Lecture 1 - Introduction

bit - unit of information, state/content - one of two possible values, 0 or 1

bit state: $|0\rangle = \begin{pmatrix}1\\0\end{pmatrix}$ $|1\rangle = \begin{pmatrix}0\\1\end{pmatrix} \to \begin{cases} 0 \text{ with probability } 0 \\ 1 \text{ with probability } 1 \end{cases}$

pbit state: $\begin{pmatrix}a\\b\end{pmatrix}$, $a,b \in [0,1]$, $a+b=1$ $\begin{cases} 0 \text{ with probability } a \\ 1 \text{ with probability } b \end{cases}$

qubit state: $\begin{pmatrix}\alpha\\\beta\end{pmatrix}$, $\alpha,\beta \in \mathbb{C}$, $|\alpha|^2+|\beta|^2=1$ $\begin{cases} 0 \text{ with probability } |\alpha|^2 \\ 1 \text{ with probability } |\beta|^2 \end{cases}$

qubit - unit of quantum information, state - normalized, complex 2-vector

state of qubit:

1) Vector of length 2
2) Contains complex numbers
3) Vector's norm is 1

$z = x+yi \Rightarrow |z| = \sqrt{x^2+y^2} \Rightarrow |z|^2 = x^2+y^2$, $|z| = \sqrt{z \cdot z^*}$

$\vec{z} = \begin{pmatrix}z_1\\z_2\end{pmatrix} \Rightarrow \|\vec{z}\| = \sqrt{|z_1|^2+|z_2|^2} = \sqrt{x_1^2+y_1^2+x_2^2+y_2^2}$

$\begin{pmatrix}a\\b\end{pmatrix} = \begin{pmatrix}a\\0\end{pmatrix} + \begin{pmatrix}0\\b\end{pmatrix} = a\begin{pmatrix}1\\0\end{pmatrix} + b\begin{pmatrix}0\\1\end{pmatrix} = a|0\rangle + b|1\rangle$

superposition - neither a nor b is 0 (or 1)

Dirac Notation

$|x\rangle = \begin{pmatrix}\alpha\\\beta\end{pmatrix} = \alpha\begin{pmatrix}1\\0\end{pmatrix} + \beta\begin{pmatrix}0\\1\end{pmatrix} = \alpha|0\rangle + \beta|1\rangle$ "ket x" $\dagger \to$ conjugate transpose

$\langle x| = \begin{pmatrix}\alpha\\\beta\end{pmatrix}^\dagger = \begin{pmatrix}\alpha^*\\\beta^*\end{pmatrix}^T = (\alpha^* \;\beta^*)$ "bra x" $z = x+yi$ $z^* = x-yi \leftarrow$ complex conjugate

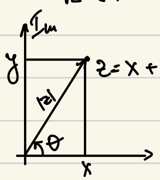
$\langle x|y\rangle = (\alpha^* \;\beta^*)\begin{pmatrix}\gamma\\\delta\end{pmatrix} = (\alpha^*\gamma + \beta^*\delta)$ "braket" (inner product) $\| |x\rangle \| = \sqrt{\langle x|x\rangle}$

Born's Rule: measuring $\begin{pmatrix}a\\b\end{pmatrix}$ returns single bit $\begin{cases} 0 \text{ with probability } |a|^2 \\ 1 \text{ with probability } |b|^2 \end{cases}$

measuring $|\phi\rangle$ returns $x \in \{0,1\}$ with probability $|\langle x|\phi\rangle|^2$

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

$|-\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\-1\end{pmatrix} = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$ $\langle 0|1\rangle = \langle 1|0\rangle = 0 \Rightarrow$ orthogonal



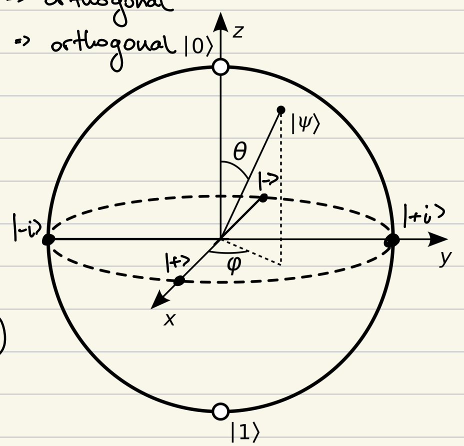
$z = x+yi = |z|e^{i\theta} = |z|(\cos\theta + i\sin\theta)$

$|\eta\rangle = e^{i\theta}(\alpha|0\rangle + \beta|1\rangle)$

$= \alpha e^{i\theta}|0\rangle + \beta e^{i\theta}|1\rangle$

$\langle 0|\eta\rangle = |\alpha \cdot e^{i\theta}|^2 = |\alpha|^2 |e^{i\theta}|^2 = |\alpha|^2$

Bloch sphere



$\boxed{\text{Th}}$ qubit state = unique

$\cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\phi}\sin\left(\frac{\theta}{2}\right)|1\rangle$,

$\theta \in [0,\pi]$, $\phi \in [0,2\pi]$

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

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

Lecture 2 - Quantum Gates

$|\varphi\rangle = \begin{pmatrix}\alpha \\ \beta\end{pmatrix}$, $\alpha, \beta \in \mathbb{C}$: $|\alpha|^2 + |\beta|^2 = 1$

$|\psi\rangle = e^{i\delta}\left(\cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\phi}\sin\left(\frac{\theta}{2}\right)|1\rangle\right)$ $\quad \left.\begin{matrix} 0 \le \theta \le \pi \\ 0 \le \phi \le 2\pi \end{matrix}\right\}$ Bloch Sphere

