Quantum algorithms II: Grover

Quantum computing

G. Chênevert

Feb. 12, 2021

Last time

- reversible evaluation of boolean functions U_f
- quantum circuit model of computation
- complexity $=$ $\#$ of gates

  ($+$ complexity of classical pre- and post-processing)
- quantum advantage
- example: Deutsch-Josza algorithm

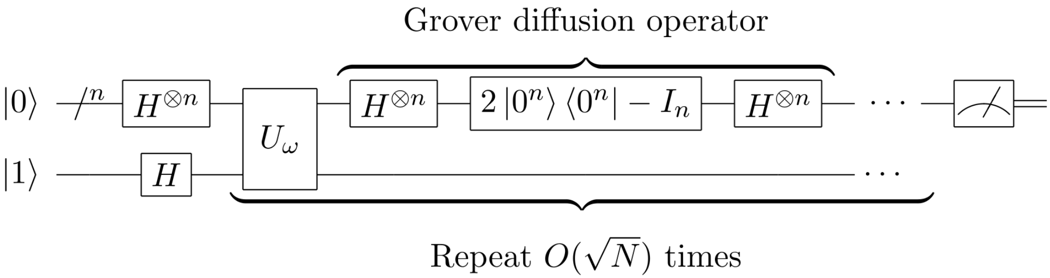
Quantum algorithms II: Grover

Grover's algorithm

Towards Shor

Grover (1970)

Grover (1996)


Grover diffusion operator
$|0\rangle$
n
$H^{\otimes n}$
$|1\rangle$
H
U_ω
$H^{\otimes n}$
$2\,|0^n\rangle\langle 0^n| - I_n$
$H^{\otimes n}$
$\cdots$
$\cdots$
Repeat $O(\sqrt{N})$ times

Search problem

Suppose we have a decision function $f : X \to \{0, 1\}$ defined on a set X of size N.

The search problem defined by f is to find some $x \in X$ for which $f(x) = 1$.

Examples: database queries, factoring integers, bitcoin mining, ...

In the general (unstructured) case: a classical algorithm requires $\mathcal{O}(N)$ queries.

(Of course can do better if *e.g.* the data is sorted)

Grover's algorithm

Performs unstructured searches for arbitrary criteria in $\mathcal{O}(\sqrt{N})$ time.

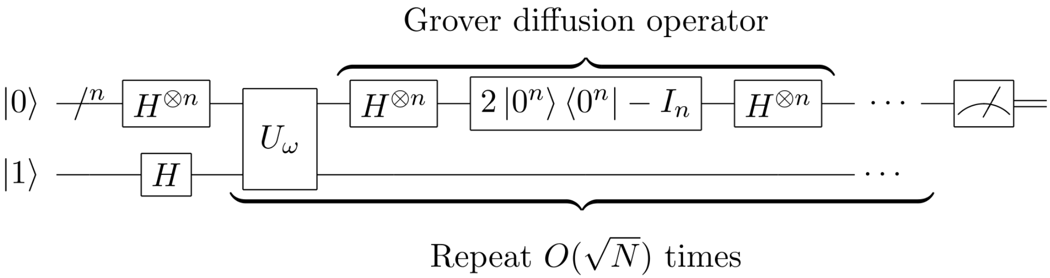
$\implies$ **quadratic speedup**

Works in two steps:

- phase inversion
- amplitude amplification

iterated a certain number of times

Circuit for Grover's algorithm



Phase inversion

Simplifying assumptions:

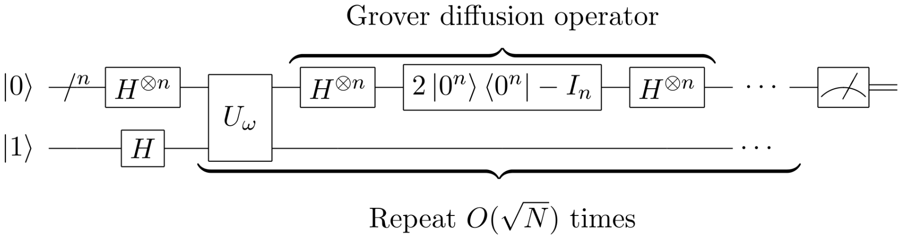
- $X = [\![0, N[\![$
- $N = 2^n$
- the equation $f(x) = 1$ admits a unique solution $\omega \in X$

