ISSN 1984-820X
Anais do CNMAC v.3
PUBLICAÇÃO DA SBMAC
CNMAC2010
XXXIII CONGRESSO NACIONAL DE MATEMÁTICA APLICADA E COMPUTACIONAL

Algoritmos Quânticos em Tempo Sub-exponencial sobre 2-Grupos

Demerson N. Gonçalves[1,2], **Renato Portugal**[2],
[1]Universidade Católica de Petrópolis,
25685-070, Petrópolis, RJ
[2]Laboratório Nacional de Computação Científica,
25651-075, Petrópolis, RJ
E-mail: [1]demerson.goncalves@ucp.br, [2]portugal@lncc.br

Resumo: *Neste trabalho, apresentamos um novo algoritmo quântico com complexidade de tempo sub-exponencial* $2^{O(\sqrt{n})}$ *para o problema do subgrupo oculto (PSO) sobre 2-grupos de ordem* 2^{n+1}*, que possuem subgrupos cíclicos de ordem* 2^n*, para todo inteiro* $n \geq 3$*. O nosso método combina as idéias do algoritmo de Kuperberg para o PSO diedral com um critéiro de redução à subgrupos cíclicos, que está presente em alguns algoritmos apresentados na literatura.*

Palavras-chave: *Computação Quântica, Algoritmos Quânticos, Problema do Subgrupo Oculto, Transformada de Fourier*

1 Introdução

Já se passaram mais do que 25 anos desde o início da Computação Quântica com o trabalho pioneiro de David Deutsch [3] sobre a máquina de Turing quântica. A área de algoritmos quânticos está em pleno desenvolvimento como mostram os dois recentes artigos de revisão [2, 10].

Uma enorme classe de algoritmos foi desenvolvida para atacar problemas algébricos [2]. Uma percentagem muito grande destes problemas é formulada em termos da teoria de grupos computacionais. A maioria pode ser colocada na forma de busca por um subgrupo oculto, que é conhecida com o nome de *Problema do Subgrupo Oculto* (PSO) [9]. Este problema pode ser definido da seguinte maneira: dado um grupo finito G e uma função f que é constante nas classes laterais de um subgrupo H de G e distinta em cada classe lateral, determinar um conjunto gerador para H, a partir de informações obtidas da função f. Dizemos que a função f oculta o subgrupo H em G, ou ainda que f separa as classes laterais de H em G. Assim, o subgrupo H é dito o subgrupo oculto em G por f.

Um algoritmo ingênuo para o PSO em qualquer grupo finito G, consiste em chamar a função separadora de classes laterais várias vezes, cada vez, calculando $f(g)$ e verificando se $f(g) = f(e)$, para todo $g \in G$. Sempre que encontramos um elemento g com a propriedade $f(g) = f(e)$, nós acrescentamos este elemento ao conjunto H. Assim, após $|G|$ chamadas à função f seremos capazes de determinar o subgrupo H. Claramente este algoritmo é ineficiente, e sua complexidade é $O(|G|)$. Um algoritmo quântico para o PSO é dito eficiente, quando a complexidade computacional do algoritmo é polilogaritmo na ordem do grupo, isto é, $O(\text{poli}(\log |G|))$. São exemplos de algoritmos quânticos eficientes para o PSO, o algoritmo de Simon [13] e o algoritmo de Shor [12] para fatoração de números inteiros e cálculo de logaritmo discreto. No problema de Simon, temos $G = \mathbb{Z}_2^n$, com a promessa de que existe um elemento $y \in \mathbb{Z}_2^n$ tal que $f(x) = f(x+y)$ para todo $x \in \mathbb{Z}_2^n$; neste caso, o subgrupo oculto é dado por $H = \{0, y\}$, onde y é o parâmetro a ser determinado. No algoritmo de Shor, $G = \mathbb{Z}_N$, onde N é o número que desejamos fatorar,

f é dada por $f(x) = y^x \bmod N$, com $y \in \mathbb{Z}_N^*$ satisfazendo $y^r \equiv 1 \bmod N$. Neste caso, H é o subgrupo de $\mathbb{Z}_N$ gerado pelo elemento r.

