Abelian Hidden Subgroup Problem

Laura Mancinska
University of Waterloo,
Department of C&O

December 12, 2007
Abelian hidden subgroup problem

Outline

- Basic concepts in quantum computing
- Statement of the hidden subgroup problem (HSP)
- Quantum Fourier transformation
- Quantum algorithm for HSP
- Complexity and applications of the algorithm
If we are to understand a system that does a computation we have to answer two main questions:

1. What are the **states** of the system?
2. How does the system **evolve** from one state to another?
The state of the system is \([x]\), where \(x \in \{0, 1\}^n\)

The evolution of the system is \(f : \{0, 1\}^n \rightarrow \{0, 1\}^n\)
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

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

\[ \sum_x \alpha_x[x], \]

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 \( \beta_x = \sum_y u_{xy} \alpha_y. \)
Dirac notation

In quantum computation there is a convention to write vectors inside angled brackets. Therefore we will write the state of quantum system as:

$$|\psi\rangle = \sum_{x} \alpha_{x} |x\rangle$$

**Bra and ket vectors**

- $|\psi\rangle$ - column vector with components $\alpha_{x}$
- $\langle \psi |$ - row vector with components $\overline{\alpha_{x}}$ (dual of $\psi$)
- $\langle \psi | \phi \rangle$ - inner product of vectors $\psi$ and $\phi$
Dirac notation

Example with standard basis vectors of $\mathbb{C}^2$

\[
\begin{pmatrix} 1 \\ 0 \end{pmatrix} \equiv |0\rangle, \quad \begin{pmatrix} 0 \\ 1 \end{pmatrix} \equiv |1\rangle.
\]

Another example

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

\[
\langle \psi | = \frac{1}{\sqrt{2}} \langle 0 | + \frac{i}{\sqrt{2}} \langle 1 | \equiv \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ i \end{pmatrix}
\]
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 $|\psi\rangle = \sum_{i=1}^{n} \alpha_i |b_i\rangle$ (where $\sum_{i=1}^{n} |\alpha_i|^2 = 1$) gives $i$ with probability $|\alpha_i|^2$ and leaves the system in a state $|b_i\rangle$. 
Abelian Hidden Subgroup Problem (HSP)

We are given:

- a finite Abelian group \((G, +)\)
- quantum black box for function \(f : G \rightarrow X\) which is hiding some unknown subgroup \(H\) (\(f\) is constant and distinct on cosets of \(H\)).

Our goal is to determine the subgroup \(H\).

**Figure:** Black boxes for classical and quantum computing
Quantum Fourier transformation (QFT)

**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 $G$.

**Theorem**

QFT is a unitary transformation.
Quantum Fourier transformation (QFT)

QFT acts on basis states as follows:

\[
|g\rangle \mapsto \frac{1}{\sqrt{\lvert G \rvert}} \sum_{\psi \in \widehat{G}} \psi(g) |\psi\rangle,
\]

\(|\widehat{G}| = \# \text{ of conjugacy classes of } G = |G|\)

Therefore we can identify irreducible representations with group elements. It turns out that there is a natural way how to do that.

Example

Let \( G = \mathbb{Z}_n \) (cyclic group). Then \( \widehat{G} = \{ \psi_t(g) = e^{2\pi itg/n} | t \in G \} \) and QFT acts on basis states as follows:

\[
|g\rangle \mapsto \frac{1}{\sqrt{n}} \sum_{t=0}^{n-1} e^{2\pi itg/n} |t\rangle
\]
But how do we identify irreducible representations of Abelian group $G$ with its elements, if $G$ is not cyclic?

**Structure theorem**

We know that every finite Abelian group $G$ can be expressed as $G = \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \ldots \times \mathbb{Z}_{n_k}$.

Therefore for Abelian group $G$ we have:

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

where $g = (g_1, g_2, \ldots, g_k)$ and $t = (t_1, t_2, \ldots, t_k)$ are elements of group $G$. We identify $\psi_t$ with $t$. 
Quantum algorithm for HSP

**Step 1** Construct a uniform superposition over group elements in the first register:

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

**Step 2** Query the black box $Q_f$ with the state constructed in Step 1:

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

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

State after Step 2:

$$|\varphi_2\rangle = \frac{1}{\sqrt{|G|}} \sum_{g \in G} |g\rangle |f(g)\rangle$$

**Step 3** Measure rightmost register in basis $B_r = \{|x\rangle\}_{x \in X}$. 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 $r \in R$ (the set of the representatives for the cosets of subgroup $H$).