So the problem is now: find $\omega \in X$ given access to a oracle for $f : [\![0, N[\![\to \{0, 1\}$

$$\text{where} \quad f(x) = \begin{cases} 1 & \text{if } x = \omega \\ 0 & \text{else.} \end{cases}$$

Phase inversion

ω is detected by inverting its phase: "$U_\omega|x\rangle \; = (-1)^{f(x)}|x\rangle$"



Actually

$$U_\omega\,|x\rangle \otimes |-\rangle = (-1)^{f(x)}\,|x\rangle \otimes |-\rangle$$

This is exactly what the oracle U_f does! So in fact "$U_\omega = U_f$".

Amplitude amplification

The **Grover diffusion operator** G is

$$G = 2|s\rangle\langle s| - I$$

where

$$|s\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle.$$

Geometrical interpretation:

$$G|s\rangle = |s\rangle$$

$$G|\psi\rangle = -|\psi\rangle \qquad \text{when } \langle s|\psi\rangle = 0$$

$U_s = -G$ is a reflection through the hyperplane normal to $|s\rangle$

Amplitude amplification

Remark: U_ω is a reflection, too.

Actually U_ω acts on $\mathcal{V} = \mathcal{V}_N \otimes |-\rangle$ as

$$I - 2|\omega\rangle\langle\omega| = \mathrm{diag}(1, \ldots, \underbrace{-1}_{\omega}, \ldots, 1).$$

In general $I - 2|\psi\rangle\langle\psi|$ is a reflection through the hyperplane normal to $|\psi\rangle$.

GU_ω: unitary transformation of $\mathcal{V}$ that inverts every vector $|\psi\rangle$ orthogonal to both $|s\rangle$ and $|\omega\rangle$ – and acts as a rotation in the plan spanned by $|s\rangle$ and $|\omega\rangle$

Amplitude amplification

Consider unitary $|s'\rangle \sim |s\rangle - \langle\omega|s\rangle|\omega\rangle$, and write $\langle\omega|s\rangle = \frac{1}{\sqrt{N}} = \sin\frac{\theta}{2}$.

Initial state:

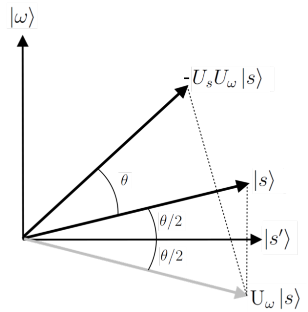
$$|\psi\rangle = |s\rangle = \cos\tfrac{\theta}{2}\,|s'\rangle + \sin\tfrac{\theta}{2}\,|\omega\rangle$$

GU_ω is a rotation of θ (exercise!), so after k iterations:

$$(GU_\omega)^k|\psi\rangle = \cos(\tfrac{\theta}{2} + k\theta)\,|s'\rangle + \sin(\tfrac{\theta}{2} + k\theta)\,|\omega\rangle$$

$$\mathbb{P}\big[\,\mathcal{M}(GU_\omega)^k|\psi\rangle = |\omega\rangle\,\big] = \sin^2(\tfrac{\theta}{2} + k\theta)$$

Optimal number of iterations



Each iteration brings the state closer to $|\omega\rangle$ by an angle of $\theta = 2 \arcsin \frac{1}{\sqrt{N}}$.

Until it starts moving away. . . Sage visualization

Optimal number of iterations

So, in order to maximize the probability of measuring $|\omega\rangle$, take

$$(k + \tfrac{1}{2})\theta \approx \frac{\pi}{2} \qquad \Longleftrightarrow \qquad k \approx \frac{\pi}{2\theta} - \frac{1}{2}$$

When N is large (interesting case!) we have $\theta \approx \sin\theta = \dfrac{2}{\sqrt{N}}$

so the optimal number of iterations is $k \approx \dfrac{\pi\sqrt{N}}{4}$.

Closely related to this rather surprising way to approximate π !

