Hidden Subgroup Quantum Algorithms for a Class of Semi-Direct Product Groups

Wim van Dam[1] and Siladitya Dey[2]

1 **Department of Computer Science, Department of Physics, University of California, Santa Barbara, California, 93106, United States of America**
vandam@cs.ucsb.edu

2 **Department of Computer Science, University of California, Santa Barbara California, 93106, United States of America**
siladitya_dey@cs.ucsb.edu

Abstract

A quantum algorithm for the Hidden Subgroup Problem over the group $\mathbb{Z}/p^r\mathbb{Z} \rtimes \mathbb{Z}/q^s\mathbb{Z}$ is presented. This algorithm, which for certain parameters of the group qualifies as 'efficient', generalizes prior work on related semi-direct product groups.

1998 ACM Subject Classification F.1.2 Modes of Computation, F.2.2 Nonnumerical Algorithms and Problems

Keywords and phrases quantum algorithms, quantum complexity theory, computational group theory

Digital Object Identifier 10.4230/LIPIcs.TQC.2014.110

1 Introduction and Related Work

1.1 Introduction

The quantum algorithm to factorize integers as given by Shor [8] in 1994 is exponentially faster than any known classical algorithm. The success of Shor's algorithm resulted in a great deal of interest in quantum computing, subsequently resulting in the design of several more quantum algorithms that are exponentially faster than their classical counterparts. Several of these algorithms solve the problem of finding subgroup generators of a group using evaluations of a function that "hides" the subgroup [2]. This generalized framework is captured by the Hidden Subgroup Problem (referred henceforth as HSP) and has been successful in admitting quantum algorithms that are exponentially faster than their classical counterparts. It is known that there exists an efficient solution to the HSP for finite Abelian groups, but this is not known to hold for non-Abelian groups. The motivation for research in this area stems from knowledge that an efficient solution to the HSP over the symmetric group (dihedral group) will result in an efficient quantum algorithm for graph isomorphism (shortest vector in a lattice). In this article, we present an algorithm to solve the hidden subgroup in the specific class of non-Abelian groups, i.e. the semi-direct product groups of the form $G := \mathbb{Z}/p^r\mathbb{Z} \rtimes \mathbb{Z}/q^s\mathbb{Z}$, where p, q are prime with $p \neq q$ and $r, s \in \mathbb{Z}^+$ with the relative sizes of the subgroups bounded by $p^r/q^{t-j} \in O(\mathrm{poly}(\log p^r))$ where $j \in \{0, \ldots, t-1\}$ is a parameter specific to the group. For certain parameters of G and its subgroup, this algorithm has running time $O(\mathrm{poly}(\log |G|))$, and hence qualifies as 'efficient'.

In Section 2 we clarify the structure of the group $\mathbb{Z}/p^r\mathbb{Z} \rtimes \mathbb{Z}/q^s\mathbb{Z}$ and its subgroups. The quantum algorithm that will help solve for the hidden subgroup, H within this specific class of non-Abelian groups is presented in Section 3.


9th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC'14).
Editors: Steven T. Flammia and Aram W. Harrow; pp. 110–117

Leibniz International Proceedings in Informatics
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

1.2 Related Work

There has been considerable work in trying to solve the HSP in semi-direct product groups. In this article we discuss the case $\mathbb{Z}/p^r\mathbb{Z} \rtimes \mathbb{Z}/q^s\mathbb{Z}$. It was shown in [1] that the HSP in $\mathbb{Z}/N\mathbb{Z} \rtimes \mathbb{Z}/q\mathbb{Z}$, for positive integers N, q such that $N/q \in O(\text{poly}(\log N))$, reduces to finding cyclic subgroups of order q and can be efficiently solved. This work was extended in [6], which developed an efficient HSP algorithm in $(\mathbb{Z}/p^r\mathbb{Z})^m \rtimes \mathbb{Z}/p\mathbb{Z}$, with p prime and integers r, m. Following this, in 2009 an efficient quantum algorithm to solve the HSP in $\mathbb{Z}/p\mathbb{Z} \rtimes \mathbb{Z}/q^s\mathbb{Z}$ for distinct odd primes and $s > 0$ such that $p/q \in O(\text{poly}(\log p))$ was shown [4]. More recently in [5], the HSP problem was considered in $\mathbb{Z}/p^r\mathbb{Z} \rtimes \mathbb{Z}/q^s\mathbb{Z}$ where p, q are distinct primes such that $p^r/q \in O(\text{poly}(\log p^r))$. The current article extends this previous result [5]. Specifically, the group $\mathbb{Z}/p^r\mathbb{Z} \rtimes \mathbb{Z}/q^s\mathbb{Z}$ has a parameter t (as explained in the next section) that characterizes the group. In [5] an algorithm was presented for the $t = 1$ case; here we deal with all possible values $t \in \{0, \ldots, s\}$. Whether or not our algorithm qualifies as efficient depends on the specific parameters of G and its subgroup, which will be explained in Section 3.

