10/14/10 QIC 710 Lecture 10 : Factoring recap, Hidden subgroup problems

Order Finding algorithm (version 2):

Given x, N, $\gcd(x, N) = 1$

Find: $\text{order}(x) = r$.

Let $U_x|y\rangle = \begin{cases} |x \cdot y \bmod N\rangle & \text{if } 0 \le y \le N-1 \\ |y\rangle & \text{otherwise} \end{cases}$

on n qubits $2^{n-1} < N \le 2^n$.

$$|v_t\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} \omega_r^{kt} |x^k \bmod N\rangle$$

$$U_x|v_t\rangle = \omega_r^{-t}|v_t\rangle$$

use phase estimation to get these $\frac{t}{r}$

- but can't prepare $|v_t\rangle$

instead prepare

$$\frac{1}{\sqrt{r}} \sum_{t=0}^{r-1} |v_t\rangle = \frac{1}{r} \sum_{k=0}^{r-1} |x^k\rangle \cdot \underbrace{\sum_{t=0}^{r-1} \omega_r^{kt}}_{0 \text{ unless } k=0}$$

$$= |x^0\rangle = |1\rangle$$

$\Rightarrow$ get an estimate of $\frac{t}{r}$ for a uniformly random $t \in \{0, 1, \ldots, r-1\}$.

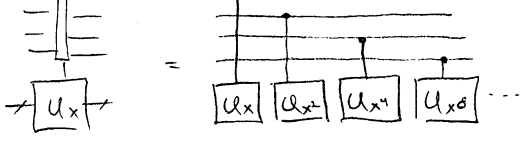
(provided can implement $c\text{-}U_x^k$)

use continued fractions to get the denominator

$$U_x : |y\rangle \xrightarrow{\text{mult.}} |y, x \cdot y\rangle \xrightarrow{\text{division}} |y - \tfrac{x \cdot y}{y}, x \cdot y\rangle$$

division is multiplication by x^{-1}

use the extended Euclidean algorithm to compute the modular multiplicative inverse x^{-1} (classically)



"Hidden subgroup" problems

Problem: Let G be a known group, H an unknown subgroup.
Let $f: G \to X$ be constant only on cosets of H.
ie. $\forall g \in G$, $h, h' \in H$ $f(gh) = f(gh')$
and $f(g) = f(g') \iff g^{-1}g' \in H$.
Goal: Determine H (ie., a set of generators for H)

Examples:
1. $G = (\mathbb{Z}/2\mathbb{Z})^n$ under addition, $H = \{0, a\}$
↖ base case for Simon's Problem
2. $G = (\mathbb{Z}_2^n)$, $H = \langle a_1, \ldots, a_k \rangle$ HW3 #3
3. $G = \mathbb{Z}_{p-1}^2$, $H = \{(0,0), (1,y), (2,2y), \ldots, ((p-2),(p-2)y)\}$
↖ used in the DLog algorithm
4. $G = \mathbb{Z}$, $H = r\mathbb{Z}$
↖ order finding for Shor's factoring algorithm

"Standard algorithm"

$$|G\rangle := \frac{1}{\sqrt{|G|}} \sum_{g \in G} |g\rangle \xrightarrow{f} \sum_g |g, f(g)\rangle$$

$$\xrightarrow{\text{measure}} |gH\rangle = \frac{1}{\sqrt{|H|}} \sum_h |gh\rangle$$

for random, unknown

$$\xrightarrow{\text{QFT}}$$

(for abelian or nonabelian groups)

5. Dihedral group = group of symmetries of regular N-gon
$= \langle$ rotation, reflection$\rangle$
H = hidden reflection ⇒ hidden shift problem
Best algorithm known: Kuperberg 03 02 11 2 $2^{\sqrt{\log N}}$
closely connected to lattice-based cryptosystems. (SVP, etc.)
6. S_n = symmetric group on n elements
application: qu. algorithm for graph isomorphism

Status of quantum algorithms, and fault-tolerance problem QKD

Mixed states & density matrices

Recall: For a system with N configurations,

- a deterministic classical state is a configuration ("computational basis state")
- a randomized classical state is a probability distribution over configurations
  $\vec{p} \in \mathbb{R}^N \quad \sum_{i=1}^{N} p_i = 1, \quad \forall i \; p_i \geq 0.$
- a quantum state is a vector
  $\vec{q} \in \mathbb{C}^N \quad \|q\|_2 = 1 = \left(\sum_i |q_i|^2\right)^{1/2}$

What about distributions over such states?

eg. $\begin{cases} |0\rangle \text{ with prob. } 1/2 \\ \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \text{ with prob. } 1/2 \end{cases}$

→ In general, a quantum state (mixed state) can be an ensemble of pure states

Such states arise naturally:

- when you or the noisy environment measures or partially measures a pure state
- when you analyze a subsystem of an entangled quantum state — by the principle of deferred measurement

  eg. $\frac{1}{\sqrt{2}}\left(|0\rangle \otimes |0\rangle + |1\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\right)$

  a purification of the previous ensemble

Philosophy: "Church of the Larger Hilbert Space"
"all states are pure states (in a larger system), all evolution is unitary" -measurements? black holes?

eg. Measurement is really a form of CNOT gate

$\frac{1}{\sqrt{2}}\left(|0\rangle \otimes |0\rangle + |+\rangle \otimes |1\rangle\right) \otimes |\text{measurement device}\rangle$

$\longrightarrow \frac{1}{\sqrt{2}}\left(|0\rangle \otimes |0\rangle \otimes |\text{measured } 0\rangle + |+\rangle \otimes |1\rangle \otimes |\text{measured } 1\rangle\right)$ etc.

but in practice a formalism for mixed states is still needed, entanglement theory...

in a computer using dead/alive cats, what do they remember at the end? many worlds, Copenhagen, ...