Algoritmos Quânticos para uma Classe de Produtos Semi-diretos de Grupos

Demerson N. Gonçalves, **Renato Portugal**,
Laboratório Nacional de Computação Científica - LNCC
25651-075, Petrópolis, RJ
E-mail: dnunes@lncc.br, portugal@lncc.br,

Carlos Magno M. Cosme
UFVJM - Departamento de Matemática
Campus Teófilo Otoni
39801-000, Teófilo Otoni, MG
E-mail: cmagnomc@ufvjm.edu.br.

Resumo

Nós apresentamos um algoritmo quântico eficiente para o problema do subgrupo oculto (PSO) sobre produto semi-direto de grupos $\mathbb{Z}_N^m \rtimes_\phi \mathbb{Z}_p$, onde p é um número primo ímpar, m, N inteiros positivos. Nós mostramos que impondo algumas restrições sobre a fatoração prima de N, o grupo $\mathbb{Z}_N^m \rtimes_\phi \mathbb{Z}_p$ é isomorfo ao produto direto de grupos $G' = \mathbb{Z}_{N'}^m \times (\mathbb{Z}_{p^r}^m \rtimes_\psi \mathbb{Z}_p)$. A partir deste ponto nós resolvemos o PSO em G' determinando uma solução eficiente para o PSO em cada parte do produto direto de grupos. Este algoritmo quântico é exponencialmente mais rápido do que qualquer algoritmo clássico para a mesma finalidade.

1 Introduction

A maioria dos algoritmos quânticos com ganho exponencial em relação aos seus análogos clássicos, tais como o algoritmo de Simon [20] e o algoritmo de Shor para cálculo de ordem e logaritmo discreto [19], são obtidos resolvendo algumas instâncias do problema do subgrupo oculto (PSO). O problema consiste em determinar os geradores de um subgrupo H de um grupo finito G oculto por uma função que é constante nas classes laterais do subgrupo H e distinta em cada classe lateral. Para ser eficiente, um algoritmo quântico para o PSO tem rodar em tempo polilogaritmo na ordem do grupo. Um fato bem estabelecido na literatura é que para grupos abelianos o PSO pode ser resolvido eficientemente por um computador quântico [10], enquanto nenhuma solução eficiente é conhecida para o caso geral de grupos não abelianos [8]. Dois importantes casos que continuam em aberto são os PSOs nos grupos simétrico e diedral. Um algoritmo eficiente para o primeiro caso implica numa solução eficiente para o problema de isomorfismo de grafos [2, 1], e o último essencialmente resolve instâncias do problema do menor vetor em um reticulado, tendo este aplicações importantes em criptografia [17, 15, 16].

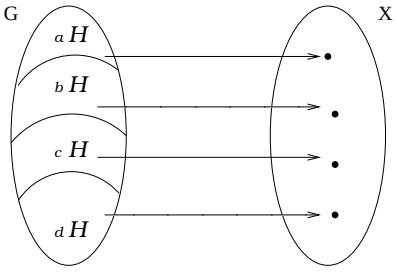

Figura 1: A função f é constante nas classes laterais de H e distinta em cada classe lateral.

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 semi-direto 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 $a \in \mathbb{Z}_N$, onde $\mathrm{Aut}(\mathbb{Z}_N)$ denota o grupo de automorfismos de $\mathbb{Z}_N$.

Para resolver o PSO sobre D_N, Ettinger e Høyer [7] mostraram que é suficiente resolver o caso onde o subgrupo oculto possui ordem 2. A idéia principal do algoritmo dado em [7] 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. No caso do grupo $\mathbb{Z}_N^m \rtimes_\phi \mathbb{Z}_p$ que abordaremos no nosso trabalho, utilizaremos apenas a transformada de Fourier abeliana, e mostraremos que ela é suficiente para resolver o PSO em $\mathbb{Z}_N^m \rtimes_\phi \mathbb{Z}_p$ em tempo polinomial.

Todo algoritmo quântico conhecido com ganho exponencial em relação aos seus equivalentes clássicos utilizam a transformada de Fourier. Para grupos não abelianos a transformada de Fourier é descrita em termos das representações irredutíveis do grupo, isto é, homomorfismos ρ de G no conjunto $\mathrm{GL}(V)$ das matrizes invertíveis sobre V, onde V é um espaço de dimensão finita qualquer. Assim, dada uma função $f : G \to \mathbb{C}$ e uma representação irredutível ρ de G de dimensão d_ρ, podemos definir a transformada de Fourier de f na representação ρ como sendo

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

Para grupos abelianos, as representações irredutíveis são uni-dimensionais, no entanto, se G é um grupo não abeliano, então existe pelo menos uma representação irredutível de G com dimensão maior que um. Neste caso, a transformada de Fourier depende da escolha da base para as representações irredutíveis, dificultando a extensão do algoritmo quântico abeliano para o cenário não abeliano.

