Chapter 0 - Linear Algebra Prerequisit

Vectors & Vector Spaces

vector space V over a field F - set of objects (vectors) s.t. the following hold:

1) vector addition $|a\rangle, |b\rangle \in V \Rightarrow |a\rangle + |b\rangle = |c\rangle$, $|c\rangle \in V$
2) scalar multiplication $|a\rangle \in V$, $n \in F \Rightarrow n|a\rangle \in V$

Matrices & Matrix Operations

matrix - transforms vectors into other vectors $|v\rangle \to |v'\rangle = M|v\rangle$

quantum gate = matrix

Pauli-X gate $\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ $\sigma_x|0\rangle = |1\rangle$ $\sigma_x|1\rangle = |0\rangle$

Hermitian matrix - conjugate transpose ($\dagger$)

Pauli-Y matrix $\sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$ $\sigma_y^\dagger = \sigma_y$

Unitary matrix - the inverse matrix is the conjugate transpose of the original one

$A^{-1}A = AA^{-1} = \mathbb{I}$, identity matrix

$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ $\det A = ad - bc \Rightarrow A^{-1} = \frac{1}{\det A}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$

Pauli-Y is unitary: $\sigma_y^\dagger \sigma_y = \mathbb{I}$

Spanning Sets, Linear Dependence & Bases

$V_s \subset V$ - any vector in V_s as linear combination of vectors containted within S, $|v\rangle = \sum_i f_i |v_i\rangle$

set of vectors $|v_1\rangle, \dots, |v_n\rangle$ - linearly dependent if $\sum_i b_i |v_i\rangle = 0$, $b_i \neq 0$

$\sum_i b_i|v_i\rangle = b_a|v_a\rangle + \sum_{i, i\neq a} b_i|v_i\rangle = 0 \Rightarrow |v_a\rangle = -\sum_{i, i\neq a} \frac{b_i}{b_a}|v_i\rangle = -\sum_{i, i\neq a} c_i|v_i\rangle$

linearly independent set of vectors - a vector can't be expressed as combination of others

basis - linearly independent spanning set, size of basis = dimension of vector space

Hilbert Spaces, Orthonormality & Inner Product

inner product: $\langle a|b\rangle = |a\rangle^\dagger|b\rangle = a_1^* b_1 + a_2^* b_2 + \dots + a_n^* b_n$, $\langle \varphi|\varphi\rangle = 1$

Bloch sphere = valid Hilbert space, $r = 1$, $||\varphi\rangle| = 1$, $\langle\varphi|\varphi\rangle = 1$, $|\langle\varphi|| = ||\varphi\rangle^\dagger| = ||\varphi\rangle| = 1$

unitary matrices = preserve inner product $U|\varphi\rangle = |\varphi'\rangle \Rightarrow \langle\varphi'|\varphi'\rangle = (U|\varphi\rangle)^\dagger U|\varphi\rangle = \langle\varphi|\varphi\rangle = 1$

Outer & Tensor Products

outer product $|a\rangle\langle b| = \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}(b_1^* \dots b_n^*) = \begin{pmatrix} a_1 b_1^* & \dots & a_1 b_n^* \\ \vdots & \ddots & \vdots \\ a_n b_1^* & \dots & a_n b_n^* \end{pmatrix}$

$\sigma_x = \begin{pmatrix}0&1\\1&0\end{pmatrix} = \begin{pmatrix}0&1\\0&0\end{pmatrix} + \begin{pmatrix}0&0\\1&0\end{pmatrix} = \begin{pmatrix}1\\0\end{pmatrix}\begin{pmatrix}0&1\end{pmatrix} + \begin{pmatrix}0\\1\end{pmatrix}\begin{pmatrix}1&0\end{pmatrix} = |0\rangle\langle 1| + |1\rangle\langle 0|$

tensor product $|a\rangle \otimes |b\rangle = |ab\rangle = \begin{pmatrix} a_1 \begin{pmatrix}b_1\\b_2\end{pmatrix} \\ a_2\begin{pmatrix}b_1\\b_2\end{pmatrix}\end{pmatrix} = \begin{pmatrix}a_1b_1\\a_1b_2\\a_2b_1\\a_2b_2\end{pmatrix}$

$A\otimes B = \begin{pmatrix} a_{11}B & \cdots & a_{1n}B \\ \vdots & \ddots & \vdots \\ a_{m1}B & \cdots & a_{mn}B\end{pmatrix}$

