The Abelian Hidden Subgroup Problem

Laura Mancinska
(ID 20286922)

November 28, 2007

1 Introduction to Quantum Computing

1.1 What is Quantum Computing?

In order to understand how a quantum system behaves, first we will consider deterministic and probabilistic systems. There are two main questions we have to answer if we want to describe a system that does a computation:

1. What are the states of the system?
2. How does the system evolve from one state to another? (We will consider only systems that undergo discrete evolution.)

Deterministic computation

This is the simplest type of computation that also functions in the ordinary computers we are using every day. Each memory cell of the system can be either 0 or 1 and its state in the next time momentum depends on the present state of the whole memory (that is, all memory cells combined). So to answer previous two questions:

1. The state of the system is $[x]$, where $x \in \{0,1\}^n$
2. The evolution of the system is $f : \{0,1\}^n \to \{0,1\}^n$

Probabilistic computation

A probabilistic system is a generalization of a deterministic system. Each memory cell c of a probabilistic system is 0 with probability $p_{c,0}$ and 1 with probability $p_{c,1}$ such that $p_{c,0} + p_{c,1} = 1$. Therefore a state of the probabilistic system is a probability distribution over $\{0,1\}^n$ — states of the deterministic system. We allow evolutions that map each valid state of the system to another valid state of the system (i.e. evolutions that preserve L_1 norm).

1. The state of the system is a formal sum over $x \in \{0,1\}^n$:

$$\sum_x p_x[x],$$

where $\sum_x p_x = 1$ and $\forall x : p_x \geq 0$.

2. The evolution of the system is realized by a *stochastic* matrix $A = (a_{xy})$:

$$A : \sum_x p_x[x] \mapsto \sum_x q_x[x],$$

where $q_x = \sum_y a_{xy} p_y$.

Quantum computation

We can generalize our model of computation even further by allowing "probabilities" (we will call them *amplitudes*) to be complex numbers. Now the state of a memory cell c is 0 with amplitude $\alpha_{c,0}$, and 1 with amplitude $\alpha_{c,1}$ such that $|\alpha_{c,0}|^2 + |\alpha_{c,1}|^2 = 1$. As before we will allow evolutions that map each valid state of the system to another valid state of the system. In this case, these will be evolutions that preserve L_2 norm.

1. The state of the system is a is a formal sum (known as the *superposition*) over $x \in \{0,1\}^n$

$$\sum_x \alpha_x[x], \tag{1}$$

where $\sum_x |\alpha_x|^2 = 1$.

2. The evolution of the system is realized by a *unitary* matrix $U = (u_{xy})$:

$$U : \sum_x \alpha_x[x] \mapsto \sum_x \beta_x[x],$$

where $\beta_x = \sum_y u_{xy} \alpha_y$.

1.2 Dirac notation

In quantum computation there is a convention to write vectors inside angled brackets. Thus, the superposition (1) becomes

$$|\psi\rangle = \sum_x \alpha_x |x\rangle . \tag{2}$$

This is called the *Dirac (Bracket) notation*. One can think of $|\psi\rangle$ (called *ket* vector) as a column vector with components α_x. Its dual row vector is written as $\langle\psi|$ (called *bra* vector). The bra vector $\langle\psi|$ is obtained from $|\psi\rangle$ by taking its conjugate transpose, i.e., $\langle\psi| = |\psi\rangle^\dagger$. As one can easily imagine $\langle\psi|\phi\rangle$ stands for the inner product of vectors $|\psi\rangle$ and $|\phi\rangle$.

Example 1. It is common to denote the standard basis vectors of $\mathbb{C}^2$ as

$$\begin{pmatrix}1\\0\end{pmatrix} \equiv |0\rangle , \ \begin{pmatrix}0\\1\end{pmatrix} \equiv |1\rangle .$$

A *qubit* (quantum bit) is a superposition of $|0\rangle$ and $|1\rangle$. It is often used as a building block of quantum memory (compared to bit in deterministic computing). An instance of a valid qubit state is

$$|\psi\rangle = \frac{1}{\sqrt{2}} |0\rangle - \frac{i}{\sqrt{2}} |1\rangle \equiv \frac{1}{\sqrt{2}} \begin{pmatrix}1\\-i\end{pmatrix} .$$

The dual of $|\psi\rangle$ is

$$\langle\psi| = \frac{1}{\sqrt{2}}\langle 0| + \frac{i}{\sqrt{2}}\langle 1| \equiv \frac{1}{\sqrt{2}}\begin{pmatrix}1 & i\end{pmatrix}.$$

If we have two quantum systems in states $|\psi\rangle$ and $|\phi\rangle$ respectively then the state of the composite quantum system is $|\psi\rangle \otimes |\phi\rangle$. It is common to omit the tensor sign and write just $|\psi\rangle\,|\phi\rangle$.

