QWORLD

Classical systems and introduction to quantum systems

Jibran Rashid

Tuesday, July 12

WOMANIUM QUANTUM 2022

Quantum Programming I - QBronze

Successful completion – *what you need to do*

- Pass each quiz on canvas with score > 50%
- Have an average score > 70% for entire module
- Complete module by July 25
- Multiple attempts allowed for the quizzes

Quantum Programming I - QBronze

Successful completion – *what you need to do*

- Pass each quiz on canvas with score > 50%
- Have an average score > 70% for entire module
- Complete module by July 25
- Multiple attempts allowed for the quizzes

Prepare for quizzes by working through programming exercises in Jupyter notebooks!

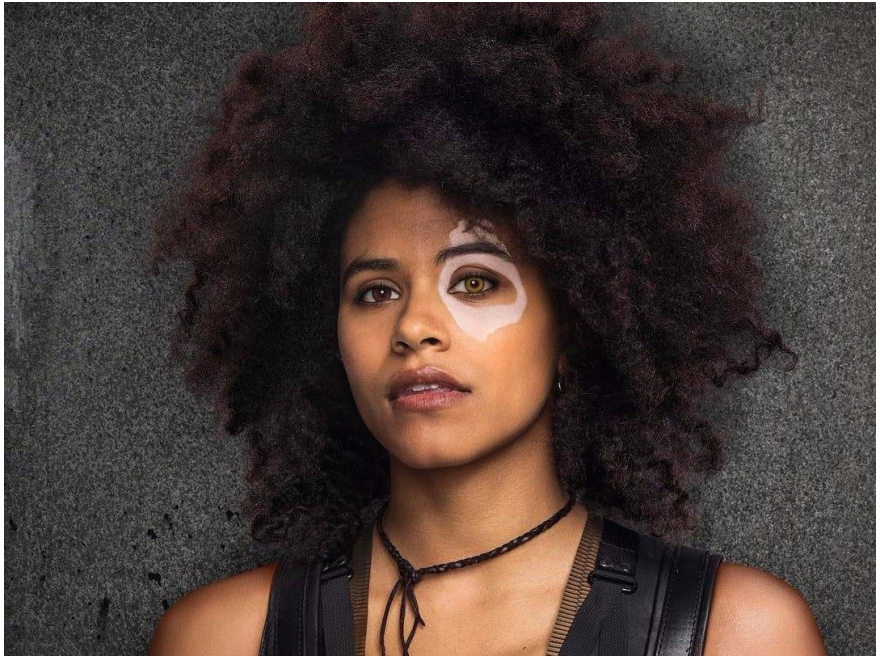
Mentors are on Discord to help

- *@saba* – 9:30am to 11am ET
  (Qbronze days except 18th July)
- *@Jyoti* – 11am to 1pm ET
  (12 – 16 July)
- *@Rumlah* – 3pm to 5pm ET
  (QBronze days)
- *@Shantanu* – 12:30am to 2:30am ET
  (13, 14, 18, 20 and 25 July)

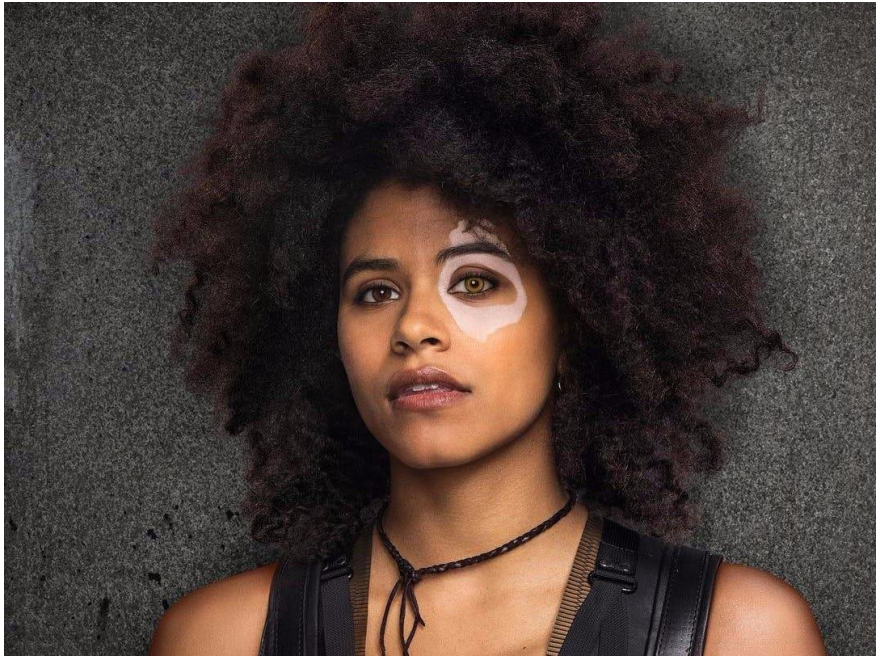
An engineer, a physicist and a mathematician…

What is Your Favourite Super Power?

