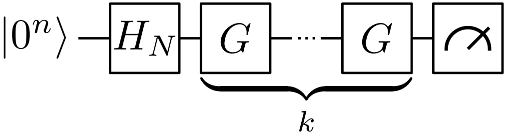
ADVANCED QUANTUM ALGORITHMS (AQALG): PRIMER ON CIRCUITS, QFT AND GROVER



Simon Apers
(CNRS & IRIF, Paris)
(simonapers.github.io/mckinsey.html)

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 1 qubit

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

unitary dynamics

$$|\psi\rangle \quad -\boxed{U}- \qquad |\psi'\rangle = U\,|\psi\rangle = \begin{bmatrix} U_{00} & U_{10} \\ U_{01} & U_{11} \end{bmatrix} \begin{bmatrix} \alpha_0 \\ \alpha_1 \end{bmatrix}$$

quantum state on 1 qubit

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

unitary dynamics

$$|\psi\rangle \quad \text{—}\boxed{U}\text{—} \quad |\psi'\rangle = U|\psi\rangle = \begin{bmatrix} U_{00} & U_{10} \\ U_{01} & U_{11} \end{bmatrix} \begin{bmatrix} \alpha_0 \\ \alpha_1 \end{bmatrix}$$

measurement

$$|\psi\rangle = \alpha_0 |0\rangle + \alpha_1 |1\rangle$$

$|0\rangle$ with probability $|\alpha_0|^2$

$|1\rangle$ with probability $|\alpha_1|^2$

Hadamard gate

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

Hadamard gate

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

such that

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

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

X or NOT gate

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

X or NOT gate

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

Z gate

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

X or NOT gate

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

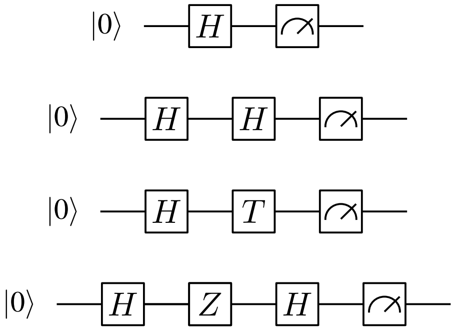
Z gate

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

phase or T gate

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

EX: what is the outcome of the following circuits?

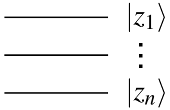


quantum states on n qubits ($N = 2^n$):

quantum states on n qubits ($N = 2^n$):

basis state ($z \in \{0,1\}^n$)

$$|z\rangle = |z_1\rangle \otimes \cdots \otimes |z_n\rangle = |z_1 \ldots z_n\rangle$$



quantum states on n qubits ($N = 2^n$):

basis state ($z \in \{0,1\}^n$)

$$|z\rangle = |z_1\rangle \otimes \cdots \otimes |z_n\rangle = |z_1 \ldots z_n\rangle$$

$|z_1\rangle$

$\vdots$

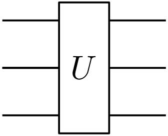
$|z_n\rangle$

superposition

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

unitary dynamics

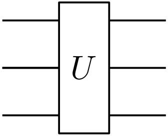
$|\psi\rangle$



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

unitary dynamics

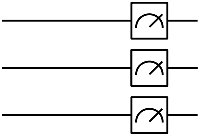
$|\psi\rangle$



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

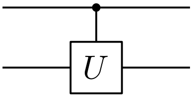
measurement

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

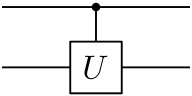


$|z\rangle$ with probability $|\alpha_z|^2$

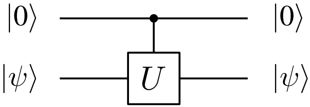
controlled unitary

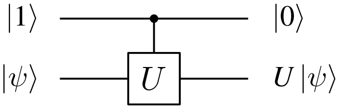


controlled unitary

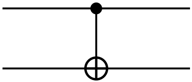


such that

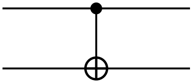




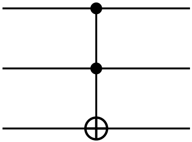
CNOT



CNOT

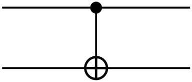


CCNOT or Toffoli



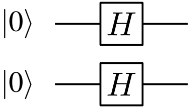
EX:

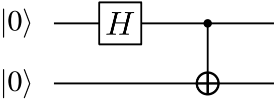
fill in:



$$\equiv \begin{bmatrix} ? & ? & ? & ? \\ ? & ? & ? & ? \\ ? & ? & ? & ? \\ ? & ? & ? & ? \end{bmatrix}$$

what is the outcome of the following circuits?





universality:

any unitary operation can be approximated with

universality:

any unitary operation can be approximated with

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

universality:

any unitary operation can be approximated with

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

or

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

universality:

any unitary operation can be approximated with

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

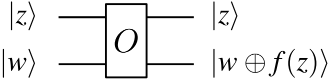
or

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

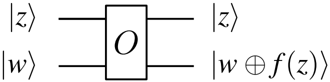
or

$$\{H, CCNOT\}$$

quantum oracle/RAM query (for function f)



quantum oracle/RAM query (for function f)



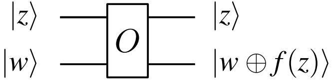
such that

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

and

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

quantum oracle/RAM query (for function f)



such that

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

and

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

EX: which function does CNOT evaluate?

