Linear algebra

Inner product $\langle\psi| \times |\phi\rangle = \langle\psi|\phi\rangle = \sum_{i=1}^{n} \psi_i^* \phi_i$. Outer product $|\psi\rangle\langle\phi| = \sum_{i=1}^{n} \sum_{j=1}^{n} \psi_i \phi_j^* |i\rangle\langle j|$.

Tensor / Kronecker product $|\psi\rangle \otimes |\phi\rangle = |\psi_1\phi, \psi_2\phi, ..., \psi_n\phi\rangle$.

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

Hadamard / Element-wise product $|\psi\rangle \circ |\phi\rangle = |\psi\rangle \odot |\phi\rangle = |\psi\phi\rangle = |\psi_1\phi_1, \psi_1\phi_2, ..., \psi_n\phi_n\rangle$.

$$A \circ B = A \odot B = \begin{bmatrix} a_{11}b_{11} & \cdots & a_{1n}b_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1}b_{m1} & \cdots & a_{mn}b_{mn} \end{bmatrix}.$$

Eigenvalues λ_i / (normalised) eigenvectors $|v_i\rangle$ $\boxed{U|v_i\rangle = \lambda_i|v_i\rangle}$, for unitary matrix U.

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

Unitary $\cap$ Hermitian: $A^2 = I$ (self-inverse), e.g. X, Y, Z, H.

$\subseteq$ Hermitian $A = A^\dagger$ (self-adjoint) $\vee$ **Unitary** $A^\dagger A = I \implies A^{-1} = A^\dagger$ (unique inverse).

$\subseteq$ 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: $\{H, T, CNOT\}$. Pauli gates $X = HZH$, $Y = iXZ = SXSZ$.

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

Rotation $R_k = \text{diag}(1, e^{i\frac{2\pi}{2^k}})$, $R_k^\dagger = \text{diag}(1, e^{-i\frac{2\pi}{2^k}})$. $R_0 = I$, $R_1 = Z$, $R_2 = S$, $R_3 = T$, ...

$R_z(\theta) = \text{diag}(e^{-i\frac{\theta}{2}}, e^{i\frac{\theta}{2}})$, ignoring the global phase.

$$
\begin{aligned}
T &= \text{diag}(1, e^{i\frac{\pi}{4}}) && = R_3 = R_z(\frac{\pi}{4}) = e^{i\frac{\pi}{8}}\text{diag}(e^{-i\frac{\pi}{8}}, e^{i\frac{\pi}{8}}). \\
S = T^2 &= \text{diag}(1, e^{i\frac{\pi}{2}} = i) && = R_2 = R_z(\frac{\pi}{2}) = e^{i\frac{\pi}{4}}\text{diag}(e^{-i\frac{\pi}{4}}, e^{i\frac{\pi}{4}}). \\
Z = S^2 &= \text{diag}(1, e^{i\pi} = -1) && = R_1 = R_z(\pi) = e^{i\frac{\pi}{2}}\text{diag}(e^{-i\frac{\pi}{2}}, e^{i\frac{\pi}{2}}). \\
I = Z^2 &= \text{diag}(1, 1) && = R_0 = R_z(0).
\end{aligned}
$$

[T, S are not self-invertible and Z is self-inverse].

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

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.

sender: $|00\rangle \rightarrow^{H\otimes I + \text{CNOT}}_{superposition}$ Bell state $\rightarrow^{\{I,X,Z,XZ\}}_{\text{two bits}}$ Bell states.

receiver: Bell states $\rightarrow^{\text{CNOT}+H\otimes I}_{interference}$ two bits.

Lecture 7: Deutsch-Jozsa algorithm

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

- Prepare state: $|\psi\rangle|-\rangle$.
  - where the uniform superposition $|\psi\rangle = |+\rangle^{\otimes n} = \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle$ of all $N = 2^n$ states.
- Unitary operation U_f, a phase operator on the state $|x\rangle$,

- $U_f|x\rangle|y\rangle = |x\rangle|y \oplus f(x)\rangle$, where $y \in \{0,1\}$.
- $U_f|x\rangle|-\rangle = (-1)^{f(x)}|x\rangle|-\rangle$.

- Interference $H^{\otimes n}$ and measure the first n qubits in $|0\rangle^{\otimes n}$ basis.

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

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.

Lecture 8: Grover's search

- Quadratic speedup over unstructured classical search, from $O(N)$ to $O(\sqrt{N})$.
- M is the number of solutions (marked states $f(x) = 1$) to the search problem.
- Prepare state: $|\psi\rangle|-\rangle$.
  - where the uniform superposition $|\psi\rangle = |+\rangle^{\otimes n} = \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle$ of all $N = 2^n$ states.

