"No theorist — ________

'' — Craig Higam

'' ________________ ''

Scott Aaronson

* Ordinary Prob Theory

States

$|H\rangle$

$|T\rangle$

$\frac{1}{2}|H\rangle + \frac{1}{2}|T\rangle$

$\frac{1}{3}\,|H\rangle + \frac{2}{3}\,|T\rangle$

Any $p_0\,|H\rangle + p_1\,|T\rangle$

w/ $p_0, p_1 \geq 0$ $\quad p_0+p_1 = 1$

Transforms

Transformations

Shake hand:

$$p_0 |H\rangle + p_1 |T\rangle \longmapsto$$

$$(\tfrac{1}{2}p_0 + \tfrac{1}{2}p_1)\tfrac{1}{2} |H\rangle + (\tfrac{1}{2}p_0 + \tfrac{1}{2}p_1)\tfrac{1}{2} |T\rangle$$

:

$$p_0 |H\rangle + p_1 |T\rangle \longrightarrow$$

$$\tfrac{1}{3} |H\rangle + \tfrac{2}{3} |T\rangle$$

If $|H\rangle$, leave alone

If $|T\rangle$, flip:

$$p_0 |H\rangle + p_1 |T\rangle \longrightarrow$$

$$(p_0 + \tfrac{1}{2} p_1) |H\rangle +$$

$$\tfrac{1}{2} p_1 |T\rangle$$

If $|H\rangle$, then $a |H\rangle + b |T\rangle$

If $|T\rangle$, then $a' |H\rangle + b' |T\rangle$

$$p_0 |H\rangle + p_1 |T\rangle \longrightarrow$$

$$(a p_0 + a' p_1) |H\rangle +$$

$$(\beta p_0 + \beta' p_1)\,|T\rangle$$

All linear

Measurement

~~To~~ Perform a measurement

$p_0\,|H\rangle + p_1\,|T\rangle$

gives $|H\rangle$ w/ prob p_0

$|T\rangle$ w/ prob p_1

~~Out~~ Rules of ordinary probability

~~Basis~~

Gen ~~Hum~~ fin set of basis states

~~[illegible]~~ ~~[illegible]~~

$\{|x_1\rangle, \ldots, |x_n\rangle\}$

$(\{|H\rangle, |T\rangle\})$

Set of all States is

$$\{ p_1 |x_1\rangle + \cdots p_n |x_n\rangle \mid p_1, \ldots, p_n \geq 0, \; p_1 + \cdots + p_n = 1 \}$$