CIRCUITS

QFT

GROVER

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

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

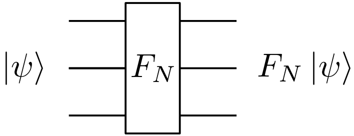
discrete Fourier transform $F_N : \mathbb{C}^N \to \mathbb{C}^N$

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

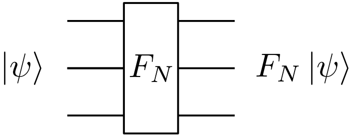
Fourier modes

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

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

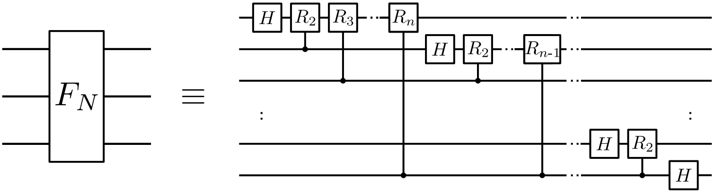


! F_N unitary matrix on $n = \log(N)$ qubits

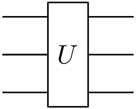
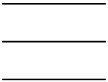


lemma:

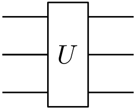
can implement F_N using $O(n^2)$ 2-qubit gates

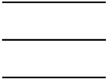


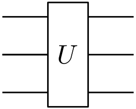
application 1: quantum phase estimation (Kitaev ’95)

given: circuit  , state $|\phi\rangle$ 

application 1: quantum phase estimation (Kitaev ’95)

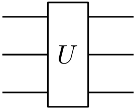
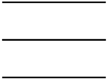
given: circuit 

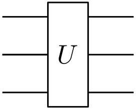
, state $|\phi\rangle$ 

promise: $|\phi\rangle$ 

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

application 1: quantum phase estimation (Kitaev ’95)

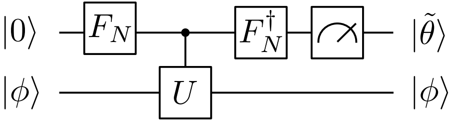
given: circuit  , state $|\phi\rangle$ 

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

goal: find θ

Kitaev '95:

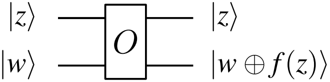
ε-approximation of θ with $O(1/\varepsilon)$ calls to U and 1 copy of $|\phi\rangle$



(details in exercises)

application 2: quantum period finding

given: oracle



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

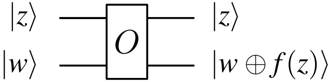
application 2: quantum period finding

given: oracle $\begin{array}{c} |z\rangle \\ |w\rangle \end{array} \boxed{O} \begin{array}{l} |z\rangle \\ |w \oplus f(z)\rangle \end{array}$ with $f : \mathbb{N} \to [N]$

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

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:

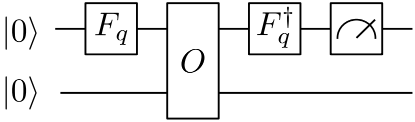
Shor '94:

1. factoring and discrete log reduce to period finding

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

problem: unstructured search

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

problem: unstructured search

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

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

problem: unstructured search

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

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

goal: find x

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 1: phase oracle

$$|x\rangle \; -\!\boxed{O}\!- \; (-1)^{f(x)}\,|x\rangle$$

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

$$|\pi\rangle \; -\!\boxed{R_\pi}\!- \; |\pi\rangle$$

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

reflection 1: phase oracle

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

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

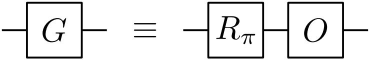
$$|\pi\rangle \; -\boxed{R_\pi}- \; |\pi\rangle$$

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

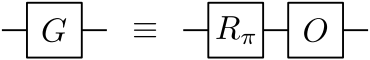
s.t.

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

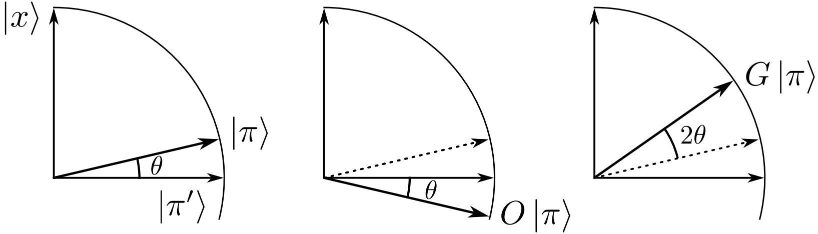
Grover operator



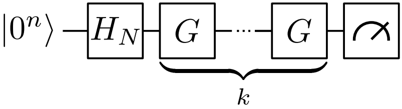
Grover operator



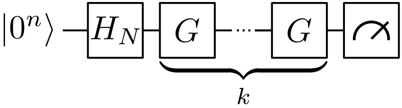
rewriting $|\pi\rangle = \sin\theta\,|x\rangle + \cos\theta\,|\pi'\rangle$ we get



Grover's algorithm

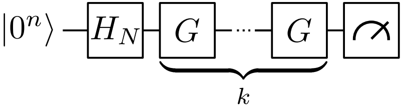


Grover's algorithm



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

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

matching $\Omega(\sqrt{N})$ lower bound

for M marked elements:

complexity $\Theta(\sqrt{N/M})$

matching $\Omega(\sqrt{N})$ lower bound

for M marked elements:

complexity $\Theta(\sqrt{N/M})$

generalizations:

- amplitude amplification
- quantum mean estimation