Os algoritmos de Simon e Shor são casos particulares do PSO abeliano. É conhecido na literatura que para grupos abelianos finitos arbitrários o PSO pode ser resolvido eficientemente em um computador quântico [9]. Infelizmente, não é conhecida nenhuma solução geral para o caso de grupos não-abelianos.

Dois problemas importantes que vem merecendo a atenção da comunidade científica e que continuam em aberto são os PSOs nos grupos não-abelianos simétrico e diedral. Um algoritmo eficiente para o primeiro caso implica numa solução eficiente para o problema de isomorfismo de grafos [1], e o último essencialmente resolve instâncias do problema do menor vetor em um reticulado, tendo este aplicações importantes em criptografia [11].

O grupo diedral foi o primeiro grupo não-abeliano para o qual o PSO foi estudado. Em parte, essa iniciativa deu-se pela simplicidade da estrutura de seus subgrupos e pelo grande número de subgrupos de ordem 2. O grupo diedral de ordem $2N$ é formado pelas rotações e reflexões do plano que preservam um polígono regular com N vértices. Algebricamente, o grupo diedral pode ser representado como o produto semidireto de grupos $D_N = \mathbb{Z}_N \rtimes_\phi \mathbb{Z}_2$, onde o homomorfismo $\phi : \mathbb{Z}_2 \to \mathrm{Aut}(\mathbb{Z}_N)$ é tal que $\phi(b)(a) = (-1)^b a$ para todo $b \in \mathbb{Z}_2$ e $a \in \mathbb{Z}_N$, e $\mathrm{Aut}(\mathbb{Z}_N)$ denota o grupo de automorfismos de $\mathbb{Z}_N$. Para resolver o PSO sobre D_N, Ettinger e Høyer [4] mostraram que é suficiente resolver no caso onde o subgrupo oculto possui ordem 2. A idéia principal do algoritmo dado por esses autores é aplicar a transformada de Fourier abeliana ao produto direto de grupos $\mathbb{Z}_N \times \mathbb{Z}_2$. Este método, que não usa o fato de D_N ser não-abeliano, é suficiente para obter informações sobre o subgrupo oculto. Entretanto, o pós-processamento do algoritmo, que consiste em obter um conjunto de geradores para o subgrupo oculto a partir destas informações toma tempo exponencial, tornando assim o algoritmo ineficiente. Embora não seja conhecido nenhum algoritmo quântico em tempo polinomial para o PSO diedral, Kuperberg [7] descobriu um algoritmo quântico com complexidade sub-exponencial $2^{O(\sqrt{\log N})}$. A partir deste ponto, começamos a nos questionar se o método dado por Kuperberg para o PSO diedral poderia ser estendido para outros grupos não-abelianos, como por exemplo, para 2-grupos[1]

Neste trabalho, nós respondemos esta pergunta de uma maneira positiva. Nós mostramos que o PSO sobre 2-grupos de ordem 2^{n+1} que possuem um subgrupo cíclico de ordem 2^n, pode ser resolvido por um computador quântico em tempo sub-exponencial $2^{O(\sqrt{n})}$. Nós reduzimos o PSO ao problema de encontrar subgrupos da forma $H = \langle x^a y \rangle$, onde $a \in \mathbb{Z}_{2^n}$ é o parâmetro a ser determinado. Este resultado estende a classe analisada na Ref. [5], que se concentrou em grupos metacíclicos da forma $\mathbb{Z}_p \rtimes \mathbb{Z}_{q^s}$ onde p e q são números primos e s um inteiro positivo.

2 Caracterização do Problema

Nesta seção, mostramos que o caso geral do PSO sobre 2-grupos se reduz ao PSO sobre certas classes de grupos bem conhecidas, a saber, os grupos quasi-diedral e quatérnios generalizados. Consideremos então o seguinte teorema.

Teorema 2.1. *Seja G um grupo tal que $|G| = 2^{n+1}$ onde $n \geq 3$ e tal que G possui um subgrupo cíclico maximal $\langle x \rangle$ (isto é, $|\langle x \rangle| = 2^n$). Então G é isomorfo a um dos seguintes grupos:*

i) *O grupo Q_{2^n} dos quatérnios generalizados:* $Q_{2^n} = \left\langle x, y \mid x^{2^n} = 1,\ y^2 = x^{2^{n-1}},\ y^{-1}xy = x^{-1} \right\rangle$.

ii) *O grupo diedral:* $D_{2^n} = \left\langle x, y \ \mid x^{2^n} = y^2 = 1,\ y^{-1}xy = x^{-1} \right\rangle$.

iii) *O grupo quasi-diedral:* $QD_{2^n} = \left\langle x, y \mid x^{2^n} = y^2 = 1,\ y^{-1}xy = x^{2^{n-1}-1} \right\rangle$.

