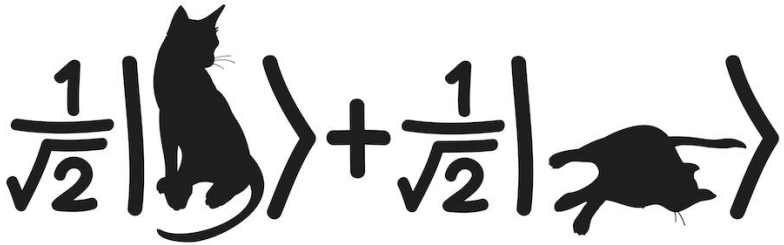
Quantum Mechanics & Quantum Computation

Umesh V. Vazirani
University of California, Berkeley



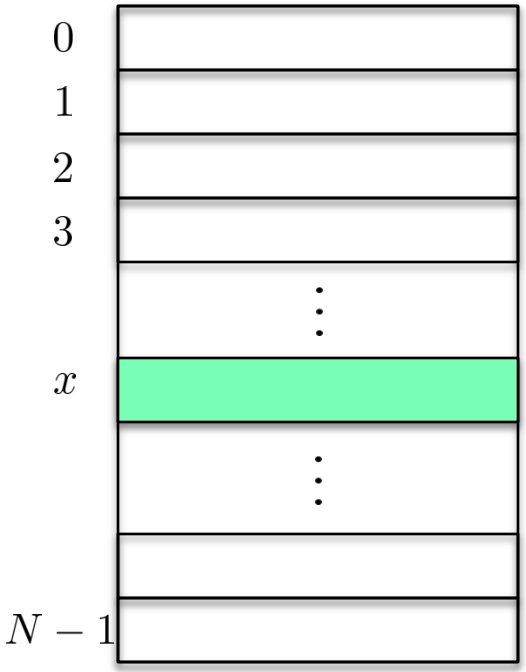
Lecture 15: Quantum Search

Needle in a haystack

Searching for a needle in a haystack

Unstructured search

"Digital haystack"



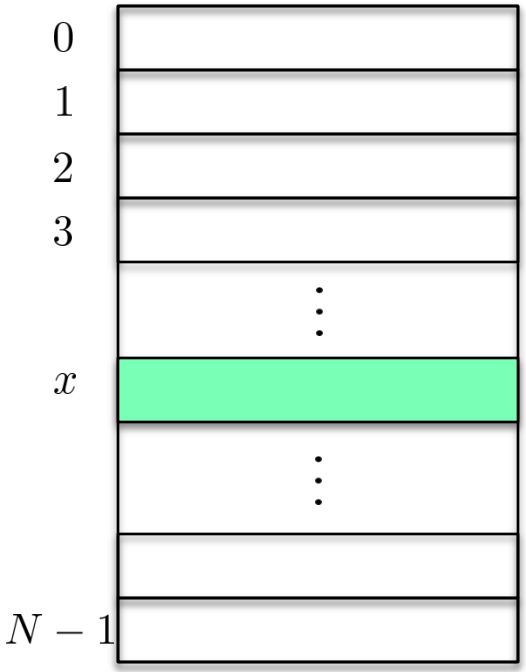
Goal: Search for the marked entry.

Classically: try random entries.
O(N/2) expected time.

Quantum??

Unstructured search

"Digital haystack"

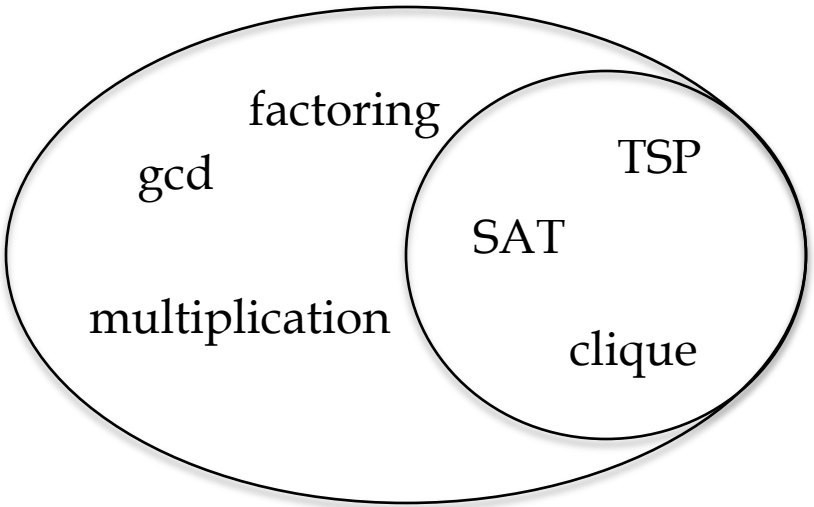


Quantum??

NP-Complete Problems:

What does it mean?

For most computational problems, finding an answer is very difficult, but checking an answer is easy.



Finding a solution to an NP-complete problem can be viewed as a search problem.

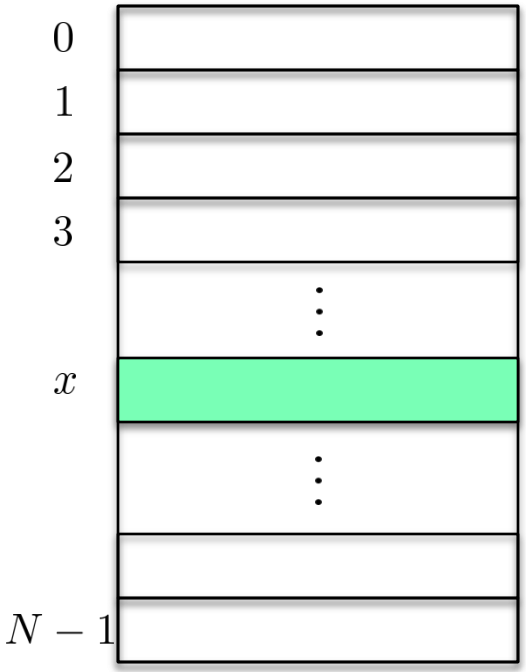
$$(x_1 \vee \neg x_2 \vee x_3) \wedge (x_2 \vee \neg x_5 \vee x_6) \wedge \cdots$$

Is there a configuration of $x_1, x_2, \cdots$ that satisfy the above formula?

There are 2^n possible configurations.

Unstructured search

"Digital haystack"



NP-Complete Problems:

Satisfiability:

Finding a solution to an NP-complete problem can be viewed as a search problem.

$$(x_1 \vee \neg x_2 \vee x_3) \wedge (x_2 \vee \neg x_5 \vee x_6) \wedge \cdots$$

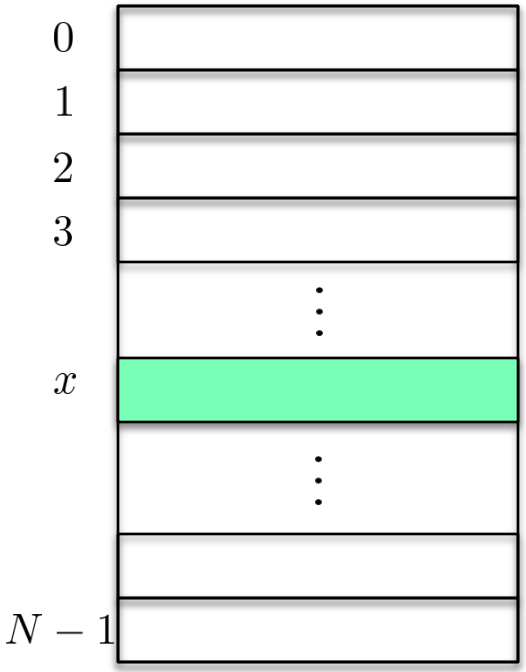
Is there a configuration of $x_1, x_2, \cdots$ that satisfy the above formula?

There are 2^n possible configurations.

$N = 2^n$

Unstructured search

"Digital haystack"



n qubits $\quad 2^n = N$

$$\frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} |y\rangle \rightarrow \boxed{U_f} \rightarrow |y\rangle, |f(y)\rangle$$

Random y

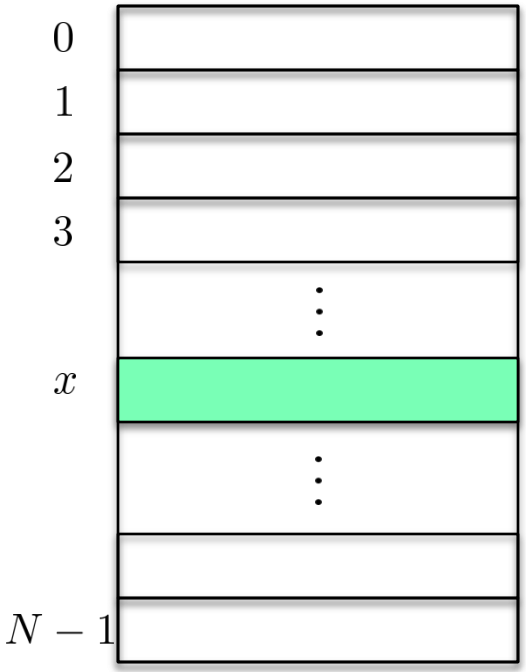
No better than probing random entry!!

$$f(x_1, x_2 \ldots x_n) = (x_1 \vee \bar{x}_2 \vee x_3) \wedge (\quad) \wedge (\quad) \ldots \wedge (\quad)$$

Unstructured search

$N = 2^n$

"Digital haystack"



Goal: Search for the marked entry.

Classically: try random entries.
O(N/2) expected time.

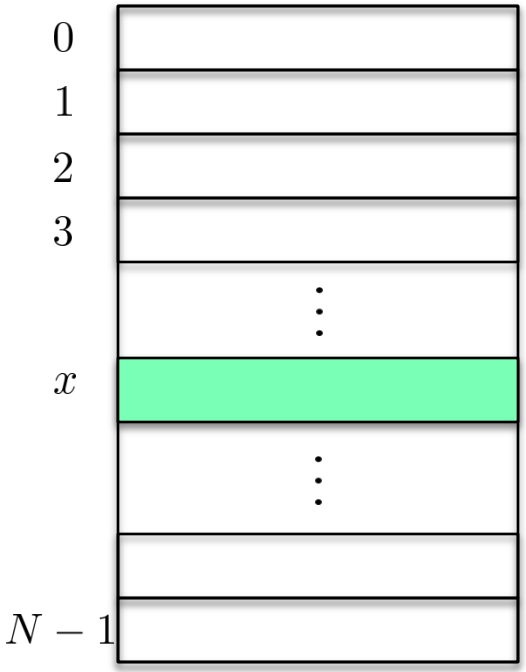
Quantum??

Theorem: Any quantum algorithm must take at least $\sqrt{N}$ time.

$= 2^{n/2}$

Unstructured search

"Digital haystack"



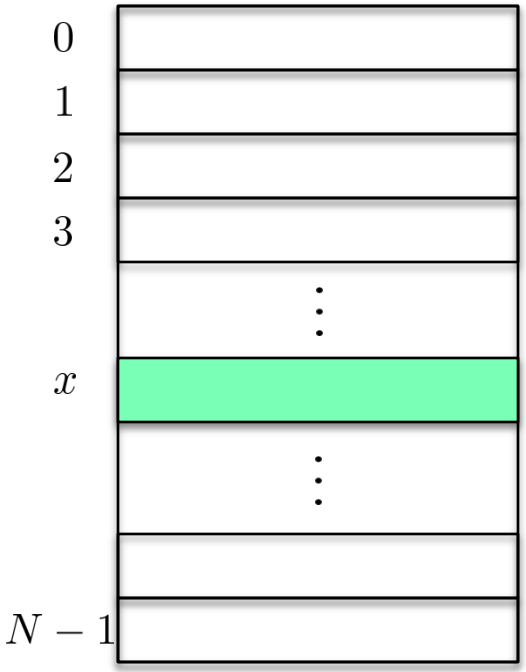
Quantum??

Theorem: Any quantum algorithm must take at least $\sqrt{N}$ time.

Grover's Algorithm: Quantum algorithm for unstructured search that takes $O(\sqrt{N})$ time.

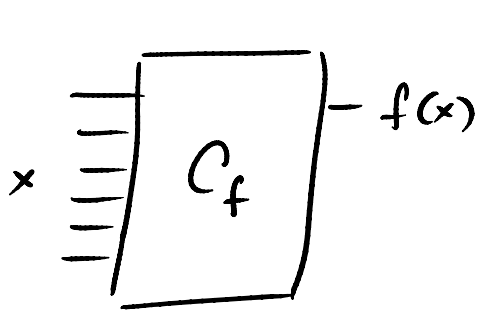
Unstructured search

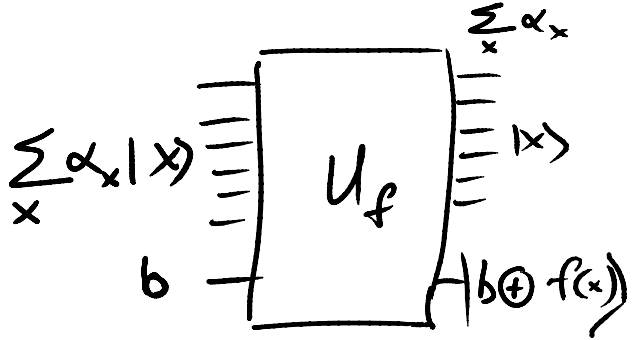
"Digital haystack"



Problem. Given f:{0, 1, …, N–1} → {0,1}, find x: f(x) = 1.

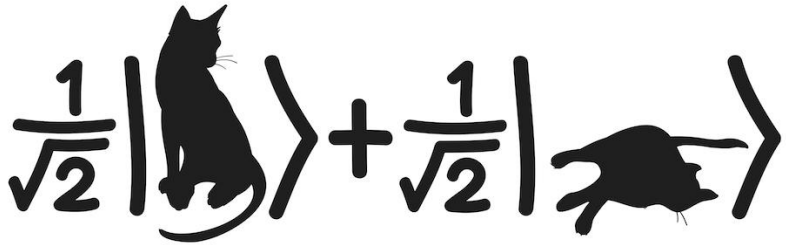
Hardest case: There is exactly one x: f(x) = 1.





Quantum Mechanics & Quantum Computation

Umesh V. Vazirani
University of California, Berkeley



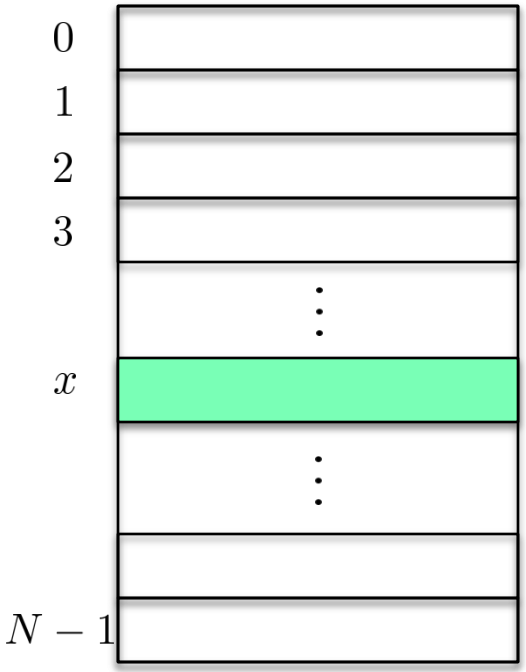
Lecture 15: Quantum Search

Grover's Algorithm

Unstructured search

$N = 2^n$

"Digital haystack"



Problem. Given f:{0, 1, …, N–1} → {0,1}, find x: f(x) = 1.

Hardest case: There is exactly one x: f(x) = 1.

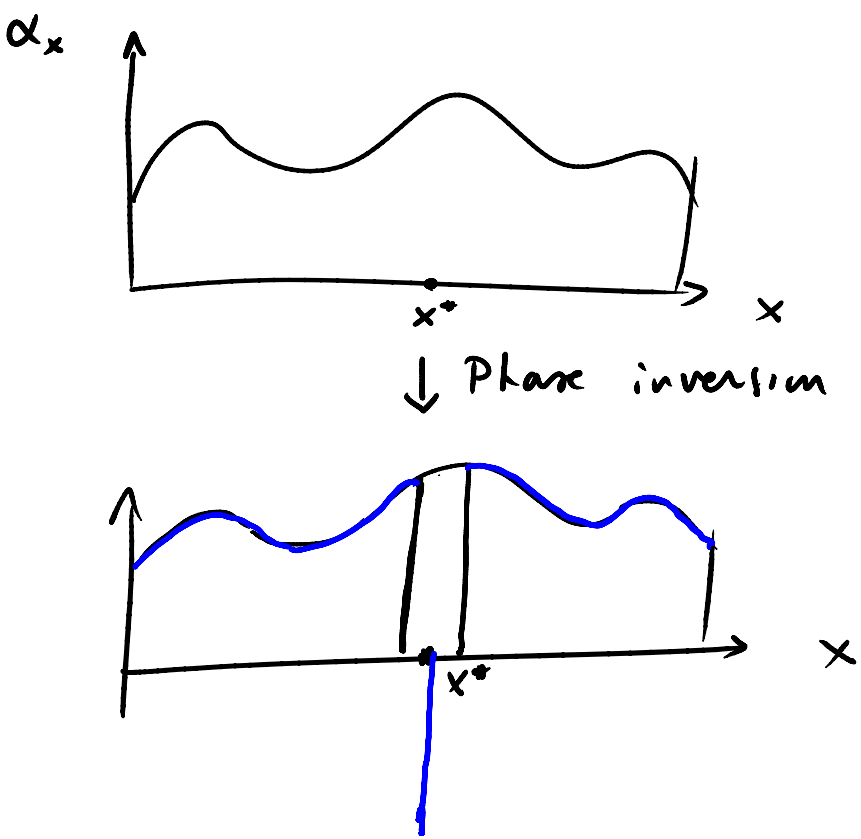
Phase Inversion

$f(x^*) = 1$

$\sum_x \alpha_x |x\rangle$

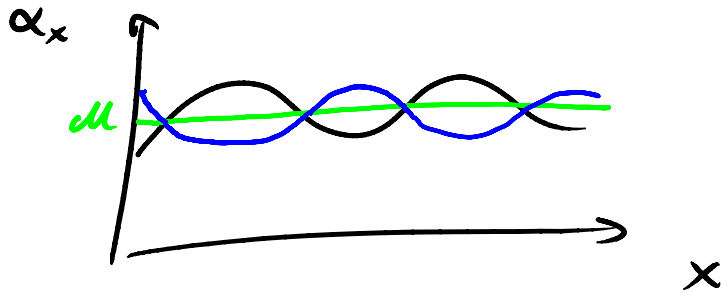
↓ Phase inversion

$\sum_{x \neq x^*} \alpha_x |x\rangle - \alpha_{x^*} |x^*\rangle$



Inversion About Mean

$$\sum_x \alpha_x |x\rangle$$



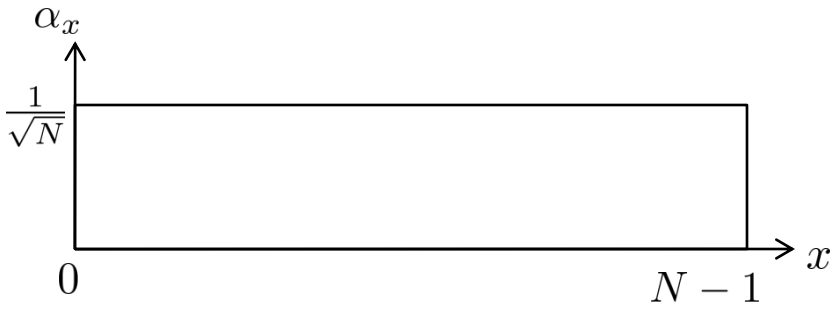
$$\sum_x (2m - \alpha_x)|x\rangle$$

$$\alpha_x \longrightarrow m + (m - \alpha_x)$$

$$m - \alpha_x$$

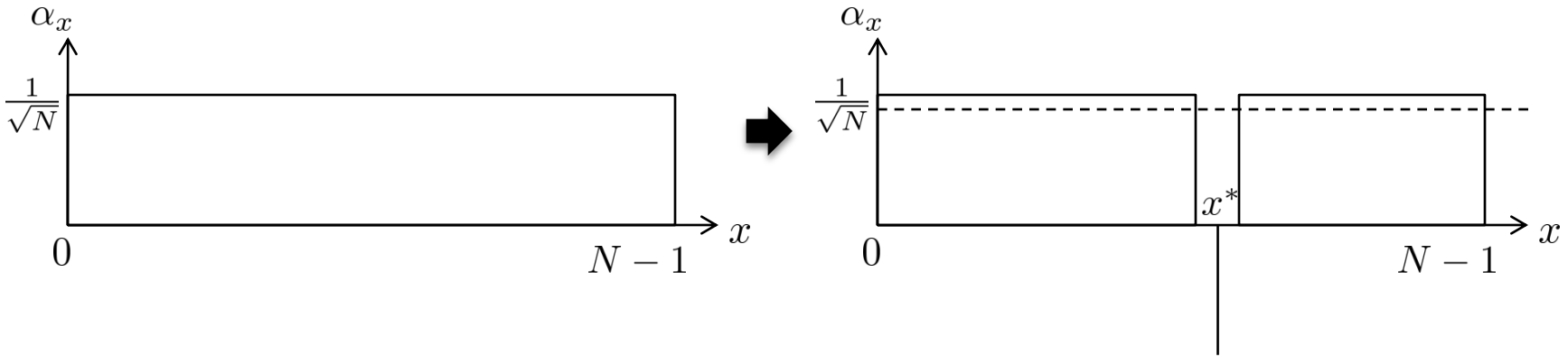
Grover's algorithm

Problem. Given $f : \{0, \ldots, N-1\} \to \{0, 1\}$ such that $f(x) = 1$ for exactly one x, find x.



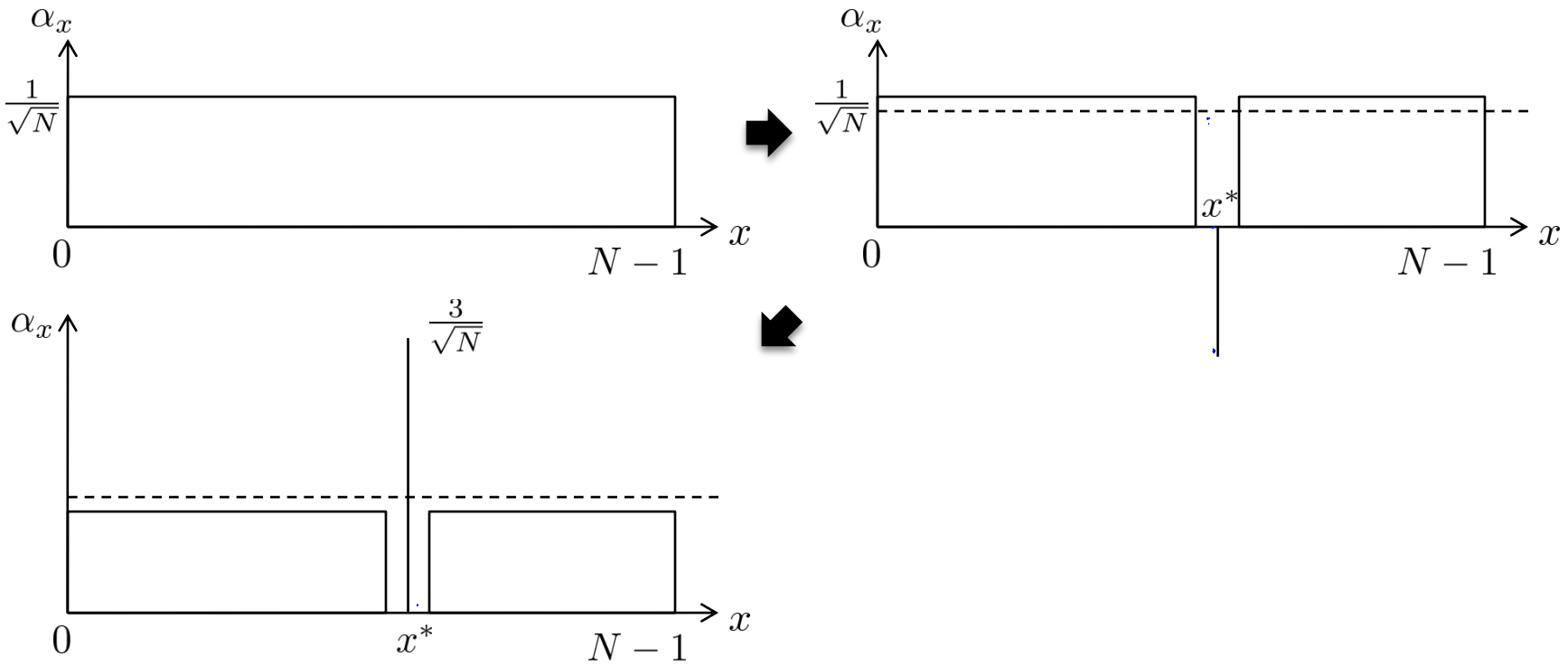
Grover's algorithm

Problem. Given $f : \{0, \ldots, N-1\} \to \{0, 1\}$ such that $f(x) = 1$ for exactly one x, find x.



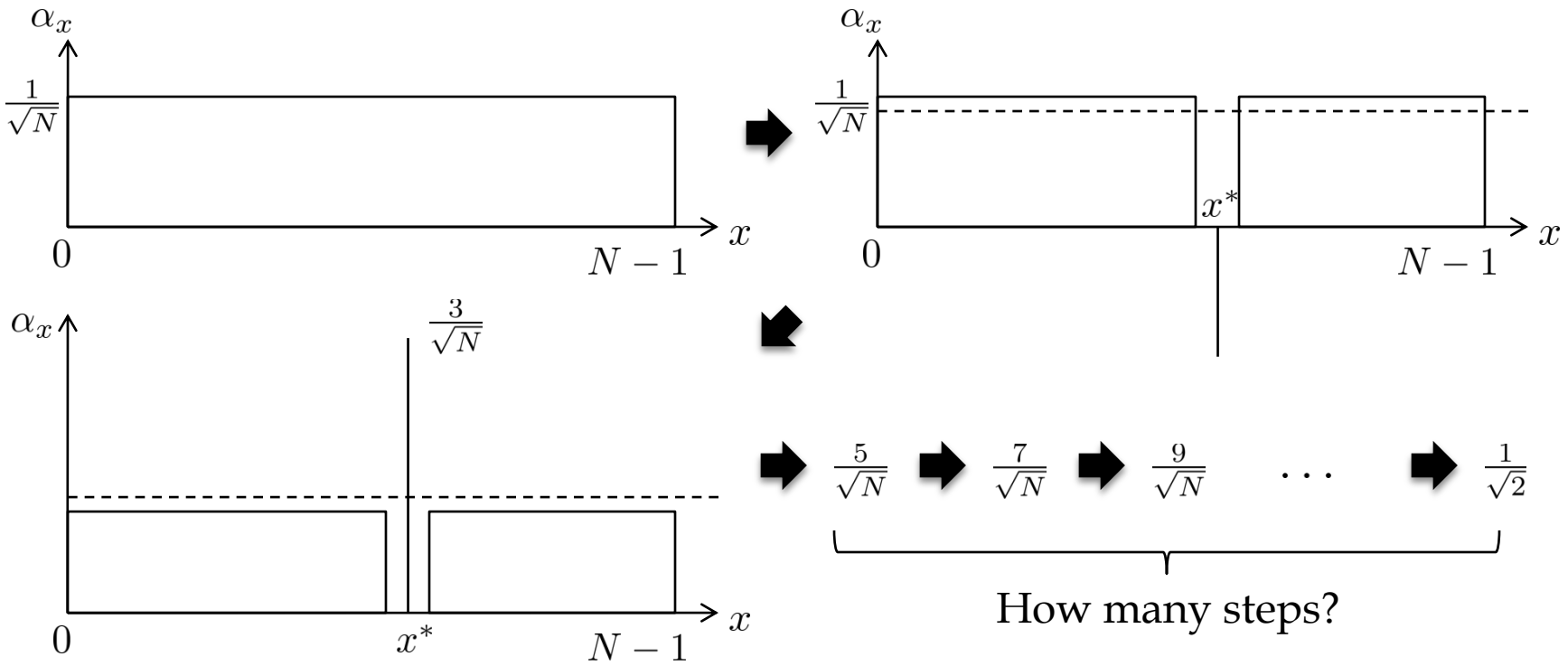
Grover's algorithm

Problem. Given $f : \{0, \ldots, N-1\} \to \{0, 1\}$ such that $f(x) = 1$ for exactly one x, find x.



Grover's algorithm

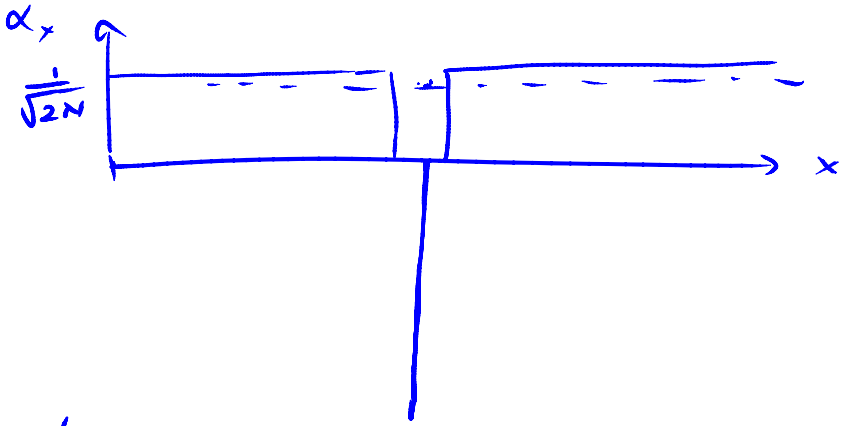
Problem. Given $f : \{0, \ldots, N-1\} \to \{0, 1\}$ such that $f(x) = 1$ for exactly one x, find x.



Grover's algorithm

What is the amplitude of the rest when the needle has $\frac{1}{\sqrt{2}}$? $\frac{1}{\sqrt{2N}}$

At this point how much improvement are we making per step? $2 \times \frac{1}{\sqrt{2N}} = \sqrt{\frac{2}{N}}$

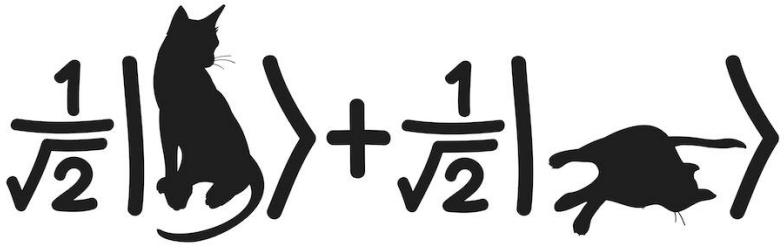


We will reach $\frac{1}{\sqrt{2}}$ in $O(\sqrt{N})$ steps.

$\frac{1/\sqrt{2}}{\sqrt{2}/\sqrt{N}} = \frac{\sqrt{N}}{2}$ steps.

Quantum Mechanics & Quantum Computation

Umesh V. Vazirani
University of California, Berkeley

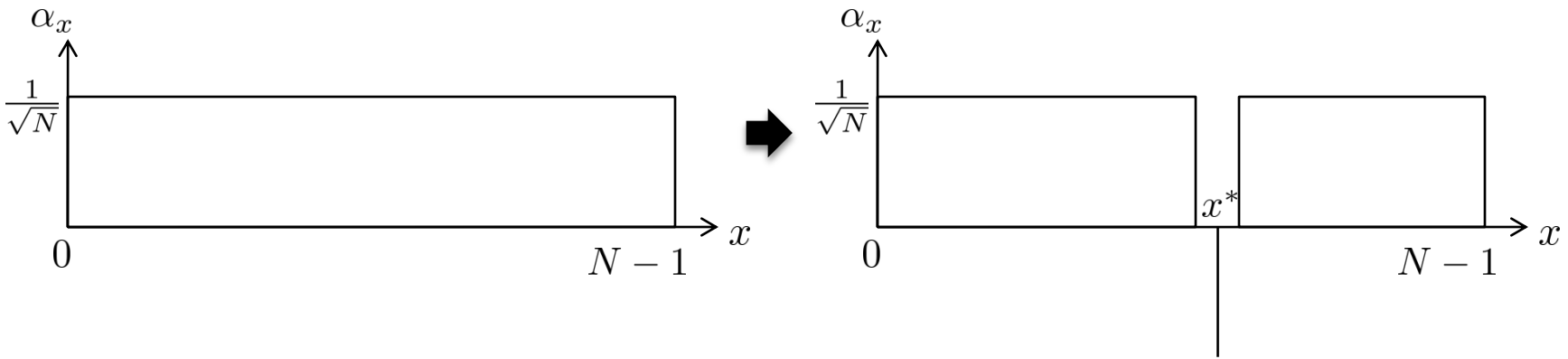


Lecture 15: Quantum Search

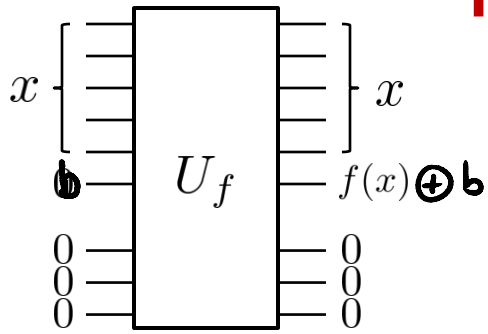
Implementing Grover's Algorithm

Phase Inversion

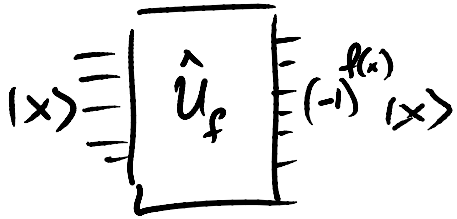
Problem. Given $f : \{0, \ldots, N-1\} \to \{0, 1\}$ such that $f(x) = 1$ for exactly one x, find x.



