The hidden subgroup problem in quantum computing

Gábor Ivanyos
Computer and Automation Research Institute
of the Hungarian Academy of Sciences

$(CS)^2$
Szeged, July 5, 2008.

Outline

Contents

Qubits

- **State:** a unit vector in the complex euclidean space $B = \mathbb{C}^2$:

  a superposition (linear combination) $a|0\rangle + b|1\rangle$,

  where $|a|^2 + |b|^2 = 1$
- **Computational basis:** $|0\rangle, |1\rangle$
- **After measurement:**
  - 0: with probability $|a|^2$,
  - 1: with probability $|b|^2$.

n-qubit system

- **State:** a unit vector in the complex euclidean space $B^{\otimes n} = \mathbb{C}^{2^n}$:

$$\text{superposition } \sum_{s\in S} a_s|s\rangle,$$

$$\text{where } S = \{0,1\}^n \text{ and } \sum_{s\in S} |a_s|^2 = 1.$$

- **Computational basis:** $|s\rangle$, where $s \in S$:

$$|0\ldots 00\rangle, |0\ldots 01\rangle, |1\ldots 11\rangle.$$

- **After measurement:** bit string s with probability $|a_s|^2$.

Quantum gates

- ***d*-qubit gate:** a unitary transformation of $\mathbb{C}^{2^d}$.

Examples:

- **Hadamard gate:** $Had : |0\rangle \mapsto \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle),$
  $$|1\rangle \mapsto \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle).$$
- **Controlled phase shift:**
  $$|0x\rangle \mapsto |0x\rangle,\ |10\rangle \mapsto |10\rangle,$$
  $$|11\rangle \mapsto \omega|11\rangle, \text{ where } |\omega| = 1.$$

Quantum circuits and the "computing" phase

- n-qubit circuit $=$ a sequence of one-and two-qubit gates
  wired to qubits or pairs of qubits
  in an n-qubit system
- Formally:
  $$T \otimes I,$$
  where T acts on the appropriate $\mathbb{C}^2$ or $\mathbb{C}^4$
- **Operation:** the composition (product) of the individual transformations
- **Time complexity:** length of the sequence
- **Remark:** For any constant $d > 2$, the quantum circuits built from 1- or 2-qubit gates are polynomially equivalent to circuits built from $\leq d$-qubit gates.

Quantum circuits: operation and the measurement

- the composition of the transformations applied to the computational basis element corresponding to the input
- then the state obtained is **measured**
- result: a probability distribution over the n-bit strings

decision $\sim$ one-bit results:

$$\mathrm{Prob}[s_1 = 1] = \sum_{s \in \{0,1\}^{n-1}} \mathrm{Prob}[1s].$$

corresponding class: **BQP**

analogous to BPP

Speedup with quantum computers

- Exploit parallelness in superpositions (Feynman)?
- Not that easy (measurements)
- First groundbreaking results (1994):
  - **Grover:** search in time $\sqrt{n}$
    (in a list of size n)
  - **Shor:** factoring and discrete log
    in polynomial time
- More recently: exponential speedup also in algebraic number theory (Hallgren; Schmidt and Vollmer 2005):
  class number and unit group computations
  (spec. case: Pell's equations).

Contents

Background

- **The hidden subgroup paradigm** is a common generalization of
  - Shor's order finding (the critical step in factoring),
  - discrete log
  - also captures the graph isomorphism problem
- All the currently known cases of exponential speedup with quantum computer are closely related.

Definition

- G (finite) group
- Function $f : G \rightarrow \{\text{bit strings}\}$

  hides subgroup $H \leq G$ if

  $$f(x) = f(y) \Leftrightarrow xH = yH$$

  (in words, f is constant on each left coset of H but takes distinct values on different cosets.)
- f is given by quantum oracle (or an efficient algorithm).

  Quantum oracle: unitary map $|x\rangle|0\rangle \mapsto |x\rangle|f(x)\rangle$

  Convention: two or more parts, called **registers**
- Task: find (generators for) H

  time measured in $\log|G|$: polynomial $= (\log|G|)^{O(1)}$

Special instances

- Oder finding $G = \mathbb{Z}$, $a \in A$ (commutative group),
  - $f(k) = a^k$.
  - $H = m\mathbb{Z}$, where $m =$ order of a.
- Discrete logarithm $G = \mathbb{Z} \times \mathbb{Z}$, $a, b \in A$
  - $f(k, \ell) = a^k b^{-\ell}$.
  - $H = \{(k, \ell) | a^k = b^\ell\}$.

Graph Isomorphism

- **permuted graph:**

  Γ graph with vertex set $\{1, \ldots, n\}$ $\sigma \in S_n$,
  edges of the permuted graph Γ^σ:
  $[i, j]$, where $[\sigma(i), \sigma(j)]$ edge of Γ.

