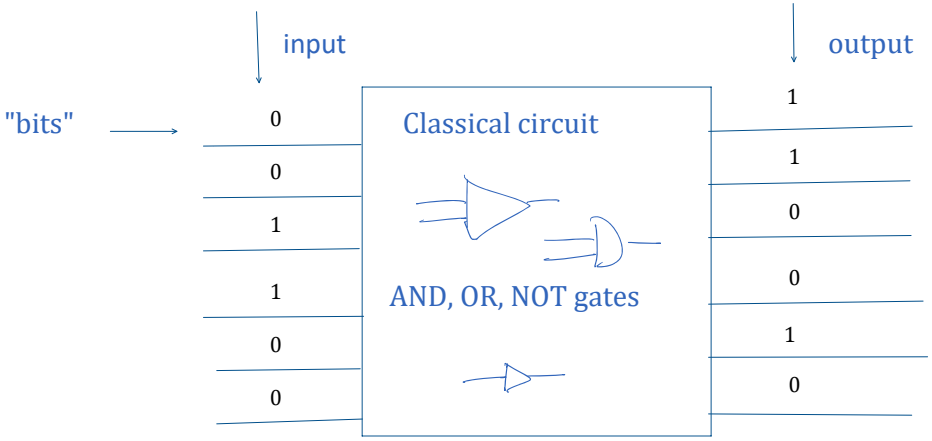
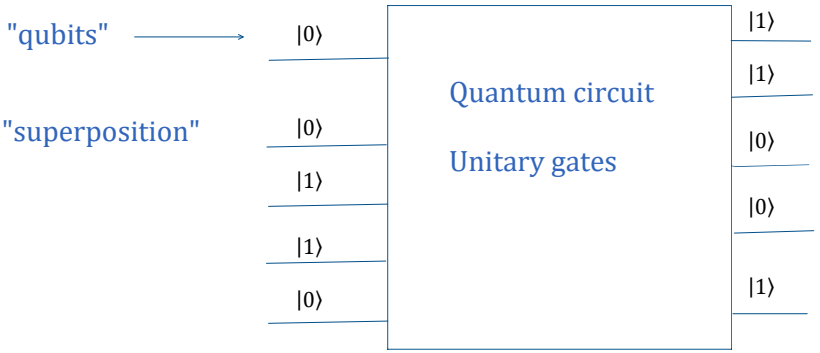
Lecture-1

Thursday, 14 January 2021 9:46 AM

Classical computation



Quantum computation



Classical-states

X-register

Pr(X=0) = 1/4 ; Pr(X=1) = 3/4

$v = \begin{pmatrix} \frac{1}{4} \\ 3 \end{pmatrix}$ Saw as 1 $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$

Operations

$NOT = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} b \\ a \end{pmatrix}$

$INIT_0 = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$

$IDENTITY = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} a \\ b \end{pmatrix}$

$INIT_1 = \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$

$v = \begin{pmatrix} \frac{1}{4} \\ \frac{3}{4} \end{pmatrix}$ Saw as 1 → $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$

Saw as 0 → $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$

$IDENTITY = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} a \\ b \end{pmatrix}$ $INIT_1 = \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$

$v = \begin{pmatrix} a \\ b \end{pmatrix}$; ℓ_1 norm is 1: $\|v\|_1 = |a| + |b| = 1$

Stochastic-matrix

1. All entries are non − negative
2. All columns add to 1

$A = \begin{pmatrix} a_{00} & a_{01} \\ a_{10} & a_{11} \end{pmatrix}$

$a_{ij} \geq 0$

$a_{00} + a_{10} = 1$

$a_{01} + a_{11} = 1$

3. ℓ_1 norm preserving: Let $Au = v$, then $\|u\|_1 = \|v\|_1$

$u = \begin{pmatrix} b_0 \\ b_1 \end{pmatrix}$

$v = \begin{pmatrix} a_{00} & a_{01} \\ a_{10} & a_{11} \end{pmatrix}\begin{pmatrix} b_0 \\ b_1 \end{pmatrix} = \begin{pmatrix} a_{00}b_0 + a_{01}b_1 \\ a_{10}b_0 + a_{11}b_1 \end{pmatrix}$

$(a_{00} + a_{10})b_0 + (a_{01} + a_{11})b_1 = b_0 + b_1$

Qubits $v = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$ $\alpha, \beta \in \mathbb{C}$ (the set of complex numbers)

ℓ_2 norm is 1: $\|v\|_2^2 = |\alpha|^2 + |\beta|^2 = 1$

$\alpha = a + ib$; $i = \sqrt{-1}$; $a, b \in \mathbb{R}$; $|\alpha| = \sqrt{a^2 + b^2}$

$\alpha^* = a - ib$

Examples $\begin{pmatrix} \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \end{pmatrix}$ $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ $\begin{pmatrix} \frac{3}{5} \\ \frac{4i}{5} \end{pmatrix}$

$\left|\frac{3}{5}\right|^2 + \left|\frac{4i}{5}\right|^2 = \left(\frac{3}{5}\right)^2 + \left(\frac{4}{5}\right)^2 = 1$

$\frac{3}{5} = \frac{3}{5} + i \cdot 0$ $\frac{4}{5}i = 0 + \frac{4}{5}i$

Unitary-Matrices

$Uv = w$ $v = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$

ℓ_2 norm a. k. a. Euclidean norm

$\|v\|_2 = \sqrt{|\alpha|^2 + |\beta|^2}$

1. ℓ_2 norm preserving: $\|v\|_2 = \|w\|_2$
2. Invertible: $U^\dagger U = UU^\dagger = I$
3. Orthonormal columns
4. Orthonormal rows

$U = \begin{pmatrix} u_{00} & u_{01} \\ u_{10} & u_{11} \end{pmatrix}$; $U^T = \begin{pmatrix} u_{00} & u_{10} \\ u_{01} & u_{11} \end{pmatrix}$

$U^* = \begin{pmatrix} u_{00}^* & u_{01}^* \\ u_{10}^* & u_{11}^* \end{pmatrix}$; $U^\dagger = \begin{pmatrix} u_{00}^* & u_{10}^* \\ u_{01}^* & u_{11}^* \end{pmatrix}$

$u_0 = \begin{pmatrix} u_{00} \\ u_{10} \end{pmatrix}$; $u_1 = \begin{pmatrix} u_{01} \\ u_{11} \end{pmatrix}$

Normal: $\|u_0\|_2 = \|u_1\|_2 = 1$

Orthogonal: $u_0^\dagger u_1 = 0$

U^{T} = "transpose"
U^* = "conjugate"
$U^\dagger$ = "conjugate-transpose"

Examples of unitary matrices

Inner-product

Hadamard Matrix

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

NOT Matrix

$$NOT = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

Identity Matrix

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

Rotation Matrix

$$R_\theta = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$$

$$v = \begin{pmatrix} v_0 \\ v_1 \end{pmatrix} \qquad w = \begin{pmatrix} w_0 \\ w_1 \end{pmatrix}$$

$$v^\dagger = (v_0^* \; v_1^*) \qquad w^\dagger = (w_0^* \; w_1^*)$$

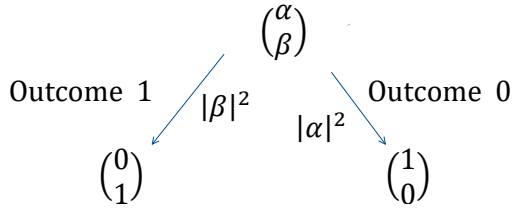
$$v^\dagger w = v_0^* w_0 + v_1^* w_1$$

$$w^\dagger v = w_0^* v_0 + w_1^* v_1$$

Lecture-2

Thursday, 21 January 2021 9:58 AM

Measurement



Ex:

$$v_0 = \begin{pmatrix}\frac{1}{\sqrt{2}}\\ \frac{1}{\sqrt{2}}\end{pmatrix} \qquad v_1 = \begin{pmatrix}\frac{1}{\sqrt{2}}\\ \frac{-1}{\sqrt{2}}\end{pmatrix}$$

$$Hv_0 = \begin{pmatrix}1\\0\end{pmatrix} \;;\; Hv_1 = \begin{pmatrix}0\\1\end{pmatrix}$$

Multiple bits

$$\begin{pmatrix}\frac{1}{8}\\ \frac{1}{2}\\ 0\\ \frac{3}{8}\end{pmatrix} \begin{matrix}\leftarrow 00\\ \leftarrow 01\\ \leftarrow 10\\ \leftarrow 11\end{matrix}$$

Stochastic -Matrix Example

$$\begin{pmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 1/2 & 1/2\\ 0 & 0 & 1/2 & 1/2\end{pmatrix}$$

Multiple-qubits

$$v = \begin{pmatrix}\frac{1}{\sqrt{2}}\\ 0\\ \frac{1}{2}\\ -\frac{1}{2}\end{pmatrix} \qquad \|v\|_2^2 = \frac{1}{2} + 0 + \frac{1}{4} + \frac{1}{4} = 1$$

Unitary

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

CNOT: "Controlled-Not"

Tensor product (a.k.a Kronecker product)

$$v = \begin{pmatrix}\frac{2}{3}\\ \frac{1}{3}\end{pmatrix}; \qquad w = \begin{pmatrix}\frac{1}{4}\\ \frac{3}{4}\end{pmatrix}$$

$$v \otimes w = \begin{pmatrix}\frac{2}{3}\times\frac{1}{4}\\ \frac{2}{3}\times\frac{3}{4}\\ \frac{1}{3}\times\frac{1}{4}\\ \frac{1}{3}\times\frac{3}{4}\end{pmatrix} = \begin{pmatrix}\frac{1}{6}\\ \frac{1}{2}\\ \frac{1}{12}\\ \frac{1}{4}\end{pmatrix}$$

$$A = \begin{pmatrix}a_{11} & a_{12}\\ a_{21} & a_{22}\end{pmatrix} \;;\; B = \begin{pmatrix}b_{11} & b_{12}\\ b_{21} & b_{22}\end{pmatrix}$$

$$A \otimes B = \begin{pmatrix}a_{11}B & a_{12}B\\ a_{21}B & a_{22}B\end{pmatrix} \;;\; B \otimes A = \begin{pmatrix}b_{11}A & b_{12}A\\ b_{21}A & b_{22}A\end{pmatrix}$$

$$a_{11}B = \begin{pmatrix}a_{11}b_{11} & a_{11}b_{12}\\ a_{11}b_{21} & a_{11}b_{22}\end{pmatrix}$$

Properties of tensor product

Properties of tensor product

1. Associative: $(A \otimes B) \otimes C = A \otimes (B \otimes C) = A \otimes B \otimes C$

2. $(A \otimes B)(C \otimes D) = (AC) \otimes (BD)$

3. Distributive over addition

$A \otimes (B + C) = A \otimes B + A \otimes C$
$(A + B) \otimes C = A \otimes C + B \otimes C$