Eigenvectors & Eigenvalues

$A|v\rangle = \lambda|v\rangle$, $|v\rangle$-eigenvector, λ-eigenvalue

$A|v\rangle - \lambda|v\rangle = 0 \Rightarrow (A-\lambda I)|v\rangle = 0$, $A-\lambda I$ is non-invertible $\Rightarrow \det(A-\lambda I) = 0$

Pauli-Z $\sigma_z = \begin{pmatrix}1&0\\0&-1\end{pmatrix}$, $\det(\sigma_z-\lambda I) = \lambda^2-1=0 \Rightarrow \lambda = \pm 1$ characteristic polynomial

$\lambda = 1$: $\begin{pmatrix}1&0\\0&-1\end{pmatrix}|v\rangle = |v\rangle \Rightarrow \begin{pmatrix}a\\-b\end{pmatrix} = \begin{pmatrix}a\\b\end{pmatrix} \Rightarrow b=0$, $a=1$ s.t. $\||v\rangle\| = 1$ $\quad \begin{pmatrix}1\\0\end{pmatrix} = |0\rangle$

$\lambda = -1$: $\begin{pmatrix}1&0\\0&-1\end{pmatrix}|v\rangle = -|v\rangle \Rightarrow \begin{pmatrix}a\\-b\end{pmatrix} = \begin{pmatrix}-a\\-b\end{pmatrix} \Rightarrow a=0$, $b=1$ s.t. $\||v\rangle\| = 1$ $\quad \begin{pmatrix}0\\1\end{pmatrix} = |1\rangle$

Hermitian matrix - linearly independent eigenvectors (# = dimension of vector space)

↳ distinct eigenvalues = orthogonal eigenvectors

Unitary matrix - eigenvectors form orthonormal basis for vector space

Matrix Exponentials

$U = e^{i\gamma H}$, $U^\dagger = (e^{i\gamma H})^\dagger = e^{-i\gamma H^\dagger}$, H-Hermitian $\Rightarrow H^\dagger = H$

$g(x) = \sum_{n=0}^{\infty} \frac{x^n}{n!} = e^x \Rightarrow e^{i\gamma H} = \sum_{n=0}^{\infty} \frac{(i\gamma H)^n}{n!}$

$\exists B$ s.t. $B^2 = I$ (involutory matrix) $\Rightarrow e^{i\gamma B} = \cos(\gamma) I + i\sin(\gamma) B$

$I\sum_{n=0}^{\infty} \frac{(-1)^n \gamma^{2n}}{(2n)!} + iB\sum_{n=0}^{\infty} \frac{(-1)^n \gamma^{2n+1}}{(2n+1)!} = \cos(\gamma) I + i\sin(\gamma) B$

$\sigma_x = \begin{pmatrix}0&1\\1&0\end{pmatrix}$, $\sigma_y = \begin{pmatrix}0&-i\\i&0\end{pmatrix}$, $\sigma_z = \begin{pmatrix}1&0\\0&-1\end{pmatrix}$ - Hermitian and Involutory

$e^{H}|v\rangle = \sum_{n=0}^{\infty} \frac{H^n|v\rangle}{n!} = \sum_{n=0}^{\infty} \frac{\lambda^n|v\rangle}{n!} = e^{\lambda}|v\rangle$

Chapter 1 - Quantum States & Qubits

1. Representing Qubit States

Qubit: $|0\rangle = \begin{pmatrix}1\\0\end{pmatrix}$, $|1\rangle = \begin{pmatrix}0\\1\end{pmatrix}$, $|q_0\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\i\end{pmatrix} = \frac{1}{\sqrt{2}}|0\rangle + \frac{i}{\sqrt{2}}|1\rangle$

Rule of Measurement

$p(|x\rangle) = |\langle x|\psi\rangle|^2$ "braket", $\langle x|$ - "bra", $|\psi\rangle$ - "ket"

$|q_0\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\i\end{pmatrix} \Rightarrow \langle 0|q_0\rangle = \frac{1}{\sqrt{2}} \Rightarrow |\langle 0|q_0\rangle|^2 = \frac{1}{2}$

$\langle\psi|\psi\rangle = 1$, $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \Rightarrow \alpha^2 + \beta^2 = 1$

$\begin{pmatrix}0\\i\end{pmatrix} = i|1\rangle \Rightarrow |\langle x|(i|1\rangle)|^2 = |i\langle x|1\rangle|^2 = |\langle x|1\rangle|^2$

global phase, $|\gamma| = 1 \Rightarrow |\langle x|(\gamma|a\rangle)|^2 = |\gamma\langle x|a\rangle|^2 = |\langle x|a\rangle|^2$