Implementation of G

$$G = 2|s\rangle\langle s| - I$$

- G is more easily computed if we change the basis:

$$G = H^{\otimes n} \otimes \underbrace{(2|0\rangle\langle 0| - I)}_{G_0} \otimes H^{\otimes n}$$

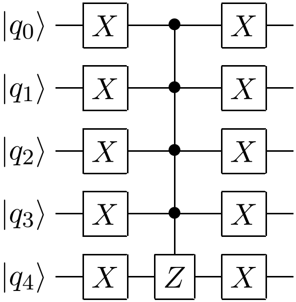
- $G_0 \sim -G_0 = U_0 = \mathrm{diag}(-1, 1, \ldots, 1)$:

$$U_0|x\rangle = \begin{cases} -|x\rangle & \text{if } x = 0 \\ |x\rangle & \text{if } x \neq 0. \end{cases}$$

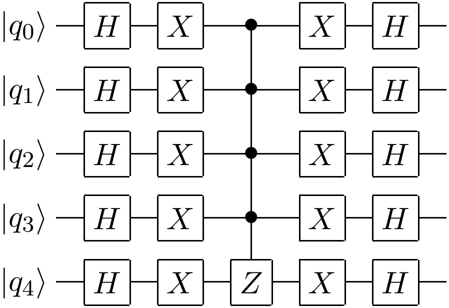
Implementation of G

Example: with $n = 4$

G_0:

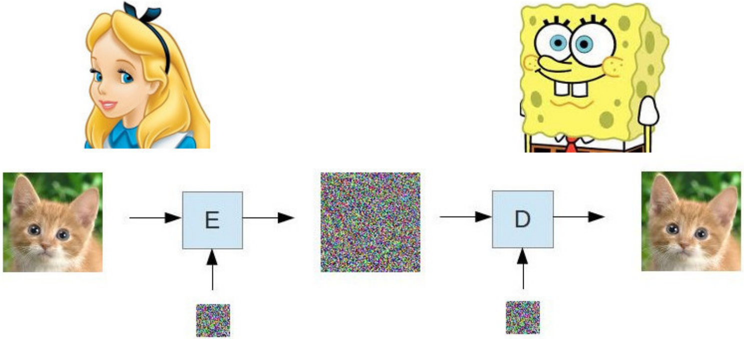


G:



Application: breaking cryptography

Alice sends secret messages to Bob:



Application: breaking cryptography

They agree on a secret n-bit encryption key k.

Alice encrypts her messages with k:

$$c = E(k, m)$$

and Bob decrypts them using the same k:

$$m = D(k, c).$$

Known plaintext attack

Imagine the attacker, Eve, knows the message m corresponding to *one* ciphertext c.

Then she can try to recover the secret key k in order to be able to decrypt *all* messages exchanged by Alice and Bob.

(A plausible scenario: this is exactly what happened with Enigma during WWII).

This is a search problem: she's looking for $k \in [\![0, 2^n[\![$ for which $D(k, c) = m$.

Brute force attack on the key

Suppose $n = 128$ (today's standard for AES).

With a classical computer: Eve will need to go through the 2^{128} possibilities: impractical for at least the next 30 years.

$\implies$ secure communication ✓

With a quantum computer running Grover's algorithm: Eve will recover the key in $\sqrt{2^{128}} = 2^{64}$ steps: doable today using specialized hardware.

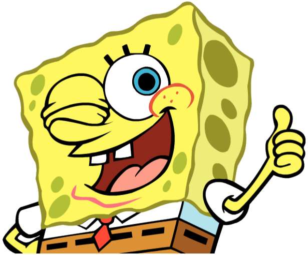
$\implies$ no more confidentiality ✗

Solution

In case this happens:

"post-quantum symmetric cryptography": just move to 256-bit keys

No biggie!