4. "Scalars float freely": α = scalar = complex number
$(\alpha A) \otimes B = A \otimes (\alpha B) = \alpha(A \otimes B)$

Dirac notation (named after Paul Dirac)

$|0\rangle = \begin{pmatrix}1\\0\end{pmatrix}$: "ket-0"

$|1\rangle = \begin{pmatrix}0\\1\end{pmatrix}$: "ket-1"

} form a basis for $\mathbb{C}^2$

$$\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\0\end{pmatrix} + \frac{1}{\sqrt{2}}\begin{pmatrix}0\\1\end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix}$$

$$|00\rangle = |0\rangle|0\rangle = |0\rangle \otimes |0\rangle = \begin{pmatrix}1\\0\end{pmatrix} \otimes \begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}1\\0\\0\\0\end{pmatrix}$$

$$|01\rangle = |0\rangle|1\rangle = \begin{pmatrix}1\\0\end{pmatrix} \otimes \begin{pmatrix}0\\1\end{pmatrix} = \begin{pmatrix}0\\1\\0\\0\end{pmatrix}$$

Independent random variables XY

$w_1 = \begin{pmatrix}a\\b\end{pmatrix}$; $w_2 = \begin{pmatrix}c\\d\end{pmatrix}$;
$v = w_1 \otimes w_2$

Correlated random variables XY

$$v = \begin{pmatrix}1/2\\0\\0\\1/2\end{pmatrix} \stackrel{?}{=} \begin{pmatrix}ac\\ad\\bc\\bd\end{pmatrix}$$ ← Not possible

Entanglement

$$v = \begin{pmatrix}\frac{1}{\sqrt{2}}\\0\\0\\\frac{1}{\sqrt{2}}\end{pmatrix} \stackrel{?}{=} w_1 \otimes w_2$$ ← Not possible

Independent

$v = w_1 \otimes w_2$

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\1 & -1\end{pmatrix} \quad ; \quad I = \begin{pmatrix}1 & 0\\0 & 1\end{pmatrix}$$

$$H|0\rangle = H\begin{pmatrix}1\\0\end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\1 & -1\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix} = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$$

$$H|1\rangle = H\begin{pmatrix}0\\1\end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\1 & -1\end{pmatrix}\begin{pmatrix}0\\1\end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\-1\end{pmatrix} = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$$

$$I|0\rangle = I\begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}1 & 0\\0 & 1\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}1\\0\end{pmatrix} = |0\rangle$$

$$I|1\rangle = I\begin{pmatrix}0\\1\end{pmatrix} = \begin{pmatrix}1 & 0\\0 & 1\end{pmatrix}\begin{pmatrix}0\\1\end{pmatrix} = \begin{pmatrix}0\\1\end{pmatrix} = |1\rangle$$

$\forall|v\rangle : I|v\rangle = |v\rangle$

$$|01\rangle = |0\rangle|1\rangle = \begin{pmatrix}1\\0\end{pmatrix} \otimes \begin{pmatrix}0\\1\end{pmatrix} = \begin{pmatrix}0\\1\\0\\0\end{pmatrix}$$

$$|10\rangle = \begin{pmatrix}0\\0\\1\\0\end{pmatrix} \quad ; \quad |11\rangle = \begin{pmatrix}0\\0\\0\\1\end{pmatrix}$$

$$\frac{1}{\sqrt{2}}|000000\rangle + \frac{1}{\sqrt{2}}|111111\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\0\\\vdots\\\vdots\\0\\1\end{pmatrix} \begin{matrix}\leftarrow \text{0th location}\\ \\ \\ \\ \\ \leftarrow \text{63rd location}\end{matrix}$$

$\{|x\rangle \mid x \in \{0,1\}^n\}$ form a basis for $\mathbb{C}^{2^n}$

$$|\phi\rangle = \sum_{x\in\{0,1\}^n} \alpha_x|x\rangle \quad ; \quad \sum_{x\in\{0,1\}^n} |\alpha_x|^2 = 1 = \||\phi\rangle\|_2^2$$

$\forall|v\rangle : I|v\rangle = |v\rangle$

Let $|\psi\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$

$$\begin{aligned}
&(H \otimes I)|\psi\rangle \\
&= (H \otimes I)\frac{1}{\sqrt{2}}(|0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle) \\
&= \tfrac{1}{\sqrt{2}}((H \otimes I)\,(|0\rangle \otimes |0\rangle) + (H \otimes I)(|1\rangle \otimes |1\rangle)) \\
&= \frac{1}{\sqrt{2}}(H|0\rangle \otimes I|0\rangle + H|1\rangle \otimes I|1\rangle) \\
&= \frac{1}{2}((|0\rangle + |1\rangle) \otimes |0\rangle + (|0\rangle - |1\rangle) \otimes |1\rangle) \\
&= \frac{1}{2}(|00\rangle + |10\rangle + |01\rangle - |11\rangle) \\
&= \frac{1}{2}\begin{pmatrix}1\\1\\1\\-1\end{pmatrix}
\end{aligned}$$

Bra-ket notation

$|\phi\rangle$: ket-phi

bra-psi: $\langle\psi| = |\psi\rangle^\dagger$: ket-psi dagger

†: dagger = conjugate transpose

$\langle\psi|^\dagger = |\psi\rangle$; $\alpha^\dagger = \alpha^*$

$(A+B)^\dagger = A^\dagger + B^\dagger$; $(AB)^\dagger = B^\dagger A^\dagger$

$$|\theta\rangle = \sum_x \alpha_x|x\rangle$$

$$\langle\theta| = \left(\sum_x \alpha_x|x\rangle\right)^\dagger = \sum_x (\alpha_x|x\rangle)^\dagger = \sum_x \alpha_x^*\langle x|$$

$$|\psi\rangle = \begin{pmatrix}\alpha\\\beta\end{pmatrix} \quad ; \quad \langle\psi| = (\alpha^* \quad \beta^*)$$

$$|\phi\rangle = \begin{pmatrix}\gamma\\\delta\end{pmatrix}$$

$\langle\psi|\phi\rangle = \langle\psi||\phi\rangle$: "bra-ket" = "inner-product" = scalar

$$\langle\psi|\phi\rangle = (\alpha^* \quad \beta^*)\begin{pmatrix}\gamma\\\delta\end{pmatrix} = \alpha^*\gamma + \beta^*\delta$$

$|\phi\rangle\langle\psi|$: "ket-bra" = "outer-product" = matrix

$$|\phi\rangle\langle\psi| = \begin{pmatrix}\gamma\\\delta\end{pmatrix}(\alpha^* \quad \beta^*) = \begin{pmatrix}\gamma\alpha^* & \gamma\beta^*\\\delta\alpha^* & \delta\beta^*\end{pmatrix}$$

$$\langle\theta| = \left(\sum_x \alpha_x |x\rangle\right)^\dagger = \sum_x (\alpha_x |x\rangle)^\dagger = \sum_x \alpha_x^* \langle x|$$

$$|\psi\rangle\langle\psi| = \begin{pmatrix}\delta\\ \end{pmatrix}(\alpha^* \quad \beta^*) = \begin{pmatrix}\delta\alpha^* & \delta\beta^*\end{pmatrix}$$

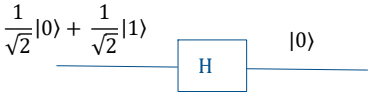
$$(|\psi\rangle\langle\phi|)|\gamma\rangle = (|\psi\rangle)\,(\langle\phi|\gamma\rangle) = (\langle\phi|\gamma\rangle)|\psi\rangle$$

Lecture-3

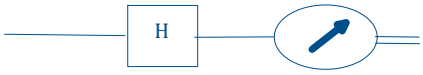
Thursday, 28 January 2021 9:52 AM

Quantum Circuits

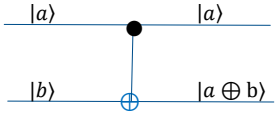
Hadamard-gate



Measurement

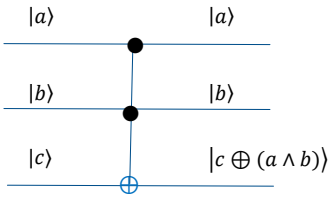


CNOT-gate



Input	Output
00	00
01	01
10	11
11	10

Controlled-controlled-NOT Toffoli-gate



Input	Output
101	101
111	110

$\oplus$: Parity a. k. a. XOR

$\wedge$: AND

$\vee$: OR

Linearity: $U(\alpha|v\rangle + \beta|w\rangle) = \alpha U|v\rangle + \beta U|w\rangle$

$$\alpha|01\rangle + \beta|11\rangle \xrightarrow{U} \alpha U|01\rangle + \beta U|11\rangle$$

$$\frac{1}{\sqrt{2}}|01\rangle + \frac{1}{\sqrt{2}}|11\rangle \xrightarrow{U} \frac{1}{\sqrt{2}}U|01\rangle + \frac{1}{\sqrt{2}}U|11\rangle$$

Rules for circuits

1. Time goes from left to right.
2. Horizontal lines represent qubits.
3. Gates and measurements are represented by various symbols.
4. Classical bits are represented by double-lines.

Partial-measurements

$$|\psi\rangle = \frac{1}{2}|00\rangle - \frac{i}{2}|10\rangle + \frac{1}{\sqrt{2}}|11\rangle$$
$$= |0\rangle\left(\frac{1}{2}|0\rangle\right) + |1\rangle\left(\frac{-i}{2}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\right)$$

$$|\psi\rangle = |0\rangle \otimes |\psi_0\rangle + |1\rangle \otimes |\psi_1\rangle$$

Measuring the first-qubit:

1. $\Pr(\text{outcome} = 0) = \||\psi_0\rangle\|_2^2 = \left\|\frac{1}{2}|0\rangle\right\|_2^2 = \frac{1}{4}$
2. $\Pr(\text{outcome} = 1) = \||\psi_1\rangle\|_2^2$
$= \left\|\frac{-i}{2}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\right\|_2^2 = \frac{3}{4}$

State of the second qubit on outcome 0:

$$\frac{|\psi_0\rangle}{\||\psi_0\rangle\|} = \frac{\frac{1}{2}|0\rangle}{\frac{1}{2}} = |0\rangle$$

State of the second qubit on outcome 1:

$$\frac{|\psi_1\rangle}{\||\psi_1\rangle\|} = \frac{\frac{-i}{2}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle}{\frac{\sqrt{3}}{2}} = \frac{-i}{\sqrt{3}}|0\rangle + \sqrt{\frac{2}{3}}|1\rangle$$

Measure the third-qubit:

$$|\psi\rangle = \frac{1}{2}|000\rangle + \frac{1}{2}|100\rangle + \frac{1}{2}|101\rangle - \frac{1}{2}|111\rangle$$
$$= \frac{1}{2}(|00\rangle + |10\rangle)|0\rangle + \frac{1}{2}(|10\rangle - |11\rangle)|1\rangle$$

Lecture-4

Thursday, 4 February 2021 9:41 AM

Deutsch's algorithm

Task

$f: \{0,1\} \to \{0,1\}$

Input	f_0	f_1	f_2	f_3
0	0	0	1	1
1	0	1	0	1

Determine if f is

1. a constant function (f_0, f_3) ?