Bloch Sphere

$|q\rangle = \alpha|0\rangle + \beta|1\rangle$, $\alpha, \beta \in \mathbb{C}$, $|q\rangle = \alpha|0\rangle + e^{i\phi}\beta|1\rangle$, $\alpha, \beta, \phi \in \mathbb{R}$

$\sqrt{\alpha^2 + \beta^2} = 1$, $\sqrt{\sin^2 x + \cos^2 x} = 1 \Rightarrow \alpha = \cos\frac{\theta}{2}$, $\beta = \sin\frac{\theta}{2} \Rightarrow |q\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle$, $\theta, \phi \in \mathbb{R}$

$|+\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix} \Rightarrow \theta_+ = \frac{\pi}{2}$, $\phi_+ = 0$

2. Single Qubit Gates

The Pauli Gates

$X = \begin{pmatrix}0 & 1\\1 & 0\end{pmatrix} = |0\rangle\langle 1| + |1\rangle\langle 0|$, $X|0\rangle = |1\rangle$, NOT-gate, rotation by π around X-axis

$Y = \begin{pmatrix}0 & -i\\i & 0\end{pmatrix} = -i|0\rangle\langle 1| + i|1\rangle\langle 0|$, rotation by π around Y-axis

$Z = \begin{pmatrix}1 & 0\\0 & -1\end{pmatrix} = |0\rangle\langle 0| - |1\rangle\langle 1|$, rotation by π around Z-axis

Hadamard (H-) Gate

$H = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\1 & -1\end{pmatrix}$, $H|0\rangle = |+\rangle$, $H|1\rangle = |-\rangle$, $HZH = X$, transformation between X and Z bases

Phase (P-) Gate

$P(\phi) = \begin{pmatrix}1 & 0\\0 & e^{i\phi}\end{pmatrix}$, $\phi \in \mathbb{R}$, rotation of ϕ around Z-axis

$\mathbb{I}$, S, T - Gates

$\mathbb{I} = \begin{pmatrix}1 & 0\\0 & 1\end{pmatrix}$ - identity, $\mathbb{I} = XX$

$S = \begin{pmatrix} 1 & 0 \\ 0 & e^{\frac{i\pi}{2}} \end{pmatrix}$, $S^\dagger = \begin{pmatrix} 1 & 0 \\ 0 & e^{-\frac{\pi i}{2}} \end{pmatrix}$, $\sqrt{Z}$-Gate, P-Gate with $\phi = \frac{\pi}{2}$, $SS|q\rangle = Z|q\rangle$
$T = \begin{pmatrix} 1 & 0 \\ 0 & e^{\frac{i\pi}{4}} \end{pmatrix}$, $T^\dagger = \begin{pmatrix} 1 & 0 \\ 0 & e^{-\frac{\pi}{4}i} \end{pmatrix}$, $\sqrt[4]{Z}$-Gate, P-Gate with $\phi = \frac{\pi}{4}$

<u>U-Gate</u>

general single-qubit quantum gate: $U(\theta, \phi, \lambda) = \begin{pmatrix} \cos(\frac{\theta}{2}) & -e^{i\lambda}\sin(\frac{\theta}{2}) \\ e^{i\phi}\sin(\frac{\theta}{2}) & e^{i(\phi+\lambda)}\cos(\frac{\theta}{2}) \end{pmatrix}$
$U(\frac{\pi}{2}, 0, \pi) = H$, $U(0, 0, \lambda) = P(\lambda)$

Chapter 2 - Multiple Qubits & Entanglement

1. Multiple Qubits & Entangled States

Representing Multi-Qubit States

$|a\rangle = a_{00}|00\rangle + a_{01}|01\rangle + a_{10}|10\rangle + a_{11}|11\rangle = \begin{pmatrix} a_{00} \\ a_{01} \\ a_{10} \\ a_{11} \end{pmatrix}$ $\quad p(|00\rangle) = |\langle 00|a\rangle|^2 = |a_{00}|^2$

$|a_{00}|^2 + |a_{01}|^2 + |a_{10}|^2 + |a_{11}|^2 = 1$

$|a\rangle = \begin{pmatrix} a_0 \\ a_1 \end{pmatrix} \quad |b\rangle = \begin{pmatrix} b_0 \\ b_1 \end{pmatrix} \quad |ba\rangle = |b\rangle \otimes |a\rangle = \begin{pmatrix} b_0 \times \begin{pmatrix} a_0 \\ a_1 \end{pmatrix} \\ b_1 \times \begin{pmatrix} a_0 \\ a_1 \end{pmatrix} \end{pmatrix} = \begin{pmatrix} b_0 a_0 \\ b_0 a_1 \\ b_1 a_0 \\ b_1 a_1 \end{pmatrix}$

