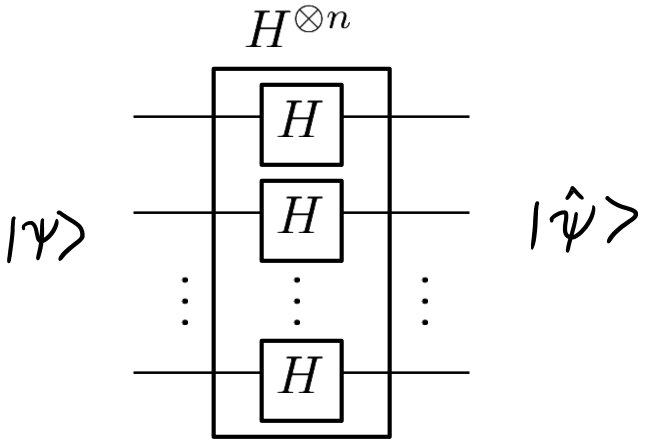
Quantum Mechanics & Quantum Computation

Umesh V. Vazirani
University of California, Berkeley

Lecture 8: Early Quantum Algorithms

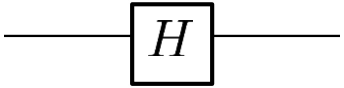
Fourier Sampling

Hadamard Transform



Hadamard Transform

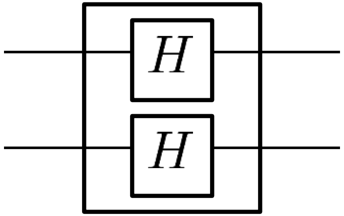
- Basic Building Block



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

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

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

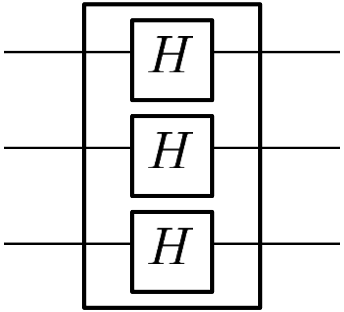


$$|00\rangle \rightarrow \left(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\right)\left(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\right) = \frac{1}{2}|00\rangle + \frac{1}{2}|01\rangle + \frac{1}{2}|10\rangle + \frac{1}{2}|11\rangle$$

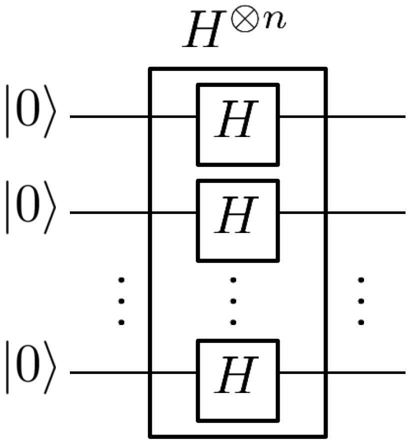
$$|01\rangle \rightarrow \left(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\right)\left(\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle\right) = \frac{1}{2}|00\rangle - \frac{1}{2}|01\rangle + \frac{1}{2}|10\rangle - \frac{1}{2}|11\rangle$$

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

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



Hadamard Transform



$$|0\cdots0\rangle \longrightarrow \left(\tfrac{1}{\sqrt{2}}|0\rangle + \tfrac{1}{\sqrt{2}}|1\rangle\right)^{\otimes n}$$

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

$$\underset{u_1u_2\cdots u_n}{\underset{\shortparallel}{|u\rangle}} \longrightarrow \sum_{x\in\{0,1\}^n} \frac{(-1)^{u\cdot x}}{2^{n/2}}|x\rangle$$

$$u\cdot x = u_1x_1 + u_2x_2 + \cdots + u_nx_n$$

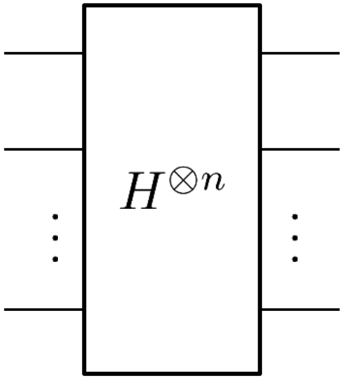
$u = 1\;0\;1$

$v = 1\;1\;1$

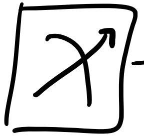
$u\cdot x = 1\cdot1 + 0\cdot1 + 1\cdot1 = 2$ $\qquad (-1)^{u\cdot x} = 1.$