What is Your Favourite Super Power?



What is Your Favourite Super Power?



MANIPULATE PROBABILITY!!!

The Church-Turing Thesis

Any ‘reasonable’ model of computation can be simulated on a standard Turing machine

Foundations of Computer Science

The Church-Turing Thesis

Any ‘reasonable’ model of computation can be simulated on a standard Turing machine

Lemma

Existence of a software industry

Foundations of Computer Science

The Church-Turing Thesis

Any ‘reasonable’ model of computation can be simulated on a standard Turing machine

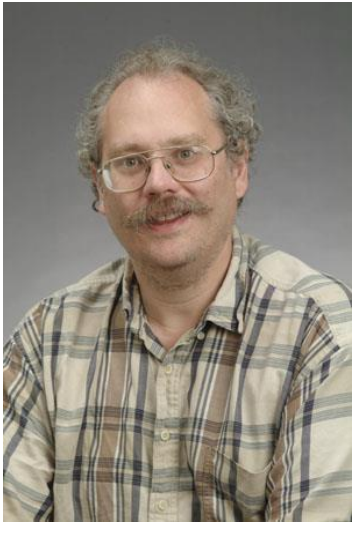
Lemma

Existence of a software industry

The Extended Church Turing Thesis

Any ‘reasonable’ model of computation can be *efficiently* simulated on a standard Turing machine

Peter Shor's (Potential) Counterexample (1994)



Integer Factorization

Given an integer N, find its prime factors.

Consequently, we can break public-key cryptography systems such as RSA!

Deterministic Classical Information

A physical device X has some finite, non-empty set of states.

$\Sigma = \{0,1\}$ $\{H,T\}$, $\{A,O\}$ $\{0,1,2,3\}$

How does the state of the system change?

X	f_0	f_1	f_2	f_3
0	0	0	1	1
1	0	1	0	1

$f_i : \{0,1\} \longrightarrow \{0,1\}$

Two devices X

What about multiple such devices?

$\Sigma^2 = \{00, 01, 10, 11\}$

$\Sigma^n = 2^n$

$\underbrace{2 \times 2 \times \cdots \times 2}_{n} = 2^n$

How many boolean fcts are there on n bits.

x_1 x_2 ... x_n	$f(x_1, \ldots x_n)$
0 0 ... 0	
1 1 ... 1	

$2^{2^n} = 2^N$

$2^n = N$ # of rows

x_1 x_2 ... x_{10}	f_i
0 0 0 ... 0	
1 1 ... 1	

2^{10}

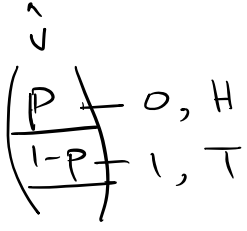
What if we have Incomplete Information?

What if we have Incomplete Information?

Probability

Probability (State of $X=0$) $= p$

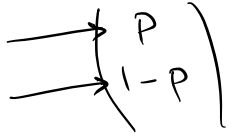
Probability (State of $X=1$) $= 1-p$



Note: When we look at X we do not see $\hat{v}, p$

but rather some state $\sigma \in \Sigma$ with probability v_σ

What if we have Incomplete Information?



$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} p \\ 1-p \end{pmatrix} = \begin{pmatrix} 1-p \\ p \end{pmatrix}$$

→ Flip of the bias

How does the State of the System change?

Deterministic Operations

$$A_0 = \begin{array}{c} \\ H \\ T \end{array}\begin{array}{c} \begin{array}{cc} H & T \end{array} \\ \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} \end{array}, \quad A_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad A_2 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad A_3 = \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix}$$

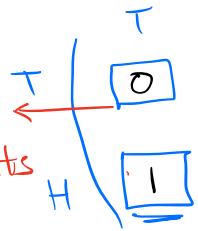
Probabilistic Operation $B = \sum_{i=0}^{3} p_i A_i$, $\sum_i p_i = 1$

e.g. $F = \frac{1}{2}A_1 + \frac{1}{2}A_2 = \frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$

How does the State of the System change?