↳ global phase, $0 \le \delta \le 2\pi$

Quantum gate - unitary matrix (reversible) - its columns are orthonormal vectors
$\quad$ norm preserving +

$U^\dagger \cdot U = U \cdot U^\dagger = I$, $|\varphi\rangle \xrightarrow{U} U \cdot |\varphi\rangle$, $I|v\rangle = |v\rangle$, $I \cdot M = M = M \cdot I$

Th] U - unitary iff $\forall |\varphi\rangle, |\psi\rangle$: $\langle\varphi|U^\dagger U|\psi\rangle = \langle\varphi|\psi\rangle$

Pauli Gates

$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = |0\rangle\langle 1| + |1\rangle\langle 0|$, $\quad |a\rangle\langle b| = |a\rangle \cdot \langle b| \to 1$ at row a, column b

$X|0\rangle = |1\rangle$, $X|1\rangle = |0\rangle$, $X|+\rangle = |+\rangle$, $X|-\rangle = -|-\rangle$, $\{|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)\}$

$Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$ $\quad Y|+i\rangle = |+i\rangle$, $Y|-i\rangle = -|-i\rangle$, $\{|\pm i\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm i|1\rangle\}$

$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ $\quad Z|0\rangle = |0\rangle$, $Z|1\rangle = -|1\rangle$, $\{|0\rangle, |1\rangle\}$

$\{|v_0\rangle, |v_1\rangle\}$ - orthonormal basis $\Rightarrow |v_0\rangle\langle v_0| + |v_1\rangle\langle v_1| = I$

$$U(\theta, \phi, \lambda) = \begin{pmatrix} \cos\left(\frac{\theta}{2}\right) & -e^{i\lambda}\sin\left(\frac{\theta}{2}\right) \\ e^{i\phi}\sin\left(\frac{\theta}{2}\right) & e^{i(\phi+\lambda)}\cos\left(\frac{\theta}{2}\right) \end{pmatrix}$$

$R_{\hat{n}}(\theta) = \cos\left(\frac{\theta}{2}\right)I - i\sin\left(\frac{\theta}{2}\right)[n_x \cdot X + n_y \cdot Y + n_z \cdot Z]$, $n_x, n_y, n_z \in \mathbb{R}$, $\|\hat{n}\| = 1$

$R_{(0,0,1)}(\pi) = -iZ$, $\quad Z|\pm\rangle = |\mp\rangle$, $Z|\pm i\rangle = |\mp i\rangle$

$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \frac{X+Z}{\sqrt{2}} = R_{\left(\frac{1}{\sqrt{2}}, 0, \frac{1}{\sqrt{2}}\right)}(\pi)$ $\quad H|0\rangle = |+\rangle$, $H|+\rangle = |0\rangle$, $H|1\rangle = |-\rangle$, $H|-\rangle = |1\rangle$

$HZH = X$, $HXH = Z$

Properties:

- → involutory: $X \cdot X = Y \cdot Y = Z \cdot Z = I$
- → cyclicity: $X \cdot Y = iZ$, $Y \cdot Z = iX$, $Z \cdot X = iY$
- → anticommutation: $X \cdot Y = -Y \cdot X$, $X \cdot Z = -Z \cdot X$, $Y \cdot Z = -Y \cdot Z$

$U_1(\lambda) = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\lambda} \end{pmatrix}$, $\quad U_2(\phi, \lambda) = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & -e^{i\lambda} \\ e^{i\phi} & e^{i(\lambda+\phi)} \end{pmatrix}$

Lecture 3 - Multiple Qubits

$|\psi\rangle -\boxed{U}- |\psi\rangle$, $|\psi\rangle = U \cdot |\varphi\rangle$ $\quad U^\dagger |\psi\rangle = U^\dagger (U|\varphi\rangle) = I_2 |\varphi\rangle = |\varphi\rangle$

$\hookrightarrow$ 2×2 unitary matrix $\Rightarrow U \cdot U^\dagger = U^\dagger \cdot U = I_2 = \begin{pmatrix}1&0\\0&1\end{pmatrix}$, $U^{-1} = U^\dagger$, reversible

2	X	Y	Z
$+1$	$\|+\rangle$	$\|+i\rangle$	$\|0\rangle$
-1	$\|-\rangle$	$\|-i\rangle$	$\|1\rangle$

$|+\rangle = \frac{1}{\sqrt2}\begin{pmatrix}1\\1\end{pmatrix}$ $\quad i|+\rangle = \frac{1}{\sqrt2}\begin{pmatrix}i\\i\end{pmatrix}$ $\quad |+\rangle \neq i|+\rangle$, $|+\rangle \cong i|+\rangle$

$H = \frac{1}{\sqrt2}\begin{pmatrix}1&1\\1&-1\end{pmatrix}$ $\quad -H = \frac{1}{\sqrt2}\begin{pmatrix}-1&-1\\-1&1\end{pmatrix}$ $\quad H \neq -H$, $H \cong -H$

$H|+\rangle = |0\rangle$ $\quad -H \cdot i|+\rangle = -i|0\rangle$ $\quad |0\rangle \neq -i|0\rangle$, $|0\rangle \cong -i|0\rangle$