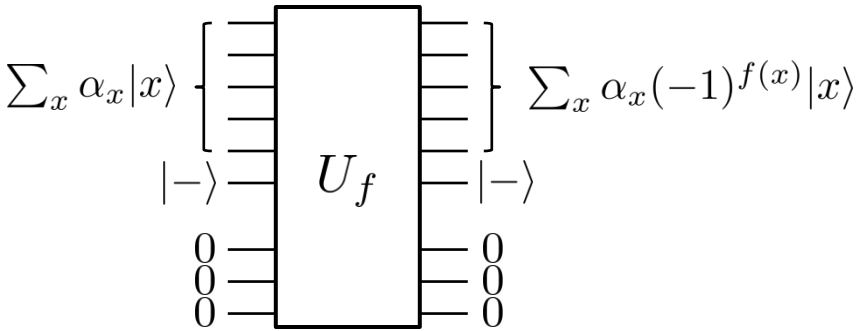
Phase Inversion

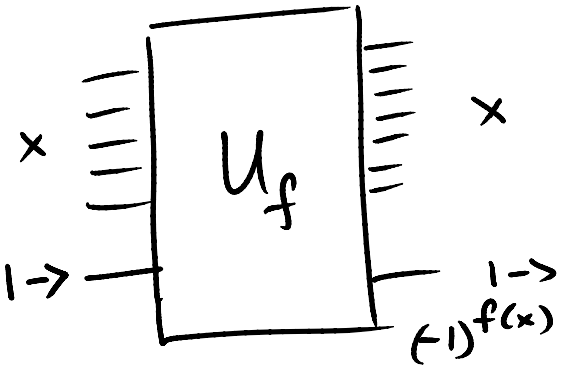


How do we send f(x) to the phase?



$$\sum_x \alpha_x |x\rangle \rightarrow \sum_x (-1)^{f(x)} \alpha_x |x\rangle$$





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

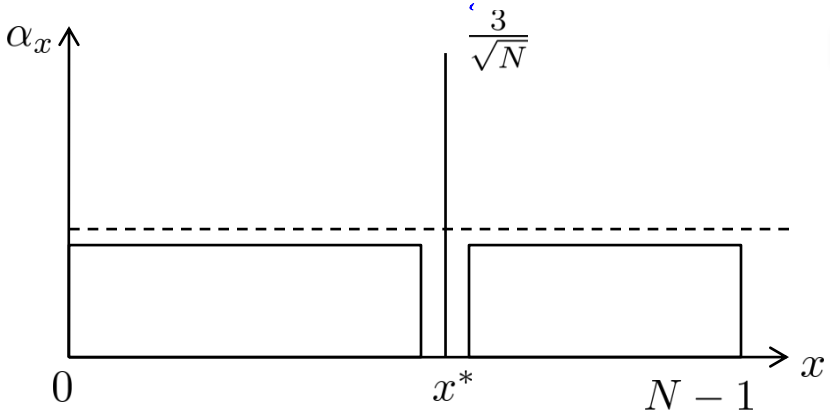
$|-\rangle \rightarrow \frac{1}{\sqrt{2}}|1\rangle - \frac{1}{\sqrt{2}}|0\rangle$

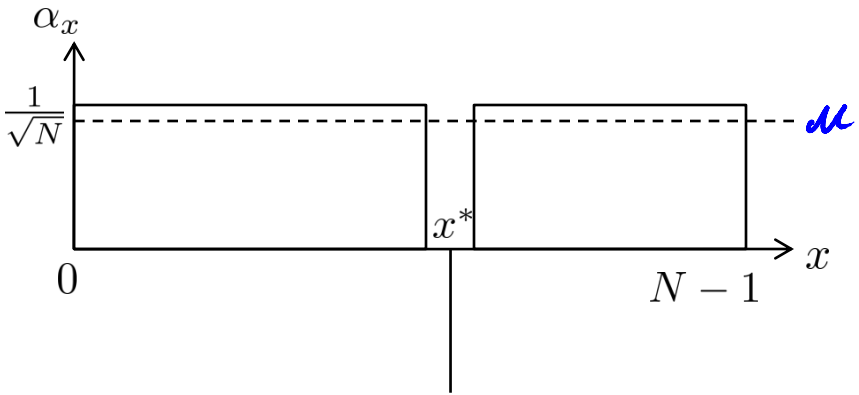
Case 1: $f(x)=0$ $\quad |-\rangle \rightarrow |-\rangle$ $\quad$ Case 2: $f(x)=1$ $\quad = -|-\rangle$

Reflection About Mean

$$\sum_x \alpha_x |x\rangle$$

$$\mu = \frac{\sum \alpha_x}{N}$$

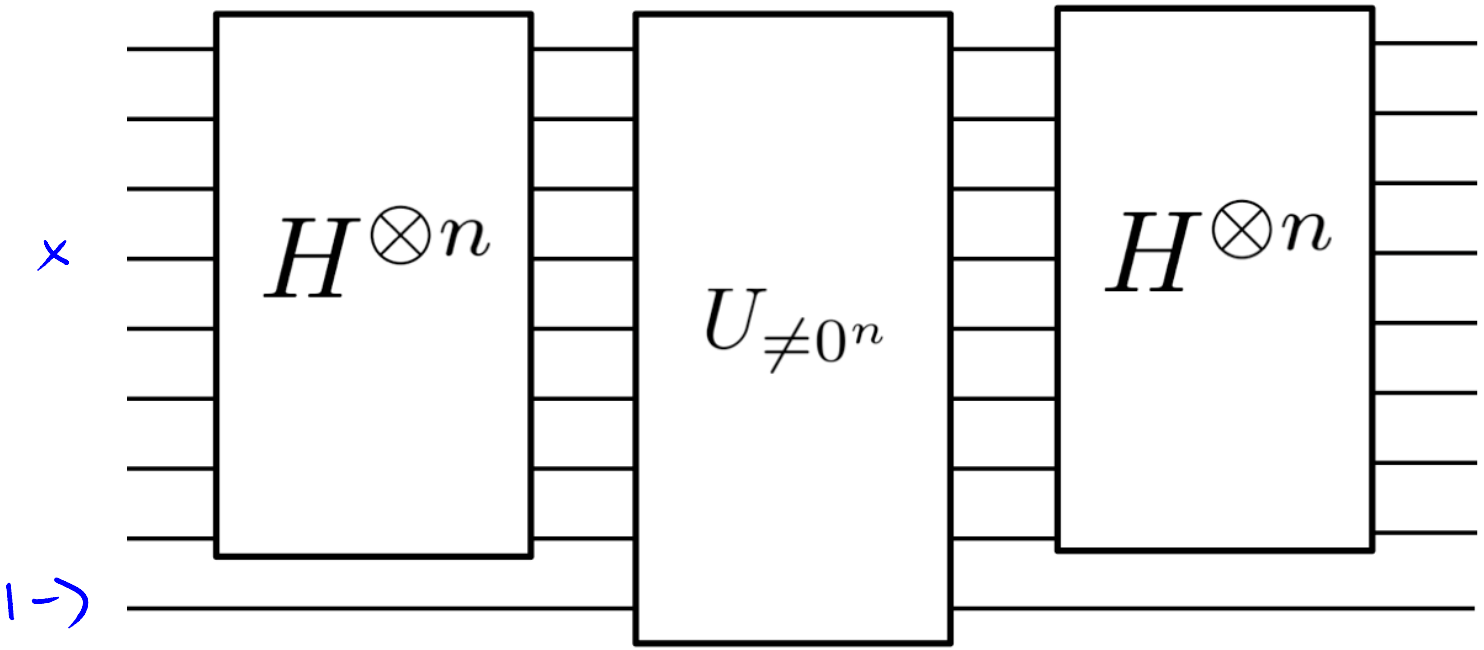




$$\sum_x (2\mu - \alpha_x)|x\rangle$$

Reflection About Mean

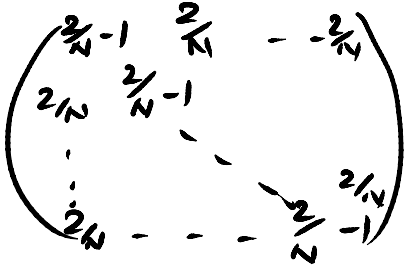
$$g(x) = \begin{cases} 0 & \text{if } x = 0\cdots0 \\ 1 & \text{o.w.} \end{cases}$$



Reflection about the mean is the same as doing reflection about $|u\rangle = \frac{1}{\sqrt{N}} \sum_x |x\rangle$

$$H^{\otimes n} \begin{pmatrix} 1 & & & \\ & -1 & & \\ & & \ddots & \\ & & & -1 \end{pmatrix} H^{\otimes n}$$

$|0\cdots0\rangle$



$$= H^{\otimes n} \left[\begin{pmatrix} 2 & & \\ & \ddots & \\ & & 0 \end{pmatrix} - \begin{pmatrix} 1 & & \\ & \ddots & \\ & & 1 \end{pmatrix} \right] H^{\otimes n}$$

$$= H^{\otimes n} \begin{pmatrix} 2 & & \\ & \ddots & \\ & & 0 \end{pmatrix} H^{\otimes n} - \underbrace{H^{\otimes n} I H^{\otimes n}}_{I} = \begin{pmatrix} \frac{2}{N} & \frac{2}{N} & \cdots & \frac{2}{N} \\ \frac{2}{N} & & & \\ \vdots & & & \\ \frac{2}{N} & \cdots & \cdots & \frac{2}{N} \end{pmatrix} - I$$

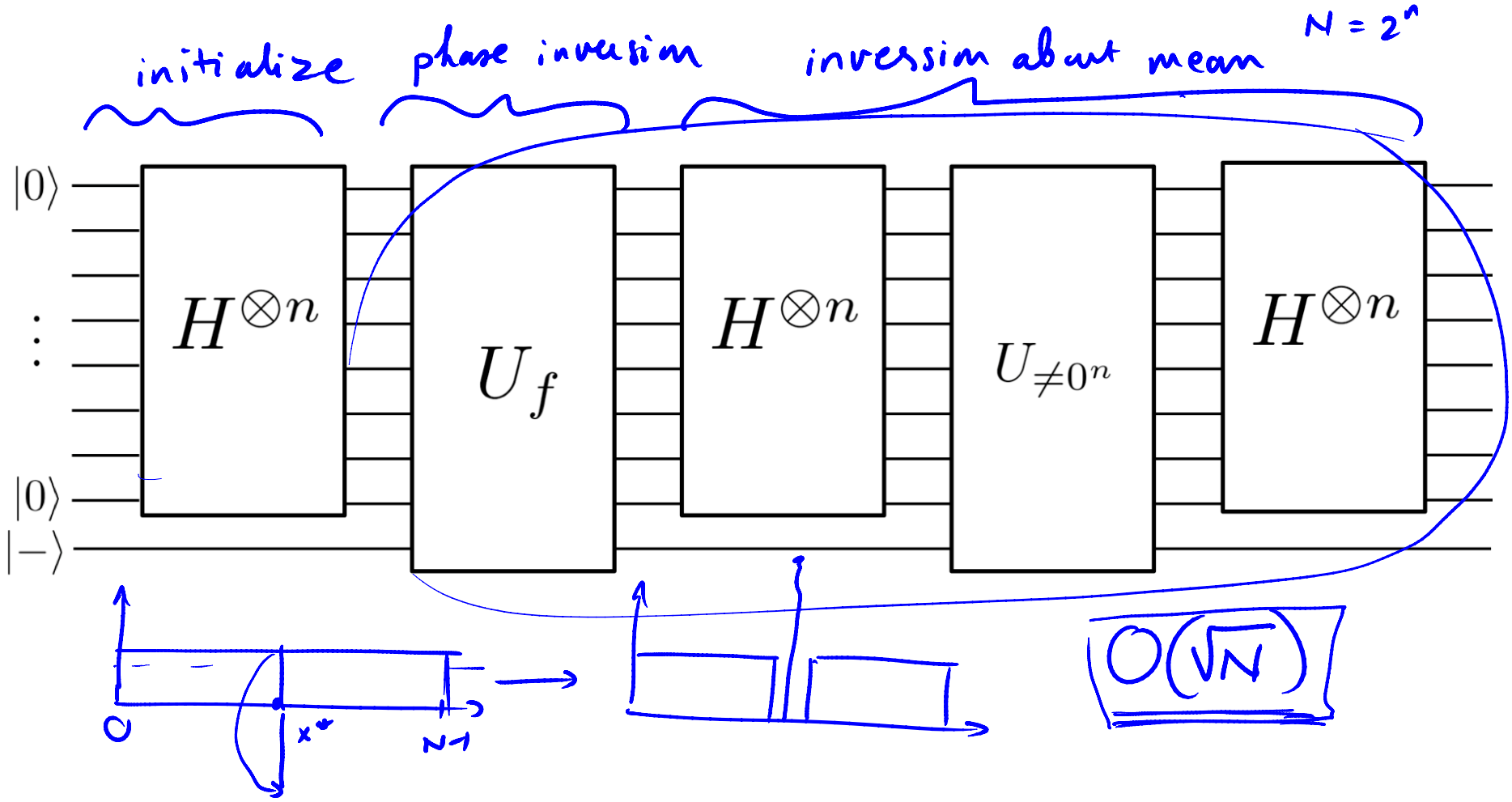
Reflection about the mean is the same as doing reflection about $|u\rangle = \frac{1}{\sqrt{N}} \sum_x |x\rangle$

$$H^{\otimes n} \begin{pmatrix} 1 & & 0 \\ & -1 & \\ & & \ddots \\ 0 & & -1 \end{pmatrix} H^{\otimes n} = \begin{pmatrix} \frac{2}{N}-1 & \frac{2}{N} & \cdots & \frac{2}{N} \\ \frac{2}{N} & \ddots & & \\ \vdots & & \ddots & \frac{2}{N} \\ \frac{2}{N} & & \frac{2}{N} & \frac{2}{N}-1 \end{pmatrix} \begin{pmatrix} \alpha_0 \\ \vdots \\ \alpha_{N-1} \end{pmatrix}$$

$$\sum_x \alpha_x |x\rangle \longrightarrow \sum_x (2\mu - \alpha_x)|x\rangle = \begin{pmatrix} 2\mu - \alpha_0 \\ 2\mu - \alpha_1 \\ \vdots \\ 2\mu - \alpha_{N-1} \end{pmatrix}$$

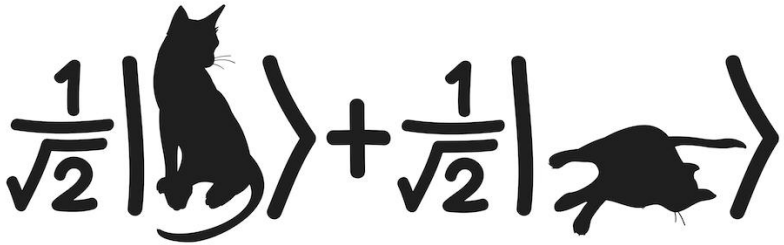
$$\frac{2}{N}(\alpha_0 + \alpha_1 + \cdots + \alpha_{N-1})$$

$$= 2\mu$$


initialize
phase inversion
inversion about mean
$N = 2^n$
$|0\rangle$
$|0\rangle$
$|-\rangle$
$H^{\otimes n}$
U_f
$H^{\otimes n}$
$U_{\neq 0^n}$
$H^{\otimes n}$
0
x^*
N-1
$O(\sqrt{N})$

Quantum Mechanics & Quantum Computation

Umesh V. Vazirani
University of California, Berkeley

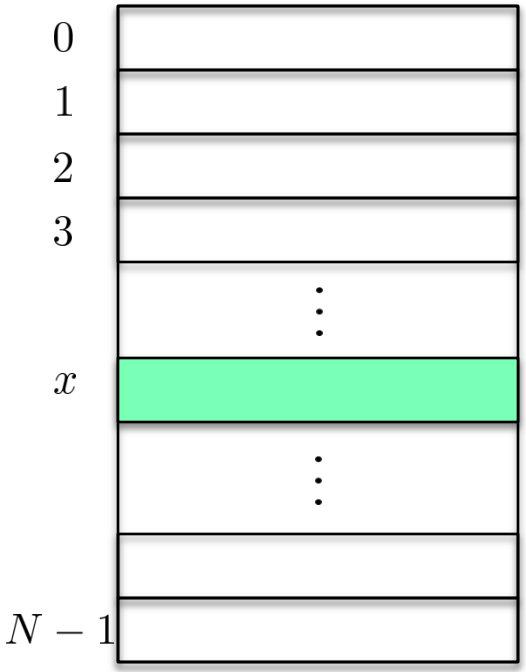


Lecture 16: Quantum Complexity Theory

Lower bound for quantum search

Unstructured search

"Digital haystack"

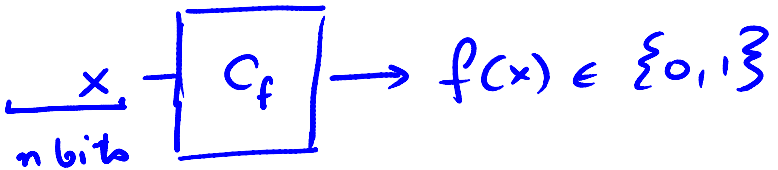


$N = 2^n$

Goal: Search for the marked entry.

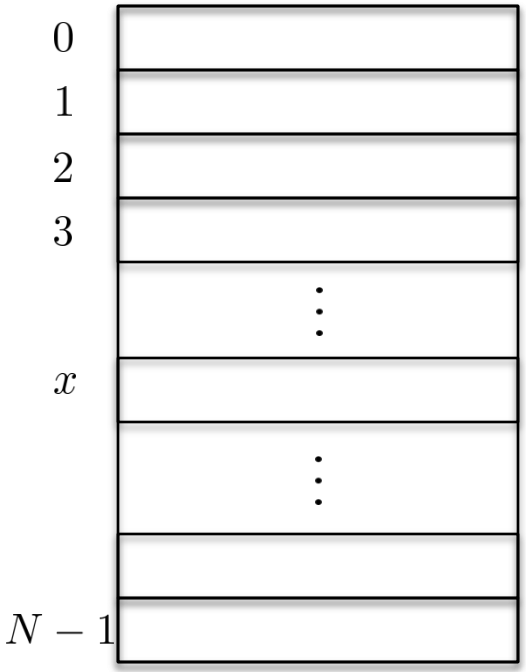
Theorem: Any quantum algorithm must take at least $\sqrt{N}$ time. queries

$= 2^{n/2}$



Unstructured search

"Digital haystack"



1 quantum query: no algorithm can guarantee success probability > c/N.

Perform test run with empty haystack.
Suppose algorithm makes query

$\sum_x \alpha_x |x\rangle$ $\quad \sum |\alpha_x|^2 = 1$

$|\alpha_x|^2 \leq \frac{1}{N}$.

Place needle in location that gets queried with minimum squared amplitude.

amplitude queries $x^* \leq \frac{1}{\sqrt{N}}$

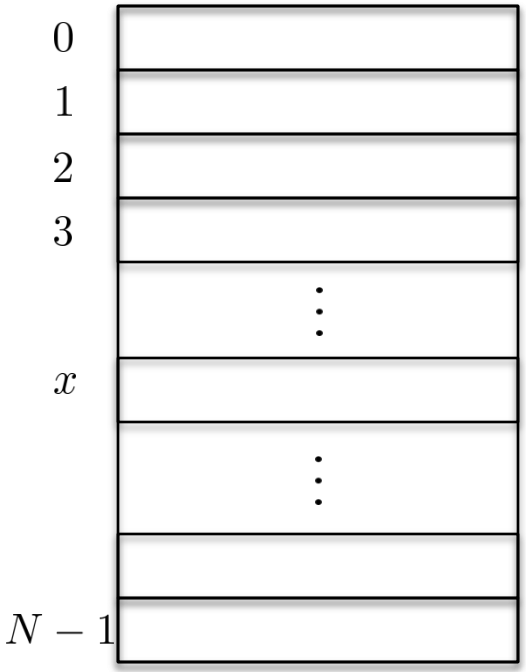
Unstructured search

t quantum queries:

Quantum Alg: t steps

$P[\text{success}] = \frac{O(t^2)}{N}$.

"Digital haystack"



Perform test run with empty haystack.

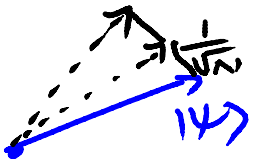
Place needle in location that gets queried with minimum squared amplitude.

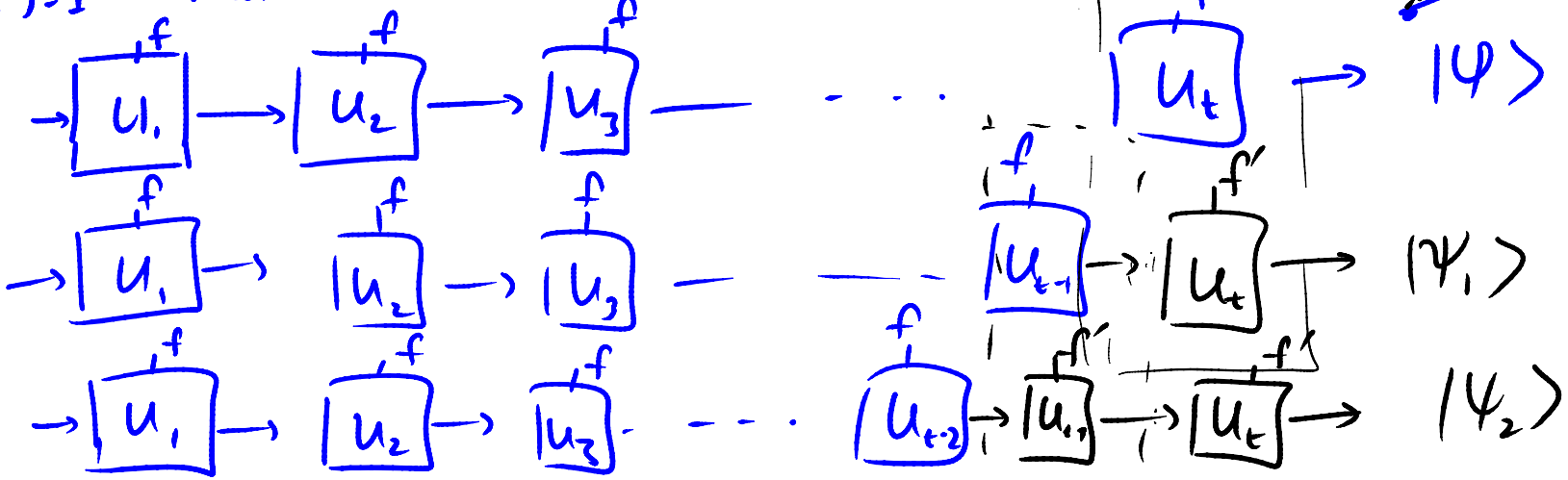
But subsequent queries amplitudes can change depending on previous answers.

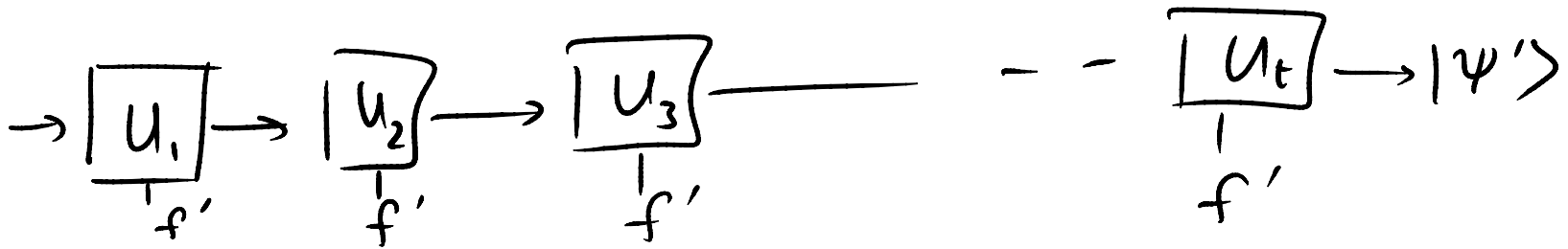
$f \equiv 0$ test run.

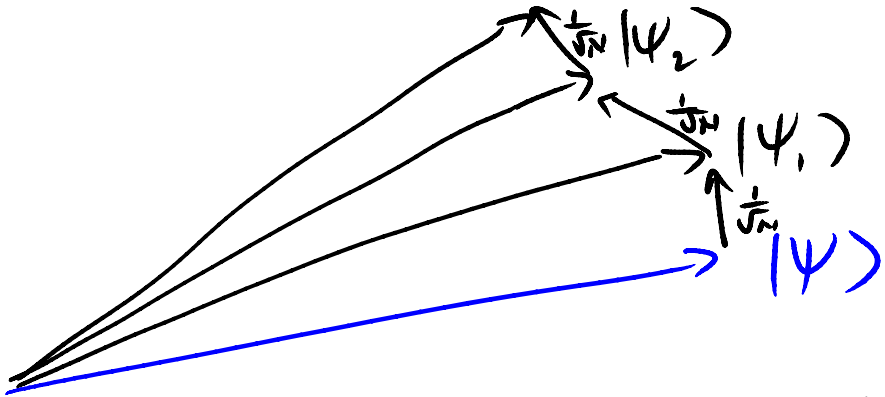
$f'(x^*) = 1$ real run.

Hybrid Argument









$\frac{t}{\sqrt{N}}$

Prob changes by $O\left(\frac{t^2}{N}\right)$.

Does this mean quantum computers cannot solve NP-complete problems in polynomial time? No.

Not necessarily. But it does mean that any quantum algorithm must use the structure of the problem.

[Farhi, et. al. Science 2001] Framework of adiabatic quantum optimization. Simulations on small examples seemed to show polynomial time for random instances of 3SAT.

http://arxiv.org/pdf/quant-ph/0001106v1.pdf

Isn't this ruled out by previous lowerbound?

Quantum computing

Orion's belter

Feb 15th 2007 | VANCOUVER

From *The Economist* print edition

The world's first practical quantum computer is unveiled

AS CALIFORNIA is to the United States, so British Columbia is to Canada. Both are about as far south-west as you can go on their respective mainlands. Both have high-tech aspirations. And, although the Fraser Valley does not yet have quite the cachet of Silicon Valley, it may be about to steal a march on its southern neighbour. For, on February 13th, D-Wave Systems, a firm based in Burnaby, near Vancouver, announced the existence of the world's first practical quantum computer.

Exponential Speedup for NP-Complete Problems?

Economist.com

Quantum computing

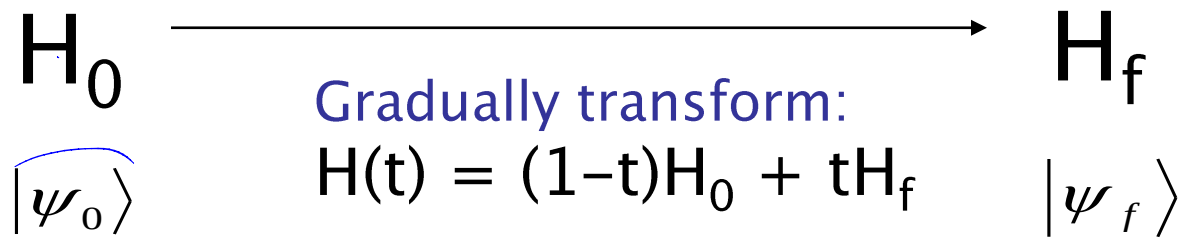
Orion's belter

Feb 15th 2007 | VANCOUVER

From *The Economist* print edition

Quantum computers provide a neat shortcut to solving a range of mathematical tasks known as NP-complete problems. They do so by encoding all possible permutations in the form of a small number of "qubits". In a normal computer, bits of digital information are either 0 or 1. In a quantum computer these normal bits are replaced by a "superposition" (the qubit) of both 0 and 1 that is unique to the ambiguous world of quantum mechanics. Qubits have already been created in the laboratory using photons (the particles of which light is composed), ions and certain sorts of atomic nuclei. By a process known as entanglement, two qubits can encode four different values simultaneously (00, 01, 10 and 11). Four qubits can represent 16 values, and so on. That means huge calculations can be done using a manageable number of qubits. In principle, by putting a set of entangled qubits into a suitably tuned magnetic field, the optimal solution to a given NP-complete problem can be found in one shot.

Adiabatic Quantum Optimization



E_0 = ground energy
E_1 = 1st excited "

$g = E_1 - E_0$

- How fast? $T = \frac{1}{Min_t\, g(t)^2}$ where g(t) is the difference between 2 smallest eigenvalues of H(t)

3SAT as a local Hamiltonian Problem

$$f(x_1,\cdots,x_n) = c_1 \wedge \cdots \wedge c_m$$

$H_f = H_1 + H_2 + \cdots + H_m$

- n bits ---> n qubits
- Clause $c_i = x_1 \vee x_2 \vee x_3$ corresponds to 8x8 Hamiltonian matrix acting on first 3 qubits:

$$h_i = \begin{pmatrix} 1 & & & & & & & \\ & 0 & & & & & & \\ & & 0 & & & & & \\ & & & 0 & & & & \\ & & & & 0 & & & \\ & & & & & 0 & & \\ & & & & & & 0 & \\ & & & & & & & 0 \end{pmatrix}$$

- Satisfying assignment is eigenvector with evalue 0.
- All truth assignments are eigenvectors with eigenvalue = # unsat clauses.

- How fast? $T = \frac{1}{Min_t\ g(t)^2}$ where g(t) is the difference between 2 smallest eigenvalues of H(t)

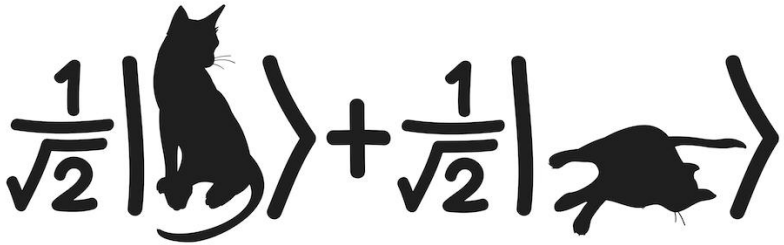
- Adiabatic optimization gives quadratic speedup for search, but exponential time in general: http://arxiv.org/pdf/quant-ph/0206003v1.pdf

- Exponential time for NP-complete problems, but can tunnel through local optima in certain special circumstances: http://ww2.chemistry.gatech.edu/~brown/QICS08/reichardt-adiabatic.pdf

- Anderson localization based arguments that it typically gets stuck in local optima: http://arxiv.org/pdf/0912.0746.pdf

Quantum Mechanics & Quantum Computation

Umesh V. Vazirani
University of California, Berkeley



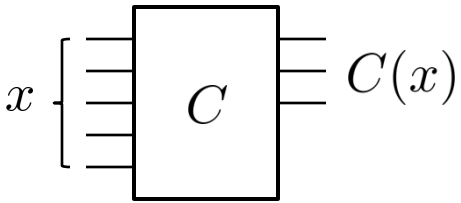
Lecture 16: Quantum Complexity Theory

BQP and Extended Church-Turing Thesis

Computational problems:
e.g. multiply matrices M, N.
test whether N is prime
write N as a product of prime factors.
is the boolean formula f(x) satisfiable?

A polynomial time algorithm is one that on inputs of size n, halts in time $O(n^k)$ for some constant k, and outputs the answer.

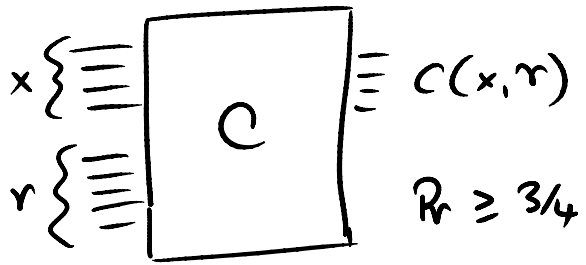
running time ≡ size of C



A polynomial time algorithm is one that on inputs of size n, halts in time $O(n^k)$ for some constant k, and outputs the answer.

The class P or polynomial time, is the class of all computational problems with polynomial time algorithms.

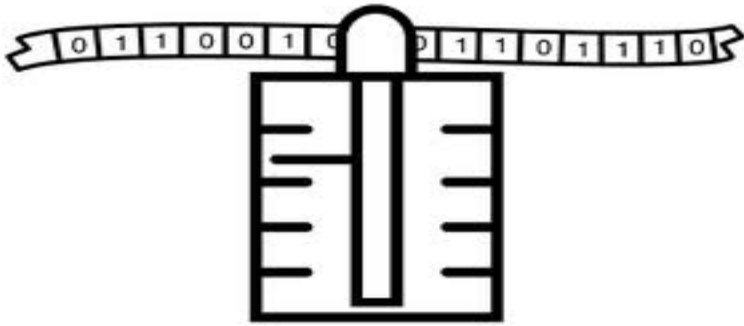
The class BPP, or bounded error probabilistic polynomial time, is the class of computational problems which have polynomial time randomized algorithms that output the correct answer with high probability.



Polynomial time good,
Exponential time bad!!