Single Qubit Gates on Multi-Qubit Statevectors

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

$X|q_1\rangle \otimes H|q_0\rangle = (X \otimes H)|q_1 q_0\rangle \quad X \otimes H = \begin{pmatrix} 0 & H \\ H & 0 \end{pmatrix}, \quad X \otimes S = \begin{pmatrix} 0 & S \\ S & 0 \end{pmatrix}$

Multi-Qubit Gates

CNOT - X-gate on second qubit (target) if state of first (control) is $|1\rangle$

input	00	01	10	11
output	00	11	10	01

$CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} \quad |a\rangle = \begin{pmatrix} a_{00} \\ a_{01} \\ a_{10} \\ a_{11} \end{pmatrix} \quad CNOT|a\rangle = \begin{pmatrix} a_{00} \\ a_{11} \\ a_{10} \\ a_{01} \end{pmatrix}$

$|0+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |01\rangle) \quad CNOT|0+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \rightarrow$ Bell state

2. Phase Kickback

$|++\rangle = \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle) \quad CNOT|++\rangle = |++\rangle$

$|-+\rangle = \frac{1}{2}(|00\rangle + |01\rangle - |10\rangle - |11\rangle) \quad CNOT|-+\rangle = |--\rangle = \frac{1}{2}(|00\rangle - |01\rangle - |10\rangle + |11\rangle)$

H-gate: $|+\rangle \rightarrow |0\rangle, \quad |-\rangle \rightarrow |1\rangle \quad H\,CNOT\,H|ab\rangle = CNOT|ba\rangle$

$X|-\rangle = -|-\rangle \quad CNOT|-0\rangle = |-0\rangle \quad CNOT|-1\rangle = -|-1\rangle \quad CNOT|-+\rangle = |--\rangle$

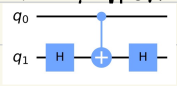
$T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix} \quad T|1\rangle = e^{i\pi/4}|1\rangle \quad |1+\rangle = \frac{1}{\sqrt{2}}(|10\rangle + |11\rangle)$

Controlled-$T = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & e^{i\pi/4} \end{pmatrix}$ $\quad$ Controlled-$T|1+\rangle = \frac{1}{\sqrt{2}}(|10\rangle + e^{i\pi/4}|11\rangle)$

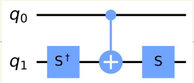
3. More Circuit Identities

Controlled-Z from CNOT

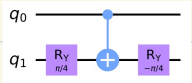
$HXH = Z, \quad HZH = X$



controlled-Z

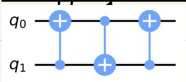


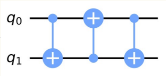
controlled-Y



controlled-H

Swapping Qubits



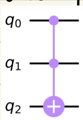


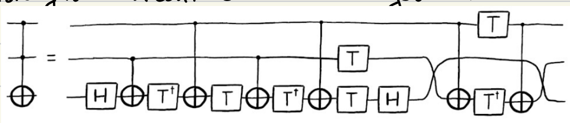
Controlled Rotations

$ABC = \mathbb{1}$, $e^{i\alpha} AZBZC = V$

The Toffoli

three-qubit gate - 2 controls and 1 target -> AND or NAND of controls





4. Proving Universality

4.1. Matrices

Outer Product

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

$M = \begin{pmatrix}m_{00}&m_{01}\\m_{10}&m_{11}\end{pmatrix} = m_{00}|0\rangle\langle 0| + m_{01}|0\rangle\langle 1| + m_{10}|1\rangle\langle 0| + m_{11}|1\rangle\langle 1|$

Unitary & Hermitian

Hermitian conjugate $M^\dagger$ - conjugate transpose of M

Unitary: $U^\dagger U = UU^\dagger = \mathbb{1}$ $\quad (\langle\varphi_0|U^\dagger)(U|\varphi_1\rangle) = \langle\varphi_0|U^\dagger U|\varphi_1\rangle = \langle\varphi_0|\varphi_1\rangle$

$\{|\varphi_j\rangle\}$ - orthonormal basis $\Rightarrow$ $\{|\psi_j\rangle = U|\varphi_j\rangle\}$ - orthonormal basis

