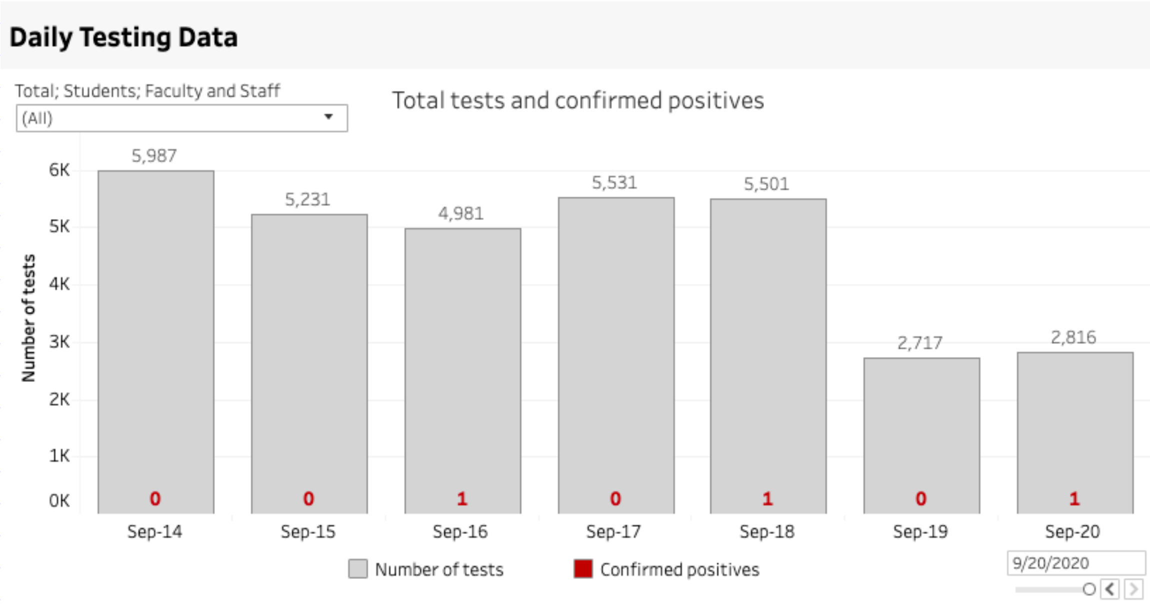
Lecture 6, 22 Sep 2020



3 pos out of over 30K tests

Assign states

1 qubit, start with $|0\rangle$

$|0\rangle \rightarrow |\psi\rangle$

then find some orthogonal $|\varphi\rangle$

$\langle\varphi|\psi\rangle = 0$

$|1\rangle \rightarrow |\varphi\rangle$ defines unitary

$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ $\qquad U = \begin{pmatrix} \alpha & -\beta^* \\ \beta & \alpha^* \end{pmatrix}$

$|0\rangle$ — $\boxed{U}$ — $|\psi\rangle$

complete basis $|i\rangle$

$$\sum_i |i\rangle\langle i| = \mathbb{1}$$

$|\psi\rangle = \alpha_i |i\rangle$

$$\left(\begin{array}{l} \sum_j |j\rangle\langle j|\psi\rangle \quad \swarrow \delta_{ij} \\ = \sum_j |j\rangle \alpha_i \langle j|i\rangle = \sum_i \alpha_i |i\rangle \end{array} \right)$$

$$u|i\rangle = \sum_j |j\rangle\langle j|u|i\rangle = \sum_j u_{ji}|j\rangle$$

$$u_{ji} \equiv \langle j|u|i\rangle$$

so $u \sum \alpha_i |i\rangle = \alpha_i u_{ji} |j\rangle = u_{ij}\alpha_j |i\rangle$

and $\alpha_i \to \sum_j u_{ij}\alpha_j$

$$\Sigma = \left(\begin{array}{ccc|c} s_0 & & & \\ & s_1 & & 0 \\ & & \ddots & \\ & & & s_{m-1} \end{array} \right)$$

$M = U \Sigma V^\dagger$

if M is $m \times n$, U is $m \times m$

V is $n \times n$

Σ is $m \times n$

Proof: U, V defined by

$M M^\dagger = U \Lambda U^\dagger$

$M^\dagger M = V \Lambda V^\dagger$

$s_i = \sqrt{\lambda_i} \qquad \Sigma \approx \sqrt{\Lambda}$

$M = U\Sigma V^\dagger$

$|\psi\rangle = M_{ij}|i\rangle|j\rangle = \sum s_k U_{ik} V^*_{jk}|i\rangle|j\rangle = s_k|u_k\rangle|v^*_k\rangle$

where $|u_k\rangle \equiv \sum_i u_{ik}|i\rangle$ $\quad |v^*_k\rangle \equiv \sum_j v^*_{jk}|j\rangle$

product state iff single $s_k \neq 0$

$|\psi\rangle = \alpha_{ij}|i\rangle|j\rangle$

2 qubit $\quad \alpha = u\Sigma v^\dagger \quad \alpha_{ij} = \sum u_{ik} s_k v^*_{jk}$

