Invited Paper

Dihedral Hidden Subgroup Problem: A Survey

Hirotada Kobayashi† and François Le Gall††,†††

After Shor's discovery of an efficient quantum algorithm for integer factoring, hidden subgroup problems play a central role in developing efficient quantum algorithms. In spite of many intensive studies, no efficient quantum algorithms are known for hidden subgroup problems for many non-Abelian groups. Of particular interest are the hidden subgroup problems for the symmetric group and for the dihedral group, because an efficient algorithm for the former implies an efficient solution to the graph isomorphism problem, and that for the latter essentially solves a certain lattice-related problem whose hardness is assumed in cryptography. This paper focuses on the latter case and gives a comprehensive survey of known facts related to the dihedral hidden subgroup problem.

1. Introduction

The *hidden subgroup problem* (*HSP*) nicely captures the structure of problems for which quantum computers can (or may be able to) significantly outperform classical computers. Besides the integer factoring and discrete logarithm problems for which celebrated quantum algorithms were presented by Shor [23], most of the problems having efficient quantum algorithms can be rephrased in terms of HSPs. Typical examples are Simon's order finding problem [24] and Kitaev's Abelian stabilizer problem [13]. Although HSPs are usually discussed for finite groups, Pell's equation problem, one of the oldest studied problem in number theory for which Hallgren [9] gave an efficient quantum algorithm, may also be viewed as an HSP for the infinite group $\mathbb{R}$.

All of the problems mentioned so far can be treated as HSPs for some Abelian groups. In fact, HSPs for all (finite) Abelian groups are known to have efficient quantum algorithms, which is essentially due to Kitaev [13] who gave an efficient construction of quantum Fourier transformations over Abelian groups. For HSPs for most of non-Abelian groups, however, it is unclear if they are tractable by quantum computers. Two important cases remaining open are HSPs for the *symmetric group* and *dihedral group*, since the graph isomorphism problem is reducible to the former [3),4)] and a certain lattice problem which is important in cryptography is reducible to the problem of solving the latter via some standard approach [21]. This paper concentrates on the latter and tries to give a comprehensive survey of known facts related to the *dihedral hidden subgroup problem* (*DHSP*).

This paper is organized as follows. After formally defining the hidden subgroup problem, and in particular, the dihedral hidden subgroup problem in Section 2, we start in Section 3 with the connection between lattice problems and the DHSP pointed out by Regev [21]. This gives a strong motivation to study algorithms for the DHSP. Section 4 revisits two quantum algorithms for the DHSP. The first is the subexponential-time quantum algorithm due to Kuperberg [14], which is the current fastest algorithm for the DHSP. The second is the algorithm due to Regev [22]. This algorithm still requires subexponential time, and is slightly slower than Kuperberg's actually, but runs in polynomial space, which is in contrast to that Kuperberg's algorithm requires subexponential space. Section 5 reviews a latest result by Bacon, Childs, and van Dam [2] that shows an optimal measurement for the DHSP. For HSPs for some non-Abelian groups closely related to the dihedral group, efficient quantum algorithms have been known already. Friedl, Ivanyos, Magniez, Santha, and Sen [7] gave an efficient quantum algorithm for the HSP for the semidirect product group $\mathbb{Z}_{p^r}^n \rtimes \mathbb{Z}_2$ with p a fixed odd prime. Moore, Rockmore, Russell, and Schul-

† Foundations of Information Research Division, National Institute of Informatics.
The earlier draft of this paper was written while at the Quantum Computation and Information Project, Exploratory Research for Advanced Study, Japan Science and Technology Agency.
†† Department of Computer Science, Graduate School of Information Science and Technology, The University of Tokyo.
††† Quantum Computation and Information Project, Exploratory Research for Advanced Study, Japan Science and Technology Agency.

man [15] solved the case of the q-hedral group. Very recently, the case of the semidirect product group $\mathbb{Z}_{p^r} \rtimes \mathbb{Z}_p$ with p a prime has also been settled by Inui and Le Gall [11]. Such results are summarized in Section 6. Finally, we conclude with Section 7 by mentioning some future directions.

2. Preliminaries

We start with reviewing several fundamental notions used in this paper. Let $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Z}^+$, and $\mathbb{R}$ denote the sets of natural numbers, integers, nonnegative integers, and real numbers, respectively. For $n \in \mathbb{N}$, $\mathbb{Z}_n$ denotes the set of all nonnegative integers less than n. Furthermore, for $m, n \in \mathbb{Z}$ satisfying $m < n$, $\mathbb{Z}_{[m,n]}$ denotes the set of all integers at least m and at most n. Throughout this paper it is assumed that all groups discussed are finite. The unit element of a group G is denoted by 1_G.

