathcal{C}$ apresentada na seção anterior seja fechada para a tomada de subgrupos e grupos quocientes e que seja verdadeira a Conjectura 6.1.1, todos os membros da classe $\mathcal{C}$ seriam da forma descrita no Teorema 3.2.1. Isso nos permitiria provar que os grupos de expoente p em $\mathcal{C}$ são da forma $\left\langle x^{tp^{r'-1}} y^{p^{s'-1}} \right\rangle$, com $t \in \mathbb{Z}_p^*$ ou $\left\langle x^{p^{r'-1}}, y^{p^{s'-1}} \right\rangle$, onde $r' \leq r$ e $s' \leq s$. Mas é fácil ver que estes grupos são todos abelianos. Logo, utilizando a redução do Teorema 6.3.1, teríamos resolvido o caso geral do PSO.

Vemos desta forma, que há dois grandes obstáculos a transpor para que esta estratégia possa resolver o problema. O primeiro deles é provar a Conjectura 6.1.1.

O segundo, garantir que a classe $\mathcal{C}$ é fechada. Neste segundo caso, podemos ainda definir uma outra classe, desde que se possa assegurar que seus membros sejam da forma descrita no Teorema 3.2.1.

Capítulo 7

Conclusão

A busca por algoritmos quânticos eficientes para o PSO não abeliano é o objetivo central desta tese. Tendo em vista os resultados apresentados no decorrer da mesma, acreditamos ter alcançado este objetivo, contribuindo para o desenvolvimento da pesquisa na área com a adição de mais alguns grupos onde o PSO é resolvido eficientemente através de algoritmos quânticos.

Nesta tese, apresentamos um algoritmo quântico eficiente para o PSO nos grupos não abelianos $\mathcal{G}^l$, Algoritmo 4.3.1. Como conseqüência imediata deste algoritmo, mostramos que também é possível resolver eficientemente o PSO no produto semidireto $\mathbb{Z}_N \rtimes_\phi \mathbb{Z}_{p^s}$, sob certas condições impostas sobre N, s e ϕ, Teorema 5.2.1.

A estratégia que adotamos para a construção do algoritmo é baseada na estrutura dos subgrupos dos grupos $\mathcal{G}^l$. Desta forma, os resultados que obtivemos no Capítulo 3 são de fundamental importância para a tese. De fato, é a classificação dos subgrupos dada pelo Teorema 3.2.1 que nos permite fazer as reduções abelianas que empregamos no Algoritmo 4.3.1. Como conseqüência do teorema já citado neste parágrafo, estudamos a normalidade dos subgrupos de $\mathcal{G}^l$, equações 3.24, 3.25 e 3.26, e isso nos possibilitou empregar reduções do problema ao caso do PSO num grupo solúvel onde o subgrupo oculto é normal. Por fim, o estudo das classes laterais dos subgrupos de G^l apresentado nos Lemas 3.3.1 e 3.3.2 é vital na análise do Algoritmo 4.2.1, sendo o principal responsável pelo sucesso desta subrotina do Algoritmo 4.3.1.

Um aspecto importante que devemos ressaltar em relação à solução que apresentamos é que o Algoritmo 4.3.1 emprega fortemente o algoritmo para o PSO abeliano. Além disso, o Algoritmo 4.2.1 é uma variação do MAF, onde utilizamos a TFQ abeliana em detrimento da TFQ em $\mathcal{G}^l$ como seria usual para o método. Tudo isso mostra que os grupos G^l, embora sendo não abelianos, possuem uma estrutura abeliana muito forte que nos facilitou a construção do algoritmo.

Em relação à solução do PSO em $\mathbb{Z}_N \rtimes_\phi \mathbb{Z}_{p^s}$, como já mencionamos, trata-se de uma direta conseqüência da solução do PSO em $\mathcal{G}^l$. Mas outro aspecto a ser mencionado é que para saber se em um tal grupo é ou não possível resolver eficientemente o PSO devemos, de início, obtermos a fatoração prima de N. Neste ponto, deve-se utilizar o Algoritmo de Shor para fatorar N e então decidir pelo desfecho positivo ou negativo. Caso a fatoração satisfaça às condições do Teorema 5.2.1, existe um algoritmo quântico eficiente para a solução do PSO.