Example 2. A two-qubit system is obtained by combining two one-qubit systems. A general two-qubit state is a normalized vector in vector space $\mathbb{C}^{2^2} = C$. In bracket notation the standard basis vectors would look as follows:

$$\begin{pmatrix}1\\0\\0\\0\end{pmatrix} = \begin{pmatrix}1\\0\end{pmatrix} \otimes \begin{pmatrix}1\\0\end{pmatrix} \equiv |0\rangle\,|0\rangle \equiv |00\rangle\,, \quad \begin{pmatrix}0\\1\\0\\0\end{pmatrix} = \begin{pmatrix}1\\0\end{pmatrix} \otimes \begin{pmatrix}0\\1\end{pmatrix} \equiv |0\rangle\,|1\rangle \equiv |01\rangle\,,$$

$$\begin{pmatrix}0\\0\\1\\0\end{pmatrix} = \begin{pmatrix}0\\1\end{pmatrix} \otimes \begin{pmatrix}1\\0\end{pmatrix} \equiv |1\rangle\,|0\rangle \equiv |10\rangle\,, \quad \begin{pmatrix}0\\0\\0\\1\end{pmatrix} = \begin{pmatrix}0\\1\end{pmatrix} \otimes \begin{pmatrix}0\\1\end{pmatrix} \equiv |1\rangle\,|1\rangle \equiv |11\rangle$$

It is now straightforward how to denote the standard basis vectors of $\mathbb{C}^{2^n}$ (n-qubit system).

Example 3. Let $G = \{g_1, g_2, g_3\}$ be a group. In a framework of the probabilistic computing it makes sense to consider the following state

$$s = \frac{1}{4}[g_1] + \frac{1}{4}[g_2] + \frac{1}{2}[g_3],$$

We take g_1 and g_2 with the probability $\frac{1}{4}$ each and g_2 with the probability $\frac{1}{2}$.

If we return to quantum computing we can consider quantum states that correspond to a superposition over group elements:

$$|\psi\rangle = \alpha_1\,|g_1\rangle + \alpha_2\,|g_2\rangle + \alpha_3\,|g_3\rangle$$

where $\alpha_1, \alpha_2, \alpha_3 \in \mathbb{C}$ and $|\alpha_1|^2 + |\alpha_2|^2 + |\alpha_3|^2 = 1$ and $|g_1\rangle\,, |g_2\rangle\,, |g_3\rangle$ serve as an orthonormal basis vectors.

1.3 Measurements

Although it may seem that quantum computation is very powerful, in turns that we can not obtain a complete description of the state of a quantum system. When we have finished the computation in order to read the result we must perform a *measurement* which is not a unitary evolution. In this essay we will use only *projective measurements*.

Definition. *Projective* or *von Neumann* measurement with respect to some given orthonormal basis $\mathcal{B} = \{|b_1\rangle\,, |b_2\rangle\,, \ldots, |b_n\rangle\}$ of the state space of some quantum system, when performed on a state

$$\psi = \sum_{i=1}^{n} \alpha_i\,|b_i\rangle$$

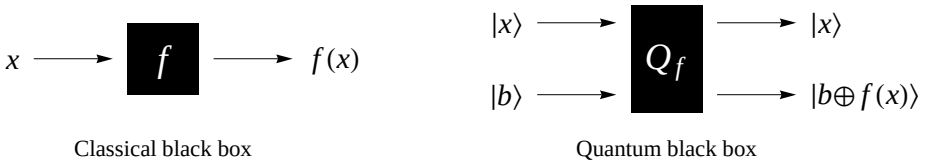

Figure 1: Black boxes for classical and quantum computing

(where $\sum_{i=1}^{n} |\alpha_i|^2 = 1$) gives i with probability $|\alpha_i|^2$ and leaves the system in a state $|b_i\rangle$.