Two updates

Transformations: A <u>Linear</u> maps from $\mathbb{R}^n$ to $\mathbb{R}^n$

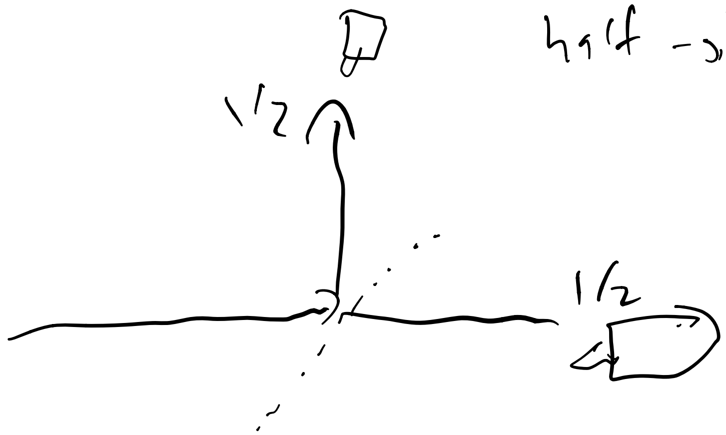
s.t. States get mapped to states

Measurement: $p_1 |x_1\rangle + \ldots \; p_n |x_n\rangle$

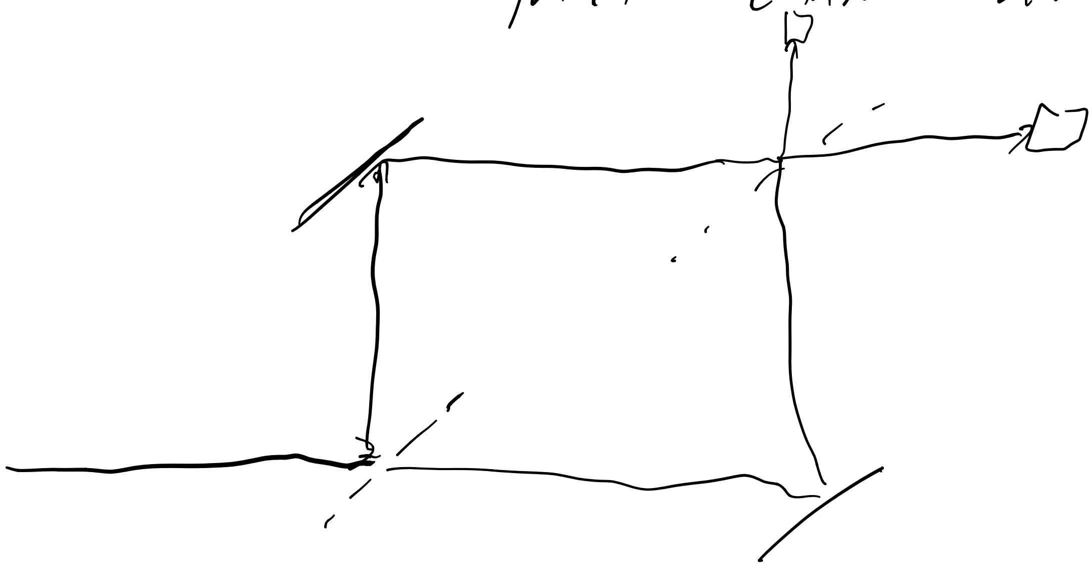
$\to |x_j\rangle$ w/ prob. p_j

Interference

half-silver mirror

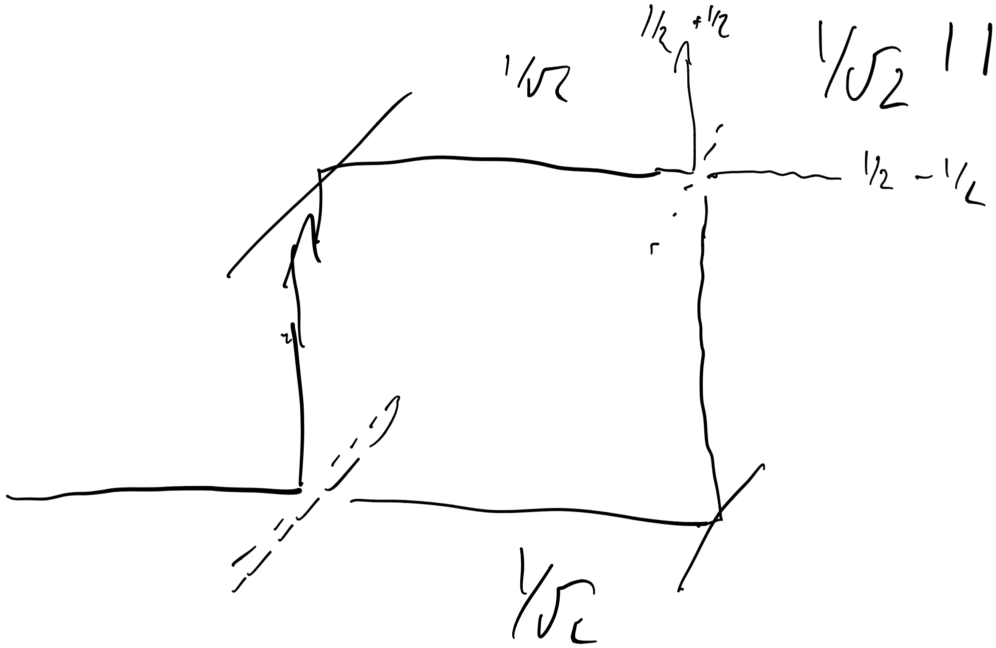


Mach-Zehnder Interferometer



$$|\text{upper}\rangle \longmapsto \frac{1}{\sqrt{2}}|\text{upper}\rangle + \frac{1}{\sqrt{2}}|\text{lower}\rangle$$