2 The Group $\mathbb{Z}/p^r\mathbb{Z} \rtimes \mathbb{Z}/q^s\mathbb{Z}$ and Its Subgroups

2.1 Some Properties of the Group $\mathbb{Z}/p^r\mathbb{Z} \rtimes \mathbb{Z}/q^s\mathbb{Z}$

In this section we discuss and prove various properties of the semi-direct product group $G := \mathbb{Z}/p^r\mathbb{Z} \rtimes \mathbb{Z}/q^s\mathbb{Z}$, with p, q prime and $r, s \in \mathbb{Z}^+$. We know that $\mathbb{Z}/p^r\mathbb{Z}$ and $\mathbb{Z}/q^s\mathbb{Z}$ are finite, cyclic, Abelian groups. Let $\phi\colon \mathbb{Z}/q^s\mathbb{Z} \to \text{Aut}(\mathbb{Z}/p^r\mathbb{Z})$ be the group homomorphism that defines G, for all $a, c \in \mathbb{Z}/p^r\mathbb{Z}$ and all $b, d \in \mathbb{Z}/q^s\mathbb{Z}$:

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

As $\mathbb{Z}/q^s\mathbb{Z}$ is cyclic, we have for all b that $\phi(b) = \phi(1 + \cdots + 1) = \phi(1)^b$. In a similar vein, since $\mathbb{Z}/p^r\mathbb{Z}$ is also cyclic, we have $\phi(1)(c) = \phi(1)(1 + \cdots + 1) = \phi(1)(1) + \cdots + \phi(1)(1) = c\phi(1)(1)$. We thus see that ϕ is completely determined by the single value $\phi(1)(1)$, which from now on will be denoted by $\alpha := \phi(1)(1) \in (\mathbb{Z}/p^r\mathbb{Z})^*$. The group operation in $G = \mathbb{Z}/p^r\mathbb{Z} \rtimes_\alpha \mathbb{Z}/q^s\mathbb{Z}$ thus simplifies to

$$(a, b)(c, d) = (a + \alpha^b c, b + d). \tag{2}$$

The identity in G is $(0, 0)$ and the inverse is expressed by $(a, b)^{-1} = (-\alpha^{-b}a, -b)$.

Because it must hold that $1 = \alpha^0 = \alpha^{(q^s)}$ we have that there exists a smallest integer $t \in \{0, \ldots, s\}$ such that $\alpha^{(q^t)} = 1$. As explained in [5], if the groups $G = \mathbb{Z}/p^r \rtimes_\alpha \mathbb{Z}/q^s\mathbb{Z}$ and $G' = \mathbb{Z}/p^r \rtimes_{\alpha'} \mathbb{Z}/q^s\mathbb{Z}$ have the same t-parameter ($t = t'$), then these groups are isomorphic. Additionally, if $t = 0$ we have that $\alpha = 1$, making G Abelian. From now on we will thus assume that $t \in \{1, \ldots, s\}$. It can be shown that $q^t \mid (p - 1)$. We also note that it can be shown that G is supersolvable.

2.2 Subgroups of $\mathbb{Z}/p^r\mathbb{Z} \rtimes \mathbb{Z}/q^s\mathbb{Z}$

Following [5, Theorem 2], the subgroups of the group $G = \mathbb{Z}/p^r\mathbb{Z} \rtimes_\alpha \mathbb{Z}/q^s\mathbb{Z}$ are from either one of three types. With $t \in \{1, \ldots, s\}$ the parameter of G as explained in the previous section, these types are as follows.