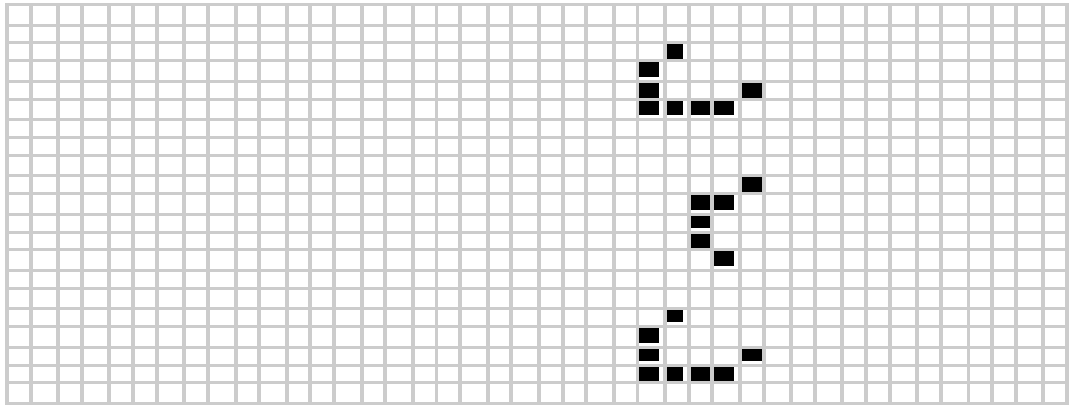
Extended Church-Turing Thesis

Any "reasonable" model of computation can be simulated on a (probabilistic) Turing Machine with at most polynomial simulation overhead. T steps $\rightarrow$ $O(T^2)$

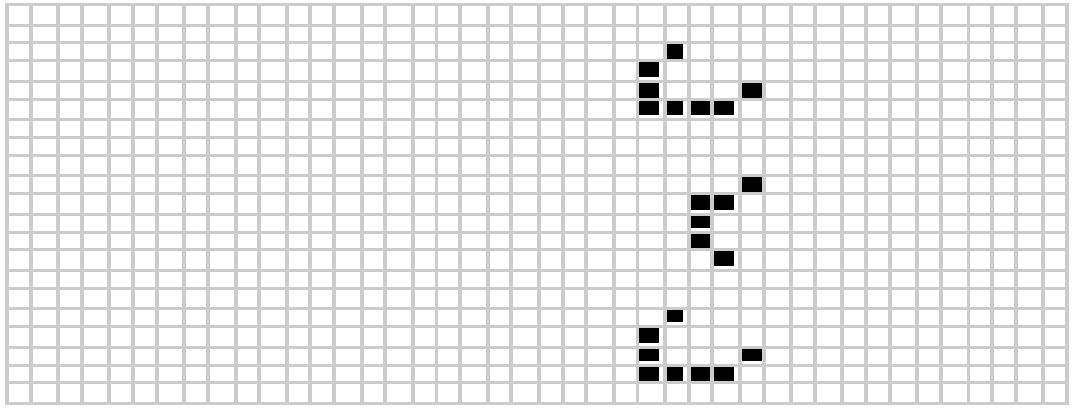


- Turing Machine describes the set of functions that are humanly computable. i.e. the class P describes what you could compute with an unlimited amount of pape at your disposal.

- The class P represents what can be physically computed.



Nature as a Computer



Classical physics — local differential equations

Cellular automata discretization of LDE. ⊙
digital abstraction.

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

Evidence:

Black box separations:
Recursive fourier sampling
Simon's problem.

Breaks cryptography:
Factoring
Discrete logs

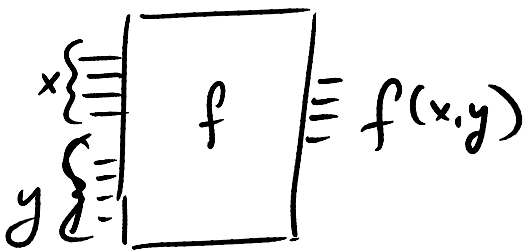
Why can't we prove an unconditional result?

The class BQP, or bounded error ~~probabilistic~~ quantum polynomial time, is the class of computational problems which have polynomial time quantum algorithms that output the correct answer with high probability.

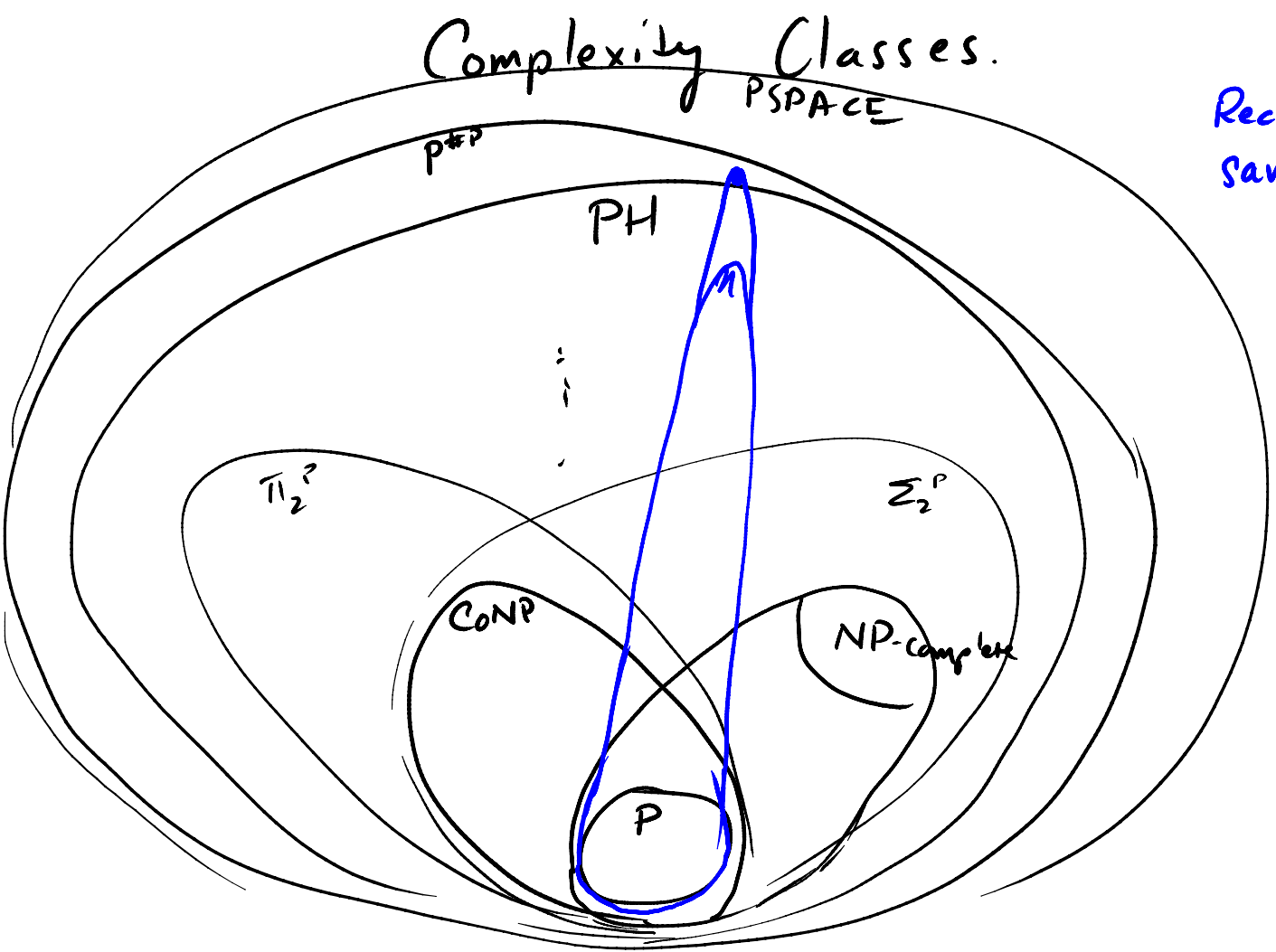
$$P \subseteq BPP \subseteq BQP \subseteq P^{\#P} \subseteq PSPACE$$

P vs PSPACE Open Question

#P counting class.



$$C(x) = \sum_y f(x,y)$$



Recursive fourier sampling : $\notin$ MA

Black box or oracle model

Could BQP contain problems much outside NP?

BQP vs PH: central open question in quantum complexity.

Conjecture (1993): Fourier sampling $\notin$ PH

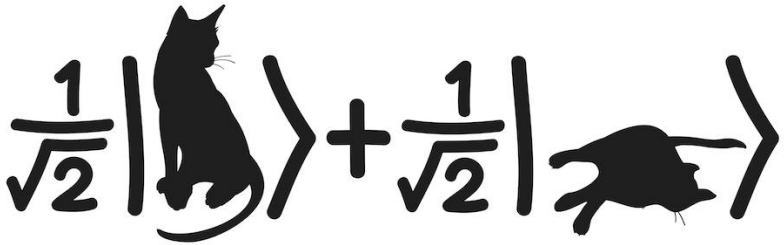
New conjecture: [Aaronson 09] Fourier checking $\notin$ PH
http://www.scottaaronson.com/papers/bqpph.pdf

v, w random unit vectors in R^N $N = 2^n$
Distinguish f = sgn(v) & g = sgn(Hv) from f = sgn(v) & g = sgn(w)
Where $f,g:\{0,1\}^n \rightarrow \{1,-1\}$

$K \rightarrow sgn(K)$

Quantum Mechanics & Quantum Computation

Umesh V. Vazirani
University of California, Berkeley



Lecture 16: Quantum Complexity Theory

Wrapping Up

- Course has been a learning experience for me
- Lecture format
- Multiple choice homeworks
- Scale

Seung Woo Shin

- Roughly the first eight weeks of the course we teach at Berkeley.
- The last four weeks of the course focus on physical implementation of qubits, quantum gates, measurements.
- We will try to offer a second segment of the course that includes that material.
- Other possible topics:
  - quantum cryptography
  - density matrices
  - decoherence
  - quantum error correction
  - quantum adiabatic algorithm

Survey:

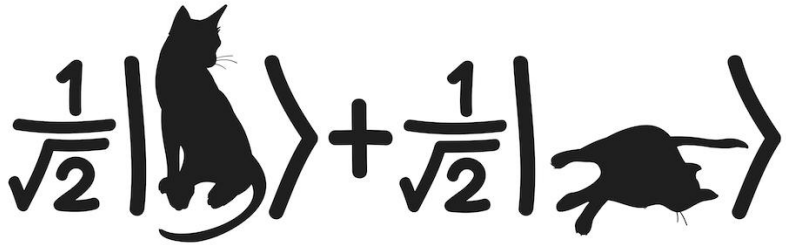
- About yourself

- About the course:
  - Level of difficulty
  - “just in time” approach to presenting math
  - Multiple choice Assignments

Survey:

- About the future:
  - Basic material, simple, concrete, easy to understand…
  - Discussion of and pointers to research results
  - Philosophical aspects: what is a measurement, …
  - Physical implementation
  - More CS: algorithms, complexity.
  - Assignments, exams

Quantum Mechanics & Quantum Computation



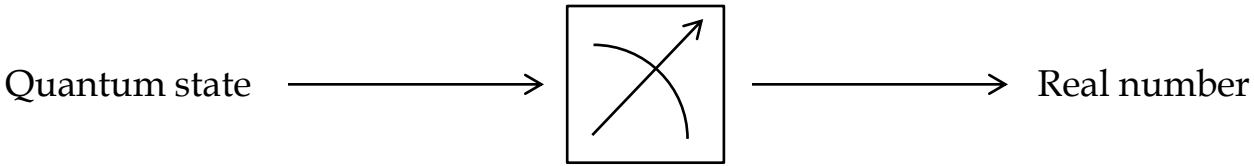
Umesh V. Vazirani
University of California, Berkeley

Lecture 7: Observables and Schrödinger's equation

Observables (part 1)

Observable

- An **observable** is a quantity like energy, position, momentum



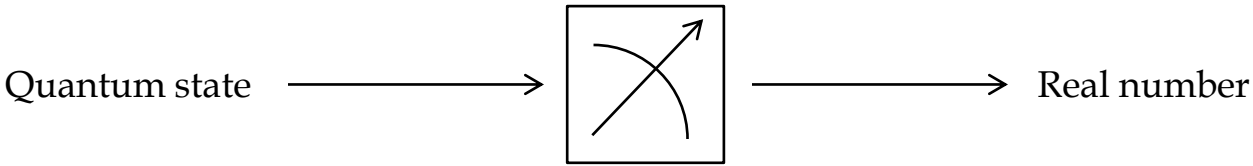
Observable

- Suppose we have a k-level system: $|\psi\rangle \in \mathbb{C}^k$

- An observable A for this system is an operator: a kxk Hermitian matrix.

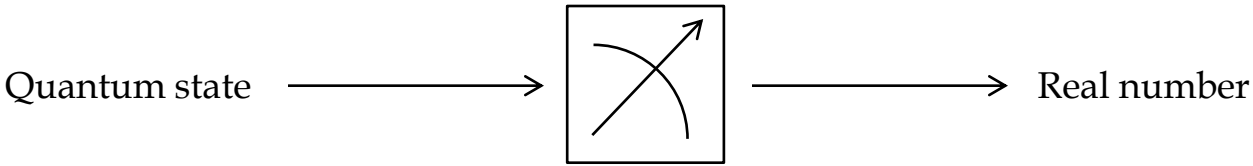
$$A = A^\dagger$$

e.g. $\begin{pmatrix} 1 & 1+i \\ 1-i & -2 \end{pmatrix}$



Measurement?

- An **observable** is a quantity like energy, position, momentum



- **Measure** in orthonormal basis $|\phi_1\rangle, \ldots, |\phi_k\rangle$ with corresponding outcomes
  1 , . . . , k

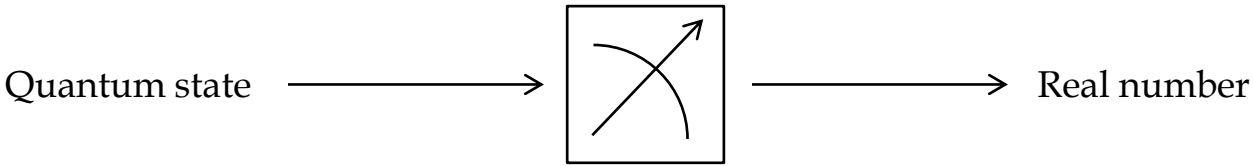
Observable

- Suppose we have a k-level system: $|\psi\rangle \in \mathbb{C}^k$

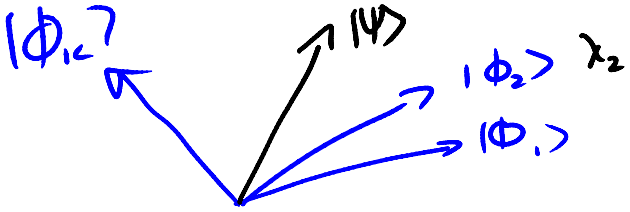
- An observable A for this system is an operator: a kxk Hermitian matrix.

$$A = A^\dagger$$

e.g. $\begin{pmatrix} 1 & 1+i \\ 1-i & -2 \end{pmatrix}$



Observable



- Suppose we have a k-level system: $|\psi\rangle \in \mathbb{C}^k$
- An observable A for this system is an operator: a kxk Hermitian matrix.

$$A = A^\dagger$$

e.g. $\begin{pmatrix} 1 & 1+i \\ 1-i & -2 \end{pmatrix}$

What's special about it? **Spectral theorem!**

A has orthonormal eigenvectors $|\phi_1\rangle, \ldots, |\phi_k\rangle$ with real eigenvalues $\lambda_1, \ldots, \lambda_k$

$$A|\phi_i\rangle = \lambda_i|\phi_i\rangle$$

How do we measure with it?

Let $|\psi\rangle = \sum \alpha_i|\phi_i\rangle$. Measurement outcome is λ_i with probability $|\alpha_i|^2$

new state $|\psi_{new}\rangle = |\phi_i\rangle$

- Example $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$.
- Observable $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$

eigenvectors $|\phi_1\rangle = |+\rangle$ $\lambda_1 = 1$

$|\phi_2\rangle = |-\rangle$ $\lambda_2 = -1$.

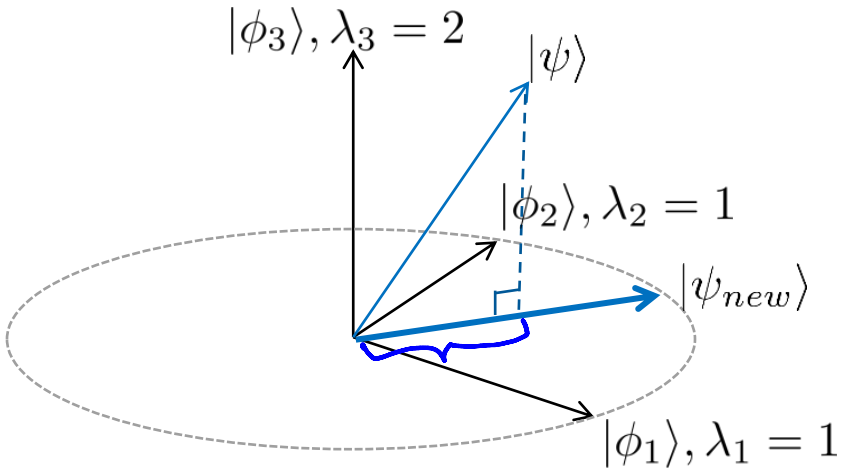
$|\psi\rangle = \frac{\alpha+\beta}{\sqrt{2}}|+\rangle + \frac{\alpha-\beta}{\sqrt{2}}|-\rangle$

Outcome: $+1$ wp $\left|\frac{\alpha+\beta}{\sqrt{2}}\right|^2$ New state $|+\rangle$

-1 wp $\left|\frac{\alpha-\beta}{\sqrt{2}}\right|^2$ New state $|-\rangle$

Expected value $= 1\left|\frac{\alpha+\beta}{\sqrt{2}}\right|^2 + (-1)\left|\frac{\alpha-\beta}{\sqrt{2}}\right|^2$

- Repeated eigenvalues?



What happens if the measurement outcome is 1?

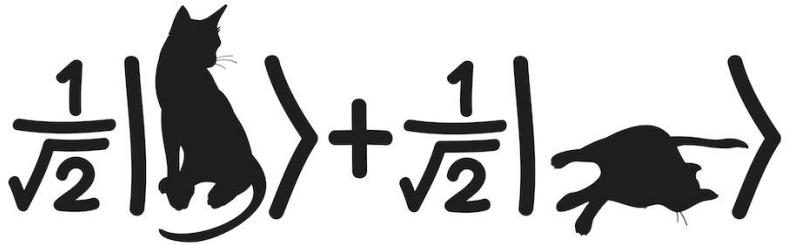
Does it collapse to $|\phi_1\rangle$ or $|\phi_2\rangle$?

It gets projected into the eigenspace.

$A\left(\frac{1}{\sqrt{2}}|\phi_1\rangle + \frac{1}{\sqrt{2}}|\phi_2\rangle\right)$

$= \frac{1}{\sqrt{2}}|\phi_1\rangle + \frac{1}{\sqrt{2}}|\phi_2\rangle$

Quantum Mechanics & Quantum Computation

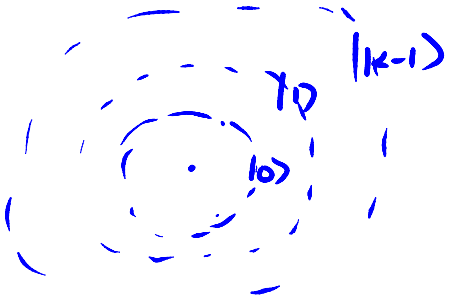


Umesh V. Vazirani
University of California, Berkeley

Lecture 7: Observables and Schrödinger's equation

Observables (part 2)

Observable



- Suppose we have a k-level system: $|\psi\rangle \in \mathbb{C}^k$
- An observable A for this system is an operator: a kxk Hermitian matrix.

$$\begin{bmatrix} E_0 & & 0 \\ & E_1 & \\ & \ddots & \\ 0 & & E_{k-1} \end{bmatrix}$$

$$A = A^\dagger$$

e.g. $\begin{pmatrix} 1 & 1+i \\ 1-i & -2 \end{pmatrix}$

What's special about it? **Spectral theorem!**

A has orthonormal eigenvectors $|\phi_1\rangle, \ldots, |\phi_k\rangle$ with real eigenvalues $\lambda_1, \ldots, \lambda_k$

$$A|\phi_i\rangle = \lambda_i|\phi_i\rangle$$

How do we measure with it?

Let $|\psi\rangle = \sum \alpha_i|\phi_i\rangle$. Measurement outcome is λ_i with probability $|\alpha_i|^2$

new state $|\psi_{new}\rangle = |\phi_i\rangle$

Observable

- Suppose we have a k-level system: $|\psi\rangle \in \mathbb{C}^k$

- An observable A for this system is an operator: a kxk Hermitian matrix.

$$A = A^\dagger \qquad \text{e.g.} \begin{pmatrix} 1 & 1+i \\ 1-i & -2 \end{pmatrix}$$

- How general is this?

- Suppose we wish to measure in an arbitrary basis $|\phi_1\rangle, \ldots, |\phi_k\rangle$
  and want arbitrary real outcomes $\lambda_1, \ldots, \lambda_k$
  is there an observable A with corresponding eigenvectors and eigenvalues?

- Example: $|+\rangle, |-\rangle$ with $2, -3$

$$|+\rangle\langle+| = \begin{pmatrix} 1/\sqrt{2} \\ 1/\sqrt{2} \end{pmatrix} \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{pmatrix} = \begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix}$$

$$(2|+\rangle\langle+|)|\psi\rangle = 2|+\rangle(\langle+|\psi\rangle) = 2\langle+|\psi\rangle\,|+\rangle$$

$$\begin{pmatrix} 5/2 & -1/2 \\ -1/2 & 5/2 \end{pmatrix}$$

If $|\psi\rangle = |+\rangle$

$$|-\rangle\langle-| = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \end{pmatrix} \begin{pmatrix} \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix} = \begin{pmatrix} \frac{1}{2} & -\frac{1}{2} \\ -\frac{1}{2} & \frac{1}{2} \end{pmatrix}$$

$$\left(2\,|+\rangle\langle+| + (-3)\,|-\rangle\langle-|\right)|+\rangle = 2\,|+\rangle + 0 = 2|+\rangle$$

- In general: Given $|\phi_i\rangle, \lambda_i$ corresponding observable is:

$$A = \sum \lambda_i |\phi_i\rangle\langle\phi_i|$$

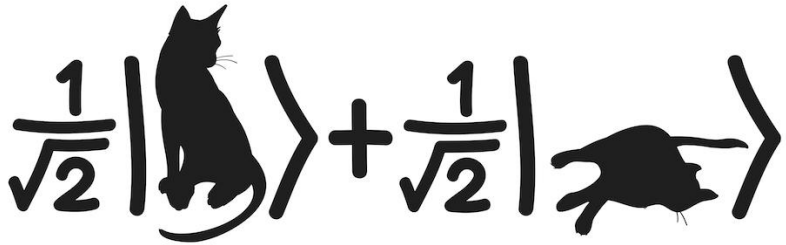
$A|\phi_j\rangle = \lambda_j$

- Therefore equivalent to our previous notion of measurement

observable $\equiv$ Pick an orthonormal basis $|\phi_i\rangle$'s

$A = A^\dagger$ λ_i's

Quantum Mechanics & Quantum Computation



Umesh V. Vazirani
University of California, Berkeley

Lecture 7: Observables and Schrödinger's equation

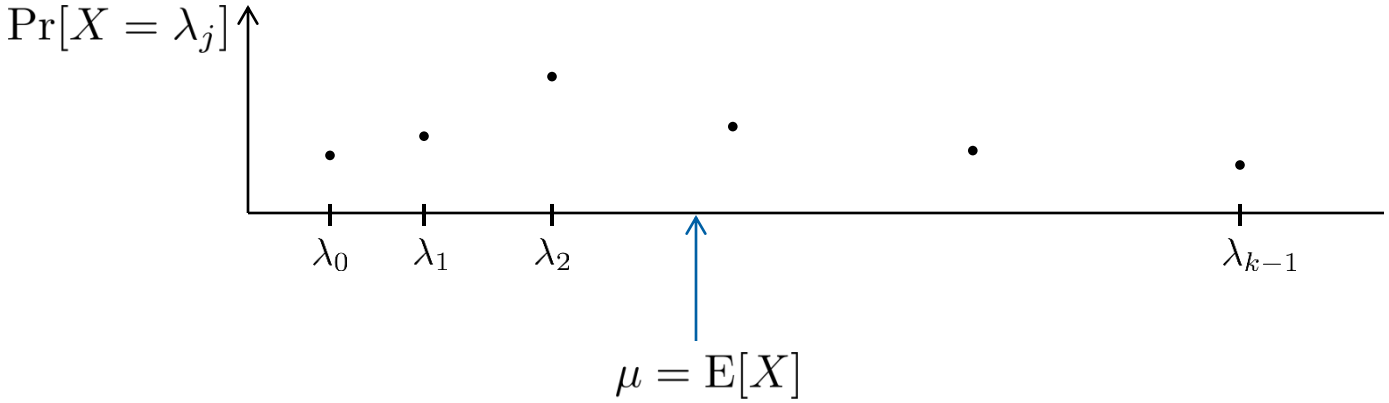
Expectation value and Variance

$M = M^\dagger$

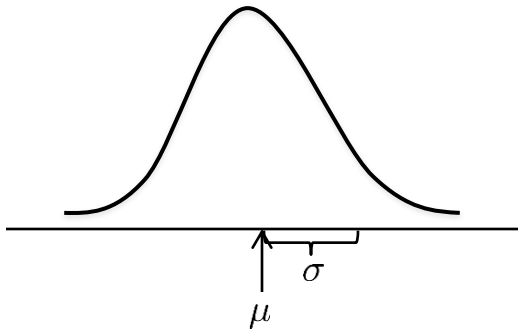
- An observable M for a k-level quantum system is a kxk Hermitian matrix.
  Random variable X denotes outcome of measurement of state $|\psi\rangle = \sum \alpha_i |\phi_i\rangle$

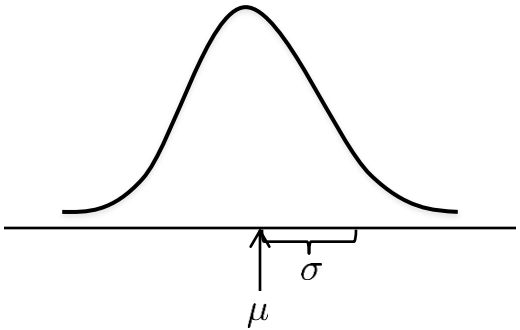
- Distribution of X:

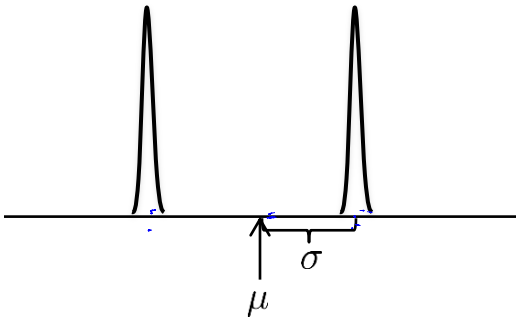
$P[X = \lambda_j] = |\alpha_j|^2$



$$\sigma^2 = \mathrm{Var}[X] = \mathrm{E}[(X - \mu)^2]$$


σ
μ


σ
μ


σ
μ

- Observable M on state $|\psi\rangle$

M $|\phi_j\rangle$ λ_j

$|\psi\rangle = \sum \alpha_j |\phi_j\rangle$

$$\mu = \mathrm{E}[X] = \langle\psi|M|\psi\rangle$$

$$\mu = E[x] = \sum |\alpha_j|^2 \lambda_j = (\alpha_0^* \alpha_1^* \cdots \alpha_{k-1}^*) \begin{pmatrix} \lambda_0 & & 0 \\ & \lambda_1 & \\ 0 & & \lambda_{k-1} \end{pmatrix} \begin{pmatrix} \alpha_0 \\ \alpha_1 \\ \\ \alpha_{k-1} \end{pmatrix}$$

$$= \sum \alpha_j^* \lambda_j \alpha_j = \sum \alpha_j^* \alpha_j \lambda_j$$

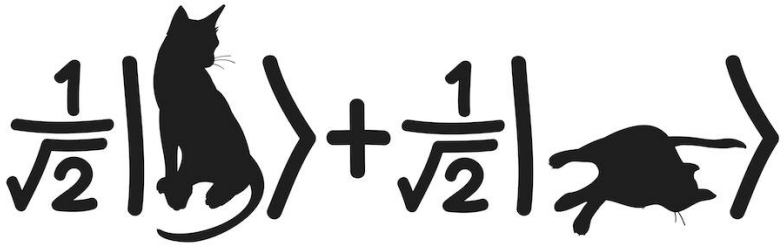
$$\sigma^2 = \mathrm{Var}[X] = \mathrm{E}[X^2] - (\mathrm{E}[X])^2 = E[x^2] - \mu^2$$

$$= \langle\psi|M^2|\psi\rangle - \langle\psi|M|\psi\rangle^2$$

$$E[x^2] = \sum |\alpha_j|^2 \lambda_j^2 = (\alpha_0^* \alpha_1^* \cdots \alpha_{k-1}^*) \begin{pmatrix} \lambda_0^2 & & \\ & \lambda_1^2 & \\ & & \lambda_{k-1}^2 \end{pmatrix} \begin{pmatrix} \alpha_0 \\ \vdots \\ \alpha_{k-1} \end{pmatrix}$$

Quantum Mechanics & Quantum Computation

Umesh V. Vazirani
University of California, Berkeley



Lecture 7: Observables and Schrödinger's equation

Schrödinger's equation (part 1)

Axiom of unitary evolution

- **Unitary evolution axiom**: a quantum system evolves by a unitary rotation of the Hilbert space.

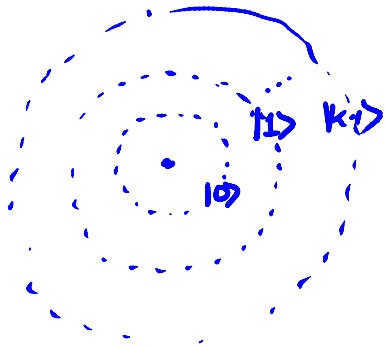
$$UU^\dagger = U^\dagger U = I$$

- But… by *which* unitary rotation?

This is described by **Schrödinger's equation,**
"the quantum equation of motion"

Schrödinger's equation

- Energy observable H, called the Hamiltonian of the system.
  - Its eigenvectors $|\phi_i\rangle$'s are the states with definite energy.
  - The eigenvalues λ_i's are the energy of the corresponding state.



$|\psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle + \cdots + \alpha_{k-1}|k-1\rangle$

- Example $H = \begin{pmatrix} -\frac{1}{2} & \frac{5}{2} \\ \frac{5}{2} & -\frac{1}{2} \end{pmatrix}$
  - $|+\rangle$ with energy = 2
  - $|-\rangle$ with energy = −3

$$H = \begin{pmatrix} E_0 & & & 0 \\ & E_1 & & \\ & & \ddots & \\ 0 & & & E_{k-1} \end{pmatrix}$$

Schrödinger's equation

- Energy observable H, called the Hamiltonian of the system.
  - Its eigenvectors $|\phi_i\rangle$'s are the states with definite energy.
  - The eigenvalues λ_i's are the energy of the corresponding state.