$\Rightarrow U = \sum_j |\psi_j\rangle\langle\varphi_j|$

Hermitian: $H^\dagger = H$ (also X, Y, Z) (subset of Unitary)

$M = \sum_j \lambda_j |h_j\rangle\langle h_j|$ - diagonalization, λ_j - eigenvalues, $|h_j\rangle$ - eigenstates

$\lambda_j \lambda_j^* = 1$ since $UU^\dagger = \mathbb{1}$ (unitary), $H = H^\dagger \Rightarrow \lambda_j = \lambda_j^*$ (hermitian), $U = e^{iH}$

Pauli Decomposition

$|0\rangle\langle 0| = \frac{\mathbb{1}_2 + Z}{2}$ $\quad |1\rangle\langle 1| = \frac{\mathbb{1}_2 - Z}{2}$ $\quad X|0\rangle = |1\rangle \Rightarrow |0\rangle\langle 1| = \frac{X+iY}{2}$ $\quad |1\rangle\langle 0| = \frac{X-iY}{2}$

$M = \begin{pmatrix}m_{00}&m_{01}\\m_{10}&m_{11}\end{pmatrix} = \frac{m_{00}+m_{11}}{2}\mathbb{1}_2 + \frac{m_{01}+m_{10}}{2}X + i\frac{m_{01}-m_{10}}{2}Y + \frac{m_{00}-m_{11}}{2}Z$

4.2. Basic Gate Sets

Clifford Gates

$H = |+\rangle\langle 0| + |-\rangle\langle 1| = |0\rangle\langle +| + |1\rangle\langle -|$ $\quad |0\rangle \leftrightarrow |+\rangle$, $|1\rangle \leftrightarrow |-\rangle$ $\quad HXH = Z, \quad HZH = X$

$SXS^\dagger = Y, \quad SYS^\dagger = -X, \quad SZS^\dagger = Z$

U - Clifford, P - Pauli $\Rightarrow UPU^\dagger$ - Pauli

$ZXZ = -X, \quad ZYZ = -Y, \quad ZZZ = Z$

$CX\,(X \otimes \mathbb{1})\,CX = X \otimes X$

Non-Clifford Gates

$R_x(\theta), R_y(\theta), R_z(\theta)$

$R_x(\theta) = e^{i\frac{\theta}{2}X} \qquad UR_x(\theta)U^\dagger = e^{i\frac{\theta}{2}UXU^\dagger}$

Expanding Gate Set

$CX\,(R_x(\theta) \otimes \mathbb{1})\,CX = CX\, e^{i\frac{\theta}{2}(X \otimes \mathbb{1})} CX = e^{i\frac{\theta}{2} CX(X\otimes\mathbb{1})CX} = e^{i\frac{\theta}{2} X \otimes X}$

$(\mathbb{1} \otimes S)\, e^{i\frac{\theta}{2} X\otimes X} (\mathbb{1} \otimes S^\dagger) = e^{i\frac{\theta}{2} X \otimes Y}$

4.3. Proving Universality

$U = e^{i(aX + bZ)}, \quad R_x(\theta) = e^{i\frac{\theta}{2}X}, \quad R_z(\theta) = e^{i\frac{\theta}{2}Z} \Rightarrow R_x(2a) = e^{iaX}, \quad R_z(2b) = e^{ibZ}$

$e^{iaX} e^{ibZ} \neq e^{i(aX+bZ)}, \quad U = \lim_{n\to\infty} \left(e^{iaX/n} e^{ibZ/n}\right)^n, \quad e^{iaX/n} e^{ibZ/n} = e^{i(aX+bZ)/n} \quad O\left(\frac{1}{n^2}\right)$

5. Classical Computation

$f(x)$ - oracle

Boolean oracle: $U_f|x, \bar{0}\rangle = |x, f(x)\rangle$

Phase oracle: $P_f|x\rangle = (-1)^{f(x)}|x\rangle$

$V_f|x, \bar{0}, \bar{0}\rangle = |x, f(x), g(x)\rangle \Rightarrow V_f^\dagger U_f |x, 0, 0\rangle = V_f^\dagger |x, f(x), 0\rangle = |x, 0, g(x)\rangle$

$\Rightarrow V_f: |x, 0, 0, 0\rangle \to |x, f(x), g(x), 0\rangle \Rightarrow V_f: |x, f(x), g(x), 0\rangle \to |x, f(x), g(x), f(x)\rangle$

$V_f^\dagger: |x, f(x), g(x), 0\rangle \to |x, 0, 0, f(x)\rangle$

Chapter 3 - Quantum Protocols & Algorithms

1. Quantum Circuits

→ computational routine of coherent quantum operations on quantum data, such as qubits, and concurrent real-time classical computation