Como já discutimos no início dessa seção, uma forma alternativa de tratar o PSO não abeliano é investigar a estrutura de todos os subgrupos de um dado grupo, e então determinar um algoritmo quântico que se aplique a estes subgrupos utilizando simplesmente a transformada de Fourier abeliana. Esta estratégia foi primeiramente adotada por [7] e [21]. Inui e Le Gall [21] apresentaram um algoritmo quântico eficiente para o PSO em grupos da forma $\mathbb{Z}_{p^r} \rtimes \mathbb{Z}_p$ com p primo. Mais tarde, Chi *et al.*[3] encontraram uma solução para o PSO sobre $\mathbb{Z}_N \rtimes \mathbb{Z}_p$, onde N é fatorado como $N = p_1^{r_1} p_2^{r_2} \cdots p_n^{r_n}$ e p um primo ímpar que não divide cada $p_j - 1$. Mais recentemente, também utilizando o método da ref. [21] C.C.M. Cosme e R. Portugal [4] encontraram um algoritmo quântico em tempo polinomial para o PSE sobre $\mathbb{Z}_{p^r} \rtimes \mathbb{Z}_{p^s}$, com p um primo ímpar e r, s inteiros satisfazendo algumas restrições. Ainda nesta direção, Bacon *et al.*[5] mostraram que para determinar uma solução para PSO sobre grupos da forma $A \rtimes \mathbb{Z}_p$, com A abeliano e p um número primo, basta considerar o PSO para subgrupos de ordem p em $A_2 \rtimes \mathbb{Z}_p$, onde A_2 é um subgrupo de A dado por $A_2 := \frac{A}{A_1}$ com A_1 satisfazendo $H_1 := H \cap A \times \{0\} := A_1 \times \{0\}$. Este trabalho foi uma generalização do trabalho de Ettinger e Høyer [7]. Estes autores mostraram que para o grupo Diedral, é suficiente considerar os casos onde o subgrupo oculto é trivial ou gerado por uma reflexão.

Neste trabalho, utilizando as técnicas mencionadas acima, nós apresentaremos uma solução eficiente para o PSO sobre o grupo $\mathbb{Z}_N^m \rtimes_\phi \mathbb{Z}_p$, onde p é um número primo ímpar, m, N inteiros positivos, e N fatorado como $N = p_1^{r_1} ... p_n^{r_n}$, com $1 \leq r_1 \leq \ldots \leq r_n$ onde $p \nmid p_i^k - 1$ para todo $i = 1, \ldots, n$ e $k = 1, \ldots, m$. Este trabalho é uma generalização dos resultados obtidos por [3] para o PSO sobre o produto semi-direto de grupos $\mathbb{Z}_N \rtimes \mathbb{Z}_p$.

Este artigo está organizado como segue. Na seção 2 nós introduzimos brevemente o conceito de produto semi-direto de grupos e exibimos algumas propriedades de homomorfismo de grupos. Na seção 3 nós mostramos que existe um algoritmo quântico eficiente para o problema do subgrupo oculto em $\mathbb{Z}_N^m \rtimes_\phi \mathbb{Z}_p$. Por fim, na seção 4 apresentamos nossas conclusões.

2 Preliminares

O produto semi-direto de dois grupos A, B é definido em termos de um homomorfismo $\phi : B \to \mathrm{Aut}(A)$, onde $\mathrm{Aut}(A)$ denota o grupo de automorfismos do grupo A. Suponha que

os grupos A e B sejam munidos com a operação aditiva. O produto semi-direto de grupos $A \rtimes_\phi B$ consiste de pares ordenados (a, b) com $a \in A$ e $b \in B$ com a operação em $A \rtimes_\phi B$ definida como $(a, b)(a', b') = (a + \phi(b)(a'), b + b')$. O inverso de um elemento $(a, b) \in A \rtimes_\phi B$ é definido como $(a, b)^{-1}$ e satisfaz $(a, b)^{-1} = (\phi(-b)(-a), -b)$.

Nós consideramos o problema do subgrupo oculto no produto semi-direto de grupos $\mathbb{Z}_N^m \rtimes_\phi \mathbb{Z}_p$. Neste caso, como ϕ é um homomorfismo de um grupo cíclico, este homomorfismo é completamente determinado por $\phi(1)$, e em particular, $\phi(p)$ é a aplicação identidade.

