Proceeding Series of the Brazilian Society of Computational and Applied Mathematics

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

Demerson Nunes Gonçalves[1]

Coordenação de Licenciatura em Física, CEFET, Petrópolis, RJ

Renato Portugal[2]

Coordenação de Ciência da Computação, LNCC, Petrópolis, RJ

Tharso D. Fernandes[3]

Departamento de Matemática Pura e Aplicada, UFES, Alegre, ES

Programa de Pós-Graduação em Modelagem Computacional, LNCC, Petrópolis, RJ

Abstract. The hidden subgroup problem (HSP) plays an important role in quantum computation, because many quantum algorithms that are exponentially faster than classical algorithms are special cases of the HSP. In this paper we show that there exist 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.

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) [7]. 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 [10, 11]. It is known that for finite abelian groups, the HSP can be solved efficiently on a quantum computer [7]. 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 would imply in an efficient solution for the graph isomorphism problem [1] and for

[1]demerson.goncalves@gmail.com
[2]portugal@lncc.br
[3]tharso.fernandes@ufes.br

 © 2015 SBMAC

the latter would solve instances of the problem of finding the shortest vector in a lattice, which has applications in cryptography [9].

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 $p_1^{r_1} \dots p_n^{r_n}$ 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 $i \neq k$. Te parameter $t \in \{0, 1, \dots, s\}$ characterizes the group as can be checked in Sec. 2. Our algorithm was inspired by the work of Chi et. al. [2] that solved the HSP in $\mathbb{Z}_N \rtimes \mathbb{Z}_p$, where p is a prime that does not divide $p_i - 1$ for any of the prime factors p_i of N. As in [2], we use the homomorphic properties of $G = \mathbb{Z}_N \rtimes \mathbb{Z}_{q^s}$ to reduce the problem to similar ones with known efficient solutions. As far as we know this is the first efficient quantum algorithm to solve the HSP in this class of groups.

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

2 Semi-direct Product Groups

The semi-direct product of two groups A and B is defined by a homomorphism $\phi : B \to \mathrm{Aut}(A)$, where $\mathrm{Aut}(A)$ denotes the automorphism group of A. The semi-direct product $A \rtimes_\phi B$ is the set $\{(a, b) : a \in A, b \in B\}$ with the group operation defined as $(a, b)(a', b') = (a + \phi(b)(a'), b + b')$. One easily checks that the group inversion operation satisfies $(a, b)^{-1} = (\phi(-b)(-a), -b)$.

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 $p_1^{r_1} \dots p_n^{r_n}$ and there exist 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 $t \in \{0, 1, \dots, s\}$ 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 $\mathrm{Aut}(\mathbb{Z}_N)$ 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 $\mathrm{Aut}(\mathbb{Z}_N)$. 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 $\mathrm{ord}(\alpha) = q^t$ 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 [7]. Since $\alpha \in \mathbb{Z}_N^*$, q^t divides $\varphi(N) = p_1^{r_1 - 1} \dots p_n^{r_n - 1}(p_1 - 1) \dots (p_n - 1)$, where φ is the Euler phi-function. Then, we can choose the option $q^t \mid p_n - 1$ with no loss of generality.

Now note that due to factorization of N, the group $\mathbb{Z}_N$ is isomorphic to product of cyclic groups $\mathbb{Z}_{p_1^{r_1}} \times \dots \times \mathbb{Z}_{p_n^{r_n}}$, which implies

$$\mathbb{Z}_N \rtimes_\phi \mathbb{Z}_{q^s} \cong (\mathbb{Z}_{p_1^{r_1}} \times \dots \times \mathbb{Z}_{p_n^{r_n}}) \rtimes_\phi \mathbb{Z}_{q^s}. \tag{1}$$

