# Quantum algorithms

David Jao

August 14, 2023

# Basic principles

Uncertainty principle: There is no way to determine a quantum state without measuring it.

Quantum superposition: Prior to measurement, all possible potential outcomes of the measurement are valid. (Schrödinger's cat!)

Quantum entanglement: In an entangled pair, measuring one object constrains the possible states for the other object. (The second object's unmeasured state must be consistent with the first object's measurement.)

# Quantum states

## Definition

A quantum state is a line through the origin in a complex Hilbert space. (We usually normalize quantum states to have unit norm.)

## Example

Consider $\mathbb{C}^2$ with basis $\{|0\rangle, |1\rangle\}$. Then, as quantum states,

$$\begin{aligned}\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) &= -\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\ &\neq \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\end{aligned}$$

# Measurement

Measuring a quantum state $v = \sum c_i b_i$ with respect to an orthonormal basis $\{b_1, \ldots, b_n\}$ yields $b_i$ with probability $|c_i|^2$.

## Example

Suppose $v = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$.

- Measuring $v$ with respect to $\{|0\rangle, |1\rangle\}$ yields either $|0\rangle$ or $|1\rangle$, with probability $\frac{1}{2}$ for each.
- Measuring $v$ with respect to $\left\{\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\right\}$ always yields $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$.

# Tensor products

We denote tensor products using concatenation, e.g.

$$
\begin{aligned}
|0\rangle \otimes |0\rangle \otimes |0\rangle &= |0\rangle\,|0\rangle\,|0\rangle = |0,0,0\rangle = |000\rangle \in (\mathbb{C}^2)^{\otimes 3} = \mathbb{C}^8 \\
|0\rangle \otimes |0\rangle \otimes |1\rangle &= |0\rangle\,|0\rangle\,|1\rangle = |0,0,1\rangle = |001\rangle \in (\mathbb{C}^2)^{\otimes 3} = \mathbb{C}^8 \\
&\vdots \\
|1\rangle \otimes |1\rangle \otimes |1\rangle &= |1\rangle\,|1\rangle\,|1\rangle = |1,1,1\rangle = |111\rangle \in (\mathbb{C}^2)^{\otimes 3} = \mathbb{C}^8
\end{aligned}
$$

By abuse of notation, we write $|0\rangle = |000\rangle$, $|1\rangle = |001\rangle$, $|2\rangle = |010\rangle$, etc.

# Quantum computation

Quantum computers operate on entangled particles (“qubits”).

- On classical computers, a logic bit is either 0 or 1.
- On quantum computers, a qubit is simultaneously 0 and 1.
    - A set of $n$ qubits ranges simultaneously from 0 to $2^n - 1$.

Therefore, for any function $f$:

- On a classical computer, computing $f(0), f(1), \ldots f(2^n - 1)$ requires $2^n$ operations.
- On a quantum computer, computing $f(0), f(1), \ldots f(2^n - 1)$ simultaneously requires one operation:

$$\sum_{i=0}^{2^n-1} |i\rangle \to \sum_{i=0}^{2^n-1} |i\rangle |f(i)\rangle$$

- Unfortunately, extracting the results of the computation requires a measurement, which yields only one (random) output.

# Quantum computation

The allowed operations on quantum states are unitary operators. In particular, all such operations are invertible, or *reversible*.

## Example

Let $f\colon \mathbb{Z}/2^n \to \mathbb{Z}/2^n$ be a function. We can evaluate $f$ on quantum states as follows (ignoring normalization):

$$\sum_{i=0}^{2^n-1} |i\rangle|0\rangle \mapsto \sum_{i=0}^{2^n-1} |i\rangle|f(i)\rangle$$

- This operation is reversible — we retain the input values $i$.
- $|i\rangle$ and $|f(i)\rangle$ are *entangled*. Measuring one of them constrains the other.
- For example if we measure $|i\rangle$ and obtain $|5\rangle$, then $|f(i)\rangle$ must equal $|f(5)\rangle$ — **even though it was not measured**.

# Quantum algorithms

The most important quantum algorithms:

Grover's algorithm: Inverts any function $f\colon \{0,1\}^n \to A$ in $2^{n/2}$ quantum operations.

Shor's algorithm: Factors integers and finds discrete logarithms in a polynomial number of quantum operations.

