Tema
Tendências em Matemática Aplicada e Computacional, **18**, N. 2 (2017), 215-223
© 2017 Sociedade Brasileira de Matemática Aplicada e Computacional
www.scielo.br/tema
doi: 10.5540/tema.2017.018.02.0215

An Efficient Quantum Algorithm for the Hidden Subgroup Problem over some Non-Abelian Groups[†]

D.N. GONÇALVES[1*], T.D. FERNANDES[2] and C.M.M. COSME[3]

Received on December 20, 2015 / Accepted on May 2, 2017

ABSTRACT. The hidden subgroup problem (HSP) plays an important role in quantum computing because many quantum algorithms that are exponentially faster than classical algorithms are special cases of the HSP. In this paper we show that there exists a new efficient quantum algorithm for the HSP on groups $\mathbb{Z}_N \rtimes \mathbb{Z}_{q^s}$ where N is an integer with a special prime factorization, q prime number and s any positive integer.

Keywords: Quantum Algorithms, Hidden Subgroup Problem, Quantum Computational Group Theory.

1 INTRODUCTION

The most important problem in group theory in terms of quantum algorithms is called hidden subgroup problem (HSP) [14]. The HSP can be described as follows: given a group G and a function $f : G \to X$ on some set X such that $f(x) = f(y)$ iff $x \cdot H = y \cdot H$ for some subgroup H, the problem consists in determining a generating set for H by querying the function f. We say that the function f hides the subgroup H in G or that f separates the cosets of H in G. A quantum algorithm for the HSP is said to be efficient when the running time is $O(\text{poly}(\log |G|))$. There are many examples of efficient quantum algorithms for the HSP in particular groups [17, 18]. It is known that for finite abelian groups, the HSP can be solved efficiently on a quantum computer [14]. On the other hand, an efficient solution for a generic non-abelian group is not known. Two important groups in this context are the symmetric and the dihedral groups. An efficient algorithm for solving the HSP for the former group would imply in an efficient solution for the graph isomorphism problem [1, 2, 12, 8] and for the latter one would solve instances of the problem of finding the shortest vector in a lattice, which has applications in cryptography [16].

One way to design new quantum algorithms for the HSP is to investigate the structures of all subgroups of a given group, and then to find a quantum algorithm applicable to each subgroup

[†]Short version in: III CMAC-SE, Vitória, 2015

[*]Corresponding author: Demerson Nunes Gonçalves – E-mail: demerson.goncalves@cefet-rj.br

[1]Coordenação de Licenciatura em Física, CEFET-RJ, Petrópolis, RJ, Brasil.

[2]Departamento de Matemática Pura e Aplicada, UFES, Alegre, ES, Brasil. E-mail: tharso.fernandes@ufes.br

[3]Departamento de Física e Matemática, CEFET-MG, Belo Horizonote, MG, Brasil. E-mail: cmagnomc@des.cefetmg.br

structure. Following this, Inui & Le Gall presented an efficient quantum algorithm for the HSP on groups of the form $\mathbb{Z}_{p^r} \rtimes \mathbb{Z}_p$ with prime p and positive integer r[13]. Later, Cosme [6] presented an efficient quantum algorithm for the HSP in $\mathbb{Z}_{p^r} \rtimes_\phi \mathbb{Z}_{p^s}$ 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 $r \geq 2s-l$. Subsequently, in [10] the authors presented an efficient quantum algorithm for the HSP in $\mathbb{Z}_p \rtimes \mathbb{Z}_{q^s}$, with $p/q = \text{poly}(\log p)$, where p, q are distinct odd prime numbers and s is an arbitrary positive integer. The case $\mathbb{Z}_{p^r} \rtimes \mathbb{Z}_{q^s}$ with p, q distinct odd prime numbers and $r, s > 0$ such that $p^r/q^t = \text{poly}(\log p^r)$ was discussed in [11]. The parameter $t \in \{0, 1, \ldots, s\}$ characterizes the group. The case $t = 0$ reduces to the abelian group $\mathbb{Z}_{p^r} \times \mathbb{Z}_{q^s}$ and the case $t = 1$ was addressed by the authors, with unsuccessful results. This work established, for the first time, a complete description of the structure of the subgroups of $\mathbb{Z}_{p^r} \rtimes \mathbb{Z}_{q^s}$. Recently, using the algebraic structure of the subgroups of $\mathbb{Z}_{p^r} \rtimes \mathbb{Z}_{q^s}$, van Dam & Dey [7] presented a new quantum algorithm for the HSP over $\mathbb{Z}_{p^r} \rtimes \mathbb{Z}_{q^s}$ for all possible values of $t \in \{0, 1, \ldots, s\}$ by imposing a restriction on the parameters p and q: the relative sizes of subgroups are bounded by $p^r/q^{t-j} \in O(\text{poly}(\log p^r))$, where $j \in \{0, \ldots, t-1\}$.