- With the target state $|x_t\rangle = \frac{1}{\sqrt{M}} \sum_{x \text{ s.t. } f(x)=1} |x\rangle$,

$$\begin{aligned}
|\psi\rangle|-\rangle &= \frac{1}{\sqrt{N}}[\sum_{x \text{ s.t. } f(x)=0} |x\rangle + \sum_{x \text{ s.t. } f(x)=1} |x\rangle] \\
&= \frac{1}{\sqrt{N}}[\sum_{x \text{ s.t. } f(x)=0} |x\rangle + \sqrt{M}\frac{1}{\sqrt{M}} \sum_{x \text{ s.t. } f(x)=1} |x\rangle] \\
&= \frac{1}{\sqrt{N}}[\sum_{x \text{ s.t. } f(x)=0} |x\rangle + \sqrt{M}|x_t\rangle]
\end{aligned}$$

- Each iteration $(W \otimes I)V$: rotate the state towards the target state $|x_t\rangle$ by 2θ, where $\theta = \arcsin \frac{\sqrt{M}}{\sqrt{N}}$.
  - Oracle V flips the sign of the target state $|x_t\rangle$, i.e. $V|x\rangle = (-1)^{\mathbb{I}(x=x_t)}|x\rangle$.
  - Diffusion operator $W = 2|\psi\rangle\langle\psi| - I$, rotating $|\psi'\rangle = V|\psi\rangle$ around the axis $|\psi\rangle$.
    - reflected vector: $|\psi''\rangle = 2|\psi\rangle\langle\psi||\psi'\rangle - |\psi'\rangle$, where the former is the projected vector of $|\psi'\rangle$ onto the axis $|\psi\rangle$.

```
|a> = |psi> <psi|psi'>, projected vector
|b> = 2|psi> <psi|psi'>,
|psi''> = |b> - |psi'>,  by parallelogram.
        = 2 |psi> <psi|psi'> - |psi'>.

    /> |psi''>
   /
  /  |a>   |b>
 ---->|----->-----> |psi>
  \   |   /> |psi''>
   \  |  /
    \ | /
     \> |psi'>
```

- After n_{it} iterations, the angle between the final state and the target state is $(2n_{it}+1)\theta$.
  - $n_{it} = \frac{\frac{\pi}{2}-\theta}{2\theta} = \frac{\pi}{4\theta} \approx \frac{\pi}{4\sin\theta}$.
  - the final state is $\frac{1}{\sqrt{N}}[\cos((2n_{it}+1)\theta)\sum_{x \text{ s.t. } f(x)=0}|x\rangle + \sin((2n_{it}+1)\theta)|x_t\rangle]$.
  - the probability of measuring the target state is $\sin^2((2n_{it}+1)\theta)$.

QFT & QPE

QFT transforms a sequence of N complex numbers $\{x\}$ into another $\{y\}$ of the same length,

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

- The normalization term is $\frac{1}{N}$ and exponential term is negated in DFT.
  - here, we use $\frac{1}{\sqrt{N}}$ to satisfy the unitary condition, where the dimension of Hilbert space for n qubits is $N = 2^n$.

- The time series coefficients x_j are transformed into the frequency domain coefficients y_k.
  - DFT is the change of basis operator that converts from euclidean basis to the Fourier basis.
  - each y_k corresponds to how much of the sinusoid with frequency $f = \frac{k}{N}$ [cycles per sample] is present in the signal.
  - $w^{jk} = e^{i\frac{2\pi}{N}jk} = \cos(\frac{2\pi k}{N}j) + i\sin(\frac{2\pi k}{N}j)$, forming an orthogonal basis over the space of N complex vectors.
  - note that $w^N = e^{i2\pi} = 1$.

Alternatively, we can express the QFT as a matrix transformation $\mathbf{M}$, where N is the dimension of the Hilbert space.

The DFT is thus $y = \mathbf{M}x$, which in the matrix form is expressed as,

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

The matrix $\mathbf{M}$ can be expressed as a sum of outer products of the basis states $|k\rangle$, and $\langle j|$,

$$\mathbf{M} = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} \sum_{k=0}^{N-1} \omega^{jk} |k\rangle\langle j|.$$

where the outer product maps the state from $|j\rangle$ to $|k\rangle$,

$$\mathbf{M}|j\rangle = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} \omega^{jk} |k\rangle\langle j|j\rangle,$$

$$|j\rangle \to^{\mathbf{M}} \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} \omega^{jk} |k\rangle.$$

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 $w^{-jk} = e^{-i\frac{2\pi}{N}jk}$.

- The exponential term is negated from the QFT.

Quantum Phase Estimation (QPE)

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

- 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: $U = e^{-i(H_1+H_2)t} = U_1 U_2 = e^{-iH_1 t} e^{-iH_2 t} + O(t^2)$, 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.