$|\psi\rangle$ - measure in orthonormal basis $\{|v\rangle, |v^\perp\rangle\}$

outcome	probability	post state
$+1$	$\|\langle v\|\varphi\rangle\|^2$	$\|v\rangle$
-1	$\|\langle v^\perp\|\varphi\rangle\|^2$	$\|v^\perp\rangle$

send	action	Pr(+1)	state	action	Pr(+1)
$\|0\rangle$	-	-	$\|0\rangle$	Z	1
$\|0\rangle$	Z, $+1$	1	$\|0\rangle$	Z	1
$\|+\rangle$	Z, $+1$	$\frac{1}{2}$	$\|0\rangle$	X	$\frac{1}{2}$
$\|+\rangle$	X, $+1$	1	$\|+\rangle$	X	1

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

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

$10011_2 = 19_{10}$

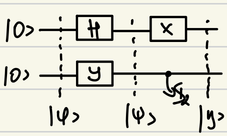
$|10011\rangle = \left.\begin{pmatrix}0\\ \vdots\\ 1\\ \vdots\\ 0\end{pmatrix}\right\} 2^5 = 32$ (pos)

Def. n-qubit state $|\psi\rangle$ - 2^n-dimensional complex vector of norm 1

$|\psi\rangle = \sum_{x\in\{0,1\}^n} \alpha_x |x\rangle$ where $\alpha_x \in \mathbb{C}$ and $\sum_x |\alpha_x|^2 = 1$

Def. entangled two-qubit state - cannot be written as Kronecker product of 2 single-qubits

$(V\otimes W)\cdot(C\otimes D) = ((V\cdot C)\otimes(W\cdot D))$ $\qquad V\otimes W + V\otimes C = V\otimes(W+C)$



$|\psi\rangle = |00\rangle = |0\rangle\otimes|0\rangle$

$|\psi\rangle = (H\otimes Y)|\psi\rangle = (H\otimes Y)(|0\rangle\otimes|0\rangle) = (H|0\rangle)\otimes(Y|0\rangle) = |+\rangle\otimes i|1\rangle = i|+\rangle|1\rangle$

$|\gamma\rangle = (X\otimes I)|\psi\rangle = (X\otimes I)\cdot i|+\rangle|1\rangle = i|+\rangle|1\rangle$

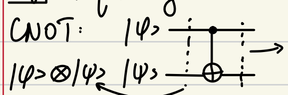
Def n-qubit gate - $2^n \times 2^n$ unitary matrix

$(A\cdot B)^\dagger = B^\dagger \cdot A^\dagger$ $\quad (A\otimes B)^\dagger = A^\dagger \otimes B^\dagger$

$(H\otimes Y)^\dagger \cdot (H\otimes Y) = (H^\dagger \otimes Y^\dagger)\cdot(H\otimes Y) =$

$= H^\dagger H \otimes Y^\dagger Y = I_2 \otimes I_2 = I_4$

CNOT:

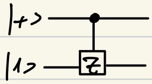


$\rightarrow \begin{cases} \text{id } |\varphi\rangle = 0: |\varphi\rangle\otimes|\psi\rangle \\ \text{id } |\varphi\rangle = 1: |\varphi\rangle\otimes X|\psi\rangle \end{cases}$

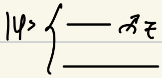
$|\psi\rangle = CNOT\left(\frac{|00\rangle - |11\rangle}{\sqrt2}\right) = \frac{1}{\sqrt2} CNOT(|00\rangle - |11\rangle) = \frac{1}{\sqrt2}(CNOT|00\rangle - CNOT|11\rangle) = \frac{1}{\sqrt2}(|00\rangle - |1\rangle\otimes X|1\rangle)$

$= \frac{1}{\sqrt2}(|0\rangle - |1\rangle)\otimes|0\rangle = |-\rangle\otimes|0\rangle = |-\rangle|0\rangle = |-0\rangle$

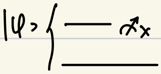
$$CNOT(0,1) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} = |0\rangle\langle 0| \otimes I_2 + |1\rangle\langle 1| \otimes I_2 \qquad CNOT(1,0) = I_2 \otimes |0\rangle\langle 0| + X \otimes |1\rangle\langle 1|$$



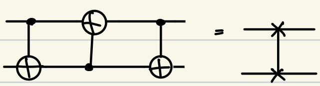
$$CZ|+1\rangle = CZ \cdot \tfrac{1}{\sqrt2}(|0\rangle+|1\rangle)|1\rangle = \tfrac{1}{\sqrt2}\left(CZ|01\rangle + CZ|11\rangle\right) = \tfrac{1}{\sqrt2}\left(|0\rangle\otimes I_2|1\rangle + |1\rangle\otimes Z|1\rangle\right)$$
$$= \tfrac{1}{\sqrt2}\left(|01\rangle + |1\rangle\otimes -|1\rangle\right) = \tfrac{1}{\sqrt2}\left(|01\rangle - |11\rangle\right)$$



$$|\psi\rangle = \tfrac12|00\rangle + \tfrac{1}{\sqrt2}|01\rangle + \tfrac12|10\rangle + 0|11\rangle$$
$$\Pr(+1 \overset{|0\rangle}{\text{on top}}) = \left|\tfrac12\right|^2 + \left|\tfrac{1}{\sqrt2}\right|^2 = \tfrac34, \quad \text{post} = \left(\tfrac12|00\rangle + \tfrac{1}{\sqrt2}|01\rangle\right)\cdot \frac{1}{\sqrt{\frac34}}$$



$$|\psi\rangle = \tfrac12\left(|00\rangle + |01\rangle + |10\rangle - |11\rangle\right) = \tfrac{1}{\sqrt2}|+0\rangle + \tfrac{1}{\sqrt2}|-1\rangle \rightarrow \Pr(+1 \overset{|+\rangle}{\text{on top}}) = \tfrac12$$
$$|0\rangle = \frac{|+\rangle+|-\rangle}{\sqrt2}, \quad |1\rangle = \frac{|+\rangle-|-\rangle}{\sqrt2} \Rightarrow |00\rangle = \left(\frac{|+\rangle+|-\rangle}{\sqrt2}\right)\otimes|0\rangle = \frac{|+0\rangle+|-0\rangle}{\sqrt2} \qquad \text{post: } |+0\rangle$$