Definition. Let $\mathcal{B} = \{|b_0\rangle, |b_1\rangle, \ldots, |b_n\rangle\}$ be an orthonormal basis of the state space of some quantum system and

$$|\psi\rangle = \sum_{i=1}^{n} \alpha_i |b_i\rangle, \text{ where} \sum_{i=1}^{n} |\alpha_i|^2 = 1$$

be a state of this system. If we perform a *projective* or *von Neumann* measurement on $|\psi\rangle$ with respect to basis $\mathcal{B}$, we get outcome i with probability $|\alpha_i|^2$ and the state of the system collapses to $|b_i\rangle$.

Example 4. Suppose we are given one of the following one-qubit quantum states

$$|\psi_+\rangle = \frac{1}{\sqrt{2}} |0\rangle + \frac{i}{\sqrt{2}} |1\rangle$$
$$|\psi_-\rangle = \frac{1}{\sqrt{2}} |0\rangle - \frac{i}{\sqrt{2}} |1\rangle$$

and we want to find out which one it is. In order to extract information from the state we have to measure it. Since $|\psi_+\rangle$ and $|\psi_-\rangle$ are orthogonal, it is possible to distinguish them perfectly, if we measure in $\mathcal{B} = \{|\psi_+\rangle, |\psi_-\rangle\}$. However, if we measured in $\mathcal{B} = \{|0\rangle, |1\rangle\}$, we would get 0 with probability 1/2 and 1 with probability 1/2 no matter which of the states $|\psi_+\rangle$ and $|\psi_-\rangle$ we were given. Hence, this would be a very bad choice of basis as we would not be able to distinguish between these two states. It turns out that we can perfectly distinguish two quantum states if and only if they are orthogonal (see [2] or [3]).

1.4 Quantum Black Box Model

First, let us consider black box model in the deterministic computation. A *black box* or an *oracle* is a resource that computes some unknown function $f : \{0,1\}^n \to \{0,1\}^m$. Note that we can think of an arbitrary finite set X as a subset of $\{0,1\}^n$ for some n, since we can encode each element of X into a binary string of length n. If we input some argument $[x]$ into a back box, it outputs $[f(x)]$ (see Fig. 1).

In the quantum case this does not work, because the input and the output may have different sizes, thus the corresponding operation clearly is not unitary. We can redefine the black box as follows: it transforms $|x\rangle |b\rangle$ to $|x\rangle |b \oplus f(x)\rangle$,

where "$\oplus$" denotes the addition modulo 2 (see Fig. 1). This operation is unitary, since it is a permutation of the basis states. Note that if we apply it twice, we get back the initial state $|x\rangle |b\rangle$, therefore it is self inverse. We will denote the corresponding unitary matrix by Q_f. Usually the goal of the algorithm which uses a black box Q_f is to determine some property of the function f with as few queries to the black box as possible. The *query complexity* of an algorithm is the number of queries it makes.

Example 5. Suppose we are given a quantum black box Q_f for computing function $f : \{0,1\} \to \{0,1\}$ such that $f(x) = \mathrm{NOT}(x)$, for all x. Then the black box acts on the basis states as follows:

$$Q_f |0\rangle |0\rangle = |0\rangle |0 \oplus f(0)\rangle = |0\rangle |0 \oplus 1\rangle = |0\rangle |1\rangle$$
$$Q_f |1\rangle |0\rangle = |1\rangle |0 \oplus f(1)\rangle = |1\rangle |0 \oplus 0\rangle = |1\rangle |0\rangle$$

If instead we input a superposition $|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle |0\rangle - |1\rangle |0\rangle)$, we get:

$$Q(f) |\psi\rangle = \frac{1}{\sqrt{2}} \Big(|0\rangle |0 \oplus f(0)\rangle - |1\rangle |0 \oplus f(1)\rangle \Big) = \frac{1}{\sqrt{2}} \Big(|0\rangle |1\rangle - |1\rangle |0\rangle \Big)$$

2 Hidden Subgroup Problem

2.1 The Problem

We are given a finitely generated group $(G, +)$ and a quantum black box computing a function $f : G \to X$ that maps elements of G to elements of some finite set X. Also, we know that the function f is constant and distinct on each of the cosets of some unknown subgroup H of G. The goal is to determine the subgroup H. This problem is called "hidden subgroup" since the function f "hides" the subgroup H.