We can discard the last register and redefine $|\varphi_{3,r}\rangle$ as follows:

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

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

**Step 4** Apply quantum Fourier transformation (QFT) to state obtained in Step 3:

\[ |\varphi_{4,r}\rangle = \text{QFT} |\varphi_{3,r}\rangle = \frac{1}{\sqrt{|H| \cdot |G|}} \sum_{h \in H} \sum_{\psi \in \hat{G}} \psi(r + h) |\psi\rangle = \]

\[ = \frac{1}{\sqrt{|G|}} \sum_{\psi \in \hat{G}} \psi(r) |\psi\rangle \left( \frac{1}{\sqrt{|H|}} \sum_{h \in H} \psi(h) \right) \]

\[ = \sum_{\psi \in \hat{G}/H} \sqrt{\frac{|H|}{|G|}} \psi(r) |\psi\rangle \]
State after Step 3:

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

**Step 4** Apply quantum Fourier transformation (QFT) to state obtained in Step 3:

\[ |\varphi_{4,r}\rangle = \text{QFT} |\varphi_{3,r}\rangle = \frac{1}{\sqrt{|H| \cdot |G|}} \sum_{h \in H} \sum_{\psi \in \hat{G}} \psi(r + h) |\psi\rangle = \]
\[ = \frac{1}{\sqrt{|G|}} \sum_{\psi \in \hat{G}} \psi(r) |\psi\rangle \left( \frac{1}{\sqrt{|H|}} \sum_{h \in H} \psi(h) \right) \]

Now let us compute

\[ S(\psi) := \frac{1}{\sqrt{|H|}} \sum_{h \in H} \psi(h), \]
\[ = \sum_{\psi \in G/H} \sqrt{\frac{|H|}{|G|}} \psi(r) |\psi\rangle \]
State after Step 4:

\[ |\varphi_{4,r}\rangle = \sum_{\psi \in \hat{G}/H} \sqrt{|H|/|G|} \psi(r) |\psi\rangle \]

**Step 5** Measure the state \( |\varphi_{4,r}\rangle \) in basis \( \mathcal{B}_\psi = \{|\psi\rangle\}_{\psi \in \hat{G}} \). We get outcome \( \psi \in \hat{G}/H \) with probability

\[
p_{\psi} = \left| \sqrt{|H|/|G|} \psi(r) \right|^2 = \frac{|H|}{|G|}.
\]
Let us review the steps we have done so far.

\[ |\varphi_1\rangle \xrightarrow{Q_f} |\varphi_2\rangle \xrightarrow{B_r} |\varphi_{3,r}\rangle \xrightarrow{\text{QFT}} |\varphi_{4,r}\rangle \xrightarrow{B_\psi} |\varphi_{5,r,\psi}\rangle \]

- \( p = \frac{|H|}{|G|} \)
- \( r \in R \)

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

The state after Step 5 is:

\[ |\varphi_5\rangle = |\psi\rangle \]

with probability \( |R| \cdot p_{r,\psi} = \frac{|H|}{|G|} \), where \( \psi \in \hat{G}/H \) (irreps trivial on \( H \)).
Step 6 Repeat $c + 4 \in O(\log(|G|))$ times steps 1 to 5, where $c = \sum_{i=1}^{l} c_i$ and $|G| = \prod_{i=1}^{l} p_i^{c_i}$. Each time we sample uniformly from those irreducible representations of $G$ which are trivial on $H$. After $c + 4$ iterations we have enough information to output the full set of the generators of $H$ with probability at least $2/3$. 
Complexity of Quantum HSP algorithm

Both query and time complexities for quantum algorithm are polynomial in $\log(|G|)$, which is significantly smaller than classical complexities.

Applications

- Order Finding
- Shor’s Factorization algorithm with time complexity $O(\log^2 N)$. At the same time best known classical (probabilistic algorithm) runs in time $O(2^{\sqrt{\log N}})$
- Discrete logarithm


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