SWAP gate

$SWAP(|\varphi\rangle\otimes|\psi\rangle) = |\psi\rangle\otimes|\varphi\rangle$

Lecture 4 - Universality

Def. Quantum computer (Set of quantum gates) is universal if it can achieve any unitary on any number of qubits

Th Any 2×2 matrix $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ can be decomposed as

$|0\rangle\langle 0| = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \frac{I+Z}{2} \quad |0\rangle\langle 1| = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \frac{X+iY}{2}$ $\qquad M = \frac{a+d}{2}I + \frac{b+c}{2}X + i\,\frac{b-c}{2}Y + \frac{a-d}{2}Z$

$|1\rangle\langle 0| = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \frac{X-iY}{2} \quad |1\rangle\langle 1| = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \frac{I-Z}{2}$ $\qquad M = a\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + b\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} + c\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} + d\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$

$X = |0\rangle\langle 1| + |1\rangle\langle 0| = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad Y = i|1\rangle\langle 0| + (-i)|0\rangle\langle 1|$

Def. n-qubit Pauli string is Kronecker product of n Paulis

Th Any $2^n\times2^n$ matrix can be decomposed as $M = \sum_{i_1=1}^{4}\dots\sum_{i_n=1}^{4} \underbrace{\alpha_{i_1,\dots,i_n}}_{\in\mathbb{C}} P_{i_1}\otimes P_{i_2}\otimes\dots\otimes P_{i_n}$

$CNOT = |0\rangle\langle 0|\otimes I + |1\rangle\langle 1|\otimes X = \frac{I+Z}{2}\otimes I + \frac{I-Z}{2}\otimes X = \frac12\left[I\otimes I + Z\otimes I + I\otimes X - Z\otimes X\right]$

Th N-qubit unitary U is Clifford if $UPU^\dagger$ is $\alpha\in\mathbb{C}$ Pauli string, for each Pauli string P

$HIH^\dagger = HH^\dagger = I, \quad HXH^\dagger = Z \Rightarrow XH^\dagger = H^\dagger Z \Rightarrow X = H^\dagger ZH = HZH^\dagger, \quad HYH^\dagger = -Y$

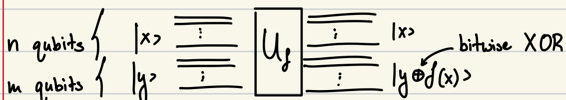
$CNOT.(I\otimes X).CNOT^\dagger = (|0\rangle\langle 0|\otimes I + |1\rangle\langle 1|\otimes X)(I\otimes X).CNOT^\dagger = \left[(|0\rangle\langle 0|\otimes I).(I\otimes X) + (|1\rangle\langle 1|\otimes X).(I\otimes X)\right].CNOT^\dagger$

$= \left[|0\rangle\langle 0|.I\otimes I.X + |1\rangle\langle 1|I\otimes XX\right].CNOT^\dagger = \dots$

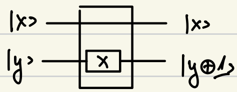
Th $\{CNOT, \text{every single qubit gate}\}$ is universal.

Th $\alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle$ is entangled iff $\alpha\delta - \beta\gamma \neq 0$

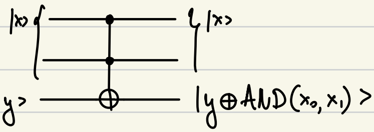
Def. Boolean function maps bitstrings to bitstrings, $f: \{0,1\}^n \rightarrow \{0,1\}^m$



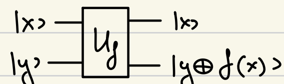
x	0	1
SET(x)	1	1



x_0	0	0	1	1
x_1	0	1	0	1
AND(x)	0	0	0	1



Boolean oracle:



$U_f |x, 0\rangle = |x, f(x)\rangle$

$\hookrightarrow U_f |x, 0, 0\rangle = |x, f(x), g(x)\rangle$

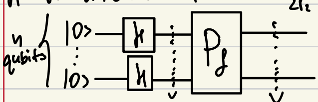
Phase oracle:

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

Lecture 5 - Deutsch-Josza Algorithm

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

$H \otimes H \otimes H |000\rangle = |+++\rangle = \frac{1}{2\sqrt{2}}(|000\rangle + |001\rangle + \dots + |110\rangle + |111\rangle) \Rightarrow H^{\otimes n} |0\rangle^{\otimes n} = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle$



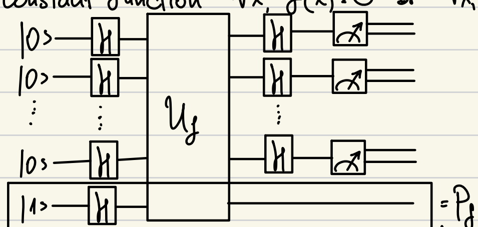
$\frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle \qquad \frac{1}{\sqrt{2^n}} \sum_x (-1)^{f(x)} |x\rangle$