For a subgroup H of a group G and every group element $g \in G$, the *left coset* and *right coset* of H determined by g are the sets $gH = \{gh \mid h \in H\}$ and $Hg = \{hg \mid h \in H\}$, respectively. In this paper we simply say a coset to mention a left coset. For a finite set X, a function $f\colon G \to X$ is *H-periodic* if, for all $g_1, g_2 \in G$, $f(g_1) = f(g_2)$ if and only if g_1 and g_2 are in the same coset of H.

Now we are ready to define the *hidden subgroup problem* (*HSP*).

Definition 1 Given a generating set of a group G and a black box that computes a function f that is promised to be H-periodic for some unknown subgroup H of G, the hidden subgroup problem (HSP) is the problem of finding a generating set of H.

The complexity of the HSP is discussed with respect to $\log(|G|)$, because only the generating set of G is given as input.

The *dihedral group* D_N of order $2N$ is the set
$$\{x, y \mid x^N = y^2 = yxyx = 1_{D_N}\}.$$
This is the set of the N reflections and the N rotations that leaves the regular N-gon invariant, and the group is in fact generated by the reflection y and the rotation x of angle $\frac{2\pi}{N}$. Algebraically it is denoted by the semidirect product $D_N \cong \mathbb{Z}_N \rtimes \mathbb{Z}_2$. Each element of D_N can be represented of the form $y^s x^t$ for some $s \in \mathbb{Z}_2$ and $t \in \mathbb{Z}_N$.

Definition 2 The dihedral hidden subgroup problem (DHSP) is an HSP in which the underlying group G is dihedral.

One established method to solve HSPs is the *coset sampling*, which is often referred to as the "standard method". In the coset sampling, we first prepare the uniform superposition of all the elements of the underlying group G, and then evaluate the function f to have the state
$$|\phi\rangle = \frac{1}{\sqrt{|G|}} \sum_{g \in G} |g\rangle |f(g)\rangle.$$
Now we measure the second register of $|\phi\rangle$. If this results in, say, $f(g_0)$, then we have obtained the state
$$\frac{1}{\sqrt{|H|}} \sum_{h \in H} |g_0 h\rangle$$
in the first register, which is the uniform superposition of all the elements of the coset $g_0 H$. This procedure is repeated many times until sufficiently many samples are obtained. Thus, the HSP is reduced to the problem of finding H from these coset samples.

In the case of the DHSP, Ettinger and Høyer [5] proved that it is sufficient for the DHSP to solve the case where the hidden subgroup is of the form $\langle yx^d \rangle$. Note that each element $y^s x^t$ of D_N may be represented as (s, t) for $s \in \mathbb{Z}_2$ and $t \in \mathbb{Z}_N$. Therefore, the DHSP is reduced to the following *dihedral coset problem* (*DCP*).

Definition 3 For $N \in \mathbb{N}$, let $d \in \mathbb{Z}_N$ be an unknown constant. Given a black box that chooses $t \in \mathbb{Z}_N$ arbitrarily and outputs a pure quantum state
$$\frac{1}{\sqrt{2}}(|0, t\rangle + |1, (t + d) \bmod N\rangle)$$
of $(1 + \lceil \log N \rceil)$ qubits, the dihedral coset problem (DCP) is the problem of finding d by using this black box.

The complexity of algorithms for the DCP is discussed with respect to $\log N$. We say that the DCP has an efficient algorithm if it runs in time polynomial and solves the problem with some noticeable probability. The result by Ettinger and Høyer [5] implies that linearly many samples from the black box are sufficient to solve the DCP, although their method requires exponential time to find the solution from these samples. Ettinger, Høyer, and Knill [6] generalized this by showing that polynomially many coset states are sufficient to solve the HSP for any finite group.

3. Relation to Lattice Problems

Besides the fact that the dihedral group is a

non-Abelian group having a simple expression, perhaps the primal reason why the DHSP is so intensively studied among other non-Abelian HSPs would be that it is closely related to certain lattice problems whose hardness is assumed in some cryptographic systems. Indeed, lattice-based cryptosystems are one of the most likely candidates that may replace RSA or other factoring- or discrete-log-based ones, which are no longer secure against adversaries using quantum computers.

A *lattice* of dimension n is a set of all integer linear combinations of n linearly independent vectors in $\mathbb{R}^n$. These n linearly independent vectors form a *basis* of the lattice. The *shortest vector problem* (*SVP*) in a lattice is a natural problem of finding the shortest nonzero vector in the lattice, or in other words, of finding the lattice point closest to the origin.

Definition 4 Given a basis of a lattice, the shortest vector problem (SVP) is the problem of finding the shortest nonzero vector in the lattice.

For cryptographic use, we often consider a special version of the SVP having additional promises, which is called the $f(n)$-*unique shortest vector problem* ($f(n)$-*uSVP*).

Definition 5 Let $f\colon \mathbb{Z}^+ \to \mathbb{R}$ be a function. The $f(n)$-unique shortest vector problem ($f(n)$-uSVP) is the SVP in which the given lattice of dimension n is promised to have the unique shortest nonzero vector whose length is shorter at least by a factor of $f(n)$ than all the other nonparallel vectors.