Type I: $H^{\text{I}}_{i,j} = \langle (p^i, q^j) \rangle$, for each $i \in \{0, \ldots, r\}$ and $j \in \{t, \ldots, s\}$.
Type II: $H^{\text{II}}_{j,\eta} = \langle (\eta, q^j) \rangle$, for each $j \in \{0, \ldots, t-1\}$ and $\eta \in \mathbb{Z}/p^r\mathbb{Z}$.
Type III: $H^{\text{III}}_{i,j,\eta} = \langle (p^i, 0), (\eta, q^j) \rangle$, for each $i \in \{0, \ldots, r-1\}$, $j \in \{0, \ldots, t-1\}$, and $\eta \in \{0, \ldots, p^i - 1\}$.

We point out that [5, Theorem 2] allows the η parameter for Type III subgroups to be from the whole set $\{0, \ldots, p^r - 1\}$ but that this creates ambiguity as, for example, $H^{\mathrm{III}}_{0,0,0} = \langle (1,0),(0,1)\rangle = G$ and $H^{\mathrm{III}}_{0,0,1} = \langle (1,0),(1,1)\rangle = G$ as well. By limiting η to the set $\{0, \ldots, p^i - 1\}$ each triplet of parameters (i, j, η) defines a unique Type III subgroup.

Next, we will describe the parameterization of the elements of these three types of subgroups. The elements of the Type I subgroup are of the form $(p^i, q^j)^z = (zp^i, zq^j)$ where $z \in \mathbb{Z}$ and where we used the fact that $\alpha^{(q^j)} = 1$ as $j \geq t$. Because $\gcd(p^r, q^s) = 1$ we can further simplify this description to

$$H^{\mathrm{I}}_{i,j} = \{(xp^i, yq^j) : x \in \{0, \ldots, p^{r-i} - 1\}, y \in \{0, \ldots, q^{s-j} - 1\}\}, \tag{3}$$

showing that $H^{\mathrm{I}}_{i,j}$ has $p^{r-i}q^{s-j}$ elements.

The subgroups of Type II and III are less trivial to describe. To better understand the elements of the subgroup $\langle (\eta, q^j)\rangle$, consider first some small powers of the generating element (η, q^j):

$$\begin{cases} (\eta, q^j)^{-1} & = (-\eta\alpha^{(-q^j)}, -q^j) \\ (\eta, q^j)^0 & = (0,0) \\ (\eta, q^j)^1 & = (\eta, q^j) \\ (\eta, q^j)^2 & = (\eta + \eta\alpha^{(q^j)}, 2q^j) \\ (\eta, q^j)^3 & = (\eta + \eta\alpha^{(q^j)} + \eta\alpha^{(2q^j)}, 3q^j) \end{cases} \tag{4}$$

and so on. In general we have the following characterization.

▶ **Lemma 1.** *Let $G = \mathbb{Z}/p^r\mathbb{Z} \rtimes_\alpha \mathbb{Z}/q^s\mathbb{Z}$ and let $t \in \{1, \ldots, s\}$ be the smallest positive integer such that $\alpha^{(q^t)} = 1$. For any $\eta \in \mathbb{Z}/p^r\mathbb{Z}$ and $j \in \{0, \ldots, t-1\}$ consider the cyclic subgroup $H = \langle (\eta, q^j)\rangle$. For each exponent $y \in \mathbb{Z}$, the elements of H can be described by $(\eta, q^j)^y = (\eta S(y), yq^j)$ where $S\colon \mathbb{Z} \to \mathbb{Z}/p^r\mathbb{Z}$ is defined by*

$$S(y) := \frac{\alpha^{(yq^j)} - 1}{\alpha^{(q^j)} - 1}. \tag{5}$$

As a result, the subgroup has q^{s-j} elements such that

$$H^{\mathrm{II}}_{j,\eta} := \langle (\eta, q^j)\rangle = \{(\eta S(y), yq^j) : y \in \{0, \ldots, q^{s-j} - 1\}\}. \tag{6}$$

Proof. In [5, Lemma A2] it is shown that $\alpha^{(q^j)} - 1$ is invertible in $\mathbb{Z}/p^r\mathbb{Z}$ hence the definition of S in Equation 5 does indeed make sense. Assuming for a given y that $(\eta, q^j)^y = (\eta S(y), yq^j)$ we get $(\eta, q^j)^{y+1} = (\eta, q^j)(\eta S(y), yq^j) = (\eta(1 + \alpha^{(q^j)}S(y)), (y+1)q^j)$. With this relation $S(y+1) = 1 + \alpha^{(q^j)}S(y)$ and $S(0) = 0$ the Equality 5 can be proven by induction on y.