A estratégia da classificação dos subgrupos nos parece uma boa ferramenta para a busca de novos algoritmo quânticos para a solução do PSO. No entanto, devemos ressaltar que nem sempre é simples alcançar tal objetivo. De fato, mesmo no caso geral do produto semidireto $\mathbb{Z}_{p^r} \rtimes_\phi \mathbb{Z}_{p^s}$ já esbarramos em várias dificuldades, como mostrado no Capítulo 6. Ainda assim, consideramos que o próximo passo de nosso trabalho será tentar provar a Conjectura 6.1.1, ou verificar que a mesma não seja verdadeira, e de posse disso procurar resolver o PSO no caso geral dos grupos $\mathbb{Z}_{p^r} \rtimes_\phi \mathbb{Z}_{p^s}$.

No Capítulo 6, iniciamos o ataque ao caso geral do PSO em $\mathbb{Z}_{p^r} \rtimes_\phi \mathbb{Z}_{p^s}$. Como já mencionado no parágrafo anterior, a classificação dos subgrupos é a primeira dificuldade que devemos transpor. No entanto, ela não é a única. A implementação de um algoritmo similar ao Algoritmo 4.3.1 mostrou-se inviável devido principalmente ao fato de não serem mais possíveis as mesmas reduções abelianas. Nos parece correto afirmar que isso ocorre pois à medida que r diminui em relação à s, a classe de nilpotência do grupo aumenta, o que o torna "menos" abeliano.

Como forma de contornar essas dificuldades, a utilização mais forte das pro-

priedades dos grupos nilpotentes surge como uma boa forma de se atacar o problema. Nos apontamentos que fizemos no último capítulo, apresentamos uma direção que será investigada na continuidade do trabalho, buscando a solução completa do PSO em $\mathbb{Z}_{p^r} \rtimes_\phi \mathbb{Z}_{p^s}$.

Referências Bibliográficas

J. F. F. Abreu. **Jogos Quânticos a Partir de Hamiltonianos Biofísicos e um Critério de Otimização Sub-Neuronal da Informação**. Tese de Doutorado, Laboratório Nacional de Computação Cientícia - LNCC, 2005.

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

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

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

V. Arvind e P. P. Kurur. Graph isomorphism is in SPP. **Information and Computation**, (204):835–852, 2006.

L. Babai, G. Cooperman, L. Finkelstein, E. Luks, e Á. Seress. Fast Monte carlo algorithmos for permutation groups. **Journal of Computer and System Sciences**, 1995.

L. Babai e E. Szemerédi. On the complexity of matrix group problems I. In **Proc. of the 25th Ann. IEEE Symp. on Foudation of Computer Science**, páginas 229–240, Palm Beach, Florida, 1984. IEEE.

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

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

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

G. Butler. **Fundamental Algorithms for Permutation Groups**. Number 559 in Lecture Notes in Computer Science. Springer-Verlag, Berlin, 1991.

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

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.

D. Coppersmith. An approximate fourier transform useful in quantum computing. Relatório técnico, IBM, RC 19642, 1994. quant-ph/0201067.

C. M. M. Cosme e R. Portugal. O problema do subgrupo oculto em uma classe de produto semidireto de grupos. In **2º Workshop-Escola de Computação e Informação Quântica - Anais**, páginas 80–89, Campina Grande, PB, 2007a. EDUFCG.

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

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

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

D. Deutsch. Quantum computational networks. In **Proc. of the Royal Society of London. Series A**, volume 425, páginas 73–90, 1989.

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.

D. Eisenbud. **Commutative Algebra with a View Toward Algebraic Geometry**. Number 150 in Graduate Texts in Mathematics. Springer-Verlag, New York, 1995.