For instance, the cryptosystem by Ajtai and Dwork [1] is based on the hardness of the $O(n^8)$-uSVP (and that of the $O(n^7)$-uSVP in its modified version [8]) and the one recently proposed by Regev [20] is based on that of the $O(n^{\frac{3}{2}})$-uSVP ☆.

Regev [21] showed that the DHSP is closely related to the $f(n)$-uSVP. Loosely speaking, what he proved is that an efficient algorithm for the DCP could be used to efficiently solve the $f(n)$-uSVP for *some* polynomially bounded function f. This essentially implies that if the DHSP is efficiently solvable using the "standard method" of coset sampling, the $f(n)$-uSVP has efficient algorithms for some polynomially bounded function f. The following *two-point problem* is the key to connect the DCP and the uSVP.

Definition 6 For $N, n \in \mathbb{N}$, let a vector $\boldsymbol{d} \in \mathbb{Z}^n_{[-(N-1),N-1]}$ be unknown but fixed. Given a black box that chooses $\boldsymbol{t} \in \mathbb{Z}^n_N$ arbitrarily such that $\boldsymbol{t} + \boldsymbol{d} \in \mathbb{Z}^n_N$ and outputs a pure quantum state

$$\frac{1}{\sqrt{2}}(|0, \boldsymbol{t}\rangle + |1, \boldsymbol{t} + \boldsymbol{d}\rangle)$$

of $(1 + n\lceil \log N \rceil)$ qubits, the two-point problem is the problem of finding $\boldsymbol{d}$ by using this black box.

The complexity of algorithms for the two-point problem is discussed with respect to $n \log N$. The concept of efficient algorithms is defined in a manner similar to the case of the DCP.

It is not so hard to see that this two-point problem is reducible to the DCP. The harder part is the reduction from the uSVP to the two-point problem. Given a basis of a lattice of the $f(n)$-uSVP to solve, we take some space large enough and create a superposition of many lattice points in this space. Then we partition the space into small regions of some appropriate size so that at most two lattice points are inside the same region. It is easy to compute which region each lattice point belongs to, and thus, by measuring the information of the region we can obtain a superposition of at most two lattice points that belong to the measured region. Using this idea, Regev showed that the $f(n)$-uSVP is quantumly reducible (in a truth-table-like manner) to (a modified version of) the two-point problem.

More precisely, consider some modified versions of the DCP and two-point problem: the *dihedral coset problem with failure parameter* δ (δ-*DCP*) and *two-point problem with failure parameter* δ in which now only a certain imperfect black box is given instead of the ideal black box in their original definitions.

Definition 7 For $N \in \mathbb{N}$, let $d \in \mathbb{Z}_N$ be an unknown constant. For a positive real number δ, the dihedral coset problem with failure parameter δ (δ-DCP) is the DCP of finding d in which the given black box works well with probability at least $1 - \frac{1}{(\log N)^\delta}$ and otherwise outputs a state $|s, t\rangle$ by choosing $s \in \mathbb{Z}_2$ and

☆ It does not mean that efficient algorithms for the underlying lattice problems can break these cryptosystems; here it is claimed that breaking them is *at least* as hard as such lattice problems. This is in contrast to the case of RSA in which breaking the cryptosystem is *at most* as hard as factoring integers. As for the upper bound for the Ajtai-Dwork cryptosystem, it is known that an efficient $n^{\frac{4}{3}}$-approximating algorithm for the closest vector problem (CVP) could be used to break it [19].

$t \in \mathbb{Z}_N$ arbitrarily.

Definition 8 For $N, n \in \mathbb{N}$, let a vector $\boldsymbol{d} \in \mathbb{Z}^n_{[-(N-1),N-1]}$ be unknown but fixed. For a positive real number δ, the two-point problem with failure parameter δ is the two-point problem of finding $\boldsymbol{d}$ in which the given black box works well with probability at least $1 - \frac{1}{(n \log 2N)^\delta}$ and otherwise outputs a state $|s, \boldsymbol{t}\rangle$ by choosing $s \in \mathbb{Z}_2$ and $\boldsymbol{t} \in \mathbb{Z}^n_N$ arbitrarily.

The concepts of efficient algorithms for these two problems are defined in a manner similar to the cases of the original DCP and two-point problem. Using these problems, Regev [21] proved the following statement, which is actually a stronger claim than what has been mentioned above.

Theorem 9 Let δ be a positive real number. If the δ-DCP has an efficient algorithm, then there exists a polynomial-time quantum algorithm that solves the $\Theta(n^{\frac{1}{2}+2\delta})$-uSVP with high probability.