   OR

2. a balanced function (f_1, f_2)?

1. We are allowed "black-box" queries to f
2. Two classical queries are necessary and sufficient.
3. One quantum query (in superposition) is necessary and sufficient.

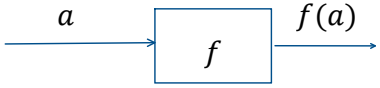
Alternate way of framing the task:

Input: $a_0 \in \{0,1\}, a_1 \in \{0,1\}$
in the database which can be queried

Task: Determine $a_0 \oplus a_1$?

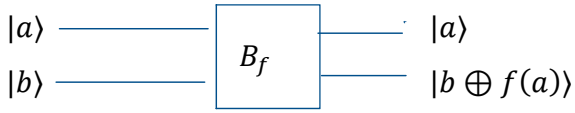
Black-box queries

$f: \{0,1\} \to \{0,1\}$



Not invertible, not unitary

B_f: $\forall a, b$: $|a\rangle|b\rangle = |a\rangle|b \oplus f(a)\rangle$



a, b	$a, b \oplus f(a)$
0, 0	$0, f(0)$
0, 1	$0, \overline{f(0)}$
1,0	$1, f(1)$
1, 1	$1, \overline{f(1)}$

1. Distinct inputs give distinct outputs.
2. Gate is invertible.
3. Gate matrix is a permutation matrix.
4. Permutation matrix is a unitary matrix.

Example of a permutation matrix.

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

in the database which can be queried

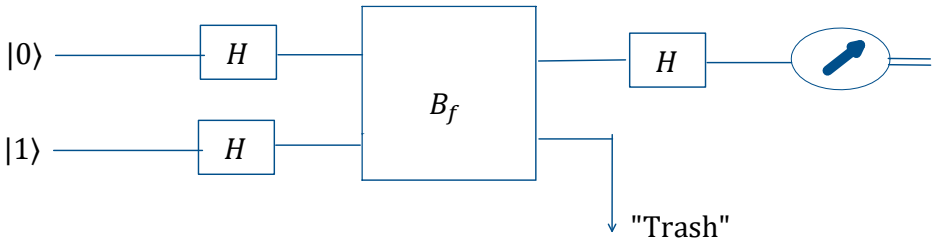
Task: Determine $a_0 \oplus a_1$?

Example of a permutation matrix.

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

Note: Every row and every column has a unique 1.

Circuit



Some formulae

$\forall a \in \{0,1\}: |a\rangle - |1 \oplus a\rangle = (-1)^a(|0\rangle - |1\rangle)$

$\forall a, b \in \{0,1\}: (-1)^a(-1)^b = (-1)^{a \oplus b}$

$\forall a \in \{0,1\}: \frac{1}{\sqrt{2}}(|0\rangle + (-1)^a|1\rangle) \xrightarrow{H} |a\rangle$

Analysis

$$H|0\rangle \otimes H|1\rangle$$
$$= \frac{1}{2}(|0\rangle + |1\rangle) \otimes (|0\rangle - |1\rangle)$$
$$= \frac{1}{2}(|00\rangle - |01\rangle + |10\rangle - |11\rangle)$$
$$\xrightarrow{B_f} \frac{1}{2}(|0\rangle|f(0)\rangle - |0\rangle|1 \oplus f(0)\rangle + |1\rangle|f(1)\rangle - |1\rangle|1 \oplus f(1)\rangle)$$
$$= \frac{1}{2}(|0\rangle(|f(0)\rangle - |1 \oplus f(0)\rangle) + |1\rangle(|f(1)\rangle - |1 \oplus f(1)\rangle))$$
$$= \frac{1}{2}\left((-1)^{f(0)}|0\rangle(|0\rangle - |1\rangle) + (-1)^{f(1)}|1\rangle(|0\rangle - |1\rangle)\right)$$
$$= \frac{1}{2}\left((-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle\right) \otimes (|0\rangle - |1\rangle) \longrightarrow$$ function has appeared in phase, this is referred to as "phase-kickback"
$$= \frac{1}{2}(-1)^{f(0)}\left(|0\rangle + (-1)^{f(0)\oplus f(1)}|1\rangle\right) \otimes (|0\rangle - |1\rangle)$$
$$\xrightarrow{H} \frac{1}{\sqrt{2}}(-1)^{f(0)}(|f(0) \oplus f(1)\rangle) \otimes (|0\rangle - |1\rangle)$$

desired output

Lecture-5

Thursday, 11 February 2021 9:51 AM

Deutsch-Jozsa algorithm

Task

$$f: \{0,1\}^n \to \{0,1\}$$

1. f is constant:

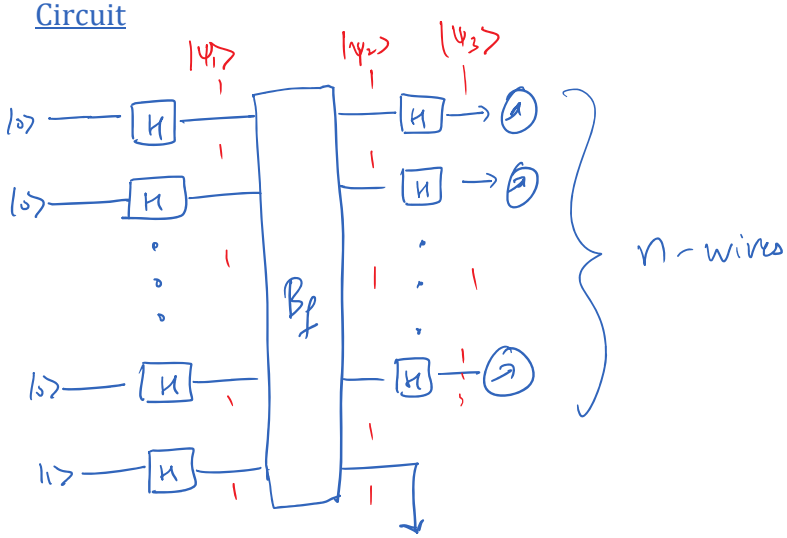
Either $|f^{-1}(0)| = 2^n$ OR $|f^{-1}(1)| = 2^n$

2. f is balanced

$|f^{-1}(0)| = |f^{-1}(1)| = 2^{n-1}$

Determine which is the case?

Circuit



Analysis

B_f: $\forall x \in \{0,1\}^n, \forall b \in \{0,1\}$:
$|x\rangle|b\rangle = |x\rangle|b \oplus f(x)\rangle$

Some formulae

$$H^{\otimes n}|x\rangle = \frac{1}{\sqrt{2^n}} \sum_{y \in \{0,1\}^n} (-1)^{x \cdot y} |y\rangle$$

$$x \cdot y = \sum_{i=1}^{n} x_i y_i \pmod 2$$

$\forall a \in \{0,1\}$: $|a\rangle - |1 \oplus a\rangle = (-1)^a(|0\rangle - |1\rangle)$

$$|\psi_1\rangle = (H^{\otimes n}|0^n\rangle) \otimes H|1\rangle$$

$$= \left(\frac{1}{\sqrt{2^n}} \sum_{x} |x\rangle\right) \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

$$|\psi_3\rangle = \frac{1}{\sqrt{2^n}} \sum_{y} (-1)^{f(y)} H^{\otimes n}|y\rangle$$

$$= \frac{1}{2^n} \sum_{y} (-1)^{f(y)} \left(\sum_{x} (-1)^{x \cdot y} |x\rangle\right)$$

$$= \frac{1}{2^n} \sum_{x} |x\rangle \left(\sum_{y} (-1)^{f(y) \oplus x \cdot y}\right)$$

$$\Pr(x = 0^n) = \frac{1}{2^{2n}} \left(\sum_{y} (-1)^{f(y)}\right)^2$$

$= 1$ if f is constant

$= 0$ if f is balanced

Measurement result of circuit

$$|\psi_1\rangle = (H^{\otimes n}|0^n\rangle) \otimes H|1\rangle$$
$$= \frac{1}{\sqrt{2^n}} \left(\sum_{y \in \{0,1\}^n} |y\rangle \right) \otimes \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle)$$

$$|\psi_2\rangle = \frac{1}{\sqrt{2^{n+1}}} \left(\sum_y |y\rangle |f(y)\rangle \; - \sum_y |y\rangle |1 \oplus f(y)\rangle \right)$$
$$= \frac{1}{\sqrt{2^{n+1}}} \sum_y |y\rangle \otimes (|f(y)\rangle - |1 \oplus f(y)\rangle)$$

$$= \frac{1}{\sqrt{2^n}} \left(\sum_y (-1)^{f(y)} |y\rangle \right) \otimes \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle)$$

phase kickback

Orthonormal set of vectors
$\{|v_i\rangle_{n\times 1} : i \in \{1, \dots, n\}\}$

$$U = \begin{pmatrix} \langle v_1| \\ \vdots \\ \langle v_n| \end{pmatrix} \quad ; \quad U|v_i\rangle = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{pmatrix} \leftarrow i-th$$

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

Measurement result of circuit
$= 000 \dots 0 = 0^n$

iff f is a constant function

1. If measurement result is 0^n, output = constant.
2. If measurement result is anything other than 0^n, output = balanced.

A simple search problem

Task

$$f: \{0,1\}^2 \to \{0,1\}$$

f_{00}

Input	Output
00	1
01	0
10	0
11	0

f_{01}

Input	Output
00	0
01	1
10	0
11	0

f_{10}

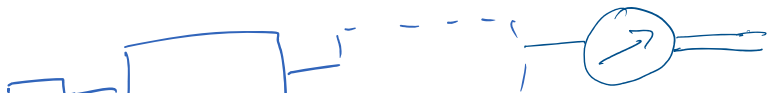
Input	Output
00	0
01	0
10	1
11	0

f_{11}

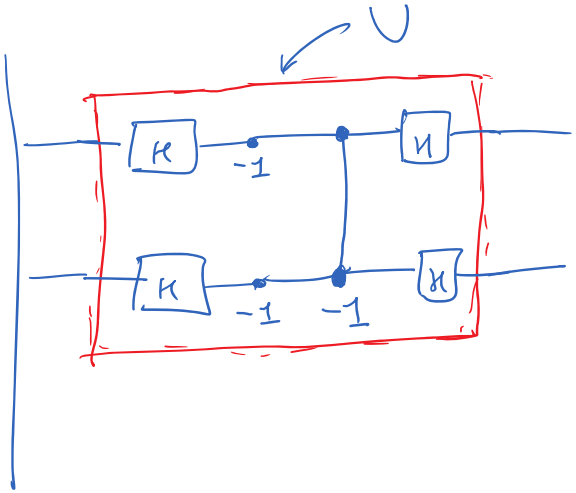
Input	Output
00	0
01	0
10	0
11	1

Determine which is the case?