From the $\mathbb{Z}/q^s\mathbb{Z}$ part of G it is obvious that the values y such that $(\eta S(y), yq^j) = (0,0)$ must obey that y is a multiple of q^{s-j}. Conversely, if $y = \lambda q^{s-j}$, then $S(y) = (\alpha^{(\lambda q^s)} - 1)/(\alpha^{(q^j)} - 1) = 0$. Hence $(\eta S(y), yq^j) = (0,0)$ if and only if $y = 0 \bmod q^{s-j}$. ◀

Upon further inspection it is clear that S has period q^{t-j}, which will be helpful in the reduction of the complexity of finding the hidden subgroup H in G.

The Type III subgroups are obviously extensions of the previous type. As we have $(p^i, 0)(\eta S(y), yq^j) = (p^i + \eta S(y), yq^j)$ and $(\eta S(y), yq^j)(p^i, 0) = (\eta S(y) + \alpha^{(yq^j)}p^i, yq^j)$ it is clear that the elements of H^{III} can be described by

$$H^{\mathrm{III}}_{i,j,\eta} = \{(xp^i + \eta S(y), yq^j) : x \in \{0, \ldots, p^{r-i} - 1\}, y \in \{0, \ldots, q^{s-j} - 1\}\}, \tag{7}$$

which also shows that it has $p^{r-i}q^{s-j}$ elements, and hence that $H^{\mathrm{III}}_{0,0,\eta} = G$, regardless of η. More generally, it is only the value $\eta \bmod p^i$ that matters in the definition of this subgroup.

3 Quantum Algorithm for HSP in $\mathbb{Z}/p^r\mathbb{Z} \rtimes \mathbb{Z}/q^s\mathbb{Z}$

3.1 Overview of Algorithm

In this section we will present a quantum algorithm that solves the hidden subgroup problem in $G = \mathbb{Z}/p^r\mathbb{Z} \rtimes_\alpha \mathbb{Z}/q^s\mathbb{Z}$, but before doing so we will reduce the problem significantly. As in the previous section, the group operation is defined by $(a,b)(c,d) = (a + \alpha^b c, b + d)$ where $\alpha \in (\mathbb{Z}/p^r\mathbb{Z})^*$ and for which there exists a smallest integer $t \in \{1,\ldots,s\}$ such that $\alpha^{(q^t)} = 1$. Let f be the subgroup hiding function on G, which obeys

$$f((a,b)) = f((a',b')) \text{ if and only if } (a,b)^{-1}(a',b') \in H. \tag{8}$$

In other words, f is constant on the left cosets of H and f is different between different cosets of H.

Recall from Section 2.2 that the subgroups of G are one of three types with potentially unknown parameters i, j, η. In [5, Section 3] it was claimed that it was sufficient to solve the HSP for Type II subgroups but the current authors were unable to reproduce this result. Instead we will present an alternative way of finding the hidden subgroup.

We assume that all the parameters (p, r, q, s, α, and t) of the group G are known. For our purposes, an algorithm is considered efficient if its running time is bounded by $O(\text{poly}(\log(|G|)) = O(\text{poly}(r\log p + s\log q))$. Note that when an algorithm suggests that a group H' is the hidden subgroup, then that suggestion can be checked by querying f on $(0,0)$ and on the generators of H'. If H' passes this check we can conclude that $H' \leq H$; otherwise a mistake was made and the algorithm should be executed again to find another suggestion for H. Repeating the above procedure will give a 'largest' subgroup that with high probability will equal the true hidden subgroup.

Because of the just described approach to solve the HSP, it is sufficient to use an algorithm that finds the hidden subgroup with a success rate that is significant enough. For the current case of possible subgroups of G it is therefore sufficient to simply guess the parameters $i \in \{0,\ldots,r\}$ and $j \in \{0,\ldots,s\}$ as the probability of doing so correctly equals $1/rs \in \Omega(1/\text{poly}(\log|G|))$. If the subgroup is of Type I this will have answered the HSP completely. In the case of Type II or Type III subgroups the following quantum algorithms will have to be employed to find the unknown parameter $\eta \in \mathbb{Z}/p^r\mathbb{Z}$ (Type II) or $\eta \in \{0,\ldots,p^i - 1\}$ (Type III).

