KU LEUVEN

Introduction to Quantum Computation

March, 2018

Alan Szepieniec
alan.szepieniec@esat.kuleuven.be

imec-COSIC, KU Leuven

Table of Contents

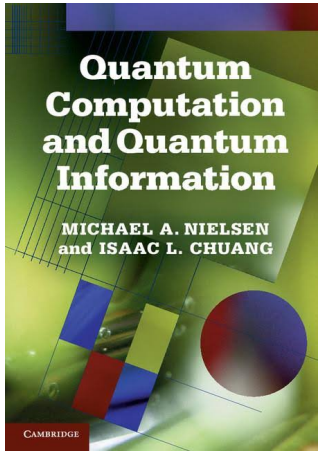
Introduction

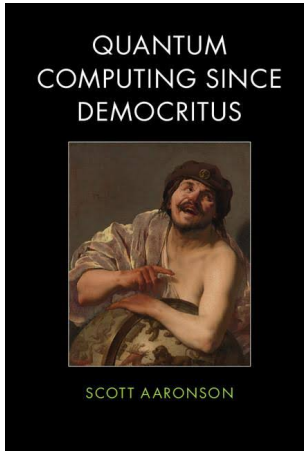
Applications of Quantum Computers

- simulate QM for science
- simulate QM for industry
  - pharmaceuticals
  - nanomaterials
  - circuits $\Rightarrow$ bootstrapping potential?
- break crypto
- prove crypto

  } my field
- do crypto
- optimization / machine learning
- ~~big data~~
- finance (?)
- ~~blockchain~~
- money / identity
- ~~**NP**-complete problems~~ (depends ...)
- in general: small data + big complexity

Resources

- bible 

- poetry 

- zoo
  - NIST Quantum Algorithm Zoo: `https://math.nist.gov/quantum/zoo/`
- lecture notes
  - Preskill: `http://www.theory.caltech.edu/%7Epreskill/ph219/index.html`
  - De Wolf: `https://homepages.cwi.nl/~rdewolf/qcnotes.pdf`

Quantum Computation

Postulates of Quantum Computation

1. A quantum system is fully defined by its *state* $|\psi\rangle \in \mathcal{H}$ where $\mathcal{H} \subset \mathbb{C}^{2^k}$ is a Hilbert space of unit-length vectors, *i.e.*, $\||\psi\rangle\|_2^2 = |\psi\rangle^{*\mathsf{T}}|\psi\rangle = \langle\psi|\psi\rangle = 1$.
2. Any valid computation is a unitary transformation $T : \mathcal{H} \to \mathcal{H} : |\psi\rangle \mapsto T|\psi\rangle$ of the state and can be described by a unitary matrix $T \in \mathbb{C}^{2^k \times 2^k}$ such that $T^{*\mathsf{T}}T = I$.
3. The composition of two quantum states $|\psi\rangle \in \mathcal{H}_1 \subset \mathbb{C}^{2^k}$ and $|\phi\rangle \in \mathcal{H}_2 \subset \mathbb{C}^{2^\ell}$ is described by their *tensor product*: $|\psi\phi\rangle = |\psi\rangle \otimes |\phi\rangle \in \mathcal{H}_1 \otimes \mathcal{H}_2 \subset \mathbb{C}^{2^{k+\ell}}$.

Tensor Product

Inner product:

$$\begin{pmatrix} a_1 \\ a_2 \end{pmatrix}^{\mathsf{T}} \begin{pmatrix} b_1 \\ b_2 \end{pmatrix} = a_1 b_1 + a_2 b_2$$

Outer product:

$$\begin{pmatrix} a_1 \\ a_2 \end{pmatrix} \begin{pmatrix} b_1 \\ b_2 \end{pmatrix}^{\mathsf{T}} = \begin{pmatrix} a_1 b_1 & a_1 b_2 \\ a_2 b_1 & a_2 b_2 \end{pmatrix}$$

Tensor product:

$$\begin{pmatrix} a_1 \\ a_2 \end{pmatrix} \otimes \begin{pmatrix} b_1 \\ b_2 \end{pmatrix} = \begin{pmatrix} a_1 b_1 \\ a_1 b_2 \\ a_2 b_1 \\ a_2 b_2 \end{pmatrix}$$

Postulates of Quantum Computation

1. A quantum system is fully defined by its *state* $|\psi\rangle \in \mathcal{H}$ where $\mathcal{H} \subset \mathbb{C}^{2^k}$ is a Hilbert space of unit-length vectors, *i.e.*, $\||\psi\rangle\|_2^2 = |\psi\rangle^{*\mathsf{T}}|\psi\rangle = \langle\psi|\psi\rangle = 1$.
2. Any valid computation is a unitary transformation $T : \mathcal{H} \to \mathcal{H} : |\psi\rangle \mapsto T|\psi\rangle$ of the state and can be described by a unitary matrix $T \in \mathbb{C}^{2^k \times 2^k}$ such that $T^{*\mathsf{T}}T = I$.
3. The composition of two quantum states $|\psi\rangle \in \mathcal{H}_1 \subset \mathbb{C}^{2^k}$ and $|\phi\rangle \in \mathcal{H}_2 \subset \mathbb{C}^{2^\ell}$ is described by their *tensor product*: $|\psi\phi\rangle = |\psi\rangle \otimes |\phi\rangle \in \mathcal{H}_1 \otimes \mathcal{H}_2 \subset \mathbb{C}^{2^{k+\ell}}$.
4. Measurement M happens with respect to an orthogonal basis $|b_1\rangle, |b_2\rangle, \ldots, |b_k\rangle \in \mathcal{H}$ and fixes the state to one basis vector $\mathsf{M}(|\psi\rangle) = |b_i\rangle$ with probability $\langle\psi|b_i\rangle\langle b_i|\psi\rangle$.

Quantum Computation Example

(4.) Use the basis $|0\rangle, |1\rangle$ for $\mathcal{H}$.

(1.) A qubit $|\psi\rangle \in \mathcal{H}$ is described by a vector $(\alpha, \beta) \in \mathbb{C}^2$ such that $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$.

(4.) Measuring yields $|0\rangle$ with probability $\alpha^*\alpha$ and $|1\rangle$ with $\beta^*\beta$.

▷ Let $|\psi\rangle, |\phi\rangle \in \mathcal{H}$ be two qubits set to zero, *i.e.*, $|\psi\rangle = |\phi\rangle = |0\rangle$.

(3.) The composite system is described by $|\psi\phi\rangle = |\psi\rangle \otimes |\phi\rangle = \alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle$ with e.g. $\alpha = 1$ and $\beta = \gamma = \delta = 0$.

(2.) Apply the unitary transformation

$$T = \begin{pmatrix} \frac{1}{2}\sqrt{2} & 0 & 0 & -\frac{1}{2}\sqrt{2} \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ \frac{1}{2}\sqrt{2} & 0 & 0 & \frac{1}{2}\sqrt{2} \end{pmatrix} \text{ to } |\psi\phi\rangle \cong \begin{pmatrix} \alpha \\ \beta \\ \gamma \\ \delta \end{pmatrix}.$$

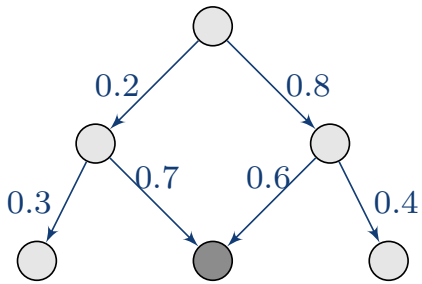
▷ Result: $T|\psi\phi\rangle = \frac{1}{2}\sqrt{2}|00\rangle + 0|01\rangle + 0|10\rangle + \frac{1}{2}\sqrt{2}|11\rangle$.

(4.) Measuring yields $|00\rangle$ with probability $\frac{1}{2}$ and $|11\rangle$ with $\frac{1}{2}$.

