Speed-up of Quantum Algorithms

Unconventional Models of Computation (Alberto Leporati)

Adrián Puerto Aubel,
PhD Student of the XXXIst cycle

March 14, 2018

Qubit: measure and state

Measure of a qubit ψ:

- $\mu(\psi) \in \{0, 1\}$
- $\alpha, \beta \in \mathbb{C} : |\alpha|^2 + |\beta|^2 = 1$
- $P(\mu(\psi) = 0) = |\alpha|^2$
- $P(\mu(\psi) = 1) = |\beta|^2$

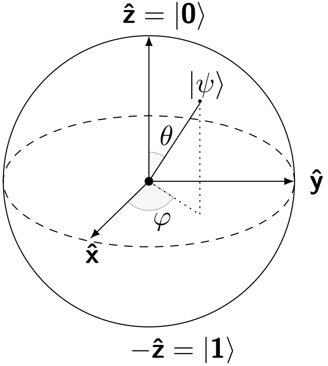
State of ψ:

- $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$

$= \cos(\theta/2)|0\rangle + e^{i\phi}\sin(\theta/2)|1\rangle$

- θ encodes the probability of measuring 0 or 1
- the phase ϕ allows to encode more information

Bloch Sphere



Single qubit gates

Operation on a single classic bit:

- Not ($\neg$)

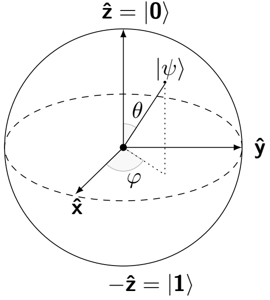
Operations on a single qubit:

- Any operation on the bloch sphere: Pauli gates in the ($|0\rangle, |1\rangle$) basis
- X gate: $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} : \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \longrightarrow \begin{pmatrix} \beta \\ \alpha \end{pmatrix}$
- Y gate: $\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} : \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \longrightarrow \begin{pmatrix} -i\beta \\ i\alpha \end{pmatrix}$
- Z gate: $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} : \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \longrightarrow \begin{pmatrix} \alpha \\ -\beta \end{pmatrix}$

Basic Algorithm building blocks

- Rotations
- Symmetries

Bloch Sphere



Single qubit gates

Operation on a single classic bit:

- Not $(\neg)$

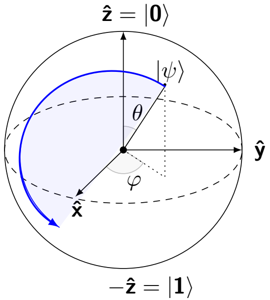
Operations on a single qubit:

- Any operation on the bloch sphere: Pauli gates in the $(|0\rangle, |1\rangle)$ basis
- X gate: $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} : \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \longrightarrow \begin{pmatrix} \beta \\ \alpha \end{pmatrix}$
- Y gate: $\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} : \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \longrightarrow \begin{pmatrix} -i\beta \\ i\alpha \end{pmatrix}$
- Z gate: $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} : \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \longrightarrow \begin{pmatrix} \alpha \\ -\beta \end{pmatrix}$

Basic Algorithm building blocks

- Rotations
- Symmetries

Bloch Sphere



Single qubit gates

Operation on a single classic bit:

- Not ($\neg$)

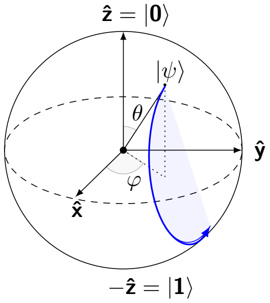
Operations on a single qubit:

- Any operation on the bloch sphere: Pauli gates in the $(|0\rangle, |1\rangle)$ basis
- X gate: $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} : \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \longrightarrow \begin{pmatrix} \beta \\ \alpha \end{pmatrix}$
- Y gate: $\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} : \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \longrightarrow \begin{pmatrix} -i\beta \\ i\alpha \end{pmatrix}$
- Z gate: $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} : \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \longrightarrow \begin{pmatrix} \alpha \\ -\beta \end{pmatrix}$

Basic Algorithm building blocks

- Rotations
- Symmetries

Bloch Sphere



Single qubit gates

Operation on a single classic bit:

- Not ($\neg$)