O lema a seguir é fundamental no desenvolvimento do nosso algoritmo.

Lema 2.1. *Seja o homomorfismo de grupos $\phi : \mathbb{Z}_p \to \mathrm{Aut}(\mathbb{Z}_{q^s}^m \times \mathbb{Z}_{p^r}^m)$. Dados $a \in \mathbb{Z}_{q^s}^m$, $b \in \mathbb{Z}_{p^r}^m$ e $c \in \mathbb{Z}_p$, existem $a' \in \mathbb{Z}_{q^s}^m$ e $b' \in \mathbb{Z}_{p^r}^m$ tais que $\phi(c)(a, 0) = (a', 0)$ e $\phi(c)(0, b) = (0, b')$.*

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

$$\begin{aligned}(0,0) &= \phi(c)(0,0) = \phi(c)(q^s e_i, 0) \\ &= q^s \phi(c)(e_i, 0) = (q^s a_i, q^s b_i).\end{aligned}$$

Como p e q são primos distintos temos que

$$q^s b_i \ = 0 \,(\mathrm{mod}\, p^r), \tag{2}$$

mas isto implica que $b_i = 0 \,(\mathrm{mod}\, p^r)$. Assim,

$$\begin{aligned}\phi(c)(a,0) &= \phi(c)(\sum_i a_i e_i, 0) \\ &= \sum_i \phi(c)(a_i e_i, 0) \\ &= \sum_i a_i \phi(c)(e_i, 0) \\ &= \sum_i a_i(\alpha_i, 0) = (a', 0).\end{aligned}$$

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

Teorema 2.1. *Sejam p e q primos ímpares distintos satisfazendo $p^k \nmid (q-1)$ para todo $1 \le k \le m$ e $m, r, s \in \mathbb{N}$. Então*

$$(\mathbb{Z}_{q^s}^m \times \mathbb{Z}_{p^r}^m) \rtimes_\phi \mathbb{Z}_p = \mathbb{Z}_{q^r}^m \times (\mathbb{Z}_{p^r}^m \rtimes_\psi \mathbb{Z}_p)$$

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

Demonstração. De fato, note que sendo $\phi(c)$ um automorfismo, a' é único tal que $\phi(c)(a, 0) = a'$. Observe também que

$$\mathrm{mdc}(|\mathbb{Z}_{q^s}^m|, |\mathbb{Z}_{p^r}^m|) = 1. \tag{3}$$

Assim temos que $\mathrm{Aut}(\mathbb{Z}_{q^s}^m \times \mathrm{Aut}\mathbb{Z}_{p^r}^m) = \mathrm{Aut}(\mathbb{Z}_{q^s}^m) \times \mathrm{Aut}(\mathbb{Z}_{p^r}^m)$. Logo, pelo lema 2.1 podemos definir um homomorfismo $\psi : \mathbb{Z}_p \to \mathrm{Aut}(Z_{q^s}^m)$ pondo $\psi(c) \in \mathrm{Aut}(\mathbb{Z}_{q^s}^n)$ com $\psi(c) = \phi(c)\Big|_{\mathbb{Z}_{q^s}^m}$, isto é, $\psi(c)(a) = a'$ onde $\phi(c)(a, 0) = (a', 0)$. Considere agora $\ker(\psi)$. Como p é primo, ou $\ker(\psi) = \{e\}$ ou $\ker(\psi) = \mathbb{Z}_p$. Suponhamos que $\ker(\psi) = \{e\}$. Então ψ é injetora, e portanto, $\psi(\mathbb{Z}_p)$ é um subgrupo de $\mathrm{Aut}(\mathbb{Z}_{q^s}^m)$ com $|\psi(\mathbb{Z}_p)| = p$. Isto implica que p divide $|\mathrm{Aut}(\mathbb{Z}_{q^s}^m)|$. Como

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

Então ou p divide q ou p divide $q^k - 1$ para algum k, contrariando nossa hipótese. Logo $\psi(b) = Id$ para todo $b \in \mathbb{Z}_p$.