- Schrödinger's equation:

$|\psi(t)\rangle$ = state of system at time t
Given $|\psi(0)\rangle$ & H

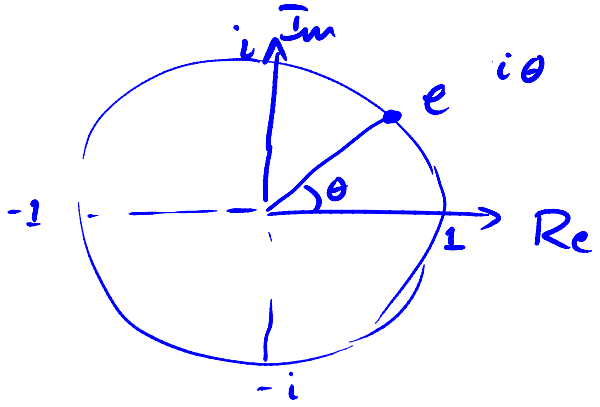
$$i\hbar\frac{\partial}{\partial t}|\psi(t)\rangle = H|\psi(t)\rangle$$

Solving Schrödinger's equation

$$i\hbar\frac{\partial}{\partial t}|\psi(t)\rangle = H|\psi(t)\rangle$$

$|\psi(0)\rangle = |\phi_j\rangle$ where $|\phi_j\rangle$ is some eigenvector of H with a corresponding eigenvalue $|\lambda_j\rangle$

Then $|\psi(t)\rangle = e^{-\frac{i\lambda_j t}{\hbar}}|\phi_j\rangle$



$$H|\phi_j\rangle = \lambda_j|\phi_j\rangle$$

$$\Rightarrow \quad |\psi(t)\rangle = a(t)|\phi_j\rangle$$

$$i\hbar\frac{d\,a(t)|\phi_j\rangle}{dt} = H\left(a(t)|\phi_j\rangle\right)$$

$$= a(t)\,\lambda_j\,|\phi_j\rangle$$

$$\frac{d\,a(t)}{a(t)} = -i\frac{\lambda_j}{\hbar}\,dt$$

$$a(t) = e^{-\frac{i\lambda_j t}{\hbar}}$$

Solving Schrödinger's equation

$$i\hbar\frac{\partial}{\partial t}|\psi(t)\rangle = H|\psi(t)\rangle$$

In general: $|\psi(0)\rangle = \sum_j \alpha_j |\phi_j\rangle$

$$|\psi(t)\rangle = \sum_j \alpha_j e^{-\frac{i\lambda_j t}{\hbar}}|\phi_j\rangle$$

In the eigenbasis, we can write

$$|\psi(t)\rangle = \begin{pmatrix} e^{-\frac{i\lambda_1 t}{\hbar}} & & 0 \\ & \ddots & \\ 0 & & e^{-\frac{i\lambda_k t}{\hbar}} \end{pmatrix} |\psi(0)\rangle$$

$= U(t)$

unitary $U(t) = e^{-\frac{iHt}{\hbar}}$ (shorthand notation)

$U U^\dagger = U^\dagger U = I$

$B = e^A$

B has same eveckers

evalue of A is λ_j

$\updownarrow$

evalue of $B = e^{\lambda_j}$

Schrödinger's equation

$$i\hbar\frac{\partial}{\partial t}|\psi(t)\rangle = H|\psi(t)\rangle$$

In general: $|\psi(0)\rangle = \sum \alpha_j |\phi_j\rangle$

$$|\psi(t)\rangle = \sum \alpha_j e^{-\frac{i\lambda_j t}{\hbar}} |\phi_j\rangle$$

Example $|\psi(0)\rangle = |0\rangle$

$H = X$

What is $|\psi(t)\rangle$?

$$|\psi(0)\rangle = \frac{1}{\sqrt{2}}|+\rangle + \frac{1}{\sqrt{2}}|-\rangle$$

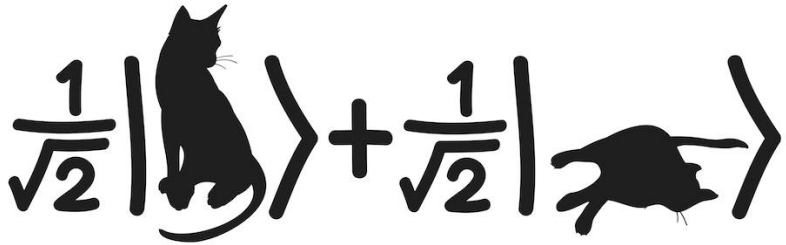
$$|\psi(t)\rangle = \frac{1}{\sqrt{2}} e^{\frac{-it}{\hbar}} |+\rangle + \frac{1}{\sqrt{2}} e^{+it/\hbar} |-\rangle$$

We know that X's eigenvectors are :

$|+\rangle$ with eigenvalue 1

$|-\rangle$ with eigenvalue -1

Quantum Mechanics & Quantum Computation



Umesh V. Vazirani
University of California, Berkeley

Lecture 7: Observables and Schrödinger's equation

Symmetry and Conservation Laws

Schrödinger's equation

- Energy observable H, called the Hamiltonian of the system.
  - Its eigenvectors $|\phi_i\rangle$'s are the states with definite energy.
  - The eigenvalues λ_i's are the energy of the corresponding state.

- Schrödinger's equation:

$$i\hbar\frac{\partial}{\partial t}|\psi(t)\rangle = H|\psi(t)\rangle$$

Emmy Noether 1882-1935

Why is H special?

Unitary evolution $\Rightarrow$ $U = e^{-iMt}$ for some hermitian M.

Why is $M = H$?

If A is any observable $\equiv$ conserved physical quantity

then A commutes with M

$$A \cdot M = M \cdot A$$

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

$$XZ = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

$$\neq$$

$$ZX = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

Why is H special?

$|\psi\rangle \qquad |\psi'\rangle = U|\psi\rangle = e^{-iMt}|\psi\rangle$ at time t.

A conserved quantity means:

$$\langle\psi|A|\psi\rangle = \langle\psi'|A|\psi'\rangle = \langle\psi|U^\dagger A U|\psi\rangle$$

$$\Rightarrow A = U^\dagger A U = e^{iMt} A e^{-iMt}$$

$$\approx (1 + iMt) A (1 - iMt)$$

$$\approx A + \underbrace{it[MA - AM]}_{0} + O(t^2)$$

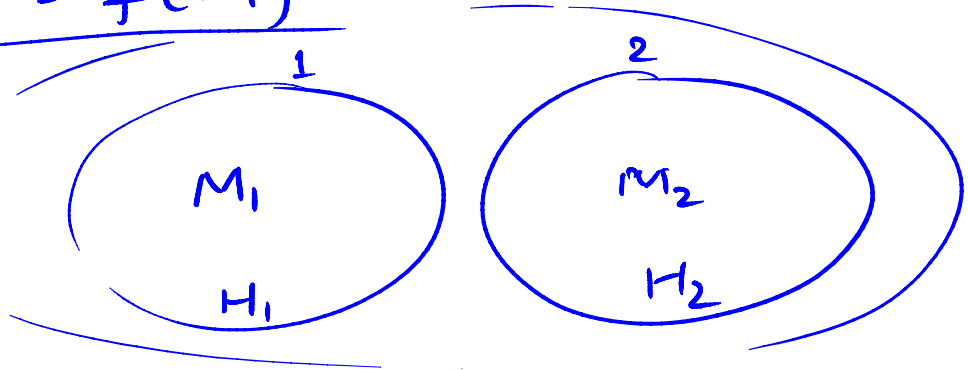
$$MA = AM$$

Why is H special?

* $U = e^{-iMt}$ M hermitian.
* A conserved $\Rightarrow$ $AM = MA$
* Intrinsic reason why M & H commute.

$H = \hbar M$

$H = f(M)$ $\Rightarrow$ f must necessarily be linear.



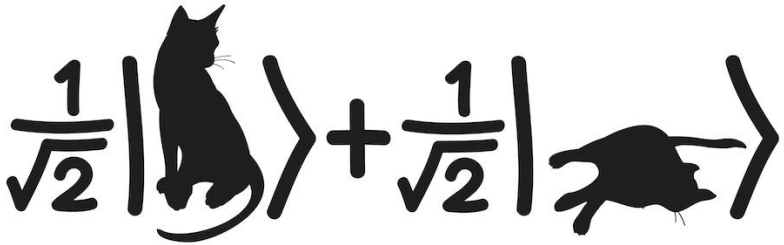
$f(M_1)$ $f(M_2)$

$H = H_1 + H_2$

$H = f(M_1 + M_2)$

$f(M_1 + M_2) = f(M_1) + f(M_2)$

Quantum Mechanics & Quantum Computation



Umesh V. Vazirani
University of California, Berkeley

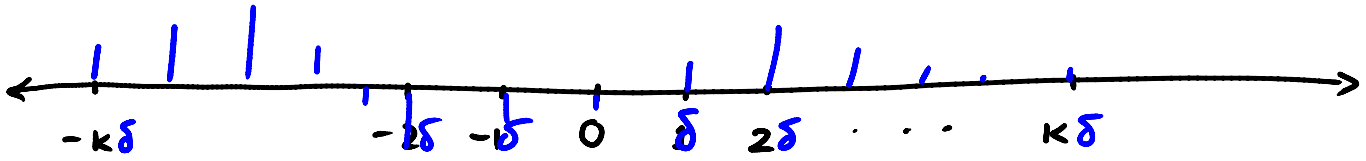
Lecture 9: Continuous quantum states, Schrödinger's equation, uncertainty principle

Continuous quantum states

represent continuous quantum state?
observables?

Schrödinger's eqn for free particle in 1D.

Uncertainty principle – position & momentum.



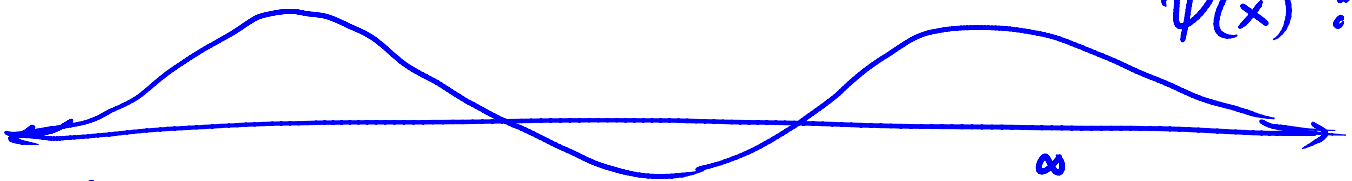
$$|\psi\rangle = \sum_{j=-k}^{k} \alpha_j |j\rangle$$

$$||\psi\rangle|^2 = \sum |\alpha_j|^2 = 1$$

$$\alpha_j = \psi(j)$$

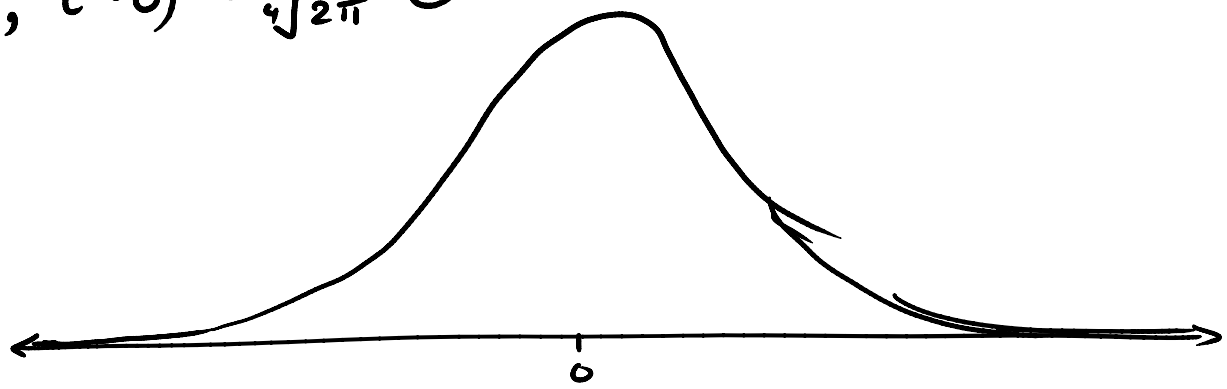
$\delta \to 0 \qquad k \to \infty$

$\psi(x) : \mathbb{R} \to \mathbb{C}$



wavefunction $\psi(x)$ $\int_{-\infty}^{\infty} \psi(x)^* \psi(x)\, dx = \int_{-\infty}^{\infty} |\psi(x)|^2\, dx = 1$

$$\psi(x, t=0) = \sqrt[4]{\frac{1}{2\pi}}\, e^{-x^2}$$

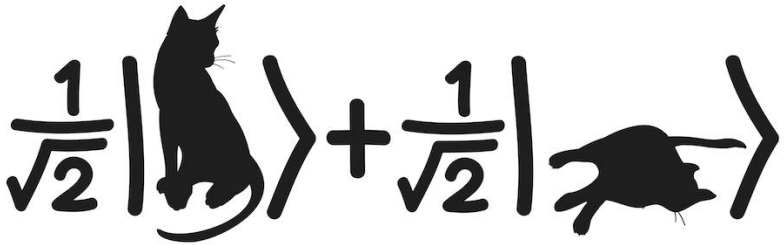


- How does $\psi(x, t)$ evolve with time?
- What is the velocity of the particle?

momentum

mv

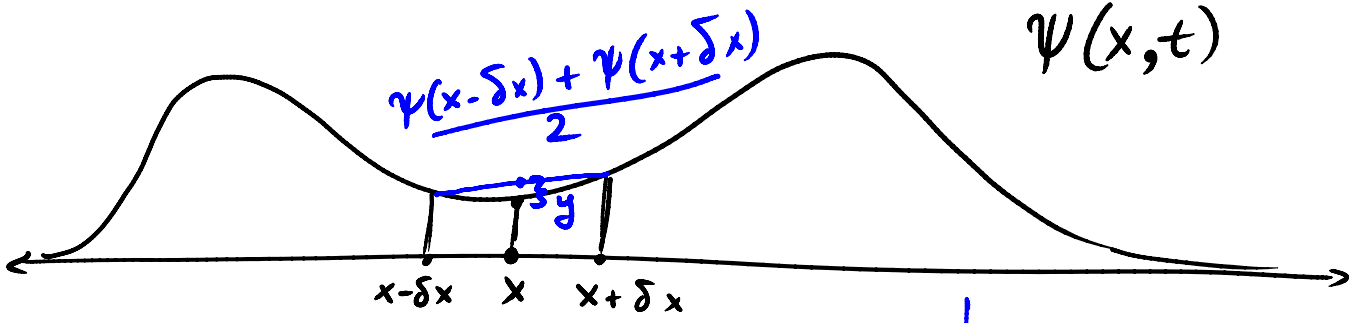
Quantum Mechanics & Quantum Computation



Umesh V. Vazirani
University of California, Berkeley

Lecture 9: Continuous quantum states, Schrödinger's equation, uncertainty principle

Schrödinger's equation



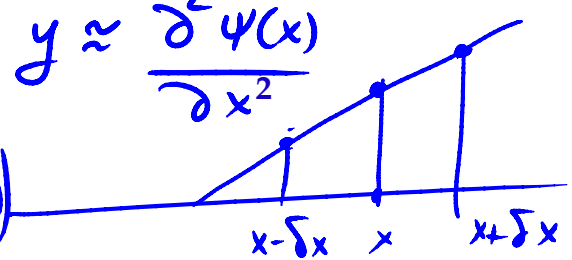
$$\frac{\partial \psi(x,t)}{\partial t} \propto y$$

$$i\frac{\partial \psi(x,t)}{\partial t} = \frac{\partial^2 \psi(x,t)}{\partial x^2}$$

Describe y in terms of $\psi(x)$?

$$y \approx \frac{\partial \psi(x)}{\partial x}$$

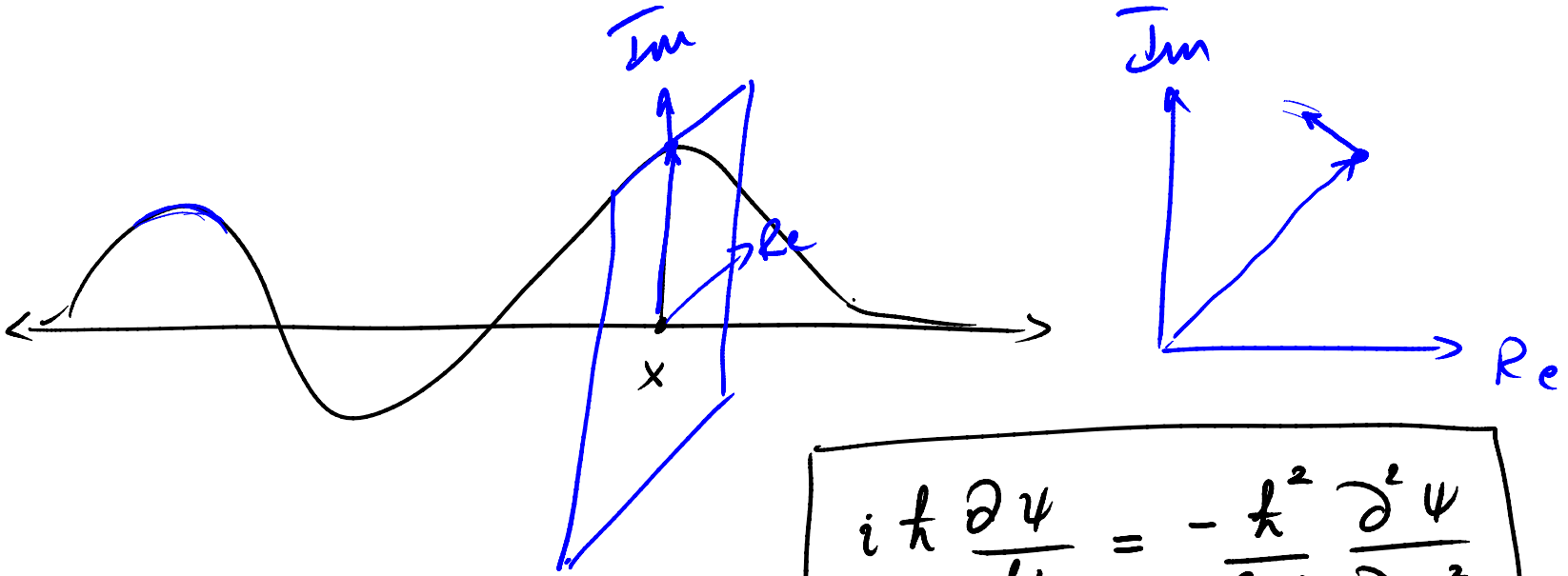
$$y \approx \frac{\partial^2 \psi(x)}{\partial x^2}$$



$$\frac{\psi(x-\delta x)+\psi(x+\delta x)}{2} - \psi(x)$$

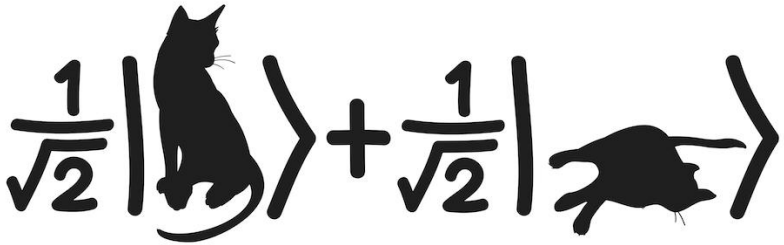
$$= \frac{(\psi(x+\delta x)-\psi(x)) - (\psi(x)-\psi(x-\delta x))}{2}$$

$$i\,\frac{\partial\,\psi(x,t)}{\partial\,t} = \frac{\partial^2\,\psi(x,t)}{\partial\,x^2}$$



$$i\hbar\,\frac{\partial\,\psi}{dt} = -\frac{\hbar^2}{2m}\,\frac{\partial^2\,\psi}{\partial\,x^2}$$

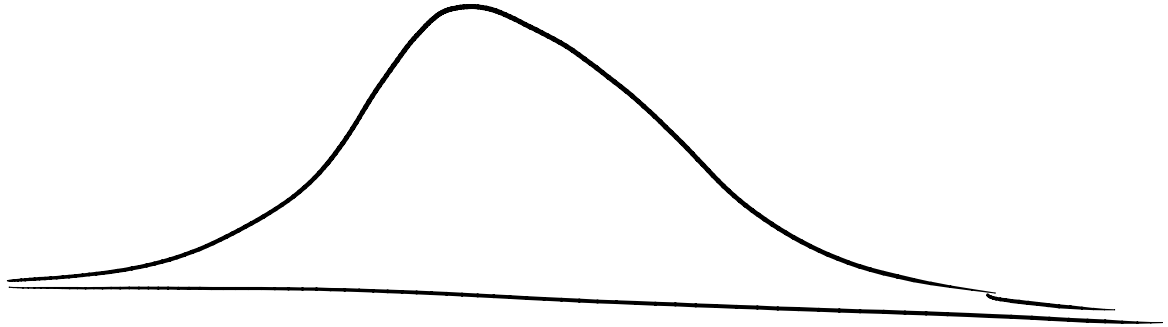
Quantum Mechanics & Quantum Computation



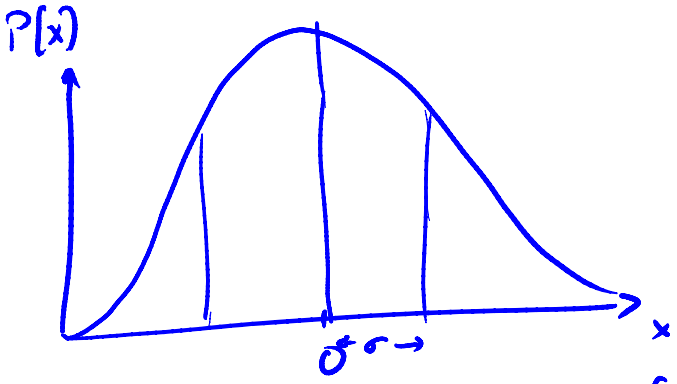
Umesh V. Vazirani
University of California, Berkeley

Lecture 9: Continuous quantum states, Schrödinger's equation, uncertainty principle

Uncertainty principle



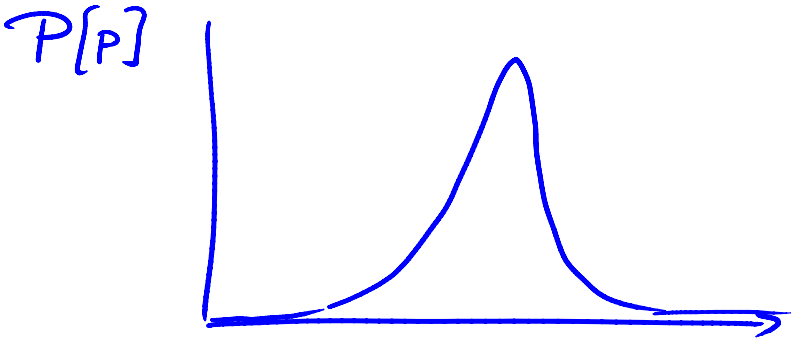
Measure its position:



$E(x) = 0$ $\quad \Delta x = E[x^2] - E(x)^2$

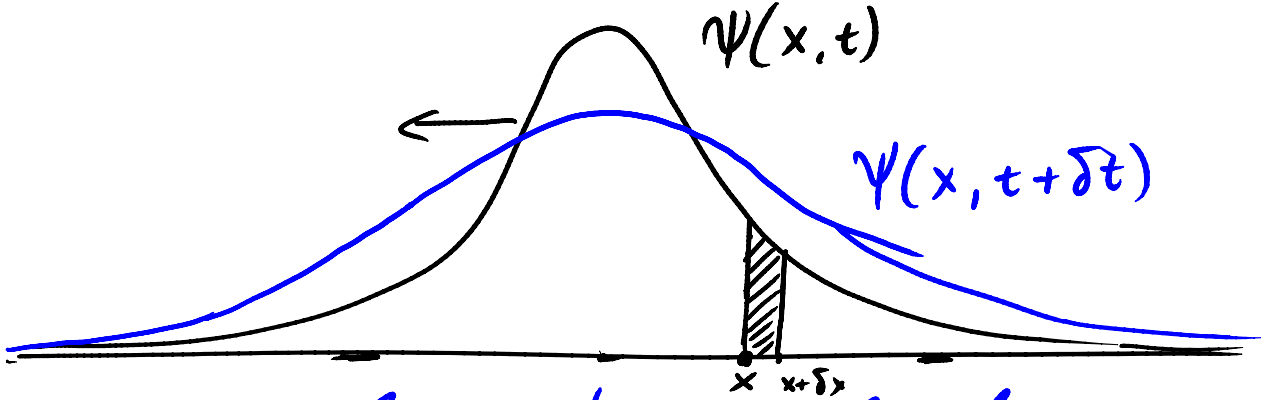
σ^2

Measure its momentum



$\Delta p = E[p^2] - E(p)^2$

$\Delta x \, \Delta p \geq \hbar/2$



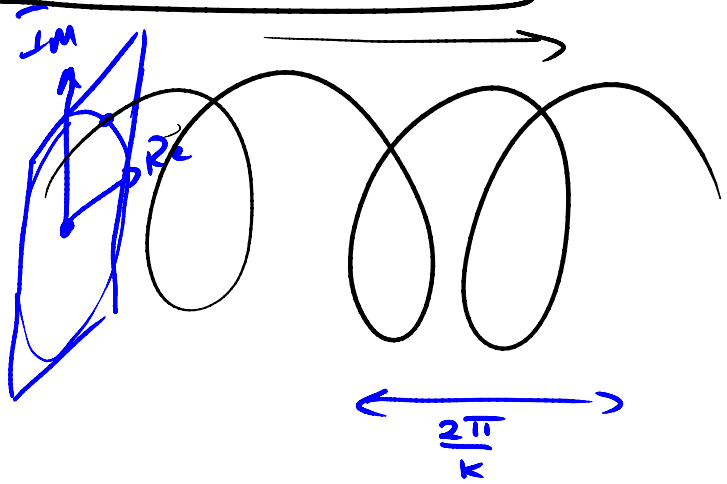
What is the velocity of the particle at time t?

$$\int_{x}^{x+\delta x} |\psi(x,t)|^2 \, dx$$

In a superposition of <u>velocities</u>.

$$\psi(x, t=0) = e^{ikx}$$

$$\psi(x) = \psi\left(x + \frac{2\pi}{k}\right)$$



velocity = k

period = $2\pi/k$

time = $2\pi/k^2$

$$\text{velocity} = \frac{2\pi/k}{2\pi/k^2} = k$$

$$\psi(x,t) = e^{i(kx + \omega t)}$$

$$\omega = k^2$$

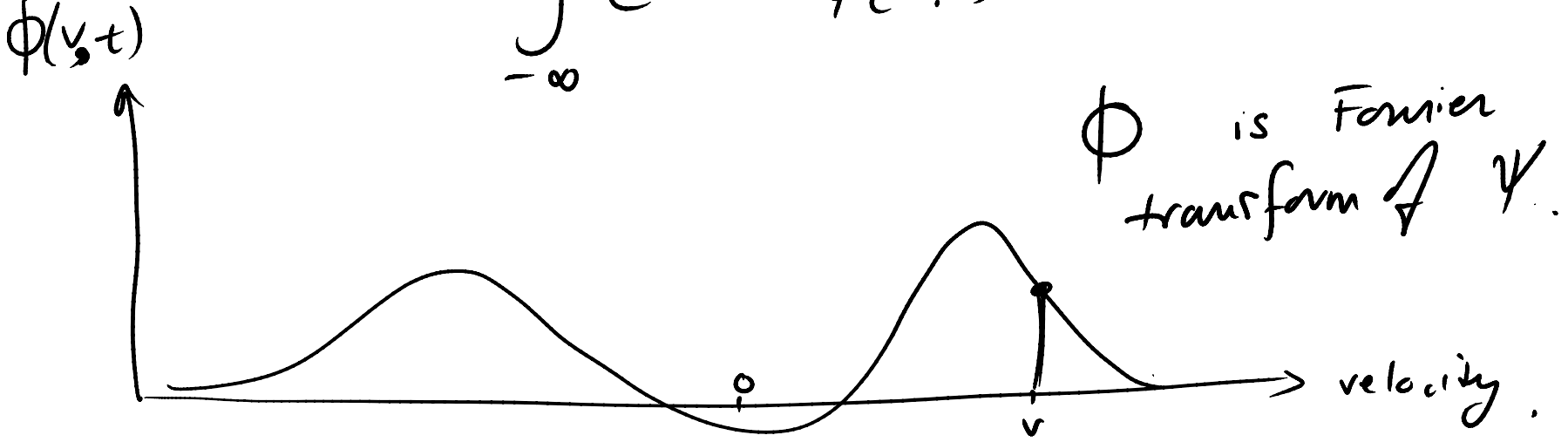
$$i\omega\, e^{i(kx+\omega t)} = (ik)^2 e^{i(kx+\omega t)}$$

$$\psi(x,t) = e^{ik(x+kt)}$$

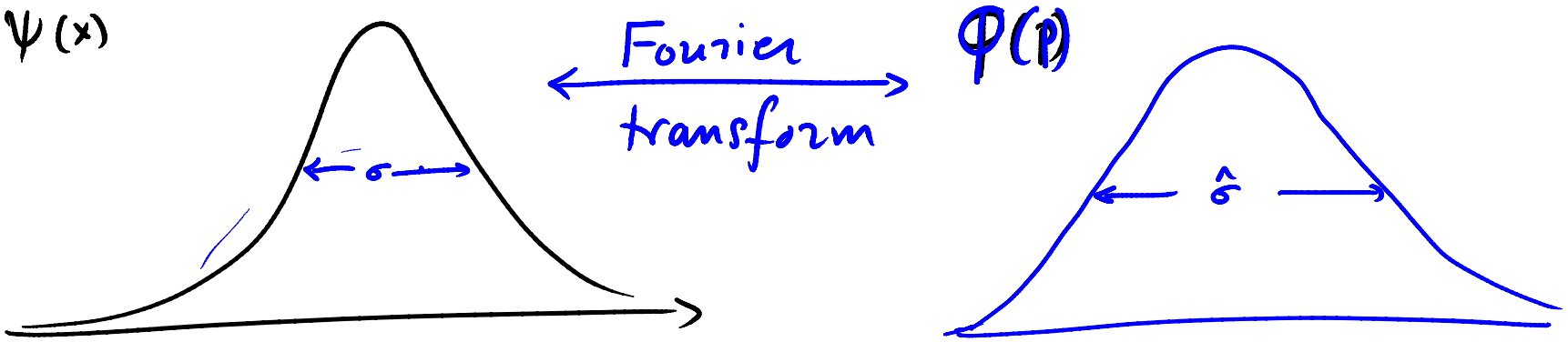
$\psi(x,t)$ $\underline{\underline{e^{ikx}}}$ $\underline{\underline{\kappa}}$

$$\phi(v,t) = \langle e^{ikx}, \psi(x,t) \rangle$$

$$= \int_{-\infty}^{\infty} e^{-ikx} \cdot \psi(x,t)\, dx$$

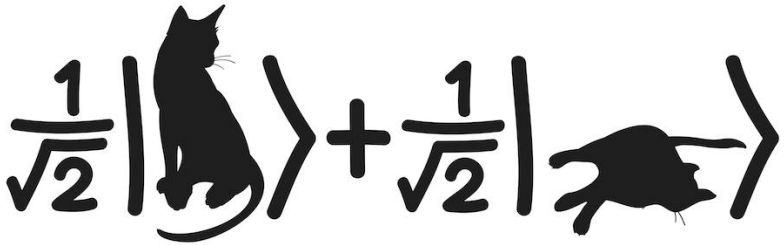


ϕ is Fourier transform of ψ.



$$\Delta x \, \Delta p \geq \frac{\hbar}{2}$$

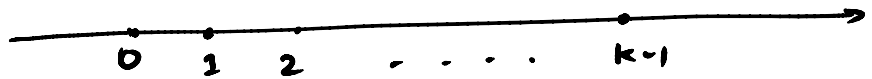
Quantum Mechanics & Quantum Computation



Umesh V. Vazirani
University of California, Berkeley

Lecture 10: Observables, Schrödinger's equation, Particle in a box

Position & Momentum Observables



$$|\psi\rangle = \sum_{j=0}^{k-1} \alpha_j |j\rangle$$

Position observable M: $M = M^+$

$$M = \begin{bmatrix} 0 & & & \\ & 1 & & \\ & & 2 & \\ & & & \ddots \\ & & & & k-1 \end{bmatrix}$$

$M|j\rangle = j|j\rangle$

$\frac{1}{\sqrt{3}}|0\rangle + \sqrt{\frac{2}{3}}|1\rangle$

$|\psi\rangle \begin{pmatrix} \alpha_0 \\ \alpha_{k-1} \end{pmatrix}$ wavefunction $\psi(x)$

$\psi(x) : \mathbb{R} \to \mathbb{C}$

$$\int_{-\infty}^{\infty} |\psi(x)|^2 dx = 0$$

Inner product: $\psi(x)$ & $\phi(x)$

$$\langle \phi(x) | \psi(x) = \int_{-\infty}^{\infty} \overline{\phi(x)}\, \psi(x)\, dx$$

$\alpha = a + ib$

$\alpha^* = a - ib = \bar{\alpha}$

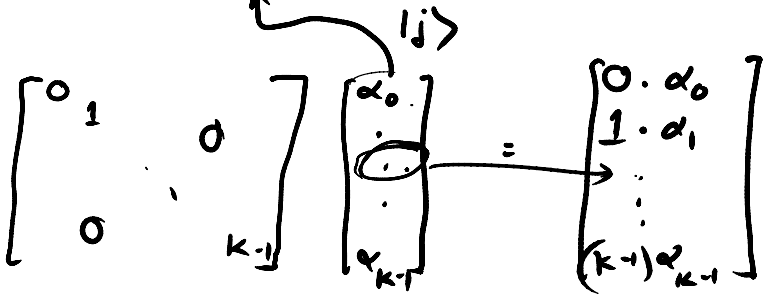
M Hermitian $\quad M = M^\dagger \iff \langle i|M|j\rangle = \overline{\langle j|M|i\rangle}$

self-adjoint $\quad \langle\phi|M|\psi\rangle = \overline{\langle\psi|M|\phi\rangle}$

Observable: self-adjoint M that maps wavefunctions to wavefunctions.

Position observable $\hat{x}$

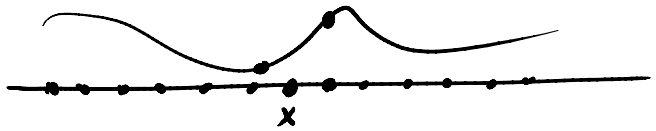
$$\hat{x}\,\psi(x) = \phi(x) \qquad \text{where} \quad \phi(x) = x\,\psi(x)$$



Momentum Operator:

$$\hat{p} = -i\hbar \frac{\partial}{\partial x}$$

$$\hat{p}\,\psi(x) = -i\hbar \frac{\partial}{\partial x}\psi(x)$$



$$\begin{pmatrix} 0 & i & & \\ & \ddots & \ddots & \\ & & \ddots & i \\ -i & & & 0 \end{pmatrix} \begin{pmatrix} \alpha_0 \\ \alpha_1 \\ \alpha_{j-1} \\ \alpha_j \\ \alpha_{j+1} \\ \alpha_{k-1} \end{pmatrix} = \begin{pmatrix} \\ \\ \alpha_{j+1} - \alpha_{j-1} \\ \\ \\ \end{pmatrix}$$

Momentum operator $\hat{p} = -i\hbar \frac{\partial}{\partial x}$

Free particle

$i\hbar \frac{\partial |\psi\rangle}{\partial t} = H|\psi\rangle$

H Hamiltonian

energy operator.