In this essay we will consider the hidden subgroup problem (HSP) for the case when G is a finite Abelian group.

2.2 Quantum Fourier Transformation

In this section we will define the quantum Fourier transformation over an Abelian group G and prove that it is a unitary transformation.

Definition. *Quantum Fourier transformation* (QFT) over an Abelian group G is defined as a linear map that acts on basis vectors $|g\rangle$, $g \in G$ in the following way:

$$|g\rangle \mapsto \frac{1}{\sqrt{|G|}} \sum_{\psi \in \hat{G}} \psi(g) |\psi\rangle ,$$

where $\hat{G}$ is the set of irreducible representations of the group G. By linearity we can extend the definition of QFT to any superposition of the basis vectors. Note that we can think of $\{|g\rangle\}_{g \in G}$ and $\{|\psi\rangle\}_{\psi \in \hat{G}}$ as two orthonormal basis.

In order to use QFT in a quantum computation we have to show that it is a valid evolution of a quantum system.

Theorem 1. QFT is a unitary transformation.

First, let us list some theorems we will need in the proof of Theorem 1.

Theorem 2 (see [1], pp. 25)**.** A finite group G is Abelian if and only if all the irreducible representations of G are of degree 1.

Theorem 3 (see [1], pp. 20)**.** Let $\chi_1, \chi_2, \ldots, \chi_h$ be the irreducible characters of a finite group G. Let $g \in G$ and $c(g)$ be the number of elements in the conjugacy class of g. Then

1. we have: $\sum_{i=1}^{h} \overline{\chi_i(g)}\chi_i(g) = \frac{|G|}{c(g)}$
2. if $s \in G$ is not conjugate to g, we have $\sum_{i=1}^{h} \overline{\chi_i(g)}\chi_i(s) = 0$

Proof. (Theorem 1) Note that the matrix of the QFT is a square matrix, since the number of rows (the number of irreducible representations) equals the number of columns (the number of group elements). Therefore it suffices to show that the columns of the QFT matrix are orthonormal vectors.

Let $g_i, g_j \in G$ be two arbitrary group elements. Then we have

$$\begin{aligned}(\mathrm{QFT}\,|g_i\rangle)^\dagger \mathrm{QFT}\,|g_j\rangle &= \frac{1}{\sqrt{|G|}} \sum_{\psi\in\hat{G}} \psi(g_i)^\dagger \langle\psi| \frac{1}{\sqrt{|G|}} \sum_{\phi\in\hat{G}} \phi(g_j)\,|\phi\rangle \\ &= \frac{1}{|G|} \sum_{\psi,\phi\in\hat{G}} \overline{\psi(g_i)}\phi(g_j)\,\langle\psi|\phi\rangle \\ &= \frac{1}{|G|} \sum_{\psi\in\hat{G}} \overline{\psi(g_i)}\psi(g_j), \end{aligned} \tag{3}$$

where $\psi(g_i)^\dagger = \overline{\psi(g_i)}$, since ψ is one-dimensional (Theorem 2). Due to the same reason the character of representation ψ equals ψ itself, $\chi_\psi = \psi$. Therefore, we can apply Theorem 3 to simplify (3). Since G is Abelian, $|c(g)| = 1$ for all $g \in G$. Thus, expression (3) is equal to 1 if $i = j$ and 0 if otherwise. So, we get:

$$(\mathrm{QFT}\,|g_i\rangle)^\dagger \mathrm{QFT}\,|g_j\rangle = \delta_{ij}$$

This means that the columns of the QFT matrix are orthonormal vectors. □

Theorem 4 (see [1], pp. 19)**.** The number of irreducible representations of a finite group G (up to isomorphism) is equal to the number of conjugacy classes of G.

Since G is Abelian, it has $|G|$ conjugacy classes. Therefore, from Theorem 4 we conclude that G has $|G|$ irreducible representations. So, we can make a bijection between group elements and irreducible representations. Moreover, it turns out that there will always be a natural way how to define this bijection. If we identify irreducible representations with the group elements using this bijection, then the QFT sends each group element to some linear combination of the group elements.