# Grover's algorithm

Grover's algorithm slightly affects the security of symmetric-key cryptosystems:

- Brute-force attack against a $k$-bit key requires $O(2^{k/2})$ quantum operations.
- Collisions in $k$-bit hash functions require $O(2^{k/3})$ quantum operations.
- Attack applies to symmetric-key encryption schemes, MAC schemes, and hash functions.
- Generally, doubling the key length restores security.

# Shor's algorithm

Shor's algorithm breaks most public-key cryptosystems in use today, including:

- RSA
- Diffie-Hellman
- Elgamal
- DSA/ECDSA/EdDSA

# Shor's algorithm

To factor an integer $N$:

1. Choose $Q$ such that $N^2 \leq 2^Q \leq 2N^2$ (usually $Q$ is unique).
2. Choose $x \in \mathbb{Z}_N^*$. Let $\operatorname{ord}(x)$ denote the period of $j \mapsto x^j$.
3. Compute the quantum state
$$\frac{1}{\sqrt{2^Q}} \sum_{j=0}^{2^Q-1} |j\rangle \left| x^j \bmod N \right\rangle.$$
4. Measure the second register, and discard the result.
5. Apply the quantum Fourier transform.
6. Measure the first register. Let $z$ denote its value.
7. Then $z/2^Q$ is very very very close to $c/\operatorname{ord}(x)$ for some $c$.
8. Use continued fractions to find $c/\operatorname{ord}(x)$, and hence $\operatorname{ord}(x)$.
9. Factor $N$.

# Example (Credit: Srinivasan Arunachalam)

Suppose we want to factor $N = 21$.

1. Choose $Q$ such that $N^2 \le 2^Q \le 2N^2$ ($Q = 9$).
2. Choose $x \in \mathbb{Z}_N^*$ (say $x = 2$).
3. Compute the quantum state

$$\frac{1}{\sqrt{512}} \sum_{j=0}^{511} |j\rangle|0\rangle \mapsto \frac{1}{\sqrt{512}} \sum_{j=0}^{511} |j\rangle\left|2^j \bmod N\right\rangle$$

4. Measure the second register. Suppose we get $|2\rangle$. The quantum state is now

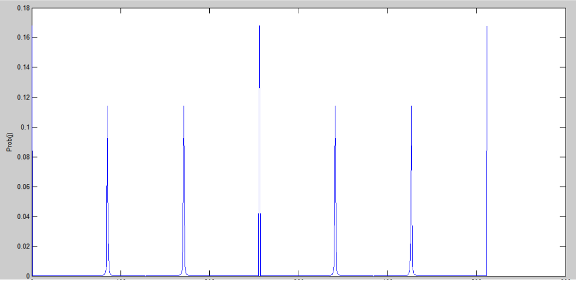
$$\frac{1}{\sqrt{86}}(|1\rangle + |7\rangle + \ldots + |505\rangle + \ldots)|2\rangle = \frac{1}{\sqrt{86}} \sum_{k=0}^{85} |6k+1\rangle|2\rangle$$

5. Apply the quantum Fourier transform.

$$\left(\frac{1}{\sqrt{86}}\sum_{k=0}^{85}|6k+1\rangle|2\rangle\right) \overset{\text{QFT}}{\mapsto} \frac{1}{\sqrt{512}}\sum_{j=0}^{511}\left(\frac{1}{\sqrt{86}}\sum_{a=0}^{85} e^{\frac{-2\pi i j(6a+1)}{512}}|j\rangle\right)|2\rangle$$

$$\text{Prob}(j) = \frac{1}{512\times 86}\left|\sum_{a=0}^{85} e^{-2\pi i\frac{6ja}{512}}\right|^2$$

The DFT plots the *frequencies* which occur in the input distribution.



# Obtaining $\operatorname{ord}(x)$

6. Measure the first register. Suppose we get $|85\rangle$. (The peaks are at 0, 85, 171, 256, 341, and 427.)
7. $\frac{85}{512}$ is very close to $\frac{c}{r}$ for some $r = \operatorname{ord} 2 \ll 2^Q = 512$.
8. Use continued fractions to find $\operatorname{ord}(2)$.

$$\frac{85}{512} = \cfrac{1}{6 + \cfrac{1}{42 + \cfrac{1}{2}}} \approx \frac{1}{6}$$

Hence $\operatorname{ord}(2) = 6$. We verify that $2^6 \equiv 1 \pmod{21}$.