4. Quantum Algorithms for DHSP

We now present two quantum algorithms for the DHSP, both of which are subexponential-time algorithms. The first one is the $2^{O(\sqrt{\log N})}$-time algorithm due to Kuperberg [14], where N is the parameter specifying that the underlying dihedral group is D_N. Although this is the current fastest algorithm for the DHSP, it unfortunately requires $2^{O(\sqrt{\log N})}$ quantum space. The second algorithm due to Regev [22] modifies Kuperberg's algorithm to a polynomial-space one at the cost of slight slow-down with time complexity.

4.1 Kuperberg's Algorithm

The key element for Kuperberg's algorithm is the Sample Creation Procedure described in **Fig. 1**.

In the case of f hiding the subgroup $H = \{(0,0), (1,d)\}$ of D_N, the first two steps of the Sample Creation Procedure are essentially the dihedral coset sampling, and we obtain a state of the form

$$\frac{1}{\sqrt{2}}(|0\rangle|t\rangle + |1\rangle|(t+d) \bmod N\rangle),$$

where t is chosen from $\mathbb{Z}_N$ uniformly at random.

Now at the end of Step 3, if the measurement outcome is k chosen from $\mathbb{Z}_N$ uniformly at random, the qubit in the first register collapses to the state (up to a phase)

$$|\psi_k^{d,N}\rangle = \frac{1}{\sqrt{2}}(|0\rangle + e^{2\pi i \frac{kd}{N}}|1\rangle),$$

Sample Creation Procedure over D_N

Input: an integer N and a black box that computes a function $f\colon \mathbb{Z}_2 \times \mathbb{Z}_N \to X$, where X is some finite set

Output: a one-qubit quantum state

1. Prepare the state
$$\frac{1}{\sqrt{2N}} \sum_{s=0}^{1} \sum_{t=0}^{n} |s\rangle|t\rangle|f(s,t)\rangle.$$
2. Measure the third register.
3. Apply the quantum Fourier transformation over $\mathbb{Z}_N$
$$|j\rangle \mapsto \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2\pi i \frac{jk}{N}}|k\rangle$$
to the second register and measure it.
4. Output the first register.

Fig. 1 The sample creation procedure.

which is the output of the Sample Creation Procedure. Notice that, when the state $|\psi_k^{d,N}\rangle$ is obtained, the values of k and N are already known and only d is unknown. We now show how to find d using such samples.

4.1.1 Case of N a Power of Two

We first consider the easier case where $N = 2^n$. In this case, the problem of finding d is easily reduced to the problem of finding the parity b of d. To see this, suppose that, given N and a black box that computes an H-periodic f, we have an algorithm that finds b with high probability, where $H = \{(0,0), (1,d)\}$ is the hidden subgroup to find. We can thus write $d = 2d' + b$ where b is known. Define a function $f'\colon \mathbb{Z}_2 \times \mathbb{Z}_{\frac{N}{2}} \to X$ as $f'(s,t) = f(s, 2t+b)$. Then this f' is H'-periodic where $H' = \{(0,0), (1,d')\}$ is a subgroup of $D_{\frac{N}{2}}$. Therefore, the parity of d' can be found with high probability, and all the bits of d can be computed with high probability by repeating the same procedure.

We thus have only to show how to find the parity of d. The point is the following observation. If we could obtain $|\psi_{2^{n-1}}^{d,N}\rangle = \frac{1}{\sqrt{2}}(|0\rangle + e^{\pi i d}|1\rangle)$, it is easy to know the parity of d by applying the Hadamard transformation. However, the probability of obtaining this state from the Sample Creation Procedure is $\frac{1}{N}$, which is exponentially small. Kuperberg settled this by using a sieve method to obtain the state $|\psi_{2^{n-1}}^{d,N}\rangle$ in subexponential time.

The key construction is as follows. For two samples $|\psi_k^{d,N}\rangle$ and $|\psi_l^{d,N}\rangle$, the product state $|\psi_k^{d,N}\rangle \otimes |\psi_l^{d,N}\rangle$ can be rewritten as

$$\frac{1}{2}(|00\rangle + e^{2\pi i \frac{ld}{N}}|01\rangle + e^{2\pi i \frac{kd}{N}}|10\rangle + e^{2\pi i \frac{(k+l)d}{N}}|11\rangle).$$

Therefore, applying CNOT using the first qubit as the control qubit yields the state

$$\frac{1}{2}(|00\rangle + e^{2\pi i \frac{ld}{N}}|01\rangle + e^{2\pi i \frac{(k+l)d}{N}}|10\rangle + e^{2\pi i \frac{kd}{N}}|11\rangle).$$

Now, measuring the second qubit in the $\{|0\rangle, |1\rangle\}$ basis gives, up to a phase, either the state $|\psi_{k+l}^{d,N}\rangle$ with probability 1/2 or the state $|\psi_{k-l}^{d,N}\rangle$ with probability 1/2. Moreover, we can know which of the two states has been obtained from the outcome of the measurement.