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

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

Demonstração: Veja ref. [8].

■

Primeiro, começamos investigando os grupos $P_{2,n}$. Este grupo pode ser encarado como um produto semidireto da forma $P_{2,n} \simeq \mathbb{Z}_{2^n} \rtimes_\alpha \mathbb{Z}_2$, onde o homomorfismo α é definido por $\alpha = 2^{n-1} + 1$. O grupo $P_{2,n}$ é nilpotente de classe 2; assim, o PSO nesta classe de grupos pode ser resolvido eficientemente em um computador quântico [6]. Na classe ii), temos o grupo diedral, podendo também ser representado por um produto semidireto $D_{2^n} \simeq \mathbb{Z}_{2^n} \rtimes_\phi \mathbb{Z}_2$, onde $\phi = 2^n - 1$. Neste caso, o melhor algoritmo quântico conhecido para o PSO é devido à Kuperberg [7], e possui complexidade sub-exponencial $2^{O(\sqrt{n})}$. Por fim, consideremos o PSO sobre os grupos das classes i) e iii). Estes grupos são nilpotentes de classe n, logo não podemos aplicar os resultados apresentados em [6], para grupos nilpotentes de classe de nilpotência constante, nestas classes de grupos. Assim, o PSO sobre 2-grupos de ordem 2^{n+1} que possuem um subgrupo cíclico de ordem 2^n, se reduz ao PSO sobre os grupos das classes i) e iii).

Na próximas seções, apresentaremos algoritmos quânticos com complexidade de tempo sub-exponencial para o PSO sobre os grupos das classes i) e iii). Nossa abordagem reúne as idéias apresentadas em [7], para o PSO diedral, com um critério de redução primeiramente utilizado por [4]. Este critério consiste basicamente em conhecer a estrutura dos subgrupos de um determinado grupo e utilizar a transformada de Fourier abeliana para obter informações sobre o subgrupo oculto.

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

O grupo quasi-diedral, apresentado no Teorema 2.1, pode também ser representado pelo produto semidireto $QD_{2^n} = \mathbb{Z}_{2^n} \rtimes_\phi \mathbb{Z}_2$, onde o homomorfismo $\phi : \mathbb{Z}_2 \to \mathrm{Aut}(\mathbb{Z}_{2^n})$ é tal que $\phi(1)(1) = 2^{n-1} - 1$. Denotamos por $x = (1, 0)$ e $y = (0, 1)$ os geradores do QD_{2^n} nesta nova notação, assim, cada elemento $x^a y^b$ de QD_{2^n} pode ser representado como (a, b) com $a \in \mathbb{Z}_{2^n}$ e $b \in \mathbb{Z}_2$.

A proposição seguinte classifica todos os subgrupos de QD_n.

Proposição 3.1. *Os subgrupos de QD_{2^n} são da forma $\left\langle x^{2^i} \right\rangle$ ou $\left\langle x^{2^i}, x^a y \right\rangle$ para todo $0 \le i \le n$ e $0 \le a \le 2^n - 1$.*

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

■

Seja f a função que oculta o subgrupo H em QD_n. De acordo com a Proposição 3.1 existem duas possibilidades para o subgrupo H, ou de forma equivalente, existem dois parâmetros a serem determinados i e a. O parâmetro a é o mais difícil de ser encontrado. Mostraremos como a pode ser determinado na próxima seção.