We flip a coin $\begin{pmatrix} T & p \\ H & q \end{pmatrix}$.

{ if we get a head, flip again
if " " " tail, turn over coin to head.



Given tails, it represents the probability to transition to other state, in this case tail (row).

$$\begin{matrix} & H \\ T & p \\ H & q \end{matrix} \begin{pmatrix} p \\ q \end{pmatrix} = \begin{pmatrix} pq \\ p+q^2 \end{pmatrix}$$

In general, a square matrix is a valid classical transformation

Stochastic ← { 1. all entries ≥ 0
2. sum of entries in each col. $= 1$

Multiple Devices with Incomplete Information

Coin X_1 $\begin{pmatrix} p \\ q \end{pmatrix} = v_1$ $\quad$ Coin X_2 $\begin{pmatrix} r \\ s \end{pmatrix} = v_2$ $\quad$ HH, HT, TH, TT

$$\begin{pmatrix} p \\ q \end{pmatrix} \otimes \begin{pmatrix} r \\ s \end{pmatrix} = \begin{pmatrix} pr \\ ps \\ qr \\ qs \end{pmatrix} \begin{matrix} HH \\ HT \\ TH \\ TT \end{matrix}$$

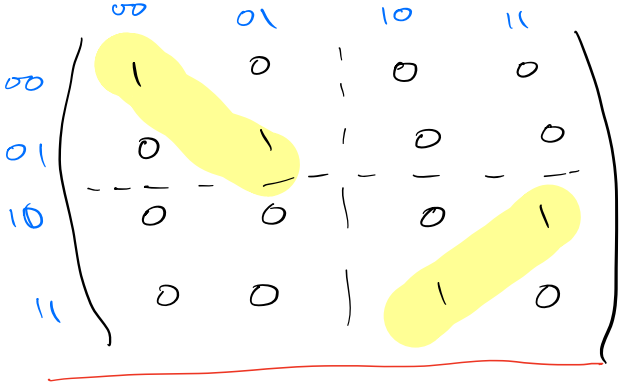
Note Not all valid 4-dim prob. vectors can be represented by tensor $v_1 \otimes v_2$

$$\frac{1}{2}\begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix} \neq \begin{pmatrix} pr \\ ps \\ qr \\ qs \end{pmatrix} = \begin{pmatrix} p \\ q \end{pmatrix} \otimes \begin{pmatrix} r \\ s \end{pmatrix}$$

$$\frac{1}{2}\begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \end{pmatrix}$$

Multiple Devices with Incomplete Information

$$A \otimes B = \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} \otimes \begin{pmatrix} b_1 & b_2 \\ b_3 & b_4 \end{pmatrix} = \underbrace{\begin{pmatrix} a_1 B & a_2 B \\ a_3 B & a_4 B \end{pmatrix}}_{4 \times 4 \text{ matrix}}$$



CNOT — Controlled Not

CNOT $e_{00} = e_{00}$

$e_{01} = e_{01}$

$e_{10} = e_{11}$

$e_{11} = e_{10}$

$$\left\{ \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} \right\}$$

e_{00} e_{01} e_{10} e_{11}

How can a Biased Coin Simulate a Fair Coin?

Assume you have a coin $\begin{pmatrix} p \\ 1-p \end{pmatrix}$, $p \neq 0$, $p \neq 1/2$.

How can we simulate a fair coin.

QWORLD

Basics of a Quantum Program

Jibran Rashid

Wednesday, July 13

WOMANIUM QUANTUM 2022

Quantum Bit (Qubit)

Modelling a qtm device X with $\Sigma = \{0,1\}$

Central Claim of Qtm Physics

To describe an isolated qtm system we need to give an amplitude ($\alpha \in \mathbb{C}$) for each possible state we can find the system to be in when we measure it.

