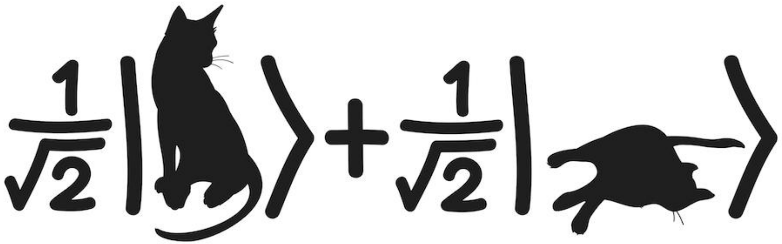
Quantum Mechanics & Quantum Computation

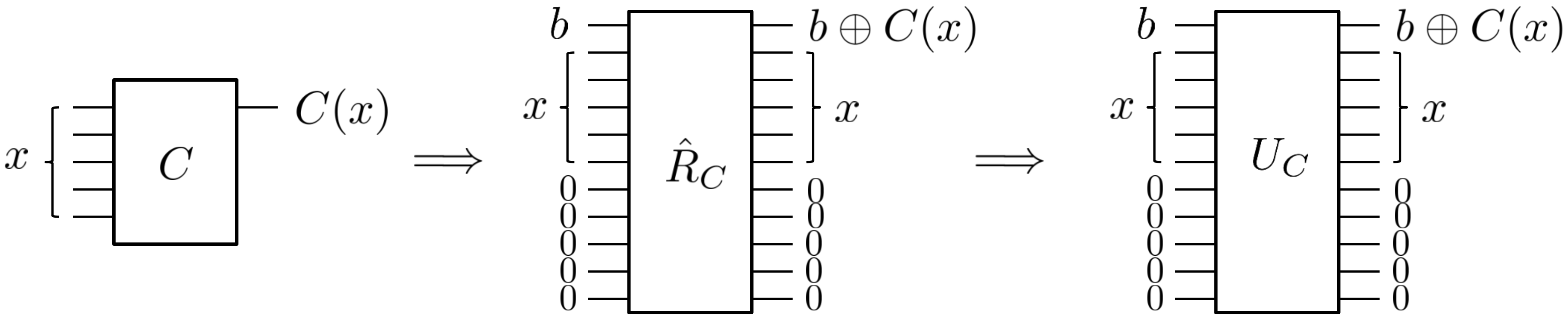


Umesh V. Vazirani
University of California, Berkeley

Lecture 12: Early Quantum Algorithms

Fourier Sampling

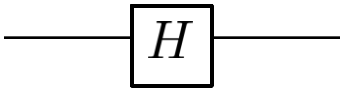
Classical reversible computation



$$\sum_x \alpha_x |x\rangle |b\rangle \longrightarrow \sum_x \alpha_x |x\rangle |b \oplus C(x)\rangle$$

Hadamard Transform

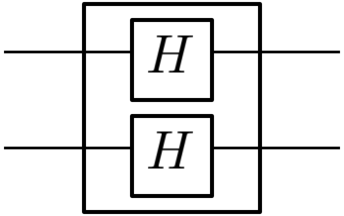
- Basic Building Block



$$\begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix}$$

$|0\rangle \rightarrow |+\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$

$|1\rangle \rightarrow |-\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$



$$\begin{pmatrix} \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & -\frac{1}{2} & \frac{1}{2} & -\frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} \\ \frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} & \frac{1}{2} \end{pmatrix}$$

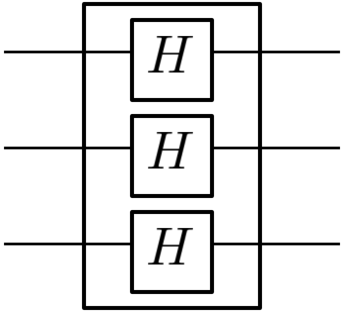
$|00\rangle \rightarrow |++\rangle = \left(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\right) \otimes \left(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\right)$

$= \frac{1}{2}|00\rangle + \frac{1}{2}|01\rangle + \frac{1}{2}|10\rangle + \frac{1}{2}|11\rangle$

$\vdots$

$|11\rangle \rightarrow \left(\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle\right) \otimes \left(\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle\right)$

$= \frac{1}{2}|00\rangle - \frac{1}{2}|01\rangle - \frac{1}{2}|10\rangle + \frac{1}{2}|11\rangle$



$|000\rangle \rightarrow \frac{1}{2\sqrt{2}}|000\rangle + \cdots + \frac{1}{2\sqrt{2}}|111\rangle$