DOI: 10.5540/03.2015.003.02.0045 © 2015 SBMAC

The elements of $(\mathbb{Z}_{p_1^{r_1}} \times \ldots \times \mathbb{Z}_{p_n^{r_n}}) \rtimes_\phi \mathbb{Z}_{q^s}$ have the form $((a_1, \ldots, a_n), b)$, where $(a_1, \ldots, a_n) \in \mathbb{Z}_{p_1^{r_1}} \times \ldots \times \mathbb{Z}_{p_n^{r_n}}$ and $b \in \mathbb{Z}_{q^s}$. For each b in $\mathbb{Z}_{q^s}$ the element $\phi(b)$ is an automorphism on $\mathbb{Z}_{p_1^{r_1}} \times \ldots \times \mathbb{Z}_{p_n^{r_n}}$ such that $\alpha = \phi(1)(1)$ is an element in $\mathbb{Z}^*_{p_1^{r_1}} \times \ldots \times \mathbb{Z}^*_{p_n^{r_n}}$ 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 $\mathbb{Z}_{p_1^{r_1}} \times \ldots \times \mathbb{Z}_{p_n^{r_n}}$, where $\mathcal{I}_1$ is the identity on $\mathbb{Z}_{p_1^{r_1}} \times \ldots \times \mathbb{Z}_{p_{i-1}^{r_{i-1}}}$ and $\mathcal{I}_2$ is the identity on $\mathbb{Z}_{p_{i+1}^{r_{i+1}}} \times \ldots \times \mathbb{Z}_{p_n^{r_n}}$, for all $i = 1, \ldots, n$. 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 two results. The proofs follow similar strategies as proving Lemmas 1 and 2 in Ref. [2].

Lemma 2.1. *Let $\mathbb{Z}_{p_1^{r_1}} \times \ldots \times \mathbb{Z}_{p_n^{r_n}}$ and $\mathbb{Z}_{q^s}$ be finite abelian groups with distinct odd prime numbers $p_1, \ldots, p_n$ and q and positive integers $r_1, \ldots, r_n$ and s. Define the semi-direct product group $(\mathbb{Z}_{p_1^{r_1}} \times \ldots \times \mathbb{Z}_{p_n^{r_n}}) \rtimes_\phi \mathbb{Z}_{q^s}$. Then for each $b \in \mathbb{Z}_{q^s}$ and $a_i \in \mathbb{Z}_{p_i^{r_i}}$ there exist 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 $\mathbb{Z}_{p_1^{r_1}} \times \ldots \times \mathbb{Z}_{p_n^{r_n}}$ with all components equal zero except the i-th one which is 1. 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, let us suppose that $\phi(b)(e_i) = (d_1, \ldots, d_n)$. Note that

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

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

Theorem 2.1. *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 exist 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*

$$\mathbb{Z}_N \rtimes_\phi \mathbb{Z}_{q^s} \cong (\mathbb{Z}_{p_1^{r_1}} \times \ldots \times \mathbb{Z}_{p_{n-1}^{r_{n-1}}}) \times (\mathbb{Z}_{p^r} \rtimes_\psi \mathbb{Z}_{q^s}), \tag{2}$$

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 2.1 that $e_i = \phi(q^s)e_i = (0 \ldots, {d_i}^{q^s}, \ldots, 0)$. Then ${d_i}^{q^s} = 1 \bmod p_i^{r_i}$ and $d_i \in \mathbb{Z}^*_{p_i^{r_i}}$ has order $q^{t'}$, for some $t' \in \{1, \ldots, s\}$. Suppose $d_i \neq 1$. 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 d_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

$$\phi(b)(a_1, \ldots, a_n) = (a_1, \ldots, a_{n-1}, \psi(b)(a_n)). \tag{3}$$

DOI: 10.5540/03.2015.003.02.0045 © 2015 SBMAC

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

$$\begin{aligned} gg' &= ((a_1, \ldots, a_n) + \phi(b)(a'_1, \ldots, a'_n), b + b') \\ &= ((a_1 + a'_1, \ldots, a_{n-1} + a'_{n-1}, a_n + \psi(b)(a'_n), b + b'). \end{aligned} \tag{4}$$