Now the sieve algorithm starts with $2^{\Theta(\sqrt{n})}$ samples of the form $|\psi_k^{d,N}\rangle$ with k uniformly distributed over $\mathbb{Z}_N$. Denote this set of states by L_0. The sieve algorithm will find all the pairs $|\psi_{k_1}^{d,N}\rangle$ and $|\psi_{k_2}^{d,N}\rangle$ such that the last $m = \lceil \sqrt{n-1} \rceil$ bits of k_1 and k_2 are identical. Then, for each of these pairs, use the previous procedure to generate, with probability 1/2, the state $|\psi_{k_1-k_2}^{d,N}\rangle$. Denote the set of all these states by L_1. The point is that all the states in L_1 are of the form $|\psi_k^{d,N}\rangle$ such that the m trailing bits of k are all zeros. By repeating the procedure m times, we obtain a set L_m of states of the form $|\psi_k^{d,N}\rangle$ such that k has $n-1$ trailing zeros. Now the only possibilities are $k = 0$ and $k = 2^{n-1}$.

We have just to show that, with high probability, the final set contains at least one state of the form $|\psi_{2^{n-1}}^{d,N}\rangle$. Intuitively, this is because, if $|L_j| \gg 2^{\Theta(\sqrt{n})}$ for $0 \le j \le m$, then almost all states in L_j can be used to form a pair $(|\psi_{k_1}^{d,N}\rangle, |\psi_{k_2}^{d,N}\rangle)$ such that $k_1 - k_2$ is divisible by 2^{jm}. Thus $|L_{j+1}|/|L_j| \approx 1/4$. A precise analysis shows that taking $|L_0| = 2^{\Theta(\sqrt{n})}$ is indeed sufficient to obtain, with high probability, a set L_m that contains at least one sample of $|\psi_{2^{n-1}}^{d,N}\rangle$.

4.1.2 Case of General N

Now consider the case of general N, and write $N = 2^l N'$ with N' odd. Then the last l bits of d can be determined as before. Moreover, by denoting $d = 2^l d' + r$ we can do as above to obtain states of the form $|\psi_k^{d',N'}\rangle$. Thus we have only to consider the case where N is odd.

The idea is to create all the states $|\psi_{2^j}^{d,N}\rangle$ for $0 \le j \le \log N$. Then the well-known phase estimation algorithm enables us to find d with high probability.

First, we explain how to obtain the state $|\psi_1^{d,N}\rangle$. Once again write $m = \lceil \sqrt{\log N - 2} \rceil$. We start with the set L_0 of $2^{\Theta(\sqrt{N})}$ samples of the form $|\psi_k^{d,N}\rangle$ randomly generated by the Sample Creation Procedure. Then divide the set into pairs of $|\psi_{k_1}^{d,N}\rangle$ and $|\psi_{k_2}^{d,N}\rangle$ satisfying $k_1 - k_2 \le 2^{m^2-m+1}$. The set L_1 now consists of the states of the form $|\psi_{k_1-k_2}^{d,N}\rangle$. We repeat this m times. At the jth step, the set L_j contains the states of the form $|\psi_k^{d,N}\rangle$ with $0 \le k < 2^{m^2-mj+1}$. Now the states $|\psi_{k_1}^{d,N}\rangle$ and $|\psi_{k_2}^{d,N}\rangle$ in L_j satisfying $k_1 - k_2 \le 2^{m^2-m(j+1)+1}$ are coupled to form the states in the set L_{j+1}. Then, each state in the final set L_m must be either $|\psi_0^{d,N}\rangle$ or $|\psi_1^{d,N}\rangle$, and it can be proved that, with high probability, L_m contains at least one sample of $|\psi_1^{d,N}\rangle$.

Now, for $1 \le q \le \log N$, define the function $f^{(q)} : \mathbb{Z}_2 \times \mathbb{Z}_N \to X$ as $f^{(q)}(s,t) = f(2^q s, t)$. Using the Sample Creation Procedure with the integer N and the black box that computes $f^{(q)}$, we obtain samples of the form $|\psi_k^{2^q d,N}\rangle$. Then, using the method described above yields the state $|\psi_{2^q}^{d,N}\rangle$ with high probability. From the collection of the states $\{|\psi_{2^q}^{d,N}\rangle\}_{q=0}^{\lceil \log N \rceil}$ we can recover d with high probability by applying the phase estimation algorithm.

Theorem 10 There is a quantum algorithm that solves the hidden subgroup problem for the dihedral group D_N with high probability in $2^{O(\sqrt{\log N})}$ time.

4.2 Polynomial-Space Algorithm

Kuperberg's algorithm described in the last subsection needs to store a subexponential number of samples to create the final set with sufficiently high success probability. Regev [22] modified the algorithm so that it runs only in polynomial space.