$|\text{lower}\rangle \longrightarrow \frac{1}{\sqrt{2}}|\text{upper}\rangle - \frac{1}{\sqrt{2}}|\text{lower}\rangle$



complementarity

~~particle~~

electrons have a spin

→ can be measured in any direction

→ the output of measurement will be either $+\frac{1}{2}$ or $-\frac{1}{2}$

$\hbar$ Suppose 

$|Right\rangle$

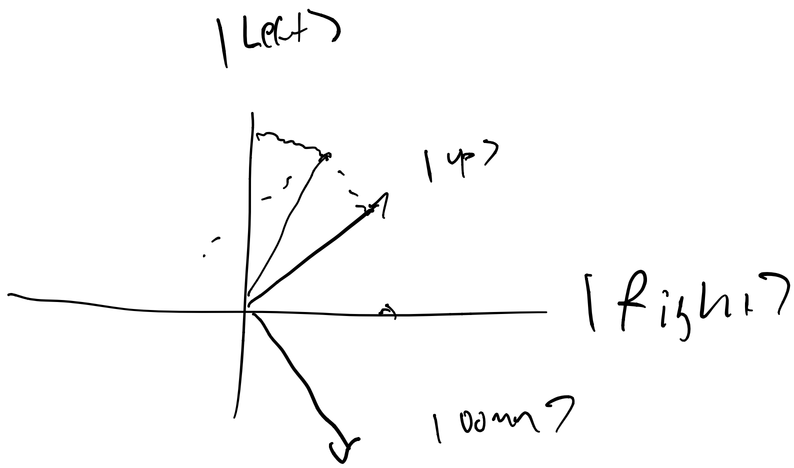
$|Left\rangle$

$$\alpha |Left\rangle + \beta |Right\rangle$$

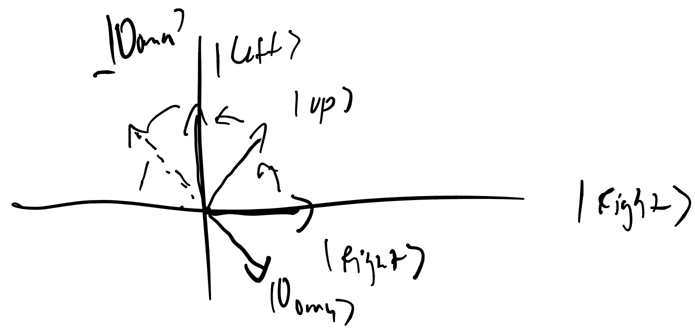
$$|\alpha|^2 + |\beta|^2 = 1$$

$$|Up\rangle = \frac{1}{\sqrt{2}} |Left\rangle + \frac{1}{\sqrt{2}} |Right\rangle$$

$$|Down\rangle = \frac{1}{\sqrt{2}} |Left\rangle + \frac{1}{\sqrt{2}} |Right\rangle$$



Consider rotate-by-90°



$|Right\rangle \longrightarrow |Up\rangle \longmapsto |Left\rangle \longmapsto$

$-|Down\rangle \longrightarrow |Right\rangle$

rotate-by-360° $(\psi) = -\psi$

Performing rotation on ψ is same as

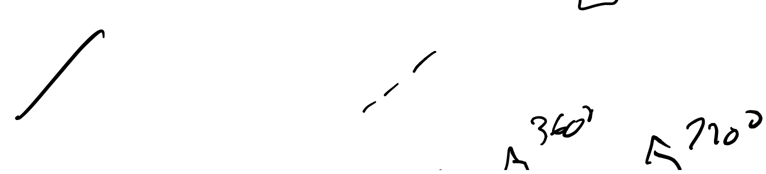
$-\psi$

But ψ & $-\psi$ could act differently

when they're part of superposition

□ |up⟩ 100%

□ ~~100%~~



Feynman belt trick

Reason Prob No-Cloning Thm

"Ordinary" Probability Theory

Suppose two two systems

$|\psi\rangle, |\phi\rangle$ A; w/ basis states $|a_1\rangle, \ldots |a_n\rangle$