Fourier Sampling

$$\sum_{x\in\{0,1\}^n} \alpha_x |x\rangle = |\psi\rangle$$



$|\hat{\psi}\rangle$



$\rightarrow$ See x wp $|\hat{\alpha}_x|^2$.

$$\Big\downarrow H^{\otimes n}$$

$$\sum_{x} \hat{\alpha}_x |x\rangle = |\hat{\psi}\rangle$$

Quantum Mechanics & Quantum Computation

Umesh V. Vazirani
University of California, Berkeley

Lecture 8: Early Quantum Algorithms

Fourier Sampling

Parity problem

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

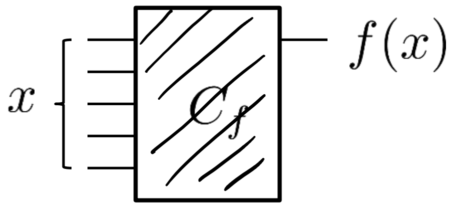
$= u_1 x_1 + \cdots + u_n x_n \pmod 2$

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

n bit string.

$u = 1011$
$x = 1001$
$u \cdot x = 1+0+0+1 \pmod 2$
$= 0$

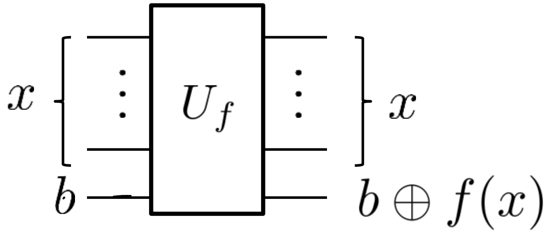
$x = 1011$
$u \cdot x = 1+0+1+1 \pmod 2$
$= 1$.



1 bit.

$x = 100\cdots0$ $\quad f(x) = u_1$
$x = 010\cdots0$ $\quad f(x) = u_2$
$\vdots$
$x = 0\cdots01$ $\quad f(x) = u_n$

n queries.



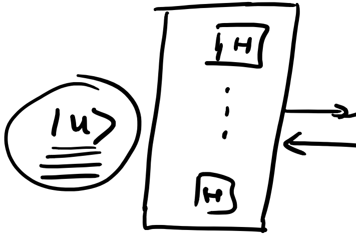
$0 \longrightarrow f(x)$
$1 \longrightarrow 1 \oplus f(x)$

Bernstein-Vazirani Algorithm

We are given a function $f : \{0,1\}^n \rightarrow \{0,1\}$ 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 $\frac{1}{2^{n/2}} \sum_x (-1)^{f(x)} |x\rangle \;=\; \sum_x \frac{(-1)^{u \cdot x}}{2^{n/2}} |x\rangle$
- Fourier sample to obtain u.

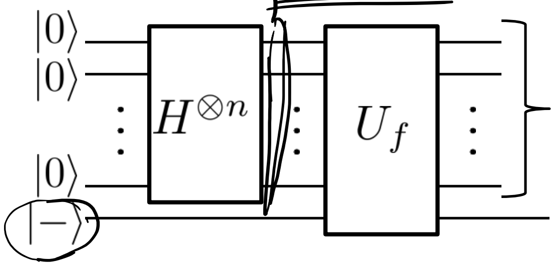


Setting up superposition

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

$\sum_x \frac{1}{2^{n/2}} |x\rangle$



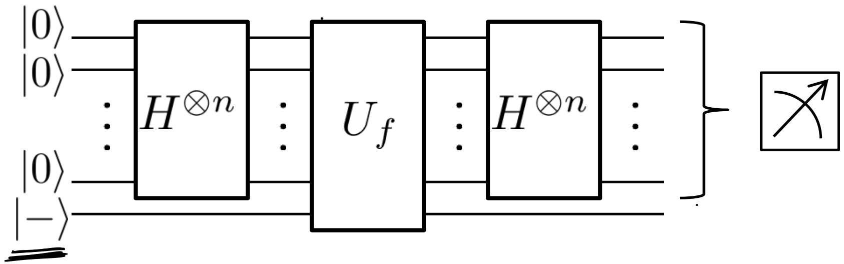
$|-\rangle = \frac{1}{\sqrt{2}} |0\rangle - \frac{1}{\sqrt{2}} |1\rangle.$

