BRICS Mini-course on Quantum Computation

A. Berthiaume
C.W. I.

Session I: Introduction
Interferometer:

\[ s \rightarrow M_1 \rightarrow \text{Mirror} \rightarrow M_2 \rightarrow D_H \text{ (click!) \rightarrow D_v } \]

\[ \sim \text{: Mirror} \]

\[ \sim \text{: Half-Silvered Mirror} \]
Historical Remarks:

- 1982 Benioff/Feynman
  idea of a fully QM comp.

- 1985 Deutsch
  Formalism for QTM

- 1989 Deutsch
  Formalism for Q circuits

- 1993 Yao
  QTM = Q circuits

- 1995 BBC et al.
  Quantum gate results
Quantum Basics:

Basis States: all classically distinct alternative of a given property.

- position
- path
- orientation

Notation: if $x$ is the label of an alternative, then that state is noted

$|x\rangle$

N.B.: $\frac{1}{2} |4\rangle \neq |2\rangle$

NO!
Quantum Basics (cont.):

Amplitude: The probability of an alternative \( X \) is given by the square norm of a complex number \( \alpha \).

\[
P(1X>) = 1|\alpha|^2
\]

State Vector: A sum of all alternatives weighted by their amplitudes.

\[
\psi > = \sum_{i \in B} \alpha_i 1_i >
\]

where

\( B = \{i \mid i \text{ is a label}\} \)

is a set of basis states
Quantum Basics (cont.):

All possible $\sum_{i \in B} a_i |i\rangle$ form a complex vector space (a Hilbert space).

$$|y\rangle = \sum_{i \in B} a_i |i\rangle \quad \rightarrow \quad \begin{pmatrix} x_1 \\ x_2 \\ \vdots \end{pmatrix} \in \mathbb{C}^n$$

$$\text{Dim} (\mathbb{C}^n) = \# B$$
Quantum Basics (cont.):

Evolution: state vectors are transformed through unitary matrices.

\[ UU^\dagger = I \]

\[ U|\psi\rangle = |\psi\rangle' \]

ex:  

\[ U|H\rangle = \alpha|H\rangle + \beta|V\rangle \]

where \( |\alpha|^2 = |\beta|^2 = \frac{1}{2} \)
Quantum Basics (cont.):

Observable: an observable $\mathcal{O}$ is a partition of $\mathcal{H}$ in $E_1, \ldots, E_k$ subspaces such that

$$\mathcal{H} = E_1 \times E_2 \times \cdots \times E_k$$

and $\forall i \neq j \ E_i \perp E_j$

N.B.: The property determines the partitionning.
Quantum Basics (cont.):

Observation: Let \( |\phi \rangle = \sum_{i \in B} \alpha_i |i\rangle \) in \( B \).

H. We want to observe this state with \( \mathcal{O} = \{ E_1, \ldots, E_k \} \):

\[
|\phi \rangle = \sum_{i \in B} \alpha_i |i\rangle \quad \Rightarrow \quad |\phi \rangle = \sum_{j=1}^{k} \beta_j |\phi_j \rangle
\]

where \( |\phi_j \rangle \in E_j \).

Observing will:

1) select \( E_j \) with prob. \( |\beta_j|^2 \)
2) \( |\phi \rangle \rightarrow |\phi_j \rangle \)
3) All we learn is \( "j" \)
Quantum Basics (cont.):

Notation: if $|\psi\rangle = \sum_i x_i |i\rangle$
then

$\langle \psi | = \sum_i x_i^* \langle i |$

Projection: (inner product)

Let $|\psi\rangle = \sum_i x_i |i\rangle$ and

$|\psi\rangle = \sum_i \beta_i |i\rangle$
then

$|\psi\rangle \cdot |\psi\rangle = \langle \psi | \psi \rangle$

$= \sum_{i,j} \beta_i^* x_j \langle i | j \rangle$

$= \sum_{i,j} \beta_i^* x_j \delta_{ij}$

$= \sum_i \beta_i^* x_i$
Working out the interferometer:

Basis States: \( B = \{ \text{1H} >, \text{1V} > \} \)

Initial State: \( |s> = |\text{1H}> \)

Transformations:

\[
\begin{align*}
|\text{1H}> & \rightarrow \frac{1}{\sqrt{2}} (|\text{1H}> + i|\text{1V}>) \\
|\text{1V}>& \rightarrow \frac{1}{\sqrt{2}} (i|\text{1H}> + |\text{1V}>)
\end{align*}
\]

if \( |\text{1H}>= (1) \) and \( |\text{1V}>= (0) \) then

\[
M_{\frac{1}{2}} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix}
\]

Note: \( M_{\frac{1}{2}} M_{\frac{1}{2}}^\dagger = I \)
Working out...

2) $M_1 \rightarrow \mathcal{H} \rightarrow i\mathcal{V}
\quad |H\rangle \rightarrow i|V\rangle$ 
\quad $|V\rangle \rightarrow i|H\rangle$

so $M = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$

Note: $MM^T = I$
Working out...:

\[ |H\rangle \rightarrow \frac{1}{\sqrt{2}} (|H\rangle + i|V\rangle) \]

\[ \rightarrow \frac{1}{\sqrt{2}} (-|H\rangle + i|V\rangle) \]

\[ \rightarrow \frac{1}{\sqrt{2}} \left[ -\frac{1}{\sqrt{2}} (|H\rangle + i|V\rangle) \right. \]

\[ \left. + \frac{1}{\sqrt{2}} (i|H\rangle + |V\rangle) \right] \]

\[ = \frac{1}{2} (-|H\rangle - i|V\rangle - |H\rangle + i|V\rangle) \]

\[ = -|H\rangle \]

\[ M_{\frac{1}{2}} M_{\frac{1}{2}} |H\rangle = M_{\frac{1}{2}} M_{\frac{1}{2}} \left( \frac{1}{\sqrt{2}} \right) \]

\[ = M_{\frac{1}{2}} \left( \frac{1}{\sqrt{2}} \right) \]

\[ = M_{\frac{1}{2}} \left( \frac{-1}{\sqrt{2}} \right) \]

\[ = \left( \begin{array}{c} -1 \\ 0 \end{array} \right) \]
Quantum Computation Basics:

Qubit: a quantum state of the form

\[ |\psi\rangle = \alpha |0\rangle + \beta |1\rangle \]

where \( |\alpha|^2 + |\beta|^2 = 1 \)

Qugate: (for 1 qubit) is a \( 2 \times 2 \) (or gate) unitary matrix \( U \).

\[ U |\psi\rangle = |\psi'\rangle \]

Notation:

\[ |\psi\rangle \quad \boxed{U} \quad |\psi'\rangle \]

ex: \( U = M_{1/2} \)

\[ |0\rangle \quad \boxed{M_{1/2}} \quad \frac{1}{\sqrt{2}} (|0\rangle + i|1\rangle) \]
The interferometer in gates:

\[ |H\rangle \xrightarrow{M'_{1/2}} | \frac{1}{\sqrt{2}} (|H\rangle + i|V\rangle) \xrightarrow{M} | \frac{1}{\sqrt{2}} (i|H\rangle - |V\rangle) \xrightarrow{M'_{1/2}} -|H\rangle \]
QC Basics (cont.):

Qugate: (for 2 qubits)

\[ |b_1\rangle \quad U \quad |b_2\rangle \]

What's the joint basis?