3.2 Quantum Algorithm for Finding HSP in $\mathbb{Z}/p^r\mathbb{Z} \rtimes \mathbb{Z}/q^s\mathbb{Z}$

▶ **Theorem 2.** *Let p and q be distinct primes and let r and s be positive integers. Define the semi-direct product group $G := \mathbb{Z}/p^r\mathbb{Z} \rtimes_\alpha \mathbb{Z}/q^s\mathbb{Z}$ by the non-commuting group operation that, for all $a,c \in \mathbb{Z}/p^r\mathbb{Z}$ and all $b,d \in \mathbb{Z}/q^s\mathbb{Z}$, has $(a,b)(c,d) = (a + \alpha^b c, b + d)$ for an $\alpha \in (\mathbb{Z}/p^r\mathbb{Z})^*$. Let $t \in \{1,\ldots,s\}$ be the smallest positive integer such that $\alpha^{(q^t)} = 1$.*

Let the function f on G hide a Type II subgroup $H = \langle(\eta, q^j)\rangle$ and assume that the parameter $j \in \{0,\ldots,t-1\}$ is known. There exists a probabilistic quantum algorithm that determines the unknown parameter $\eta \in \mathbb{Z}/p^r\mathbb{Z}$ with success probability $(1-1/p)(q^{t-j}/p^r)$ using only one query to f.

Proof. This proof is inspired by the PGM algorithm described in [1], but it uses several additional ingredients specific to the properties of this group G and its subgroups (for which see Section 2).

1. Initialize the register in the state,

$$|\psi_1\rangle = \frac{1}{\sqrt{p^r q^{t-j}}} \sum_{x \in \mathbb{Z}/p^r\mathbb{Z}} \sum_{y=0}^{q^{t-j}-1} |x, yq^j, f((x, yq^j))\rangle.$$

   Note how the second register contains only multiples of q^j and how the range of yq^j goes only to q^t and not q^s.
2. The p^r different left cosets of H that are relevant for this algorithm are described by $(\ell, 0)H = \{(\ell + \eta S(y), yq^j) : y \in \{0, \ldots, q^{t-j} - 1\}\}$, for each $\ell \in \mathbb{Z}/p^r\mathbb{Z}$. After measuring (and ignoring) the third register of $|\psi_1\rangle$ in the computational basis we thus get the state

$$|\psi_2\rangle = \frac{1}{\sqrt{q^{t-j}}} \sum_{y=0}^{q^{t-j}-1} |\ell + \eta S(y), yq^j\rangle,$$

   for an unknown and irrelevant $\ell \in \mathbb{Z}/p^r\mathbb{Z}$.
3. Applying the Fourier Transform over $\mathbb{Z}/p^r\mathbb{Z}$ to the first register of $|\psi_2\rangle$ we get, with $\omega := \exp(\mathrm{i}2\pi/p^r)$,

$$\begin{aligned} |\psi_3\rangle &= \frac{1}{\sqrt{p^r q^{t-j}}} \sum_{k \in \mathbb{Z}/p^r\mathbb{Z}} \sum_{y=0}^{q^{t-j}-1} \omega^{k(\ell + \eta S(y))} |k, yq^j\rangle \\ &= \frac{1}{\sqrt{p^r q^{t-j}}} \sum_{k \in \mathbb{Z}/p^r\mathbb{Z}} \omega^{k\ell} |k\rangle \sum_{y=0}^{q^{t-j}-1} \omega^{k\eta S(y)} |yq^j\rangle. \end{aligned}$$

4. Measure the first register in the computational basis and assume the result is some invertible $k \in (\mathbb{Z}/p^r\mathbb{Z})^*$ (which occurs with probability $(1 - 1/p)$). Tracing out this k register gives us the remaining superposition

$$|\psi_4\rangle = \frac{1}{\sqrt{q^{t-j}}} \sum_{y=0}^{q^{t-j}-1} \omega^{k\eta S(y)} |yq^j\rangle.$$

5. We now take the yq^j register in $|\psi_4\rangle$ and use it to append a second register with the value $kS(y) = k(\alpha^{(yq^j)} - 1)/(\alpha^{(q^j)} - 1) \bmod p^r$. As α, q, j, p^r, k are known and $(\alpha^{(q^j)} - 1)$ is invertible, this transformation can be done efficiently, yielding

$$|\psi_5\rangle = \frac{1}{\sqrt{q^{t-j}}} \sum_{y=0}^{q^{t-j}-1} \omega^{k\eta S(y)} |yq^j, kS(y)\rangle.$$