$f(x) = 1.$

$|-\rangle = \frac{1}{\sqrt{2}} |0\rangle - \frac{1}{\sqrt{2}} |1\rangle \longrightarrow \frac{1}{\sqrt{2}} |1\rangle - \frac{1}{\sqrt{2}} |0\rangle = -\left(\frac{1}{\sqrt{2}} |0\rangle - \frac{1}{\sqrt{2}} |1\rangle\right).$

Bernstein-Vazirani Algorithm

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



$\underline{u}$

constant # queries instead of n queries.

Recursive Fourier Sampling

- Recursive version of the parity problem.

- Classical algorithms satisfy the recursion

  $\underline{T(n)} > \underline{n}T(n/2) + n$ $\quad n \cdot \frac{n}{2} \cdot \frac{n}{4} \cdots\cdots$

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

- Quantum algorithm satisfies recursion

  $\underline{T(n)} = 2\underline{T(n/2)} + O(n)$

  Solution: T(n) = $\underline{O(n \log n)}$ $\quad$ polynomial

Quantum Mechanics & Quantum Computation

Umesh V. Vazirani
University of California, Berkeley

Lecture 8: Early Quantum Algorithms

Simon's Algorithm

Challenge

We are given a 2-1 function $f : \{0,1\}^n \to \{0,1\}^n$ such that:
there is a secret string $s \in \{0,1\}^n$ such that : $f(x) = f(x \oplus s)$
Challenge: find s.

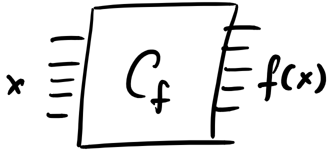
Example)

$n = 3$

$s = 101$

x	f(x)
000	000
001	010
010	001
011	100
100	010
101	000
110	100
111	001

$2^n = N$



Birthday $O(\sqrt{N})$.

Classically $\approx \sqrt{N} = 2^{n/2}$ steps.

poly(n) steps Quantum.

Simon's algorithm

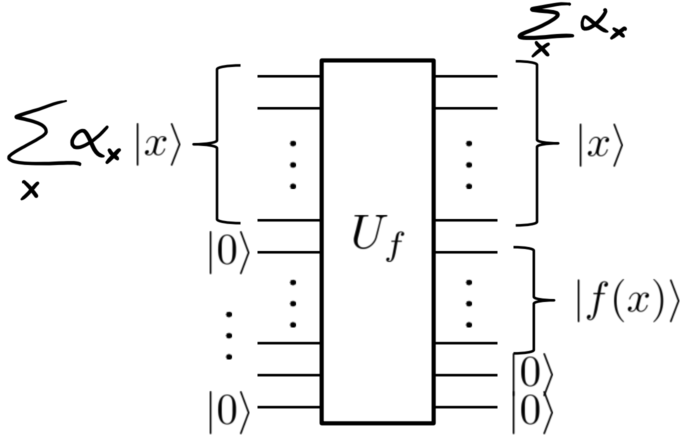
$s \in \{0,1\}^n \qquad r \in \{0,1\}^n$

- Set up random superposition $\frac{1}{\sqrt{2}}|r\rangle + \frac{1}{\sqrt{2}}|r \oplus s\rangle$
- Fourier sample to get a random y : $y \cdot s = 0(\text{mod}2)$ $\qquad y_1 s_1 + y_2 s_2 + \cdots + y_n s_n \equiv 0 (\text{mod } 2)$
- Repeat steps n-1 times to generate n-1 linear equations in s.

Solve for s.