Modes of Computation

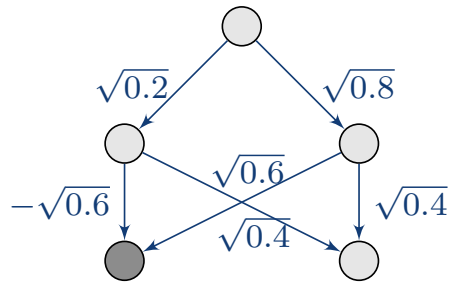
$P = 1$

deterministic



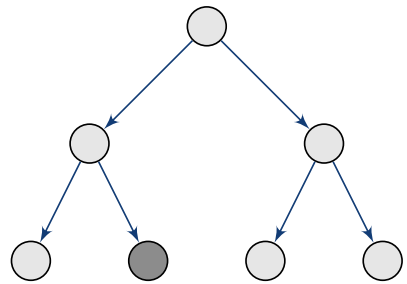
$P = 0.2 \times 0.7 + 0.8 \times 0.6 = 0.62$

probabilistic



$P = \left(-\sqrt{0.2}\sqrt{0.6} + \sqrt{0.8}\sqrt{0.6}\right)^2 \approx 0.35^2 \approx 0.12$

quantum



$P = 1$

nondeterministic

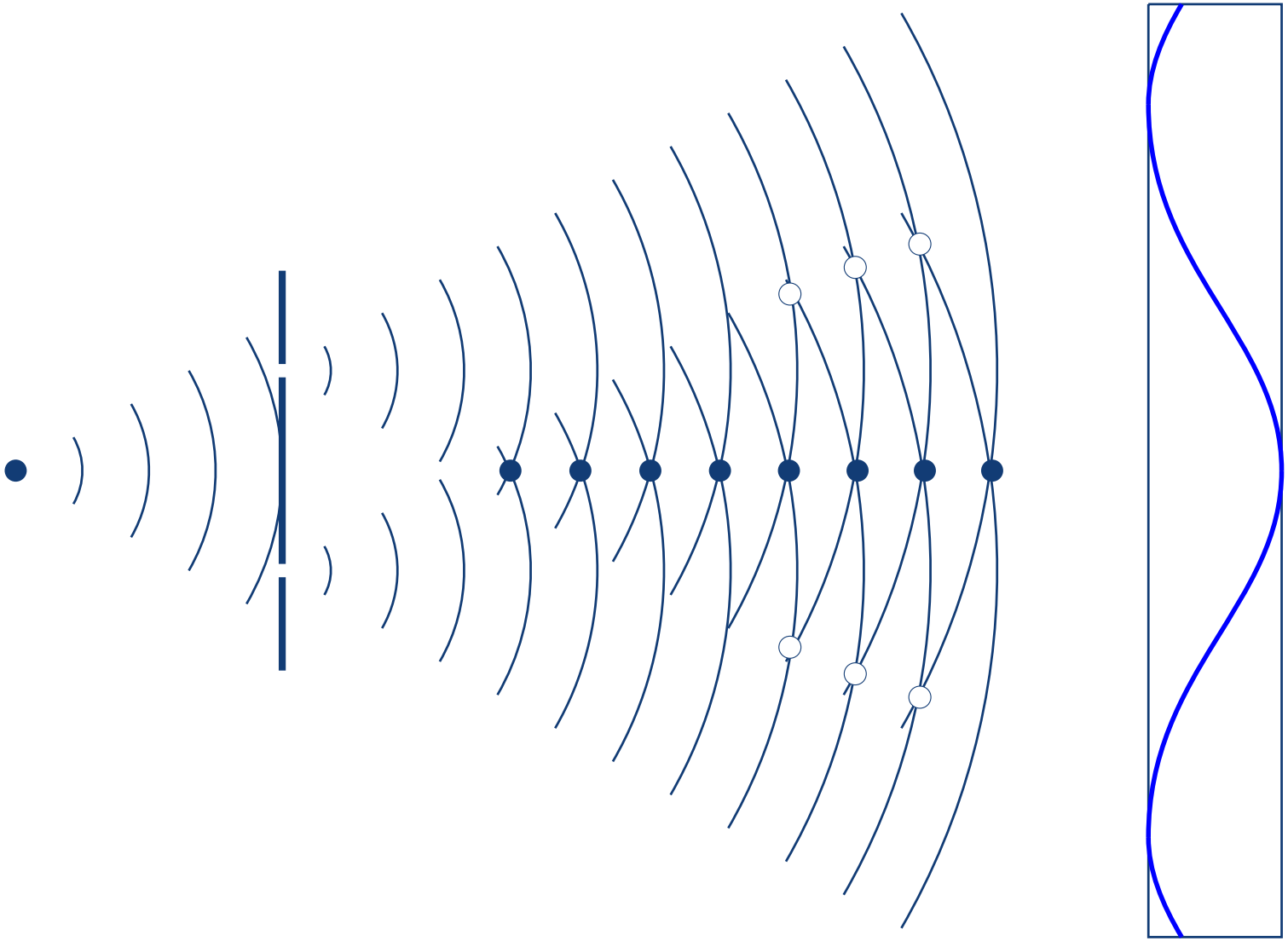
Postulates of Probabilistic Computation

1. A ~~quantum~~ probabilistic system is fully defined by its *state* (or *probability distribution*) $\psi \in [0;1]^{2^k}$ having ~~ℓ_2~~ ℓ_1-norm equal to 1
2. Any valid computation is a transformation $T : \psi \mapsto T\psi$ of the state and can be described by a ~~unitary~~ stochastic matrix $T \in [0;1]^{2^k \times 2^k}$ such that all rows and columns sum to 1.
3. The composition of two states $\psi \in [0;1]^{2^k}$ and $\phi \in [0;1]^{2^\ell}$ is described by their *tensor product*: $\psi \otimes \phi \in [0;1]^{2^{k+\ell}}$.
4. ~~Measurement~~ Sampling (denoted by M) happens with respect to an orthogonal basis $b_1, b_2, \ldots, b_k \in [0;1]^{2^k}$ and fixes the state to one basis vector $\mathsf{M}(\psi) = b_i$ with probability ~~$\langle\psi|b_i\rangle\langle b_i|\psi\rangle$~~ $b_i^\mathsf{T}\psi$.

Quantum Computation in 2 Easy Steps

0. Start with probabilistic computation.
1. Compute with *probability distributions* as opposed to *samples*.
   - sample afterwards
2. Use *continuous* transitions as opposed to *discrete* ones.
   - the nth root of a computation is always well defined
   - $\longrightarrow$ complex numbers, ℓ_2 norm
   - fixedness of quantum circuits is a minor detail
   - use *unitary local* transformations

Interference

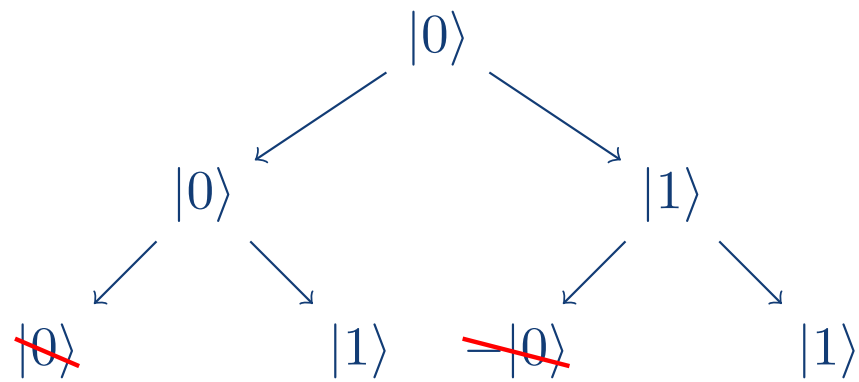


Interference for Quantum Computers

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

$$U|0\rangle = \tfrac{1}{\sqrt{2}}|0\rangle + \tfrac{1}{\sqrt{2}}|1\rangle \text{ and } U^2|0\rangle = |1\rangle$$

observable outcomes:



- *destructive interference is the source of all quantum wierdness*
- quantum algorithm design = engineering interference

Density Operator

- equivalent characterization of quantum computation
- in terms of state matrices instead of state vectors via $|\psi\rangle\langle\psi| \cong |\psi\rangle$
- useful for
  - probability distributions over quantum states
  - partial quantum systems (*i.e.*, ignoring certain qubits)
- ultimately not necessary to understand quantum computation

EPR Paradox

- How to define existence?
- Einstein: something *exists* iff
  - it has a *state*
  - that has a *value*
  - that can be *exposed through experimental measurement*
  - while being *independent of measurement*.
- Einstein: whatever QM describes, is not something that *exists*.