Classically: $P.E. + K.E.$ ($P.E. = 0$)

$\frac{p^2}{2m}$ ← momentum

mass

$$i\hbar \frac{\partial \psi}{\partial t} = \frac{\hat{p}^2}{2m} |\psi\rangle$$

$$= -i\hbar \frac{\partial}{\partial x}(-i\hbar \frac{\partial}{\partial x}) \cdot \frac{1}{2m} |\psi\rangle$$

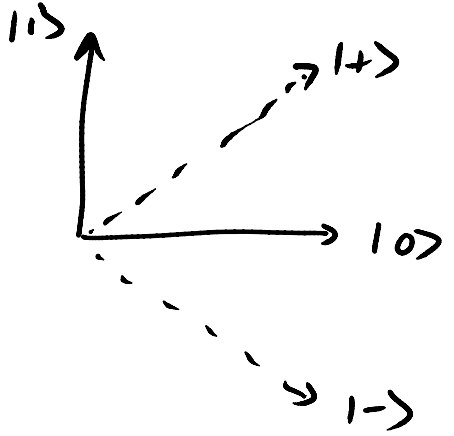
$$= -\frac{\hbar^2}{2m} \frac{\partial^2}{\partial x^2} |\psi\rangle$$

bit & sign

$$Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \qquad X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

$|0\rangle$ & $|1\rangle$ $\qquad$ $|+\rangle$ $\quad$ $|-\rangle$

1 $\qquad$ -1 $\qquad$ 1 $\qquad$ -1.



$$XZ \neq ZX$$

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$$

$$ZX = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$$

$$[X,Z] = XZ - ZX = \begin{bmatrix} 0 & -2 \\ 2 & 0 \end{bmatrix}$$

Position - momentum Uncertainty:

$$[\hat{x}, \hat{p}] = \hat{x}\hat{p} - \hat{p}\hat{x} = i\hbar$$

Thm $\quad \Delta\hat{x}\,\Delta\hat{p} \geq \frac{|[\hat{x}, \hat{p}]|}{2} \geq \frac{\hbar}{2}.$ $\qquad (\Delta A)^2 = |\langle\psi|A^2|\psi\rangle|$

Thm $\quad \Delta A\,\Delta B \geq \frac{|[A, B]|}{2}$

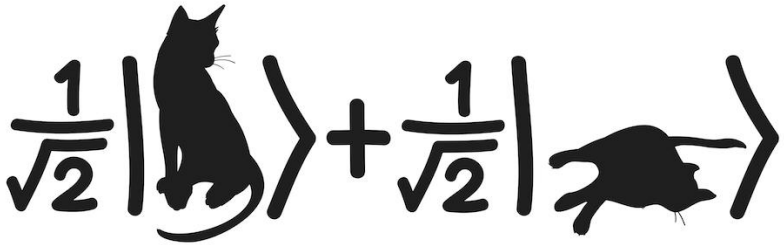
$$(\hat{x}\hat{p} - \hat{p}\hat{x})\psi(x) = \hat{x}\hat{p}\,\psi(x) - \hat{p}\hat{x}\,\psi(x)$$

$$= x\left(-i\hbar\frac{\partial}{\partial x}\psi(x)\right) - \left(-i\hbar\frac{\partial}{\partial x}x\,\psi(x)\right)$$

$$= -i\hbar\left[x\frac{\partial\psi}{\partial x} - \frac{\partial}{\partial x}x\,\psi(x)\right]$$

$$= i\hbar\,\psi(x) \qquad \psi(x) + x\frac{\partial\psi(x)}{\partial x}$$

Quantum Mechanics & Quantum Computation



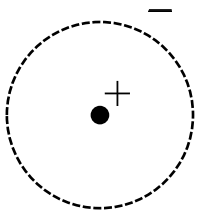
Umesh V. Vazirani
University of California, Berkeley

Lecture 10: Observables, Schrödinger's equation, Particle in a box

Particle in a box

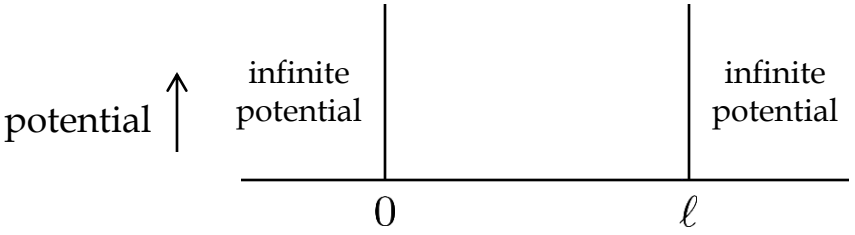
Particle in a box

- Toy model for a hydrogen atom.



Coulomb attraction confines the electron to within some distance ℓ

We model this in 1D (radial distance)



We will solve Schrödinger's equation:

$$i\hbar\frac{\partial\psi}{\partial t} = H\psi = \frac{\hat{p}^2}{2m}|\psi\rangle + V(x)|\psi\rangle = -\frac{\hbar^2}{2m}\frac{\partial^2}{\partial x^2}|\psi\rangle$$

Boundary conditions: $\psi(0) = \psi(\ell) = 0$

$H|\phi\rangle = \lambda|\phi\rangle$ $\qquad$ $\psi(0) = |\phi\rangle \Rightarrow \psi(t) = e^{-i\lambda t/\hbar}|\phi\rangle$

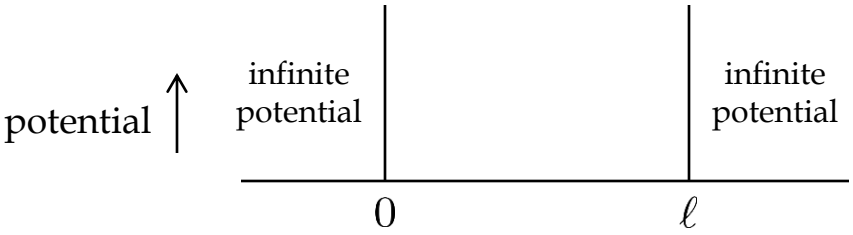
Guess: $H = -\frac{\hbar^2}{2m}\frac{\partial^2}{\partial x^2}$ $\qquad$ $\phi(x) = e^{ikx}$

$$H\phi(x) = -\frac{\hbar^2}{2m}\frac{\partial^2}{\partial x^2}e^{ikx} = \frac{\hbar^2}{2m}k^2 e^{ikx} \qquad E = \frac{\hbar^2 k^2}{2m}.$$

$$\phi_E(x) = Ae^{ikx} + Be^{-ikx} \qquad E_k = \frac{\hbar^2 k^2}{2m}$$

$$= C\sin kx + D\cos kx$$

$e^{ikx} = \cos kx + i\sin kx$



We will solve Schrödinger's equation:

$$i\hbar\frac{\partial\psi}{\partial t} = H\psi = \frac{\hat{p}^2}{2m}|\psi\rangle + V(x)|\psi\rangle = -\frac{\hbar^2}{2m}\frac{\partial^2}{\partial x^2}|\psi\rangle$$

Boundary conditions: $\psi(0) = \psi(\ell) = 0$

$\Phi_E(x) = C \sin kx + D \cos kx$

$E_k = \frac{\hbar^2 k^2}{2m}$

$\Phi(0) = 0 = C \times 0 + D \times 1$ ($=0$)

$\Phi_E(\ell) = 0 = C \sin k\ell$

$k\ell = n\pi$ $\quad n$ integer

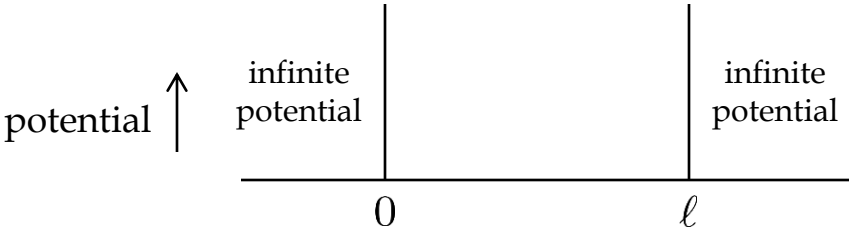
$k_n = \frac{n\pi}{\ell}$

$E_n = \frac{\hbar^2 k_n^2}{2m} = \frac{\hbar^2 n^2 \pi^2}{2m\ell^2}$

$\Phi_n(x) = C \sin \frac{n\pi}{\ell} x$

$\int_0^\ell C^2 \sin^2 \frac{n\pi}{\ell} x \, dx = 1 \Rightarrow C^2 = 2/\ell$

$C = \sqrt{2/\ell}$.



We will solve Schrödinger's equation:

$$i\hbar\frac{\partial\psi}{\partial t} = H\psi = \frac{\hat{p}^2}{2m}|\psi\rangle + V(x)|\psi\rangle = -\frac{\hbar^2}{2m}\frac{\partial^2}{\partial x^2}|\psi\rangle$$

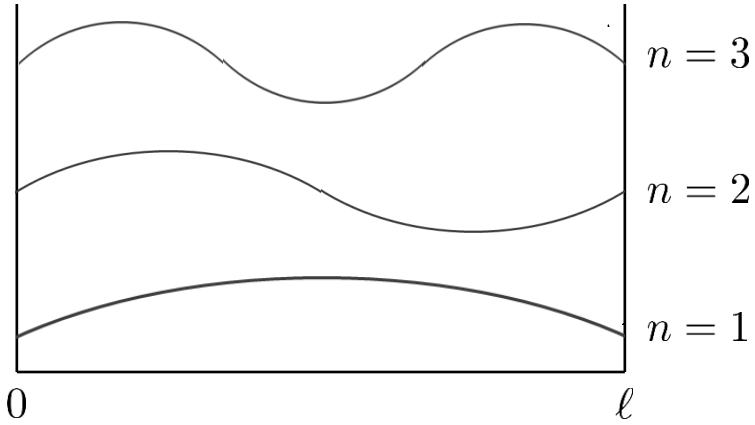
Boundary conditions: $\psi(0) = \psi(\ell) = 0$

Solution: $E_n = \frac{\hbar^2 n^2 \pi^2}{2m\ell^2}$ $\psi_n(x) = \sqrt{\frac{2}{\ell}}\sin\frac{n\pi x}{\ell}$

Quantization:

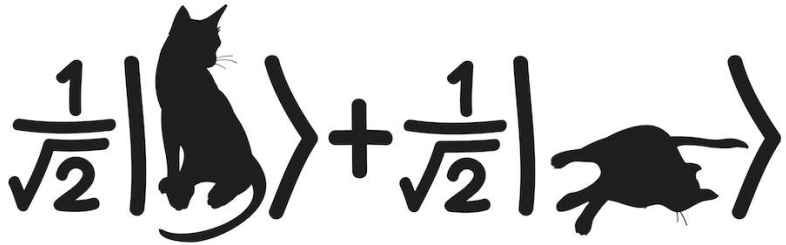
$\psi(x) = \alpha_n \psi_n(x)$

$\psi(x,t) = \alpha_n e^{-iE_n t/\hbar} \psi_n(x)$



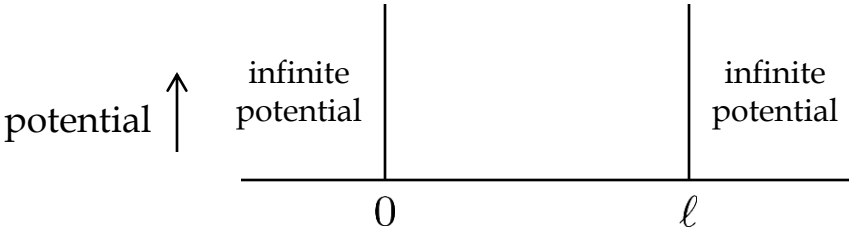
Quantum Mechanics & Quantum Computation

Umesh V. Vazirani
University of California, Berkeley



Lecture 10: Observables, Schrödinger's equation, Particle in a box

Qubits



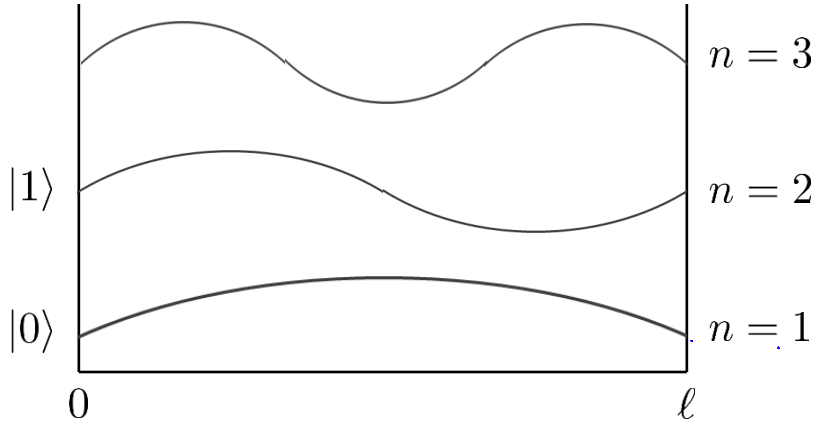
We will solve Schrödinger's equation:

$$i\hbar\frac{\partial\psi}{\partial t} = H\psi = \frac{\hat{p}^2}{2m}|\psi\rangle + V(x)|\psi\rangle = -\frac{\hbar^2}{2m}\frac{\partial^2}{\partial x^2}|\psi\rangle$$

Boundary conditions: $\psi(0) = \psi(\ell) = 0$

Solution: $E_n = \frac{\hbar^2 n^2 \pi^2}{2m\ell^2}$ $\psi_n(x) = \sqrt{\frac{2}{\ell}}\sin\frac{n\pi x}{\ell}$

Quantization:



Implementing qubits

- Restrict the energy to be small enough: $E < E_3$

$$|0\rangle \quad \Rightarrow \quad |\psi_1\rangle$$
$$|1\rangle \quad \Rightarrow \quad |\psi_2\rangle$$

- Suppose $|\psi(t=0)\rangle = \alpha|0\rangle + \beta|1\rangle = \alpha\sqrt{\frac{2}{\ell}}\sin\frac{\pi x}{\ell} + \beta\sqrt{\frac{2}{\ell}}\sin\frac{2\pi x}{\ell}$

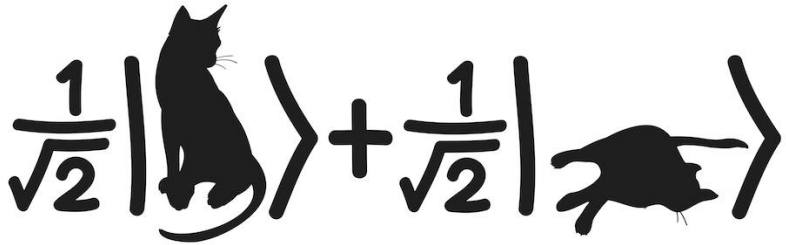
- Then:

$$|\psi(t)\rangle = \alpha\sqrt{\frac{2}{\ell}}e^{-\frac{iE_1 t}{\hbar}}\sin\frac{\pi x}{\ell} + \beta\sqrt{\frac{2}{\ell}}e^{-\frac{iE_2 t}{\hbar}}\sin\frac{2\pi x}{\ell}$$
$$= \sqrt{\frac{2}{\ell}}e^{-\frac{iE_1 t}{\hbar}}\left(\alpha\sin\frac{\pi x}{\ell} + \beta e^{-\frac{i(E_2-E_1)t}{\hbar}}\sin\frac{2\pi x}{\ell}\right)$$

$\Delta E = E_2 - E_1 \approx 10\ eV$

$\nu \approx 2.5 \times 10^{15}\ Hz$

Quantum Mechanics & Quantum Computation

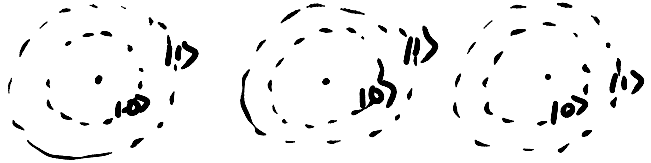


Umesh V. Vazirani
University of California, Berkeley

Lecture 11: Quantum Circuits

n qubit systems

Exponential Growth



- One qubit $\in \mathbb{C}^2$ $\alpha_0|0\rangle + \alpha_1|1\rangle$
- Two qubits $\in \mathbb{C}^4$ $\alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$
- Three qubits $\in \mathbb{C}^8$ $\alpha_{000}|000\rangle + \alpha_{001}|001\rangle + \alpha_{010}|010\rangle + \alpha_{011}|011\rangle + \cdots + \alpha_{111}|111\rangle$

$\mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^2$

- n qubits $\in \mathbb{C}^{2^n}$ $\alpha_{0\ldots00}|0\cdots00\rangle + \alpha_{0\ldots01}|0\cdots01\rangle + \cdots + \alpha_{1\ldots11}|1\cdots11\rangle$

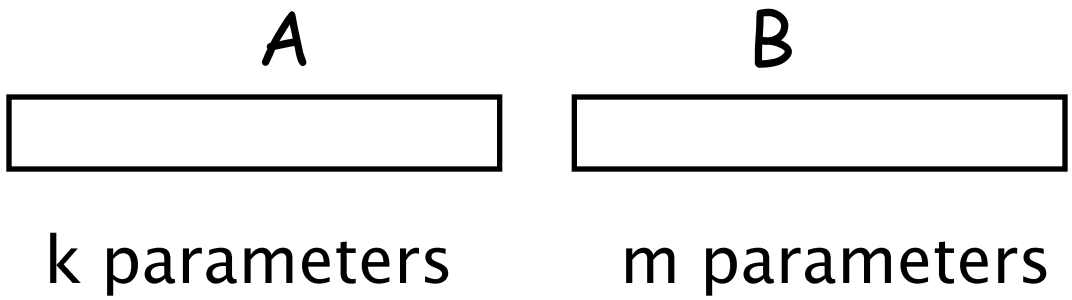
$\mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \cdots \otimes \mathbb{C}^2$

$n \approx 500$

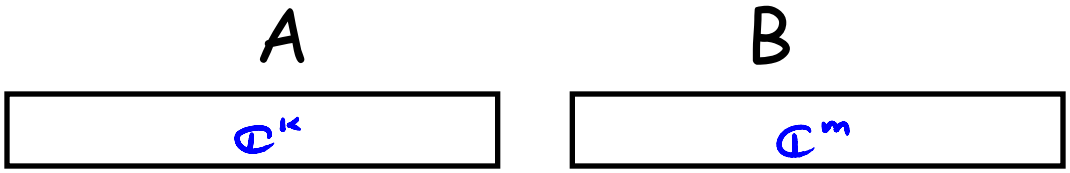
$2^n = 2^{500}$

$>$ (# particles in the universe) $\cdot$ (age of universe in femtoseconds)

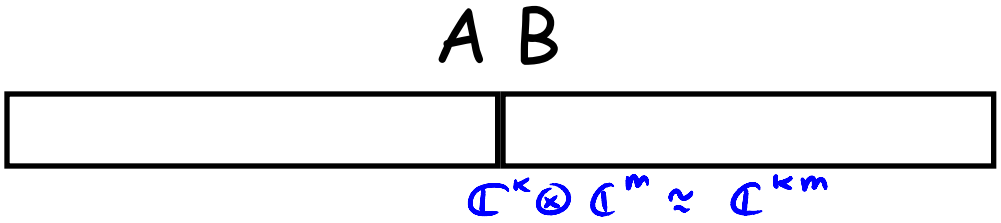
Tensor Products



Tensor Products



k parameters m parameters



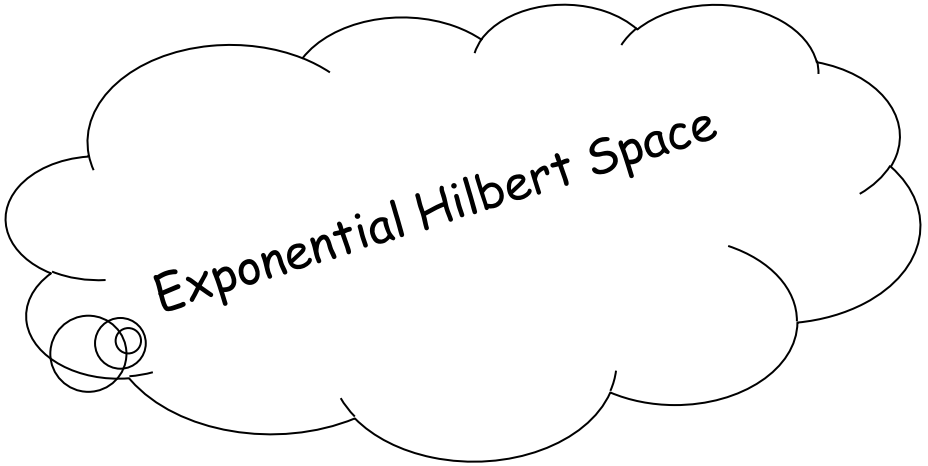
km parameters

Quantum entanglement

Exponential Growth

Axiom 1: Superposition principle

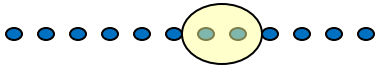
n qubits

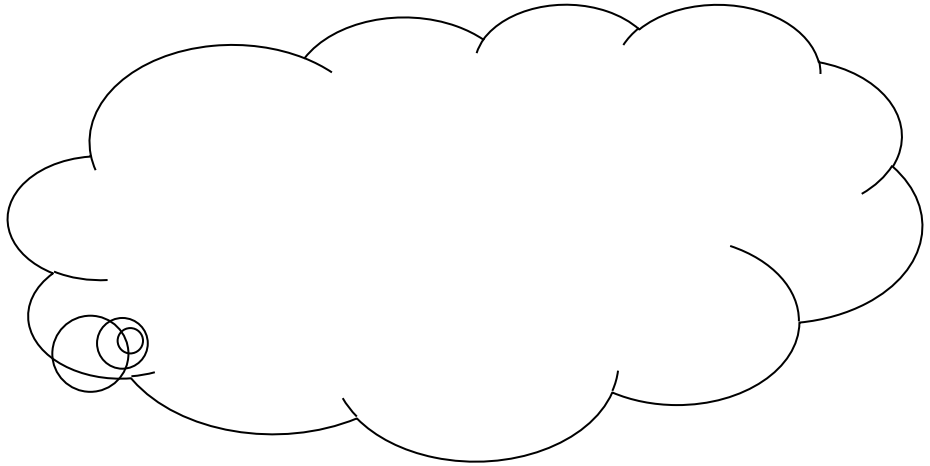


$$\Psi = \sum_x \alpha_x |x\rangle \qquad \sum_x |\alpha_x|^2 = 1$$

all n-bit strings

Axiom 2: Unitary Evolution



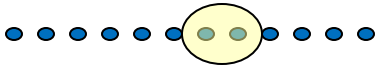


$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & i \\ 0 & 0 & -i & 0 \end{bmatrix} \otimes I_{n-2}$$

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

all n-bit strings

Axiom 2: Unitary Evolution



$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & i \\ 0 & 0 & -i & 0 \end{bmatrix} \otimes I_{n-2}$$

$$\Psi = \sum_x \alpha'_x |x\rangle$$

all n-bit strings

$\alpha_{0x'} \; |0x'\rangle$

$\alpha_{1x'} \; |1x'\rangle$

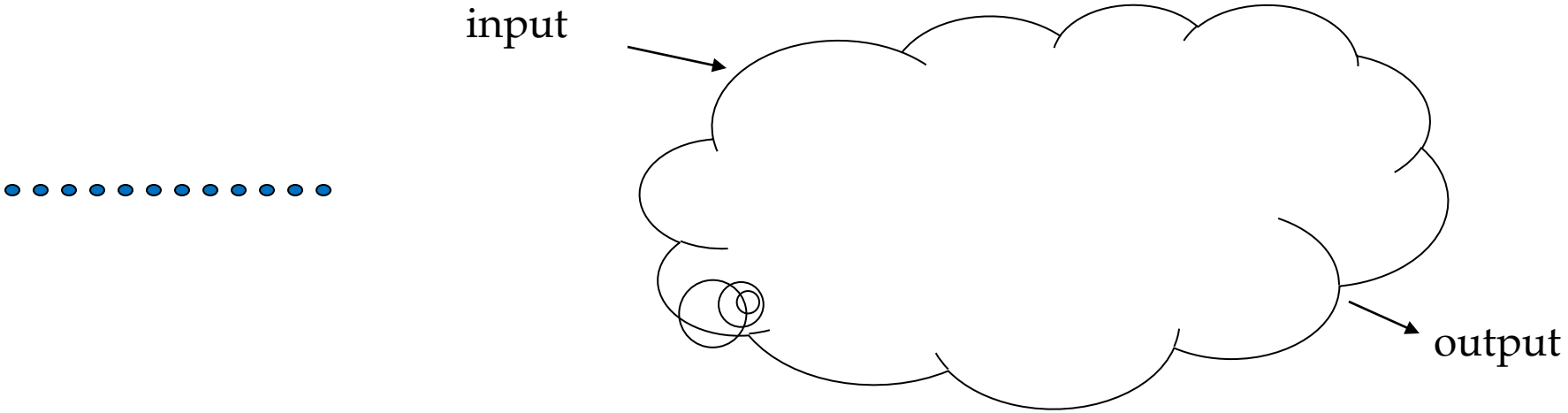
$\Big\}$

$\frac{\alpha_{0x'} + \alpha_{1x'}}{\sqrt{2}} \; |0x'\rangle$

$\frac{\alpha_{0x'} - \alpha_{1x'}}{\sqrt{2}} \; |1x'\rangle$

Updating all 2^n amplitudes α_x.

Limited Access – Measurement

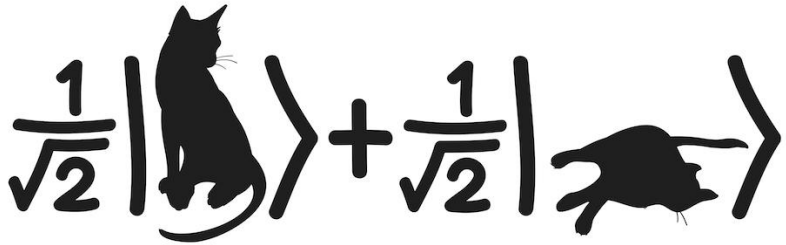


$$\Psi = \sum_x \alpha_x |x\rangle \qquad \sum_x |\alpha_x|^2 = 1$$

- Measurement: See $|x\rangle$ with probability $|\alpha_x|^2$

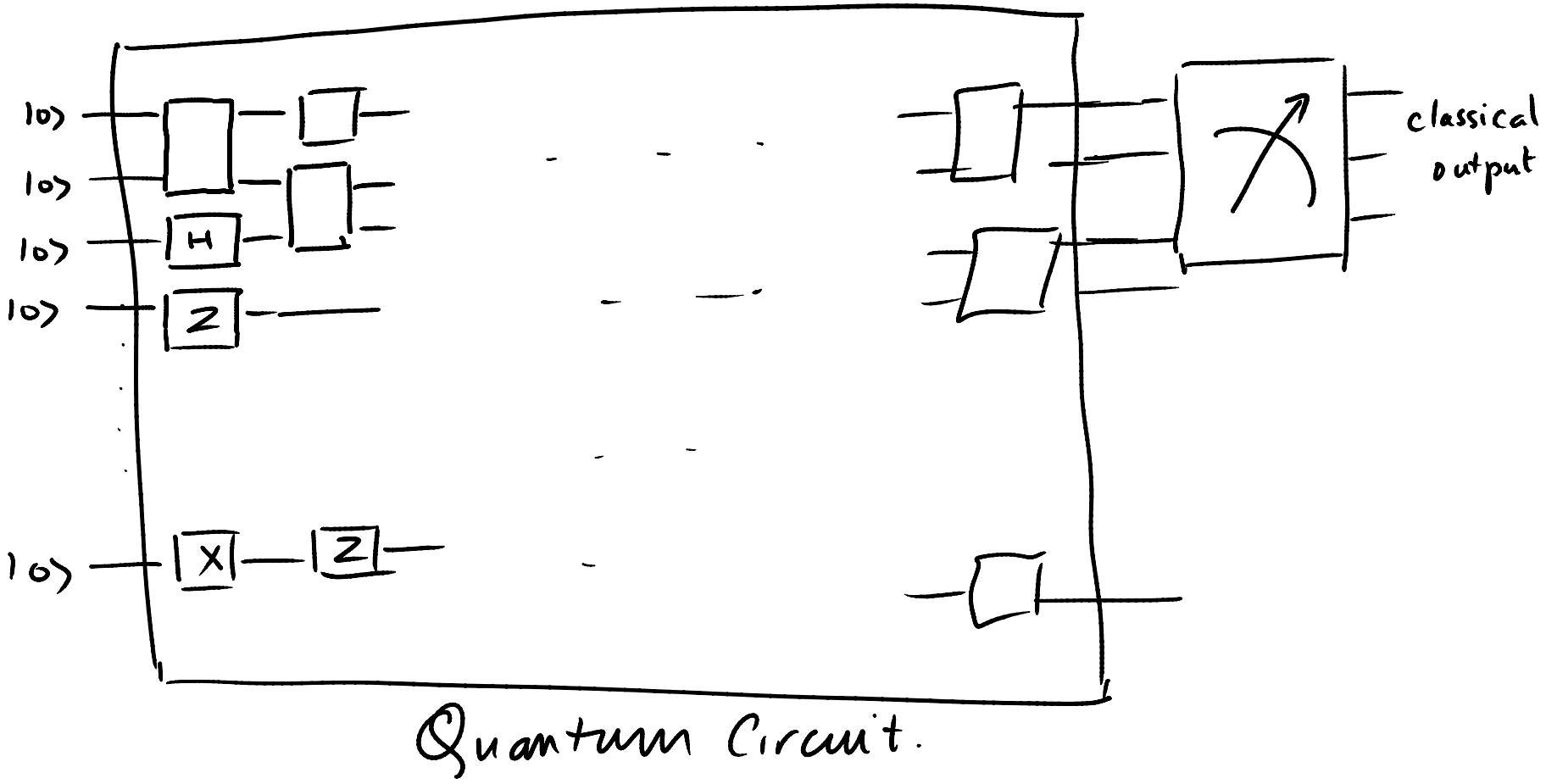
Quantum Mechanics & Quantum Computation

Umesh V. Vazirani
University of California, Berkeley



Lecture 11: Quantum Circuits

Universal family of gates

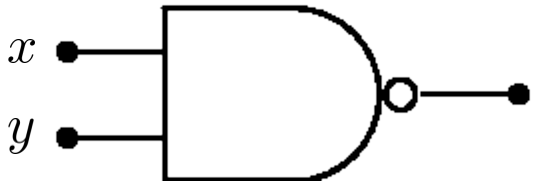


Quantum Circuit.

Universal quantum gate set

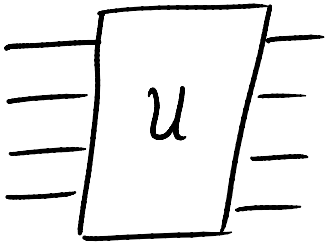
- In classical circuits, a certain set of gates enables universal computation.

- Ex) NAND is universal



1 unless $x = y = 1$

Universal quantum gate set



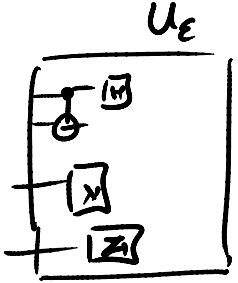
16 x 16

- Quantum analogue?
  - CNOT, H, X, Z, $\frac{\pi}{8}$ rotations

- What does it mean?
  - Clearly, we cannot implement an arbitrary U with infinite precision.
  - Instead, given ϵ, we implement U_ϵ which is ϵ-close to U.

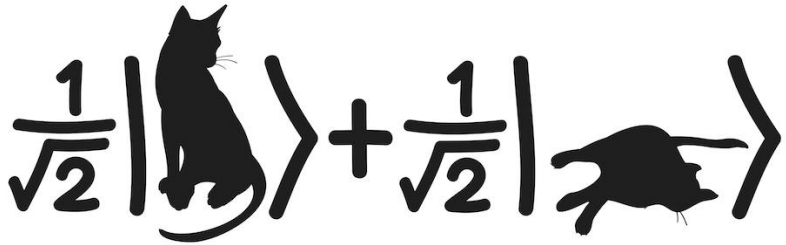
$d \times d$

$O(d^2 \log^3 \frac{1}{\epsilon})$



$\| U - U_\epsilon \| \leq \epsilon$.

Quantum Mechanics & Quantum Computation



Umesh V. Vazirani
University of California, Berkeley

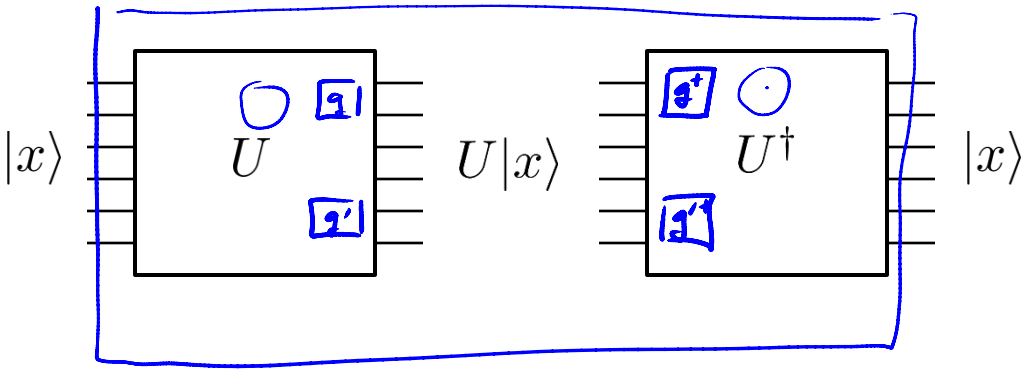
Lecture 11: Quantum Circuits

Reversible Computation

Reversible computation

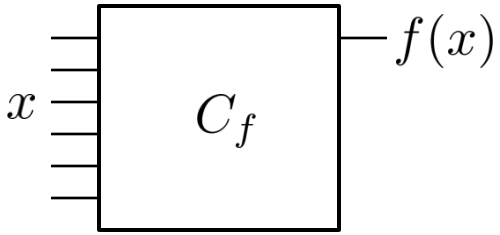
- Quantum computers are reversible.