In this article, we describe a new efficient quantum algorithm to solve the HSP in the specific class of non-abelian groups, i.e., the semi-direct product groups of the form $G = \mathbb{Z}_N \rtimes \mathbb{Z}_{q^s}$, where, N is factorized as $p_1^{r_1} \ldots p_n^{r_n}$ and there exists a $1 \leq k \leq n$ such that q^t (q odd prime) divides $p_k - 1$ and q does not divide $p_i - 1$ for all $i \neq k$. The parameter t is related to the type of the homomorphism that describes the group, as can be checked in Section 3. Using a similar approach presented in [5], we define an isomorphism between $\mathbb{Z}_N \rtimes \mathbb{Z}_{q^s}$ and the direct product of $\mathbb{Z}_{p^r} \rtimes_\psi \mathbb{Z}_{q^s}$ with cyclic groups, reducing the HSP in G to similar HSPs, solutions which are already known.

This work is organized as follows: In Section 2, we review some fundamental notations and definitions of finite groups. In Section 3, we give the relevant definitions and results concerning the semi-direct product groups and explain its homomorphisms and their properties. In Section 4, we present our main result and we show that there exist an efficient quantum algorithm for the HSP in the groups. In Section 5, we draw our conclusions.

2 PRELIMINARIES

We begin by reviewing some fundamental notations and definitions of finite groups that will be used throughout the text. More details can be found in lots of textbooks of abstract algebra such as in [3, 9].

Let G be a finite group. We use $|G|$ to denote the *order* of G. A nonempty subset H of a group G is called a subgroup of G, denoted by $H \leq G$, if $H^2 \subseteq H$ and $H^{-1} \subseteq H$, where $H^2 = \{h_1h_2 | h_1, h_2 \in H\}$ and $H^{-1} = \{h^{-1} | h \in H\}$. For a subgroup H of G and every group element $g \in G$, the *left coset* of H determined by g is the set $gH = \{gh, h \in H\}$.

Let M be a set of elements in G. The intersection of all subgroups of G containing M is called the *subgroup generated by* M, denoted by $\langle M \rangle$. If $\langle M \rangle = G$, M is said to be a *generating set* of

G or G is generated by M. A group generated by one element is called a *cyclic group*. For an element $g \in G$, we call the order of the subgroup $\langle g \rangle$ the *order* of g, denoted by $\text{ord}(g)$, that is, $\text{ord}(g) = | \langle g \rangle |$. One can show that $\text{ord}(g)$ is the smallest positive integer n satisfying $g^n = 1$.

Given two groups G and H, a map $\alpha : G \to H$ is called a *homomorphism* of G into H if

$$\alpha(ab) = \alpha(a)\alpha(b), \quad \forall\, a, b \in G.$$

If the homomorphism α is a bijection, then α is an *isomorphism* from G onto H. In this case, G and H are said to be *isomorphic*, denoted by $G \cong H$. An isomorphism from G to itself is called an *automorphism* of G. We use $\text{Aut}(G)$ to denote the set of automorphism of G. For the composition of maps, $\text{Aut}(G)$ is a group, called the *automorphism group* of G.

A subgroup N of a group G is called *normal*, denoted by $N \trianglelefteq G$ if $Ng = gN, \forall\, g \in G$. The group $n\mathbb{Z}$, for any integer n, is a normal subgroup of the integer group $\mathbb{Z}$. The factor group $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z} = \{0, 1, \ldots, n-1\}$ is called the (additive) *group of integers modulo n*. In this group, $(n\mathbb{Z})a.(n\mathbb{Z})b = (n\mathbb{Z})c$ if and only if $a + b = c \pmod n$. The *unit group*, denoted by $\mathbb{Z}_n^*$, for any positive integer n, is the group of invertible integers $\bmod n$ (i.e, those $a \in \mathbb{Z}_n$ with $\gcd(a, n) = 1$).

The *direct product* of two groups G and H, denoted by $G \times H$, is the set $\{(g, h)|g \in G, h \in H\}$, where the multiplication operation is defined by $(g, h)(g', h') = (gg', hh')$ for all $g, g' \in G$ and $h, h' \in H$. In the same way, one may define the direct product of n groups $G_1, \ldots, G_n$ as $G = G_1 \times \ldots \times G_n$.