EPR Paradox

- Einstein, Podolsky, Rosen:
  - Take two electrons in state $|\uparrow\uparrow\rangle + |\downarrow\downarrow\rangle$;
  - send one to Alice and one to Bob.
  - If Alice measures $|\uparrow\rangle$, she knows *instantly* Bob will measure $|\uparrow\rangle$.
  - If Alice measures $|\downarrow\rangle$, she knows *instantly* Bob will measure $|\downarrow\rangle$.
  - But before Alice measures, Bob has 50-50 chance.
  - So: Alice *influences* Bob's probabilities *faster than the speed of light*.
  - So: *QM is not reconcilable with GR.*

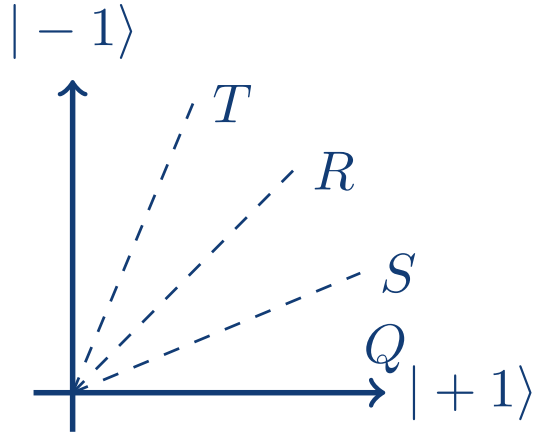
Bell's Theorem

- Bell identifies assumptions in EPR paradox:
  - *realism*: all observable behavior of an object is completely determined by its state
  - *locality*: an object's state is affected only by its immediate surroundings
  - "local realism" / "local hidden variables theory"
- Bell:
  - local realism is testable!
  - there are functions (inequalities) of experiment outcomes (variables) that hold for all probability distributions, but not for QM
  - Bell inequality holds for all experiments $\Longrightarrow$ local realism is true
  - some experiments violate Bell inequality $\Longrightarrow$ local realism is false

Bell-CHSH Inequality

- Alice and Bob receive one qubit each from $|-1,-1\rangle + |+1,+1\rangle$
- Alice flips a coin and measures with Q or R
- Bob flips a coin and measures with S or T
- measurement outcomes: $+1$ or -1
- If Q, R, S, T measure different aspects of the same state vector, they must follow a joint probability distribution
- If Q, R, S, T follow a classical probability distribution, then:
  $\mathrm{E}[QS] + \mathrm{E}[RS] + \mathrm{E}[RT] - \mathrm{E}[QT] \leq 2$
  (Bell-)CHSH Inequality ↑
- experiments violate Bell inequalities

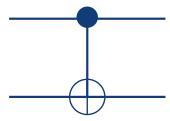
Bell-CHSH Inequality



- Let $|\varphi\rangle = \frac{1}{\sqrt{2}}|+1,+1\rangle + \frac{1}{\sqrt{2}}|-1,-1\rangle$
- Let $L = \begin{pmatrix} \cos 22.5^\circ & -\sin 22.5^\circ \\ \sin 22.5^\circ & \cos 22.5^\circ \end{pmatrix}$, *i.e.*, CCW rotation by 22.5°
- $Q = \mathsf{M}_A$, $S = \mathsf{M}_B \circ (I \otimes L)$, $R = \mathsf{M}_A \circ (L^2 \otimes I)$, $T = \mathsf{M}_B \circ (I \otimes L^3)$
- $\mathrm{E}[QS] = \Pr[A = B|Q,S] - \Pr[A \neq B|Q,S]$
  $= \|\langle +1,+1|(I \otimes L)|\varphi\rangle\|^2 + \|\langle -1,-1|(I \otimes L)|\varphi\rangle\|^2 - \|\langle +1,-1|(I \otimes L)|\varphi\rangle\|^2 - \|\langle -1,+1|(I \otimes L)|\varphi\rangle\|^2 = (\cos 22.5^\circ)^2 - (\sin 22.5^\circ)^2 = \mathrm{E}[RT] = \mathrm{E}[RS]$
- $\mathrm{E}[QT] = \Pr[A = B|Q,T] - \Pr[A \neq B|Q,T]$
  $= \|\langle +1,+1|(I \otimes L^3)|\varphi\rangle\|^2 + \|\langle -1,-1|(I \otimes L^3)|\varphi\rangle\|^2 - \|\langle -1,+1|(I \otimes L^3)|\varphi\rangle\|^2 - \|\langle +1,-1|(I \otimes L^3)|\varphi\rangle\|^2 = (\sin 22.5^\circ)^2 - (\cos 22.5^\circ)^2$
- $\mathrm{E}[QS] + \mathrm{E}[RS] + \mathrm{E}[RT] - \mathrm{E}[QT] = 4(\cos 22.5^\circ)^2 - 4(\sin 22.5^\circ)^2$
  $\approx 2.82 > 2 \Rightarrow$ QM violates Bell-CHSH inequality

Quantum Gates

- CNOT: $|x, y\rangle \mapsto |x, x \oplus y\rangle$



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

- Hadamard: $|x\rangle \mapsto (-1)^x \frac{1}{\sqrt{2}}|x\rangle + \frac{1}{\sqrt{2}}|\neg x\rangle$

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

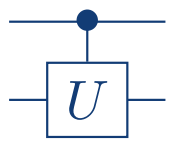
- T (AKA. $\pi/8$) : $|x\rangle \mapsto e^{xi\pi/4}|x\rangle$

$$\begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}$$

- S (AKA. phase) : $|x\rangle \mapsto i^x|x\rangle$

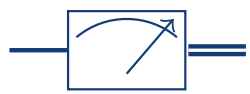
$$\begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$$

- C-U: $|x\rangle \otimes |y\rangle \mapsto |x\rangle \otimes U^x|y\rangle$



$$|0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes U$$

- Measurement



- { CNOT, H, T } is a universal gate set

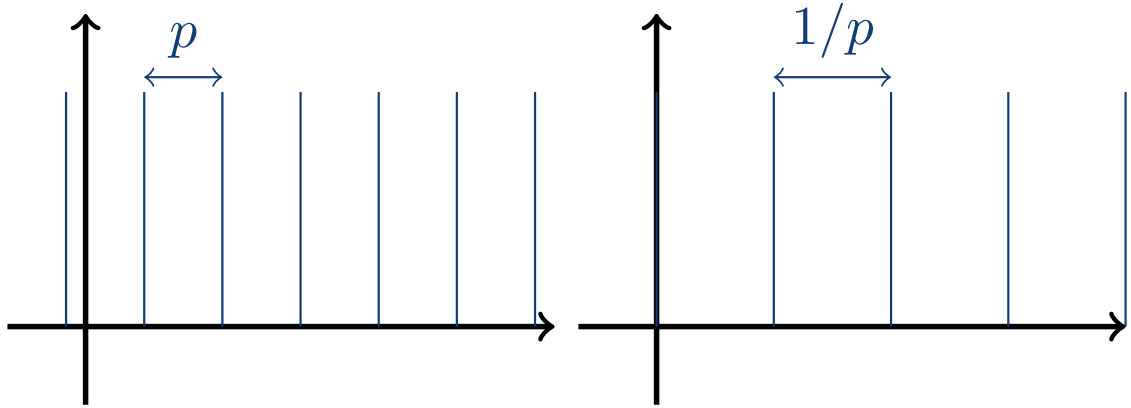
Shor's Algorithm

Shor's Algorithm: Generic

- first quantum algorithm for real world problem
- breaks RSA ... and DLOG ... and ECC
- reduces factorization of $n = pq$ to order finding
- order $\varphi(n) \Leftrightarrow a^{\varphi(n)} = 1 \bmod n$