Circuit



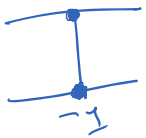
$$U = \begin{pmatrix} \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} & -\frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & -\frac{1}{2} \end{pmatrix}$$

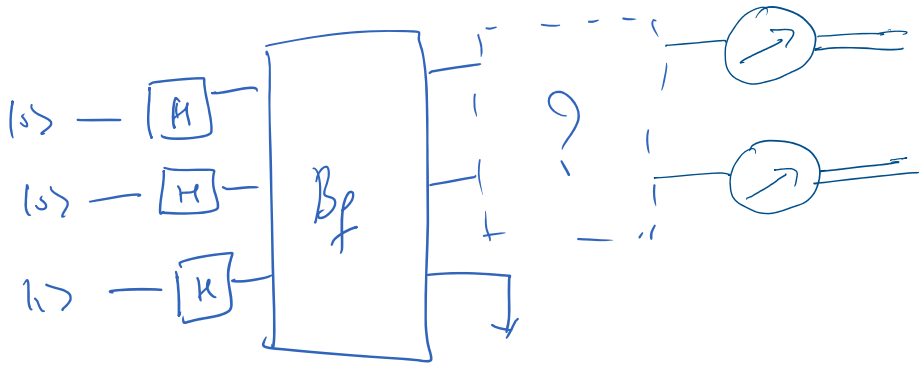


Phase-flip a.k.a. σ_z gate

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Controlled-phase-flip gate





Analysis

$$|0\rangle|0\rangle|1\rangle$$

$$\xrightarrow{H^{\otimes 3}} \frac{1}{\sqrt{2^3}}(|0\rangle + |1\rangle)(|0\rangle + |1\rangle)(|0\rangle - |1\rangle)$$

$$= \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

Ignore

$$\xrightarrow{B_f} \frac{1}{2}\left((-1)^{f_{00}}|00\rangle + (-1)^{f_{01}}|01\rangle + (-1)^{f_{10}}|10\rangle + (-1)^{f_{11}}|11\rangle\right) \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

$$f = f_{00} \Rightarrow |\phi_{00}\rangle = \frac{1}{2}(-|00\rangle + |01\rangle + |10\rangle + |11\rangle)$$

$$f = f_{01} \Rightarrow |\phi_{01}\rangle = \frac{1}{2}(|00\rangle - |01\rangle + |10\rangle + |11\rangle)$$

$$f = f_{10} \Rightarrow |\phi_{10}\rangle = \frac{1}{2}(|00\rangle + |01\rangle - |10\rangle + |11\rangle)$$

$$f = f_{11} \Rightarrow |\phi_{11}\rangle = \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle - |11\rangle)$$

Orthonormal

Lecture-6

Thursday, 18 February 2021 9:57 AM

Simon's Algorithm

Classical deterministic algorithms: $\frac{2^n}{2} = 2^{\Omega(n)}$

Classical randomized algorithms ("Birthday Paradox"): $\sqrt{2^n} = 2^{\frac{n}{2}} = 2^{\Omega(n)}$

Quantum algorithms: polynomial time $poly(n)$

Task $f: \{0,1\}^n \to \{0,1\}^n$

$\exists s \in \{0,1\}^n$:
$\forall x, y \in \{0,1\}^n$: $[f(x) = f(y)] \leftrightarrow [x \oplus y = s]$

Find s

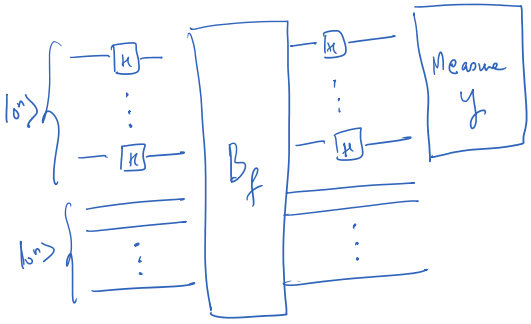
E.g.

x	$f(x)$
000	101
001	010
010	000
011	110
100	000
101	110
110	101
111	010

$s = 110$

$x \oplus y$
$= (x_1 \oplus y_1, \dots, x_n \oplus y_n)$

Circuit



$$\left\| \sum_z \alpha_z |z\rangle \right\|_2^2 = \sum_z |\alpha_z|^2$$

$$a \cdot b = \sum_{i=1}^{n} a_i b_i \pmod 2$$

Analysis B_f: $\forall x \in \{0,1\}^n, \forall y \in \{0,1\}^n$: $|x\rangle|y\rangle = |x\rangle|y \oplus f(x)\rangle$

$|0^n\rangle|0^n\rangle$

$$\xrightarrow{H^{\otimes n}} \frac{1}{2^{\frac{n}{2}}} \left(\sum_{x \in \{0,1\}^n} |x\rangle \right) \otimes |0^n\rangle$$

$$\xrightarrow{B_f} \frac{1}{2^{\frac{n}{2}}} \left(\sum_{x \in \{0,1\}^n} |x\rangle \right) \otimes |f(x)\rangle$$

$$\xrightarrow{H^{\otimes n}} \frac{1}{2^{\frac{n}{2}}} \left(\sum_{x \in \{0,1\}^n} H^{\otimes n} |x\rangle \right) \otimes |f(x)\rangle$$

$$= \frac{1}{2^n} \left(\sum_{x \in \{0,1\}^n} \sum_{y \in \{0,1\}^n} (-1)^{x \cdot y} |y\rangle \right) \otimes |f(x)\rangle$$

$$= \frac{1}{2^n} \left(\sum_{y \in \{0,1\}^n} |y\rangle \sum_{x \in \{0,1\}^n} (-1)^{x \cdot y} |f(x)\rangle \right)$$

$\mathcal{L}$:
$s \cdot y^1 = 0$
$s \cdot y^2 = 0$
$\vdots$
$s \cdot y^{n-1} = 0$

success $\stackrel{\Delta}{=} \{y^1, y^2, \dots, y^{n-1}\}$ are linearly independent

$\Pr(\text{success}) \geq \prod_{k=1}^{\infty} \left(1 - \frac{1}{2^k}\right) > \frac{1}{4}$

On success, solve for s from $\mathcal{L}$.

Repeat this process $4m$ times.

$\Pr(\text{fail each time}) \leq \left(1 - \frac{1}{4}\right)^{4m} < e^{-m}$

$m = O(1) =$ large constant

$\Pr(\text{output} = y)$

$$= \left\| \frac{1}{2^n} \sum_{x \in \{0,1\}^n} (-1)^{x \cdot y} |f(x)\rangle \right\|_2^2$$

$$= \left\| \frac{1}{2^n} \sum_{z \in \text{Range}(f)} \left((-1)^{x_z \cdot y} + (-1)^{x_z' \cdot y} \right) |z\rangle \right\|_2^2 \qquad (f(x_z) = f(x_z') = z)$$

$$= \left\| \frac{1}{2^n} \sum_{z} \left((-1)^{x_z \cdot y} + (-1)^{(x_z \oplus s) \cdot y} \right) |z\rangle \right\|_2^2 \qquad (x_z \oplus s = x_z')$$

$$= \left\| \frac{1}{2^n} \sum_{z} \left((-1)^{x_z \cdot y} + (-1)^{(x_z \cdot y) \oplus (s \cdot y)} \right) |z\rangle \right\|_2^2 \qquad ((a \oplus b) \cdot c = (a \cdot c) \oplus (b \cdot c))$$

$$= \begin{cases} 0 & : s \cdot y = 1 \\ \frac{1}{|T|} & : s \cdot y = 0 \end{cases}$$

$T = \{y \mid s \cdot y = 0\}$; $|T| = \begin{cases} 2^{n-1} & : s \neq 0^n \\ 2^n & : s = 0^n \end{cases}$

Lecture 7

Wednesday, 14 August 2024 1:54 PM

Arithmetic/Number-Theoretic problems

Integer addition

Input: $x, y \in \mathbb{Z}$ (the set of integers)
Output: $x + y$

Time complexity: $O(\lg x + \lg y)$

$$\lg(x) \triangleq \begin{cases} x & : \text{if } x = 0 \\ \lfloor \log_2 |x| \rfloor + 2 & : \text{if } x \neq 0 \end{cases}$$

```
  1 1 1
--------
  1 1 0 1
+ 0 1 1 1
--------
 1 0 1 0 0
--------
```

Integer multiplication

Input: $x, y \in \mathbb{Z}$

Output: $x \times y$

Time complexity: $O(\lg x \times \lg y)$

Schönhage-Strassen algorithm complexity: $O(n \log n \times \text{loglogn})$

$n = \lg x = \lg y$

Integer division

Input: $x, y \in \mathbb{Z}, y \neq 0$

Output: $a, b \in \mathbb{Z}$

$$x = ay + b \quad ; \quad 0 \leq b < |y|$$

a = quotient
b = remainder

Time complexity: $O(\lg x \times \lg y)$

Schönhage-Strassen algorithm complexity: $O(n \log n \times \text{loglogn})$

$n = \lg x = \lg y$

Greatest Common Divisor (GCD)

Input: $x, y \in \mathbb{Z}_+$ (the set of non − negative integers)

Output: $\gcd(x, y)$

Euclid's algorithm, 2000+ years old

Time complexity: $O(\lg x \times \lg y)$

Primality testing

Input: $N \in \mathbb{Z}_+$

Output: "prime" if N is a prime number, otherwise "not prime"

Classical randomized algorithms: $O((\lg N)^3)$

Classical deterministic algorithm:

Agrawal, Kayal, Saxena 2002: $O((\lg N)^6)$

Modular integer addition

Input: $N \in \mathbb{Z}_+$; $x, y \in \mathbb{Z}_N$

$$\mathbb{Z}_N = \{0, 1, \ldots, N-1\}$$

Output: $x + y \pmod N$

Time complexity: $O(\lg N)$

Modular integer multiplication

Input: $N \in \mathbb{Z}_+$; $x, y \in \mathbb{Z}_N$

Output: $x \times y \pmod N$

Time complexity: $O(\lg N \times \lg N)$

Integer factoring

Input: $N \in \mathbb{Z}_+$

Output: A prime factorization $N = p_1^{a_1} \ldots p_k^{a_k}$

Classical deterministic/randomized algorithms: $2^{O((\lg N)^{1/3} (\lg \lg N)^{2/3})}$

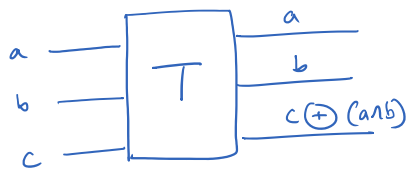
Shor's algorithm: $O((\lg N)^3)$

Lecture-8

Friday, February 4, 2022 6:31 PM

Reversible computation

Toffoli-gate (reversible gate)