$|\psi\rangle, |\phi\rangle$ B; w/ basis states $|b_1\rangle, \ldots |b_m\rangle$

then, the composite system $A \otimes B$ has nm basis states

$|a_1 b_1\rangle, |a_1 b_2\rangle, \ldots \quad |a_1 b_m\rangle$

$|a_2 b_1\rangle, |a_2 b_2\rangle, \ldots \quad |a_2 b_m\rangle$

$\vdots \quad \ldots \quad \vdots$

$|a_n b_1\rangle, \ldots \quad |a_n b_m\rangle$

$\otimes$ extends to non basis states

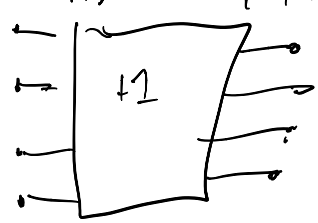
$$\left(\tfrac{1}{2}|H\rangle + \tfrac{1}{2}|T\rangle\right) \otimes \left(\tfrac{1}{3}|H\rangle + \tfrac{2}{3}|T\rangle\right)$$

$$= \tfrac{1}{6}|H\rangle\otimes|H\rangle + \tfrac{1}{6}|T\rangle\otimes|H\rangle$$

$$+ \tfrac{1}{3}|H\rangle\otimes|T\rangle + \tfrac{1}{3}|T\rangle\otimes|T\rangle$$

If a state φ of $A\otimes B$ can be written as $\varphi_A \otimes \varphi_B$ it's called <u>simple</u> or distributions on A & B are <u>independent</u>. Otherwise the distributions are dependent.

~~Possible to duplicate information,~~ $\{0,1\}^4 \longrightarrow \{0,1\}^4$

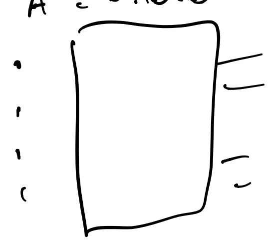


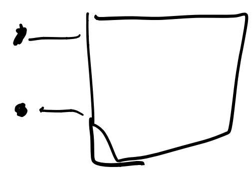
(Classical) Bit is a 0 or 1

Classical ~~operations~~ computation gates on streams of bits

Qubit is any quantum system A w/ states $\alpha|0\rangle + \beta|1\rangle$

$A^{\otimes n} = A\otimes A\otimes A\otimes A \longrightarrow$ A...



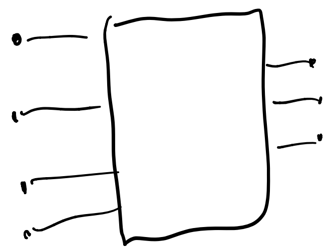


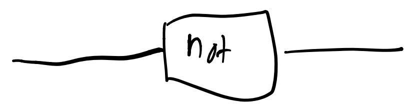
Circuits

(Classical) bit is 0 or 1

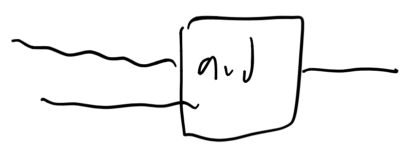
any fn from $\{0,1\}^n \to \{0,1\}^m$

and a classical circuit



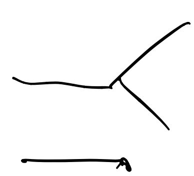


$0 \to 1$
$1 \to 0$



$$\left.\begin{matrix}0,0\\0,1\\1,0\end{matrix}\right\} \to 0$$

$1,1 \to 1$



Quantum bit (qubit)