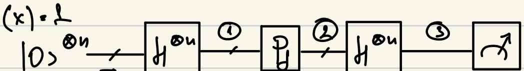
Th| $x \in \{0,1\}^n \to H^{\otimes n} |x\rangle = \frac{1}{\sqrt{2^n}} \sum_{y \in \{0,1\}^n} (-1)^{x \cdot y} |y\rangle$

Deutsch-Josza

Balanced function: exactly half of x, $f(x) = 0$, other half $f(x) = 1$

Constant function: $\forall x, f(x) = 0$ or $\forall x, f(x) = 1$





1) $\frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle$

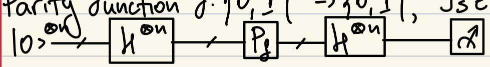
2) $\frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} P_f |x\rangle$, $P_f |x\rangle = (-1)^{f(x)} |x\rangle$

3) $\frac{1}{\sqrt{2^n}} \sum_x (-1)^{f(x)} \cdot \frac{1}{\sqrt{2^n}} \sum_{y \in \{0,1\}^n} (-1)^{x \cdot y} |y\rangle$

coefficient in front of $|00\dots00\rangle = \frac{1}{2^n} \sum_x (-1)^{f(x)} \cdot (-1)^{x \cdot (0 \dots 0)} = \frac{1}{2^n} \sum_x (-1)^{f(x)} = \begin{cases} \left.\begin{matrix} 1 & \forall x, f(x) = 0 \\ -1 & \forall x, f(x) = 1 \end{matrix}\right\} \text{const} \\ 0 \quad f\text{-balanced} \end{cases}$

Bernstein-Vazirani

Parity function $f: \{0,1\}^n \to \{0,1\}$, $\exists s \in \{0,1\}^n$ s.t. $f(x) = s \cdot x \pmod 2$

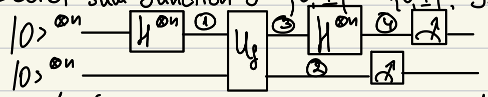


$\frac{1}{2^n} \sum_x (-1)^{f(x)} \sum_y (-1)^{x \cdot y} |y\rangle = \frac{1}{2^n} \sum_x \sum_y (-1)^{s \cdot x + x \cdot y} |y\rangle$

$y = s \to s \cdot x + x \cdot y = 0 \Rightarrow$ coefficient in front of $|s\rangle = \frac{1}{2^n} \sum_x 1 = 1$

Simon's

Secret sum function $f: \{0,1\}^n \to \{0,1\}^n$, $\exists s \in \{0,1\}^n \neq 0^{\otimes n}$ s.t. $f(x) = f(y) \iff x = y \oplus s$



1) $\frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |0\rangle^{\otimes n} |x\rangle$

2) $|0 \oplus f(x)\rangle = |f(x)\rangle \to \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |f(x)\rangle |x\rangle$

3) $\frac{1}{\sqrt{2}} \left(|f(x)\rangle |x\rangle + |f(x)\rangle |x \oplus s\rangle \right) = |f(x)\rangle \frac{1}{\sqrt{2}} \left(|x\rangle + |x \oplus s\rangle \right)$

4) $|x\rangle \xrightarrow{H^{\otimes n}} \frac{1}{\sqrt{2^n}} \sum_y (-1)^{x \cdot y} |y\rangle \Rightarrow \frac{1}{\sqrt{2}} \frac{1}{\sqrt{2^n}} \sum_{y \in \{0,1\}^n} \left((-1)^{x \cdot y} |y\rangle + (-1)^{(x \oplus s)\cdot y} |y\rangle \right)$

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

output $|y\rangle \Rightarrow x \cdot y = (x \oplus s) \cdot y \pmod 2 \Rightarrow s \cdot y = 0 \pmod 2$

Lecture 6 - Quantum Fourier Transform

Def. $e^{2\pi i \frac{x}{N}}$, $x = 0, 1, 2, \dots, N-1$ are N^{th} roots of unity ($z^N = 1$)

primitive N^{th} root: $\omega_N = e^{2\pi i \frac{1}{N}}$, $\omega_N^{x \cdot y} = \omega_{N/x}^{y}$, $x, y = 0, 1, 2, \dots$, $x \mid N$

$$F_N: N\left\{ \underbrace{\begin{pmatrix} x_0 \\ x_1 \\ \vdots \\ x_{N-1} \end{pmatrix}}_{x} \right. \longmapsto \frac{1}{\sqrt{N}} \underbrace{\begin{pmatrix} x_0 \cdot \omega_N^{0\cdot 0} + x_1 \cdot \omega_N^{1\cdot 0} + \dots + x_{N-1} \cdot \omega_N^{(N-1)\cdot 0} \\ x_0 \cdot \omega_N^{0 \cdot 1} + \dots \\ \vdots \\ x_0 \cdot \omega_N^{0\cdot(N-1)} + x_1 \cdot \omega_N^{1\cdot(N-1)} + \dots + x_{N-1} \cdot \omega_N^{(N-1)(N-1)} \end{pmatrix}}_{\tilde{x}}$$

$\tilde{x}_j = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} x_k \cdot \omega_N^{j \cdot k}$, $x_i \in \mathbb{C}$

$$F_N = \frac{1}{\sqrt{N}} \begin{pmatrix} \omega_N^{0\cdot 0} & \dots & \omega_N^{(N-1)\cdot 0} \\ \vdots & & \vdots \\ \omega_N^{0\cdot(N-1)} & \dots & \omega_N^{(N-1)\cdot(N-1)} \end{pmatrix}$$