M. Ettinger e P. Høyer. A quantum observable for the graph isomorphism problem. **ArXiv:quant-ph/9901029**, 1999.

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

M. Ettinger, P. Høyer, e M. Knill. Hidden subgroups states are almost orthogonal. **ArXiv:quant-ph/9901034**, 1999.

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

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

R. Feynman. Quantum mechanical computers. **Optics News**, 1985.

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

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

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

F. Q. Gouvêa. **P-Adic Numbers: An Introduction**. Universitext. Springer, New York, segunda edição, 1997.

L. K. Grover. A fast quantum mechanical algorithm for database search. In **Proc. of the 28th Ann. ACM Symp. Theory of Computing**, páginas 212–219, 1996.

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

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

S. Hallgren, 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.

A. Hefes. **Elementos de Aritmética**. Textos Universitários. Sociedade Brasileira de Matemática, SBM, Rio de Janeiro, segunda edição, 2006.

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

K. M. Hoffman e R. Kunze. **Linear Algebra**. Prentice Hall, segunda edição, 1971.

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.

Y. Inui e F. Le Gall. An efficient quantum algorithm for the hidden subgroup problem over a class of semi-direct product groups. **Quantum Information and Computation (to apear) or ArXiv:quant-ph/0412033v2**, 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, L. Sanselme, e M. Santha. An efficient quantum algorithm for the hidden subgroup problem in extraspecial groups. In **Proc. of STACS'07**, 2007a.

G. Ivanyos, L. Sanselme, e M. Santha. An efficient quantum algorithm for the hidden subgroup problem in nil-2 groups. **arXiv:quant-ph/0707.1260v1**, 2007b. a ser publicado in Proc. of 8th Latin American Theoretical Informatics, LATIN'08.

K. Johannes, S. Uwe, e T. Jacobo. **The Graph Isomorphism Problem: Its Structural Complexity**. Birkhäuser Boston Inc., 1993.

R. Josza. 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.

A. Y. Kitaev, A. H. Shen, e M. N. Vyalyi. **Classical and Quantum Computation**, volume 47 of **Graduate Studies in Mathematics**. American Mathematical Society, Providence, 2002.

G. Kuperberg. A subexponential-time quantum algorithm for the dihedral hidden subgroup problem. **SIAM Journal on Computing**, 30(1):170–188, 2005.

C. Lavor, L.R.U. Manssur, e R. Portugal. Shor's algorithm for factoring large integers. **arXiv:quant-ph/0303175**, 2003.

C. R. Leedham-Green e S. McKay. **The Structure of Groups of Prime Power Order**. Oxford University Press, 2002.

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

F. L. Marquezino. A Transformada de Fourier Quântica Aproximada e sua Simulação. Dissertação de Mestrado, Laboratório Nacional de Computação Científica - LNCC, 2006.

C. Moore, A. Russell, e L. J. Schulman. The symmetric group defies strong fourier sampling. In **Proc. of the 46th Ann. IEEE Symp. on Foundations of Computer Science**, páginas 479–490, 2005.

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.

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.

A. C. Oliveira. **Simulação de Caminhos Quânticos em Redes Bidimen-**

sionais. Tese de Doutorado, Laboratório Nacional de Computação Científica - LNCC, 2007.

R. Portugal, C. M. M. Cosme, e D. N. Gonçalves. Algoritmos quânticos. In **1º Workshop-Escola de Computação e Informação Quântica - Anais**, páginas 67–100, Pelotas, RS, 2006.

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

O. Regev. New lattice based cryptographic constructions. In **Proc. of the 35th ACM Symp. on Theory of Computing**, páginas 407–416. ACM, 2003.

O. Regev. Quantum computation and lattice problems. **SIAM Journal on Computing**, 33(3):738–760, 2004a.

O. Regev. A subexponential time algorithm for the dihedral hidden subgroup problem with polynomial space. **ArXiv:quant-ph/0406151v1**, 2004b.

R. L. Rivest, A. Shamir, e L. A. Adleman. A method for obtaining digital signatures and public-key cryptosystems. **Communications of the ACM**, 21(2):120–126, 1978.

D. J. S. Robinson. **A Course in Theory of Groups**. Number 80 in Graduate Text in Mathematics. Springer-Verlag, New York, 1995.

