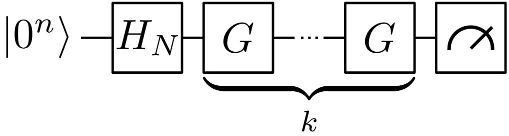
QUANTUM ALGORITHMS 1:
CIRCUITS, QFT AND GROVER



Simon Apers
(CNRS & IRIF, Paris)

McKinsey, Paris, April ’23

tutorial = overview (2h) + exercises (2h)

TUTORIAL 1: BASICS (21/4)

quantum circuits

quantum Fourier transform

Grover search

TUTORIAL 2: CHEMISTRY (28/4)

Hamiltonian simulation

energy estimation

variational quantum algorithms

TUTORIAL 3: OPTIMIZATION (26/5)

adiabatic algorithm

HHL

quantum walks

CIRCUITS

QFT

GROVER

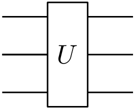
quantum state on 1 qubit

$$|\psi\rangle = \alpha_0 |0\rangle + \alpha_1 |1\rangle = \begin{bmatrix} \alpha_0 \\ \alpha_1 \end{bmatrix}$$

quantum state on n qubits ($N = 2^n$)

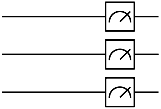
$$|\psi\rangle = \sum_{z \in \{0,1\}^n} \alpha_z |z\rangle = \begin{bmatrix} \alpha_0 \\ \alpha_1 \\ \vdots \\ \alpha_{N-1} \end{bmatrix}$$

unitary dynamics

$|\psi\rangle$ 

$|\psi'\rangle = U\,|\psi\rangle$

measurement

$|\psi\rangle = \sum_{z\in\{0,1\}^n} \alpha_z\,|z\rangle$  $|z\rangle$ with probability $|\alpha_z|^2$

Hadamard gate

$$-\boxed{H}- \quad \equiv \quad \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

such that

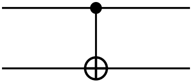
$$|0\rangle \quad -\boxed{H}- \quad \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

$$|1\rangle \quad -\boxed{H}- \quad \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

phase or T

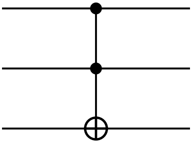
$$\equiv \begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}$$

CNOT



$$\equiv \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

CCNOT or Toffoli



EX: write down matrix for CNOT and Toffoli?

universality:

any unitary operation can be approximated with

$\{$1-qubit gates, $CNOT\}$

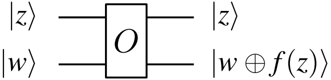
or

$$\{H, T, CNOT\}$$

or

$$\{H, CCNOT\}$$

quantum oracle/RAM query (for function f)



such that

$$O\,|z\rangle\,|0\rangle = |z\rangle\,|f(z)\rangle$$

and

$$O\left(\sum_z \alpha_z\,|z\rangle\,|0\rangle\right) = \sum_z \alpha_z\,|z\rangle\,|f(z)\rangle$$

Q: which function does CNOT evaluate? ($f(z) = z$)

CIRCUITS

QFT

GROVER

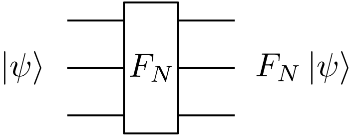
discrete Fourier transform $F_N : \mathbb{C}^N \to \mathbb{C}^N$

$$F_N = \frac{1}{\sqrt{N}} \begin{bmatrix} 1 & 1 & \dots & 1 \\ 1 & \omega_N & \dots & \omega_N^{N-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \omega_N^{N-1} & \dots & \omega_N^{(N-1)(N-1)} \end{bmatrix}, \quad \omega_N = e^{i2\pi/N}$$

Fourier modes

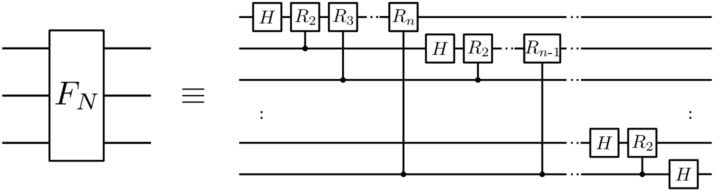
$$F_N |k\rangle = |\tilde{k}\rangle = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} \omega_N^{jk} |j\rangle$$