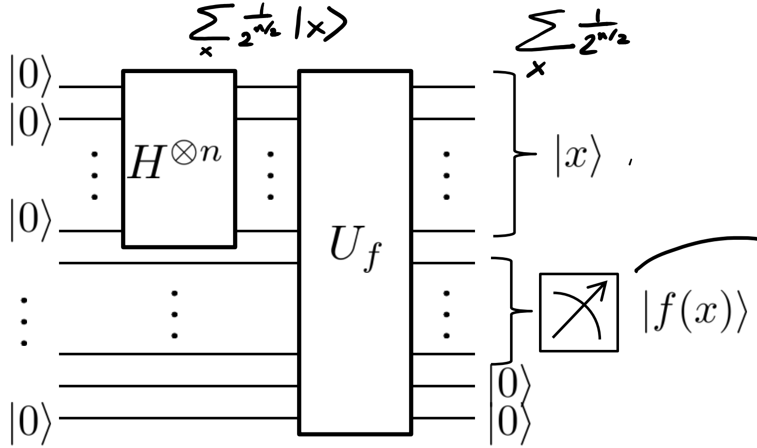
Setting up random superposition

We are given a function $f : \{0,1\}^n \to \{0,1\}^n$ as a black box.
We know that f is a 2-1 function. (There is a secret string $s \in \{0,1\}^n$ such that $f(x) = f(x \oplus s)$)



Setting up random superposition

We are given a function $f : \{0,1\}^n \to \{0,1\}^n$ as a black box.
We know that f is a 2-1 function. (There is a secret string $s \in \{0,1\}^n$ such that $f(x) = f(x \oplus s)$)

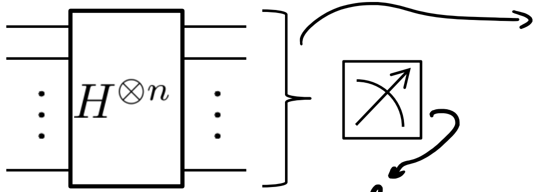


$$\boxed{\frac{1}{\sqrt{2}} |r\rangle + \frac{1}{\sqrt{2}} |r \oplus s\rangle}$$

$$\underline{a} = f(r) = f(r \oplus s).$$

Fourier Sampling

$$\frac{1}{\sqrt{2}}|r\rangle + \frac{1}{\sqrt{2}}|r \oplus s\rangle$$



$$\sum_y \beta_y |y\rangle$$

random y : $y \cdot s \equiv 0 \pmod 2$

Case 1 $\quad y \cdot s \equiv 0 \pmod 2$

$$\beta_y = \frac{(-1)^{r\cdot y}}{2^{\frac{n-1}{2}}}$$

Case 2 $\quad y \cdot s \equiv 1 \pmod 2$

$$\beta_y = 0.$$

$$\beta_y = \frac{1}{\sqrt{2}} \frac{(-1)^{r\cdot y}}{2^{n/2}} + \frac{1}{\sqrt{2}} \frac{(-1)^{(r \oplus s)\cdot y}}{2^{n/2}}$$

$$= \frac{(-1)^{r\cdot y}}{2^{\frac{n+1}{2}}} \left[\underbrace{1 + (-1)^{s\cdot y}} \right]$$

Reconstructing s:

$$\begin{cases} y_1^{(1)} s_1 + y_2^{(1)} s_2 + \cdots + y_n^{(1)} s_n = 0 \\ y_1^{(2)} s_1 + y_2^{(2)} s_2 + \cdots + y_n^{(2)} s_n = 0 \\ \vdots \\ y_1^{(n-1)} s_1 + y_2^{(n-1)} s_2 + \cdots + y_n^{(n-1)} s_n = 0 \end{cases}$$