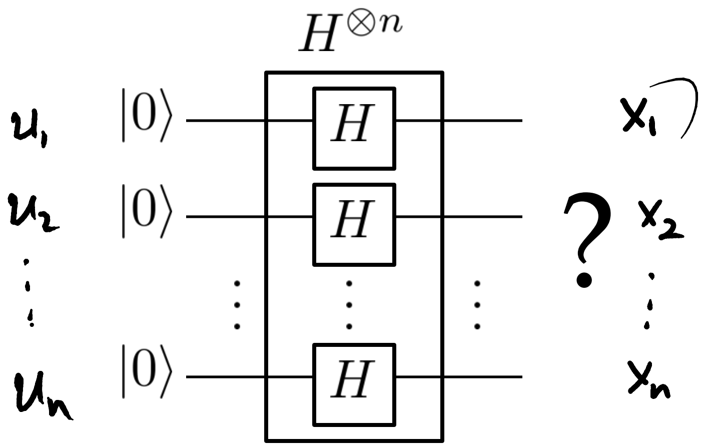
$|001\rangle$

$\cdots$

$|111\rangle \rightarrow$

What about for general n?

Hadamard Transform



$$\left(\tfrac{1}{\sqrt{2}}|0\rangle + \tfrac{1}{\sqrt{2}}|1\rangle\right) \otimes \left(\tfrac{1}{\sqrt{2}}|0\rangle + \tfrac{1}{\sqrt{2}}|1\rangle\right) \otimes \cdots \otimes \left(\tfrac{1}{\sqrt{2}}|0\rangle + \tfrac{1}{\sqrt{2}}|1\rangle\right)$$

$$= \left(\tfrac{1}{\sqrt{2}}|0\rangle + \tfrac{1}{\sqrt{2}}|1\rangle\right)^{\otimes n}$$

$$= \frac{1}{2^{n/2}} \sum_{x \in \{0,1\}^n} |x\rangle$$

$$|u\rangle = |u_1 u_2 \cdots u_n\rangle$$

$$H^{\otimes n}|u\rangle = \sum_x \frac{(-1)^{u \cdot x}}{2^{n/2}} |x\rangle$$

$$u \cdot x = u_1 x_1 + \cdots + u_n x_n$$

eg $n = 3$

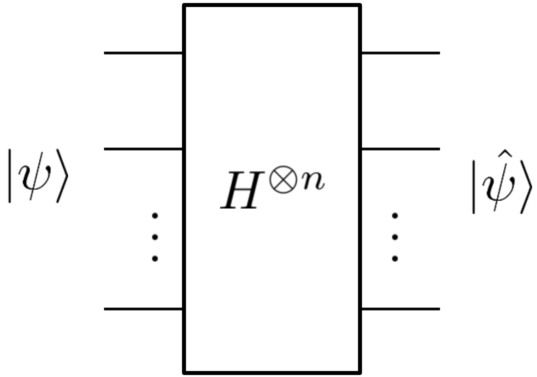
$u = 1\ 1\ 1$

$x = 1\ 0\ 1$

$u \cdot x = 1 \cdot 1 + 1 \cdot 0 + 1 \cdot 1 = 2$

$$\frac{(-1)^{u \cdot x}}{2^{n/2}} = \frac{(-1)^2}{2^{3/2}} = \frac{1}{2^{3/2}}$$

Fourier Sampling



$= \sum_x \beta_x |x\rangle$

y wp $|\beta_y|^2$.

Create some superposition $|\psi\rangle$

$H^{\otimes n}$

measure

$$|\psi\rangle = \sum_x \alpha_x |x\rangle$$

$$|\hat{\psi}\rangle = \sum_x \beta_x |x\rangle$$

Parity problem

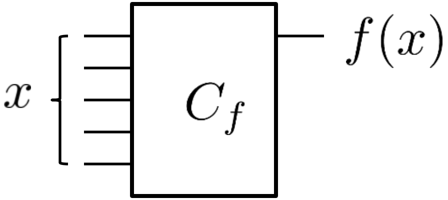
eg $n=3$
$u = 101$

$x = x_1 x_2 x_3$
$f(x) = x_1 \oplus x_3$
$= x_1 + x_3 \pmod 2$

We are given a function $f : \{0,1\}^n \to \{0,1\}$ as a black box.
We know that $f(x) = u \cdot x$ for some "hidden" $u \in \{0,1\}^n$.