recall $u|k\rangle = |i\rangle\langle i|u|k\rangle = u_{ik}|i\rangle$

$$|\psi\rangle = \sum_{ijk} u_{ik} s_k v^*_{jk}|i\rangle|j\rangle = \sum_k (u\otimes v^*) s_k|k\rangle|k\rangle$$

$$= (u\otimes v^*)(s_0|0\rangle|0\rangle + s_1|1\rangle|1\rangle)$$

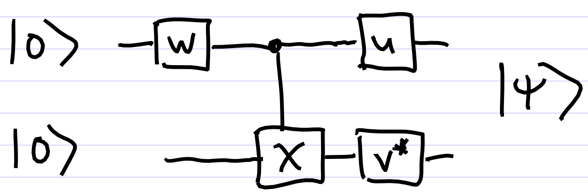
$$= (u\otimes v^*)C_{10}(s_0|0\rangle + s_1|1\rangle)|0\rangle$$

$$= (u\otimes v^*)C_{10}W_1|0\rangle|0\rangle$$

$\uparrow$ $W\otimes\mathbb{1}$

where $s_0|0\rangle + s_1|1\rangle = W|0\rangle$

all entanglement from CNOT



gives most general 2-qubit state

Table 1.1. A summary of the features of Qbits, contrasted to the analogous features of Cbits

	Cbits	Qbits
States of n Bits	$\|x\rangle_n \quad 0 \le x < 2^n$	$\sum_x \alpha_x \|x\rangle \quad \sum \|\alpha_x\|^2 = 1$
Subsets of n Bits	always have states	generally not
Reversible operations on states	permutations	unitary
Can state be learned from Bits?	yes	no
To learn state of Bits	Examine	Go ask Alice
To get information from Bits	Look	measure
Information acquired	x	x with prob $\|\alpha_x\|^2$
State after information acquired	same, $\|x\rangle$	different, now $\|x\rangle$

General computional process

x : n bit number

$f(x)$ = m bit number

need $n+m$ bits input and output

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

slight generalization

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

$\oplus$ bitwise XOR $\quad 1101 \oplus 0111 = 1010$

U_f is reversible

$$\begin{aligned} U_f U_f |x\rangle|y\rangle &= U_f |x\rangle|y \oplus f(x)\rangle \\ &= |x\rangle|y \oplus \underbrace{f(x) \oplus f(x)}_{0}\rangle \\ &= |x\rangle|y\rangle \end{aligned}$$

Magic (?)

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

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

$$H^{\otimes n}|0\rangle_n = \left(\frac{1}{\sqrt{2}}\right)^n (|0\rangle + |1\rangle)^{\otimes n}$$

$$= \frac{1}{2^{n/2}}(|0\ldots0\rangle + |0\ldots01\rangle + \ldots |11111\rangle$$

$$= \frac{1}{2^{n/2}} \sum_{0 \le x < 2^n} |x\rangle$$

$$H^{\otimes n} = \overbrace{H \otimes \ldots \otimes H}^{n \text{ times}}$$

$$U_f \left(H^{\otimes n} \otimes I_m\right) |0\rangle_n |0\rangle_m$$

$$= \frac{1}{2^{n/2}} \sum_{0 \le x < 2^n} U_f |x\rangle_n |0\rangle_m$$

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

$H^{\otimes 100} |0\rangle_{100}$ $\quad 2^{100} \simeq 10^{30}$ calculations

Quantum parallism, Multiverse?

parallel world?

$\boxed{\text{BuT}}$ we can't extract them from the state when we measure, we get $|x_0\rangle|f(x_0)\rangle$

with probability $1/2^n$

---

what if we could "clone" state?

but: "no-cloning" theorem

suppose $U|\psi\rangle_n|0\rangle_n = |\psi\rangle_n|\psi\rangle_n$

$U|\varphi\rangle_n|0\rangle_n = |\varphi\rangle_n|\varphi\rangle_n$

by linearity,

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

$= aU|\psi\rangle|0\rangle + bU|\varphi\rangle|0\rangle$

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

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

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

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

$$\overset{?}{=}\ a|\psi\rangle|\psi\rangle+b|\varphi\rangle|\varphi$$

only true for
$a=0,1$ $b=1,0$

doesn't work in general

approximate cloning?

$$U|\psi\rangle|0\rangle\approx|\psi\rangle|\psi\rangle$$

$$U|\varphi\rangle|0\rangle\approx|\varphi\rangle|\varphi\rangle$$

$$\Rightarrow \langle \varphi | \psi \rangle \approx |\langle \varphi | \psi \rangle|^2$$

$$\langle \varphi | \psi \rangle \approx 0, 1$$

so can approx clone a state or an orthog state, but everything else cloned badly

Deutsch problem

1 bit → 1 bit function

i.e., $m = n = 1$

	$x=0$	$x=1$	
f_0	0	0	const $f(x)=0$
f_1	0	1	identity $f(x)=x$
f_2	1	0	not $f(x)=1-x$
f_3	1	1	Const $f(x)=1$

Invoke f once, can't distinguish between constant and non-constant functions (f_0, f_3) vs (f_1, f_2) classically.

But quantum mechanically can make that distinction with just one call to U_f