- Why?



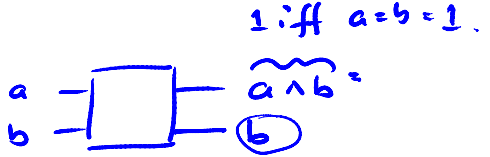
$UU^+ = U^+U = I.$

Implementing classical circuits

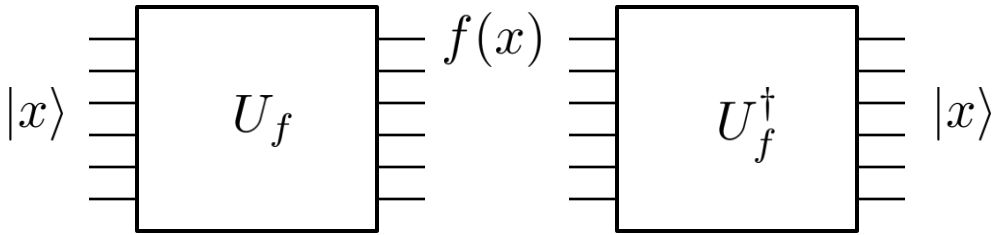


Classical circuit for computing a boolean function

$$f : \{0,1\}^n \to \{0,1\}$$



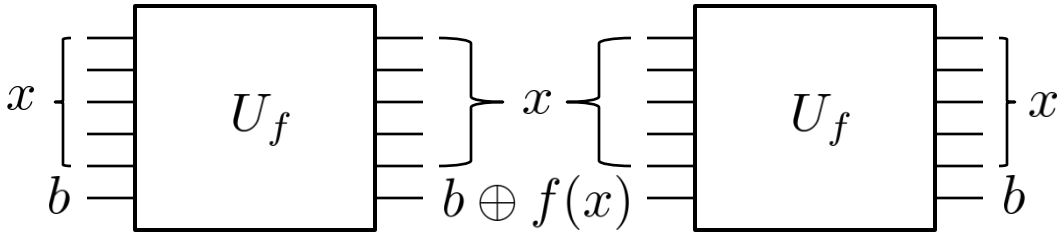
Imagine a quantum version of C_f:



Have to be reversible.

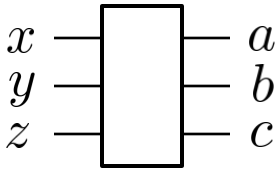
But classical gates throw away information!

Classical reversible computation



$b = 0$

Consider C-SWAP gate:



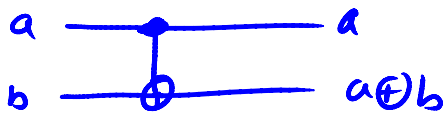
$$a = x$$

$$x = 0 \quad \Rightarrow \quad b = y, c = z$$

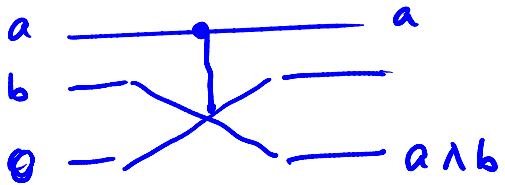
$$x = 1 \quad \Rightarrow \quad b = z, c = y$$

NOT $|0\rangle$ — X — $|1\rangle$

CNOT

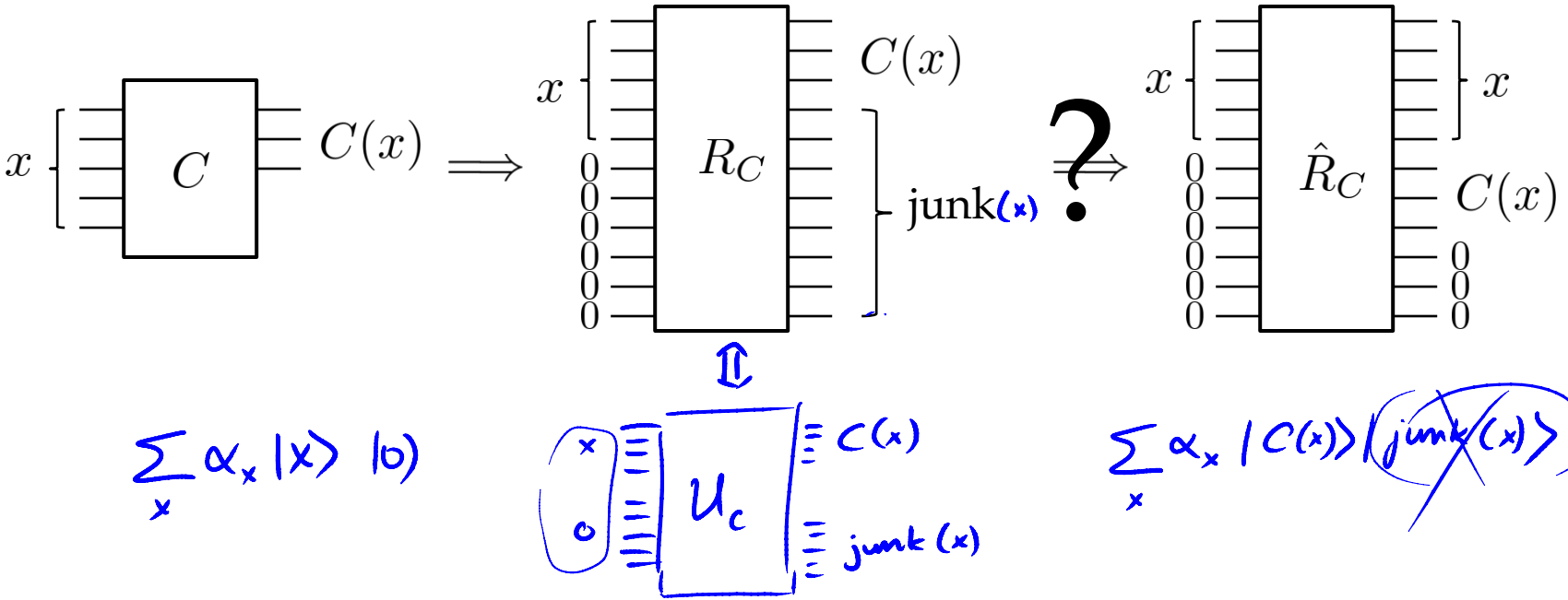


C-SWAP



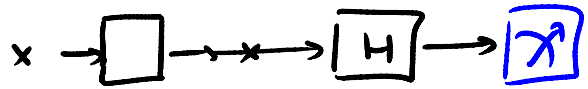
if $a=0$	0
if $a=1$	b

Classical reversible computation



Why remove junk?

Prevents interference.

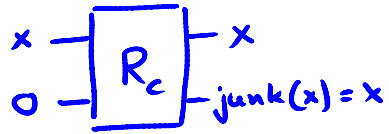


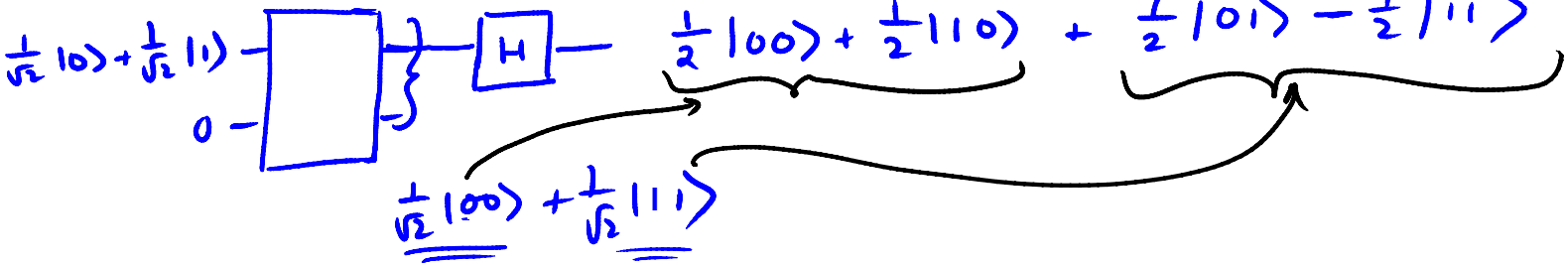
$\sum \alpha_x |x\rangle \longrightarrow \sum \alpha_x |x\rangle$

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

$\frac{1}{\sqrt{2}}|0\rangle \xrightarrow{H} \frac{1}{2}|0\rangle + \frac{1}{2}|1\rangle$

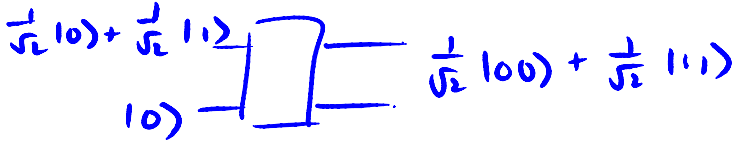
$\frac{1}{\sqrt{2}}|1\rangle \xrightarrow{H} \frac{1}{2}|0\rangle - \frac{1}{2}|1\rangle$



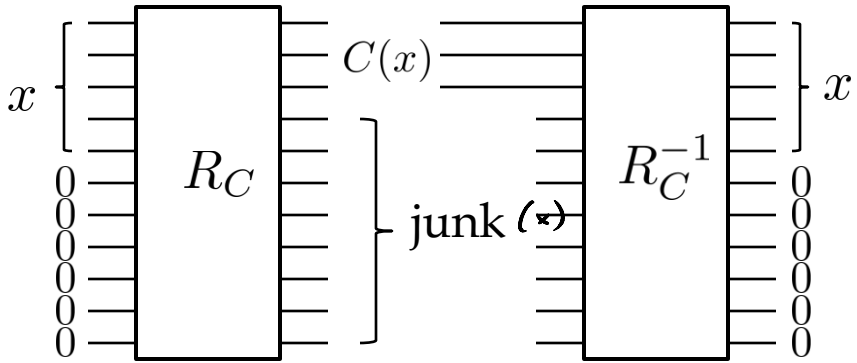


Why remove junk?

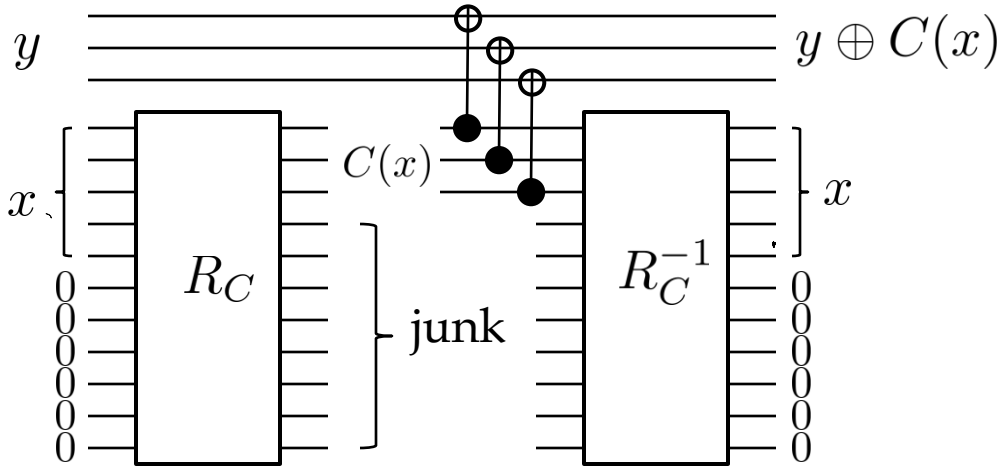
- Can't we just throw away the junk qubits?

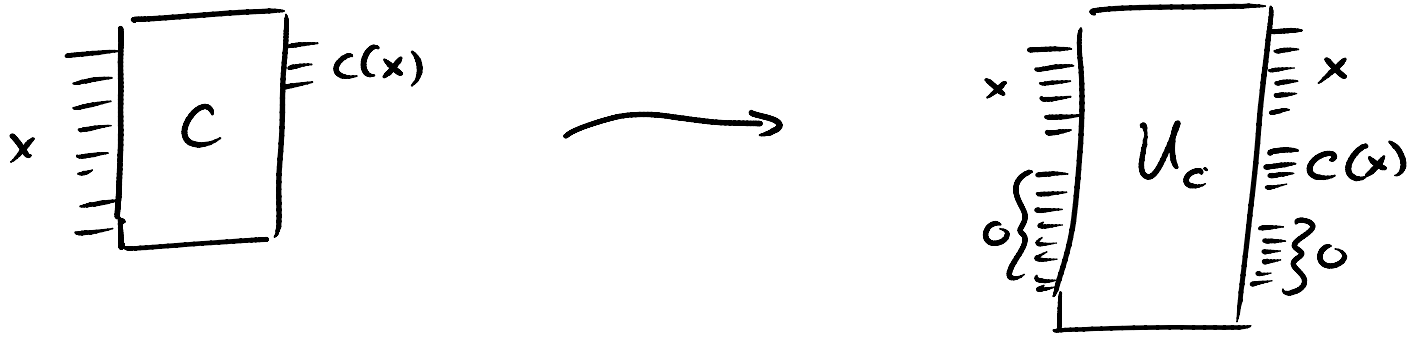


Classical reversible computation



Classical reversible computation

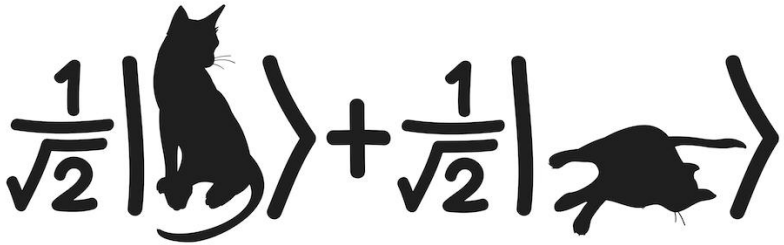




$$\sum_x \alpha_x |x\rangle |0\ldots0\rangle \xrightarrow{U_C} \sum_x \alpha_x |x\rangle |C(x)\rangle |0\ldots0\rangle$$

$$|xy\rangle = |x\rangle|y\rangle = |x\rangle \otimes |y\rangle$$

Quantum Mechanics & Quantum Computation

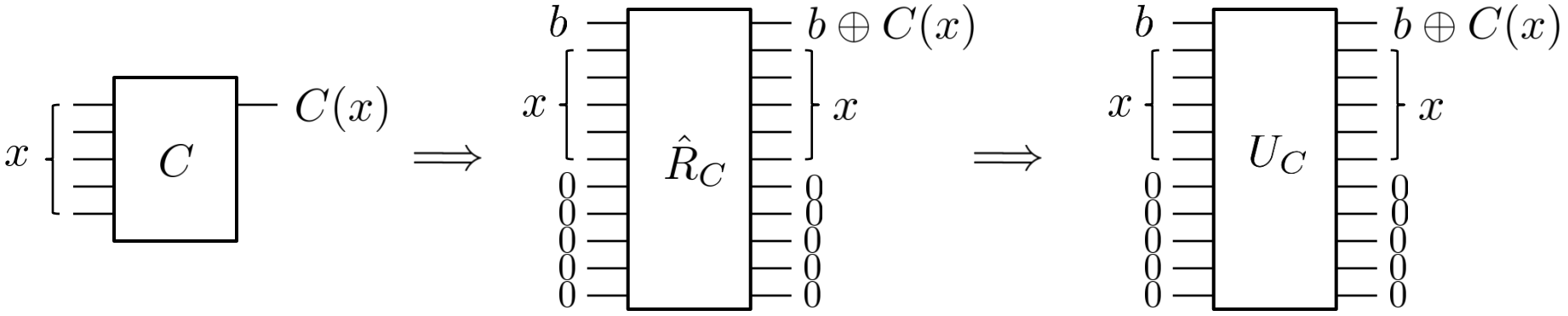


Umesh V. Vazirani
University of California, Berkeley

Lecture 12: Early Quantum Algorithms

Fourier Sampling

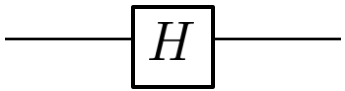
Classical reversible computation



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

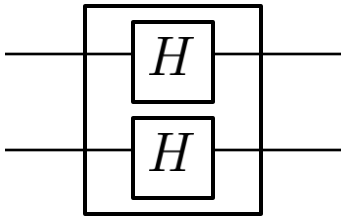
Hadamard Transform

- Basic Building Block



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

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

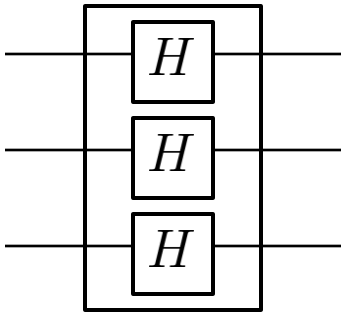


$$\begin{pmatrix} \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & -\frac{1}{2} & \frac{1}{2} & -\frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} \\ \frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} & \frac{1}{2} \end{pmatrix}$$

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

$$\vdots$$

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



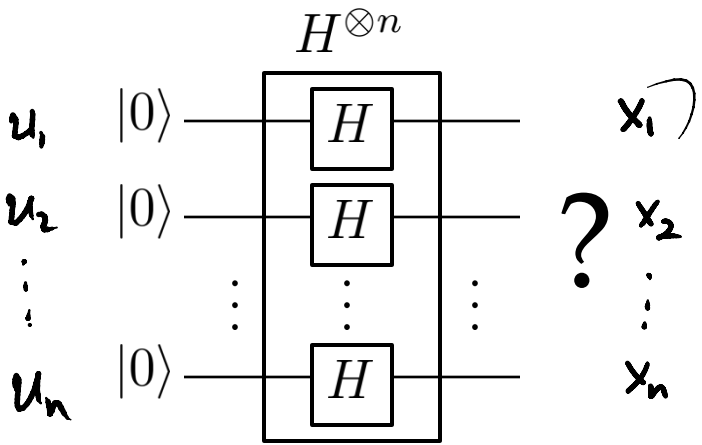
$$|000\rangle \rightarrow \frac{1}{2\sqrt{2}}|000\rangle + \cdots + \frac{1}{2\sqrt{2}}|111\rangle$$

$|001\rangle$

$|111\rangle \rightarrow$

What about for general n?

Hadamard Transform



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

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

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

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

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

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

eg $n = 3$

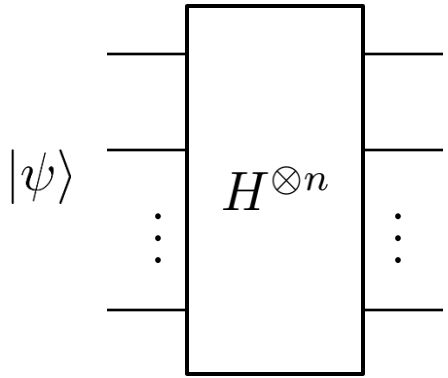
$u = 1\ 1\ 1$

$x = 1\ 0\ 1$

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

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

Fourier Sampling



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

$= \boxed{\chi} \rightarrow y$ w.p. $|\beta_y|^2$.

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

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" $u \in \{0,1\}^n$.

eg $n = 3$, $u = 101$

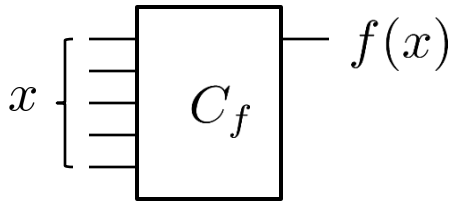
$x = x_1 x_2 x_3$

$f(x) = x_1 \oplus x_3$

$= x_1 + x_3 \pmod 2$

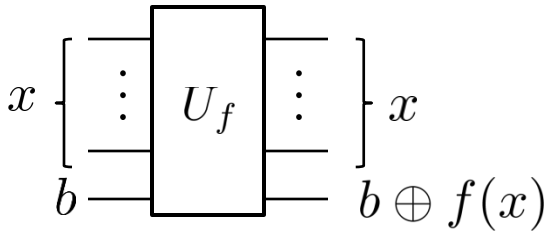
How do we figure out u with as few queries to f as possible?

Classical



Quantum?

$\sum_x \alpha_x$



Classically: Input $10\cdots0$ u_1, $010\cdots0$ u_2 ... Need $\geq n$ steps.

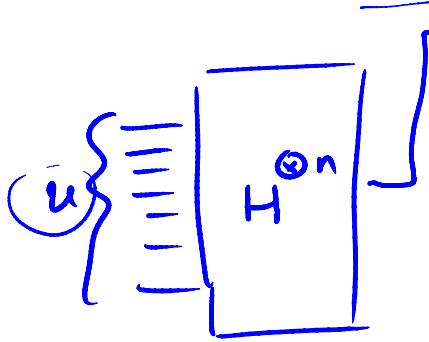
n steps $u = u_1 \cdots u_n$

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?

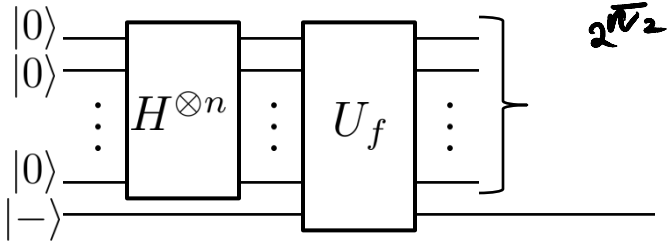
- Set up superposition $\frac{1}{2^{n/2}} \sum_x (-1)^{f(x)} |x\rangle$ $= \frac{1}{2^{n/2}} \sum_x (-1)^{u \cdot x} |x\rangle$
- Fourier sample to obtain u.



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



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

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

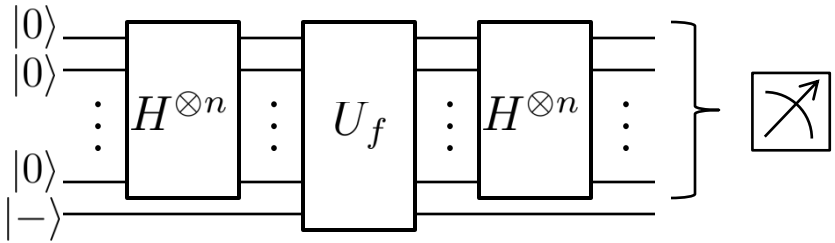
$|b\rangle = |-\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$

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

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

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.

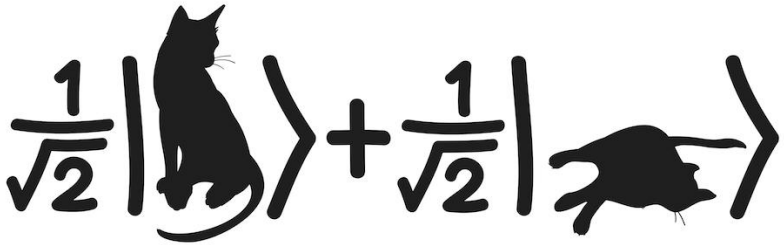
- Classical algorithms satisfy the recursion
  $T(n) > nT(n/2) + n$

  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

Quantum Mechanics & Quantum Computation



Umesh V. Vazirani
University of California, Berkeley

Lecture 12: Early Quantum Algorithms

Simon's Algorithm

Simon's algorithm

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.

000
101

101

x = 011
s = 101
x⊕s = 110

Example)

$n = 3$
$s = 101$

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

$2^n = N$

Classical Algorithm?

Collision

$\sqrt{N} = 2^{n/2}$

exponential time.

Simon's algorithm

- Set up random superposition $\frac{1}{\sqrt{2}}|r\rangle + \frac{1}{\sqrt{2}}|r \oplus s\rangle$

r random n bit string

- Fourier sample to get a random y : $y \cdot s = 0 (\mathrm{mod} 2)$
- Repeat steps n−1 times to generate n−1 linear equations in s.

  Solve for s.

$y = y_1 \cdots y_n$

$s = s_1 \cdots s_n$

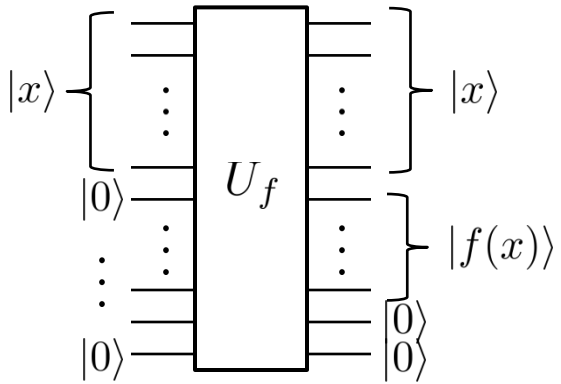
$$y_1^{(1)} s_1 + \cdots + y_n^{(1)} s_n \equiv 0 \pmod 2$$

$$\vdots \qquad\qquad \vdots$$

$$y_1^{(n-1)} s_1 + \cdots + y_n^{(n-1)} s_n \equiv 0 \pmod 2$$

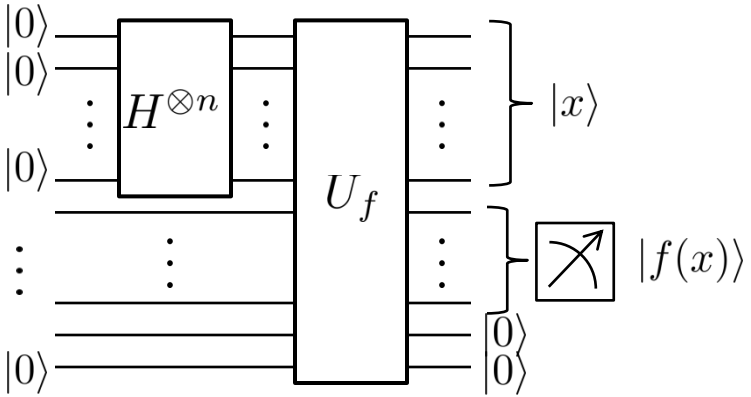
Settin up random superposition

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 $f(x) = f(x \oplus s)$)



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

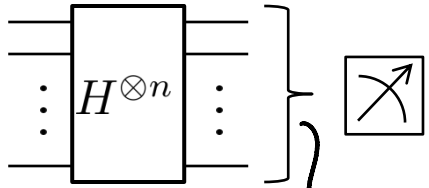
measure

see $f(x)$

1st register $= \frac{1}{\sqrt{2}}|x\rangle + \frac{1}{\sqrt{2}}|x \oplus s\rangle$

Fourier Sampling

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



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

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

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

Case 2 : $\quad s\cdot y \equiv 0 \pmod 2 \qquad \beta_y = \frac{(-1)^{r\cdot y}}{2^{\frac{n-1}{2}}} \qquad |\beta_y|^2 = \frac{1}{2^{n-1}}$

Reconstructing s:

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

$y^{(1)}, y^{(2)}, \cdots, y^{(n-1)}$

$n-1$ { $y_1 s_1 + \cdots + y_n s_n \equiv 0 \pmod 2$; $\vdots$

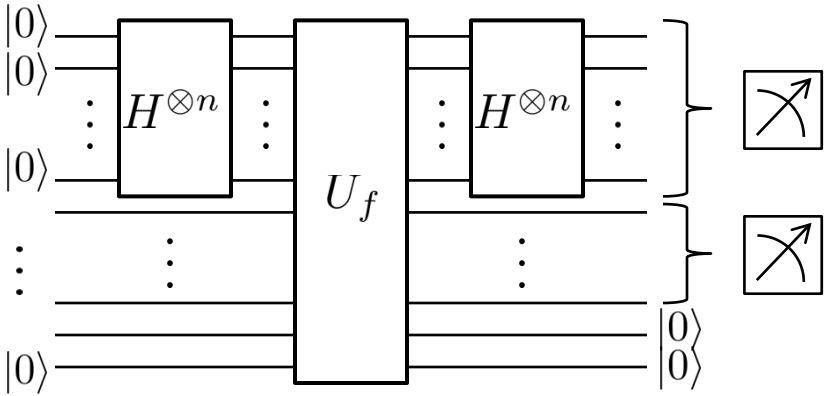
$\frac{1}{2^n} + \frac{1}{2^{n-1}} + \frac{1}{2^{n-2}} + \cdots + \frac{1}{4} \leq \frac{1}{2}$

$\therefore$ independent with prob $\geq \frac{1}{2}$.

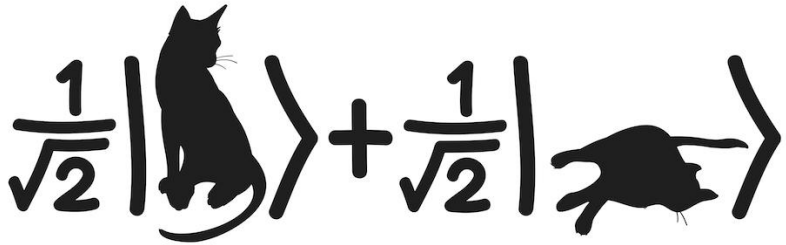
$f(x)$ $f(x \oplus s)$

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 $f(x) = f(x \oplus s)$)



Quantum Mechanics & Quantum Computation

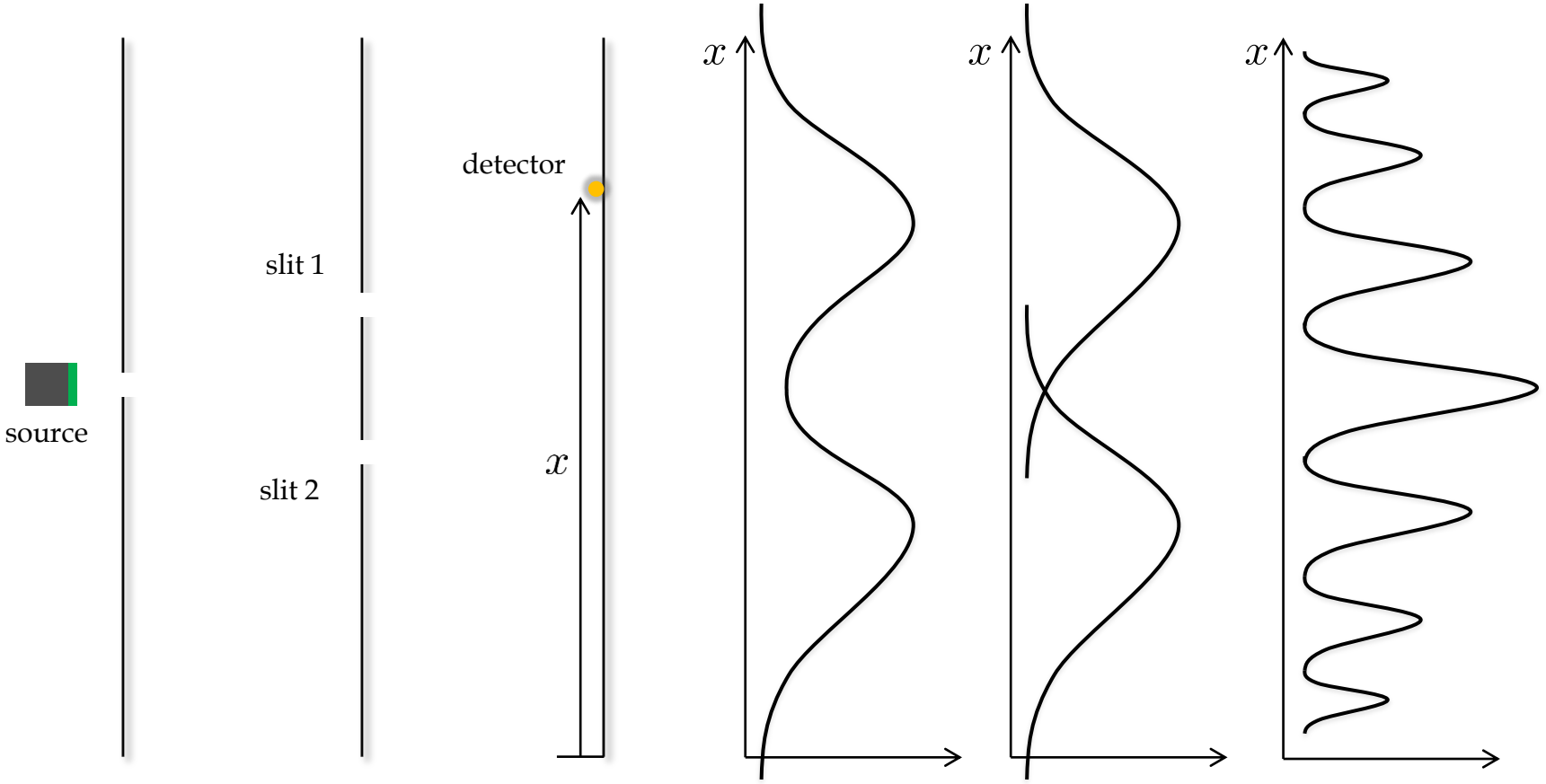


Umesh V. Vazirani
University of California, Berkeley

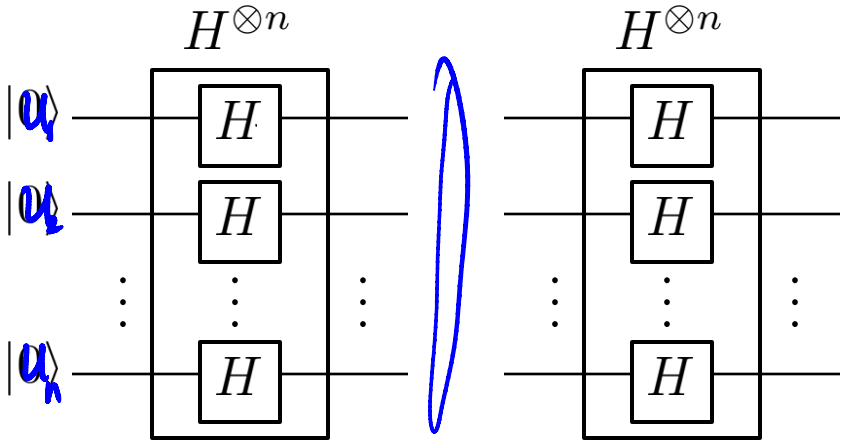
Lecture 12: Early Quantum Algorithms

Double Slit Expt.