Example 6. Let $G = \{0, 1, \ldots, n-1\}$ with the operation of addition modulo $n \in \mathbb{N}$. This group is cyclic ($G = \langle 1 \rangle$) and therefore $\hat{G} = \{\psi_0, \psi_1, \ldots, \psi_{n-1}\}$, where $\psi_t(g) = e^{2\pi itg/n}$ for all $g, t \in G$ (see [1], pp. 35). Now we can introduce a bijection between group elements and irreducible representations in a natural way by mapping an irreducible representation ψ_t to a group element t. So the QFT acts on the basis vectors in the following way:

$$|g\rangle \mapsto \frac{1}{\sqrt{n}} \sum_{t=0}^{n-1} e^{2\pi itg/n} |t\rangle$$

In the above example we saw how to define a bijection between irreducible representations and group elements if $G = \mathbb{Z}_n$. We know that every finite Abelian group G can be expressed as $G = \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \ldots \times \mathbb{Z}_{n_k}$ (see [5], pp. 472). Thus, we can obtain all the irreducible representations of G by taking tensor product of the irreducible representations of groups $\mathbb{Z}_{n_1}, \mathbb{Z}_{n_2}, \ldots, \mathbb{Z}_{n_k}$ (see [1], pp. 27). Therefore, we have

$$\hat{G} = \left\{ \psi_t(g) = e^{2\pi i \left(\frac{t_1 g_1}{n_1} + \frac{t_2 g_2}{n_2} + \cdots + \frac{t_k g_k}{n_k} \right)} \,\middle|\, t_i, g_i \in \mathbb{Z}_{n_i} \right\}, \tag{4}$$

where $g = (g_1, g_2, \ldots, g_k)$ and $t = (t_1, t_2, \ldots, t_k)$ are elements of group G. From the above we see that we can naturally define a bijection between elements of group G and irreducible representations of G as follows:

$$t \longleftrightarrow \psi_t$$

2.3 Quantum Algorithm for Abelian HSP

We are given a finite Abelian group G and a quantum black box Q_f for computing the function $f : G \to X$ which is constant and distinct on different cosets of some unknown subgroup H of G.

Step 1. Construct a quantum state whose first register corresponds to the equally weighted superposition of the group elements and the last register is set to $|0\rangle$:

$$|\varphi_1\rangle = \left(\frac{1}{\sqrt{|G|}} \sum_{g \in G} |g\rangle \right) |0\rangle = \frac{1}{\sqrt{|G|}} \sum_{g \in G} |g\rangle |0\rangle$$

Step 2. Query the black box Q_f using the state $|\varphi_1\rangle$ constructed in Step 1:

$$|\varphi_2\rangle = Q_f |\varphi_1\rangle = Q_f \frac{1}{\sqrt{|G|}} \sum_{g \in G} |g\rangle |0\rangle = \frac{1}{\sqrt{|G|}} \sum_{g \in G} Q_f |g\rangle |0\rangle =$$

$$= \frac{1}{\sqrt{|G|}} \sum_{g \in G} |g\rangle |0 \oplus f(g)\rangle = \frac{1}{\sqrt{|G|}} \sum_{g \in G} |g\rangle |f(g)\rangle$$

Step 3. Now measure the rightmost register of $|\varphi_2\rangle$ where the values of the function f are stored in basis $\mathcal{B}_r = \{|x\rangle\}_{x \in X}$. Recall that the value of $f(g)$ will be the same exactly for those group elements that are in the same coset of H. Thus, with probability $p_r = |H| / |G|$ after measurement the state collapses to

$$|\varphi_{3,r}\rangle = \frac{1}{\sqrt{|H|}} \sum_{h \in H} |r + h\rangle |f(r)\rangle = \left(\frac{1}{\sqrt{|H|}} \sum_{h \in H} |r + h\rangle \right) |f(r)\rangle$$

where $r \in R$ is the representative of some coset of H and R is the set of all representatives. Since we can tensor out the rightmost register $|f(r)\rangle$, we can discard it and continue working only with the first register (see [2] or [3]). So, we redefine $|\varphi_{3,r}\rangle$ as follows:

$$|\varphi_{3,r}\rangle = \frac{1}{\sqrt{|H|}} \sum_{h \in H} |r + h\rangle$$

Step 4. Apply quantum Fourier transformation to the quantum state $|\varphi_{3,r}\rangle$ obtained in the previous step:

$$\begin{aligned} |\varphi_{4,r}\rangle = \mathrm{QFT}\,|\varphi_{3,r}\rangle &= \frac{1}{\sqrt{|H| \cdot |G|}} \sum_{h \in H} \sum_{\psi \in \hat{G}} \psi(r+h)\,|\psi\rangle = \\ &= \frac{1}{\sqrt{|H| \cdot |G|}} \sum_{\psi \in \hat{G}} |\psi\rangle \sum_{h \in H} \psi(r)\psi(h) = \\ &= \frac{1}{\sqrt{|G|}} \sum_{\psi \in \hat{G}} \psi(r)\,|\psi\rangle \left(\frac{1}{\sqrt{|H|}} \sum_{h \in H} \psi(h) \right) \end{aligned} \tag{5}$$

In order to simplify the expression we have just obtained, let us first compute the following sum:

$$S(\psi) := \frac{1}{\sqrt{|H|}} \sum_{h \in H} \psi(h),$$

where $\psi \in \hat{G}$. We will consider two cases — when ψ is trivial on subgroup H and when it is not.

1. If representation ψ is trivial on subgroup H that is, $\forall h \in H : \psi(h) = 1$, then
$$S(\psi) = \frac{1}{\sqrt{|H|}} \sum_{h \in H} 1 = \frac{|H|}{\sqrt{|H|}} = \sqrt{|H|}$$

2. If representation ψ is not trivial on subgroup H, we can rewrite sum $S(\psi)$ as follows:
$$S(\psi) = \frac{1}{\sqrt{|H|}} \sum_{h \in H} \psi(h) = \frac{1}{\sqrt{|H|}} \sum_{h \in H} 1 \cdot \psi(h) = \frac{1}{\sqrt{|H|}} \sum_{h \in H} \overline{id(h)}\psi(h),$$
where $id : H \to \mathbb{C}$ is the trivial representation of H. Since id and ψ both are of degree 1, $\overline{id(h)}\psi(h) = \overline{\chi_{id}(h)}\chi_\psi(h)$, where χ_{id} and χ_ψ are characters of id and ψ respectively. Since irreducible characters of a finite group are orthogonal (see [1], pp. 15), we conclude that:
$$S(\psi) = \frac{1}{\sqrt{|H|}} \sum_{h \in H} \overline{id(h)}\psi(h) = \frac{1}{\sqrt{|H|}} \sum_{h \in H} \overline{\chi_{id}(h)}\chi_\psi(h) = 0$$

Now, if we want to compute the sum (5), we have to determine how many representations which are trivial on subgroup H are there in $\hat{G}$. If representation $\psi \in \hat{G}$ is trivial on subgroup H, then for every two group elements g_1, g_2 from the same coset we have

$$\psi(g_1) = \psi(rh_1) = \psi(r)\psi(h_1) = \psi(r) \cdot 1 = \psi(r)\psi(h_2) = \psi(g_2),$$

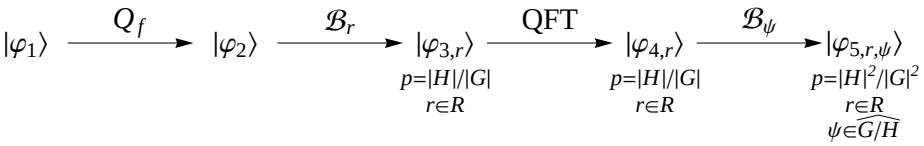

Figure 2: Intermediate states during the execution of quantum algorithm for Abelian hidden subgroup problem.

where $g_1 = rh_1, g_2 = rh_2$, and $h_1, h_2 \in H$, and r is a representative of the coset. Therefore, every representation ψ which is trivial on subgroup H is constant on all cosets of H. So, we see that there is a natural one-to-one map from those irreducible representations of group G which are trivial on subgroup H to the irreducible representations of the quotient group G/H. Since G/H is also Abelian, it has $|G/H| = |G| / |H|$ irreducible representations. Therefore, there are $|G| / |H|$ representations in $\hat{G}$ that are trivial on subgroup H. Thus we are able to compute the last sum in expression (5) and can write $|\varphi_{4,r}\rangle$ as follows:

$$|\varphi_{4,r}\rangle = \frac{1}{\sqrt{|G|}} \sum_{\psi\in\hat{G}} \psi(r) |\psi\rangle \left(\frac{1}{\sqrt{|H|}} \sum_{h\in H} \psi(h) \right) = \sum_{\psi\in\widehat{G/H}} \sqrt{\frac{|H|}{|G|}} \psi(r) |\psi\rangle ,$$

where $\widehat{G/H}$ is the set of those irreducible representations of group G which are trivial on subgroup H and $r \in R$ (i.e. the set of representatives of the cosets of subgroup H).