Quantum Fourier Transform

- Classical Fourier Transform
  - $\mathbf{x} = (x_0, \ldots, x_{N-1})^{\mathsf{T}}$
  - $\mathbf{y} = (y_0, \ldots, y_{N-1})^{\mathsf{T}}$ with $y_j = \sum_{k=0}^{N-1} e^{-2i\pi jk/N} x_k$
  - complexity: $O(N \log N)$
- Quantum Fourier Transform
  - $|\mathbf{x}\rangle = \sum_{j=0}^{N-1} x_j |j\rangle$ *i.e.*, $\log_2 N$ qubits
  - $|\mathbf{y}\rangle = \sum_{j=0}^{N-1} y_j |j\rangle$ with $y_j = \sum_{k=0}^{N-1} e^{-2i\pi jk/N} x_k$
  - complexity: $O(\log N \log \log N)$



Shor's Algorithm for Integer Factorization

factorize $n = pq$

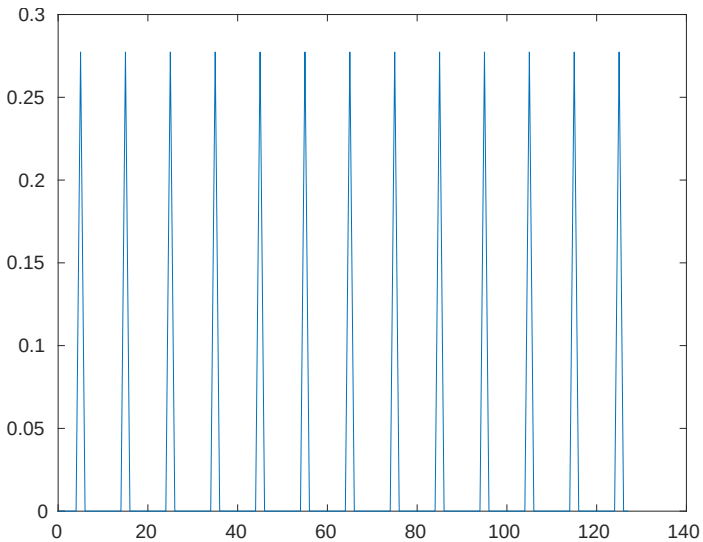
$\Leftrightarrow$ obtain order $\varphi(n)$ of $\mathbb{Z}/n\mathbb{Z}, \times$

$\triangleright$ $|a\rangle, |b\rangle$ are both quantum registers of $k > |n|$ qubits

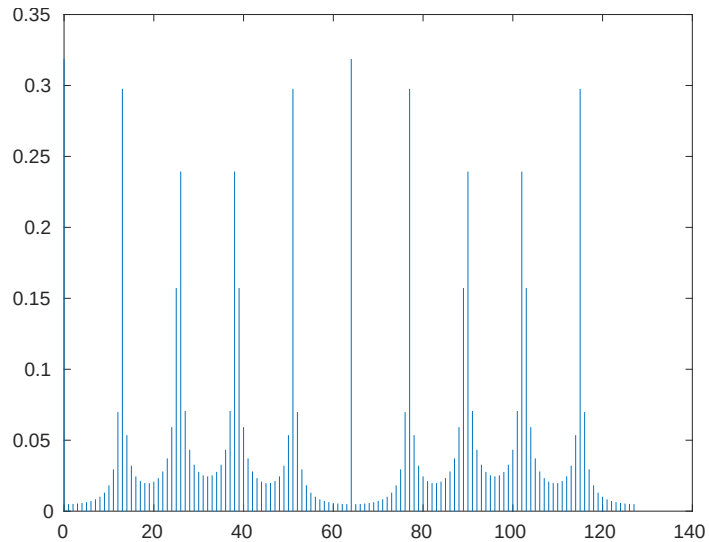
1. Set $|a\rangle = |b\rangle = |0^k\rangle$. result: $|a, b\rangle = |0, 0\rangle$
2. Apply $H = \begin{pmatrix} 1/\sqrt{2} & 1/\sqrt{2} \\ 1/\sqrt{2} & -1/\sqrt{2} \end{pmatrix}$ to each qubit of $|a\rangle$. result: $|a, b\rangle = \frac{1}{\sqrt{2^k}} \sum_{i=0}^{2^k-1} |i, 0\rangle$
3. Apply $f : |a, b\rangle \mapsto |a, b \oplus x^a \bmod n\rangle$. result: $|a, b\rangle = \cdot \sum_{i=0}^{2^k-1} |i, x^i\rangle$
4. Measure *only* $|b\rangle$. result: $|b\rangle = |x^y\rangle$
   result: $|a\rangle = \cdot \sum_{i \in (y+\varphi(n)\mathbb{Z})} |i\rangle$
5. Apply $g : |a\rangle \mapsto \mathsf{QFT}(|a\rangle)$ result: $|a\rangle = \sum_j \cdot \left| j \frac{2^k}{\varphi(n)} \right\rangle$
6. Measure $|a\rangle$ result: $|a\rangle = \left| \left\lfloor j \frac{2^k}{\varphi(n)} \right\rceil \right\rangle$
7. Repeat.

DFT Example

- factorize $n = 35$
- $x = 2, b = 32 \quad \longrightarrow$ order $r = 12$



$|a\rangle$



$|\mathrm{QFT}(a)\rangle$

Hidden Subgroup Problem

Definition

Let $G, +$ be a group with subgroup H. Let $f : G \to \{0,1\}^*$ be a function that produces the same image iff its inputs are from the same coset of H, *i.e.*,

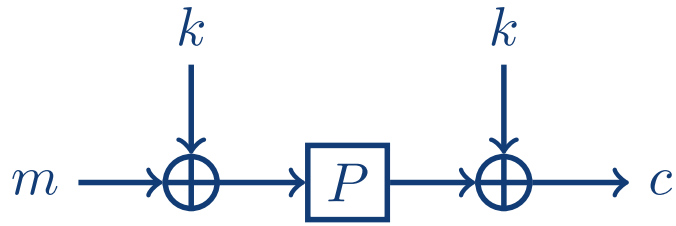
$$\forall g_1, g_2 \in G \,.\, g_1 - g_2 \in H \Leftrightarrow f(g_1) = f(g_2) \ .$$

The *Hidden Subgroup Problem (HSP)* is to find a generating set of H given oracle access to f.