- **The automorphism group as hidden subgroup**
  - $G = S_n$ $f(\sigma) = \Gamma^\sigma$.
  - the hidden subgroup is $Aut(\Gamma)$
- **Graph Isomorphism $\leftarrow$ Automorphism group**
  - Γ_1, Γ_2 connected.
  - $\Gamma_1 \cong \Gamma_2 \Leftrightarrow |Aut(\Gamma_1 \dot{\bigcup} \Gamma_2)| = 2 \cdot |Aut(\Gamma_1)| \cdot |Aut(\Gamma_2)|$.

Contents

Oracle for superposition 1.

$$\begin{aligned}
|0^n\rangle|0..0\rangle &\rightarrow \text{(prepare uniform superposition)} \\
\frac{1}{\sqrt{2^n}}\sum_{x\in\mathbb{Z}_2^n}|x\rangle|0..0\rangle &\rightarrow \text{(call the oracle)} \\
\frac{1}{\sqrt{2^n}}\sum_{x\in\mathbb{Z}_2^n}|x\rangle|f(x)\rangle &= \text{(collect by the second register)} \\
\frac{1}{\sqrt{2^n}}\sum_{s}\sum_{\substack{x\in\mathbb{Z}_2^n\\ f(x)=s}}|x\rangle|s\rangle &= \frac{1}{\sqrt{2^n}}\sum_{a\in T}\sum_{x\in H}|a+x\rangle|f(a)\rangle
\end{aligned}$$

T: cross-section (representatives of cosets)

Oracle for superposition 2.

with $|H| = 2^k$

$$\frac{1}{\sqrt{2^n}} \sum_{a \in T} \sum_{x \in H} |a + x\rangle |f(a)\rangle \quad =$$

$$\frac{1}{\sqrt{2^{n-k}}} \sum_{a \in T} \left(\frac{1}{\sqrt{2^k}} \sum_{x \in H} |a + x\rangle \right) |f(a)\rangle$$

for fixed $a \in T$ the first register contains the

coset state $|a + H\rangle := \frac{1}{\sqrt{2^k}} \sum_{x \in H} |a + x\rangle$

the second register is (and remains) constant

omit it

Fourier transform of $\mathbb{Z}_2^n$

linear extension of

$$|x\rangle \mapsto \frac{1}{\sqrt{2^n}} \sum_{y \in \mathbb{Z}_2^n} (-1)^{x \cdot y} |y\rangle,$$

where $\cdot =$ scalar product mod 2.
The transform is

$$Had^{\otimes n}$$

Applying Fourier transform

$$\text{coset state } \frac{1}{\sqrt{2^k}} \sum_{x \in H} |a+x\rangle \quad \rightarrow$$

$$\frac{1}{\sqrt{2^k}} \sum_{x \in H} \frac{1}{\sqrt{2^n}} \sum_{y \in \mathbb{Z}_2^n} (-1)^{(a+x)\cdot y} |y\rangle \quad =$$

$$\frac{1}{\sqrt{2^n}} \sum_{y \in \mathbb{Z}_2^n} \left(\frac{(-1)^{a\cdot y}}{\sqrt{2^k}} \sum_{x \in H} (-1)^{x \cdot y} \right) |y\rangle$$

Applying Fourier transform 2.

$$\text{coeff of } |y\rangle = \frac{(-1)^{a\cdot y}}{\sqrt{2^{n-k}}}\frac{1}{2^k}\sum_{x\in H}(-1)^{x\cdot y} \quad = \begin{cases} \frac{(-1)^{a\cdot y}}{\sqrt{2^{n-k}}} & \text{if } y \perp H, \\ 0 & \text{otherwise.} \end{cases}$$

$$\text{probability of } y \quad = \begin{cases} \frac{1}{2^{n-k}} & \text{if } y \perp H, \\ 0 & \text{otherwise.} \end{cases}$$

Computing the hidden subgroup H

- $H^\perp = \{y \in \mathbb{Z}_p^n \mid y \perp H\}$ a subgroup of $\mathbb{Z}_p^n$.
- Using $O(n)$ iterations probably collect a system Γ of generators for the group $H^\perp$.
- if so,

$$H = \{x \in \mathbb{Z}_p^n \mid x \cdot y \text{ for every } y \in \Gamma\}.$$

(= system of linear equations)

Contents

"Straightforward" extensions

- General commutative groups

  Fourier transforms of commutative groups

- Hidden normal subgroups in noncommutative groups

  Noncommutative generalization of the Fourier transform

Current groups with polynomial time HSP

Almost commutative

- Certain "two-step solvable" groups

  $A \lhd G$, A and G/A commutative

  Very few groups of this kind,

  Usually G/A is "large"

- Groups solvable in a constant number of steps

  with order of element bounded by a constant

  Friedl, $\sim$, Magniez, Santha, Sen 2003

  $\sim$ 2008

Hidden shift - a tool for induction

- $f_1, f_2 : \mathbb{Z}_k^n \to \{strings\}$ injective
  $f_2(x) = f_1(x + v)$ for some $v \in \mathbb{Z}_k^n$
  Find v
- A HSP in a two-step solvable group
- Friedl, $\sim$, Magniez, Santha, Sen 2003:
  poly time algorithm for k prime of constant size
- $\sim$ 2008: k prime power of constant size

Hidden shift II.