Define the map

$$\Gamma : \mathbb{Z}_N \rtimes_\phi \mathbb{Z}_{q^s} \to (\mathbb{Z}_{p_1^{r_1}} \times \ldots \times \mathbb{Z}_{p_{n-1}^{r_{n-1}}}) \times (\mathbb{Z}_{p^r} \rtimes_\psi \mathbb{Z}_{q^s}), \tag{5}$$

such that $\Gamma(a_1, \ldots, a_n, b)) = ((a_1, \ldots, a_{n-1}), (a_n, b))$. It is easy to show that this map is indeed an isomorphism. □

3 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 $N = p_1^{r_1} \ldots p_n^{r_n}$ and given a $1 \leq t \leq s$, there exists a $1 \leq k \leq n$ such that q^t divides $p_k - 1$ and $q \nmid p_i - 1$ for all $i \neq k$.

By defining $N' = N/p_n^{r_n}$ we obtain $\mathbb{Z}_{p_1^{r_1}} \times \ldots \times \mathbb{Z}_{p_{n-1}^{r_{n-1}}} \cong \mathbb{Z}_{N'}$. From Theorem 2.1, it follows that $\mathbb{Z}_N \rtimes_\phi \mathbb{Z}_{q^s} \cong \mathbb{Z}_{N'} \times (\mathbb{Z}_{p^r} \rtimes_\psi \mathbb{Z}_{q^s})$. The orders of the groups in this direct product are relatively prime. Hence, from Lemma 3 (Ref. [2]), if H is a subgroup of $\mathbb{Z}_{N'} \times (\mathbb{Z}_{p^r} \rtimes_\psi \mathbb{Z}_{q^s})$ then $H = H_1 \times H_2$, where H_1 is a subgroup of $\mathbb{Z}_{N'}$ and H_2 is a subgroup of $\mathbb{Z}_{p^r} \rtimes_\psi \mathbb{Z}_{q^s}$. The HSP on $\mathbb{Z}_N \rtimes \mathbb{Z}_{q^s}$ reduces to the HSP on each factor by the following.

Let f be the oracle function that hides the subgroup H in $\mathbb{Z}_{N'} \times (\mathbb{Z}_{p^r} \rtimes_\psi \mathbb{Z}_{q^s})$. For simplicity of notation, let us call $A = \mathbb{Z}_{N'}$ and $B = \mathbb{Z}_{p^r} \rtimes_\psi \mathbb{Z}_{q^s}$. Define oracle function f_1 by the restriction of f to A, which hides H_1 in A. Analogously, define oracle function f_2 by the the restriction of f to B, which hides H_2 in B. The solution of the HSP in the groups A and B with functions f_1 and f_2 determines generators for the subgroups H_1 and H_2, respectively. The group A is abelian and the group B was addressed in [5,6] and recently generalized by [4]. Therefore, we obtain the following result:

Theorem 3.1. *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 exist 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 $\mathbb{Z}_N \rtimes_\alpha \mathbb{Z}_{q^s}$.*

4 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 $N = p_1^{r_1} \ldots p_n^{r_n}$ 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

DOI: 10.5540/03.2015.003.02.0045 © 2015 SBMAC

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

The authors would like to tank the CNPq and Faperj for financial support and the anonymous reviewers for their valuable comments and suggestions to improve the manuscript.

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. P. Chi, J. S. Kim and 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).

[3] A. M. Childs and W. van Dam, Quantum algorithms for algebraic problems, Rev. Mod. Phys., 82(1): 1–52, (2010).

[4] W. van Dam and 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).

[5] D. N. Gonçalves, R. Portugal, and 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).

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

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

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

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

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

 © 2015 SBMAC

[11] 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).

DOI: 10.5540/03.2015.003.02.0045 © 2015 SBMAC