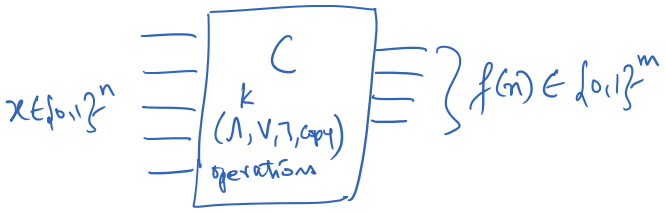


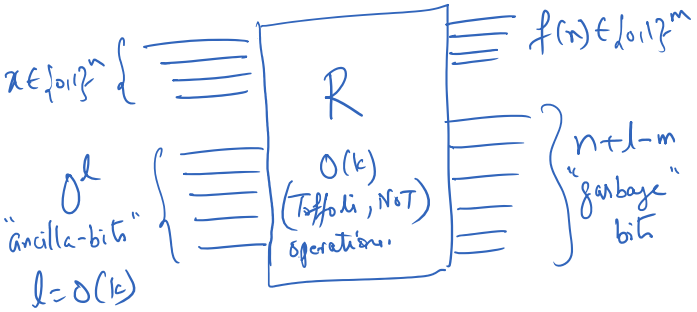
DeMorgan's Law

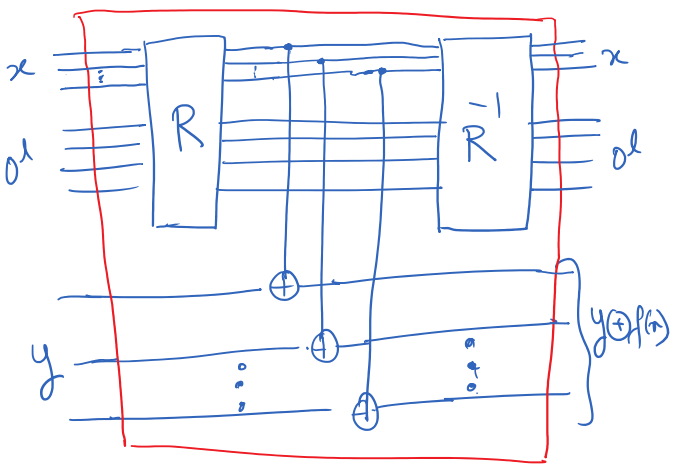
$a \vee b = \neg(\neg a \wedge \neg b)$

Using this can implement OR-gate in reversible way.

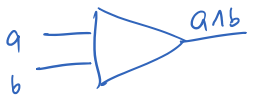
{OR, NOT, AND, Fan-out} is universal for classical computing.

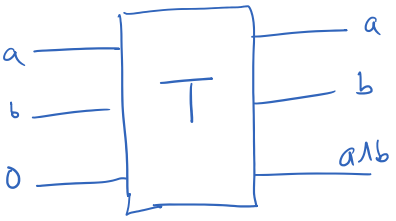






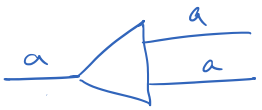
AND-gate

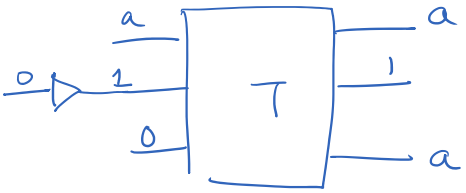




NOT-gate (reversible gate)

Fan-out (or copy)



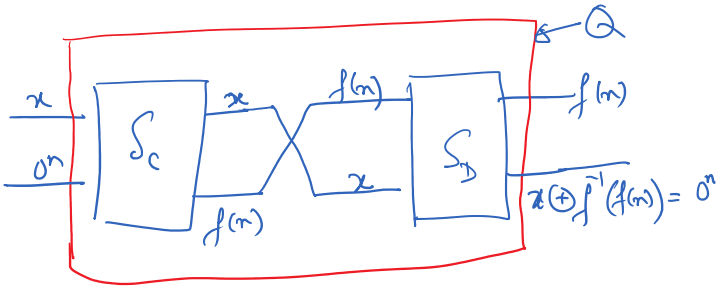


Invertible function $f: \{0,1\}^n \to \{0,1\}^n$ has circuit C

$S_C|x\rangle|y\rangle = |x\rangle|y \oplus f(x)\rangle$

$f^{-1}: \{0,1\}^n \to \{0,1\}^n$ has circuit D

$S_D|x\rangle|y\rangle = |x\rangle|y \oplus f^{-1}(x)\rangle$



$S_c|x\rangle|y\rangle|0^l\rangle = |x\rangle|y \oplus f(x)\rangle|0^l\rangle$

$S_c|x\rangle|y\rangle = |x\rangle|y \oplus f(x)\rangle$
(compactly written)

Note: CNOT is a reversible gate.

S_c: reversible circuit, unitary operation, permutation − matrix

$Q|x\rangle|0^n\rangle = |f(x)\rangle|0^n\rangle$

$Q|x\rangle = |f(x)\rangle$
(compactly written)

Lecture-9

Thursday, 15 August 2024 12:35 PM

Phase – estimation

Singular – value decomposition for any matrix A

$$A = \sum_j s_j |v_j\rangle\langle w_j|$$

s_j: singular values, non – negative real numbers

$\{|v_j\rangle\}_j$: left – singular vectors (orthonormal)

$\{|w_j\rangle\}_j$: right – singular vectors (orthonormal)

U – unitary, eigenvalue decompotion

$$U = \sum_j s_j |v_j\rangle\langle v_j|$$

s_j – eigenvalues

$|v_j\rangle$ – eigenvectors (orthonormal)

$\forall j: |s_j| = 1 \Leftrightarrow s_j = e^{2\pi i\, \theta_j}$

$i = \sqrt{-1}$; $\theta_j \in [0,1)$

$e^{i\theta} = \cos\theta + i \sin\theta$

$|e^{i\theta}| = \sqrt{\cos^2\theta + \sin^2\theta} = 1$

$\forall \theta \in \mathbb{R}$:

$\cos(2\pi + \theta) = \cos\theta$

$\sin(2\pi + \theta) = \sin\theta$

$\forall j : U|v_j\rangle = e^{2\pi i \theta_j}|v_j\rangle = s_j|v_j\rangle$

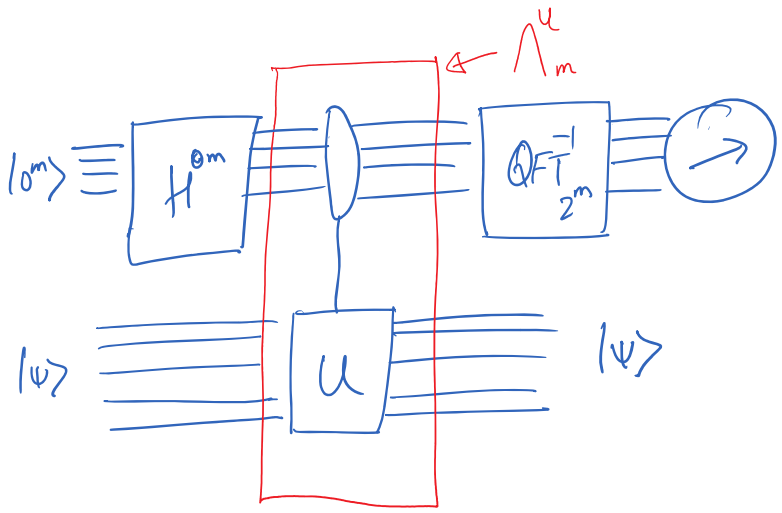
Phase – estimation problem

Input: A quantum circuit Q that performs unitary operation U, along with a quantum state $|\psi\rangle$
that is promised to be an eigenvector of U.

$U|\psi\rangle = e^{2\pi i\, \theta}|\psi\rangle$

Output: An approximation of $\theta \in (0,1]$

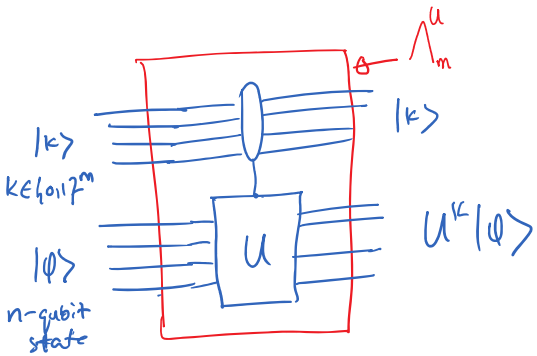
Circuit



Unitary matrix Λ^U_m

$\Lambda^U_m(|k\rangle \otimes |\phi\rangle) \rightarrow |k\rangle \otimes U^k|\phi\rangle$

$k \in \{0,1,\ldots,2^m - 1\}$



QFT: Quantum Fourier Transform

$$QFT_M = \frac{1}{\sqrt{M}} \begin{pmatrix} 1 & 1 & \cdots & 1 \\ 1 & \omega_M & \cdots & \omega_M^{M-1} \\ 1 & \omega_M^2 & \cdots & \omega_M^{2(M-1)} \\ \vdots & \vdots & \vdots & \vdots \\ 1 & \omega_M^{M-1} & \cdots & \omega_M^{(M-1)^2} \end{pmatrix}$$

$$QFT_M^\dagger = \frac{1}{\sqrt{M}} \begin{pmatrix} 1 & 1 & \cdots & 1 \\ 1 & \omega_M^{-1} & \cdots & \omega_M^{-(M-1)} \\ 1 & \omega_M^{-2} & \cdots & \omega_M^{-2(M-1)} \\ \vdots & \vdots & \vdots & \vdots \\ 1 & \omega_M^{-(M-1)} & \cdots & \omega_M^{-(M-1)^2} \end{pmatrix}$$

$\forall j$:

$QFT_M \ |j\rangle \to |\phi_j\rangle$

$QFT_M^\dagger \ |\phi_j\rangle \to |j\rangle$

$QFT_M^\dagger \ |k\rangle \to \frac{1}{\sqrt{M}} \sum_{j=0}^{M-1} \omega_M^{-kj} \ |j\rangle$

Analysis

Let $M = 2^m$.

$|0^m\rangle|\psi\rangle$

$$\xrightarrow{H^{\otimes m}} \left(\frac{1}{\sqrt{M}} \sum_{k=0}^{M-1} |k\rangle \right) |\psi\rangle$$

$$\xrightarrow{\Lambda_m^U} \left(\frac{1}{\sqrt{M}} \sum_{k=0}^{M-1} |k\rangle \right) U^k|\psi\rangle$$

$$= \left(\frac{1}{\sqrt{M}} \sum_{k=0}^{M-1} e^{2\pi i \, k\theta} \ |k\rangle \right) |\psi\rangle \longrightarrow \text{phase-kickback}$$

$U|\psi\rangle = e^{2\pi i \, \theta}|\psi\rangle$

$U^k|\psi\rangle = \left(e^{2\pi i \, \theta}\right)^k|\psi\rangle$

$= e^{2\pi i \, k\theta}|\psi\rangle$

Assume for simplicity:

$\theta = \frac{j}{M}$ for some $j \in \{0,1,\dots,M-1\}$.