3 SEMI-DIRECT PRODUCT GROUPS

The *semi-direct product* of two groups G and H is defined by a homomorphism $\phi : H \to \text{Aut}(G)$. The semi-direct product $G \rtimes_\phi H$ is the set $\{(g, h) : g \in G, h \in H\}$ with the group operation defined as $(g, h)(g', h') = (g + \phi(h)(g'), h + h')$. One can easily check that the group inversion operation satisfies $(g, h)^{-1} = (\phi(-h)(-h), -h)$.

In this paper we consider the HSP on the semi-direct product groups $G = \mathbb{Z}_N \rtimes_\phi \mathbb{Z}_{q^s}$ for positive integers N and s and odd prime number q. We assume that the prime factorization of N is $p_1^{r_1} \ldots p_n^{r_n}$ and there exists a $1 \leq k \leq n$ such that q^t divides $p_k - 1$ and q does not divide $p_i - 1$ for all $i \neq k$. The parameter $t \in \{0, 1, \ldots, s\}$ characterizes the group as shown in the following.

The elements $x = (1, 0)$ and $y = (0, 1)$ generate the groups $\mathbb{Z}_N \rtimes_\phi \mathbb{Z}_{q^s}$. Since $\text{Aut}(\mathbb{Z}_N)$ is isomorphic to $\mathbb{Z}_N^*$, the homomorphism ϕ is completely determined by $\alpha := \phi(1)(1) \in \mathbb{Z}_N^*$ and $\phi(b)(a) = a\alpha^b$ for all $a \in \mathbb{Z}_N$ and $b \in \mathbb{Z}_{q^s}$. Now, note that $\phi(0) = \phi(q^s) : \mathbb{Z}_N \to \mathbb{Z}_N$ is the identity element of the group $\text{Aut}(\mathbb{Z}_N)$. Then $\alpha^{q^s} = \phi(q^s)(1) = 1$. If the element $\alpha \in \mathbb{Z}_N^*$ satisfies the congruence relation $X^{q^s} = 1 \mod N$, then it defines the semi-direct product $\mathbb{Z}_N \rtimes_\alpha \mathbb{Z}_{q^s}$. In this case, we must have $\text{ord}(\alpha) = q^t$ for some integer $0 \leq t \leq s$. The case $t = 0$ reduces to the direct product $\mathbb{Z}_N \times \mathbb{Z}_{q^s}$, which is an abelian group. An efficient solution for the HSP is known for this case [14]. Since $\alpha \in \mathbb{Z}_N^*$, q^t divides $|\mathbb{Z}_N^*| = \varphi(N)$, where φ is the *Euler* *phi-function* [9]. Since $\varphi(N) = p_1^{r_1-1} \dots p_n^{r_n-1}(p_1 - 1)\dots(p_n - 1)$, we can choose the option $q^t \mid p_n - 1$ with no loss of generality.

For instance, let $G = \mathbb{Z}_N \rtimes_\phi \mathbb{Z}_{q^s}$, with $N = 45125$, $q = 3$ and $s = 4$. The homomorphism ϕ can be described by an element $\alpha = 2626 \in \mathbb{Z}_N^*$ with order 3^2. Since $45125 = 19^2.5^3$, the order of α satisfies $3^2|(19 - 1)$ and $3 \nmid (5 - 1)$. Then G is an example of group for which the Theorem 4.1 holds.

Let us consider the usual decomposition $\mathbb{Z}_N \cong \mathbb{Z}_{p_1^{r_1}} \times \dots \times \mathbb{Z}_{p_n^{r_n}}$, which can be found in quantum polynomial time [4]. Thus, the following isomorphism holds

$$\mathbb{Z}_N \rtimes_\phi \mathbb{Z}_{q^s} \cong (\mathbb{Z}_{p_1^{r_1}} \times \dots \times \mathbb{Z}_{p_n^{r_n}}) \rtimes_\phi \mathbb{Z}_{q^s}. \tag{3.1}$$

The elements of $(\mathbb{Z}_{p_1^{r_1}} \times \dots \times \mathbb{Z}_{p_n^{r_n}}) \rtimes_\phi \mathbb{Z}_{q^s}$ have the form $((a_1, \dots, a_n), b)$, where $(a_1, \dots, a_n) \in \mathbb{Z}_{p_1^{r_1}} \times \dots \times \mathbb{Z}_{p_n^{r_n}}$ and $b \in \mathbb{Z}_{q^s}$. For each b in $\mathbb{Z}_{q^s}$ the element $\phi(b)$ is an automorphism on $\mathbb{Z}_{p_1^{r_1}} \times \dots \times \mathbb{Z}_{p_n^{r_n}}$ such that $\alpha = \phi(1)(1)$ is an element in $\mathbb{Z}^*_{p_1^{r_1}} \times \dots \times \mathbb{Z}^*_{p_n^{r_n}}$ of order q^t. Note that $\mathbb{Z}_{p_i^{r_i}}$ is isomorphic to the subgroup $\mathcal{I}_1 \times \mathbb{Z}_{p_i^{r_i}} \times \mathcal{I}_2$ of $\mathbb{Z}_{p_1^{r_1}} \times \dots \times \mathbb{Z}_{p_n^{r_n}}$, where $\mathcal{I}_1$ is the identity on $\mathbb{Z}_{p_1^{r_1}} \times \dots \times \mathbb{Z}_{p_{i-1}^{r_{i-1}}}$ and $\mathcal{I}_2$ is the identity on