Step 5. Measure the state $|\varphi_{4,r}\rangle$ which we obtained in previous step in basis $\mathcal{B}_\psi = \{|\psi\rangle\}_{\psi\in\hat{G}}$. Since the degree of representation ψ is 1, $|\psi(r)| = 1$ for all r. Therefore, after measuring $|\varphi_{4,r}\rangle$ we get outcome $\psi \in \widehat{G/H}$ with probability

$$p_\psi = \left| \sqrt{\frac{|H|}{|G|}} \psi(r) \right|^2 = \frac{|H|}{|G|}$$

and the state collapses to $|\psi\rangle$. Recall that in Step 3 we got each $|\varphi_{3,r}\rangle$ with probability $|H|/|G|$. Therefore the state after the measurement in basis $\mathcal{B}_\psi$ is

$$|\varphi_{5,r,\psi}\rangle := |\psi\rangle$$

with probability $p_{r,\psi} = p_r \cdot p_\psi = |H|^2/|G|^2$, where $|\varphi_{5,r,\psi}\rangle$ means that after the measurement in basis $\mathcal{B}_r$ (Step 3) the state collapsed to $|\varphi_{3,r}\rangle$, but after the measurement in basis $\mathcal{B}_\psi$ (Step 5) the state collapsed to $|\psi\rangle$. Since $p_{r,\psi}$ does not depend on r and $|R| = |G|/|H|$, the final state is

$$|\varphi_5\rangle = |\psi\rangle$$

with probability $|R| \cdot p_{r,\psi} = |H|/|G|$, where $\psi \in \widehat{G/H}$. Thus, the procedure we have done so far results in uniform sampling from the set of those irreducible representations of G which are trivial on subgroup H.

Step 6. Repeat $c+4$ times steps 1 to 5, where $c = \sum_{i=1}^{l} c_i$ and $|G| = \prod_{i=1}^{l} p_i^{c_i}$. After $i-$th repetition, we get some irreducible representation ψ_i of G which is trivial on subgroup H, where $i \in \{1, \ldots, c+4\}$. Using the natural bijection we considered in Section 2.2, map each ψ_i to the corresponding group element t_i:

$$\psi_i \longleftrightarrow (t_{i,1}, t_{i,2}, \ldots, t_{i,k}) =: t_i, \tag{6}$$

where $t_{i,j} \in \mathbb{Z}_{n_j}$ and $G = \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_k}$ is the decomposition of G into cyclic groups. Find generators $h_1, h_2, \ldots$ for the solution space of the system of linear equations:

$$Tx = 0 \mod 1, \tag{7}$$

where T is the matrix whose $i-$th row is $\left(\frac{t_{i,1}}{n_1}, \frac{t_{i,2}}{n_2}, \ldots, \frac{t_{i,k}}{n_k}\right)$. Output $h_1, h_2, \ldots$.

Theorem 5. With probability at least 2/3 elements $h_1, h_2, \ldots$ generate hidden subgroup H i.e. $\langle h_1, h_2, \ldots \rangle = H$.

Proof. According to equation (4) we can write irreducible representation ψ_i from (6) as

$$\psi_i(x) = e^{2\pi i \left(\frac{t_{i,1}}{n_1} x_1 + \frac{t_{i,2}}{n_2} x_2 + \cdots + \frac{t_{i,k}}{n_k} x_k \right)} \tag{8}$$

where $x = (x_1, x_2, \ldots, x_k) \in G = \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_k}$. Since ψ_i is trivial on H we have:

$$\frac{t_{i,1}}{n_1} x_1 + \frac{t_{i,2}}{n_2} x_2 + \cdots + \frac{t_{i,k}}{n_k} x_k = 0 \mod 1$$

for all $x \in H$. It means that $t_i \in H^{\perp}$, where

$$H^{\perp} = \left\{ s \in G \,\middle|\, \forall x \in H : \frac{s_1}{n_1} x_1 + \frac{s_2}{n_2} x_2 + \cdots + \frac{s_k}{n_k} x_k = 0 \mod 1 \right\}$$