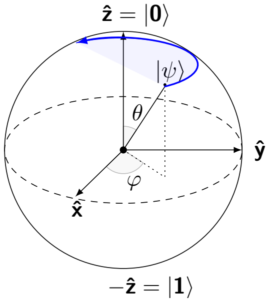
Operations on a single qubit:

- Any operation on the bloch sphere: Pauli gates in the $(|0\rangle, |1\rangle)$ basis
- X gate: $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} : \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \longrightarrow \begin{pmatrix} \beta \\ \alpha \end{pmatrix}$
- Y gate: $\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} : \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \longrightarrow \begin{pmatrix} -i\beta \\ i\alpha \end{pmatrix}$
- Z gate: $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} : \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \longrightarrow \begin{pmatrix} \alpha \\ -\beta \end{pmatrix}$

Basic Algorithm building blocks

- Rotations
- Symmetries

Bloch Sphere



Muliple qubits

- The state of a system (or register) with k qubits can be seen as $s \in \mathbb{C}^{2k}$
- HOWEVER, amplitude of qubits cannot be measured: the norm of s will remain unknown.
- Operations (or gates) on registers must be reversible: $U : \mathbb{C}^{2k} \to \mathbb{C}^{2k}$ such that $UU^* = I$ where U^* is the Hermitian conjugate of U.
- Unitary maps are rotations and symmetries.
- Example: CNOT gate: $\mathbb{C}^2 \to \mathbb{C}^2$ $\quad U|x\rangle|y\rangle = |x\rangle|x \oplus y\rangle$

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

- Input register, Output register

Special states

Features of quantum states:

Superposition:

The Hadamard gate:

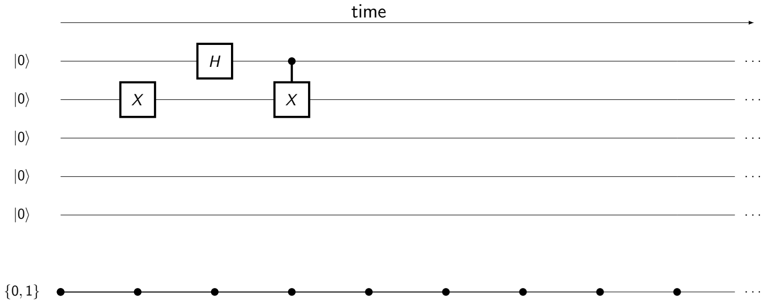
$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

applied to $|0\rangle$ or $|1\rangle$ provides a state
with equal probabilities of measuring 0 or 1.

Entanglement:

- When the control of a controlled-gate is in a superposition state, measuring the control (or input) will force the output value.
- Input and output become correlated:
  measure of either one will force the value of the other.
- BUT we can continue computations on the registers until measure.

Entanglement Example:
Creating a Bell State on IBM Q



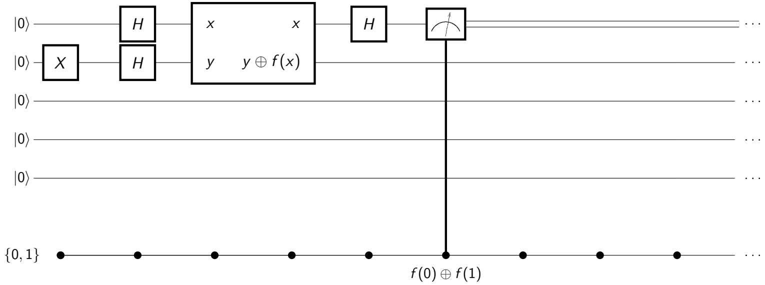
https://quantumexperience.ng.bluemix.net/qx/editor

Deutsch's XOR

Problem:

Given a function $f : \{0,1\} \rightarrow \{0,1\}$, and provided a black-box performing the unitary transformation $U|x\rangle|y\rangle = |x\rangle|y \oplus f(x)\rangle$,
determine whether f is constant or balanced.