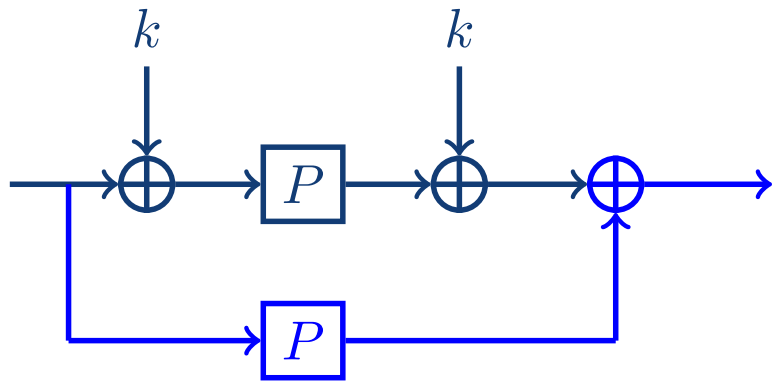
- factorization: $G = \mathbb{Z}, +$ and $H = \varphi(n)\mathbb{Z}, +$
- discrete logarithm: $G = \mathbb{Z} \times \mathbb{Z}, +$ and $H = \mathbb{Z} \begin{pmatrix} 1 \\ x \end{pmatrix}, +$
- Simon's problem: $G = \{0,1\}^k, \oplus$ and $H = \{0, p\}, \oplus$

Simon vs. Even-Mansour

- Even-Mansour construction:



- given quantum access to the circuit $\mathcal{C}|m\rangle = |c\rangle$ and given P; find k
- solution[1]:



- $f(x) = P(x \oplus k) \oplus k \oplus P(x)$
- $f(x \oplus k) = P(x) \oplus k \oplus P(x \oplus k)$
- period is k!

[1] H. Kuwakado, M. Morii. "Security on the Quantum-type Even-Mansour Cipher" IEICE 2012

Grover's Algorithm

Grover's Algorithm: Generic

- Let $F : \{0,1\}^k \to \{0,1\}$ with 1 input a satisfying $F(a) = 1$ (and $F(b) = 0$ for all $b \neq a$)
- task: given oracle access to F, find a
- captures generic search, optimization, preimage-search, NP-complete problems, ...
- best classical algorithm: exhaustive search — $O(2^k)$
- quantum oracle access: $\mathcal{F}|a, c\rangle \mapsto |a, c \oplus F(a)\rangle$
- best quantum algorithm: Grover — $O(2^{k/2})$
  - polynomial speedup — nice, but no holy grail

Grover's Algorithm: Elements

- $\mathcal{A}$ — uniform sampler
  - $\mathcal{A}|0^k\rangle = \frac{1}{\sqrt{2^k}} \sum_{i=0}^{2^k-1} |i\rangle = |\Psi\rangle$
  - Apply a Hadamard gate to each qubit
- working plane
  - the vectors $|a\rangle = |\Psi_1\rangle$ and $|\Psi\rangle$ span a plane
  - let $|\Psi_0\rangle$ lie in this plane, perpendicular to $|a\rangle$
- $\mathbf{S}_0$ — mirror about $|0^k\rangle$
  - $\mathbf{S}_0|x\rangle = \begin{cases} -|x\rangle & \text{if } x \neq 0 \\ |x\rangle & \text{else} \end{cases}$
  - compute $|x, q\rangle \mapsto |x, q \oplus (x \neq 0)\rangle$ and keep $|q\rangle = 1/\sqrt{2}(|0\rangle - |1\rangle)$
  - $1/\sqrt{2}|x\rangle(|0\rangle - |1\rangle) \mapsto 1/\sqrt{2}|x\rangle(|0\rangle - |1\rangle)$ (if $x = 0$)
  - $1/\sqrt{2}|x\rangle(|0\rangle - |1\rangle) \mapsto 1/\sqrt{2}|x\rangle(|1\rangle - |0\rangle) = -1/\sqrt{2}|x\rangle(|0\rangle - |1\rangle)$ (otherwise)
- $\mathbf{S}_\chi$ — mirror about $|\Psi_0\rangle$
  - $\mathbf{S}_\chi|x\rangle = \begin{cases} -|x\rangle & \text{if } F(x) \\ |x\rangle & \text{if } \neg F(x) \end{cases}$
  - compute $|x, q\rangle \mapsto |x, q \oplus F(x)\rangle$ and keep $|q\rangle = 1/\sqrt{2}(|0\rangle - |1\rangle)$

Grover's Algorithm: Step-by-Step

Single iteration: $|\Phi\rangle \mapsto \mathcal{Q}|\Phi\rangle = -\mathcal{A}\mathbf{S}_0\mathcal{A}^{-1}\mathbf{S}_\chi|\Phi\rangle$

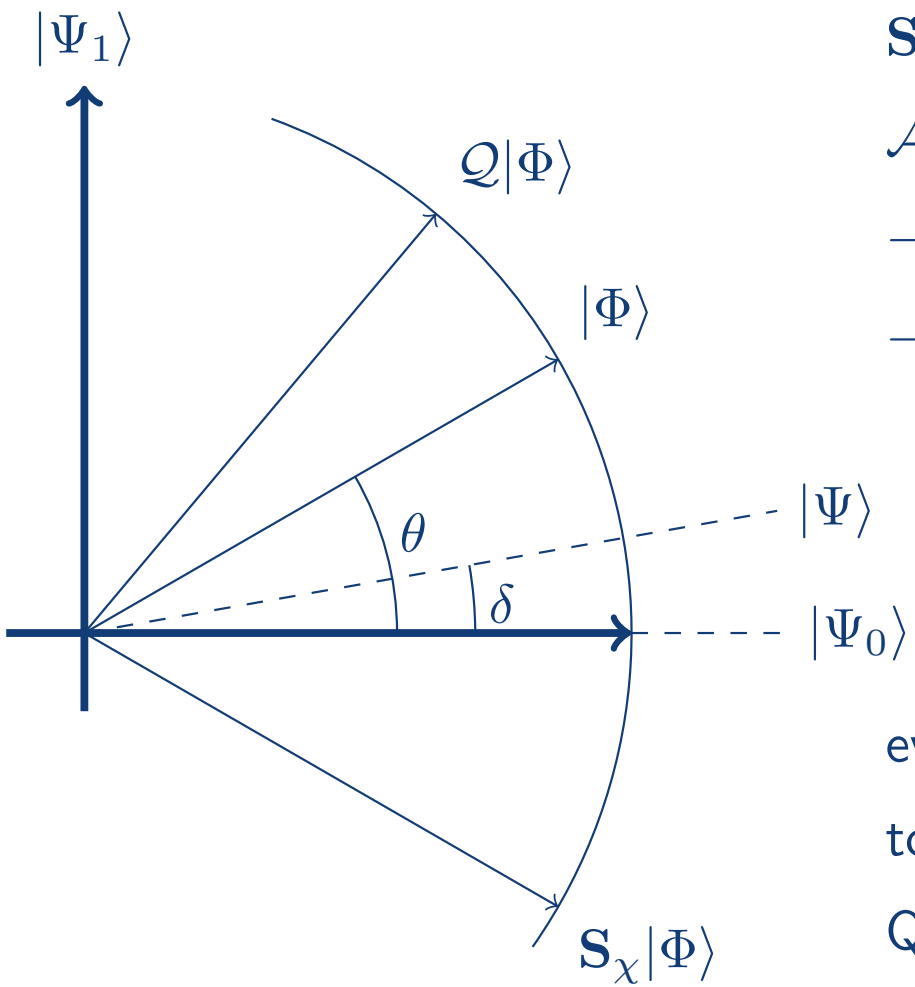
$|\Phi\rangle$ current state

$\mathbf{S}_\chi|\Phi\rangle$: flip about $|\Psi_0\rangle$

$\mathcal{A}^{-1}\mathbf{S}_\chi|\Phi\rangle$: change of basis

$-\mathbf{S}_0\mathcal{A}^{-1}\mathbf{S}_\chi|\Phi\rangle$: flip about $|\Psi\rangle$

$-\mathcal{A}\mathbf{S}_0\mathcal{A}^{-1}\mathbf{S}_\chi|\Phi\rangle$: undo change of basis