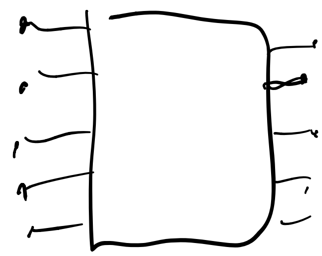
is a quantum system w/

basis states $|0\rangle$ or $|1\rangle$ $= A \otimes A \otimes A \cdots$ (n)

$\alpha|0\rangle + \beta|1\rangle$

$A^{\otimes n} \to A^{\otimes n}$ unitary

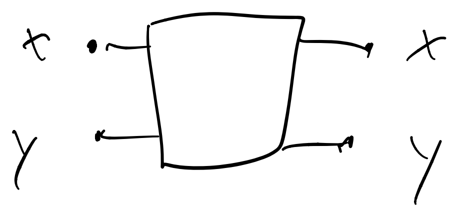
a quantum circuit

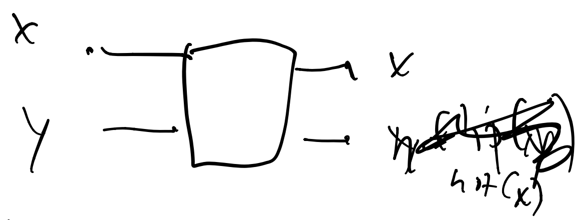


Deutsch's Algorithm ("Free of Essence")

Why: Artificial

4 quantum circuits



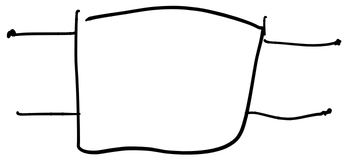


$|00\rangle \to |01\rangle$

$|01\rangle \to |00\rangle$

$|10\rangle \to |11\rangle$

$|11\rangle \to |10\rangle$



Flips y iff x is $|0\rangle$

$|00\rangle \to |01\rangle$

$|01\rangle \to |00\rangle$

$|10\rangle \to |10$

$|$

Determine whether the circuit is in the first set or second set (w/o looking at the out

$0\ 0 \to 00$

Suppose $|0\rangle = \cancel{|Left\rangle}\ |Right\rangle$

$|1\rangle = \cancel{|Right\rangle}\ |Left\rangle$

$$x = |Up\rangle = \frac{|Left\rangle + |Right\rangle}{\sqrt{2}}$$

$$y = |Down\rangle = \frac{-|Left\rangle + |Right\rangle}{\sqrt{2}}$$

$-|11\rangle - |01\rangle + |01\rangle + |10\rangle$

$-|10\rangle - |000\rangle + |01\rangle + |11\rangle$

$= (|1\rangle + |0\rangle)(-|0\rangle +$

$-|11\rangle - |01\rangle + |00\rangle + |10\rangle$

$-|00\rangle - |01\rangle + |00\rangle + |11\rangle$

$\cancel{-|0\rangle}$

$-|10\rangle + |11\rangle - |01\rangle + |00\rangle$

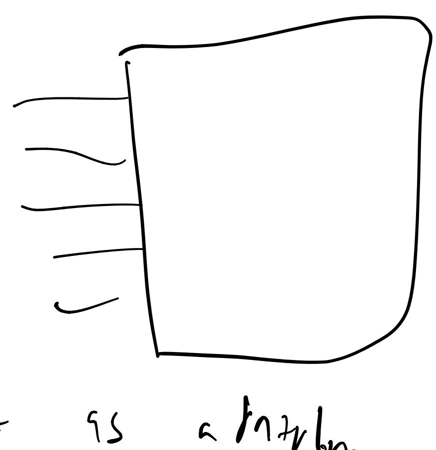
$|1\rangle(-|0\rangle + |1\rangle) - |0\rangle(+|1\rangle - |0\rangle)$

$-|0\rangle + |1\rangle$

Grover's algorithm

suppose given some arbitrary

black box circuit



Think of as a function or lookup table

e.g., maybe it maps people to

phone #'s.

Problem: Given a phone #

Classically, $O(n)$, where n is #

of people

Quantum: $O(\sqrt{n})$

Important:

How Good it is

How not good it is: suggests

Quantum computers can't solve NP

problems efficiently

Complexity Classes