Algorithm:



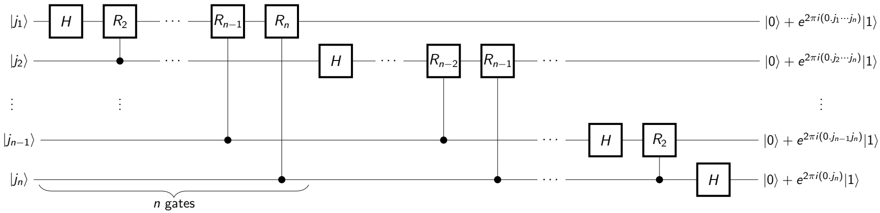
Superposition: Hadamard Gate → one call to the black-box
Entanglement: Black box → measure on input register

Quantum Fourier Transform

Classic Fourier Transform: $(x_j)_{j<N} \in \mathbb{C}^N \to 1/\sqrt{N}.(\Sigma_{j=0}^{N-1} x_j.e^{2\pi ijk/N})_{j<N}$
Quantum standard Notation: $|j\rangle \to 1/\sqrt{N}.\Sigma_{j=0}^{N-1} e^{2\pi ijk/N}|k\rangle$

$$R_k = \begin{pmatrix} 1 & 0 \\ 0 & e^{2\pi i/2^k} \end{pmatrix} \qquad 0.j_n \cdots j_m := \sum_{k=n}^{m} j_k/2^{k-n+1}$$

Algortihm:



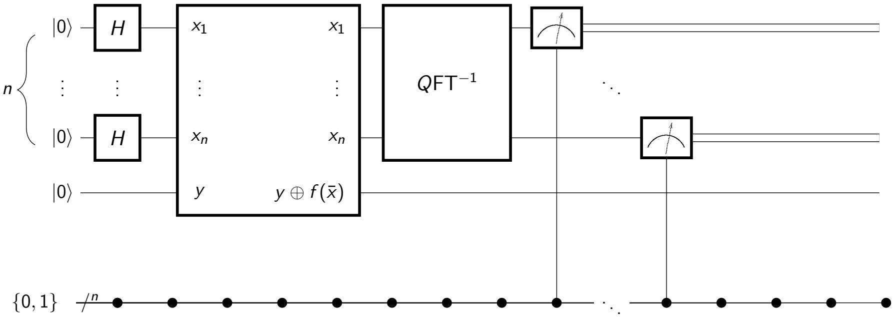
Complexity: let $N = 2^n$, $\Theta(n(n+1)/2 + n/2) = \Theta(n^2)$ — FFT: $\Theta(n2^n)$

- QFT presents substantial speedup
  BUT amplitudes cannot be measured
  $\Rightarrow$ QFT cannot be used directly for performing FT.
- HOWEVER, we can use IQFT to perform *Phase Estimation*
- Given a controlled U^j black-box, and a known eigenstate $|u\rangle$, we look for the phase ϕ_u of an eigenvalue $e^{2\pi i\phi_u}$
- $U^j : 1/\sqrt{2^t}\Sigma_{j=0}^{2^t-1}|j\rangle|u\rangle \rightarrow 1/\sqrt{2^t}\Sigma_{j=0}^{2^t-1}|j\rangle U^j|u\rangle$
  $= 1/\sqrt{2^t}\Sigma_{j=0}^{2^t-1}e^{2\pi ij\phi_u}|j\rangle|u\rangle$
- IQFT: $1/\sqrt{2^t}\Sigma_{j=0}^{2^t-1}e^{2\pi ij\phi_u}|j\rangle|u\rangle \rightarrow |\widetilde{\phi_u}\rangle|u\rangle$
- Accuracy of estimation $\widetilde{\phi_u}$ depends on the value of t

Simon's Period Finding Algorithm

Problem:
Given a periodic function f of unknown period r: $f(x+r) = f(x)$, and provided a black-box which performs the unitary transformation $U|x\rangle|y\rangle \rightarrow |x\rangle|y \oplus f(x)\rangle$, determine r

Algorithm:



Complexity: $\mathcal{O}(L^2)$ for $0 < r < 2^L$ vs. **NP** in classical.