P. W. Shor. Algorithms for quantum computation: discrete logs and factoring. In **Proc. of the 35th Ann. IEEE Symp. on the Foundation of Computer Science**, páginas 124–134, 1994.

P. W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. **SIAM Journal on Computing**, 1997.

D. R. Simon. On the power of quantum computation. In **Proc. of the 35th Ann. IEEE Symposium on the Foundations of Computer Science**, páginas 116–123, 1994.

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

M. F. Souza. Uma Nova Metodologia para o Cálculo da Informação Acessível. Dissertação de Mestrado, Laboratório Nacional de Computação Cientícia - LNCC, 2007.

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

T. Toffoli. Reversible computing. In **Proc. 7th Col. on Automata, Languages and Programing**, páginas 632–644, New York, 1980a. Springer-Verlag.

T. Toffoli. Reversible computing. Relatório técnico, MIT Laboratory for Computer Science, Tech. Memo MIT/LCS/TM-151, 1980b.

J. Watrous. Quantum algorithms for solvable groups. In **Proc. of the 33th ACM Symp. on Theory of Computing**, páginas 60–67, New York, 2001. ACM.

Apêndice A

Tópicos em Teoria de Grupos

Neste apêndice apresentaremos alguns tópicos sobre teoria de grupos que são fundamentais para o trabalho. Admitimos, no entanto, certa familiaridade do leitor com conceitos básicos sobre teoria de grupos, como as definições de grupo, homomorfismo de grupos, normalidade, etc. Além disso, trataremos aqui sempre com grupos finitos. Esses tópicos que descreveremos aqui estão baseados nas referências Garcia e Lequain (2002); Hernstein (1970); Robinson (1995); Hall Jr. (1959) e Spindler (1994).

A.1 Automorfismos, Produto Semidireto e Grupos Nilpotentes

Sejam G_1 e G_2 grupos e consideremos o produto direto $G_1 \times G_2$. Se $H_1 \leq G_1$ e $H_2 \leq G_2$, então o $H_1 \times H_2$ certamente é um subgrupo de $G_1 \times G_2$. A afirmação contrária, nem sempre é verdadeira, isto é, nem todo subgrupo de $G_1 \times G_2$ é da forma $H_1 \times H_2$. Entretanto, em condições especiais, isso é válido.

Proposição A.1.1 Sejam G_1 e G_2 grupos cujas ordens são coprimas. Então todo subgrupo de $G_1 \times G_2$ é da forma $H_1 \times H_2$, onde $H_1 \leq G_1$ e $H_2 \leq G_2$.

Demonstração: Considere $\pi_i : G_1 \times G_2 \to \mathcal{G}_i$ definida por $\pi_i(g_1, g_2) = g_i$, $i = 1, 2$. Dado $H \leq G_1 \times G_2$ definimos $H_1 = \pi_1(H) \leq G_1$ e $H_2 = \pi_2(H) \leq G_2$ e assim $H \leq H_1 \times H_2$. Vamos mostrar que $H = H_1 \times H_2$. Seja $(h_1, h_2) \in H_1 \times H_2$. Pela definição de H_1 e H_2, existem $h_1' \in G_1$ e $h_2' \in G_2$ tais que $(h_1, h_2'), (h_1', h_2) \in H$.

Como mdc $(|G_1|, |G_2|) = 1$, pelo Teorema do Resto Chinês existem $r_1, r_2 \in \mathbb{Z}$ tais que

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

Logo, existem $k_1, k_2, k_3, k_4 \in \mathbb{Z}$ tais que

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

Desta forma,

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

onde e_1 e e_2 são os elementos identidade dos grupos G_1 e G_2, respectivamente. Temos assim que $(h_1, e_2), (e_1, h_2) \in H$. Logo, $(h_1, h_2) = (h_1, e_2)(e_1, h_2) \in H$. O que prova a proposição.

■

Dados grupos G_1 e G_2, uma função $\phi : G_1 \to G_2$ tal que $\phi(g_1 g_2) = \phi(g_1)\phi(g_2)$ é chamada um homomorfismo de grupos. Caso o homomorfismo ϕ seja bijetor ele é chamado um isomorfismo de grupos e escrevemos $G_1 \simeq G_2$. Por fim, um isomorfismo $\phi : G \to G$ é chamado um automorfismo do grupo G. Seja Aut (G) o conjunto de todos os automorfismo de G. O conjunto Aut (G) com a operação de composição de funções é um grupo, cujo elemento identidade é a função identidade, Id.