$F_1 = \frac{1}{\sqrt{1}} \left(\omega_1^{0\cdot 0} \right) = 1$ $\omega_2 = e^{2\pi i \frac{1}{2}} = e^{\pi i} = -1$ $N = 2^n$

$F_2 = \frac{1}{\sqrt{2}} \begin{pmatrix} \omega_2^0 & \omega_2^0 \\ \omega_2^0 & \omega_2^1 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = H$

$x \in \{0,1\}^4$, $F_{16} |x\rangle = \frac{1}{\sqrt{16}} \left(\omega_{16}^{0 \cdot x} |0000\rangle + \omega_{16}^{1\cdot x} |0001\rangle + \omega_{16}^{2 \cdot x} |0010\rangle + \dots + \omega_{16}^{15 \cdot x} |1111\rangle \right)$

binary representation of integer value

$= \frac{1}{\sqrt{2}} \left(|0\rangle + \underbrace{\omega_{16}^{8x}}_{\omega_2^x} |1\rangle \right) \otimes \frac{1}{\sqrt{2}} \left(|0\rangle + \underbrace{\omega_{16}^{4x}}_{\omega_4^x} |1\rangle \right) \otimes \frac{1}{\sqrt{2}} \left(|0\rangle + \underbrace{\omega_{16}^{2x}}_{\omega_8^x} |1\rangle \right) \otimes \frac{1}{\sqrt{2}} \left(|0\rangle + \omega_{16}^{x} |1\rangle \right)$

$\Rightarrow F_{16}|x\rangle = x^{th}$ column of $F_{16} = \frac{1}{\sqrt{16}} \begin{pmatrix} \omega_N^{x \cdot 0} \\ \omega_N^{x \cdot 1} \\ \vdots \\ \omega_N^{x \cdot 15} \end{pmatrix} = \frac{1}{4} \left(\omega_N^{0 \cdot x} |0000\rangle + \omega_N^{1 \cdot x} |0001\rangle + \dots + \omega_N^{15 \cdot x} |1111\rangle \right)$

$= \frac{1}{4} \left(|0000\rangle + \omega_N^{x} |0001\rangle + \omega_N^{2x} |0010\rangle + \dots + \omega_N^{15x} |1111\rangle \right)$

$\tilde{v}_j = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} v_k \, \omega_N^{j \cdot k} \Rightarrow F_{16} \cdot v = \alpha_0 |0000\rangle + \alpha_1 |0001\rangle + \dots + \alpha_{15} |1111\rangle$

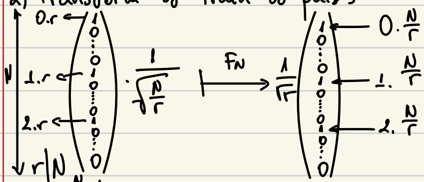
$\alpha_j = \tilde{v}_j = \frac{1}{\sqrt{16}} \left(v_0 \cdot \omega_{16}^{j \cdot 0} + v_1 \cdot \omega_{16}^{j \cdot 1} + \dots + v_{15} \cdot \omega_{16}^{j \cdot 15} \right)$

$v = |x\rangle$, $v = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$ x^{th} position $\Rightarrow \alpha_j = \tilde{v}_j = \frac{1}{\sqrt{16}} \underset{1}{\underset{\shortparallel}{v_x}} \, \omega_{16}^{j \cdot x}$

Properties

1) Unitary: $F_N \cdot F_N^{\dagger} = 1$

2) Transform of train of pulses



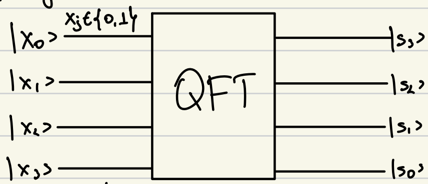
$$\sqrt{\frac{r}{N}}\sum_{j=0}^{\frac{N}{r}-1}|j\cdot r\rangle \xmapsto{F_N} \frac{1}{\sqrt{r}}\sum_{j=0}^{r-1}\left|j\cdot\frac{N}{r}\right\rangle$$

3) Linear shift keep absolute values

$$\sum_{x=0}^{N-1}\alpha_x|x\rangle = \begin{pmatrix}\alpha_{000}\\ \alpha_{001}\\ \vdots \\ \alpha_{111}\end{pmatrix} \xmapsto{F_N} \sum_{x=0}^{N-1}\beta_x|x\rangle$$

$$\sum_{x=0}^{N-1}\alpha_x|x+t \bmod N\rangle \xmapsto{F_N} \sum_{x=0}^{N-1}\gamma_x|x\rangle \text{ where } |\gamma_x| = |\beta_x|$$

$$\hookrightarrow \begin{pmatrix}\alpha_{110}\\ \alpha_{111}\\ \alpha_{000}\\ \vdots \\ \alpha_{101}\end{pmatrix} \text{ if } t=2$$



$$R_\lambda = \begin{pmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 1 & 0\\ 0 & 0 & 0 & \lambda\end{pmatrix}$$