$$\mathbb{Z}_{p_{i+1}^{r_{i+1}}} \times \dots \times \mathbb{Z}_{p_n^{r_n}}, \quad \text{for all } \ i = 1, \dots, n.$$

Thus, we can identify an element a_i in $\mathbb{Z}_{p_i^{r_i}}$ with the point $\overline{a_i}$ in $\mathcal{I}_1 \times \mathbb{Z}_{p_i^{r_i}} \times \mathcal{I}_2$ such that it has an integer value a_i in the i-th coordinate and $0's$ elsewhere.

Now we are ready to state the following results.

Lemma 3.1. *Let $\mathbb{Z}_{p_1^{r_1}} \times \dots \times \mathbb{Z}_{p_n^{r_n}}$ and $\mathbb{Z}_{q^s}$ be finite abelian groups with distinct odd prime numbers $p_1, \dots, p_n, q$ and positive integers $r_1, \dots, r_n$ and s. Define the semi-direct product group $(\mathbb{Z}_{p_1^{r_1}} \times \dots \times \mathbb{Z}_{p_n^{r_n}}) \rtimes_\phi \mathbb{Z}_{q^s}$. Then, for each $b \in \mathbb{Z}_{q^s}$ and $a_i \in \mathbb{Z}_{p_i^{r_i}}$ there exists a $c_i \in \mathbb{Z}_{p_i^{r_i}}$ such that $\phi(b)(\overline{a_i}) = \overline{c_i}$.*

Proof. Let e_i be elements in $\mathbb{Z}_{p_1^{r_1}} \times \dots \times \mathbb{Z}_{p_n^{r_n}}$ with all components equal zero except the i-th one which is 1. Because $\phi(b) \in \mathrm{Aut}(\mathbb{Z}_N)$, it is enough to show that $\phi(b)(e_i) = \overline{d_i}$, for some $d_i \in \mathbb{Z}_{p_i^{r_i}}$. In fact, $\phi(b)(\overline{a_i}) = \phi(b)(a_i e_i) = a_i \phi(b)(e_i) = a_i \overline{d_i} = \overline{c_i}$, for some $c_i \in \mathbb{Z}_{p_i^{r_i}}$.

Now let us suppose that $\phi(b)(e_i) = (d_1, \dots, d_n)$. Note that

$$\begin{aligned}(0, \dots, 0) &= \phi(b)(0, \dots, 0) = \phi(b)(0, \dots, 0, p_i^{r_i}, 0, \dots, 0)\\ &= p_i^{r_i}\phi(b)(e_i) = (p_i^{r_i} d_1, \dots, p_i^{r_i} d_n).\end{aligned}$$

Then, for all $j = 1, \dots, n$ we have $p_i^{r_i} d_j \equiv 0 \bmod p_j^{r_j}$ and this implies that $d_j \equiv 0 \bmod p_j^{r_j}$ for all $j \neq i$. Hence, $\phi(b)(e_i) = (0 \dots, d_i, 0, \dots, 0) = \overline{d_i}$ as was to be shown. □

The next lemma shows that there exists an isomorphism between $\mathbb{Z}_N \rtimes_\alpha \mathbb{Z}_{q^s}$ and the non-abelian group $\mathbb{Z}_{p_n^{r_n}} \rtimes \mathbb{Z}_{q^s}$ with cyclic groups.

Lemma 3.2. *Let N be a positive integer with prime factorization $p_1^{r_1} \ldots p_n^{r_n}$ and q an odd prime such that $q \neq p_i$ and s a positive integer. Define the semi-direct product group $G = \mathbb{Z}_N \rtimes_\alpha \mathbb{Z}_{q^s}$ for an $\alpha \in \mathbb{Z}_N^*$. Let $t \in \{1, \ldots, s\}$ be the smallest positive integer such that $\alpha^{q^t} = 1$. Let us assume that there exists a $1 \leq k \leq n$ such that $q^t \mid p_k - 1$ and $q \nmid p_i - 1$ for all $i \neq k$. By choosing $k = n$ (WLOG) we have*

$$\mathbb{Z}_N \rtimes_\phi \mathbb{Z}_{q^s} \cong (\mathbb{Z}_{p_1^{r_1}} \times \ldots \times \mathbb{Z}_{p_{n-1}^{r_{n-1}}}) \times (\mathbb{Z}_{p^r} \rtimes_\psi \mathbb{Z}_{q^s}), \tag{3.2}$$

for some homomorphism ψ from $\mathbb{Z}_{q^s}$ into the group of automorphisms of $\mathbb{Z}_{p^r}$ and $p = p_n$ and $r = r_n$.