# Completing the factorization

9. $\operatorname{ord}(x)$ is usually very close to $\phi(n) = (p-1)(q-1)$. (If not, try again with another $x$.)

   For $n = 21$, we have $\phi(n) = 12$ and $\operatorname{ord}(x) = 6$. (In general, $\phi(n)/\operatorname{ord}(x)$ is a small integer $k$.)

   Since $\phi(n) \approx n$, we can guess the value of $k$.

   Given $\operatorname{ord}(x)$ and $k = \phi(n)/\operatorname{ord}(x)$, we can find $\phi(n)$.

   Given $\phi(n) = (p-1)(q-1)$ and $n = pq$, solve for $p$ and $q$.

# Factorization and the hidden subgroup problem

## Definition

Given a group $G$ and a subgroup $H \subset G$, we say a function $f : G \to X$ *hides* $H$ if for all $g_1, g_2 \in G$,

$$f(g_1) = f(g_2) \iff g_1 H = g_2 H.$$

The *hidden subgroup problem* is to find a generating set for $H$ given $f$.

## Example

For $N \in \mathbb{Z}$ and $x \in \mathbb{Z}_N^*$, the function $f : \mathbb{Z} \to \mathbb{Z}_N$ defined by $f(j) = x^j \bmod N$ hides $H = r\mathbb{Z}$, where $r = \operatorname{ord}(x)$.

# Quantum algorithms for hidden subgroup problems

Shor's algorithm solves not only the integer factorization problem, but also the hidden subgroup problem in any abelian group.

Finding isogenies in CRS/CSIDH amounts to a hidden subgroup problem in a *dihedral* group:

1. Express the complex multiplication operation $(\mathfrak{a}, E) \mapsto \mathfrak{a} * E$ as a group action of $\mathrm{Cl}(\mathcal{O}_D)$.
2. Express the group action inverse problem in $\mathrm{Cl}(O_D)$ as a hidden subgroup problem in the dihedral group $\mathrm{Cl}(O_D) \rtimes \mathbb{Z}/2$.

Kuperberg's algorithm (arXiv:quant-ph/0302112) solves the dihedral hidden subgroup problem (and hence breaks CRS/CSIDH) in quantum subexponential time.

See also "The dihedral hidden subgroup problem", Imin Chen and David Sun, arXiv:2106.09907.

# From isogenies to hidden subgroups

- For a finite abelian group $G$, let $G \times X \to X$ be any free and transitive group action. (Example: $(\mathfrak{a}, E) \mapsto \mathfrak{a} * E$)
- We wish to compute group action inverses: Given $x_0, x_1 \in X$, find $\gamma \in G$ such that $\gamma x_1 = x_0$.
- Let $\phi \colon \mathbb{Z}/2 \to \mathrm{Aut}(G)$ be given by $\phi(b)(g) = g^{(-1)^b}$.
- Consider the function $f \colon G \rtimes_\phi \mathbb{Z}/2 \to X$, $f(g, b) = g x_b$.
- Since the group action is free, we have

$$\begin{aligned} f(g_1, b_1) = f(g_2, b_2) \iff & \; b_1 = 0, b_2 = 1, \text{ and } g_1^{-1} g_2 = \gamma \\ & \text{or } b_1 = 1, b_2 = 0, \text{ and } g_2^{-1} g_1 = \gamma \end{aligned}$$

  Hence $f$ hides the subgroup $\{(0,0), (\gamma, 1)\} \subset G \rtimes_\phi \mathbb{Z}/2$.
- If we solve the hidden subgroup problem for $f$, then we will have found $\gamma$.

# Dihedral hidden subgroup problem

- For simplicity, suppose $G = \mathbb{Z}/N$ and $D_N = \mathbb{Z}/N \rtimes \mathbb{Z}/2$.
- Suppose $f$ hides the subgroup $H = \{(0,0), (\gamma, 1)\} \subset D_N$.
- Form the state
$$\frac{1}{\sqrt{|D_N|}} \sum_{d \in D_N} |d\rangle \, |f(d)\rangle$$
- Measure the second register to obtain
$$\frac{1}{\sqrt{|(z,0)H|}} \sum_{d \in (z,0)H} |d\rangle = \frac{1}{\sqrt{2}} (|(z,0)\rangle + |(z+\gamma, 1)\rangle)$$
in the first register, for some random coset $(z,0)H$. By abuse of notation, denote this "coset state" by $|(z,0)H\rangle$.
- We can generate lots of these coset states, for random cosets. (We have no control over which cosets we obtain.)