→ ordered sequence of quantum gates, measurements and resets

2. Deutsch-Josza Algorithm

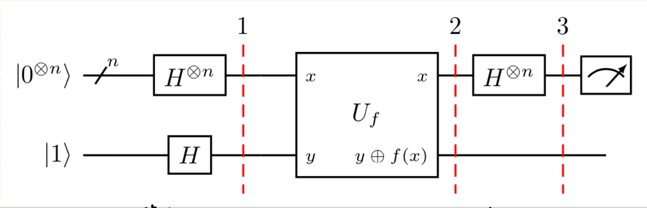
2.1 Problem

hidden boolean function f, input: string of bits - guaranteed to be constant or balanced

constant function - return all 0s or 1s for any input

balanced function - return 0s for exactly half of all inputs and 1s for the other half

2.2 Solution



$|\psi_0\rangle = |0\rangle^{\otimes n} \otimes |1\rangle$

$|\psi_1\rangle = \frac{1}{\sqrt{2^{n+1}}} \sum_{x=0}^{2^n-1} |x\rangle(|0\rangle - |1\rangle)$

quantum oracle:

$|x\rangle|y\rangle \longrightarrow |x\rangle|y \oplus f(x)\rangle$

$$|\psi_2\rangle = \frac{1}{\sqrt{2^{n+1}}} \sum_{x=0}^{2^n-1} |x\rangle(|f(x)\rangle - |1 \oplus f(x)\rangle) = \frac{1}{\sqrt{2^{n+1}}} \sum_{x=0}^{2^n-1} (-1)^{f(x)} |x\rangle(|0\rangle - |1\rangle)$$

$$|\psi_3\rangle = \frac{1}{2^n} \sum_{x=0}^{2^n-1} (-1)^{f(x)} \left[\sum_{y=0}^{2^n-1} (-1)^{x \cdot y} |y\rangle\right] = \frac{1}{2^n} \sum_{y=0}^{2^n-1} \left[\sum_{x=0}^{2^n-1} (-1)^{f(x)} (-1)^{x \cdot y}\right] |y\rangle$$

measurement: $|0\rangle^{\otimes n} = \left|\frac{1}{2^n} \sum_{x=0}^{2^n-1} (-1)^{f(x)}\right|^2 = \begin{cases} 1 \to \text{constant} \\ 0 \to \text{balanced} \end{cases}$

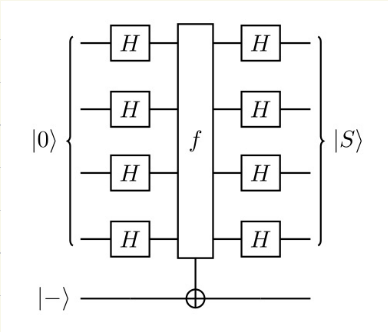
3. Bernstein-Vazirani Algorithm

3.1. Problem

black-box function f, input: string of bits

$\exists!\, s$ s.t. $f(x) = s \cdot x \pmod 2$

3.2. Solution



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

$$|x\rangle \xrightarrow{f} (-1)^{s \cdot x} |x\rangle$$

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

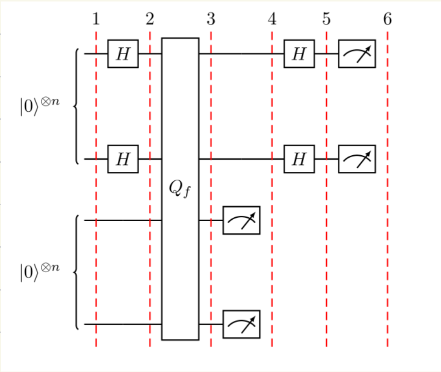
4. Simon's Algorithm

4.1. Problem

unknown black-box function f – guaranteed to be one-to-one or two-to-one

two-to-one mapping – hidden bitstring b, $f(x_1) = f(x_2) \Rightarrow x_1 \oplus x_2 = b$, $b = 0 \ldots 0$ = one-to-one

4.2. Solution



$|x\rangle|y\rangle \xrightarrow{Q_f} |x\rangle|y \oplus f(x)\rangle$

$|\psi_1\rangle = |0\rangle^{\otimes n}|0\rangle^{\otimes n}$

$|\psi_2\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle|0\rangle^{\otimes n}$