Proof. Note that $\phi(q^s)$ is the identity map $\mathcal{I}$ on $\mathbb{Z}_{p_1^{r_1}} \times \ldots \times \mathbb{Z}_{p_n^{r_n}}$. For all $i = 1, \ldots, n-1$, follows from Lemma 3.1 that $e_i = \phi(q^s)(e_i) = (0 \ldots, c_i{}^{q^s}, \ldots, 0)$. Then $c_i{}^{q^s} = 1 \bmod p_i^{r_i}$, which implies that c_i is an element in $\mathbb{Z}^*_{p_i^{r_i}}$ with order $q^{t'}$, for some $t' \in \{1, \ldots, s\}$. Let us suppose $c_i \neq 1$. Since $q^{t'}$ divides the order of $\mathbb{Z}^*_{p_i^{r_i}}$ and $\gcd(p_i, q) = 1$, we have that $q^{t'}$ divides $p_i - 1$. But that leads to an absurd, hence c_i must be 1 and ϕ acts trivially on $\mathbb{Z}_{p_1^{r_1}} \times \ldots \times \mathbb{Z}_{p_{n-1}^{r_{n-1}}}$. Thus, there exists a homomorphism ψ from $\mathbb{Z}_{q^s}$ into the group of automorphisms of $\mathbb{Z}_{p^r}$ ($p = p_n$ and $r = r_n$), such that for all $b \in \mathbb{Z}_{q^s}$ and all $(a_1, \ldots, a_n) \in \mathbb{Z}_{p_1^{r_1}} \times \ldots \times \mathbb{Z}_{p_n^{r_n}}$ we have

$$\phi(b)(a_1, \ldots, a_n) = (a_1, \ldots, a_{n-1}, \psi(b)(a_n)). \tag{3.3}$$

Now for two elements $g = ((a_1 \ldots, a_n), b)$ and $g' = ((a_1' \ldots, a_n'), b')$ in $(\mathbb{Z}_{p_1^{r_1}} \times \ldots \times \mathbb{Z}_{p_n^{r_n}}) \rtimes_\phi \mathbb{Z}_{q^s}$, the group operation is defined by

$$\begin{aligned} gg' &= ((a_1, \ldots, a_n) + \phi(b)(a_1', \ldots, a_n'), b + b') \\ &= (a_1 + a_1', \ldots, a_{n-1} + a_{n-1}', a_n + \psi(b)(a_n'), b + b'). \end{aligned} \tag{3.4}$$

Define the map

$$\Gamma : \mathbb{Z}_N \rtimes_\phi \mathbb{Z}_{q^s} \to (\mathbb{Z}_{p_1^{r_1}} \times \ldots \times \mathbb{Z}_{p_{n-1}^{r_{n-1}}}) \times (\mathbb{Z}_{p^r} \rtimes_\psi \mathbb{Z}_{q^s}), \tag{3.5}$$

such that $\Gamma(a_1, \ldots, a_n, b)) = ((a_1, \ldots, a_{n-1}), (a_n, b))$. The group operation in $\mathbb{Z}_{p^r} \rtimes_\psi \mathbb{Z}_{q^s}$ is $(a, b)(c, d) = (a + \psi(b)(c), b + d)$ for all $a, c \in \mathbb{Z}_{p^r}$ and $b, d \in \mathbb{Z}_q^s$. Note that

$$\begin{aligned} \Gamma(gg') &= \Gamma(a_1 + a_1', \ldots, a_{n-1} + a_{n-1}', a_n + \psi(b)(a_n'), b + b') \\ &= ((a_1 + a_1', \ldots, a_{n-1} + a_{n-1}'), \underbrace{(a_n + \psi(b)(a_n'), b + b'))}_{(a_n, b)\cdot_\psi(a_n', b')} \\ &= ((a_1, \ldots, a_{n-1}), (a_n, b))((a_1', \ldots, a_{n-1}'), (a_n', b')) \\ &= \Gamma(g)\Gamma(g'). \end{aligned} \tag{3.6}$$