$$\boxed{1 - \frac{1}{2^{n-1}}}$$

$$P[\text{bad}] = \frac{1}{2^{n-1}} = \frac{1}{2^{n-1}}$$

$$P[\text{bad}] = \frac{2}{2^{n-1}} = \frac{1}{2^{n-2}}$$

$$P[\text{bad}] = \frac{4}{2^{n-1}}$$

$$\vdots$$

$$1/4$$

$$\leq \frac{1}{2}$$

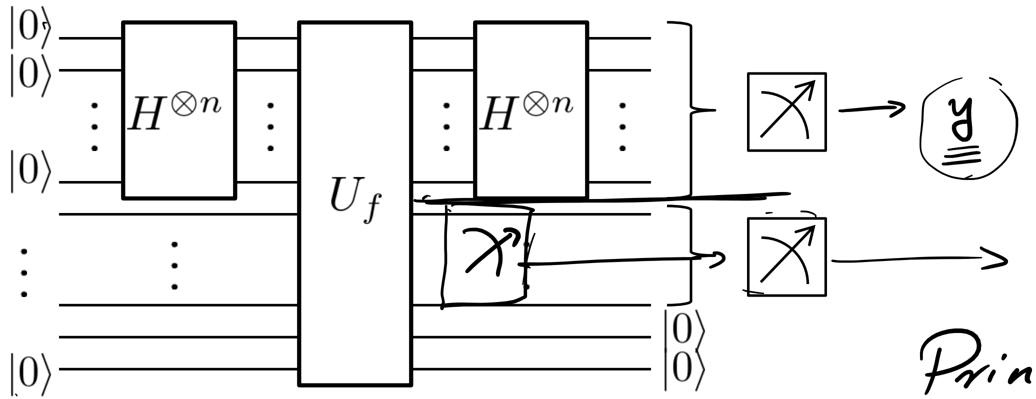
$$P[\text{bad}] = \frac{2^{n-2}}{2^{n-1}} = \frac{1}{2}$$

$$P[\text{good}] \geq \frac{1}{2} \cdot \frac{1}{2} = 1/4.$$

n-1 linear equs are independent. $\underline{\underline{S}}$ check.

Simon's algorithm

We are given a function $f : \{0,1\}^n \to \{0,1\}^n$ as a black box.
We know that f is a 2-1 function. (There is a secret string $s \in \{0,1\}^n$ such that $f(x) = f(x \oplus s)$)



Principle of deferred measurement.