$|\psi_3\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle|f(x)\rangle$

$|\psi_4\rangle = \frac{1}{\sqrt{2}}(|x\rangle + |y\rangle)$, where $y = x \oplus b$

$|\psi_5\rangle = \frac{1}{\sqrt{2^{n+1}}} \sum_{z \in \{0,1\}^n} \left[(-1)^{x \cdot z} + (-1)^{y \cdot z}\right]|z\rangle$

$(-1)^{x \cdot z} = (-1)^{y \cdot z} \rightarrow$ output from first register

$\hookrightarrow x \cdot z = y \cdot z \rightarrow x \cdot z = (x \oplus b) \cdot z \rightarrow x \cdot z = x \cdot z \oplus b \cdot z$

$\Rightarrow b \cdot z = 0 \pmod 2$

5. Quantum Fourier Transform

$$y_k = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} x_j \omega_N^{jk} \quad \text{where } \omega_N^{jk} = e^{2\pi i \frac{jk}{N}}$$

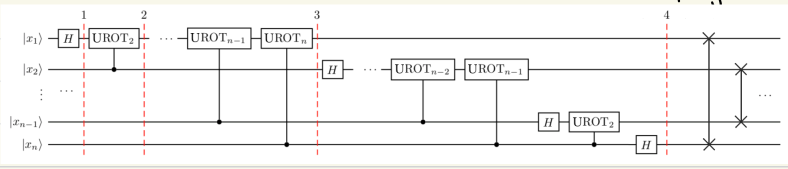
$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \Rightarrow \begin{cases} y_0 = \frac{1}{\sqrt{2}}(\alpha \omega_2^{0 \cdot 0} + \beta \omega_2^{1 \cdot 0}) = \frac{1}{\sqrt{2}}(\alpha + \beta) \\ y_1 = \frac{1}{\sqrt{2}}(\alpha \omega_2^{1 \cdot 0} + \beta \omega_2^{1 \cdot 1}) = \frac{1}{\sqrt{2}}(\alpha - \beta) \end{cases} \Rightarrow U_{QFT}|\psi\rangle = \frac{1}{\sqrt{2}}(\alpha + \beta)|0\rangle + \frac{1}{\sqrt{2}}(\alpha - \beta)|1\rangle$$

$$U_{QFT_2} \equiv H, \quad H|\psi\rangle \equiv \tilde{\alpha}|0\rangle + \tilde{\beta}|1\rangle$$

$$\begin{aligned} QFT_N|x\rangle &= \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} \omega_N^{xy}|y\rangle \\ &= \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} e^{2\pi i \frac{xy}{2^n}}|y\rangle, \quad \omega_N^{xy} = e^{2\pi i \frac{xy}{N}}, \ N = 2^n \\ &= \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} e^{2\pi i \left(\sum_{k=1}^{n} y_k / 2^k\right) x}|y_1 \ldots y_n\rangle, \quad y = y_1 \ldots y_n, \ \frac{y}{2^n} = \sum_{k=1}^{n} \frac{y_k}{2^k} \\ &= \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} \prod_{k=1}^{n} e^{2\pi i \frac{x y_k}{2^k}}|y_1 \ldots y_n\rangle \\ &= \frac{1}{\sqrt{N}} \bigotimes_{k=1}^{n} \left(|0\rangle + e^{2\pi i \frac{x}{2^k}}|1\rangle\right) \\ &= \frac{1}{\sqrt{N}} \left(|0\rangle + e^{\frac{2\pi i}{2} x}|1\rangle\right) \otimes \left(|0\rangle + e^{\frac{2\pi i}{2^2} x}|1\rangle\right) \otimes \ldots \otimes \left(|0\rangle + e^{\frac{2\pi i}{2^{n-1}} x}|1\rangle\right) \otimes \left(|0\rangle + e^{\frac{2\pi i}{2^n} x}|1\rangle\right) \end{aligned}$$

$$H|x_k\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + e^{\frac{2\pi i}{2} x_k}|1\rangle\right)$$

$$CROT_k = \begin{bmatrix} I & 0 \\ 0 & UROT_k \end{bmatrix}, \quad UROT_k = \begin{bmatrix} 1 & 0 \\ 0 & e^{\frac{2\pi i}{2^k}} \end{bmatrix} \qquad \begin{aligned} CROT_k|0 x_j\rangle &= |0 x_j\rangle \\ CROT_k|1 x_j\rangle &= e^{\frac{2\pi i}{2^k} x_j}|1 x_j\rangle \end{aligned}$$