Thus, Γ is an group homomorphism. One can easily see that Γ is injective and from the fact that $|\mathbb{Z}_N \rtimes_\phi \mathbb{Z}_{q^s}| = |(\mathbb{Z}_{p_1^{r_1}} \times \ldots \times \mathbb{Z}_{p_{n-1}^{r_{n-1}}}) \times (\mathbb{Z}_{p^r} \rtimes_\psi \mathbb{Z}_{q^s})| = Nq^s$ we have that Γ is an isomorphism. □

Lemma 3.3. *Let G_1 and G_2 be finite groups with relatively prime orders. If H is a subgroup of G then $H = H_1 \times H_2$ for some subgroups H_1 of G_1 and H_2 of G_2.*

Proof. Let $\pi_i : G_1 \times G_2 \to G_i$ such that $\pi_i(g_1, g_2) = g_i$, $i = 1, 2$. For any subgroup H of $G_1 \times G_2$ define $H_1 = \pi_1(H) \leq G_1$ and $H_2 = \pi_2(H) \leq G_2$. Then $H \leq H_1 \times H_2$. We claim that $H = H_1 \times H_2$. In fact, if $(h_1, h_2) \in H_1 \times H_2$ it follows from definition of H_1 and H_2 that there exists $h'_1 \in G_1$ and $h'_2 \in G_2$ such that (h_1, h'_2), $(h'_1, h_2) \in H$. From the fact that $\gcd(|G_1|, |G_2|) = 1$ and by the Chinese remainder theorem [9], there exist integers r_1 and r_2 such that

$$\begin{cases} r_1 \equiv 1 \mod |G_1| \\ r_1 \equiv 0 \mod |G_2| \end{cases} \text{and} \begin{cases} r_2 \equiv 0 \mod |G_1| \\ r_2 \equiv 1 \mod |G_2|. \end{cases} \tag{3.7}$$

It follows from (3.7) that there are integers k_1, k_2, k_3, k_4 such that

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

Thus,

$$(h_1, h'_2)^{r_1} = (h_1^{r_1}, h_2'^{r_1}) = (h_1^{k_1|G_1|+1}, h_2'^{k_2|G_2|}) = (h_1, e_2) \in H$$

$$(h'_1, h_2)^{r_2} = (h_1'^{r_2}, h_2^{r_2}) = (h_1'^{k_3|G_1|}, h_2^{k_4|G_2|+1}) = (e_1, h_2) \in H$$

where e_1 and e_2 are the identities elements in the groups G_1 and G_2, respectively. Hence, $(h_1, h_2) = (h_1, e_2)(e_1, h_2) \in H$. □

4 QUANTUM ALGORITHM FOR HSP IN $\mathbb{Z}_N \rtimes_\phi \mathbb{Z}_{q^s}$

In this section we present an efficient quantum algorithm that can solve the HSP in $\mathbb{Z}_N \rtimes_\phi \mathbb{Z}_{q^s}$, where N is factorized as $N = p_1^{r_1} \dots p_n^{r_n}$ and given a $1 \leq t \leq s$, there exists a $1 \leq k \leq n$ such that $q^t \mid p_k - 1$ and $q \nmid p_i - 1$ for all $i \neq k$.

Before stating our main theorem, let us introduce the last two intermediate results.

Proposition 4.1. *Let G be a finite group, H a subgroup of G and $f : G \to X$ the oracle function that hides H in G. For any subgroup $\widetilde{G}$ of G we have $\widetilde{f} = f\big|_{\widetilde{G}} : \widetilde{G} \to X$ hides $\widetilde{H} = H \cap \widetilde{G}$ in $\widetilde{G}$.*

Proof. We must show that $\widetilde{f}(a) = \widetilde{f}(b)$ if and only if $a\widetilde{H} = b\widetilde{H}$, for all $a, b \in \widetilde{G}$. In fact, let $a, b \in \widetilde{G}$ such that $\widetilde{f}(a) = \widetilde{f}(b)$. Since f hides H in G, $aH = bH$ which implies $a = bh$, for some $h \in H$. Since $a, b \in \widetilde{G}$, we have $h = b^{-1}a \in \widetilde{G}$ which implies $h \in \widetilde{H}$, hence $a\widetilde{H} = b\widetilde{H}$. Conversely, if $a\widetilde{H} = b\widetilde{H}$, since $a\widetilde{H} \subset aH$ and $b\widetilde{H} \subset bH$ we have $aH \cap bH \neq \emptyset$ which implies $aH = bH$, or equivalently $\widetilde{f}(a) = \widetilde{f}(b)$. □

Although the Proposition 4.1 establish a very simple result to be verified, it has important applications in solving the HSP. In fact, if there exists a subgroup $\widetilde{G}$ of G where the HSP can solved efficiently by a quantum computer, the Proposition 4.1 shows that is possible to obtain information about H by using the restriction of the hiding function f to the subgroup $\widetilde{H} = H \cap \widetilde{G}$. Note that if $H \subset \widetilde{G}$ then the problem is completely solved.