The idea is to work online, i.e., not to wait to proceed the step for creating the states in the set L_{j+1} until having obtained all the states in the set L_j, but to create the states in the set L_{j+1} as soon as possible, keeping only a polynomial number of samples at a time. With the pairing method of the original Kuperberg's algorithm, however, it is not possible to make it online with a good success probability. Regev [22] showed another way of pairing that can be performed in an online manner. The running time of Regev's algorithm is only slightly slower than Kuperberg's algo-

rithm, namely $2^{O(\sqrt{\log N \log\log N})}$.

Theorem 11 There is a quantum algorithm that solves the hidden subgroup problem for the dihedral group D_N with high probability in $2^{O(\sqrt{\log N \log\log N})}$ time and $O(\log N)$ space.

5. Optimal Measurement for DHSP

In the previous section, we have seen that the DHSP can be solved in polynomial space using a subexponential number of samples created by the Sample Creation Procedure. More precisely, we have seen that the DCP can be solved in polynomial space using a subexponential number of samples from the black box. On the other hand, Ettinger and Høyer [5] proved that a linear number of such samples are sufficient to solve the DCP, although their method requires a post-processing of exponential time. Now a natural question is if there is an algorithm that solves the DCP using a sublinear number of such samples.

Very recently Bacon, Childs, and van Dam [2] negatively answered this question by using the framework of quantum information theory. That is, no quantum algorithm can solve the DCP with high probability with only using sublinear number of samples from the black box. Actually, they succeeded in characterizing the optimal measurement for the DCP, that is, the joint measurement of the samples from the black box that solves the problem with the highest probability, assuming that the DCP instances are uniformly distributed.

Consider the mixed state

$$\rho_d = \frac{1}{N}\sum_{k=0}^{N-1}(|\psi_k^{d,N}\rangle\langle\psi_k^{d,N}| \otimes |k\rangle\langle k|),$$

which is the state just after Step 3 of the Sample Creation Procedure, and let $A = \sum_{j=0}^{N-1}\rho_j^{\otimes m}$. Then the argument using quantum information theory shows that the optimal positive operator-valued measure (POVM) identifying the solution d from $\rho_d^{\otimes m}$ is the so-called "pretty good measurement" [10] $\{E_j\}_{j=0}^{N-1}$ where

$$E_j = A^{-\frac{1}{2}}\rho_j^{\otimes m}A^{-\frac{1}{2}}$$

corresponds to the decision that the solution would be j.

It turns out that the probability that this measurement correctly answers the solution d is exponentially small if $\frac{m}{\log N} \le c$ for any constant $c < 1$. Thus we have the following theorem.

Theorem 12 No quantum algorithm can solve the DCP with high probability with only using sublinear number of samples from the black box.

Moore and Russell [16] extended this result and proved that the pretty good measurement defined above is optimal for the HSP for any group G if G and its hidden subgroup H forms a so-called Gel'fand pair.

6. Efficiently Solvable Non-Abelian HSPs

The dihedral group is an instance of the semidirect product groups. Although no efficient quantum algorithm is known for the DHSP, there are some semidirect product groups for which the HSP is efficiently solvable. Actually, the notion of semidirect products is not uniquely defined, and the one used in the definition of the dihedral group is only one example of them. For instance, Friedl, Ivanyos, Magniez, Santha, and Sen [7] gave a quantum algorithm for the HSP for the group $\mathbb{Z}_{p^r}^n \rtimes \mathbb{Z}_2$, for a definition of the semi-direct product that generalizes the product of the dihedral group, that runs in time polynomial in n when p is an odd prime. More general definition of the semidirect product groups is as follows.

Definition 13 Given two integers n and q and a homomorphism ϕ from $\mathbb{Z}_n$ to the group of automorphisms of $\mathbb{Z}_q$, the semidirect product group $\mathbb{Z}_n \rtimes_\phi \mathbb{Z}_q$ is the group generated by x and y satisfying $x^n = y^q = 1_{\mathbb{Z}_n \rtimes_\phi \mathbb{Z}_q}$ and $yx = x^{\phi(1)(1)}y$.

However, for arbitrary n and q, the uniqueness of the homomorphism ϕ is not guaranteed. In the case of n a power of a prime and q a prime, Inui and Le Gall [11] classified the semidirect groups into five classes.

Theorem 14 The semi-direct product groups $\mathbb{Z}_{p^r} \rtimes_\phi \mathbb{Z}_q$ for p and q primes and r an integer are exactly the groups of the following five classes.

Class 1. The direct product groups $\mathbb{Z}_{p^r} \times \mathbb{Z}_q$.

Class 2. The q-hedral groups defined for p, q, and r such that $r \ge 1$ and $q|(p-1)$, which are groups G generated by x and y satisfying $x^{p^r} = y^q = 1_G$ and $yx = x^\gamma y$ with γ verifying $\gamma^q \equiv 1 \mod p$.