Double-slit experiment



Quantum algorithms



$u = u_1 \cdots u_n$

$$\sum_{x \in \{0,1\}^n} \frac{(-1)^{u \cdot x}}{2^{n/2}} |x\rangle \xrightarrow{H^{\otimes n}} \sum_y \beta_y |y\rangle$$

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

Case 1: $y = u$

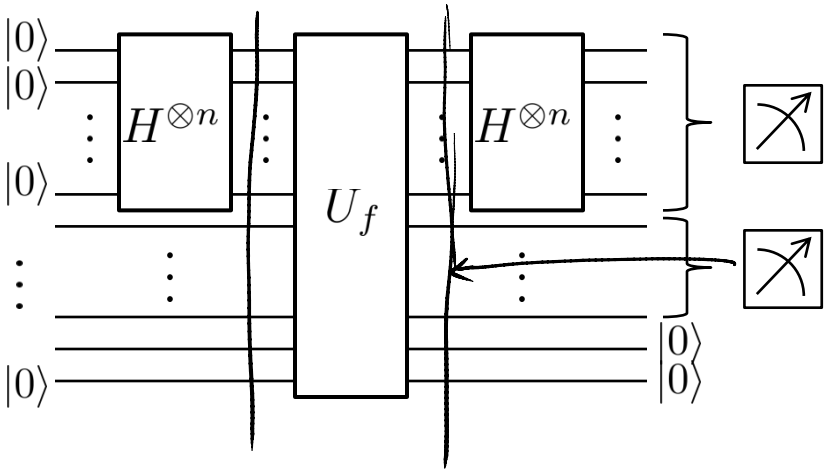
$$\beta_y = \sum_x \frac{1}{2^n} = 1.$$

Case 2: $y \neq u$

$$\beta_y = 0$$

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 $f(x) = f(x \oplus s)$)

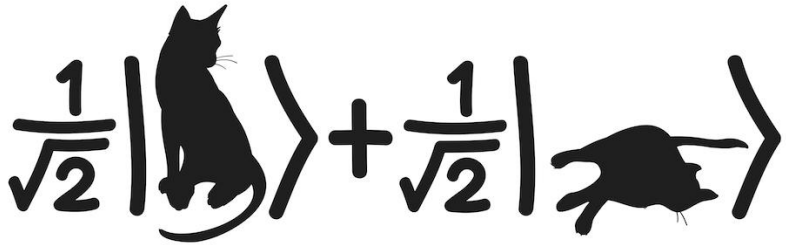


$y \cdot s = 0$

$\sum_x |x\rangle$

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

Quantum Mechanics & Quantum Computation



Umesh V. Vazirani
University of California, Berkeley

Lecture 13: Quantum Fourier Transform

Definition & Properties

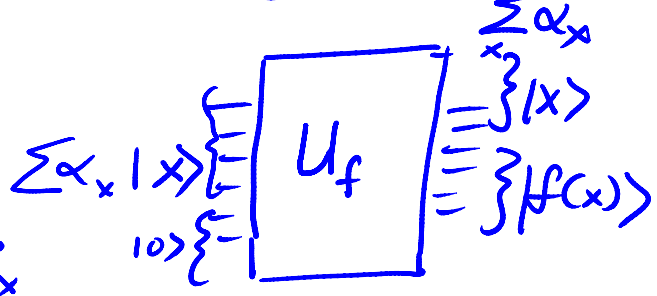
Period finding: $f: \{0, 1, \ldots, N-1\} \to S$

f is periodic with period r ← secret.

$\forall x \quad f(x) = f(x + r \pmod N)$

$x \not\equiv y \bmod r$ then $f(x) \neq f(y)$

Challenge: Find r.

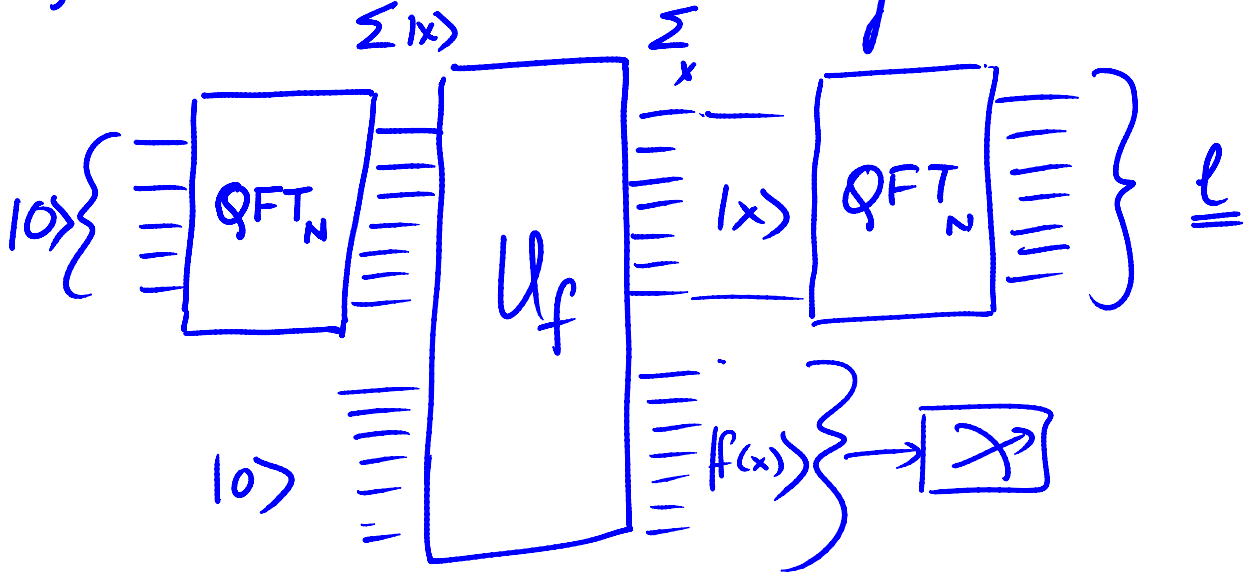


trials $\approx r$

$r = 5$

Quantum Algorithm $O(\log N)$

Quantum Period Finding:



Claim $\frac{\ell}{N} \approx \frac{k}{r}$

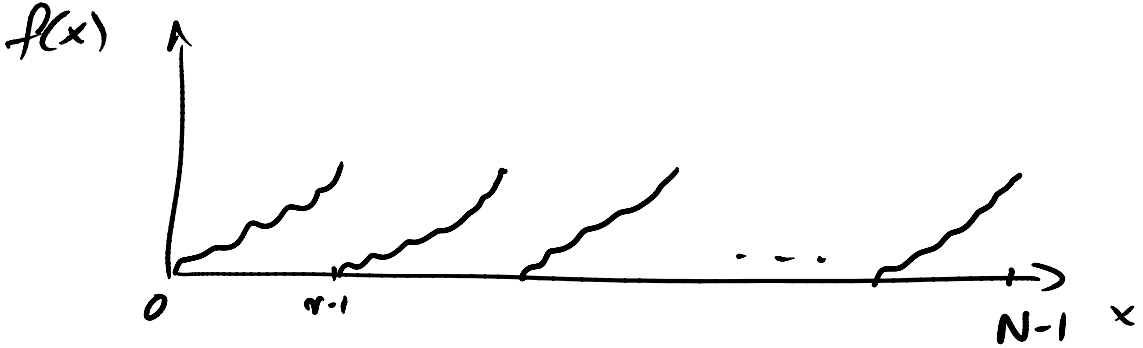
If $N \gg r$ can efficiently reconstruct r.

Special Case:

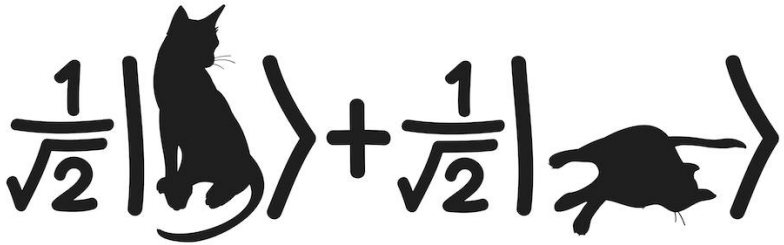
$$f : \{0, \ldots, N-1\} \to S$$

$$\forall x \quad f(x) = f(x + r \pmod N)$$

$$r \mid N$$



Quantum Mechanics & Quantum Computation

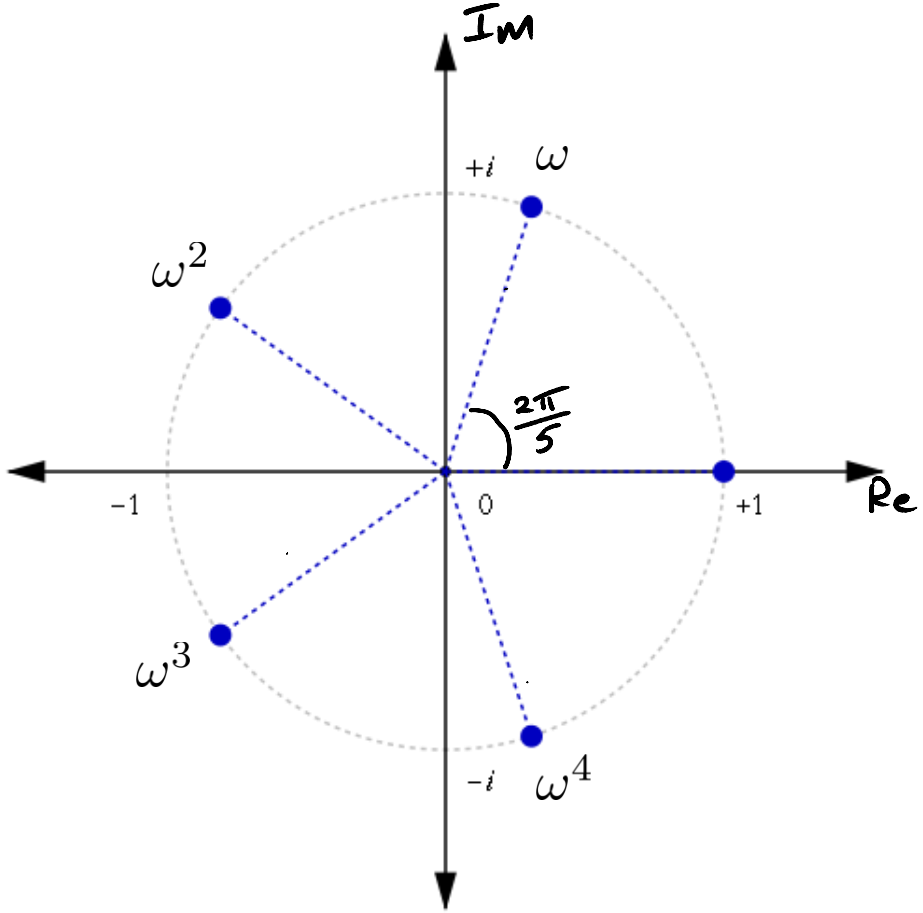


Umesh V. Vazirani
University of California, Berkeley

Lecture 13: Quantum Fourier Transform

Definition

Fourier transform



$$\omega^N = 1 \quad \omega \in \mathbb{C}$$

ω^d is also an N-th root:

$$(\omega^d)^N = e^{\frac{2\pi i \, d N}{N}} = 1$$

$i = \sqrt{-1}$

Fourier transform

$\frac{1}{N}\left(1+\omega^{j}+\omega^{2j}+\cdots+\omega^{(N-1)j}\right)=\begin{cases}1 & \text{if } j=0\\ 0 & \text{o.w.}\end{cases}$

F_N is unitary.

$$F_N = \frac{1}{\sqrt{N}}\begin{pmatrix} 1 & 1 & 1 & 1 & \cdots & 1 \\ 1 & \omega & \omega^2 & \omega^3 & \cdots & \omega^{N-1} \\ 1 & \omega^2 & \omega^4 & \omega^6 & \cdots & \omega^{2(N-1)} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{N-1} & \omega^{2(N-1)} & \omega^{3(N-1)} & \cdots & \omega^{(N-1)^2} \end{pmatrix}$$

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

$F_N =$ j — k — ω^{jk} $(F_N)_{jk} = \omega^{jk}$

Example: $N=4 \qquad \omega = i = \sqrt{-1}$

$$F_4 = \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{pmatrix}\begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} = \frac{1}{2}\begin{pmatrix} 1 \\ i \\ -1 \\ -i \end{pmatrix} = \frac{1}{2}|0\rangle + \frac{i}{2}|1\rangle - \frac{1}{2}|2\rangle - \frac{i}{2}|3\rangle$$

$$\alpha_0|0\rangle + \alpha_1|1\rangle + \alpha_2|2\rangle + \alpha_3|3\rangle = \begin{pmatrix} \alpha_0 \\ \alpha_1 \\ \alpha_2 \\ \alpha_3 \end{pmatrix}$$

$$F_N = \frac{1}{\sqrt{N}} \begin{pmatrix} 1 & 1 & \cdots & 1 \\ 1 & \omega & \omega^2 & \cdots & \omega^{N-1} \\ \vdots & & & & \vdots \\ 1 & \omega^{N-1} & \cdots & & \omega^{(N-1)^2} \end{pmatrix} \begin{pmatrix} \alpha_0 \\ \alpha_1 \\ \vdots \\ \alpha_{N-1} \end{pmatrix} = \begin{pmatrix} \beta_0 \\ \beta_1 \\ \vdots \\ \beta_{N-1} \end{pmatrix}$$

$O(N^2)$ steps

Fast Fourier Transform

FFT : $O(N \log N)$

exponential

$n = \log N$

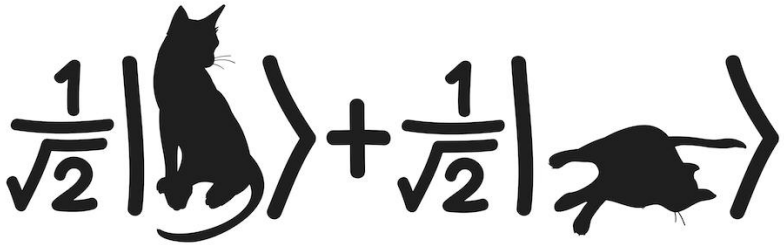
n

$$\sum_j \alpha_j |j\rangle \longrightarrow \sum_k \beta_k |k\rangle$$

QFT $O(n^2)$ steps $= O(\log^2 N)$

Measure : see $\underline{\underline{k}}$ with probability $|\beta_k|^2$

Quantum Mechanics & Quantum Computation



Umesh V. Vazirani
University of California, Berkeley

Lecture 13: Quantum Fourier Transform

Period Finding

Fourier transform

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

$$F_N = \frac{1}{\sqrt{N}} \begin{pmatrix} 1 & 1 & 1 & 1 & \cdots & 1 \\ 1 & \omega & \omega^2 & \omega^3 & \cdots & \omega^{N-1} \\ 1 & \omega^2 & \omega^4 & \omega^6 & \cdots & \omega^{2(N-1)} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{N-1} & \omega^{2(N-1)} & \omega^{3(N-1)} & \cdots & \omega^{(N-1)^2} \end{pmatrix}$$

$$(F_N)_{jk} = \omega^{jk}$$

$$\frac{1}{\sqrt{N}} \begin{pmatrix} 1 & 1 & \cdots & 1 \\ 1 & \omega & \cdots & \omega^{N-1} \\ \vdots & & & \\ 1 & \omega^{N-1} & \cdots & \omega^{(N-1)^2} \end{pmatrix} \begin{pmatrix} \alpha_0 \\ \alpha_1 \\ \vdots \\ \alpha_{N-1} \end{pmatrix} = \begin{pmatrix} \beta_0 \\ \beta_1 \\ \vdots \\ \beta_{N-1} \end{pmatrix}$$

$\boxed{\mathcal{F}}$ see k w.p. $|\beta_k|^2$

$$F_N\left(\sum_j \alpha_j |j\rangle\right) = \sum_k \beta_k |k\rangle$$

Convolution - multiplication property of F.T.

Shift

$$\frac{1}{\sqrt{N}} \begin{pmatrix} 1 & 1 & \cdots & 1 \\ 1 & \omega & \cdots & \omega^{N-1} \\ 1 & & & \\ \vdots & & & \\ 1 & \omega^{N-1} & \cdots & \end{pmatrix} \begin{pmatrix} \alpha_{N-1} \\ \alpha_0 \\ \alpha_1 \\ \vdots \\ \alpha_{N-2} \end{pmatrix} = \begin{pmatrix} 1 & \beta_0 \\ \omega & \beta_1 \\ \omega^2 & \vdots \\ \vdots & \vdots \\ \omega^{N-1} & \beta_{N-1} \end{pmatrix}$$

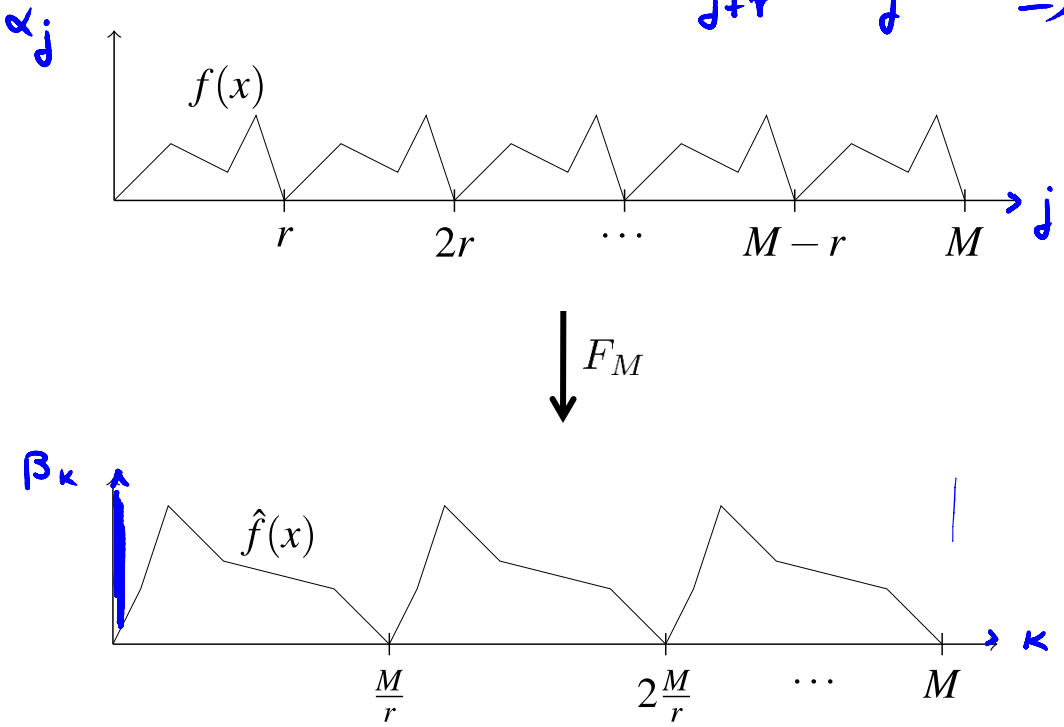
$\boxed{\mathcal{F}}$ see k w.p. $|\beta_k|^2$

Quantum Fourier Sampling:

Fourier transform

$$F_M\left(\sum_{j=0}^{M-1}\alpha_j|j\rangle\right)=\sum_{k=0}^{M-1}\beta_k|k\rangle$$

$$\alpha_{j+r}=\alpha_j \quad\Rightarrow\quad \beta_{k+\frac{M}{r}}=\beta_k$$



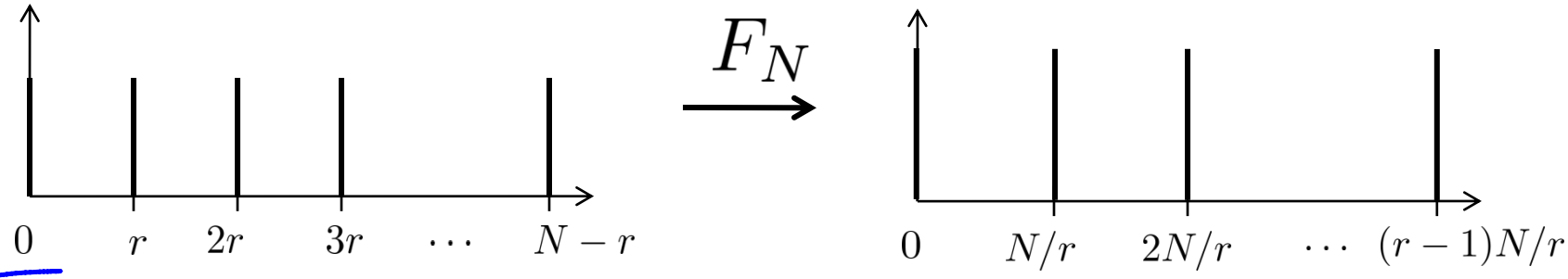
$$F_M\left(\frac{1}{\sqrt{M}}\sum_{j=0}^{M-1}|j\rangle\right)=|0\rangle$$

$r=1 \qquad \frac{M}{r}=M$

Fourier transform

$r \mid N$

We will prove a special case:



$$\sqrt{\frac{r}{N}}\left(|0\rangle + |r\rangle + |2r\rangle + \cdots + |N-r\rangle\right) \xrightarrow{F_N} \frac{1}{\sqrt{r}}\left(|0\rangle + |\tfrac{N}{r}\rangle + |\tfrac{2N}{r}\rangle + \cdots + |\tfrac{(r-1)N}{r}\rangle\right)$$

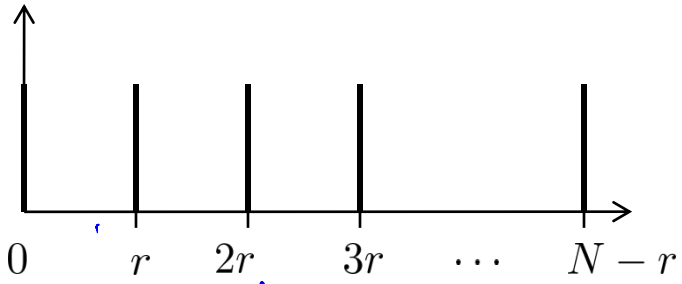
$$|0\rangle \xrightarrow{F_N} \frac{1}{\sqrt{N}}\left(|0\rangle + |1\rangle + |2\rangle + \cdots + |N-1\rangle\right)$$

$$\frac{1}{\sqrt{N}}\begin{pmatrix} 1 & 1 & \cdots & 1 \\ 1 & \omega & \cdots & \omega^{N-1} \\ \vdots & \omega^2 & \cdots & \vdots \\ 1 & \omega^{N-1} & \cdots & \cdots \end{pmatrix}\begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} = \frac{1}{\sqrt{N}}\begin{pmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{pmatrix}$$

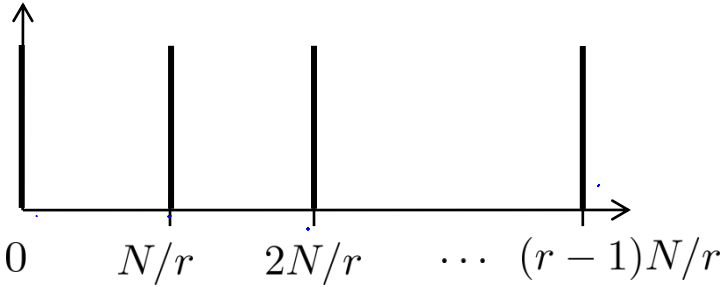
Fourier transform

$r \mid N$

We will prove a special case:



F_N



$$\sqrt{\frac{r}{N}} \sum_{j=0}^{\frac{N}{r}-1} |jr\rangle \xrightarrow{F_N} \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} |k\tfrac{N}{r}\rangle$$

$$F_N = \frac{1}{\sqrt{N}} \left(\omega^{xy} \right)_{x,y}$$

$$\sum_{j=0}^{\frac{N}{r}-1} \sqrt{\frac{r}{N}} \frac{1}{\sqrt{N}} \omega^{jrkN/r}$$

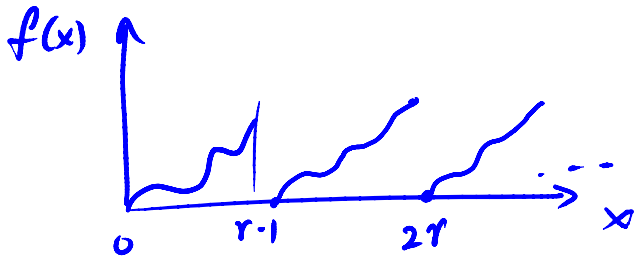
$$= \frac{\sqrt{r}}{N} \sum_{j=0}^{\frac{N}{r}-1} \omega^{jkN} = \frac{\sqrt{r}}{N} \times \frac{N}{r} = \frac{1}{\sqrt{r}}$$

Period Finding:

$f : \{0, 1, \ldots, N-1\} \to S$

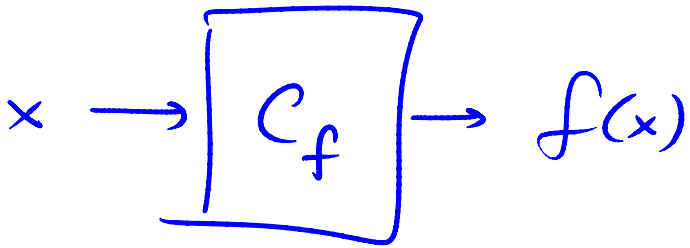
f is periodic with period r/N.

$f(x) = f(x + r \pmod N)$



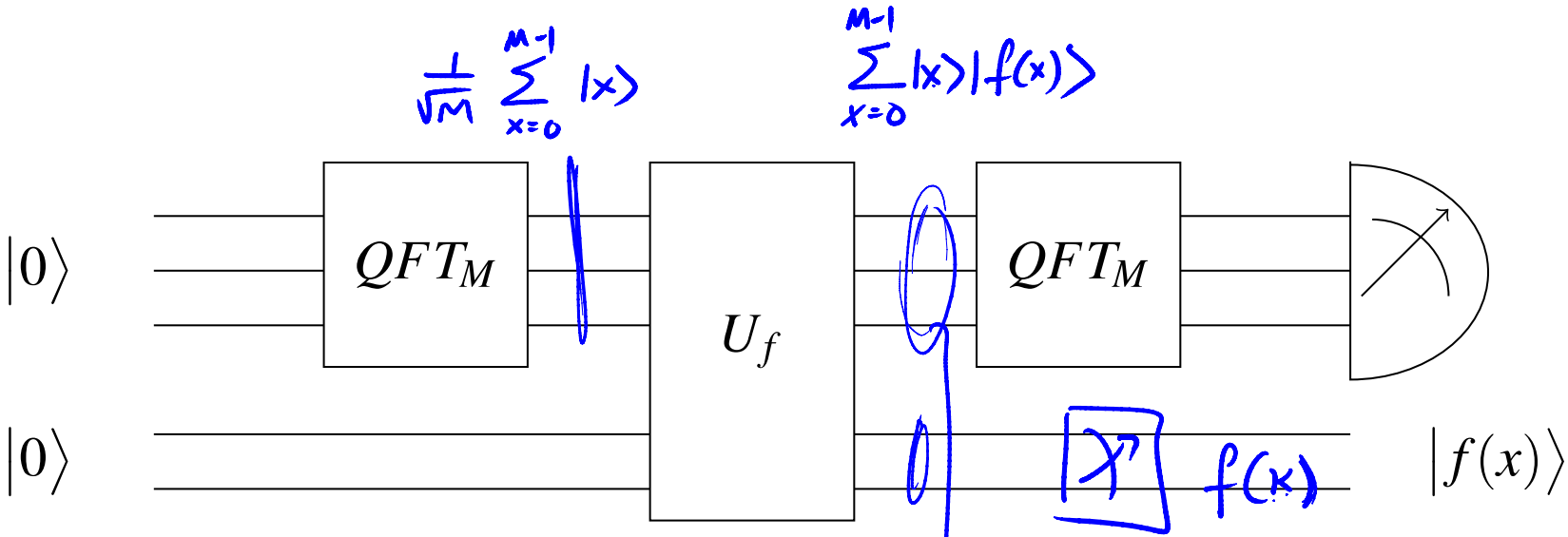
Given a black box of C_f.

Determine r.



Period finding

$f: \{0, \ldots, M-1\} \to S$ $\quad r \mid M$ $\quad f(x) = f(x+r)$

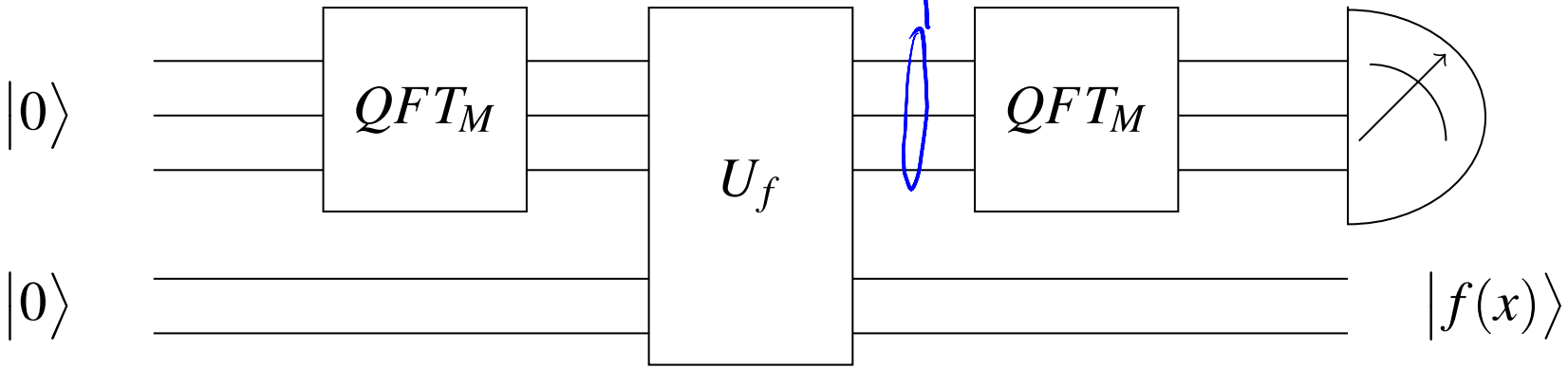


$$\frac{1}{\sqrt{M}} \begin{pmatrix} 1 & \cdots & 1 \\ 1 & \omega & \cdots \\ \vdots & & \\ 1 & \omega^{N-1} & \cdots \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} = \frac{1}{\sqrt{M}} \begin{pmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{pmatrix}$$

$$\sqrt{\frac{r}{M}} \left(|k\rangle + |k+r\rangle + |k+2r\rangle + \cdots + |k+M-r\rangle \right)$$

Period finding

$$\sqrt{\frac{r}{M}} \sum_{j=0}^{\frac{M}{r}-1} |jr+k\rangle \xrightarrow{QFT_M} \frac{1}{\sqrt{r}} \sum_{l=0}^{r-1} |l\tfrac{M}{r}\rangle$$

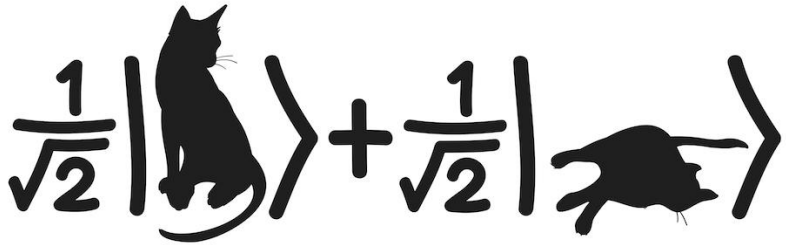


$s\frac{M}{r}$ where $s \in_R \{0, 1, \ldots, r-1\}$

Repeat GCD $= \frac{M}{r}$

Quantum Mechanics & Quantum Computation

Umesh V. Vazirani
University of California, Berkeley

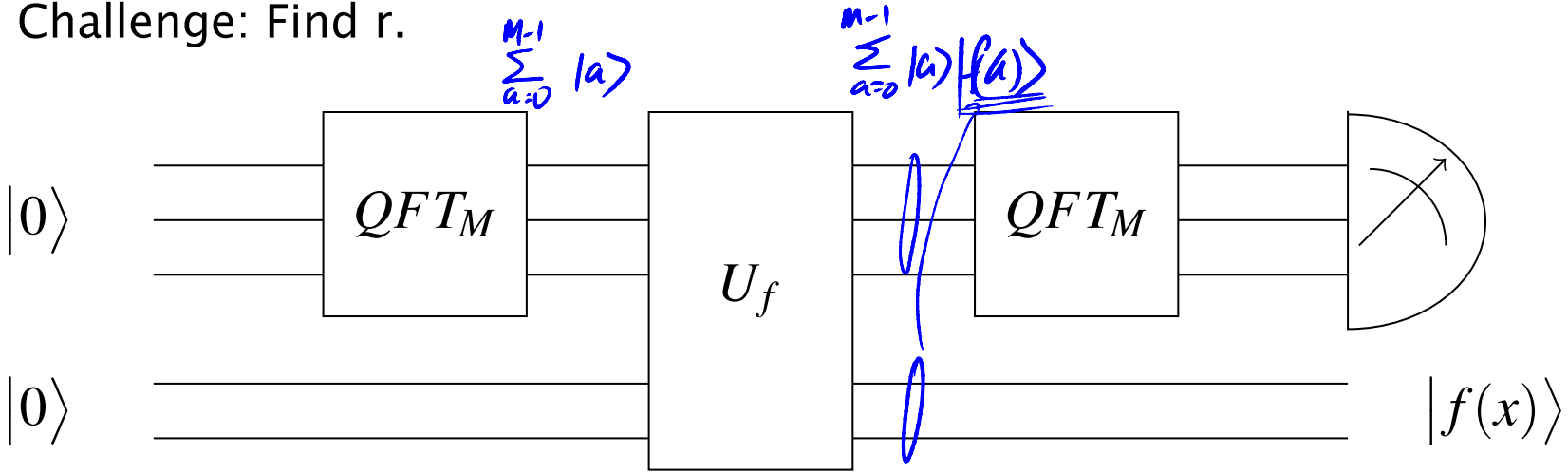


Lecture 14: Quantum Factoring

Shor's Algorithm

Period finding

f: {0, 1, …, M−1} → S, such that for all x, f(x) = f(x+r).
Challenge: Find r.