Quantum algorithms II: Grover

Grover's algorithm

Towards Shor

Quantum circuits

In the end, a quantum circuit is just a big unitary matrix.

n qubits: $2^n \times 2^n$ unitary matrix

Things we can implement using unitary matrices:

- reflections
- rotations
- ...
- **Fourier transforms**

Recall: Discrete Fourier Transform

N-point Fourier transform of a sequence $x[0], \ldots, x[N-1]$:

$$y[k] = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} e^{-\frac{2\pi ijk}{N}} x[j]$$

Matrix formulation:

$$\mathbf{y} = \mathcal{F}\,\mathbf{x} \qquad \text{with} \qquad \mathcal{F} = \frac{1}{\sqrt{N}} \begin{bmatrix} 1 & 1 & 1 & \ldots & 1 \\ 1 & \zeta & \zeta^2 & \ldots & \zeta^{N-1} \\ \vdots & \vdots & & & \vdots \\ 1 & \zeta^{N-1} & \zeta^{2(N-1)} & \ldots & \zeta^{(N-1)(N-1)} \end{bmatrix}$$

where ζ is *some* primitive N-th root of unity

Discrete Fourier Transform

Special case: $N = 2$

$$\mathcal{F} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} = H \quad (!)$$

Inverse Fourier transform:

$$\mathcal{F}^{-1} = \mathcal{F}^{*} = \mathcal{F}^{\dagger}$$

Fourier transforms are unitary

Quantum Fourier Transform

Suppose we have a quantum state $|\psi\rangle \in \mathcal{V}_N$:

$$|\psi\rangle = \sum_{x<N} \alpha_x |x\rangle$$

Its **Fourier transform** is the state

$$\mathcal{F}|\psi\rangle = \sum_{y<N} \beta_y |y\rangle$$

defined by

$$\beta_y = \frac{1}{\sqrt{N}} \sum_{x<N} \zeta^{xy} \alpha_x.$$

Quantum Fourier Transform

In other words: from a theoretical point of view

QFT of a state = DFT of the probability amplitudes

Often written in the equivalent form:

$$\mathcal{F}\,|x\rangle = \frac{1}{\sqrt{N}} \sum_{y<N} \zeta^{xy}\,|y\rangle$$

Naive classical algorithm: $\mathcal{O}(N^2)$ operations

Cooley-Tukey (1965): *Fast Fourier Transform* $\mathcal{O}(N \log N)$ operations

Quantum Fourier Transform

Theorem

There exists a quantum circuit with $\mathcal{O}((\log N)^2)$ gates that computes the QFT.

For $N = 2^n$, a circuit with $\mathcal{O}(n^2)$

- Hadamard gates $H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$
- controlled phase shifts $R_m = P(\frac{2\pi}{2^m}) = \begin{bmatrix} 1 & 0 \\ 0 & e^{\frac{2\pi i}{2^m}} \end{bmatrix}$
- swaps

suffices.

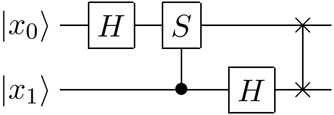
Small values of n

$n = 0$: $\mathcal{F} = I$ ✓

$n = 1$: $\mathcal{F} = H$ ✓

$n = 2$: with $S = R_2 = P(\frac{\pi}{2})$

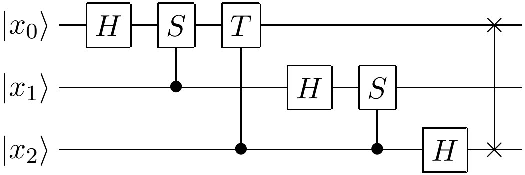
$$\mathcal{F} = \frac{1}{2}\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{bmatrix} =$$



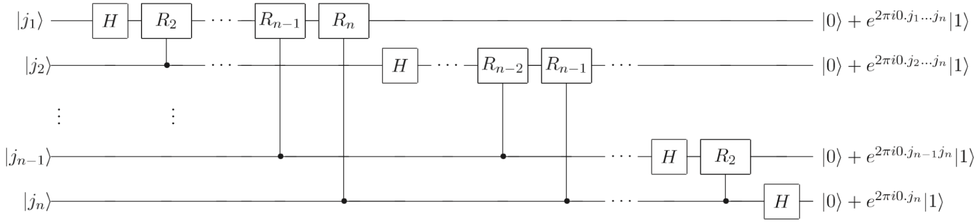
✓

Small values of n

$n = 3$: with $T = R_3 = P(\frac{\pi}{4})$



General QFT circuit



- n Hadamard gates
- $1 + 2 + \cdots + (n-1) = \binom{n}{2}$ controlled phase shifts
- $\leq \binom{n}{2}$ swaps