Class 3. The dihedral groups D_{2^r} for $r > 2$, which are groups generated by x and y satisfying $x^{2^r} = y^2 = 1_{D_{2^r}}$ and $yx = x^{2^r-1}y$.

Class 4. The quasi-dihedral groups quasi-D_{2^r} for $r > 2$, which are groups generated by x and y satisfying $x^{2^r} = y^2 = 1_{\text{quasi-}D_{2^r}}$ and

$yx = x^{2^{r-1}-1}y$.

Class 5. The groups $P_{p,r}$ for $r \geq 2$, which are groups generated by x and y satisfying $x^{p^r} = y^p = 1_{P_{p,r}}$ and $yx = x^{p^{r-1}+1}y$.

Thus there are three non-isomorphic groups $\mathbb{Z}_{2^r} \rtimes_\phi \mathbb{Z}_2$, depending on the definition of ϕ: D_{2^r}, quasi-D_{2^r}, and $P_{2,r}$. It is usual to use the symbol $\rtimes$ when there is no ambiguity on which definition of ϕ we use.

Moore, Rockmore, Russell, and Schulman [15] considered the q-hedral groups in Class 2 with $r = 1$ and presented a polynomial-time quantum algorithm that solves the HSPs for them when q is sufficiently large with respect to p. Their algorithm uses the so-called strong Fourier sampling, which requires Fourier transformations over non-Abelian groups. By using a good basis for the representations of $\mathbb{Z}_p \rtimes \mathbb{Z}_q$, it is possible to reconstruct the hidden subgroup in polynomial time. More precisely, they obtained the following result.

Theorem 15 For any primes p and q such that $q|(p-1)$ and $q = \Omega\left(\frac{p}{\log^c p}\right)$ for some constant c, there exists a quantum algorithm that solves the HSP over the group $\mathbb{Z}_p \rtimes \mathbb{Z}_q$ in polynomial time.

Inui and Le Gall [11] studied the HSP for the groups $P_{p,r}$ of Class 5. The main property of these groups is that the number of subgroups is relatively small: they are of the form $\langle x^{p^j} \rangle$ for $0 \leq j \leq r$, $\langle x^{p^j}, y \rangle$ for $0 \leq j \leq r$, or $\langle x^{tp^j} y \rangle$ for $0 \leq j < r$ and $1 \leq t < p$. However, checking all the possibilities requires $\Omega(p + r)$ time, which is exponentially large compared to the input size when, for example, r is constant. Inui and Le Gall succeeded in designing a polynomial-time quantum algorithm that solves the HSPs for such groups by using the algebraic structure of the subgroups. More precisely, they obtained the following result.

Theorem 16 There exists a quantum algorithm that solves the HSP over the group $P_{p,r}$ in time $O(\log r + \log^2 p)$.

7. Concluding Remarks

This paper reviewed almost all the results known about the dihedral hidden subgroup problem. In spite of many studies for nearly a decade, the central question of whether the DHSP has efficient quantum algorithms still remains open. It would not be a kind of "unexpected", however, even if the DHSP were efficiently solvable. Compared to the HSP for the symmetric group for which a number of negative observations [12),17),18)] are known, it seems that most of the results known about the DHSP so far are positive ones. Thus we may hope the DHSP leads to another triumph of quantum computing. On the other hand, the hardness of the DHSP may be useful to give stronger security proofs for some lattice-based cryptosystems. Hence, even negative results may not be so disappointing in the case of the DHSP. The studies on the HSPs appear to be entering another ripening period in these years. The authors hope significant progresses will be achieved on the DHSP and its related problems in the not too distant future.

References

1) Ajtai, M. and Dwork, C.: A Public-Key Cryptosystem with Worst-Case/Average-Case Equivalence, *Proc. Twenty-Ninth Annual ACM Symposium on Theory of Computing*, pp.284–293 (1997).
2) Bacon, D., Childs, A.M. and van Dam, W.: Optimal measurements for the dihedral hidden subgroup problem (2005). arXiv.org e-Print archive, quant-ph/0501044.
3) Beals, R.M.: Quantum computation of Fourier transforms over symmetric groups, *Proc. Twenty-Ninth Annual ACM Symposium on Theory of Computing*, pp.48–53 (1997).
4) Boneh, D. and Lipton, R.J.: Quantum Cryptanalysis of Hidden Linear Functions (Extended Abstract), *Advances in Cryptology—CRYPTO '95, 15th Annual International Cryptology Conference*, Lecture Notes in Computer Science, Vol.963, pp.424–437 (1995).
5) Ettinger, J.M. and Høyer, P.: On Quantum Algorithms for Noncommutative Hidden Subgroups, *Advances in Applied Mathematics*, Vol.25, No.3, pp.239–251 (2000).
6) Ettinger, J.M., Høyer, P. and Knill, E.H.: The quantum query complexity of the hidden subgroup problem is polynomial, *Information Processing Letters*, Vol.91, No.1, pp.43–48 (2004).
7) Friedl, K., Ivanyos, G., Magniez, F., Santha, M. and Sen, P.: Hidden Translation and Orbit Coset in Quantum Computing, *Proc. 35th Annual ACM Symposium on Theory of Computing*, pp.1–9 (2003).
8) Goldreich, O., Goldwasser, S. and Halevi, S.: Eliminating Decryption Errors in the Ajtai-Dwork Cryptosystem, *Advances in Cryptology—CRYPTO '97, 17th Annual International Cryptology Conference*, Lecture Notes in Computer Science, Vol.1294, pp.105–111 (1997).