Agora, observe como o problema do subgrupo oculto em QD_{2^n} pode ser reduzido ao problema de encontrar subgrupos cíclicos. De fato, primeiro rodamos o algoritmo descrito na Seção 3.1. Se o algoritmo resulta o valor de a e se $f(x^a y) = f(e)$ (lembre-se que f é prometida ser constante nas classes laterais do subgrupo H) então $H = \left\langle x^{2^i}, x^a y \right\rangle$. Caso contrário, sabemos que $H = \left\langle x^{2^i} \right\rangle$. Podemos determinar i calculando $f(x^{2^i})$ para todo $i = 0, \ldots, n$. Quando encontramos um inteiro

i com a propriedade $f(x^{2^i}) = f(e)$ então concluímos que x^{2^i} é um elemento gerador de H. Assim, o PSO em QD_{2^n} pode ser reduzido ao problema de determinar o gerador do subgrupo $\langle x^a y\rangle$, ou seja, determinar a, um número entre 0 e $2^n - 1$.

Antes de exibirmos o algoritmo que determina o parâmetro a, façamos uma última redução. Mostraremos que o problema de determinar a reduz-se ao problema de determinar a paridade r_0 de a. Com efeito, suponhamos que, dada uma função $f : QD_{2^n} \to X$ que oculta o subgrupo $H = \langle x^a y\rangle$ em QD_{2^n}, existe um procedimento quântico que determina r_0. Então, podemos escrever $a = 2a_1 + r_0$, onde a_1 é um elemento arbitrário em $\mathbb{Z}_{2^{n-1}}$ e r_0 é conhecido. Observe que r_0 fornece o bit menos significativo de a. Agora, defina a função $f^{(1)} : QD_{2^{n-1}} \to X$ tal que $f^{(1)}(x^s y^t) = f(x^{2s+tr_0} y^t)$. Temos que $f^{(1)}$ oculta o subgrupo $H^{(1)} = \langle x^{a_1} y\rangle$ de $QD_{2^{n-1}}$, logo, existe um procedimento quântico que determina a paridade r_1 de a_1, com alta probabilidade. Este procedimento acha o segundo bit menos significativo de a. De forma geral, pondo $f^{(0)} := f$, e definindo $f^{(k)} : QD_{2^{n-k}} \to X$ tal que $f^{(k)}(x^s y^t) = f^{(k-1)}(x^{2s+tr_{k-1}} y^t)$, para todo $1 \le k \le n-1$, onde r_{k-1} é o k-ésimo bit menos significativo de a, a função $f^{(k)}$ oculta o subgrupo $H^{(k)} = \langle x^{a_k} y\rangle$ em $QD_{2^{n-k}}$. Portanto, existe um procedimento quântico que encontra o k-ésimo bit menos significativo de a. Isto implica que, rodando o procedimento que acabamos de descrever, $O(n)$ vezes, obtemos todos os bits de a, e consequentemente, a.

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

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

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

Algoritmo 1 Procedimento de Amostragem sobre QD_{2^n}

Entrada: um inteiro n e a função $f : QD_{2^n} \to X$, onde X é um conjunto finito.
Saída: um estado quântico de 1 q-bit.

1. Prepare o estado quântico

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

2. Meça o último registrador:

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

3. Aplique a transformada de Fourier

$$F_{\mathbb{Z}_{2^n}} |j\rangle := \frac{1}{\sqrt{2^{n+1}}} \sum_{k=0}^{2^n-1} e^{2\pi i j \frac{k}{2^n}} |k\rangle$$

ao primeiro registrador.

4. Meça o primeiro registrador:

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

A saída do Algoritmo 1 é um estado da forma $\left|\psi_k^{a,2^n}\right\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i k \frac{a}{2^n}} |1\rangle\right)$, para algum k uniformemente distribuído em $\mathbb{Z}_{2^n}$. Nosso objetivo, é obter o estado $\left|\psi_{2^{n-1}}^{a,2^n}\right\rangle =$

$\frac{1}{\sqrt{2}}\left(|0\rangle + e^{\pi i a}|1\rangle\right)$, pois, uma única aplicação da transformada de Hadamard em $\left|\psi_{2^{n-1}}^{a,2^n}\right\rangle$ revela a paridade de a. De fato,