Let $\omega_M = e^{\frac{2\pi i}{M}}$. Let,

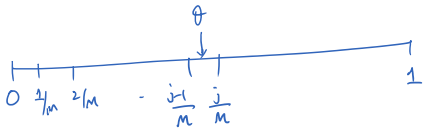
$$|\phi_j\rangle = \frac{1}{\sqrt{M}} \sum_{k=0}^{M-1} e^{2\pi i \frac{kj}{M}} \ |k\rangle = \frac{1}{\sqrt{M}} \sum_{k=0}^{M-1} \omega_M^{kj} \ |k\rangle$$

$\left\{ |\phi_j\rangle : j \in \{0,1,\dots,M-1\} \right\}$: orthonomal

Lecture-10

Thursday, 18 March 2021 9:41 AM

Phase-estimation



Let us recall that the state produced before $QFT^\dagger$ is applied is (below $\omega = e^{2\pi i}$)

$$\frac{1}{\sqrt{M}}\left(\sum_{k=0}^{M-1}\omega^{k\theta}|k\rangle\right)|\psi\rangle$$

Also recall,

$$QFT^\dagger|k\rangle = \frac{1}{\sqrt{M}}\sum_{j=0}^{M-1}\omega_M^{-kj}\,|j\rangle = \frac{1}{\sqrt{M}}\sum_{j=0}^{M-1}\omega^{\frac{-kj}{M}}\,|j\rangle$$

Hence the state before measurement is (ignoring $|\psi\rangle$)

$$\frac{1}{M}\sum_{j=0}^{M-1}\left(\sum_{k=0}^{M-1}\omega^{k\left(\theta-\frac{j}{M}\right)}\right)|j\rangle$$

Let p_j be the probability of obtaining j on measuring.

$$p_j = \left|\frac{1}{M}\sum_{k=0}^{M-1}\omega^{k\left(\theta-\frac{j}{M}\right)}\right|^2$$

$$= \frac{1}{M^2}\left|\frac{\omega^{(M\theta-j)}-1}{\omega^{\left(\theta-\frac{j}{M}\right)}-1}\right|^2 \qquad \left(\sum_{k=0}^{M-1}x^k = \frac{x^M-1}{x-1}\right)$$

$$= \frac{1}{M^2}\left|\frac{\omega^{M|\epsilon|}-1}{\omega^{|\epsilon|}-1}\right|^2 \qquad \left(\theta = \frac{j}{M}+\epsilon\,;|\epsilon| \le \frac{1}{2M}\right)$$

$$= \frac{1}{M^2}\frac{a^2}{b^2} \qquad \left(a = |\omega^{M|\epsilon|}-1|;\ b = |\omega^{|\epsilon|}-1|\right)$$

$$\geq \frac{1}{M^2}\left(\frac{4|\epsilon|M}{2\pi|\epsilon|}\right)^2 = \frac{4}{\pi^2} > \frac{1}{4}$$

$$\frac{2\pi|\epsilon|M}{a} \le \frac{\pi}{2}$$

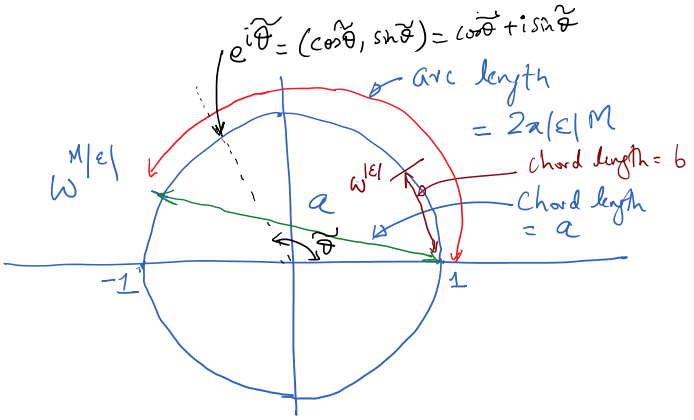
$$\Rightarrow a \geq 4\,|\epsilon|M$$

$$\frac{2\pi|\epsilon|}{b} \geq 1$$

$$\Rightarrow b \leq 2\pi\,|\epsilon|$$

Recall: $e^{i\tilde{\theta}} = \cos\tilde{\theta} + i\sin\tilde{\theta}$

$$1 \le \frac{\text{arc}-\text{length}}{\text{chord}-\text{length}} \le \frac{\pi}{2}$$

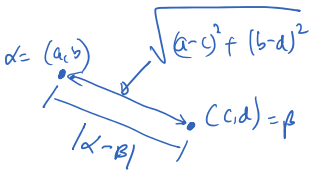


Let $\theta = \frac{l}{M} + \epsilon;\ \ \frac{l-j}{M} < |\epsilon| < \frac{1}{2}$;

$$p_l = \frac{1}{M^2}\frac{a^2}{b^2} \le \left(\frac{2}{M4|\epsilon|}\right)^2 \le \frac{1}{4|l-j|^2}$$

$$a \le 2$$

$$\frac{2\pi|\epsilon|}{b} \le \frac{\pi}{2}$$
$$\Rightarrow b \geq 4|\epsilon|$$



$$\alpha = (a,b) = a + ib\,;$$
$$\beta = (c,d) = c + id$$

$$|\alpha-\beta|^2$$
$$= |a + ib - (c + id)|^2$$
$$= |a - c + i(b-d)|^2$$
$$= (a-c)^2 + (b-d)^2$$

Lecture-11

Thursday, 25 March 2021 9:42 AM

Order finding

$N \geq 1$ is an integer ; $\mathbb{Z}_N = \{0,1, \ldots, N-1\}$

$\mathbb{Z}_N^* = \{a \in \mathbb{Z}_N \mid \gcd(a, N) = 1\}$

gcd = greatest common divisor

Euler ϕ − function
$\phi(N) = |\mathbb{Z}_N^*|$ = no of elements in $\mathbb{Z}_N^*$

$\mathbb{Z}_N^*$ forms a "group" under multiplication

1. $a, b \in \mathbb{Z}_N^* \Rightarrow a \cdot b \pmod N \in \mathbb{Z}_N^*$

2. $\forall a \in \mathbb{Z}_N^*$ there exists unique $b \in \mathbb{Z}_N^*$ such that $a \cdot b = 1 \pmod N$

b is multiplicative − inverse of a, denoted $b = a^{-1}$

Order of $a \in \mathbb{Z}_N^*$:
Smallest r such that $a^r = 1 \pmod N$

Euler's Theorem:
$a^{\phi(N)} = 1 \pmod N$

Order of a is a divisor of $\phi(N)$

E. g. $a = 4, N = 35, a \in \mathbb{Z}_N^*$ (all values are mod N)

$4^1 = 4, 4^2 = 16, 4^3 = 29, 4^4 = 11, 4^5 = 9, 4^6 = 1.$

Order finding problem

Input: $N \geq 2, a \in \mathbb{Z}_N^*$
Output: Order of $a \in \mathbb{Z}_N^*$

Order finding via phase-estimation

Let $N \leq 2^n$. Let unitary matrix M_a:

$\forall x \in \mathbb{Z}_N \subseteq \{0,1\}^n$: $M_a|x\rangle = |a \cdot x\rangle$
$\forall x \in \{0,1\}^n - \mathbb{Z}_N$: $M_a|x\rangle = |x\rangle$

Let unitary matrix $M_{a^{-1}}$:

$\forall x \in \mathbb{Z}_N : M_{a^{-1}}|x\rangle = |a^{-1}x\rangle$
$\forall x \in \{0,1\}^n - \mathbb{Z}_N : M_{a^{-1}}|x\rangle = |x\rangle$

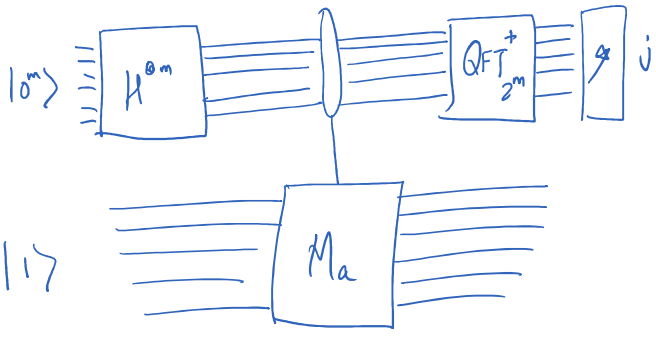
$\Rightarrow \forall x \in \{0,1\}^n : M_a M_{a^{-1}}|x\rangle = |x\rangle$
$\Rightarrow M_a\, M_{a^{-1}} = M_{a^{-1}} M_a = I$

There exists reversible cirucit for functions

$f(x) = a \cdot x$
$g(x) = a^{-1} \cdot x$

From what we have seen in previous lectures, there are reversible circuits for M_a and $M_{a^{-1}}$

Circuit



Analysis

$\Lambda_m(M_a)|k\rangle|x\rangle = |k\rangle|a^k x\rangle = |k\rangle M_a^k|x\rangle$

$O(mn^2)$ time to implement Λ

$$|1\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} |\psi_k\rangle$$

From the phase − estimation algorithm we will get $\frac{j}{2^m} \sim \frac{k}{r}$ for random $k \in [0, r-1]$

Continued-fraction algorithm (CF)

Fact: Given a real number $\alpha \in \{0,1\}, N \geq 2$, there is at most one fraction $\frac{x}{y}$ with $0 \leq x, y \leq N; y \neq 0; \gcd(x, y) = 1$ and

$$\left|\alpha - \frac{x}{y}\right| < \frac{1}{2N^2}.$$

$\Lambda_m(M_a)|k\rangle|x\rangle = |k\rangle|a^k x\rangle = |k\rangle M_a^k|x\rangle$

$O(mn^2)$ time to implement Λ_m.

What are the eigenvectors and eigenvalues of M_a?
Let r be the order of $a \in \mathbb{Z}_N^*$. Let

$$|\psi_j\rangle = \frac{1}{\sqrt{r}}(|1\rangle + \omega_r^{-j}|a\rangle + \cdots + \omega_r^{-j(r-1)}|a^{r-1}\rangle)$$

$\omega_r = e^{\frac{2\pi i}{r}}$; $\omega_r^r = 1$.

$$M_a|\psi_j\rangle$$
$$= \frac{1}{\sqrt{r}}(|a\rangle + \omega_r^{-j}|a^2\rangle + \cdots + \omega_r^{-j(r-1)}|1\rangle)$$
$$= \frac{\omega_r^j}{\sqrt{r}}(\omega_r^{-j}|a\rangle + \omega_r^{-2j}|a^2\rangle + \cdots + \omega_r^{-jr}|1\rangle)$$
$$= \omega_r^j|\psi_j\rangle.$$

$\forall k \in \{0, \ldots, r-1\}$:
$|\psi_k\rangle$ is eigenvector of M_a with eigenvalue ω_r^k.

$$\left|\alpha - \frac{x}{y}\right| < \frac{1}{2N^2}.$$

Given (α, N) algorithm CF will find (x, y) in $O\left((\lg N)^3\right)$ time.

