Hugo SALOU

Quantum Computer Science

Query

$U_f \, |x\rangle |y\rangle = |x, f(x) \oplus y\rangle$

$U_f \, |x\rangle |-\rangle = (-1)^{f(x)} |x\rangle |-\rangle$

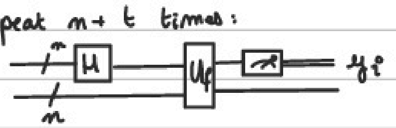
Simon's problem

Given $f : \{0,1\}^n \longrightarrow \{0,1\}^n$, find $a \in \{0,1\}^n$, $a \neq 0$ such that $\forall x \neq y$,

$f(x) = f(y) \iff y = x \oplus a$

Quantum solution:

- Repeat $n+t$ times:



- Solve over $\mathbb{F}_2$, $a \cdot y_i = 0 \ \forall i$.
- Return a non-zero such a.

$\mathbb{P}[\text{Correct}] \geq 1 - 1/2^{t+1}$ (choose $t = 10$)

Schor's factoring algorithm

- Order finding in $\mathbb{Z}/N\mathbb{Z}$

  apply phase estimation to

  $$M_a |x\rangle = \begin{cases} |ax \bmod N\rangle & \text{if } x \in \{0, \dots, N-1\} \\ |x\rangle & \text{if } x \in \{N, \dots, 2^n\} \end{cases}$$

- Classical order $\rightsquigarrow$ factorization

  → pick $a \in [\![2, N-1]\!]$
  → compute $K = \gcd(a, N)$
  → if $K \neq 1$ then $(K, N/K)$ is a factoring of N
  → find the order r of a
  → if r is odd, redo everything with a different a
  → compute $q = \gcd(N, a^{r/2} + 1)$
  → if $q \neq 1$ then $(q, N/q)$ is a factoring of N
  → otherwise redo everything with a different a

Density matrix

ρ acting on $\mathbb{C}^d$ as a $d \times d$ matrix st

$\operatorname{tr} \rho = 1$ & ρ is positive semidefinite

For $d = 2$, we can write

$\rho = \frac{1}{2}(\mathbb{1} + \vec{r} \cdot \vec{\sigma})$

where $\vec{r}$ is the Bloch vector and $\vec{\sigma} = (X, Y, Z)$

Quantum channel

$\mathcal{E} : \mathcal{B}(\mathcal{H}) \longrightarrow \mathcal{B}(\mathcal{H})$

st. $\mathcal{E}$ is linear

trace preserving · $\forall \rho$ density matrix, $\operatorname{tr}(\mathcal{E}(\rho)) = \operatorname{tr} \rho = 1$

complete positive · $\forall \mathcal{H}_R$ Hilbert space, the map $\mathcal{I}_R \otimes \mathcal{E}$ sends positive semidefinite operators to positive semidefinite op^{rs}.

CPTP

$$H(X) = -\sum_{x \in \mathcal{X}} P_X(x) \log(P_X(x))$$

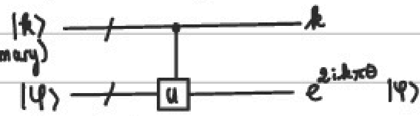
$$\Delta(P, Q) = \frac{1}{2} \sum_x |P(x) - Q(x)| = \max_{S \subseteq \mathcal{X}} |P(S) - Q(S)| \rightsquigarrow \Delta(\rho, \sigma) = \frac{1}{2} \sum_{\lambda \in \operatorname{Sp}(\rho - \sigma) \text{ with mult.}} |\lambda| = \max_{\pi \text{ proj}} |\operatorname{tr}(\pi_\rho) - \operatorname{tr}(\pi_\sigma)|$$

Any unitary can be efficiently approximated using one- and two-qubit gates.

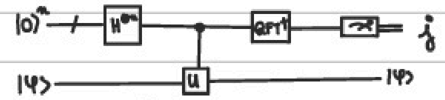
Phase Estimation

Problem: given U and $|\psi\rangle$ with $U|\psi\rangle = e^{2i\pi\theta} |\psi\rangle$, find the value of θ.

Lemma:



Solution:



$\implies \theta = j / 2^n$

Quantum Fourier Transform

$\omega := e^{2\pi i / N}$

$$\mathrm{QFT} : |x\rangle \longmapsto \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} \omega^{xk} |k\rangle$$

can be implemented in $\mathcal{O}((\log N)^2)$.

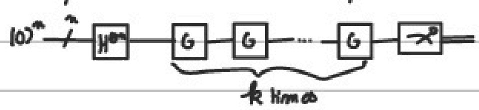
Grover's algorithm

find x st $f(x) = 1$

$Z_f |x\rangle = (-1)^{f(x)} |x\rangle$

$$Z_0 |x\rangle = \begin{cases} -|x\rangle & \text{if } |x\rangle \neq |0\rangle^n \\ |x\rangle & \text{if } |x\rangle = |0\rangle^n \end{cases} = 2|0\rangle\langle 0| - \mathbb{1}$$

Define $G := H^{\otimes n} Z_0 H^{\otimes n} Z_f$



Linear code

a $[n, k]$-code is a subspace $C \leq \mathbb{F}_2^n$ of dimension k (i.e. $|C| = 2^k$)

Quantum code

a (n, k)-code is a subspace $\mathcal{C} \leq (\mathbb{C}^2)^{\otimes n}$ of dimension 2^k

Errors $\mathcal{E} \leq \mathcal{L}((\mathbb{C}^2)^{\otimes n})$ subspace of linear maps

A code $\mathcal{C}$ corrects errors from $\mathcal{E}$ if $\forall |\varphi\rangle, |\psi\rangle \in \mathcal{C}$, $\forall A, B \in \mathcal{E}$, if $\langle \varphi | \psi \rangle = 0$ then $\langle \varphi | B^\dagger A | \psi \rangle = 0$.

Shor's code

$|0\rangle \longmapsto |{+}{+}{+}\rangle$

$|1\rangle \longmapsto |{-}{-}{-}\rangle$

Syndrome of error E is $s(E) = (s_1, \dots, s_{n-k}) \in \{\pm 1\}^{n-k}$

where $g_i E|\psi\rangle = s_i E|\psi\rangle \ \forall i$.

where $S = \langle g_1, \dots, g_{n-k} \rangle$.

Stabilizer subspace

If $S \leq \underbrace{\left\langle \bigotimes_{k=1}^{n} (u_k A_k) \;\middle|\; \begin{matrix} A_k \in \{I, X, Y, Z\} \\ u_k \in \{\pm 1, \pm i\} \end{matrix} \right\rangle}_{G_n}$ commutative,

$$\mathcal{C}_S := \{ |\psi\rangle \in (\mathbb{C}^2)^{\otimes n} \mid \forall g \in S,\ g|\psi\rangle = |\psi\rangle \}$$