# Quantum Fourier transform

- Apply the quantum Fourier transform to the first coordinate:

$$
\begin{aligned}
|(z,0)H\rangle &= \frac{1}{\sqrt{2}}(|(z,0)\rangle + |(z+\gamma,1)\rangle) \\
&\overset{\text{QFT}}{\mapsto} \frac{1}{\sqrt{2N}} \sum_{k \in \mathbb{Z}_N} (\zeta_N^{kz} |(k,0)\rangle + \zeta_N^{k(z+\gamma)} |(k,1)\rangle) \\
&= \frac{1}{\sqrt{N}} \sum_{k \in \mathbb{Z}_N} \zeta_N^{kz} |k\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle + \zeta_N^{k\gamma} |1\rangle)
\end{aligned}
$$

- Measure the first register to obtain $|k\rangle$ for some $k$. The second register is

$$
\frac{1}{\sqrt{2}}(|0\rangle + \zeta_N^{k\gamma} |1\rangle)
$$

  Denote this quantum state by $|\psi_k\rangle$. We can generate lots of these states for random $k$, with no control over $k$ (but we do know what $k$ is for each such quantum state).

# Overall strategy

We now assume for (further!) simplicity that $N$ is a power of 2. The strategy is as follows:

- If we could construct
$$|\psi_k\rangle = \frac{1}{\sqrt{2}}(|0\rangle + \zeta_N^{k\gamma}|1\rangle)$$
for $k$ of our choice, then (for example) we could find $|\psi_{N/2}\rangle = \frac{1}{\sqrt{2}}(|0\rangle + (-1)^\gamma|1\rangle)$.
- Measure $|\psi_{N/2}\rangle$ w.r.t. $\left\{\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\right\}$ to obtain the least significant bit of $\gamma$.
- Reduce to $D_{N/2}$ and use induction to find $\gamma$.

# Combining states

We can exert limited control over $|\psi_k\rangle$ by *combining states*:

$$\begin{aligned} |\psi_p, \psi_q\rangle &= \frac{1}{2}(|0,0\rangle + \zeta_N^{p\gamma}|1,0\rangle + \zeta_N^{q\gamma}|0,1\rangle + \zeta_N^{(p+q)\gamma}|1,1\rangle \\ &\overset{\text{CNOT}}{\mapsto} \frac{1}{2}(|0,0\rangle + \zeta_N^{p\gamma}|1,1\rangle + \zeta_N^{q\gamma}|0,1\rangle + \zeta_N^{(p+q)\gamma}|1,0\rangle \\ &= \frac{1}{\sqrt{2}}(|\psi_{p+q}, 0\rangle + \zeta_N^{q\gamma}|\psi_{p-q}, 1\rangle) \end{aligned}$$

We now measure the second register.

- If we get $|0\rangle$, then the first register is $|\psi_{p+q}\rangle$.
- If we get $|1\rangle$, then the first register is $\zeta_N^{q\gamma}|\psi_{p-q}\rangle = |\psi_{p-q}\rangle$.

We can't control which of $|\psi_{p\pm q}\rangle$ we get, but we know which one we got.

# Kuperberg sieve

1. Create $A \approx 4^{\sqrt{\log N}}$ quantum states $\psi_k$, for random $k \in \mathbb{Z}_N$.
2. Group the quantum states into buckets according to their last $\sqrt{\log N}$ bits (least significant bits). On average each bucket has $A/2^{\sqrt{\log N}}$ quantum states and there are $2^{\sqrt{\log N}}$ buckets.
3. Combine pairs of states in each bucket, with the goal of zeroing out the last $\sqrt{\log N}$ bits.
   - On average, combining states succeeds half the time.
   - If successful, we destroy two states and create one new state.
   - If unsuccessful, we lose two states and create nothing.
   - On average, we have $1/4$ as many states as we had before.
4. We get $A/4$ quantum states, whose last $\sqrt{\log N}$ bits are zero.
5. Repeat this bucket sorting process on the next $\sqrt{\log N}$ bits, to obtain $A/4^2$ quantum states, whose last $2\sqrt{\log N}$ bits are zero.
6. ... Eventually we obtain $A/4^{\sqrt{\log N}} \approx 1$ quantum states, with all but the most significant bit zero.