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

Quando obtemos o estado $\left|\psi_k^{a,2^n}\right\rangle$, o parâmetro k é um número uniformemente randômico no conjunto $\{0,1,\ldots,2^n-1\}$, logo a probabilidade de obtermos o estado $\left|\psi_{2^{n-1}}^{a,2^n}\right\rangle$ direto do Algoritmo 1 é $1/2^n$, que é exponencialmente pequena. Vamos mostrar como obter o estado $\left|\psi_{2^{n-1}}^{a,2^n}\right\rangle$ em tempo sub-exponencial. O procedimento é o seguinte: use o Algoritmo 1 para produzir $2^{O(\sqrt{n})}$ estados da forma $\left|\psi_k^{a,2^n}\right\rangle$, com k uniformemente distribuído em $\mathbb{Z}_{2^n}$. Vamos chamar o conjunto formado por estes estados de L_0. Dois estados $\left|\psi_{k_1}^{a,2^n}\right\rangle$ e $\left|\psi_{k_2}^{a,2^n}\right\rangle$ são escolhidos no conjunto L_0 se k_1 e k_2 possuem o mesmo conjunto de $k = \lceil\sqrt{n-1}\rceil$ bits menos significativos. Em seguida, faça o produto tensorial $\left|\psi_{k_1}^{a,2^n}\right\rangle \otimes \left|\psi_{k_2}^{a,2^n}\right\rangle$. O resultado deste produto é o estado

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

Aplique a porta C-NOT ao estado dado pela expressão (1), usando o primeiro q-bit como q-bit de controle. O resultado desta aplicação é

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

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

$$\left|\psi_{k_1-k_2}^{a,2^n}\right\rangle = \frac{1}{\sqrt{2}}(|0\rangle + e^{2\pi i\frac{(k_1-k_2)a}{2^n}}|1\rangle). \tag{3}$$

O estado quântico com rótulo k_1-k_2, possui os $k = \lceil\sqrt{n-1}\rceil$ bits menos significativos iguais a zero. Seja L_1 o conjunto formado por todos os estados $\left|\psi_{k_1-k_2}^{a,2^n}\right\rangle$ com esta propriedade. Repetindo esse procedimento k vezes, obtemos com alta probabilidade um conjunto L_k que possui pelo menos um estado da forma $\left|\psi_{2^{n-1}}^{a,2^n}\right\rangle$.

Agora precisamos mostrar que o conjunto L_k resulta pelo menos um estado da forma $\left|\psi_{2^{n-1}}^{a,2^n}\right\rangle$ com alta probabilidade. De fato, se a quantidade de estados de cada conjunto L_j for maior que $2^{\sqrt{n-1}}$ para todo $j = 0,\ldots,k$, então quase todos os estados em L_j podem ser usados para formar um par $\left(\left|\psi_{k_1}^{a,2^n}\right\rangle, \left|\psi_{k_2}^{a,2^n}\right\rangle\right)$ tal que k_1-k_2 possui os kj bits menos significativos iguais a zero. Assim, $|L_{j+1}|/|L_j| \approx 1/4$. Uma análise mais cuidadosa mostra que tomando $|L_0| = 2^{O(\sqrt{n})}$ é suficiente para obter, com alta probabilidade, um conjunto L_k que contenha pelo menos um estado da forma $\left|\psi_{2^{n-1}}^{a,2^n}\right\rangle$.

Assim, temos o seguinte resultado.

Teorema 3.1. *Existe um algoritmo quântico que resolve PSO em QD_{2^n}, com alta probabilidade e com complexidade de tempo $2^{O(\sqrt{n})}$.*

4 O Grupo Q_{2^n}

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

Como vimos no Teorema 2.1, o grupo Q_{2^n} de ordem 2^{n+1} é definido como

$$Q_{2^n} = \left\langle x, y \mid x^{2^n} = 1,\ y^2 = x^{2^{n-1}},\ y^{-1}xy = x^{-1} \right\rangle. \tag{4}$$

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

Proposição 4.1. *Os elementos de Q_{2^n} podem ser escritos da forma $x^a y^b$, com $0 \leq a \leq 2^n - 1$ e $b = 0, 1$.*

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

■

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

Proposição 4.2. *Os subgrupos de Q_{2^n} são da forma $\left\langle x^{2^i} \right\rangle$ ou $\left\langle x^{2^i}, x^a y \right\rangle$ para todo $0 \leq i \leq n$ e $0 \leq a \leq 2^n - 1$.*

Demonstração: Análoga à Proposição 3.1.