! F_N unitary matrix on $n = \log(N)$ qubits

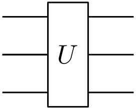


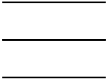
lemma:

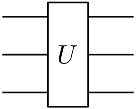
can implement F_N using $O(n^2)$ 2-qubit gates



application 1: quantum phase estimation (Kitaev '95)

given: circuit 

, state $|\phi\rangle$ 

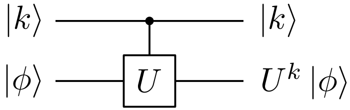
promise: $|\phi\rangle$ 

$e^{i2\pi\theta}\,|\phi\rangle$

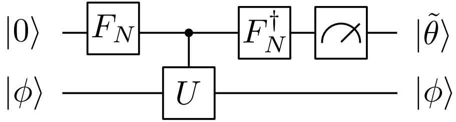
goal: find θ

Kitaev '95:
ε-approximation of θ with $O(1/\varepsilon)$ calls to U and 1 copy of $|\phi\rangle$

controlled unitary



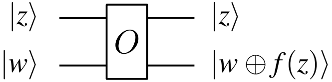
quantum phase estimation



(details in exercises)

application 2: quantum period finding

given: oracle



with $f : \mathbb{N} \to [N]$

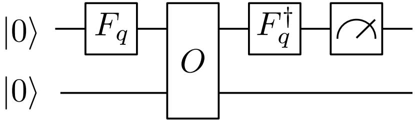
promise: period r s.t. $f(a) = f(b)$ iff $a = b \pmod r$

goal: find r

Shor '94:

1. factoring and discrete log reduce to period finding

2. quantum algorithm with $\mathrm{polylog}(N)$ calls to O



CIRCUITS

QFT

GROVER

problem: unstructured search

given: oracle access to $f : [N] \to \{0, 1\}$

promise: unique x s.t. $f(x) = 1$

goal: find x

Grover '96:
$O(\sqrt{N})$ quantum queries vs $O(N)$ classical queries

reflection 1: phase oracle

$$|x\rangle \quad -\boxed{O}- \quad (-1)^{f(x)}|x\rangle$$

reflection 2: around $|\pi\rangle := \frac{1}{\sqrt{N}}\sum_{y\in[N]}|y\rangle$

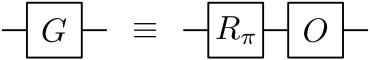
$$|\pi\rangle \quad -\boxed{R_\pi}- \quad |\pi\rangle$$

$$|\pi\rangle \perp |\phi\rangle \quad -\boxed{R_\pi}- \quad -|\phi\rangle$$

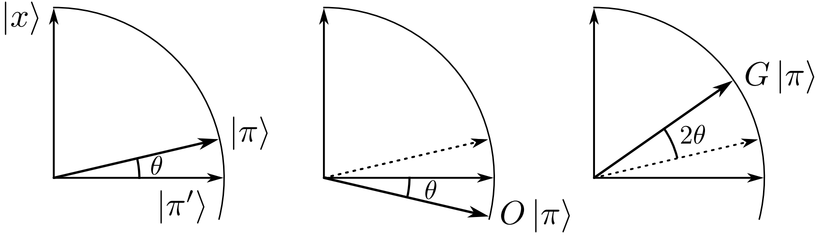
s.t.

$$-\boxed{R_\pi}- \quad \equiv \quad 2|\pi\rangle\langle\pi| - I$$

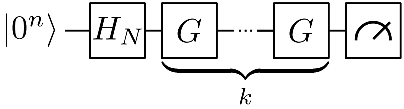
Grover operator



rewriting $|\pi\rangle = \sin\theta\,|x\rangle + \cos\theta\,|\pi'\rangle$ we get



Grover's algorithm



$$G^k\,|\pi\rangle = \sin((1+2k)\theta)\,|x\rangle + \cos((1+2k)\theta)\,|\pi'\rangle$$

finds x with constant probability after $k \in O(\sqrt{N})$ iterations matching $\Omega(\sqrt{N})$ lower bound

for ℓ marked elements: complexity $\Theta(\sqrt{N/\ell})$

generalizations:

- amplitude amplification

- quantum mean estimation