Classically

$$\hat{v} = p\begin{pmatrix}1\\0\end{pmatrix} + (1-p)\begin{pmatrix}0\\1\end{pmatrix}$$

$$= \begin{pmatrix}p\\1-p\end{pmatrix}$$

Qtm

$$\hat{v} = \alpha\begin{pmatrix}1\\0\end{pmatrix} + \beta\begin{pmatrix}0\\1\end{pmatrix}$$

$\alpha, \beta \in \mathbb{C}$

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

Getting Probabilities from Amplitudes

Born Rule

Probability to observe a particular outcome, e.g. $\Pr(X \text{ is in state } 0)$ is given by absolute value square of amplitude.

$$\alpha \text{ (amplitude)} \longrightarrow |\alpha|^2 = |a+ib|^2 = a^2+b^2.$$

So, a qubit is given by

$$\hat{v} = \alpha \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \beta \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \quad \alpha, \beta \in \mathbb{C}, \quad |\alpha|^2 + |\beta|^2 = 1$$

Quantum Bit (Qubit)

Restricting amplitudes to real numbers

$$\hat{v} = \begin{pmatrix} \cos\theta \\ \sin\theta \end{pmatrix}, \quad \cos^2\theta + \sin^2\theta = 1, \quad \theta \in [0, 2\pi)$$

Instead of a probabilistic combination, we have a superposition!

$$\hat{v} = \cos\theta \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \sin\theta \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

What is the physical reality of this state.

Quantum Operations

Want all operations that map qtm states to qtm states.

$$U \begin{pmatrix} \vdots \\ \alpha_i \\ \vdots \end{pmatrix} = \begin{pmatrix} \vdots \\ \beta_i \\ \vdots \end{pmatrix} \qquad \alpha_i, \beta_i \in \mathbb{R}$$

$$\sum_i \alpha_i^2 = 1 = \sum_i \beta_i^2 \longrightarrow \text{Euclidean norm is preserved.}$$

i) $U^T U = \mathbb{1}$

ii) U is reversible

} Unitary

Quantum Operations

e.g., $H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ (Hadamard)

$$H \begin{pmatrix} 1 \\ 0 \end{pmatrix} = H|0\rangle = \frac{1}{\sqrt{2}} \left(|0\rangle + |1\rangle \right) = |+\rangle$$

$$H \begin{pmatrix} 0 \\ 1 \end{pmatrix} = H|1\rangle = \frac{1}{\sqrt{2}} \left(|0\rangle - |1\rangle \right) = |-\rangle$$

ket notation

$|0\rangle \stackrel{\text{def}}{=} \begin{pmatrix} 1 \\ 0 \end{pmatrix}$

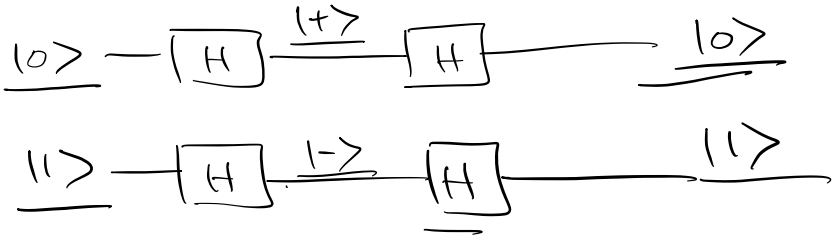
$|1\rangle \stackrel{\text{def}}{=} \begin{pmatrix} 0 \\ 1 \end{pmatrix}$

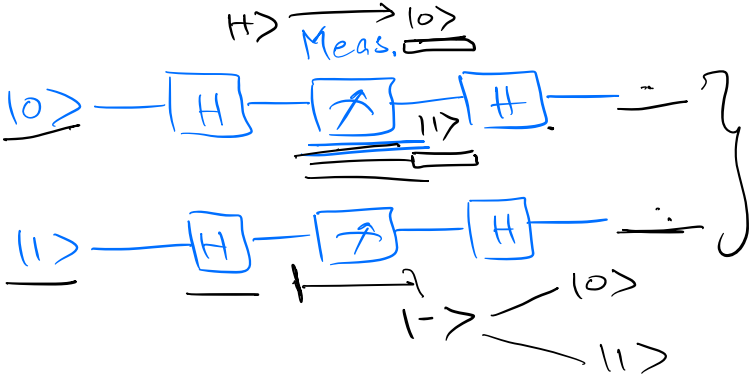
Compare to

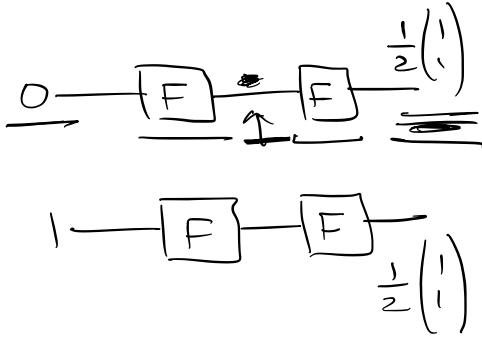
$F = \frac{1}{2} \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$