6. Because k is invertible and the function S is injective on $\{0, \ldots, q^{t-j} - 1\}$, we can determine a unique solution y from the value $kS(y)$. Using Shor's discrete logarithm algorithm we can hence efficiently implement the unitary mapping $|yq^j, kS(y)\rangle \mapsto |0, kS(y)\rangle$, giving

$$|\psi_6\rangle = \frac{1}{\sqrt{q^{t-j}}} \sum_{y=0}^{q^{t-j}-1} \omega^{k\eta S(y)} |kS(y)\rangle.$$

7. Finally, we perform an inverse Fourier transform over $\mathbb{Z}/p^r\mathbb{Z}$ in the hope of observing the unknown η. To calculate the probability of this occurring, consider the ideal state $|\hat{\eta}\rangle := \sum_{z \in \mathbb{Z}/p^r\mathbb{Z}} \omega^{z\eta} |z\rangle / \sqrt{p^r}$, which is guaranteed to give η. The fidelity squared between this perfect state and our actual state is $|\langle \psi_6 | \hat{\eta} \rangle|^2 = (q^{t-j})/p^r$, which is thus the probability of observing η at the end of this step.

The above algorithm requires one f-query and $\text{poly}(\log|G|)$ time and space. Its overall success probability equals $(1-1/p)(q^{t-j}/p^r)$. ◀

The algorithm for finding Type III subgroups is an adaptation of the just described algorithm. Crucially, the unknown parameter η is an element of the set $\{0,\ldots,p^i-1\}$, which influences the first register of the algorithm.

▶ **Theorem 3.** *Let p and q be distinct primes and let r and s be positive integers. Define the semi-direct product group $G := \mathbb{Z}/p^r\mathbb{Z} \rtimes_\alpha \mathbb{Z}/q^s\mathbb{Z}$ by the non-commuting group operation that, for all $a,c \in \mathbb{Z}/p^r\mathbb{Z}$ and all $b,d \in \mathbb{Z}/q^s\mathbb{Z}$ has $(a,b)(c,d) = (a+\alpha^b c, b+d)$ for an $\alpha \in (\mathbb{Z}/p^r\mathbb{Z})^*$. Let $t \in \{1,\ldots,s\}$ be the smallest positive integer such that $\alpha^{(q^t)} = 1$.*

Let the function f hide a Type III subgroup $H = \langle (p^i,0),(\eta,q^j)\rangle$ in G and assume that the parameters $i \in \{0,\ldots,r-1\}$ and $j \in \{0,\ldots,t-1\}$ are known. There exists a probabilistic quantum algorithm that can determine the unknown parameter $\eta \in \{0,\ldots,p^i-1\}$ with success probability $(1-1/p)(q^{t-j}/p^i)$ using only one query to f.

Proof. This algorithm is quite similar to the one of the previous theorem, except for the fact that the first register will be restricted to elements of $\mathbb{Z}/p^i\mathbb{Z}$.

1. Initialize the register in the state

$$|\psi_1\rangle = \frac{1}{\sqrt{p^i q^{t-j}}} \sum_{x=0}^{p^i-1} \sum_{y=0}^{q^{t-j}-1} |x, yq^j, f((x,yq^j))\rangle.$$

   Note how the second register contains only multiples of q^j, how the range of yq^j goes only to q^t and not q^s, and how the first register contains only p^i elements.
2. The p^i different left cosets of H that are relevant for this algorithm are described by $(\ell,0)H = \{(\ell + xp^i + \eta S(y), yq^j) : x \in \{0,\ldots,p^{r-i}-1\}, y \in \{0,\ldots,q^{t-j}-1\}\}$, for each $\ell \in \{0,\ldots,p^i-1\}$. As the first register contains values from the set $\{0,\ldots,p^i-1\}$ this description further reduces to $\{(\ell+\eta S(y) \bmod p^i, yq^j) : y \in \{0,\ldots,q^{t-j}-1\}\}$. Measuring the third register of $|\psi_1\rangle$ in the computational basis we get the state

$$|\psi_2\rangle = \frac{1}{\sqrt{q^{t-j}}} \sum_{y=0}^{q^{t-j}-1} |\ell + \eta S(y) \bmod p^i, yq^j\rangle,$$

   for an unknown and irrelevant $\ell \in \{0,\ldots,p^i-1\}$.
3. From now on we interpret the first register of $|\psi_2\rangle$ as containing values from $\mathbb{Z}/p^i\mathbb{Z}$ and we apply the Fourier Transform over $\mathbb{Z}/p^i\mathbb{Z}$ to it. With $\omega := \exp(\mathrm{i}2\pi/p^i)$, we get