An important consequence of the Proposition 4.1 follows below:

Corollary 4.1. *Let G_1 and G_2 be finite groups with relatively prime orders. Then, an efficient solution to the HSP over G_1 and G_2 implies in an efficient solution to the HSP over the direct product $G_1 \times G_2$.*

Proof. By Lemma 3.3, if H is a subgroup of $G_1 \times G_2$ then $H = H_1 \times H_2$ for some subgroup H_1 of G_1 and subgroup H_2 of G_2. Let f be the oracle function that hides H in $G_1 \times G_2$. By Proposition 4.1, the restrictions of f to G_1 and G_2 hide, respectively, H_1 and H_2. Since the HSP can solved efficiently over the groups G_1 and G_2 one can efficiently find generators to H_1 and H_2, or equivalently, generators to $H_1 \times H_2$. □

Now we are able to state and prove our main result.

Theorem 4.1. *Let N be a positive integer with prime factorization $p_1^{r_1} \ldots p_n^{r_n}$, q an odd prime such that $q \neq p_i$ and s a positive integer. Define the semi-direct product group $G = \mathbb{Z}_N \rtimes_\alpha \mathbb{Z}_{q^s}$ for an $\alpha \in \mathbb{Z}_N^*$. Let $t \in \{1, \ldots, s\}$ be the smallest positive integer such that $\alpha^{q^t} = 1$. Let us assume that there exists a $1 \leq k \leq n$ such that $q^t \mid p_k - 1$ and $q \nmid p_i - 1$ for all $i \neq k$. Then there exists an efficient quantum algorithm that solves the HSP in the semi-direct product groups $\mathbb{Z}_N \rtimes_\alpha \mathbb{Z}_{q^s}$.*

Proof. Define $N' = N/p_n^{r_n}$ then $\mathbb{Z}_{p_1^{r_1}} \times \ldots \times \mathbb{Z}_{p_{n-1}^{r_{n-1}}} \cong \mathbb{Z}_{N'}$. By Lemma 3.2,

$$\mathbb{Z}_N \rtimes_\phi \mathbb{Z}_{q^s} \cong \mathbb{Z}_{N'} \times (\mathbb{Z}_{p^r} \rtimes_\psi \mathbb{Z}_{q^s}).$$

The group $\mathbb{Z}_{N'}$ is an abelian and the HSP can be solved efficiently for abelian groups by quantum computers [14]. On the other hand, the group $\mathbb{Z}_{p^r} \rtimes_\psi \mathbb{Z}_{q^s}$ was addressed in [10, 11] and recently generalized by [7]. Since the order of $\mathbb{Z}_{N'}$ is relatively prime to order of the group $\mathbb{Z}_{p^r} \rtimes_\psi \mathbb{Z}_{q^s}$, by Corollary 4.1, the HSP over $\mathbb{Z}_N \rtimes \mathbb{Z}_{q^s}$ can be solved efficiently on a quantum computer. □

A series of efficient quantum algorithms for the non-abelian HSP over semi-direct product groups have been discovered. Among these, is the algorithm presented by Inui & Le Gall for groups of the form $\mathbb{Z}_{p^r} \rtimes \mathbb{Z}_p$ with prime p and positive integer r, which uses enumeration of subgroups and blackbox techniques. Chi, Kim & Lee [5] extended the algorithm to the case $\mathbb{Z}_N \rtimes \mathbb{Z}_p$, where N is factored as $N = p_1^{r_1} \ldots p_n^{r_n}$, and p prime does not divide each $p_j - 1$. The idea is to use a factorization of N to factor out the group and then apply Inui & Le Gall's algorithm. Later, Cosme [6] solved the case $\mathbb{Z}_{p^r} \rtimes_\phi \mathbb{Z}_{p^s}$ where p is any odd prime number, r and s are positives. Using a similar approach of [5], they extended their algorithm to the class $\mathbb{Z}_N \rtimes_\phi \mathbb{Z}_{p^s}$. In [10], the authors presented an efficient quantum algorithm for the HSP over certain metacyclic groups $\mathbb{Z}_p \rtimes \mathbb{Z}_{q^s}$, with $p/q = \text{poly}(\log p)$, where p, q are distinct odd prime numbers and s is an arbitrary positive integer. This work was extended in [7], which developed an efficient HSP algorithm in $\mathbb{Z}_{p^r} \rtimes \mathbb{Z}_{q^s}$, with p, q distinct odd prime numbers and r, s positive integers.