Let $N = 2^n; m = 2n$. Then,

$$\left|\frac{j}{2^m} - \frac{k}{r}\right| < \frac{1}{2N^2} = \frac{1}{2^{m+1}}.$$

Run algorithm A on input $\left(\frac{j}{2^m}, N\right)$ to get $\frac{k}{r}$ in the lowest form for random $k \in [0, r-1]$.

$\frac{x}{y} = \frac{k}{r} \Rightarrow y$ divides r

Run the entire procedure several times to get $y_1, y_2, \ldots, y_l$ and take LCM$(y_1, y_2, \ldots, y_l)$.

With very high probability LCM$(y_1, y_2, \ldots, y_l) = r$.

LCM = "least common multiple"

Order finding to Factoring

Input: an odd, composite integer N that is not a prime power.

Repeat

  Randomly choose $a \in \{2, \ldots, N-1\}$.

  Compute $d = \gcd(a, N)$.

  If $d \geq 2$ then /* We've been incredibly lucky. */

    Return $u = d$ and $v = N/d$.

  Else /* Now we know $a \in \mathbb{Z}_N^*$. */

    Let r be the order of a in $\mathbb{Z}_N^*$. /* Requires the order finding algorithm. */

    If r is even then

      Compute $x = a^{r/2} - 1 \pmod{N}$.

      Compute $d = \gcd(x, N)$.

      If $d \geq 2$ then

        Return $u = d$ and $v = N/d$. /* Answer is found. */

Until answer is found (or you get tired).

Figure 2: Reduction of factoring to order finding

Suppose that the random choice of a is in $\mathbb{Z}_N^*$ (which is very likely), and that the order r of a is even. Then

$$a^r \equiv 1 \pmod{N}$$

so

$$N \mid a^r - 1.$$

Because $a^r - 1 = (a^{r/2} + 1)(a^{r/2} - 1)$ we have

$$N \mid (a^{r/2} + 1)(a^{r/2} - 1).$$

It cannot happen that $N \mid (a^{r/2} - 1)$, because this would mean that r was not the order of a after all. If we are lucky and it is not the case that $N \mid (a^{r/2} + 1)$, then we know the algorithm will work. This is because the factors of N are then necessarily split between $(a^{r/2} + 1)$ and $(a^{r/2} - 1)$, so computing $\gcd(a^{r/2} - 1, N)$ will reveal a nontrivial factor of N.

Each iteration of the loop therefore fails to give an answer if either r is odd or r is even but N divides $a^{r/2} + 1$. The probability that neither of these events occur is at least $1/2$. (In fact, it is at least $1 - 2^{m-1}$ for m the number of distinct primes dividing N. This is why the assumption that N is not a prime power was important. Also, the analysis of this fact requires that N is odd.)

Lecture 12

23 March 2023 08:48

Quantum Fourier Transform Circuit

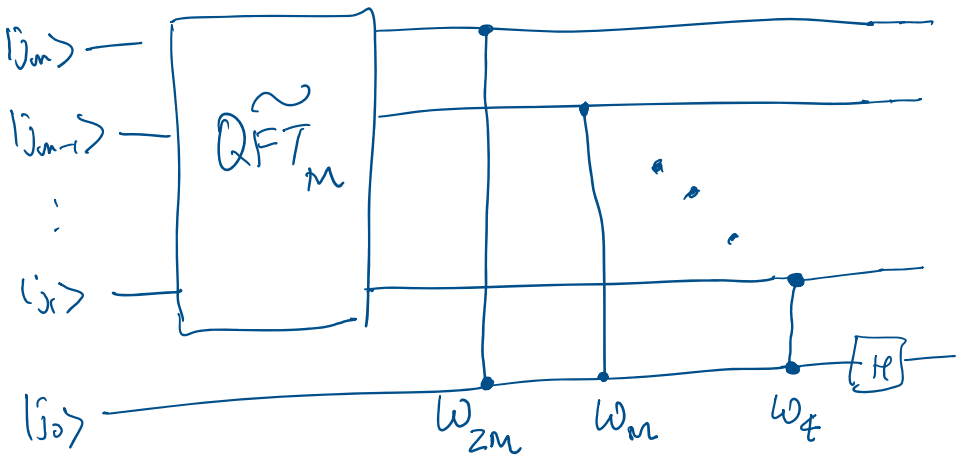
$M = 2^m$;

$$QFT_M|j\rangle = \frac{1}{\sqrt{M}} \sum_{k=0}^{M-1} \omega_M^{jk} |k\rangle$$

$$\widetilde{QFT_M}|j_{m-1}j_{m-2}\dots j_0\rangle = \frac{1}{\sqrt{M}} \sum_{k=0}^{M-1} \omega_M^{jk} |k_0 k_1 \dots k_{m-1}\rangle$$

$$QFT_2|j\rangle = \widetilde{QFT_2}|j\rangle$$
$$= \frac{1}{\sqrt{2}} \sum_{k=0}^{1} \omega_2^{jk}|k\rangle = \frac{1}{\sqrt{2}}(|0\rangle + (-1)^j|1\rangle) = H|j\rangle$$

For general $m \geq 2$:



$$H|j\rangle = \frac{1}{\sqrt{2}} \sum_{k=0}^{1} (-1)^{jk}|k\rangle$$

$e^{\pi i} = \cos\pi + i\sin\pi = -1$
$\omega = e^{2\pi i}$
$\omega_2 = e^{\frac{2\pi i}{2}} = e^{\pi i} = -1$
$\omega_N = e^{\frac{2\pi i}{N}}$
$\omega_{rN}^r = e^{\frac{2\pi i r}{Nr}} = \omega_N$
$\omega_2 = \omega_{2^{m+1}}^{2^m}$

$j = j_m j_{m-1} \dots j_0$
$= j_0 + 2j_1 + 4j_2 + \dots + 2^m j_m$

$2j'k' + j_0k'_0 + j_0(2k'_1) + \dots + j_0(2^{m-1}k'_{m-1})$
$= 2j'k' + j_0(k'_0 + 2k'_1 + \dots + 2^{m-1}k'_{m-1})$
$= 2j'k' + j_0k'$
$= (2j' + j_0)k'$
$= jk'$

$(-1)^j = (-1)^{j_0}$

$(-1)^{k_m j_0}\omega_{2M}^{jk'} = (-1)^{k_m j}\omega_{2M}^{jk'} = \omega_2^{k_m j}\omega_{2M}^{jk'}$
$= \omega_{2M}^{k_m j 2^m}\omega_{2M}^{jk'} = \omega_{2M}^{j(k'+2^m k_m)}$
$= \omega_{2M}^{jk}$

Circuit size

$g(1) = 1$
$g(m+1) = g(m) + (m+1)$
$g(m) = \sum_{j=1}^{m} j = \binom{m+1}{2} = O(m^2)$

Want to show:

$$\widetilde{QFT_{2M}}|j_m j_{m-1} \dots j_0\rangle = \frac{1}{\sqrt{2M}} \sum_{k=0}^{2M-1} \omega_{2M}^{jk} |k_0 k_1 \dots k_m\rangle$$

Let

$j' = j_m j_{m-1} \dots j_1 = \left\lfloor \frac{j}{2} \right\rfloor$
$k' = k_{m-1} k_{m-2} \dots k_0 = k - k_m 2^m$

Therefore $|j\rangle = |j'\rangle|j_0\rangle$
$\Rightarrow j = 2j' + j_0.$

After $\widetilde{QFT_M}$, the state is

$$\frac{1}{\sqrt{M}} \left(\sum_{k'=0}^{M-1} \omega_M^{j'k'} |k'_0 k'_1 \dots k'_{m-1}\rangle \right) |j_0\rangle$$

$= \omega_{2M}^{jk}$

After all controlled phase-shifts:

$$\frac{1}{\sqrt{M}} \sum_{k'=0}^{M-1} \omega_M^{j'k'} \omega_{2M}^{j_0 k'_0} \omega_M^{j_0 k'_1} \dots \omega_4^{j_0 k'_{m-1}} |k'_0 \dots k'_{m-1}\rangle |j_0\rangle$$

$$= \frac{1}{\sqrt{M}} \sum_{k'=0}^{M-1} \omega_{2M}^{2j'k' + j_0(k'_0 + 2k'_1 + \dots + 2^{m-1} k'_{m-1})} |k'_0 \dots k'_{m-1}\rangle |j_0\rangle$$

$$= \frac{1}{\sqrt{M}} \sum_{k'=0}^{M-1} \omega_{2M}^{jk'} |k'_0 \dots k'_{m-1}\rangle |j_0\rangle$$

After the Hadamard transform:

$$\frac{1}{\sqrt{2M}} \sum_{k'=0}^{M-1} \sum_{k_m=0}^{1} (-1)^{k_m j_0} \omega_{2M}^{jk'} |k'_0 \dots k'_{m-1}\rangle |k_m\rangle$$

$$= \frac{1}{\sqrt{2M}} \sum_{k'=0}^{M-1} \sum_{k_m=0}^{1} \omega_{2M}^{jk} |k'_0 \dots k'_{m-1}\rangle |k_m\rangle$$

$$= \frac{1}{\sqrt{2M}} \sum_{k=0}^{2M-1} \omega_{2M}^{jk} |k_0 k_1 \dots k_m\rangle$$

Lecture 13

Grover's Algorithm

Task

$f: \{0,1\}^n \to \{0,1\}$

Find $x \in \{0,1\}^n$ such that $f(x) = 1$

Algorithm

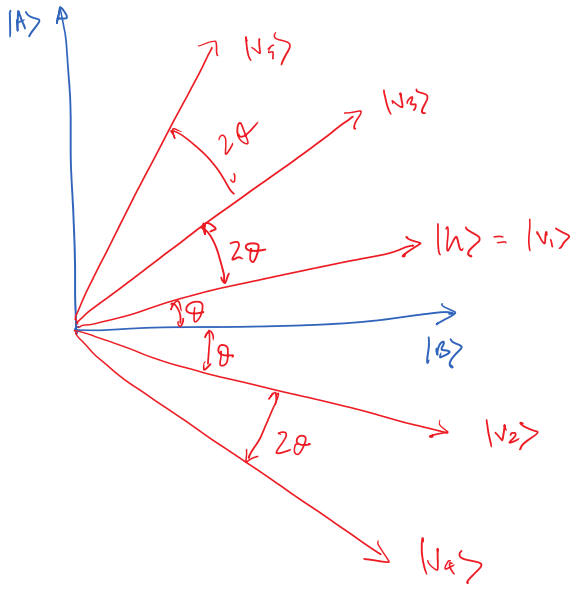
$A = \{x \in \{0,1\}^n \mid f(x) = 1\}$
$a = |A|$
$|A\rangle = \frac{1}{\sqrt{a}} \sum_{x \in A} |x\rangle$

$B = \{x \in \{0,1\}^n \mid f(x) = 0\}$
$b = |B|$
$|B\rangle = \frac{1}{\sqrt{b}} \sum_{x \in B} |x\rangle$

$N = 2^n$
$H^{\otimes n} |0^n\rangle = |h\rangle = \frac{1}{\sqrt{N}} \sum_{x \in \{0,1\}^n} |x\rangle$

1. Start with $|h\rangle$.
2. Alternately reflect about $|B\rangle$ and $|h\rangle$.
3. After k iterations angle of $|v_{2k+1}\rangle$ with $|B\rangle$ becomes $(2k+1)\theta$.