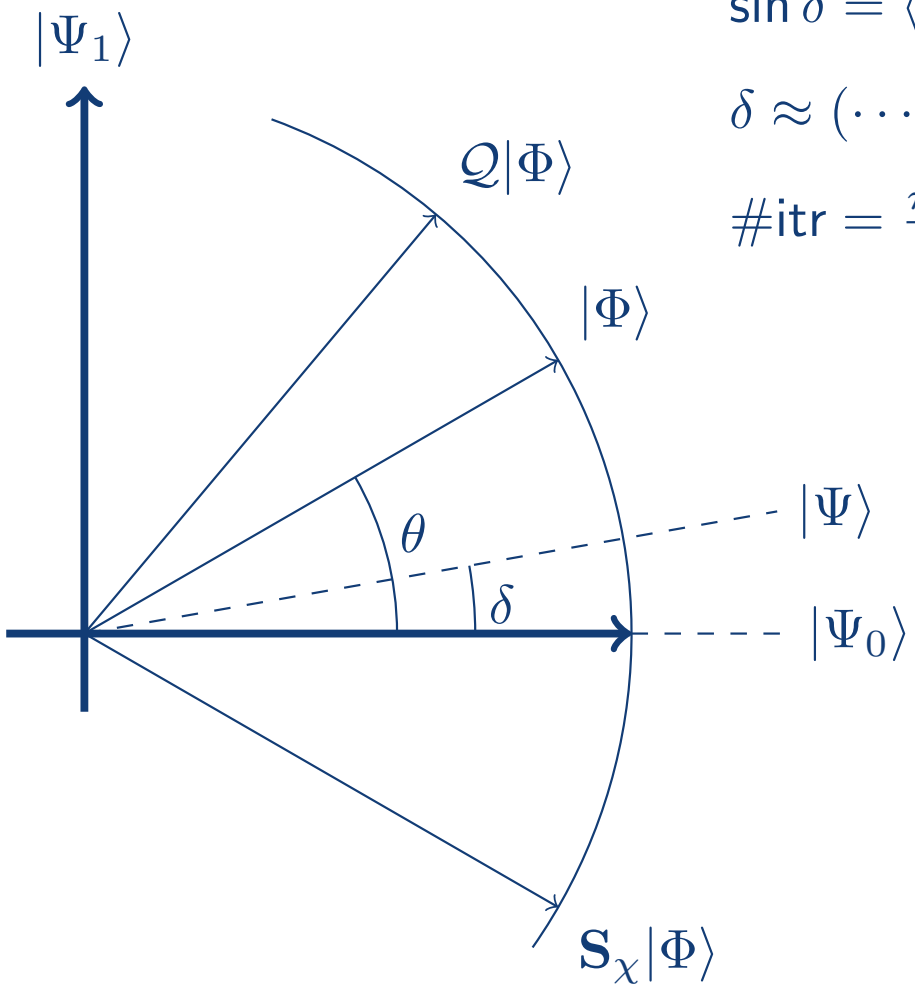


every iteration moves $|\Phi\rangle$ closer

to $|\Psi_1\rangle$ by an angle 2δ

Q: what are δ and (initially) θ?

Grover's Algorithm: Complexity

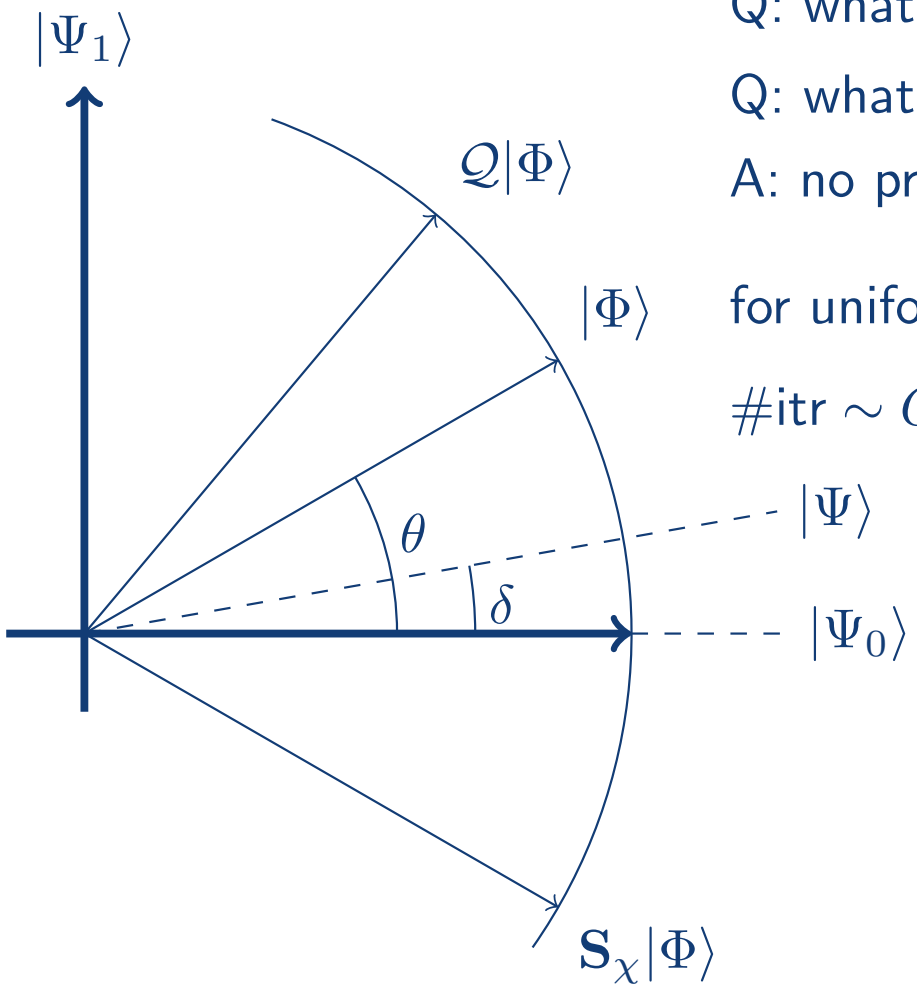


$$\sin\delta = \langle\Psi_1|\Psi\rangle$$

$$\delta \approx (\cdots 0\,1\,0\cdots)(\cdots 1/\sqrt{2^k}\cdots)^{\mathsf{T}} = 1/\sqrt{2^k}$$

$$\#\mathsf{itr} = \frac{\pi/2-\theta_{\mathsf{init}}}{2\delta} = \frac{\pi/2-\delta}{2\delta} \approx \frac{\pi}{4}2^{k/2}$$

Amplitude Amplification



Q: what if $\#A = \#\{x \mid F(x) = 1\} > 1$?

Q: what if $\mathcal{A}$ is better than uniform?

A: no problem

for uniform $\mathcal{A}$ and $\#A > 1$ holds:

$\#\text{itr} \sim O(\sqrt{2^k/\#A})$

Drawbacks of Grover's Algorithm

- quantum oracle access to F
  - expensive when F depends on big data
- no parallelism
  - partition search space
  - classically: $2\times$ faster
  - quantumly: $\sqrt{2}\times$ faster
- no meet-in-the-middle
  - requires *lots* of *quantum* memory

HHL Algorithm

HHL: Generic Description

- Harrow, Hassadim, Lloyd
- exponential speed-up
- solve *large* + *sparse* linear system
- sledgehammer waiting for killer application
- lots of fine print

- Given $A \in \mathbb{C}^{N\times N}, \mathbf{b} = (b_1, \ldots, b_N)^\mathsf{T} \in \mathbb{C}^N$, find $\mathbf{x} \in \mathbb{C}^N$ s.t. $A\mathbf{x} = \mathbf{b}$
  - A is Hermitean: $A^{*\mathsf{T}} = A$ and invertible
  - A is sparse: $\leq s$ nonzero entries per row
  - $\mathbf{b}$ is constructable as $|\mathbf{b}\rangle = \sum_{i=1}^N b_i |i\rangle$
    - superdense ↑ requires $O(\log N)$ qubits
  - output $|\mathbf{x}\rangle = \sum_{i=1}^N x_i |i\rangle$
    - measure via $\langle \mathbf{x}|M|\mathbf{x}\rangle$ for some M