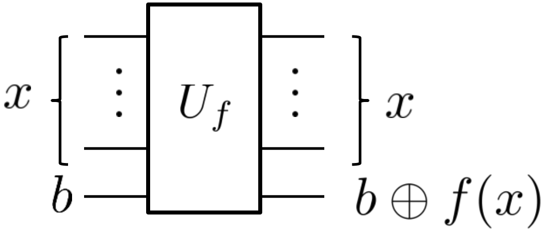
How do we figure out u with as few queries to f as possible?

<u>Classical</u>



<u>Quantum</u> ?

$\sum_x \alpha_x$



<u>Classically</u>: Input $10\cdots0$ u_1
$010\cdots0$ u_2

Need $\geq n$ steps.

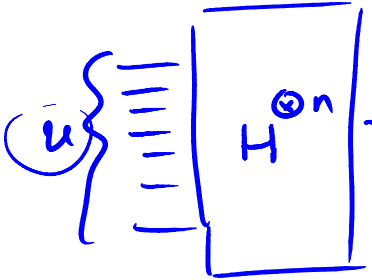
n steps $u = u_1 \cdots u_n$

Bernstein–Vazirani Algorithm

We are given a function $f : \{0,1\}^n \to \{0,1\}$ as a black box.
We know that $f(x) = u \cdot x$ for some "hidden" $u \in \{0,1\}^n$.

How do we figure out u with as few queries to f as possible?

- Set up superposition $\frac{1}{2^{n/2}} \sum_x (-1)^{f(x)} |x\rangle$ $= \frac{1}{2^{n/2}} \sum_x (-1)^{u \cdot x} |x\rangle$
- Fourier sample to obtain u.

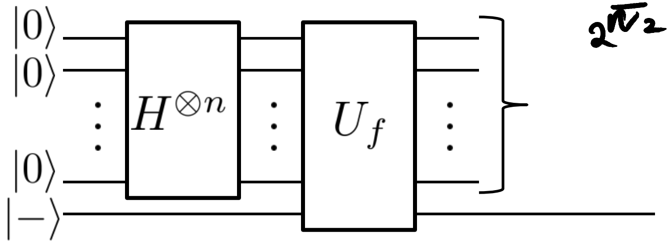


Setting up superposition

We are given a function $f : \{0,1\}^n \to \{0,1\}$ as a black box.
We know that $f(x) = u \cdot x$ for some "hidden" $u \in \{0,1\}^n$.

- Set up superposition $\frac{1}{2^{n/2}} \sum_x (-1)^{f(x)} |x\rangle$

$$|0^n\rangle \xrightarrow{H^{\otimes n}} \frac{1}{2^{n/2}} \sum_x |x\rangle$$



$$\frac{1}{2^{n/2}} \sum_x |x\rangle|-\rangle \xrightarrow{U_f} \left(\frac{1}{2^{n/2}} \sum_x (-1)^{f(x)} |x\rangle\right)|-\rangle$$

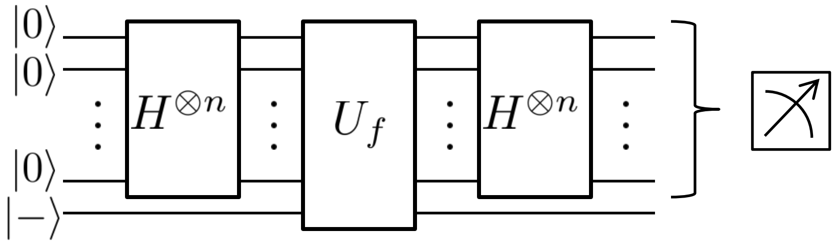
$$|b\rangle = |-\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$$

$$f(x) = 0 \qquad |b \oplus f(x)\rangle = |-\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$$

$$f(x) = 1 \qquad |b \oplus f(x)\rangle = -|-\rangle = \frac{1}{\sqrt{2}}|1\rangle - \frac{1}{\sqrt{2}}|0\rangle$$

Bernstein–Vazirani Algorithm

We are given a function $f : \{0,1\}^n \to \{0,1\}$ as a black box.
We know that $f(x) = u \cdot x$ for some "hidden" $u \in \{0,1\}^n$.



Recursive Fourier Sampling

- Recursive version of the parity problem.

- Classical algorithms satisfy the recursion

  T(n) > nT(n/2) + n

  Solution: T(n) = $\Omega(n^{\log n})$ superpolynomial

- Quantum algorithm satisfies recursion

  T(n) = 2T(n/2) + O(n)

  Solution: T(n) = O(n log n) polynomial