Linear algebra

For unitary matrix U, (normalised) eigenvectors $|v_i\rangle$ and eigenvalues λ_i: $\boxed{U|v_i\rangle = \lambda_i|v_i\rangle}$.

For diagonalisable matrix, spectral decomposition $U = \sum_{i=1}^{n} \lambda_i |v_i\rangle \langle v_i|$.

Unitary $A^\dagger A = I$, Hermitian $A = A^\dagger \subseteq$ normal matrices $A^\dagger A = AA^\dagger$.

Postulates of quantum mechanics

Superposition, interference

Entanglement: non-separability

Concepts in quantum mechanics

Measurement and the Helstrom-Holevo bound $p \leq \frac{1+\sin\theta}{2}$, where $|\langle\psi_a|\psi_b\rangle| = \cos\theta$.

The no-signalling principle: after measurement, the entanglement is collapsed, thus not possible to transmit information.

The no-cloning principle: impossible to copy an unknown quantum state. $\nexists U . U(|\psi\rangle|0\rangle) = |\psi\rangle|\psi\rangle$.

The no-deleting principle: impossible to delete one of the unknown quantum state copies. $\nexists \tilde{U} . \tilde{U}(|\psi\rangle|\psi\rangle) = |\psi\rangle|0\rangle$.

Quantum circuits

Universal gate set: $\{H, T, CNOT\}$, where $\pi/8$ gate is T. $\pi/4$ gate is S. (not self-invertible)

Phase gate $S = T^2$, $Z = S^2$, $X = HZH$, $Y = iXZ = SXSZ$.

- proof for $Z = HXH$ (L8. search)
  - either by matrix multiplication.
  - or geometric interpretation (X/Z: rotate 180 degree about x/z-axis, H: swap x and z axis).

by self-inverse, $CNOT = CX = (I \otimes H) \times CZ \times (I \otimes H)$.

SWAP can be decomposed into 3 CNOTs.

Entanglement circuits via Hadamard-CNOT combination $\boxed{\text{CNOT}(H \otimes I)|00\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)}$

Quantum information applications

Teleportation (send *a qubit* via two bits)

Super**dense** coding (send **two bits** via one qubit) $\{I, X, Z, XZ\} \rightarrow \mathrm{CNOT} + \mathrm{Hadamard}.$

Deutsch-Jozsa algorithm

$\boxed{f:\{0,1\}^n \rightarrow \{0,1\}}$, which is either constant or balanced.

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

Proof: as $|x\rangle = |x_1...x_n\rangle$, where $x_i \in \{0,1\}$ and

$$\begin{aligned} H|x_i\rangle &= \frac{1}{\sqrt{2}}(|0\rangle + (-1)^{x_i}|1\rangle) \\ &= \frac{1}{\sqrt{2}}(|z_1 = 0\rangle + (-1)^{x_i}|z_j = 1\rangle) \\ &= \frac{1}{\sqrt{2}}((-1)^{x_i\times 0}|z_1 = 0\rangle + (-1)^{x_i\times 1}|z_2 = 1\rangle) \\ &= \frac{1}{\sqrt{2}}((-1)^{x_i\times z_1}|z_1 = 0\rangle + (-1)^{x_i\times z_2}|z_2 = 1\rangle) \\ &= \frac{1}{\sqrt{2}}\sum_{z_j\in\{0,1\}}(-1)^{x_i\times z_j}|z_j\rangle \end{aligned}$$

$H^{\otimes n}|x_1...x_n\rangle = \otimes_i(H|x_i\rangle)$, and the power of the function is $\sum_i x_i \times z_i = x\cdot z$, we are done.

Quantum Search

Grover's algorithm

QFT & QPE

Quantum Fourier Transform (QFT)

$|x\rangle \rightarrow |y\rangle$: $\sum_{j=0}^{N-1} x_j|j\rangle \rightarrow \sum_{k=0}^{N-1} y_k|k\rangle$, where $\boxed{y_k = \frac{1}{\sqrt{N}}\sum_{j=0}^{N-1} w^{jk}x_j}$ and $w^{jk} = e^{i\frac{2\pi}{N}jk}$.