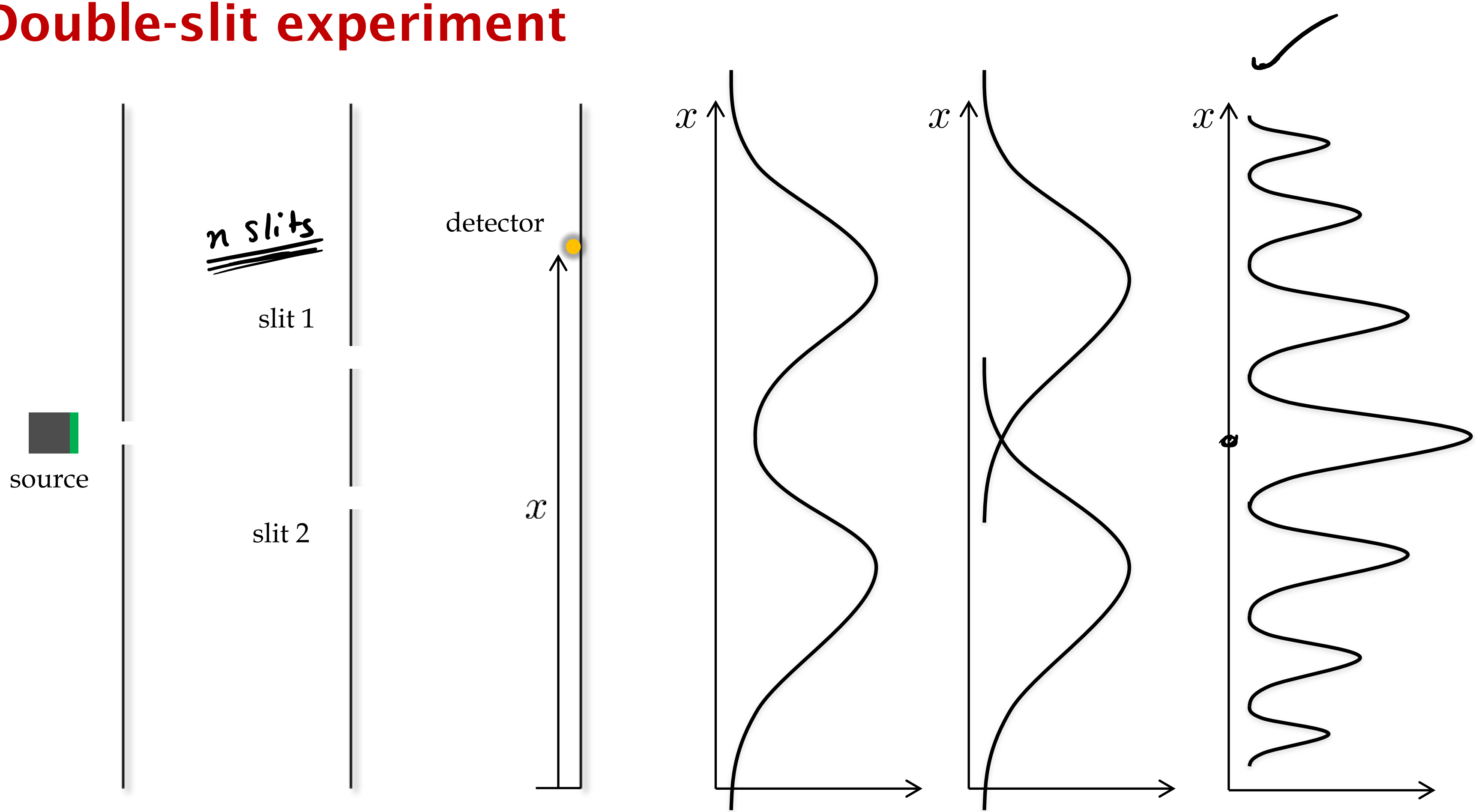
Quantum Mechanics & Quantum Computation

Umesh V. Vazirani
University of California, Berkeley

Lecture 8: Early Quantum Algorithms

2^n-slit experiment

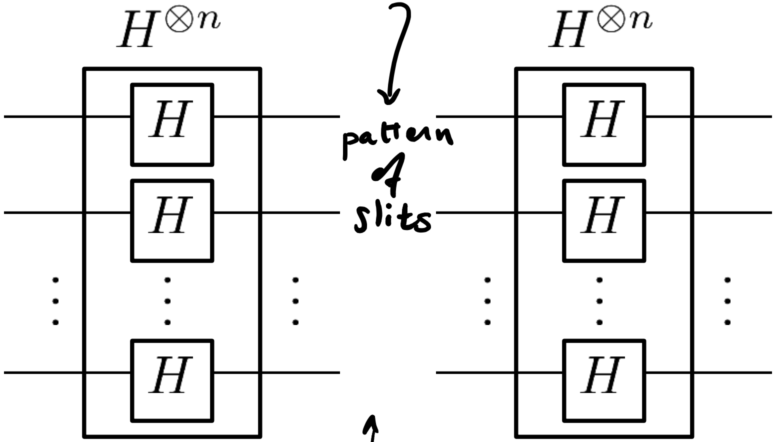
Double-slit experiment



Quantum algorithms

input

$|u\rangle$



pattern of slits

$\sum_{y} \beta_y |y\rangle$

$$\sum_{x\in\{0,1\}^n} \frac{(-1)^{u\cdot x}}{2^{n/2}} |x\rangle$$

virtual slits.

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

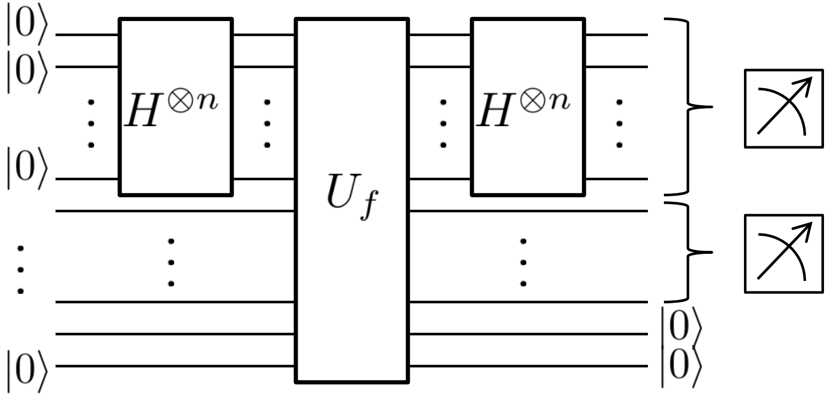
$$\boxed{\underline{\text{Case 1}} \quad u \neq y \qquad \beta_y = 0}$$