$x \in \{0,1\}^4$

$$F_{16}|x\rangle = \underbrace{\frac{1}{\sqrt2}\left(|0\rangle + \overbrace{\omega_{16}^{8x}}^{\omega_2^x}|1\rangle\right)}_{|s_3\rangle} \otimes \underbrace{\frac{1}{\sqrt2}\left(|0\rangle + \overbrace{\omega_{16}^{4x}}^{\omega_4^x}|1\rangle\right)}_{|s_2\rangle} \otimes \underbrace{\frac{1}{\sqrt2}\left(|0\rangle + \overbrace{\omega_{16}^{2x}}^{\omega_8^x}|1\rangle\right)}_{|s_1\rangle} \otimes \underbrace{\frac{1}{\sqrt2}\left(|0\rangle + \omega_{16}^{x}|1\rangle\right)}_{|s_0\rangle}$$

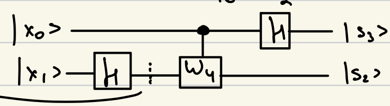
$$|s_3\rangle = \frac{|0\rangle + \omega_{16}^{8x}|1\rangle}{\sqrt2} = \frac{|0\rangle + (-1)^{x_0}|1\rangle}{\sqrt2}$$

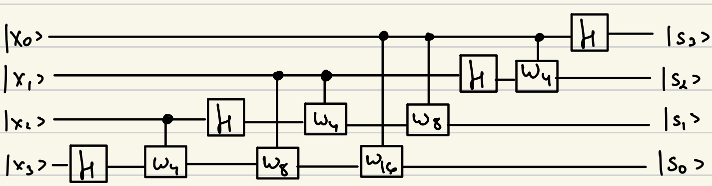
$$\underbrace{\begin{aligned}\omega_{16}^{8x} &= e^{2\pi i\frac{8x}{16}} = e^{\frac{2\pi i}{2}x} = e^{\frac{2\pi i}{2}(2^3x_3+2^2x_2+2^1x_1+2^0x_0)}\\ &= e^{2\pi i\left(x_3\frac{2^3}{2}+x_2\frac{2^2}{2}+x_1\frac{2^1}{2}+x_0\frac{2^0}{2}\right)} = 1\cdot1\cdot1\cdot e^{2\pi i x_0\frac{2^0}{2}}\\ &= e^{\pi i x_0} = \begin{Bmatrix} e^0 & \text{if } x_0=0\\ e^{\pi i}=-1 & \text{if } x_0=1\end{Bmatrix} = (-1)^{x_0}\end{aligned}}_{\omega_{16}^{8x} = \omega_2^{x_0}}$$

$$|s_2\rangle = \frac{|0\rangle + \omega_{16}^{4x}|1\rangle}{\sqrt2}, \quad \omega_{16}^{4x} = \omega_2^{x_1} + \omega_4^{x_0}$$

$$|s_2\rangle = \frac{1}{\sqrt2}\left(|0\rangle + \omega_2^{x_1}\cdot\omega_4^{x_0}|1\rangle\right)$$

$$H|x_1\rangle = \frac{1}{\sqrt2}\left(|0\rangle + \omega_2^{x_1}|1\rangle\right)$$





Lecture 7 - Phase Estimation

Th U-unitary with $|\varphi\rangle$-eigenstate and λ-eigenvalue $\Rightarrow |\lambda|^2 = 1$

$U|\varphi\rangle = \lambda|\varphi\rangle$, $\lambda\in\mathbb{C}$, $\langle\varphi|\varphi\rangle = 1$, $U^\dagger U = I$

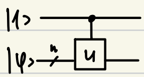
$\langle\varphi|\varphi\rangle = \langle\varphi|I|\varphi\rangle = \langle\varphi|U^\dagger U|\varphi\rangle = (\lambda|\varphi\rangle)^\dagger\cdot\lambda|\varphi\rangle = \langle\varphi|\lambda^*\lambda|\varphi\rangle = \lambda^*\cdot\lambda\,\langle\varphi|\varphi\rangle = |\lambda|^2\langle\varphi|\varphi\rangle = 1 \Rightarrow |\lambda|^2 = 1$

Collary $\lambda = e^{2\pi i\theta}$, $\theta\in[0,1)$

n-qubit unitary $\mathcal{U}$ with eigenstate $|\varphi\rangle, \exists\, \theta_1, \theta_2, \dots, \theta_t$ s.t. $\mathcal{U}|\varphi\rangle = e^{2\pi i\, \overline{0.\theta_1\theta_2\dots\theta_t}_{(2)}}|\varphi\rangle$

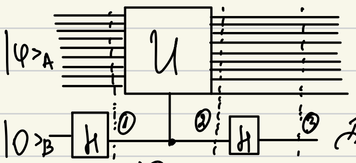
$Y|-i\rangle = -1|-i\rangle = e^{\pi i}|-i\rangle = e^{2\pi i\cdot\frac{1}{2}}|-i\rangle = e^{2\pi i\, \overline{0.100..}_{(2)}}|-i\rangle \rightarrow$ t-precision

Hadamard Test



Dirac: $|0\rangle\langle 0| \otimes \mathcal{I} + |1\rangle\langle 1| \otimes \mathcal{U}$ $\quad |j\rangle\langle k| :$ $\begin{pmatrix} 0 & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 \\ \dots & & 1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$

$\begin{pmatrix} \mathcal{I} & 0 \\ 0 & \mathcal{U} \end{pmatrix}$



1) $|+\rangle_B|\varphi\rangle_A = \frac{|0\rangle|\varphi\rangle + |1\rangle|\varphi\rangle}{\sqrt{2}}$

2) $\frac{|+\rangle\otimes\mathcal{I}|\varphi\rangle + |1\rangle\otimes\mathcal{U}|\varphi\rangle}{\sqrt{2}} = \frac{|0\rangle|\varphi\rangle + e^{2\pi i\theta}|1\rangle|\varphi\rangle}{\sqrt{2}} = \frac{|0\rangle + 2\pi i\theta|1\rangle}{\sqrt{2}} \otimes |\varphi\rangle$