Pictorial representation of the algorithm



Analysis

We need $(2k+1)\theta \sim \frac{\pi}{2}$

$\cos\theta = |\langle B|h\rangle|$

For small $\theta \sim \sin\theta = \cos\left(\frac{\pi}{2} - \theta\right) = |\langle A|h\rangle| = a\sqrt{\frac{1}{aN}} = \sqrt{\frac{a}{N}}$

$k = \left\lfloor \frac{1}{2}\left(\frac{\pi}{2\theta} - 1\right) \right\rfloor$

$k = O\left(\frac{1}{\theta}\right) = O\left(\sqrt{\frac{N}{a}}\right)$

Reflection about $|u\rangle$

$|v\rangle = \alpha|u\rangle + \beta|u^\perp\rangle$

$|u^\perp\rangle$: orthogonal to $|u\rangle$

$R_u|v\rangle = \alpha|u\rangle - \beta|u^\perp\rangle$

$R_u = 2|u\rangle\langle u| - I$

$R_u|u\rangle = (2|u\rangle\langle u| - I)|u\rangle = 2|u\rangle - |u\rangle = |u\rangle$

$R_u|u^\perp\rangle = (2|u\rangle\langle u| - I)|u^\perp\rangle = -|u^\perp\rangle$

Reflection about $|0^n\rangle$

$|v\rangle = \alpha_0|0^n\rangle + \sum_{x \neq 0^n} \alpha_x|x\rangle$

$|w\rangle = \alpha_0|0^n\rangle - \sum_{x \neq 0^n} \alpha_x|x\rangle$

Reflection about $|h\rangle$

$R_h = 2|h\rangle\langle h| - I$

$R_0 = 2|0^n\rangle\langle 0^n| - I$

$H^{\otimes n} |0^n\rangle = |h\rangle$

$H^{\otimes n} R_0 H^{\otimes n}$
$= H^{\otimes n}(2|0^n\rangle\langle 0^n| - I) H^{\otimes n}$
$= 2|h\rangle\langle h| - I$
$= R_h$

$H^\dagger = H$
$H^2 = H^\dagger H = I$

Reflection about $|B\rangle$

$|v\rangle = \alpha|A\rangle + \beta|B\rangle$

$|w\rangle = -\alpha|A\rangle + \beta|B\rangle$

$|w\rangle = Z_f|v\rangle$

$Z_f|x\rangle = (-1)^{f(x)}|x\rangle$

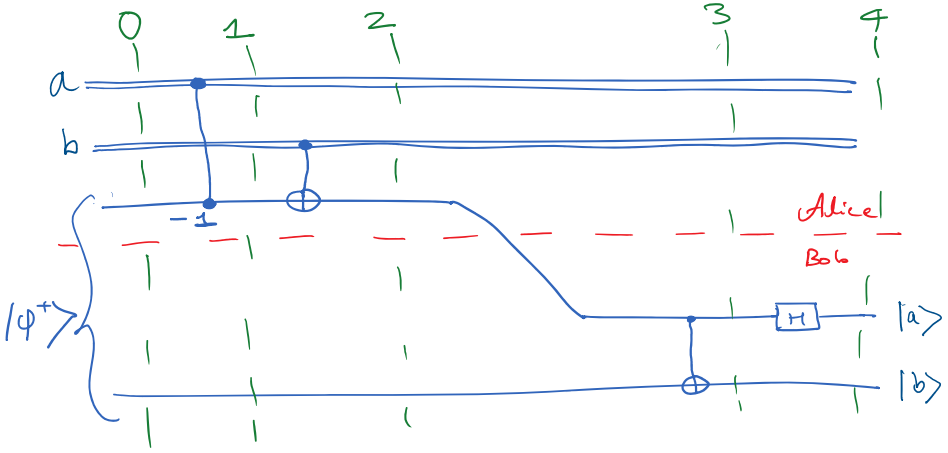
Using B_f we can implement Z_f using phase-kickback

Lecture 14

Wednesday, January 19, 2022 12:46 PM

Communication protocols

Superdense coding

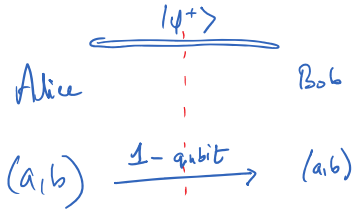


EPR (Einstein − Podolsky − Rosen) pair:

$|\phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$

ab	$\|\phi^+\rangle$	1	2	3	4
00	$\|00\rangle + \|11\rangle$	$\|00\rangle + \|11\rangle$	$\|00\rangle + \|11\rangle$	$(\|0\rangle + \|1\rangle)\|0\rangle$	$\|00\rangle$
01	$\|00\rangle + \|11\rangle$	$\|00\rangle + \|11\rangle$	$\|10\rangle + \|01\rangle$	$(\|1\rangle + \|0\rangle)\|1\rangle$	$\|01\rangle$
10	$\|00\rangle + \|11\rangle$	$\|00\rangle - \|11\rangle$	$\|00\rangle - \|11\rangle$	$(\|0\rangle - \|1\rangle)\|0\rangle$	$\|10\rangle$
11	$\|00\rangle + \|11\rangle$	$\|00\rangle - \|11\rangle$	$\|10\rangle - \|01\rangle$	$(\|1\rangle - \|0\rangle)\|1\rangle$	$-\|11\rangle$

Communication protocol



$H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$

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

$H(\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)) = |0\rangle$

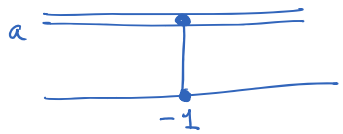
$H(\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)) = |1\rangle$

Phase flip gate

$\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$

Controlled σ_z gate:

If $a = 1$, apply σ_z on the second wire

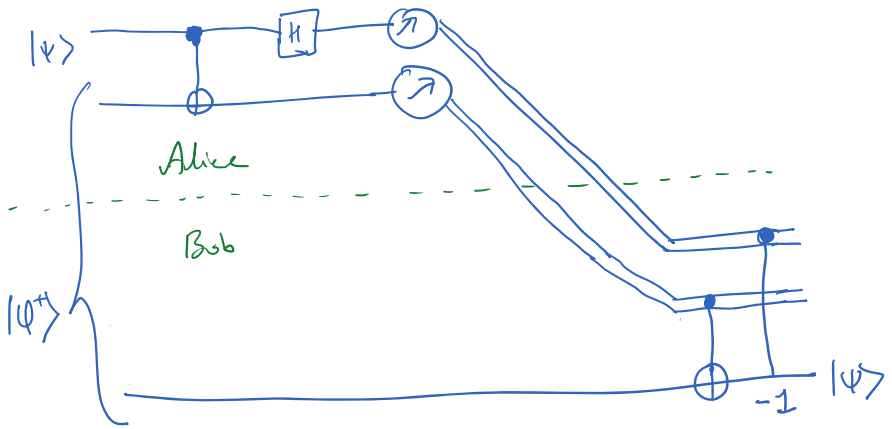


Input	Output
00	00
01	01
10	10
11	-11

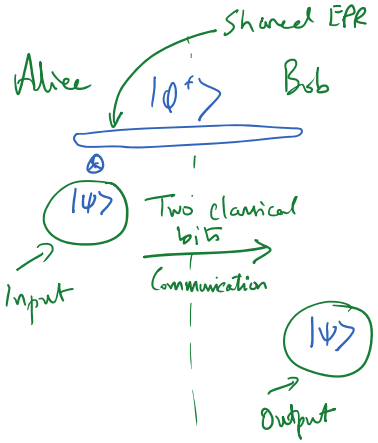
Matrix

$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$

Teleportation



Communication protocol



$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \quad ; \quad |\alpha|^2 + |\beta|^2 = 1$$

$$|\psi\rangle|\phi^+\rangle = (\alpha|0\rangle + \beta|1\rangle) \otimes \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

$$= \frac{1}{\sqrt{2}}(\alpha|000\rangle + \alpha|011\rangle + \beta|100\rangle + \beta|111\rangle)$$

$$\text{CNOT} \rightarrow \frac{1}{\sqrt{2}}(\alpha|000\rangle + \alpha|011\rangle + \beta|110\rangle + \beta|101\rangle)$$

$$H \rightarrow \frac{1}{2}(\alpha(|0\rangle + |1\rangle)|00\rangle + \alpha(|0\rangle + |1\rangle)|11\rangle + \beta(|0\rangle - |1\rangle)|10\rangle + \beta(|0\rangle - |1\rangle)|01\rangle)$$

$$= \frac{1}{2}(|00\rangle(\alpha|0\rangle + \beta|1\rangle) + |01\rangle(\alpha|1\rangle + \beta|0\rangle) + |10\rangle(\alpha|0\rangle - \beta|1\rangle) + |11\rangle(\alpha|1\rangle - \beta|0\rangle))$$

Measurement outcome	State on third wire after measurment	Prabability of outcome	State after CNOT	After C − phase flip
00	$\alpha\|0\rangle + \beta\|1\rangle$	0.25	$\alpha\|0\rangle + \beta\|1\rangle$	$\alpha\|0\rangle + \beta\|1\rangle$
01	$\alpha\|1\rangle + \beta\|0\rangle$	0.25	$\alpha\|0\rangle + \beta\|1\rangle$	$\alpha\|0\rangle + \beta\|1\rangle$
10	$\alpha\|0\rangle - \beta\|1\rangle$	0.25	$\alpha\|0\rangle - \beta\|1\rangle$	$\alpha\|0\rangle + \beta\|1\rangle$
11	$\alpha\|1\rangle - \beta\|0\rangle$	0.25	$\alpha\|0\rangle - \beta\|1\rangle$	$\alpha\|0\rangle + \beta\|1\rangle$