$$\begin{aligned}|\psi_3\rangle &= \frac{1}{\sqrt{p^i q^{t-j}}} \sum_{k\in\mathbb{Z}/p^i\mathbb{Z}} \sum_{y=0}^{q^{t-j}-1} \omega^{k(\ell+\eta S(y))} |k, yq^j\rangle \\ &= \frac{1}{\sqrt{p^i q^{t-j}}} \sum_{k\in\mathbb{Z}/p^i\mathbb{Z}} \omega^{k\ell}|k\rangle \sum_{y=0}^{q^{t-j}-1} \omega^{k\eta S(y)} |yq^j\rangle.\end{aligned}$$

4. Measure the first register in the computational basis and assume the result is some invertible $k \in (\mathbb{Z}/p^i\mathbb{Z})^*$, which occurs with probability $(1-1/p)$. Tracing out this k register gives us the remaining superposition

$$|\psi_4\rangle = \frac{1}{\sqrt{q^{t-j}}} \sum_{y=0}^{q^{t-j}-1} \omega^{k\eta S(y)} |yq^j\rangle.$$

5. We now take the yq^j register in $|\psi_4\rangle$ and use it to append a second register with the value $kS(y) = k(\alpha^{(yq^j)} - 1)/(\alpha^{(q^j)} - 1) \bmod p^i$. As α, q, j, p^i, k are known and $(\alpha^{(q^j)} - 1)$ is invertible, this transformation can be done efficiently, yielding

$$|\psi_5\rangle = \frac{1}{\sqrt{q^{t-j}}} \sum_{y=0}^{q^{t-j}-1} \omega^{k\eta S(y)} |yq^j, kS(y)\rangle.$$

6. Because k is invertible and the function S is injective on $\{0, \ldots, q^{t-j}-1\}$, we can determine a unique solution y from the value $kS(y)$. Using Shor's discrete logarithm algorithm we can hence efficiently implement the unitary mapping $|yq^j, kS(y)\rangle \mapsto |0, kS(y)\rangle$, giving

$$|\psi_6\rangle = \frac{1}{\sqrt{q^{t-j}}} \sum_{y=0}^{q^{t-j}-1} \omega^{k\eta S(y)} |kS(y)\rangle.$$

7. Finally we perform an inverse Fourier transform over $\mathbb{Z}/p^i\mathbb{Z}$ in the hope of observing the unknown η. To calculate the probability of this occurring consider the ideal state $|\hat{\eta}\rangle := \sum_{z \in \mathbb{Z}/p^i\mathbb{Z}} \omega^{z\eta} |z\rangle / \sqrt{p^i}$, which is guaranteed to give η. The fidelity squared between this perfect state and our actual state is $|\langle\psi_6|\hat{\eta}\rangle|^2 = (q^{t-j})/p^i$, which is thus the probability of observing η at the end of this step.

The above algorithm requires one f-query and $\mathrm{poly}(\log|G|)$ time and space. Its overall success probability equals $(1 - 1/p)(q^{t-j}/p^i)$. ◀

Summarizing the above theorems, we have the following result.

▶ **Corollary 4.** *Let p and q be distinct primes and let r and s be positive integers. Define the semi-direct product group $G := \mathbb{Z}/p^r\mathbb{Z} \rtimes_\alpha \mathbb{Z}/q^s\mathbb{Z}$ by the non-commuting group operation that, for all $a, c \in \mathbb{Z}/p^r\mathbb{Z}$ and all $b, d \in \mathbb{Z}/q^s\mathbb{Z}$, has $(a, b)(c, d) = (a + \alpha^b c, b + d)$ for an $\alpha \in (\mathbb{Z}/p^r\mathbb{Z})^*$. Let $t \in \{1, \ldots, s\}$ be the smallest positive integer such that $\alpha^{(q^t)} = 1$. Let the function f on G hide a subgroup H. There exists a quantum algorithm that determines H with a time complexity depending on the type of H in the following manner.*

Type I: *If $H^{\mathrm{I}}_{i,j} = \langle (p^i, q^j) \rangle$ for some unknown $i \in \{0, \ldots, r\}$ and $j \in \{t, \ldots, s\}$, then H will be found efficiently in time $O(\mathrm{poly}(\log|G|))$.*