1) $H_1|x_1x_2\ldots x_n\rangle = \frac{1}{\sqrt2}\left[|0\rangle + e^{\frac{2\pi i}{2}x_1}|1\rangle\right]\otimes|x_2x_3\ldots x_n\rangle$

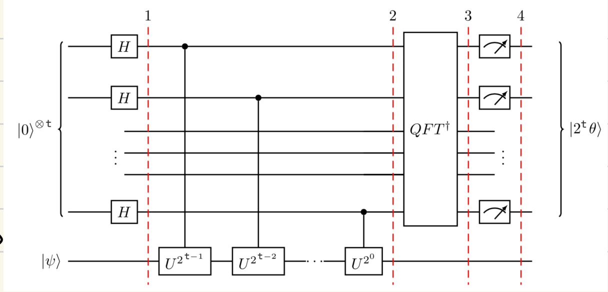
2) $\frac{1}{\sqrt2}\left[|0\rangle + e^{\frac{2\pi i}{2^2}x_2+\frac{2\pi i}{2}x_1}|1\rangle\right]\otimes|x_2x_3\ldots x_n\rangle$

3) $\frac{1}{\sqrt2}\left[|0\rangle + e^{\frac{2\pi i}{2^n}x_n+\frac{2\pi i}{2^{n-1}}x_{n-1}+\ldots+\frac{2\pi i}{2^2}x_2+\frac{2\pi i}{2}x_1}|1\rangle\right]\otimes|x_2x_3\ldots x_n\rangle$

$x = 2^{n-1}x_1+2^{n-2}x_2+\ldots+2^1x_{n-1}+2^0x_n \Rightarrow \frac{1}{\sqrt2}\left[|0\rangle+e^{\frac{2\pi i}{2^n}x}|1\rangle\right]\otimes|x_2x_3\ldots x_n\rangle$

4) $\frac{1}{\sqrt2}\left[|0\rangle+e^{\frac{2\pi i}{2^n}x}|1\rangle\right]\otimes\frac{1}{\sqrt2}\left[|0\rangle+e^{\frac{2\pi i}{2^{n-1}}x}|1\rangle\right)\otimes\ldots\otimes\frac{1}{\sqrt2}\left(|0\rangle+e^{\frac{2\pi i}{2^2}x}|1\rangle\right]\otimes\frac{1}{\sqrt2}\left[|0\rangle+e^{\frac{2\pi i}{2^1}x}|1\rangle\right]$

6. Quantum Phase Elimination



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

$|\psi_0\rangle = |0\rangle^{\otimes n}|\psi\rangle$

$|\psi_1\rangle = \frac{1}{\sqrt{2^n}}(|0\rangle+|1\rangle)^{\otimes n}|\psi\rangle$

$|\psi_2\rangle = \frac{1}{\sqrt{2^n}}\sum_{k=0}^{2^n-1} e^{2\pi i\theta k}|k\rangle\otimes|\psi\rangle$

$|\psi_3\rangle = \frac{1}{2^n}\sum_{x=0}^{2^n-1}\sum_{k=0}^{2^n-1} e^{-\frac{2\pi i k}{2^n}(x-2^n\theta)}|x\rangle\otimes|\psi\rangle$

$|\psi_4\rangle = |2^n\theta\rangle|\psi\rangle$

7. Shor's Algorithm

7.1. Problem

periodic function: $f(x)=a^x \bmod N$, $a,N\in\mathbb{N}>1$, $a<N$, a,N - no common factor

period/order r, $\min_{r\neq0} a^r \bmod N = 1$

7.2. Solution

$U|u_0\rangle = |u_0\rangle$

$U|y\rangle \equiv |ay \bmod N\rangle$, $|u_0\rangle = \frac{1}{\sqrt r}\sum_{k=0}^{r-1}|a^k \bmod N\rangle \to$ eigenstate of U, eigenvalue $=1$

$|u_1\rangle = \frac{1}{\sqrt r}\sum_{k=0}^{r-1} e^{-\frac{2\pi i k}{r}}|a^k \bmod N\rangle \Rightarrow U|u_1\rangle = e^{\frac{2\pi i}{r}}|u_1\rangle$

$|u_s\rangle = \frac{1}{\sqrt r}\sum_{k=0}^{r-1} e^{-\frac{2\pi i s k}{r}}|a^k \bmod N\rangle \Leftrightarrow U|u_s\rangle = e^{\frac{2\pi i s}{r}}|u_s\rangle$, $0\le s\le r-1 \Rightarrow \frac{1}{r}\sum_{s=0}^{r-1}|u_s\rangle = |1\rangle$