All those class of groups are special cases of the semi-direct products $\mathbb{Z}_M \rtimes \mathbb{Z}_N$, for any positive integers M and N. In this sense, our result increases the number of groups in this family for which efficient solutions are known.

We hope that these ideas will be useful for the understanding of the complexity of the HSP over semi-direct product groups and lead to new algorithms for other non-Abelian HSP instances.

5 CONCLUSION

We have addressed the HSP on the semi-direct product groups $G = \mathbb{Z}_N \rtimes \mathbb{Z}_{q^s}$ where N is factorized as $N = p_1^{r_1} \dots p_n^{r_n}$ and given a $1 \leq t \leq s$, there exists a $1 \leq k \leq n$ such that q^t divides $p_k - 1$ $q \nmid p_i - 1$ for all $i \neq k$. By employing an isomorphism between $\mathbb{Z}_N \rtimes \mathbb{Z}_{q^s}$ and the direct product of $\mathbb{Z}_{p^r} \rtimes_\psi \mathbb{Z}_{q^s}$ with cyclic groups we have shown that the HSP can be reduced to similar HSPs the solutions of which are already known. This provides a new efficient solution for the HSP on G.

ACKNOWLEDGEMENTS

We would like to tank the anonymous reviewers for their valuable comments and suggestions to improve the manuscript.

RESUMO. O problema do subgrupo oculto (PSO) tem um papel importante na computação quântica pois muitos algoritmos quânticos que são exponencialmente mais rápidos que seus equivalentes clássicos são casos especiais do PSO. Neste artigo nós mostramos a existência de um novo algoritmo quântico eficiente para o PSO sobre grupos da forma $\mathbb{Z}_N \rtimes \mathbb{Z}_{q^s}$, onde N é um número inteiro positivo com uma particular decomposição em fatores primos, q um número primo e s um inteiro positivo qualquer.

Palavras-chave: Algoritmos quânticos, problema do subgrupo oculto, teoria de grupos computacional.

REFERENCES

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

[2] D. Boneh & R.J. Lipton. "Quantum cryptanalysis of hidden linear functions", In Lecture Notes in Computer Science, volume 963, pages 424–437, Berlin, (1995).

[3] W. Burniside. Theory of Groups of Finite order, Dover Publication, Inc. – New York, (1955).

[4] K.K.H. Cheung & M. Mosca. Decomposing Finite Abelian Groups. *Quantum Information and Computation*, **1**(3) (2001), 23–32.

[5] D.P. Chi, J.S. Kim & S. Lee. Quantum algorithms for the hidden subgroup problem on some semi-direct product groups by reduction to Abelian cases. *Physics Letters A*, pages 114–116, (2006).

[6] C.M.M. Cosme. "Algoritmos Quânticos para o Problema do Subgrupo Oculto não Abeliano". Tese de Doutorado, LNCC, Petrópolis, RJ, (2008).

[7] W. van Dam & S. Dey. "Hidden Subgroup Quantum Algorithms for a Class of Semi-Direct Product Groups". Proc. of 9th Conference on the Theory of Quantum Computation, Communication and Cryptography, TQC'14, pages 110–117, (2014).

[8] M. Ettinger & P. Høyer. "A quantum observable for the graph isomorphism problem", arXiv:quant-ph/9901029, (1999).

[9] A. Garcia & Y. Lequain. Elementos de Álgebra, 3.ed. Rio de Janeiro: IMPA, 325 p. (Projeto Euclides), (2005).

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

[11] D.N. Gonçalves & R. Portugal. "Solution to the Hidden Subgroup Problem for a Class of Noncommutative Groups". Quantum Physics, Abstract quant-ph/1104.1361, (2011).

[12] P. Hoyer. "Efficient quantum transforms". arXiv:quant-ph/9702028, (1997).

[13] Y. Inui & F. Le Gall. An efficient quantum algorithm for the hidden subgroup problem over a class of semi-direct product groups. *Quantum Information and Computation*, (2005).

[14] C. Lomont. "The Hidden Subgroup Problem – Review and Open Problems". Quantum Physics, Abstract quant-ph/0411037, (2004).

[15] M. Mosca. "Quantum algorithms". Encyclopedia of Complexity and Systems Science, pages 7088–7118, (2009).

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

[17] D.R. Simon. "On the Power of Quantum Computation". Proceedings of the 35th Annual Symposium on Foundations of Computer Science, pages 116–123, (1994).

[18] P.W. Shor. "Algorithms for quantum computation: discrete logs and factoring". Proc. of the 35th Ann. IEEE Symp. on the Foundation of Computer Science, pages 124–134, (1994).