9) Hallgren, S.J.: Polynomial-Time Quantum Algorithms for Pell's Equation and the Principal Ideal Problem, *Proc. 34th Annual ACM Symposium on Theory of Computing*, pp.653–658 (2002).
10) Hausladen, P. and Wootters, W.K.: A 'Pretty Good' Measurement for Distinguishing Quantum States, *Journal of Modern Optics*, Vol.41, No.12, pp.2385–2390 (1994).
11) Inui, Y. and Le Gall, F.: An Efficient Algorithm for the Hidden Subgroup Problem over a Class of Semi-direct Product Groups (2004). arXiv.org e-Print archive, quant-ph/0412033.
12) Kempe, J. and Shalev, A.: The hidden subgroup problem and permutation group theory, *Proc. Sixteenth Annual ACM-SIAM Symposium on Discrete Algorithms*, pp.1118–1125 (2005).
13) Kitaev, A.Yu.: Quantum measurement and the Abelian Stabilizer Problem (1995). arXiv.org e-Print archive, quant-ph/9511026.
14) Kuperberg, G.: A subexponential-time quantum algorithm for the dihedral hidden subgroup problem (2003). arXiv.org e-Print archive, quant-ph/0302112.
15) Moore, C., Rockmore, D., Russell, A. and Schulman, L.J.: The Power of Basis Selection in Fourier Sampling: Hidden Subgroup Problems in Affine Groups, *Proc. Fifteenth Annual ACM-SIAM Symposium on Discrete Algorithms*, pp.1113–1122 (2004).
16) Moore, C. and Russell, A.: For Distinguishing Conjugate Hidden Subgroups, the Pretty Good Measurement is as Good as it Gets (2005). arXiv.org e-Print archive, quant-ph/0501177.
17) Moore, C. and Russell, A.: The Symmetric Group Defies Strong Fourier Sampling: Part II (2005). arXiv.org e-Print archive, quant-ph/0501066.
18) Moore, C., Russell, A. and Schulman, L.J.: The Symmetric Group Defies Strong Fourier Sampling, *46th Annual Symposium on Foundations of Computer Science* (2005). To appear.
19) Nguyen, P.Q. and Stern, J.: Cryptanalysis of the Ajtai-Dwork Cryptosystem, *Advances in Cryptology—CRYPTO '98, 18th Annual International Cryptology Conference*, Lecture Notes in Computer Science, Vol.1462, pp.223–242 (1998).
20) Regev, O.: New Lattice-Based Cryptographic Constructions, *J. ACM*, Vol.51, No.6, pp.899–942 (2004).
21) Regev, O.: Quantum computation and lattice problems, *SIAM Journal on Computing*, Vol.33, No.3, pp.738–760 (2004).
22) Regev, O.: A Subexponential Time Algorithm for the Dihedral Hidden Subgroup Problem with Polynomial Space (2004). arXiv.org e-Print archive, quant-ph/0406151.
23) Shor, P.W.: Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer, *SIAM Journal on Computing*, Vol.26, No.5, pp.1484–1509 (1997).
24) Simon, D.R.: On the power of quantum computation, *SIAM Journal on Computing*, Vol.26, No.5, pp.1474–1483 (1997).

(Received February 18, 2005)
(Accepted July 4, 2005)
(Online version of this article can be found in the IPSJ Digital Courier, Vol.1, pp.470–477.)

Hirotada Kobayashi received his B.S., M.S. and Ph.D. in Information Science from the University of Tokyo, Japan, in 1997, 1999, and 2002, respectively. He was a researcher at the Quantum Computation and Information Project, Exploratory Research for Advanced Technology, Japan Science and Technology Agency during 2000–2005. He is currently with the Foundations of Informatics Research Division, the National Institute of Informatics. His research interests include quantum computing and computational complexity. He is a member of the ACM and IEEE.

François Le Gall is a Ph.D. student in the Departement of Computer Science of the University of Tokyo, and a technical assistant in the Quantum Computation and Information Project, Exploratory Research for Advanced Technology, Japan Science and Technology Agency. He has done his undergraduate studies at Ecole Centrale de Lyon, France, and received his M.S. degree from the University of Tokyo in 2003. His research interests focus on quantum algorithms and quantum communication complexity.