- complexity HHL: $\tilde{O}(\log(N) s^2 \kappa^2/\epsilon)$
  - condition number $\kappa = \frac{\max \operatorname{eig} A}{\min \operatorname{eig} A}$
  - success probability ϵ
- classical complexity: $O(N s \sqrt{\kappa} \log(1/\epsilon))$ (for positive definite A)

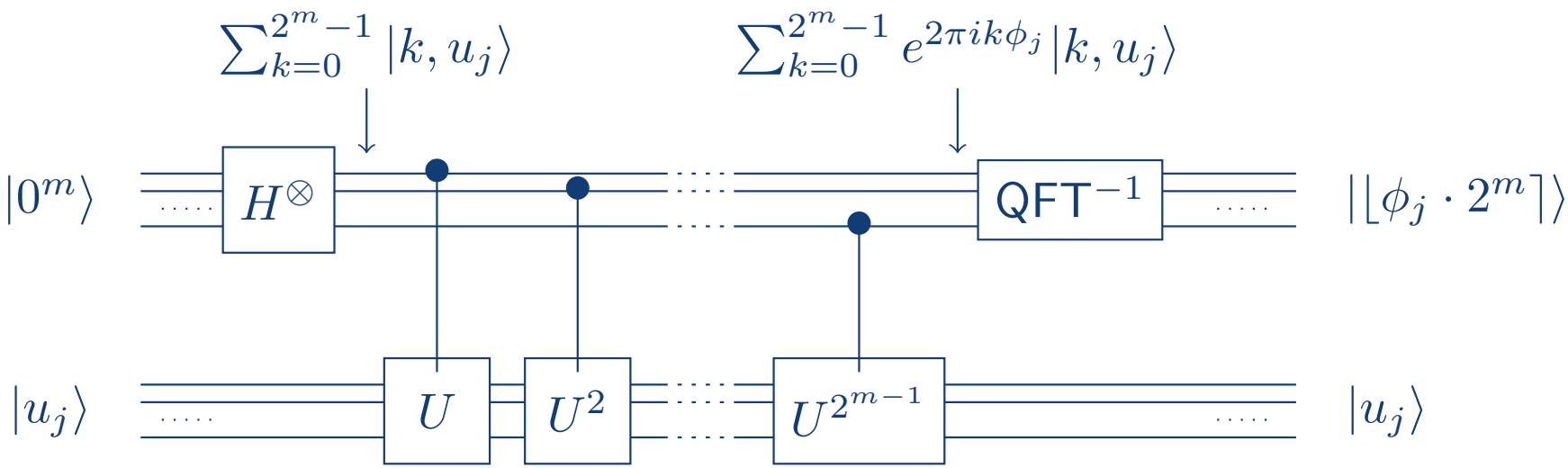
Hamiltonian Simulation

- Hamiltonian $\hat{H} \in \mathbb{C}^{2^k \times 2^k}$ describes evolution of quantum systems via
- time-dependent Schrödinger equation: $i\hbar \frac{\partial}{\partial t} |\Psi(t)\rangle = \hat{H} |\Psi(t)\rangle$ ...
- ... with general solution $|\Psi(t)\rangle = e^{i\hat{H}t/\hbar} |\Psi(0)\rangle$

- Hamiltonian Simulation:
  - Given: constant sparse $\hat{H}$, time window δt, initial state $|\Psi\rangle = |\Psi(0)\rangle$
  - Compute $|\Phi\rangle = |\Psi(\delta t)\rangle = e^{i\hat{H}\delta t} |\Psi(0)\rangle$
- doing QM with QM

Phase Estimation

- Given:
  - unitary operation $U : \mathcal{H} \to \mathcal{H}$ with eigenvector $|u_j\rangle$, eigenvalue λ_j
    i.e., $U|u_j\rangle = \lambda_j|u_j\rangle$ moreover, $\lambda_j = e^{2\pi i\phi_j}$ for *phase* $\phi_j \in [0; 1)$
  - register prepared in state $|u_i\rangle$
- Task: find (m most significant bits of) ϕ_j



HHL: Mechanics

- construct superdense vector $|0\rangle \mapsto |\mathbf{b}\rangle$
- Hamiltonian simulation $|\mathbf{b}\rangle \mapsto \sum_k e^{iA2^k}|\mathbf{b}\rangle$
- write in eigenbasis $|\mathbf{b}\rangle = \sum_{\ell=0}^{N-1} \beta_\ell |u_\ell\rangle$
- phase est. + Hamiltonian sim.: $|0, \mathbf{b}\rangle \mapsto \sum_{\ell=0}^{N-1} \beta_\ell |\phi_\ell, u_\ell\rangle$
  - ϕ_ℓ are eigenvalues of A
- invert $|\phi_\ell\rangle \mapsto \phi_\ell^{-1}|\phi_\ell\rangle$
  - add ancilla qubit $|\phi_\ell\rangle \otimes |0\rangle$
  - rotate by C/ϕ_ℓ radians
    $|\phi_\ell\rangle \otimes |0\rangle \mapsto |\phi_\ell\rangle \otimes (\sin(C/\phi_\ell)\,|1\rangle + (\cos(C/\phi_\ell)\,|0\rangle)$

    $$\approx |\phi_\ell\rangle \otimes (\tfrac{C}{\phi_\ell}|1\rangle + \sqrt{1 - \tfrac{C^2}{\phi_\ell^2}}|0\rangle)$$
  - post-select for ancilla $|1\rangle$
  - hide normalizing constant
  - nonzero probability of failure
- undo phase estimation

$$\sum_{\ell=0}^{N-1} \beta_\ell \phi_\ell^{-1} |\phi_\ell, u_\ell\rangle \mapsto \sum_{\ell=0}^{N-1} \beta_\ell\, \phi_\ell^{-1} |0, u_\ell\rangle = |0\rangle \otimes A^{-1}|\mathbf{b}\rangle = |0\rangle \otimes |\mathbf{x}\rangle$$

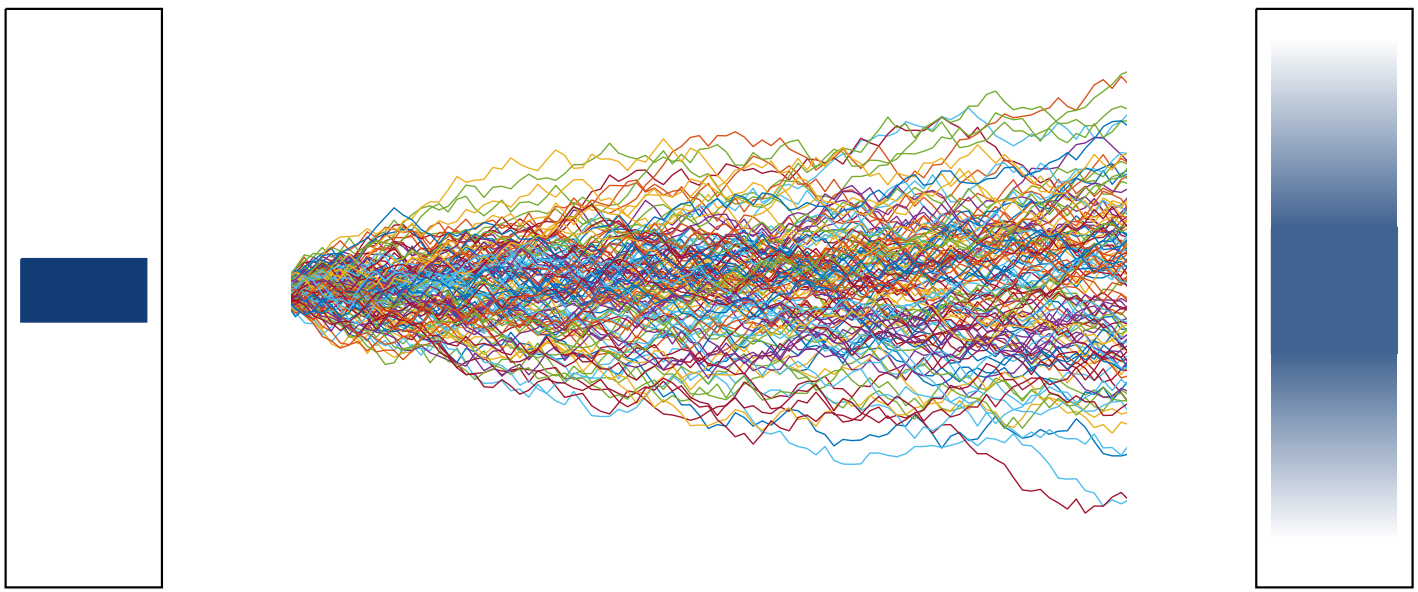
- measure aspect M of $|\mathbf{x}\rangle$ via $\langle \mathbf{x}|M|\mathbf{x}\rangle$

