basis $|x\rangle_n$

for $0 \le x < 2^n$

an n-qubit state is a unit vector in $\mathbb{C}^{2^n}$

and an operation is a unitary matrix.

$\langle Ux | Uy \rangle = \langle x | y \rangle$

We can also <u>measure</u> a state

Born Rule: if

$$|\psi\rangle_n = \sum_{0 \le x < 2^n} \alpha_x |x\rangle_n$$

$p(x)$ is $|\alpha_x|^2$

if $|\psi\rangle_2 = 0|00\rangle + \frac{1}{2}|01\rangle + \frac{i}{2}|10\rangle + \frac{-1}{\sqrt{2}}|11\rangle$

$0^2 + \frac{1}{2}^2 + \frac{i}{2}^2 + \frac{-1}{\sqrt{2}}^2 = 0 + \frac{1}{4} + \frac{1}{4} + \frac{1}{2} = 1$

so this is a unit vector.

Take a measurement

$P(00) = |0|^2 = 0$

$P(01) = |\frac{1}{2}|^2 = \frac{1}{4}$

$P(10) = |\frac{i}{2}|^2 = \frac{1}{4}$

$P(11) = |\frac{-1}{\sqrt{2}}|^2 = \frac{1}{2}$.

now the state is

$0|00\rangle + 0|01\rangle + 1|10\rangle + 0|11\rangle$

$= |10\rangle$

Prepare a state

$n+m$ qubit state

n-qubit input register

m-qubit output register

pure state: $|x\rangle_n |y\rangle_m$.

measure to get pure state

apply X gate to each 1,

to get the pure state

$|0\rangle_n |0\rangle_m$.

given a function f: n-bit $\to$ m-bit

define

$$U_f(|x\rangle_n |y\rangle_m) = |x\rangle_n |f(x) \oplus y\rangle_m$$

This is reversible, so it's a unitary operator

Then

$$U_f(|x\rangle_n |0\rangle_m) = |x\rangle_n |f(x) \oplus 0\rangle_m$$

$$= |x\rangle_n |f(x)\rangle_m$$

Recall $H \leftrightarrow \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}$

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

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

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

$$|0\rangle \leftrightarrow \begin{bmatrix}1\\0\end{bmatrix}$$

$$H|0\rangle \leftrightarrow \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}\begin{bmatrix}1\\0\end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\1\end{bmatrix} \leftrightarrow \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

$$H|1\rangle \leftrightarrow \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}\begin{bmatrix}0\\1\end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\-1\end{bmatrix} \leftrightarrow \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

$$(H \otimes H)(|0\rangle|0\rangle) = H(|0\rangle) \otimes H(|0\rangle)$$

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

$$= \frac{1}{2}\cancel{(|0\rangle^2 + 2|0\rangle|1\rangle + |1\rangle^2)}$$

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

even superposition of all 4 states

$$H^{\otimes n}|0\rangle_n = \frac{1}{2^{n/2}} \sum_{x \le 0 < 2^n} |x\rangle_n.$$

even superposition of all 2^n states.

Preparing a quantum computer:

1) Measure and flip so state is

$$|0\rangle_n |0\rangle_m$$

2) $(H^{\otimes n} \otimes \mathbb{1})(|0\rangle_n |0\rangle_m) = (H^{\otimes n}(|0\rangle_n)) \otimes |0\rangle_m$

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

3) Apply U_f

$$U_f\left(\frac{1}{2^{n/2}} \sum_{x=0}^{2^n-1} (|x\rangle_n |0\rangle_m) \right) = \frac{1}{2^{n/2}} \sum_{x=0}^{2^n-1} U_f(|x\rangle_n |0\rangle_m)$$

$$= \frac{1}{2^{n/2}} \sum_{x=0}^{2^n-1} |x\rangle_n |f(x)\rangle_m .$$

No-Cloning Theorem

Thm: Cannot copy quantum states

There is no unitary $U : \mathbb{C}^{2^{2n}} \to \mathbb{C}^{2^{2n}}$

that satisfies $U(|\psi\rangle_n |0\rangle_n) = U(|\psi\rangle_n |\psi\rangle_n)$

$\forall\ |\psi\rangle_n$.

Pf/ Suppose U exists, and ψ, φ are distinct.

$$U\big((a|\psi\rangle + b|\varphi\rangle)|0\rangle\big) = (a|\psi\rangle + b|\varphi\rangle)(a|\psi\rangle + b|\varphi\rangle)$$

$$= a^2|\psi\rangle|\psi\rangle + ab|\psi\rangle|\varphi\rangle + ab|\varphi\rangle|\psi\rangle + b^2|\varphi\rangle.$$

But!

$$U\big((a|\psi\rangle + b|\varphi\rangle)|0\rangle\big) = a\,U(|\psi\rangle|0\rangle) + b\,U(|\varphi\rangle|0\rangle)$$

$$= a|\psi\rangle|\psi\rangle + b|\varphi\rangle|\varphi\rangle$$

These are only the same if one of a, b is 0 other is 1.

Quantum Fourier Transform

If $f: \mathbb{Z}/2^n\mathbb{Z} \to \mathbb{C}$

Then the discrete Fourier transform is

$$\tilde{f}(x) = \frac{1}{2^{n/2}} \sum_{y=0}^{2^n-1} e^{2\pi i xy/2^n} f(y).$$

convert btwn time and frequency

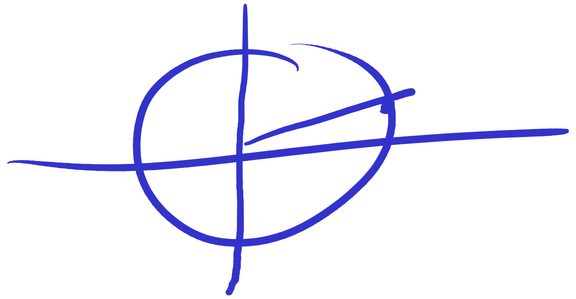
Quantum Fourier transform:

$$U_{FT}|x\rangle_n = \frac{1}{2^{n/2}} \sum_{y=0}^{2^n-1} e^{2\pi i xy/2^n} |y\rangle_n$$

$$= \frac{1}{2^{n/2}} \sum_{y=0}^{2^n-1} \left(e^{2\pi i/2^n}\right)^{xy} |y\rangle_n$$

$e^{2\pi i/K}$ is a Kth root of unity

$1/K$ around unit circle



$$U_{FT} \sum_{x=0}^{2^n-1} f(x)|x\rangle = \sum_{x=0}^{2^n-1} \tilde{f}(x)|x\rangle.$$

naive FT: $O(2^{2n}) = O(2^n \cdot 2^n)$

Fast FT: $O(n2^n)$

QFT: $O(n^2)$. Very fast.