■

De forma inteiramente análoga à Seção 3, podemos verificar que o problema do subgrupo oculto no grupo Q_{2^n} se reduz ao problema de determinar um subgrupo cíclico da forma $H = \langle x^a y \rangle$, onde a um número entre 0 e $2^n - 1$. Agora note que, como existe uma bijeção entre os elementos de Q_{2^n} e $\mathbb{Z}_{2^n} \times \mathbb{Z}_2$, podemos construir o estado quântico

$$\frac{1}{\sqrt{2^{n+1}}} \sum_{t=0}^{2^n-1} \sum_{s=0}^{1} |t\rangle\, |s\rangle\, \left| f(x^t y^s) \right\rangle. \tag{5}$$

O estado (5) corresponde ao estado inicial do Algoritmo 1.

Portanto, passando para o Algoritmo 1 a função $f : Q_{2^n} \to X$ que oculta o subgrupo $H = \langle x^a y \rangle$ em Q_{2^n} e seguindo como na seção anterior, resolvemos o PSO em Q_{2^n} em tempo sub-exponencial. Isto nos leva ao seguinte resultado:

Teorema 4.1. *Existe um algoritmo quântico que resolve PSO em Q_{2^n}, com alta probabilidade e com complexidade de tempo $2^{O(\sqrt{n})}$.*

5 Conclusão

Neste trabalho, apresentamos novos algoritmos quânticos para o PSO sobre uma família de 2-grupos não-abelianos de ordem 2^{n+1}, que possuem subgrupos cíclicos de ordem 2^n. Conhecendo a estrutura dos subgrupos do grupo estudado, nós mostramos que o PSO se reduz ao problema de encontrar subgrupos cíclicos. Este critério de redução foi primeiramente utilizado por [4]. Em seguida, nós adaptamos os resultados obtidos em [7] para o PSO no grupo diedral e exibimos um algoritmo quântico com complexidade de tempo sub-exponencial, isto é, $2^{O(\sqrt{n})}$.

O fato de encontrarmos algoritmos com complexidade de tempo sub-exponencial em vez de complexidade polinomial reforça a idéia prevalecente na literatura de que o PSO não-abeliano geral não admite solução eficiente. Esperamos que as idéias apresentadas neste texto possam contribuir de alguma forma no desenvolvimento de novos algoritmos quânticos para outras instâncias do PSO não-abeliano.

Agradecimentos

Agradecemos o suporte financeiro do CNPq.

Referências

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

[2] Andrew M. Childs and Wim van Dam. Quantum algorithms for algebraic problems. *Rev. Mod. Phys.*, 82(1):1–52, Jan 2010.

[3] David Deutsch. Quantum theory, the church-turing principle and the universal quantum computer. *Proc. Royal Society London Ser. A*, pages 96–117, 1985.

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

[5] Demerson N. Gonçalves, Renato Portugal, and Carlos M. M. Cosme. Solutions to the hidden subgroup problem on some metacyclic groups. In *Theory of Quantum Computation, Communication, and Cryptography, Lecture Notes in Computer Science Vol. 5906*, pages 1–9. Springer, 2009.

[6] G. Ivanyos, L. Sanselme, and M. Santha. An efficient quantum algorithm for the hidden subgroup problem in nil-2 groups. *Proc. of 8th Latin American Theoretical Informatics, LATIN'08*, 2007.

[7] G. Kuperberg. A Subexponential-Time Quantum Algorithm for the Dihedral Hidden Subgroup Problem. *SIAM J. Comput.*, 35(1):170–188, 2005.

[8] J. H. Kwak and M. Y. Xu. *Finite Group Theory for Combinatorists*, volume 1. Postech, 2005.

[9] C. Lomont. The Hidden Subgroup Problem - Review and Open Problems. *Quantum Physics, Abstract quant-ph/0411037*, November 2004.

[10] Michele Mosca. Quantum algorithms. In *Encyclopedia of Complexity and Systems Science*, pages 7088–7118. 2009.

[11] O. Regev. Quantum Computation and Lattice Problems. *SIAM Journal on Computing*, 33(3):738–760, 2004.

[12] 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*, pages 124–134, 1994.

[13] D. R. Simon. On the Power of Quantum Computation. In *Proceedings of the 35th Annual Symposium on Foundations of Computer Science*, pages 116–123, Los Alamitos, CA, 1994. Institute of Electrical and Electronic Engineers Computer Society Press.