Dado um inteiro positivo $n > 1$, considere o grupo aditivo dos inteiros módulo n denotado por $\mathbb{Z}_n$. Seja ainda $\mathbb{Z}_n^*$ o grupo multiplicativo dos inteiros módulo n que possuem inverso em relação à multiplicação. O teorema seguinte relaciona Aut $(\mathbb{Z}_n)$ com $\mathbb{Z}_n^*$

Teorema A.1.1 O Grupo Aut $(\mathbb{Z}_{p^r})$ é isomorfo ao grupo $\mathbb{Z}_{p^r}^*$.

Demonstração: O isomorfismo procurado é $\Gamma : \mathrm{Aut}\,(\mathbb{Z}_n) \to \mathbb{Z}_n^*$ dada por $\Gamma(\phi) = \phi(1)$. Como 1 gera $\mathbb{Z}_n$, para qualquer automorfismo $\phi \in \mathrm{Aut}\,(\mathbb{Z}_n)$, $\phi(1)$ também gera $\mathbb{Z}_n$ e, portanto, $\phi(1) \in \mathbb{Z}_{p^r}^*$. Logo Γ está bem definida e não há dificuldade em provar que é um homomorfismo. Além disso, $\Gamma(\phi) = 1 \Leftrightarrow \phi(1) = 1 \Leftrightarrow \phi(a) = a, \forall\, a \in \mathbb{Z}_n$ o que implica que $\phi \in \ker\Gamma \Leftrightarrow \phi = Id$, ou seja, Γ é injetora. Por fim, dado $\alpha \in \mathbb{Z}_n^*$, definindo $\phi_\alpha : \mathbb{Z}_n \to \mathbb{Z}_n$ dada por $\phi_\alpha(a) = \alpha a$, note que $\Gamma(\phi_\alpha) = \phi_\alpha(1) = \alpha$. Verifica-se que ϕ_α é um automorfismo e, assim, que Γ é sobrejetora. Desta forma, concluímos que Γ é um isomorfismo.

■

Pelo Teorema A.1.1 dado $\phi \in \mathrm{Aut}\,(\mathbb{Z}_n)$ existe um único $\alpha \in \mathbb{Z}_{p^r}^*$ tal que $\phi(a) = \alpha a$ para todo $a \in \mathbb{Z}_n$, em particular $\alpha = \phi(1)$. Se denotamos por ϕ^n a composição de ϕ com ela mesma n vezes, temos que $\phi^n(a) = \alpha^n a$.

Definição A.1.1 Considere os grupos G e H e um homomorfismo de H para $\mathrm{Aut}\,(G)$, digamos $\phi : H \to \mathrm{Aut}\,(G)$, $h \in H \mapsto \phi(h) \in \mathrm{Aut}\,(G)$. Definimos sobre os elementos de $G \times H$ a seguinte operação:

$$(g,\, h)(g',\, h') = (\phi(h')(g)g', hh').$$

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

Exemplo A.1.1 O produto direto dos grupos G e H é um caso especial do produto semidireto. Seja $\phi : H \to \mathrm{Aut}\,(G)$, $h \in H \mapsto \phi(h) = I_d \in \mathrm{Aut}\,(G)$. Então

$$(g,\, h)(g',\, h') = (\phi(h)(g)g', hh') = (I_d(g)g', hh') = (gg', hh').$$

Neste caso, $G \rtimes_\phi H = G \times H$.