Simon's Period Finding Algorithm

Given a periodic function f of unknown period r: $f(x+r) = f(x)$, and provided a black-box which performs the unitary transformation $U|x\rangle|y\rangle \rightarrow |x\rangle|y \oplus f(x)\rangle$, determine r

- initial state: $|0\rangle|0\rangle$
- create superposition on first register :

$$1/\sqrt{2^t}\Sigma_{x=0}^{2^t-1}|x\rangle|0\rangle$$

- apply back-box U:

$$1/\sqrt{2^t}\Sigma_{x=0}^{2^t-1}|x\rangle|f(x)\rangle \simeq 1/\sqrt{r2^t}\Sigma_{l=0}^{r-1}\Sigma_{x=0}^{2^t-1}e^{2\pi ilx/r}|x\rangle|\tilde{f}(l)\rangle$$

- IQFT:

$$1/\sqrt{r}\Sigma_{l=0}^{r-1}|\widetilde{l/r}\rangle|\tilde{f}(x)\rangle$$

- measure first register: $\widetilde{l/r}$
- continued fraction alg.: r $(\mathcal{O}(n^2))$

Order Finding

Let x and N be co-prime numbers such that N is L-bit, and provided a black-box $U_{x,n} : |j\rangle|k\rangle \rightarrow |j\rangle|x^j k \mod N\rangle$, determine the least integer $r > 0 : x^r = 1 \mod N$

- initial state: $|0\rangle|1\rangle$
- create superposition on first register :

$$1/\sqrt{2^t}\Sigma_{j=0}^{2^t-1}|j\rangle|1\rangle$$

- apply back-box $U_{x,n}$:

$$1/\sqrt{2^t}\Sigma_{j=0}^{2^t-1}|j\rangle|x^j k \mod N\rangle \simeq 1/\sqrt{r2^t}\Sigma_{s=0}^{r-1}\Sigma_{j=0}^{2^t-1}e^{2\pi isj/r}|j\rangle|u_s\rangle$$

- IQFT:

$$1/\sqrt{r}\Sigma_{s=0}^{r-1}|\widetilde{s/r}\rangle|u_s\rangle$$

- measure first register: $\widetilde{s/r}$
- continued fraction alg.: r

Generalization: Hidden subgroup Problem

Generalization:
Input register, output register $\rightarrow$ create superposition on input register $\rightarrow$ apply black-box $\rightarrow$ IQFT $\rightarrow$ measure first register $\rightarrow$ apply continuous fraction algorithm.

Can be applied to the general problem:
Let G be a finitely generated group, K be a subgroup of G, and X a finite set with a suitable binary operation $\oplus$.
A *coset* of K in G is a set: $\forall g \in G : gK := \{g.k \mid k \in K\}$.
Let $f : G \rightarrow X$ be a function which is constant on the cosets of K.
Provided a black-box $U|g\rangle|x\rangle = |g\rangle|x \oplus f(g)\rangle$ for $g \in G$ and $x \in X$, find a generating set for K

Generalization: Hidden subgroup Problem

Hidden Subgroup problem:

Let G be a finitely generated group, K be a subgroup of G, and X a finite set with a suitable binary operation $\oplus$.
A *coset* of K in G is a set: $\forall g \in G : gK := \{g.k \mid k \in K\}$.
Let $f : G \to X$ be a function which is constant on the cosets of K.
Provided a black-box $U|g\rangle|x\rangle = |g\rangle|x \oplus f(g)\rangle$ for $g \in G$ and $x \in X$, find a generating set for K

Instances:

- Deutsch: $G = \mathbb{Z}_2$; $X = \{0, 1\}$,
  $K = \{0\}$(balanced) or $K = \{0, 1\}$(constant)
- Period finding: $G = (\mathbb{Z}, +)$, X is any finite set,
  $K = \{0, r, 2r, ...\}$ for some $r \in G$
- Order finding: $G = (\mathbb{Z}, +)$, $X = \{a^j \mid j \in \mathbb{Z}_r, a^r = 1\}$,
  $K = \{0, r, 2r, ...\}$ for some $r \in G$

Conclusions and Conjectures over Quantum Speedup

- Problems such that there is a known quantum algorithm to solve them, performing qualitatively better than the classical one, are reducible to The *Hidden Subgroup Problem*.
- This improvement is achieved by exploiting *Superposition, Entanglement,* and *Phase Estimation*.
- We can implement and run such algorithms on IBM Q, but we are still limited to 5 qubits for both input and output registers.
- Main Refernece:

Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information: 10th Anniversary Edition*.
Cambridge University Press, New York, NY, USA, 10th edition, 2011