Type II: *If $H^{\mathrm{II}}_{j,\eta} = \langle (\eta, q^j) \rangle$ for some unknown $j \in \{0, \ldots, t-1\}$ and $\eta \in \mathbb{Z}/p^r\mathbb{Z}$, then H will be found in time $O(\mathrm{poly}(\log|G|, p^r/q^{t-j}))$.*

Type III: *If $H^{\mathrm{III}}_{i,j,\eta} = \langle (\eta, q^j) \rangle$ for some unknown $i \in \{0, \ldots, r-1\}$, $j \in \{0, \ldots, t-1\}$ and $\eta \in \{0, \ldots, p^i - 1\}$, then H will be found in time $O(\mathrm{poly}(\log|G|, p^i/q^{t-j}))$.*

The quantum algorithm can be considered efficient, i.e. has running time $O(\mathrm{poly}(\log|G|))$, if the subgroup is of Type I, or if the Type II subgroup $H^{II}_{j,\eta}$ has $p^r/q^{t-j} \in \mathrm{poly}(\log|G|)$, or if the Type III subgroup $H^{III}_{i,j,\eta}$ has $p^i/q^{t-j} \in \mathrm{poly}(\log|G|)$.

These running times should be compared to the classical algorithm of repeatedly simply guessing the parameters i, j, η of the hidden subgroup. For Type I, II, and III subgroups this approach gives a running time of $O(\mathrm{poly}(\log|G|))$, $O(\mathrm{poly}(\log|G|, p^r))$, and $O(\mathrm{poly}(\log|G|, p^i))$ respectively. Hence we see that the presented quantum algorithm provides a speed-up of order $\Omega(q^{t-j})$ for subgroups of Type II and III.

4 Conclusion

In this paper, we consider the Hidden Subgroup Problem in the semi-direct product group $\mathbb{Z}/p^r\mathbb{Z} \rtimes \mathbb{Z}/q^s\mathbb{Z}$ with p, q distinct primes. Our result generalizes the work in [5], which imposed

a restriction on the kind of homomorphism that the semi-direct product uses. The result here holds for all possible $\mathbb{Z}/p^r\mathbb{Z} \rtimes \mathbb{Z}/q^s\mathbb{Z}$. While our algorithm is efficient for certain cases of the parameters of G and H, it is not so in other cases. This partial result is not unexpected as the design of an efficient algorithm for the HSP for the dihedral group $\mathbb{Z}/p^r\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$ remains a major open problem in the theory of quantum algorithms.

Acknowledgements. This material is based upon work supported by the National Science Foundation under Grant No. 0747526.

References

1 Dave Bacon, Andrew M. Childs, Wim van Dam, *From optimal measurement to efficient quantum algorithms for the hidden subgroup problem over semidirect product groups*, FOCS'05: Proceedings of the 46th IEEE Symposium on Foundations of Computer Science, pp. 469–478, 2005.

2 Andrew M. Childs, Wim van Dam, *Quantum Algorithms for Algebraic Problems*, Reviews of Modern Physics, **82**(1):1–52, 2010.

3 Mark Ettinger, Peter Høyer, *On quantum algorithms for noncommutative hidden subgroups*, Advances in Applied Mathematics, 25(3):239–251, 2000.

4 Demerson N. Gonçalves, Renato Portugal, Carlos M. M. Cosme, *Solutions to the hidden subgroup problem on some metacyclic groups*, 4th Workshop on Theory of Quantum Computation, Communication, and Cryptography, Lecture Notes in Computer Science, Vol. 5906, pp. 1–9, Springer, 2009.

5 Demerson N. Gonçalves, Renato Portugal, *Solution to the Hidden Subgroup Problem for a Class of Noncommutative Groups*, arXiv:1104.1361, 2011.

6 Yoshifumi Inui, François Le Gall, *An efficient quantum algorithm for the hidden subgroup problem over a class of semi-direct product groups*, Quantum Information and Computation, **7**(5&6):559–570, 2007.

7 A. Yu. Kitaev, *Quantum measurements and the Abelian Stabilizer Problem*, arXiv:quant-ph/9511026, 1995.

8 Peter W. Shor, *Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer*, SIAM Journal on Computing, **26**(5):1484–1509, 1997.

9 Daniel R. Simon, *On the power of quantum computation*, SIAM Journal on Computing, **26**:116–123, 1994.