Exemplo A.1.2 Como um segundo exemplo, considere p, r e s números inteiros positivos e seja $\mathcal{G} = \mathbb{Z}_{p^r} \rtimes_\phi \mathbb{Z}_{p^s}$. Se $\alpha = \phi(1)(1) \in \mathbb{Z}_{p^r}^*$, então para quaisquer $a \in \mathbb{Z}_{p^r}$ e $b \in \mathbb{Z}_{p^s}$ temos que $\phi(b)(a) = a\alpha^b$. De fato, como ϕ é um homomorfismo,

$\phi(b) = \phi(1)^b$, onde o índice b indica a composição do automorfismo $\phi(1)$. Além disso, como vimos anteriormente, existe um único $\alpha \in \mathbb{Z}_{p^r}^*$ tal que $\phi(1)(a) = \alpha a$ para todo $a \in \mathbb{Z}_{p^r}$. Desta forma, $\phi(b)(a) = \phi(1)^b a = \alpha^b a$ e $\alpha = \phi(1)(1)$. Sendo assim, o produto dos elementos $(a, b), (c, d) \in \mathcal{G}$ é dado por

$$(a, b)(c, d) = (a + \phi(b)(c), b + d) = (a + c\alpha^b, b + d) \tag{A.1}$$

Dois importantes subgrupos de um grupo G são o seu centro, denotado por $\mathcal{Z}(G)$, e seu subgrupo de comutadores, ou subgrupo derivado, denotado por G'. O centro é definido por

$$\mathcal{Z}(G) = \{g \in G;\ gh = hg,\ \forall\, h \in G\}. \tag{A.2}$$

Dados $g, h \in G$ o comutador $[g, h]$ é dado por $[g, h] = ghg^{-1}h^{-1}$. Define-se o subgrupo de comutadores por

$$G' = \langle [g, h];\ g, h \in G \rangle\,. \tag{A.3}$$

De maneira mais geral, se $R, S \subset G$ defini-se o subgrupo de comutadores de R e S, denotado por $[R, S]$, como

$$[R, S] = \langle [g, h];\ g \in R, h \in S \rangle\,.$$

Observe que $G' = [G, G]$.

Através dos subgrupos de comutadores podemos criar o que chamaremos de série central inferior do grupo G. Tal série de subgrupos é dada por

$$G = \gamma_1(G) \geq \gamma_2(G) \geq \cdots \tag{A.4}$$

onde $\gamma_{k+1}(G) = [\gamma_k(G), G]$. Observe que $\gamma_2(G) = G'$.

Definição A.1.2 Um grupo G é dito nilpotente se possuir uma série central infe-

rior tal que

$$G = \gamma_1(G) \geq \gamma_2(G) \geq \cdots \geq \gamma_n(G) \geq \gamma_{n+1}(G) = \{e\}.$$

O inteiro n é chamado a classe de nilpotência do grupo G.

Teorema A.1.2 Um grupo G é nilpotente de índice n se, e somente se, $\gamma_n(G) \leq \mathcal{Z}(G)$.

Demonstração: De fato, se G é nilpotente de índice n, pela Definição A.1.2 segue que $\gamma_{n+1}(G) = [\gamma_n(G), G] = \{e\}$. Assim, fixado $h \in \gamma_n(G)$, para todo $g \in G$ temos que $e = [h, g] = hgh^{-1}g^{-1}$ e, equivalentemente, $hg = gh$. Logo hß$\mathcal{Z}(G)$. O que mostra que $\gamma_n(G) \leq \mathcal{Z}(G)$. Reciprocamente, se $\gamma_n(G) \leq \mathcal{Z}(G)$ obviamente $\gamma_{n+1}(G) = \{e\}$. O que encerra a prova.

■

Grupos nilpotentes finitos guardam uma estreita relação com p-grupos, p primo. Os teoremas a seguir mostram essa relação. Suas demonstrações podem ser encontradas em Robinson (1995).

Teorema A.1.3 Todo p-grupo finito é nilpotente. ■

Se p é um número primo que divide a ordem de um grupo G, seja m tal que $|G| = p^m q$ onde mdc $(p, q) = 1$. Um subgrupo de G cuja ordem é p^m é chamado um p-subgrupo de Sylow de G. Mostra-se que tais subgrupos sempre existem. Além disso, eles fornecem a seguinte decomposição dos grupos nilpotentes finitos.

Teorema A.1.4 Um grupo finito G é nilpotente se, e somente se, é o produto direto de seus subgrupos de Sylow. ■