Sendo assim, $\phi(c)(a, 0) = (a, 0)$ para todo $a \in \mathbb{Z}_{q^s}^m$. Isto mostra que ϕ age trivialmente sobre $\mathbb{Z}_{q^s}^m$. Assim, $\phi(c)(a, b) = (a, \psi(c)(b))$ e portanto,

$$(\mathbb{Z}_{q^s}^m \times \mathbb{Z}_{p^r}^m) \rtimes_\phi \mathbb{Z}_p = \mathbb{Z}_{q^s}^m \times (\mathbb{Z}_{p^r}^m \rtimes_\psi \mathbb{Z}_p). \tag{4}$$

■

3 O Algoritmo Quântico

Nesta seção, nós apresentaremos um algoritmo quântico eficiente para o PSO no produto semi-direto de grupos $\mathbb{Z}_N^m \rtimes_\phi \mathbb{Z}_p$, onde p é um número primo ímpar, m, N inteiros positivos, e N fatorado como $N = p_1^{r_1} ... p_n^{r_n}$, com $1 \le r_1 \le \ldots \le r_n$ onde $p \nmid p_i^k - 1$ para todo $i = 1, \ldots, n$ e $k = 1, \ldots, m$.

Note que, $\mathbb{Z}_N \simeq \mathbb{Z}_{p_1^{r_1}} \times \ldots \times \mathbb{Z}_{p_n^{r_n}}$. Assim, dado $m \in \mathbb{N}$ temos $\mathbb{Z}_N^m \simeq \mathbb{Z}_{p_1^{r_1}}^m \times \ldots \times \mathbb{Z}_{p_m^{r_n}}^m$. Logo,

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

Agora considere o homomorfismo de grupos $\phi : \mathbb{Z}_p \to \mathrm{Aut}(\mathbb{Z}_N^m) \simeq \mathrm{Aut}(\mathbb{Z}_{p^{r_1}}^m) \times \ldots \times \mathrm{Aut}(\mathbb{Z}_{p^{r_n}}^m)$ não trivial. Como p é primo, $\ker(\phi) = \{e\}$ o que implica que ϕ é um homomorfismo injetor

e, assim, $\phi(\mathbb{Z}_p)$ é um subgrupo de $\mathrm{Aut}(\mathbb{Z}_N^m)$ cuja ordem é p. Logo, $p/|\mathrm{Aut}(\mathbb{Z}_N^m)|$. Mas

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

Como $p \nmid p_i^k - 1$ para todo $i = 1, \ldots, n$ e $k = 1, \ldots, m$, segue que $p = p_i$ para algum i. Sem perda de generalidade, podemos supor $p = p_n$ e por um argumento análogo ao do teorema 2.1, segue que para todo $c \in \mathbb{Z}_p$, $\phi(c)$ age trivialmente sobre $\mathbb{Z}_{p_1^{r_1}}^m, \ldots, \mathbb{Z}_{p_{n-1}^{r_{n-1}}}^m$. Assim, $\mathbb{Z}_N^m \rtimes_\phi \mathbb{Z}_p \simeq (\mathbb{Z}_{p_1^{r_1}}^m \times \ldots \times \mathbb{Z}_{p_{n-1}^{r_{n-1}}}^m) \times (\mathbb{Z}_{p^{r_n}}^m \rtimes_\psi \mathbb{Z}_p)$. Além disso, $\mathbb{Z}_{p_1^{r_1}}^m \times \ldots \times \mathbb{Z}_{p_{n-1}^{r_{n-1}}}^m \simeq \mathbb{Z}_{\frac{N}{p^{r_n}}}^m$. Logo,

$$\mathbb{Z}_N^m \rtimes_\phi \mathbb{Z}_p \simeq \mathbb{Z}_{\frac{N}{p^{r_n}}}^m \times (\mathbb{Z}_{p^{r_n}}^m \rtimes_\psi \mathbb{Z}_p).$$

Note agora que $|\mathbb{Z}_{\frac{N}{p^{r_n}}}^m| = \frac{N^m}{p^{mr_n}}$ e $|\mathbb{Z}_{p^{r_n}}^m \rtimes_\psi \mathbb{Z}_p| = p^{mr_n+1}$. Assim temos que

$$\mathrm{mdc}(|\mathbb{Z}_{\frac{N}{p^{r_n}}}^m|, |\mathbb{Z}_{p^{r_n}}^m \rtimes_\psi \mathbb{Z}_p|) = 1.$$

Portanto, se H é um subgrupo de $\mathbb{Z}_N^m \rtimes_\phi \mathbb{Z}_p$, então $H \simeq H_0 \times H_1$, onde H_0 é um subgrupo de $\mathbb{Z}_{\frac{N}{p^{r_n}}}^m$ e H_1 um subgrupo de $\mathbb{Z}_{p^{r_n}}^m \rtimes_\psi \mathbb{Z}_p$. Agora observamos que o PSO no grupo cíclico $\mathbb{Z}_{N/p^{r_n}}^m$ e o PSO no grupo $\mathbb{Z}_{p^{r_n}}^m \rtimes_\psi \mathbb{Z}_p$ podem ser resolvidos eficientemente num computador quântico [19, 21]. Com isso, estabelecemos o seguinte teorema:

Teorema 3.1. *Existe um algoritmo quântico eficiente para para o PSO sobre o produto semi-direto de grupos $\mathbb{Z}_N^m \rtimes_\phi \mathbb{Z}_p$, desde que a decomposição de N seja $N = p_1^{r_1}...p_n^{r_n}$ e o primo p seja tal que $p \nmid p_i^k - 1$ para todo $i = 1, \ldots, n$ e $k = 1, \ldots, m$.*

4 Conclusões

Neste trabalho, nós descrevemos um algoritmo quântico eficiente para o PSO sobre produtos semi-diretos de grupos da forma $\mathbb{Z}_N^m \rtimes_\phi \mathbb{Z}_p$ com p primo, N e m inteiros positivos e N fatorado como $N = p_1^{r_1}...p_n^{r_n}$, com $p \nmid p_i^k - 1$ para todo $i = 1, \ldots, n$ e $k = 1, \ldots, m$. A estratégia que adotamos consistiu basicamente em explicitar um isomorfismo entre $\mathbb{Z}_N^m \rtimes_\phi \mathbb{Z}_p$ e o produto semi-direto de grupos $\mathbb{Z}_{p^r}^m \rtimes_\phi \mathbb{Z}_p$. A partir deste ponto empregando resultados já conhecidos na literatura para o PSO sobre cada membro do produto direto de grupos. Acreditamos que estas classes de produtos semi-diretos são bons candidatos para nos conduzir a uma solução do PSO em produtos semi-diretos mais genéricos.

5 Agradecimentos

Agradecemos a CAPES e ao CNPQ pelo apoio financeiro.

Referências

[1] L. V. Ahn. Survey: Quantum Computation and The Hidden Subgroup Problem. Technical report, Dept. of Science Computer, Carnegie Mellon University, Pittsburgh, 2002.

[2] R. Beals. Quantum Computation of Fourier transform over the symmetric groups. *In Proccedings of Symposium on Theory of Computing (STOC'97).*, 7(5).

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

[4] C.M.M Cosme and R. Portugal. Quantum algorithm for the hidden subgroup problem on a class of semidirect product groups. *arXiv:quant-ph/0703223*, 2007.

[5] A. M. Childs D. Bacon and W. van Dam. From optimal measurement to efficient quantum algorithms for the hidden subgroup problem over semidirect product groups. *arXiv:quant-ph/0504083*, 2.

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

[7] M. Ettinger and P. Høyer. On Quantum Algorithms for Noncommutative Hidden Subgroups. *Adv. Appl. Math.*, 25(3):239–251, 2000.

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

[9] R. Jozsa. Quantum factoring, discrete logarithms and the hidden subgroup problem. *Computing in Science and Engineering*, 03(2):34–43, 2001.

[10] A. Yu. Kitaev. Quantum measurements and and the abelian stabilizer problem. *ArqXiv preprint quant-ph/9511026*.

[11] C. Lavor, L.R.Y. Mansur, and R. Portugal. Grover's Algorithm: Quantum Data Search. *Quantum Physics, abstract quant-ph/0301079*, 1, June 2003.

[12] C. Lavor, L.R.Y. Mansur, and R. Portugal. Shor's Algorithm for Factoring Large Integers. *Quantum Physics, Abstract quant-ph/0303175*, 1, March 2003.

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

[14] M. Mosca. Quantum Computer Algorithms. *Ph.D. thesis, Wolfson College, University of Oxford, United Kingdom*, pages 71–81.

[15] O. Regev. A Subexponential Time Algorithm for the Dihedral Hidden Subgroup Problem with Polynomial Space. *quant-ph/0406151*, 2004.

[16] O. Regev. New Lattice-Based Cryptographic. *J. ACM*, 51(6):899–942, 2004.

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

[18] J.P Serre. Linear Representation of Finite Group. *Springer-Verlag*, 1997.

[19] P. W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. Comput.*, 26(5):1484–1509, 1997.

[20] 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.

[21] Y. Ynui and F. Le Gall. EFFICIENT QUANTUM ALGORITHMS FOR THE HIDDEN SUBGROUP PROBLEM OVER SEMI-DIRECT PRODUCT GROUPS. *Quantum Information and Computation.*, 7(5).