3) $\frac{|+\rangle + e^{2\pi i\theta}|-\rangle}{\sqrt{2}} \otimes |\varphi\rangle = \dots = \left(\frac{1+e^{2\pi i\theta}}{2}|0\rangle + \frac{1-e^{2\pi i\theta}}{2}|1\rangle\right) \otimes |\varphi\rangle$

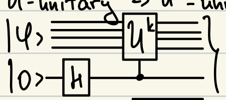
$Pr(|0\rangle) = \left|\frac{1+e^{2\pi i\theta}}{2}\right|^2 = \frac{1+\cos(2\pi\theta)}{2}$ $\quad Pr(|1\rangle) = \frac{1-\cos(2\pi\theta)}{2}$ $\quad$ outcome = coin toss

$\Rightarrow \hat{\mu} = \frac{1}{k}\sum_{j=1}^{k} c_j, \quad \mu = \frac{1-\cos(2\pi\theta)}{2}$ $\quad$ Chernoff-Hoeffding ineq.: $Pr(|\mu - \hat{\mu}| \geq \varepsilon) \leq 2^{-2\varepsilon^2 k}$

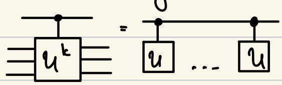
$\varepsilon = 2^{-t} \Rightarrow \underbrace{Pr(|\mu-\hat{\mu}| \geq \varepsilon) \leq 2^{-2\cdot 2^{-2t}\cdot k}}_{\delta} \Rightarrow O(2^{2t-1}\log(\frac{2}{\delta}))$

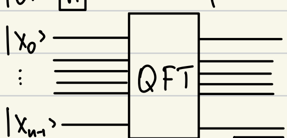
Quantum Phase Estimation

$\mathcal{U}$-unitary $\Rightarrow \mathcal{U}^k$-unitary; λ-eigenvalue of $\mathcal{U} \Rightarrow \lambda^k$-eigenvalue of $\mathcal{U}^k$



$\frac{|0\rangle + e^{2\pi i\theta k}|1\rangle}{\sqrt{2}} \otimes |\varphi\rangle$

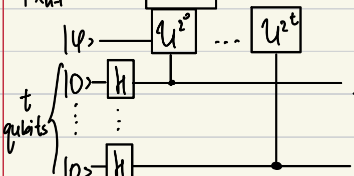




$\frac{|0\rangle + e^{2\pi i\cdot x_{n-1}/2^n}|1\rangle}{\sqrt{2}}$

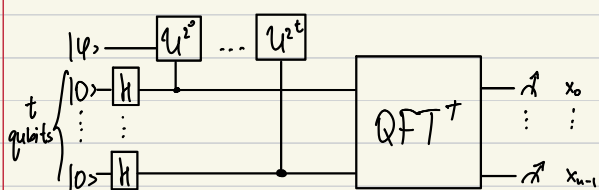
$\vdots$

$\frac{|0\rangle + e^{2\pi i\cdot x_0/2^n}|1\rangle}{\sqrt{2}}$



$\frac{|0\rangle + e^{2\pi i\theta}|1\rangle}{\sqrt{2}} = \frac{|0\rangle + e^{2\pi i x/2^t}|1\rangle}{\sqrt{2}}$

$\frac{|0\rangle + e^{2\pi i\theta\cdot 2^t}|1\rangle}{\sqrt{2}} = \frac{|0\rangle + e^{2\pi i x}|1\rangle}{\sqrt{2}}$ $\quad x = \theta\cdot 2^t \in \mathbb{N}$

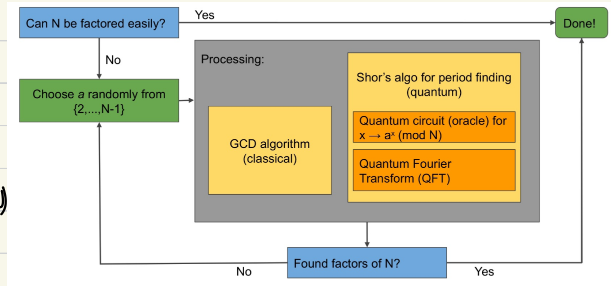


TW $x \notin \mathbb{N} \Rightarrow$ QFT-closest integer, prob. ≥ 0.4

TW prob. $\geq 1-\delta \Rightarrow \approx \log(\frac{1}{\delta})$ times

$\theta = 2^t\cdot x$

Lecture 8 - Shor's Algorithm



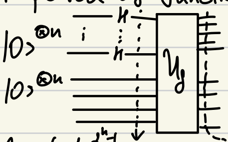
Integer factorization:

$N \in \mathbb{N}^{>1}$, $\exists\, p, q \in \mathbb{N}^{>1}$ s.t. $N = p.q$

Period finding:

$a, N \in \mathbb{N}^{>1}$, $\exists\, r \in \mathbb{N}$ s.t. $a^r = 1 \pmod N$

r-period of function $f(x) = a^x \pmod N$



$$U_f\left(\frac{1}{\sqrt{2^n}}\sum_{k=0}^{2^n-1}|k\rangle\otimes|0..0\rangle\right) = \frac{1}{\sqrt{2^n}}\sum_{k=0}^{2^n-1}|k\rangle\otimes|0+a^k \bmod N\rangle$$