Quantum Finance

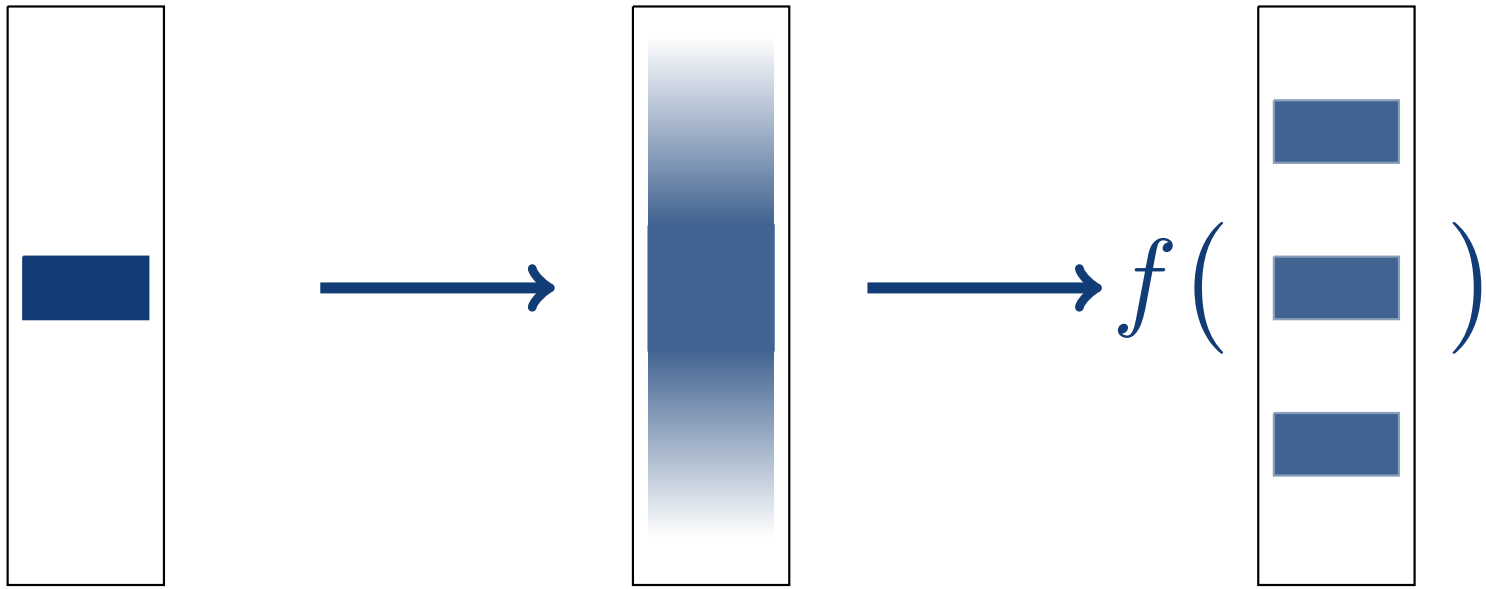
Applications of Quantum Computers to Quantum Finance

- ~~big data~~
- ~~generic optimization~~
- small data + complex problem
- interference
- superdense operations + delayed sampling
- in particular:
  - × dynamic portfolio optimization
  - ? scenario analysis
  - ✓ option pricing
  - ✓ clustering

- Black-Scholes equation $\frac{\partial V}{\partial t} + \frac{1}{2}\sigma^2 S^2 \frac{\partial^2 V}{\partial S^2} + rS\frac{\partial V}{\partial S} - rV = 0$
  - models price of (European style) options
- equivalent to heat equation $\frac{\partial u}{\partial \tau} = \frac{1}{2}\sigma^2 \frac{\partial^2 u}{\partial x^2}$
  - special case of diffusion equation

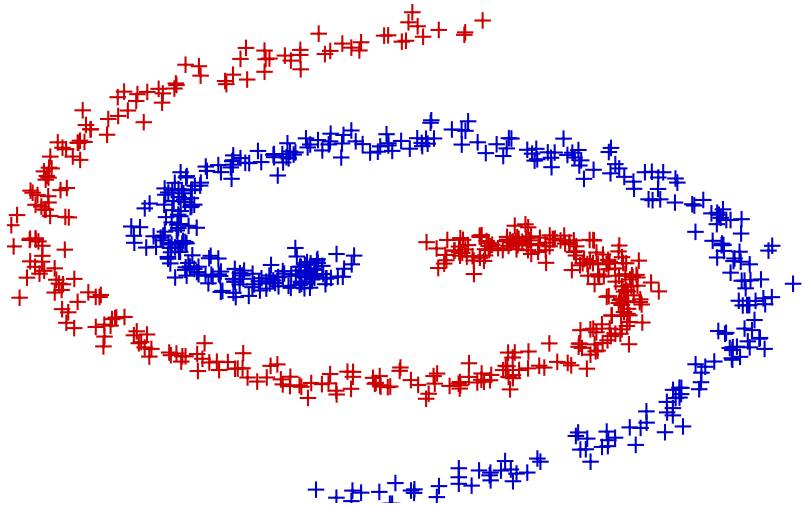


Quantum Walk



- path integral formulation
- faster spreading
- interference
- function-of-distribution (avoids sampling)

Clustering



- via Kernel Principal Component Analysis:
  - data: $(\vec{p}_0, \ldots, \vec{p}_{m-1}) \in \mathbb{R}^{n \times m}$
  - kernel matrix $K \in \mathbb{R}^{m \times m}$ with $k_{i,j} = \big(\varphi(\vec{p}_i) \cdot \varphi(\vec{p}_j)\big)$
  - principal eigenvector $\vec{v}_0$
  - color p_i red if $\vec{v}_0^{\mathsf{T}} K_{[:,i]} < 0$; and blue otherwise
- kernel trick: $\varphi : \mathbb{R}^n \to \mathbb{R}^\ell$ with $\ell \ggg n$

  but $k_{i,j} = \big(\varphi(\vec{p}_i) \cdot \varphi(\vec{p}_j)\big)$ is easy to compute

  e.g. $k_{i,j} = \exp\left(-\frac{\|\vec{p}_i - \vec{p}_j\|^2}{\sigma^2}\right)$
- quantum speedup?
  - how about $|\varphi(\vec{p}_i)\rangle$? $\Rightarrow$ more allowable kernel functions

Last Slide

1. Introduction
2. Quantum Computation
3. Shor's Algorithm
4. Grover's Algorithm
5. HHL Algorithm
6. Quantum Finance

alan.szepieniec@esat.kuleuven.be