<u>Case 2</u> $\quad u = y$

$$\sum_x \frac{1}{2^n} = 1.$$

U_f & virtual slits

We are given a function $f : \{0,1\}^n \to \{0,1\}^n$ as a black box.
We know that f is a 2-1 function. (There is a secret string $s \in \{0,1\}^n$ such that $f(x) = f(x \oplus s)$)



Constructive :

y : $\underline{\underline{y}} \cdot s = 0$ ✓

Destructive

y : $y \cdot s = 1$.

$$\sum_x \frac{1}{2^{n/2}} |x\rangle |f(x)\rangle \longrightarrow \frac{1}{\sqrt{2}} |r\rangle + \frac{1}{\sqrt{2}} |r + \underline{\underline{s}}\rangle$$

↑ measure.

Quantum Mechanics & Quantum Computation

Umesh V. Vazirani
University of California, Berkeley

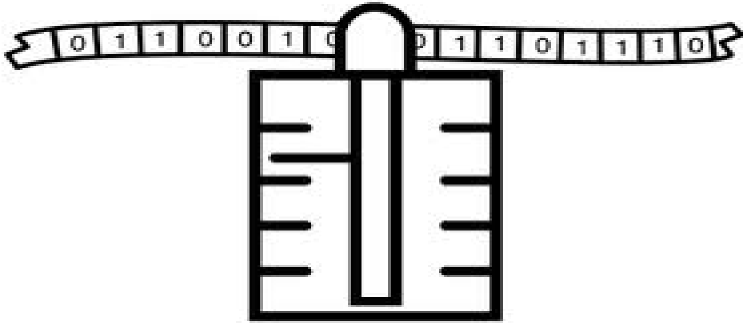
Lecture 8: Early Quantum Algorithms

Extended Church-Turing Thesis

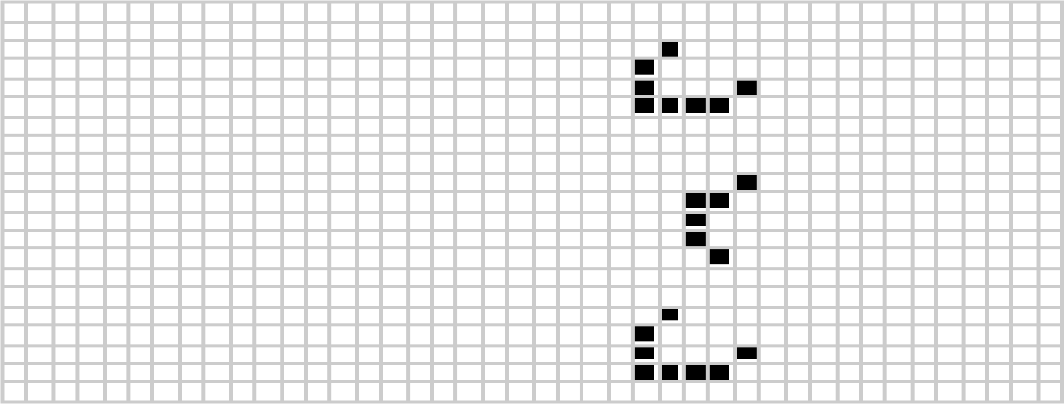
Extended Church-Turing Thesis

Any "reasonable" model of computation can be simulated on a (probabilistic) Turing Machine with at most polynomial simulation overhead.

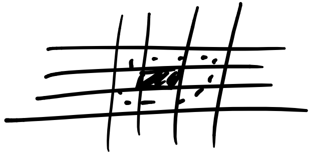
$\underline{\underline{T}}$ steps $\longrightarrow$ $\underline{\underline{O(T^2)}}$.



Nature as a Computer



local diff equs. } discretize.



Cellular Automaton.

Quantum computation is the only model of computation that violates the Extended Church-Turing thesis.

Recursive Fourier Sampling

Simon's Alg.