- Kuperberg 2006: subexponential in $n \log k$
  like $e^{\sqrt{n \log k}}$
- **Would be very good:** poly in $n \log k$
- already for $n = 1$
- $\sim$ 2008: For k =prime power, poly in n, exponential in k
- **Open:** For $k = 6$: poly in n ?????
- **Open:** poly in nk (k prime).
  Would lead to quite efficient HSP algorithms
  in a reasonably large class of solvable groups

Oracle for superposition 1.

$$
\begin{aligned}
|1_G\rangle|0..0\rangle &\rightarrow \text{(prepare uniform superposition)}\\
\frac{1}{\sqrt{|G|}}\sum_{x\in G}|x\rangle|0..0\rangle &\rightarrow \text{(call the oracle)}\\
\frac{1}{\sqrt{|G|}}\sum_{x\in G}|x\rangle|f(x)\rangle &= \\
\frac{1}{\sqrt{|G|}}\sum_{s}\sum_{\substack{x\in G\\ f(x)=s}}|x\rangle|s\rangle &= \frac{1}{\sqrt{|G|}}\sum_{a\in T}\sum_{x\in H}|ax\rangle|f(a)\rangle
\end{aligned}
$$

T: cross-section (representatives of cosets)

Oracle for superposition 2.

$$\frac{1}{\sqrt{|G|}}\sum_{a\in T}\sum_{x\in H}|ax\rangle|f(a)\rangle \quad =$$

$$\frac{1}{\sqrt{|G:H|}}\sum_{a\in T}\left(\frac{1}{\sqrt{|H|}}\sum_{x\in H}|ax\rangle\right)|f(a)\rangle$$

for fixed $a \in T$ the first register contains the

coset state $|aH\rangle := \frac{1}{\sqrt{|H|}}\sum_{x\in H}|ax\rangle$

the second register is (and remains) constant

omit it

Characters

of the finite commutative group G:
maps $\chi : G \longrightarrow \mathbb{C}^*$ s.t. $\chi(u+v) = \chi(u)\chi(v)$.
i.e. homomorphisms $G \longrightarrow \mathbb{C}^*$.
Form a group $\hat{G}$ isomorphic with G.
Example: $G = \mathbb{Z}_p^n$

$$\chi_u(v) = \omega^{u \cdot v}$$

$u \cdot v =$ scalar product modulo p
$\omega =$ primitive $\sqrt[p]{1}$.

Fourier transform

of the finite commutative group G:
linear extension of

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

$\exists$ efficient quantum implementations (QFT).
Usually $\hat{G}$ identified with G (χ_x with x above)

Example: Hadamard gate = Fourier transform of $\mathbb{Z}_2$:

$$Had : |0\rangle \mapsto \tfrac{1}{\sqrt{2}}(|0\rangle + |1\rangle),$$
$$|1\rangle \mapsto \tfrac{1}{\sqrt{2}}(|0\rangle - |1\rangle).$$

exact QFT for $\mathbb{Z}_2^n$: $Had^{\otimes n}$.

Applying Fourier transform

$$\text{coset state } \frac{1}{\sqrt{|H|}} \sum_{x \in H} |ax\rangle \quad \rightarrow$$

$$\frac{1}{\sqrt{|H|}} \sum_{x \in H} \frac{1}{\sqrt{|G|}} \sum_{\chi \in \hat{G}} \chi(ax)|\chi\rangle \quad =$$

$$\frac{1}{\sqrt{|G|}} \sum_{\chi \in \hat{G}} \left(\frac{\chi(a)}{\sqrt{|H|}} \sum_{x \in H} \chi(x) \right) |\chi\rangle$$

Applying Fourier transform 2.

coeff of $|\chi\rangle$

$$\frac{\chi(a)}{\sqrt{|G:H|}}\frac{1}{|H|}\sum_{x\in H}\chi(x) = \begin{cases} \frac{\chi(a)}{\sqrt{|G:H|}} & \text{if } \chi_H = 1, \\ 0 & \text{otherwise.} \end{cases}$$

Proof.: orthogonality relation for 1_H and χ_H:

$$\frac{1}{|H|}\sum_{x\in H}\chi(x) = \begin{cases} 1 & \text{if } \chi_H = 1, \\ 0 & \text{otherwise} \end{cases}$$

probability of χ:

$$\begin{cases} \frac{1}{|G:H|} & \text{if } \chi \in H^{\perp}, \\ 0 & \text{otherwise.} \end{cases}$$

Computing the hidden subgroup H

- $H^\perp = \{\chi \in \hat{G} \mid \chi_H = 1\}$ a subgroup of $\hat{G}$.
- In $O(\log|G|)$ iteration probably collect a system Γ of generators for the group $H^\perp$.
- if so,

$$H = \{x \in G \mid \chi(x) = 1 \text{ for every } \chi \in \Gamma\}.$$

(∼ system of linear equations)