In the matrix form, we have the following transformation,

$$\begin{bmatrix} y_0 \\ y_1 \\ y_2 \\ \dots \\ y_N \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & \omega & \omega^2 & \dots & \omega^{N-1} \\ 1 & \omega^2 & \omega^4 & \dots & \omega^{2(N-1)} \\ 1 & \dots & \dots & \dots & \dots \\ 1 & \omega^{N-1} & \omega^{2(N-1)} & \dots & \omega^{(N-1)(N-1)} \end{bmatrix} \cdot \begin{bmatrix} x_0 \\ x_1 \\ x_2 \\ \dots \\ x_N \end{bmatrix}, \text{where } \omega = e^{i\frac{2\pi}{N}}.$$

The dimension of Hilbert space for n qubits $N = 2^n$. The sinusoid's frequency $f = \frac{k}{N}$, i.e., k cycles per N samples.

inverse QFT (iQFT)

$|y\rangle \to |x\rangle$: $\sum_{k=0}^{N-1} y_k |k\rangle \to \sum_{j=0}^{N-1} x_j |j\rangle$, where $\boxed{x_j = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} w^{-jk} y_k}$ and $w^{-jk} = e^{-i\frac{2\pi}{N}jk}$.

Note that the normalizing terms should be a product of $\frac{1}{N}$, where the above satisfies unitary. The exponential term is negated in one of the two.

Quantum Phase Estimation (QPE)

precision up to t bits. If given the eigenvector $|u\rangle$ of U and eigenvalue $e^{i2\pi\phi}$ with **phase** $\phi \in [0, 1)$, we have $U|u\rangle = e^{i2\pi\phi}|u\rangle$.

- preparation
  - 1^{st} register: $H^{\otimes t}|0\rangle^{\otimes t} = \frac{1}{\sqrt{2^t}} \sum_{x\in\{0,1\}^t} |x\rangle$ (superposition)
  - 2^{nd} register: the (superposition of) given eigenvector(s) $|u\rangle$ with eigenvalue $e^{i2\pi\phi}$,
- oracle U^j on the 1^{st} register (Entanglement)
  - $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \to \frac{1}{\sqrt{2}}(|0\rangle + (e^{i2\pi\phi})^j|1\rangle)$
  - $\frac{1}{\sqrt{2^t}} \sum_{x=0}^{2^t-1} |x\rangle \to \frac{1}{\sqrt{2^t}} \sum_{j=0}^{2^t-1} (e^{i2\pi\phi})^j|j\rangle$
  - 2^{nd} register: respective $|u\rangle$ with eigenvalue $e^{i2\pi\phi}$ and phase ϕ.
- iQFT (Interference)
- measurement
  - 1^{st} register: t bits approximation of $|\tilde{\phi}\rangle$
  - 2^{nd} register: $|u\rangle$ with phase ϕ.

Application: factoring

order finding: for coprime x and N, find $x^r \equiv 1 \mod N$, where r is the least positive integer.

$U|r\rangle = |(x\cdot r) \mod N\rangle \implies$ For eigenstates $s \in [0, r-1]$, we have eigenvectors $|u_s\rangle = \frac{1}{\sqrt{r}} \sum_{j=0}^{r-1} e^{-i2\pi\frac{s}{r}} j|x^j \mod N\rangle$ with **phase** $\phi = \frac{s}{r}$.

Use QPE, 2^{nd} register prepared with equal superposition of unknown eigenvectors $\frac{1}{\sqrt{r}} \sum_{j=0}^{r-1} |u_j\rangle = |1\rangle$ (shallow-depth quantum circuit X).

factoring: for composite integer N, $N = p \cdot q$, where p and q are prime numbers.

Shor's algorithm

Application: quantum chemistry

Trotter formula: $U = e^{-i(H_1+H_2)t} = U_1U_2 = e^{-iH_1t}e^{-iH_2t} + O(t^2)$, where U_1 and U_2 don't commute.

Projective measurement with (normalized) eigenvectors

Ground state energy estimation $|e_0\rangle$ of a H with eigenvalue $\lambda_0 = E_0$.

Use QPE, 2^{nd} register should be prepared as close to the eigenvector such that it's sufficiently dominated by the ground state $|e_0\rangle$ (L15. adiabatic state preparation).

Fault tolerance

bit-flip, phase-flip, Shor code, Steane code

Fault tolerance threshold $p_{th} = \frac{1}{c}$, for suppressed error rate $p = cp_e^2 + O(p_e^3)$. Per-gate error rate $\frac{(cp_e)^{2^k}}{c}$ after k concatenation.