$N = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$

$N = P \cdot Q$

$N \approx 2^n$

1000 digit

500 digit 10^{500}

n bits $\exp(O(\sqrt{n}))$

↑ Classical

quantum – $O(n^3)$

modular arithmetic

- Modular arithmetic.
- a = b (mod N). e.g. 3 = 15 (mod 12)
- “Algorithms” by Dasgupta, Papadimitriou, Vazirani

  www.cs.berkeley.edu/~vazirani/algorithms.html

  Chapter 1: Modular Arithmetic
  Chapter 2 (2nd half): Fast fourier transform
  Chapter 10: Quantum factoring.

$N = 21$

$\sqrt{1} = \pm 1.$

$1^2 \equiv 1 \pmod{21}$

$-1^2 = 20^2 \equiv 1 \pmod{21}$

$400 \equiv 1 \pmod{21}$

$8^2 = 64 \equiv 1 \pmod{21}$

$-8^2 = 13^2 \equiv 1 \pmod{21}$

$\gcd(\overbrace{8+1}^{9}, 21) = 3$

$\gcd(\overbrace{13+1}^{14}, 21) = 7$

$\gcd(\underbrace{8-1}_{7}, 21) = 7$

$\gcd(\underbrace{13-1}_{12}, 21) = 3$

Lemma: If x is a nontrivial square root of 1 (mod N), then gcd(x+1, N) (and gcd(x−1,N)) is a nontrivial factor of N.

$x \not\equiv \pm 1 \pmod N \iff N \nmid (x \pm 1)$

$x^2 \equiv 1 \pmod N \iff x^2 - 1 \equiv 0 \pmod N$

$\iff N \mid (x^2 - 1)$

$\iff N \mid (x+1)(x-1)$

$\gcd(x+1, N)$ $\qquad$ $\gcd(x-1, N)$

P $\qquad$ Q

$2^0 = 1 \pmod{21}$

$2^1 = 2 \pmod{21}$

$2^2 = 4 \pmod{21}$

$2^3 = 8 \pmod{21}$

$2^4 = 16 \pmod{21}$

$2^5 = 11 \pmod{21}$

$2^6 = 1 \pmod{21}$

$$2^6 \equiv 1 \pmod{21}$$

$$(2^3)^2 \equiv 2^6 \equiv 1 \pmod{21}$$

$$8^2 \equiv 1 \pmod{21}$$

Lemma: Let N be an odd composite, with at least two distinct prime factors, and let x be uniformly random between 0 and N−1. If gcd(x, N) = 1, then with probability at least ½, the order r of x (mod N) is even, and $x^{r/2}$ is a nontrivial square root of 1 (mod N)

order of x

$1 \equiv x^r \pmod N$

r even & $y = x^{r/2} \not\equiv \pm 1 \bmod N$

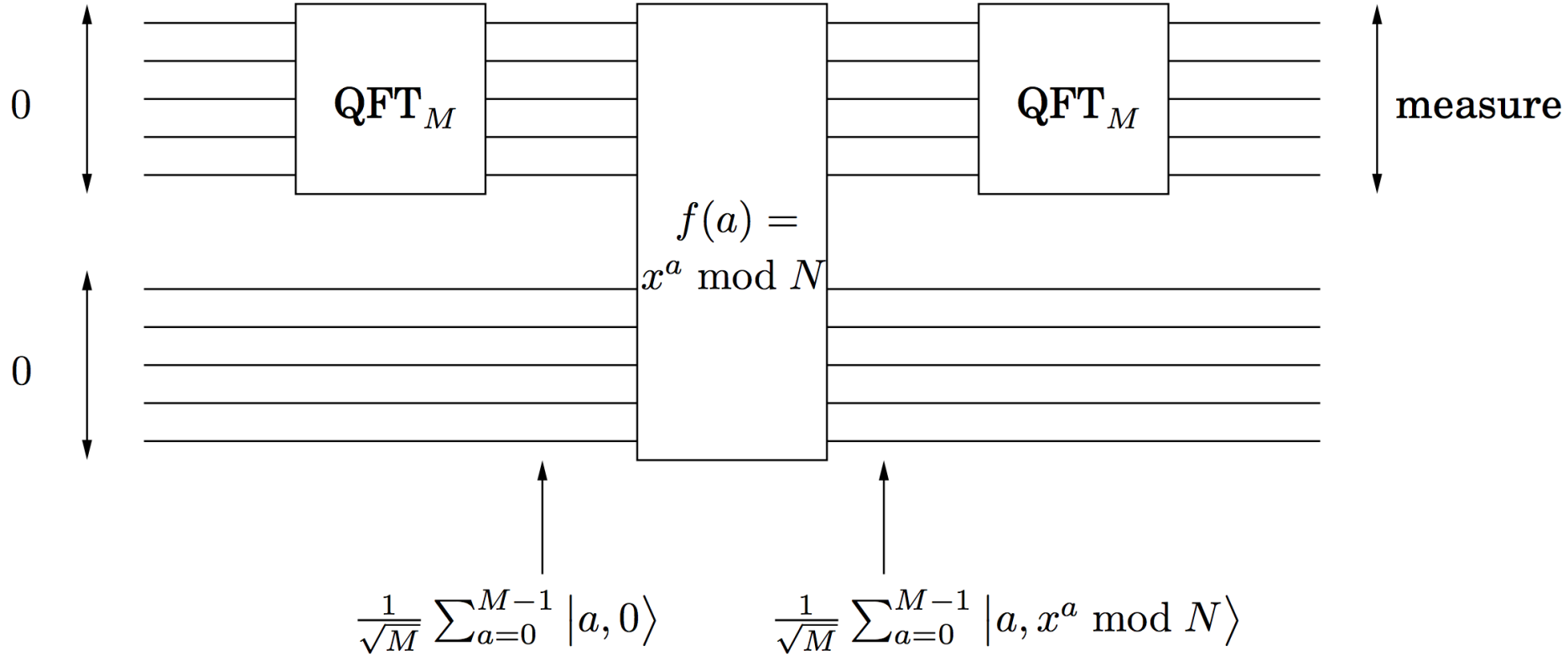
$y \not\equiv \pm 1 \bmod N$ $\qquad$ $y^2 = x^r \equiv 1 \pmod N$

$X = 2$

$N = 21$

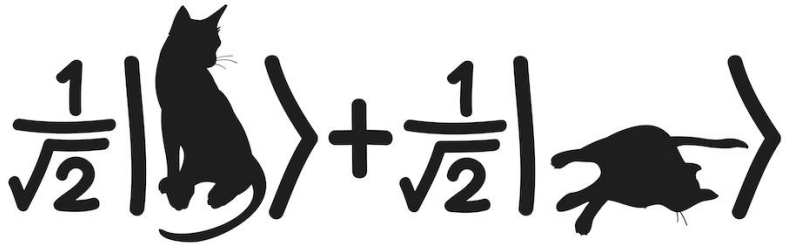
$$\frac{1}{\sqrt{M}} \sum_{a=0}^{M-1}$$

a	$f(a) = X^a \pmod N$
0	1
1	2
2	4
3	8
4	16
5	11
6	1
7	2
8	4
9	8
10	16
11	11
12	1
13	2
14	4
⋮	


0
0
$\mathbf{QFT}_M$
$f(a) = x^a \bmod N$
$\mathbf{QFT}_M$
measure
$\frac{1}{\sqrt{M}} \sum_{a=0}^{M-1} |a, 0\rangle$
$\frac{1}{\sqrt{M}} \sum_{a=0}^{M-1} |a, x^a \bmod N\rangle$

Quantum Mechanics & Quantum Computation

Umesh V. Vazirani
University of California, Berkeley



Lecture 14: Quantum Factoring

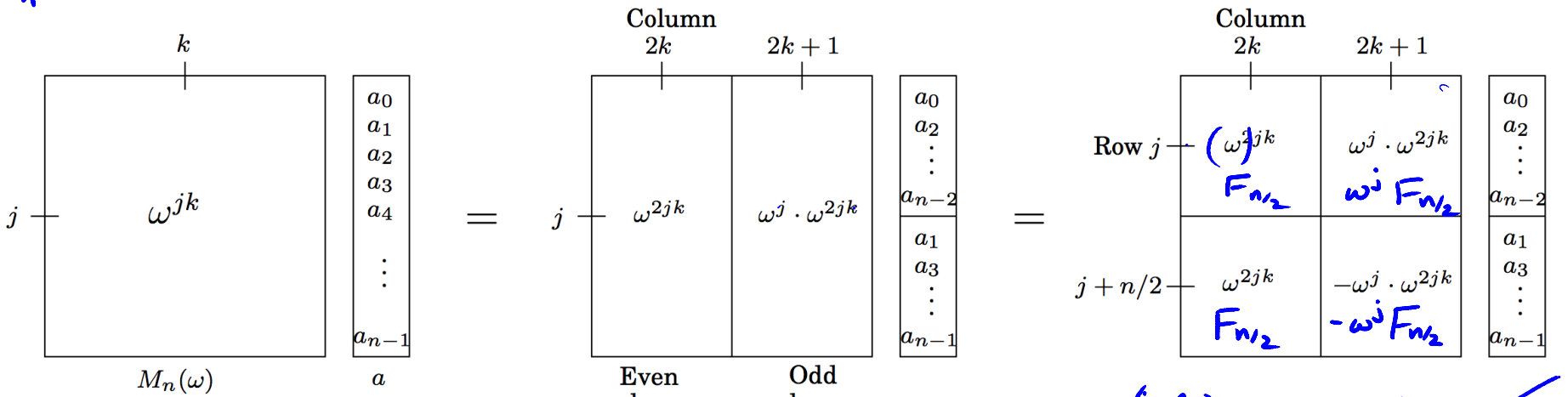
QFT Circuit

$\omega^n = 1 \qquad \omega = e^{2\pi i/n}$

$= \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$.

$$\begin{bmatrix} b_0 \\ b_1 \\ \vdots \\ b_{n-1} \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \omega & \omega^2 & \cdots & \omega^{n-1} \\ 1 & \omega^2 & \omega^4 & \cdots & \omega^{2(n-1)} \\ & & \vdots & & \\ 1 & \omega^j & \omega^{2j} & \cdots & \omega^{(n-1)j} \\ & & \vdots & & \\ 1 & \omega^{(n-1)} & \omega^{2(n-1)} & \cdots & \omega^{(n-1)(n-1)} \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \\ \vdots \\ a_{n-1} \end{bmatrix}$$

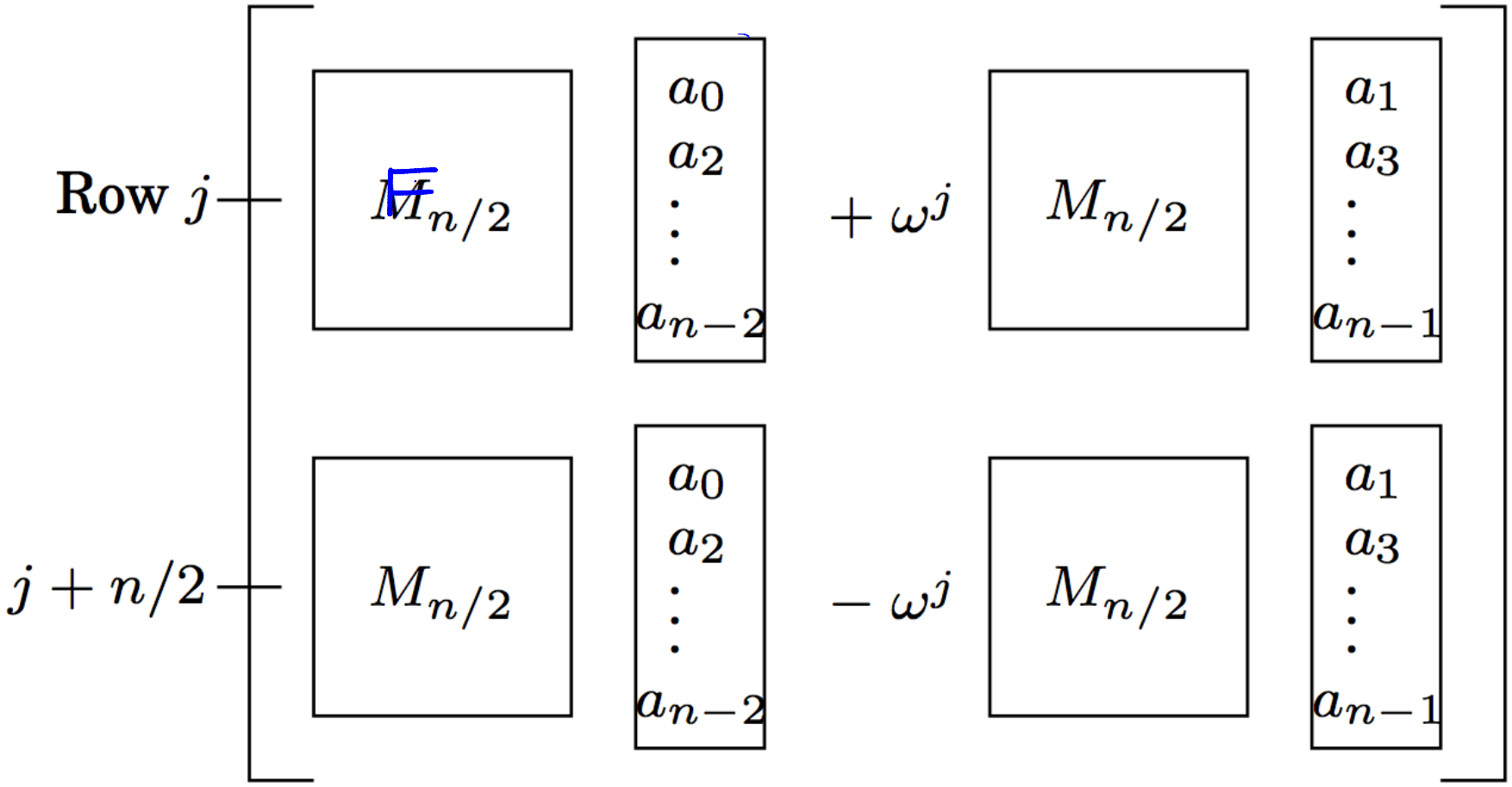
F_n



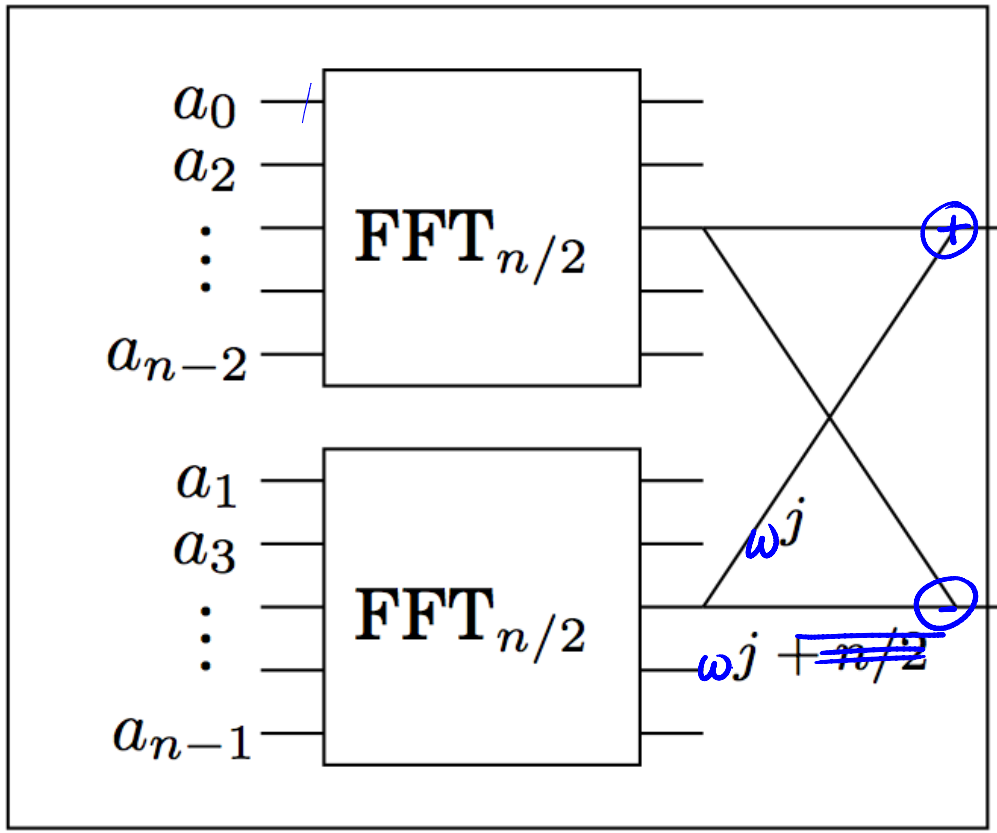
$\omega^{(j+\frac{n}{2})2k} = \omega^{2jk + nk}$

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

$\omega^2 = e^{2\pi i/(n/2)}$


Row j
$M_{n/2}$
a_0 a_2 $\vdots$ a_{n-2}
$+\ \omega^j$
$M_{n/2}$
a_1 a_3 $\vdots$ a_{n-1}
$j + n/2$
$M_{n/2}$
a_0 a_2 $\vdots$ a_{n-2}
$-\ \omega^j$
$M_{n/2}$
a_1 a_3 $\vdots$ a_{n-1}

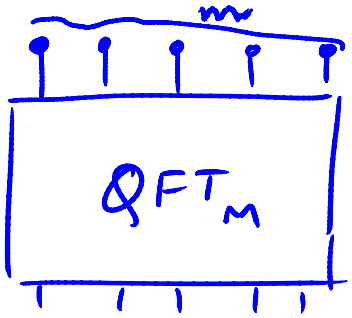
$\mathbf{FFT}_n$ (input: $a_0, \ldots, a_{n-1}$, output: $r_0, \ldots, r_{n-1}$)



$S(n) = 2S(\frac{n}{2}) + O(n)$

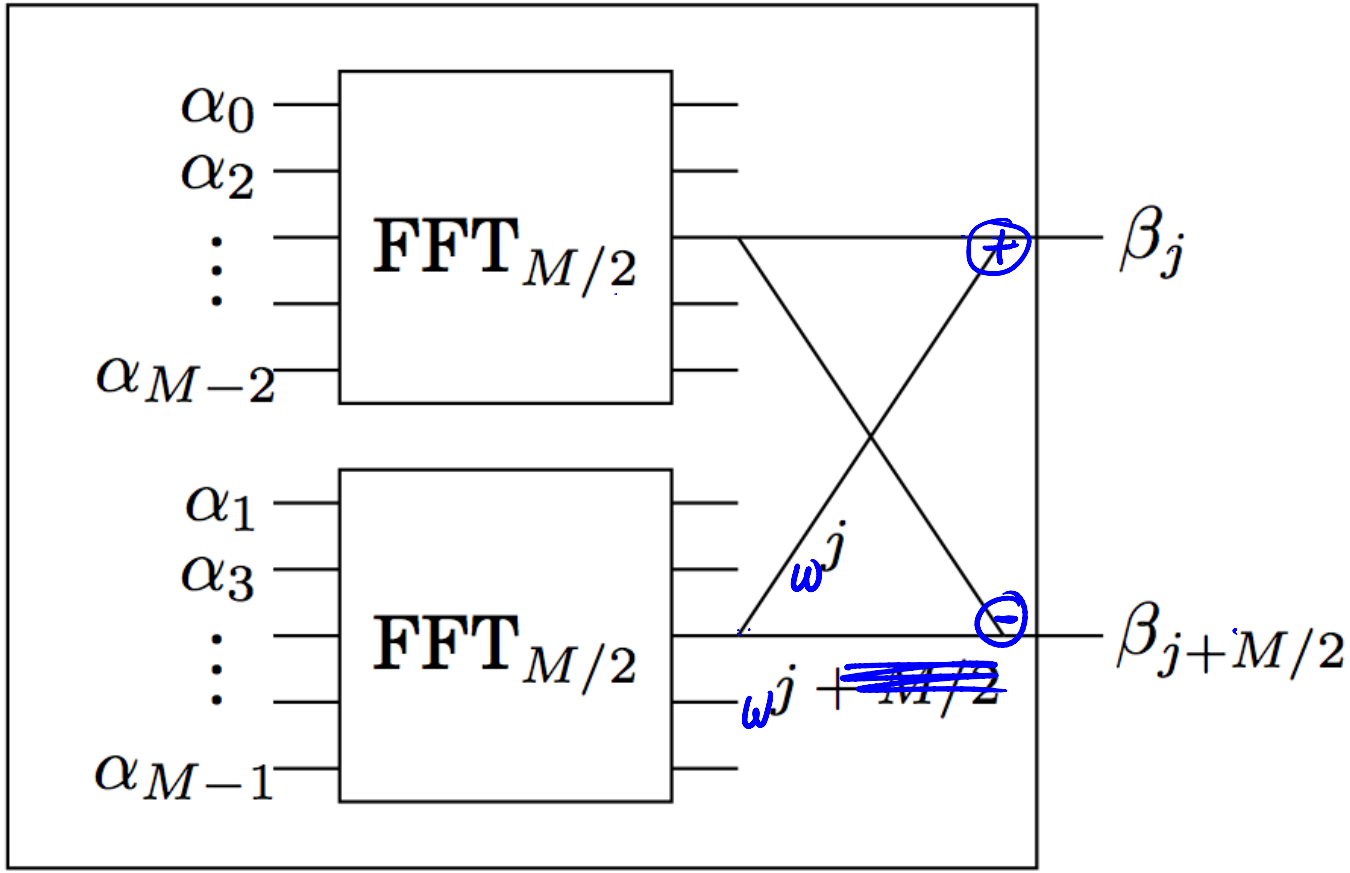
$S(n) = O(n \lg n)$

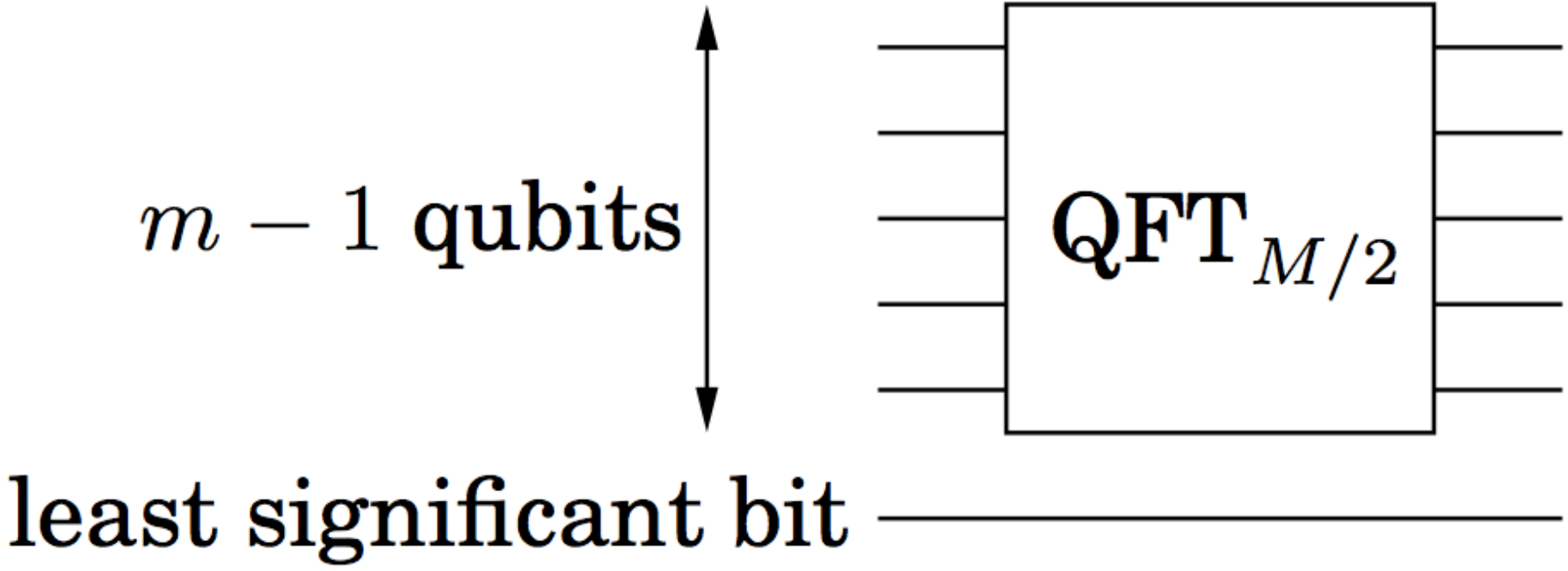
$M = 2^m$

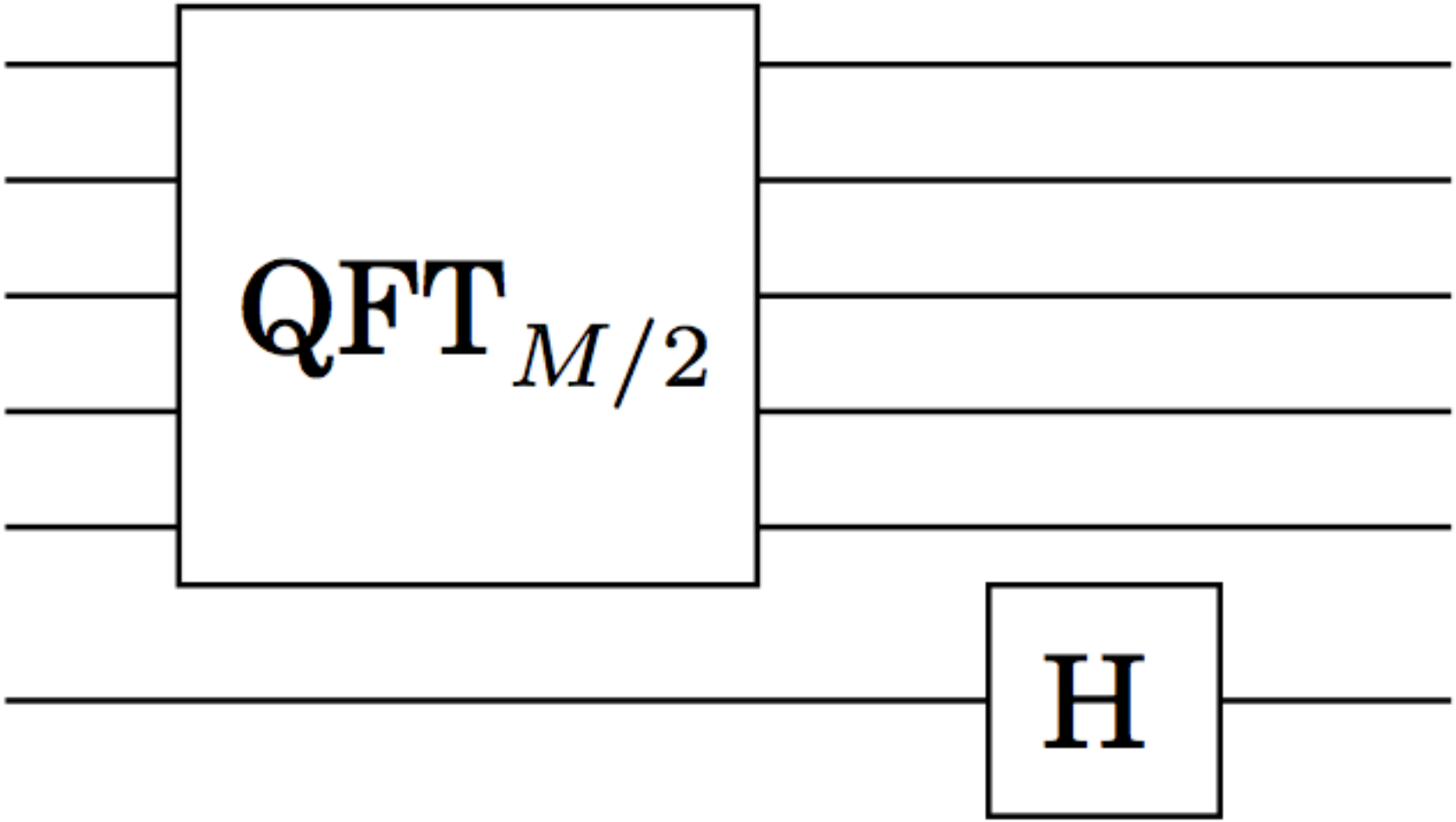


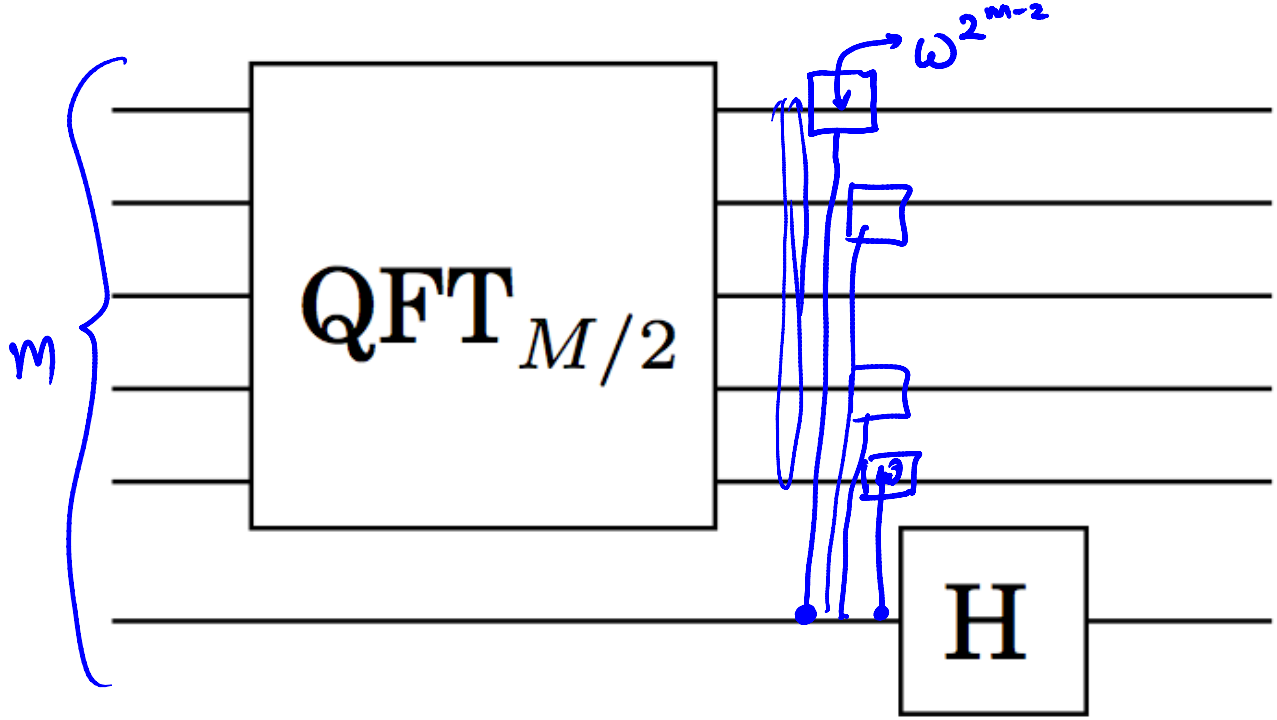
$$\begin{bmatrix} \beta_0 \\ \beta_1 \\ \beta_2 \\ \vdots \\ \beta_{M-1} \end{bmatrix} = \frac{1}{\sqrt{M}} \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \omega & \omega^2 & \cdots & \omega^{M-1} \\ 1 & \omega^2 & \omega^4 & \cdots & \omega^{2(M-1)} \\ & \vdots & & & \\ 1 & \omega^j & \omega^{2j} & \cdots & \omega^{(M-1)j} \\ & \vdots & & & \\ 1 & \omega^{(M-1)} & \omega^{2(M-1)} & \cdots & \omega^{(M-1)(M-1)} \end{bmatrix} \begin{bmatrix} \alpha_0 \\ \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_{M-1} \end{bmatrix}$$

$\mathbf{FFT}_M$ (input: $\alpha_0, \ldots, \alpha_{M-1}$, output: $\beta_0, \ldots, \beta_{M-1}$)




$m-1$ qubits
$\mathbf{QFT}_{M/2}$
least significant bit


$\mathbf{QFT}_{M/2}$
H



$S(m) = S(m-1) + O(m)$

$S(m) = O(m^2)$

$M = 2^m$

$S = O(\log^2 M)$

$\omega^j = \omega^{j_{m-2} j_{m-3} \cdots j_0} = \omega^{j_{m-2} \cdot 2^{m-2}} \times \omega^{j_{m-3} 2^{m-3}} \cdots \omega^{j_0 \cdot 2^0}$