What's the joint state?
Tensor Product: \( \otimes \)

When we have 2 qubits:

Joint basis: \( B_2 = \{ |00\rangle, |01\rangle, |10\rangle, |11\rangle \} \)

Joint state: if \( |b_1\rangle = \alpha_0 |0\rangle + \alpha_1 |1\rangle \)

\( \text{and} \)

\( |b_2\rangle = \beta_0 |0\rangle + \beta_1 |1\rangle \)

then

\( |b_1\rangle \otimes |b_2\rangle = |b_1\rangle |b_2\rangle = \sum_{ij=0}^1 \alpha_i \beta_j |i\rangle |j\rangle \)
Entanglement:

Let \( |\psi\rangle = \alpha_1 |00\rangle + \alpha_2 |10\rangle + \alpha_3 |11\rangle + \alpha_4 |11\rangle \)

If \( |\psi\rangle = (\beta_1 |0\rangle + \beta_2 |1\rangle) \otimes (\gamma_1 |10\rangle + \gamma_2 |11\rangle) \)

\[ = |b_1\rangle \otimes |b_2\rangle \]

then \( |b_1\rangle \) and \( |b_2\rangle \) are independent.

Otherwise \( |\psi\rangle \) is entangled.

\[ \text{e.g.: } |\psi\rangle = \frac{1}{2} [|100\rangle + |101\rangle + |110\rangle + |111\rangle] \]

\[ = \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}} (|10\rangle + |11\rangle) \]

\[ |\psi_2\rangle = \frac{1}{\sqrt{2}} (|100\rangle + |111\rangle) \text{ is entangled} \]
Qugates on 2 qubits:

In general: a $4 \times 4$ unitary matrix

\[
U
\]

Special Case

\[
\begin{array}{c}
A \\
B
\end{array}
\]

\[
U
\]

then

\[
U = A \otimes B = \begin{pmatrix}
a_{11} B & a_{12} B \\
a_{21} B & a_{22} B
\end{pmatrix}
\]
Quantum Register:

Def: an \( n \) qubit quantum register is a quantum state of the form

\[
|\psi\rangle = \sum_{i=0}^{2^n-1} a_i |i\rangle
\]

where \( |i\rangle \) is the \( i^{th} \) binary string on \( n \) bits.

\( n \)-qubits: qubits on \( n \) qubit registers are \( 2^n \times 2^n \) unitary matrices.
Modified Deutsch-Jozsa Problem:

Let $f : \{0,1\}^n \rightarrow \{0,1\}$ computable.

We define:

* Non-Balanced: There is a majority of 0's (or 1's)

** Non-Constant: $\exists x,y$ s.t. $f(x) \neq f(y)$

Problem: Given $f$, output $P \in \{*,**,\}$ such that $P(f)$ is true
**Lecerf-Bennett Theorem:**

**Thm:** For all $f$ computable in time $O(T)$, there exist a unitary matrix $U$ such that

$$U_f |x, o\rangle = |x, f(x)\rangle$$

(actually: $U_f |x, b\rangle = |x, b \oplus f(x)\rangle$).

**also**

$$U_f = \begin{array}{c}
\begin{array}{c}
\text{input}
\end{array}
\end{array} \quad \equiv \quad \begin{array}{c}
\begin{array}{c}
\text{output}
\end{array}
\end{array}$$

$O(\text{Poly}(T))$
Idea of the solution to MDJP:

We have

\[ \{ \begin{array}{ccc} x & \{ U_f \} & x \\ 0 & f(x) \end{array} \} \]

But

\[ U \left[ \frac{1}{\sqrt{2}} (1x, 0) + 1y, 0) \right] \]

= \[ \frac{1}{\sqrt{2}} \left( |x, f(x)\rangle + |y, f(y)\rangle \right) \]

So

\[ U \left( \frac{1}{\sqrt{2}} \sum_{i=0}^{2^n-1} |i, 0\rangle \right) = \frac{1}{\sqrt{2^n}} \sum_{i=0}^{2^n-1} |i, f(i)\rangle \]
Superposing a Register:

Let $S = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ then

$$10 > \xrightarrow{S} \frac{1}{\sqrt{2}} (10 > + 11 >)$$

Now, consider

$$\underbrace{\begin{pmatrix} S & S & \cdots & S \\ \vdots & \ddots & \ddots & \vdots \\ S & \cdots & S & \vdots \end{pmatrix}}_{n \text{ qubits}} 1y > = \bigotimes_n (\ldots)$$

$$= \frac{1}{\sqrt{2^n}} \sum_{i=0}^{2^n-1} |i\rangle$$

and $S_n = \bigotimes_n S$
Another Gate:

Let \( P = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \) then

\[
\alpha|0\rangle + \beta|1\rangle \xrightarrow{P} \alpha|0\rangle - \beta|1\rangle
\]
The Solution:

\[ 10^n, 0 \rangle \rightarrow \frac{1}{\sqrt{2^n}} \sum_{i=0}^{2^n-1} \left| i, f(i) \right\rangle \]

\[ \rightarrow \frac{1}{\sqrt{2^n}} \sum_{i=0}^{2^n-1} (-1)^{f(i)} \left| i, f(i) \right\rangle \]

\[ \rightarrow \frac{1}{\sqrt{2^n}} \sum_{i=0}^{2^n-1} (-1)^{f(i)} \left| i, 0 \right\rangle \]
Solution (cont.):

Let $|\phi\rangle = \frac{1}{\sqrt{2^n}} \sum_{i=0}^{2^n-1} |i, 0\rangle$

and consider the observable $\Theta = \{E_1, E_2\}$ where

$E_1 = \| 1\phi\rangle \|$ and $E_2 \perp E_1$

Claim: The gate array $+ \Theta$ solve the MODP.
Proof:

Final State: \( |\Psi\rangle = \frac{1}{\sqrt{2^n}} \sum_{i=0}^{2^n-1} (-1)^{f(i)} |i, 0\rangle \)

What is the proj. of \( |\Psi\rangle \) in \( E_i \)?

\[
\langle \chi | \Psi \rangle = \left( \frac{1}{\sqrt{2^n}} \sum_{j=0}^{2^n} \langle j, 0 | \right) \left( \frac{1}{\sqrt{2^n}} \sum_{i=0}^{2^n} (-1)^{f(i)} |i, 0 \rangle \right)
\]

\[
= \frac{1}{2^n} \sum_{i=0}^{2^n-1} (-1)^{f(i)}
\]

3 cases:

1) \( f \) balanced: \( \langle \chi | \Psi \rangle = 0 \)
   (always an "E_2" answer)

2) \( f \) constant: \( \langle \chi | \Psi \rangle = \pm 1 \)
   (always an "E_i" answer)

3) \( f \) not 1 or 2: \( \langle \chi | \Psi \rangle \in \mathbb{Z}, 1 \mathbb{Z} \)
   (either answer)
Improvement on the DJ problem:

\[ |y\rangle = \frac{1}{\sqrt{2^n}} \sum_{i=0}^{2^n-1} (-1)^{f(i)} |i, 0\rangle \]

Recall that \( S_n |w\rangle = \frac{1}{\sqrt{2^n}} \sum_{j=0}^{2^n-1} (-1)^{w \cdot j} |j\rangle \)

\[ S_0 \]

\[ S_n (|y\rangle) = \frac{1}{\sqrt{2^n}} \sum_{i=0}^{2^n-1} \sum_{j=0}^{2^n-1} (-1)^{f(i)} (-1)^{i \cdot j} |j\rangle \]

We now observe with the Standard basis.
Improvement (cont.):

Final State: \( \frac{1}{2^n} \sum_{j=0}^{2^n-1} \sum_{i=0}^{2^n-1} (-1)^j (-1)^i \prod_{l=0}^n 1_l 0_l \)

Consider the amplitude of \( 10^n 0 \) :

\[ \forall i \quad i \cdot c^n = 0 \quad \rightarrow \quad \frac{1}{2^n} \sum_{j=0}^{2^n-1} (-1)^j f(i) = a_0 \]

3 cases

1) \( f \) balanced: \( a_0 = 0 \) \( \rightarrow \) Never \( 10^n 0 \)

2) \( f \) constant: \( a_0 = \pm 1 \) \( \rightarrow \) always \( 10^n 0 \)

3) \( f \) other: \( a_0 \neq 0, \pm 1 \) \( \rightarrow \) maybe \( 10^n 0 \)

Same argument as before