Note that $H^{\perp}$ is a subgroup of G. Consider the following lemma:

Lemma 1. (see [3], pp. 246) Let G be a finite group, $|G| = \prod_{i=1}^{l} p_i^{c_i}$, where p_i's are primes. Let $c := \sum_{i=1}^{l} c_i$ and $t_1, t_2, \ldots, t_{c+4}$ be uniformly sampled from group G. Then $\langle t_1, t_2, \ldots, t_{c+4} \rangle = G$ with probability at least 2/3.

By repeating steps 1 to 5 we uniformly sample an irreducible representation $\psi \in \widehat{G/H}$ or equivalently, $t_i \in H^{\perp}$. According to Lemma 1, elements t_i span the space $H^{\perp}$ with probability at least 2/3. Since $(H^{\perp})^{\perp} = H$, the generators $h_1, h_2, \ldots$ of solutions of the system (7) span the space H with probability at least 2/3. Hence, we have found the generators of the hidden subgroup with probability at least 2/3. □

2.4 Complexity of quantum algorithm for Abelian HSP

First, let us compute the query complexity C_Q of quantum algorithm for Abelian HSP. Since in each iteration of Steps 1 to 5 we made only 1 query to the black box, and there were $c+4$ iterations, $C_Q = c+4$. Since $c = \sum_{i=1}^{l} c_i$, where $|G| = \prod_{i=1}^{l} p_i^{c_i}$ and p_i's are primes, we have $c = O(\log |G|)$. Hence $C_Q = O(\log |G|)$.

Now let us compute the time complexity C_T. We can encode the elements of group G into $\Theta(\log |G|)$ qubits. In each iteration of Steps 1 to 5 we perform QFT

on $\Theta(\log |G|)$ qubits. It is known that QFT on m qubits can be implemented using m^2 elementary quantum operations (see [3], pp. 117). Thus each QFT takes $O(\log^2 |G|)$ time steps. We can ignore other operations performed in Steps 1 to 5, since they can be done in constant time. Thus each iteration requires $O(\log^2 |G|)$ time steps. Since there are $c+4 \in O(\log |G|)$ iterations, the running time of quantum algorithm is $O(\log^3 |G|)$. The classical postprocessing (solving the linear system (7)) can also be done in $O(\log^3 |G|)$ time, since it consists of $c + 4 \in O(\log |G|)$ equations with $k \in O(\log |G|)$ unknowns. Thus, $C_T = O(\log^3 |G|)$.

2.5 Applications of HSP

At first glance the interest in the hidden subgroup problem may seem just a curiosity, but it turns out that the ability to find hidden subgroups can be useful to solve several natural problems, including the ones for which no efficient classical algorithm is known. One of the nontrivial examples of HSP is the Simon's problem [7]. It inspired Shor to create his celebrated algorithm for factoring large integers [6], which is based on period finding – another instance of HSP. The running time of Shor's factoring algorithm is polynomial in the length of the input. Another important algorithm due to Shor is the algorithm for computing discrete logarithm [6]. These quantum algorithms threaten most of the methods used in cryptography (e.g. RSA), as these methods are mainly based either on the assumption that there is no efficient algorithm for factoring large integers or computing discrete logarithms over various groups.

References

[1] Jean-Pierre Serre, Linear Representations of Finite Groups, Springer-Verlag, 1977.

[2] Michael A. Nielsen, Isaac L. Chuang, Quantum Computation and Quantum Information, Cambridge University Press, 2000.

[3] Phillip Kaye, Raymond Laflamme, Michele Mosca, An Introduction to Quantum Computing, Oxford University Press, 2007.

[4] Andrew M. Childs, Wim van Dam, Quantum Algorithms for Algebraic Problems, unpublished.

[5] Michael Artin, Algebra, Prentice Hall, 1991.

[6] Peter Shor, Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. SIAM J. Computing, 26:1484-1509, 1997.

[7] David Simon, On the Power of Quantum Computation, SIAM J. Computing, 26:1474-1483, 1997.