$F \begin{pmatrix} 1 \\ 0 \end{pmatrix} = F \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \frac{1}{2} \begin{pmatrix} 1 \\ 1 \end{pmatrix}$

Classical vs Quantum Coin Flipping



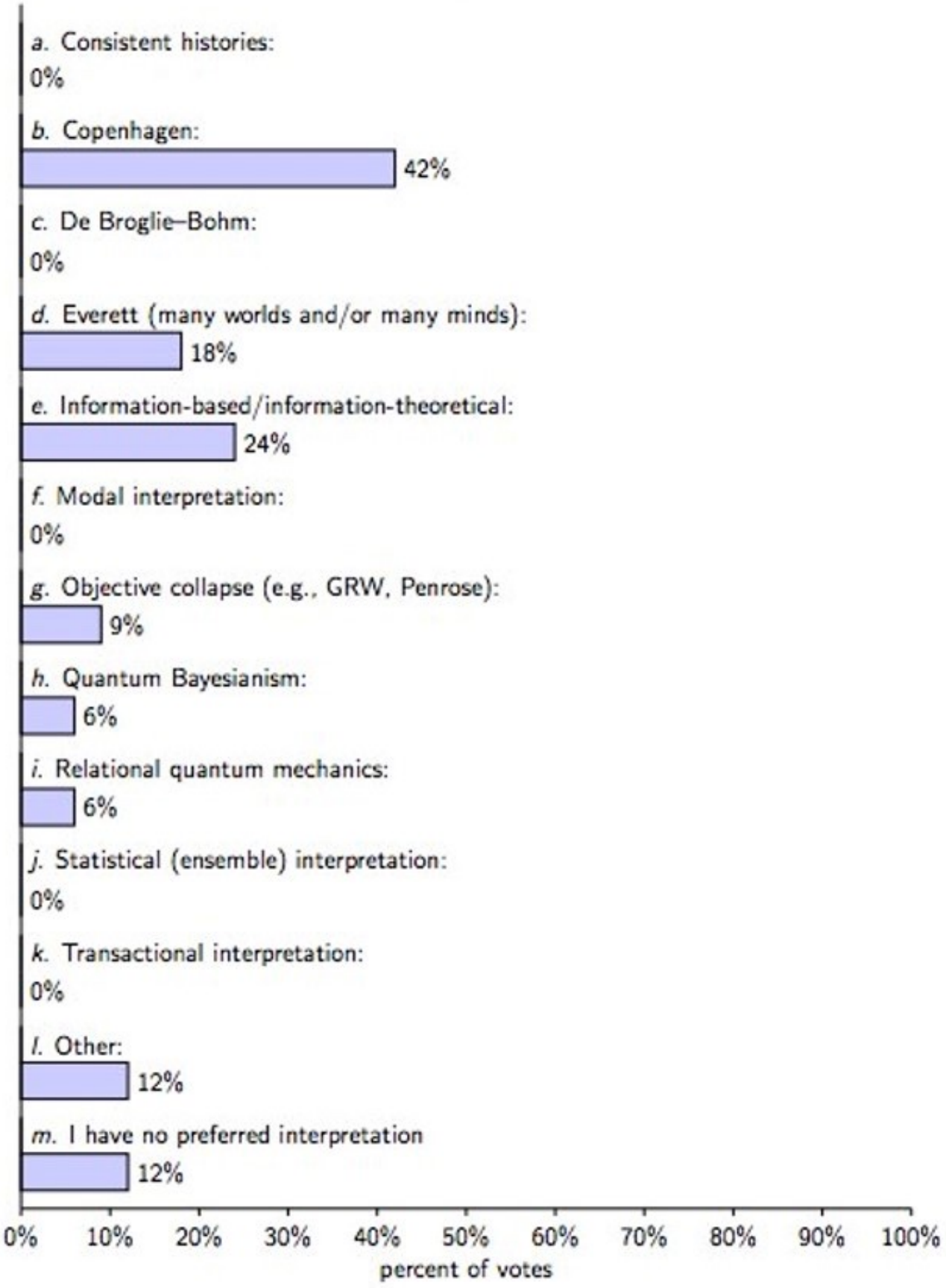




$$\frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

Classical vs Quantum Coin Flipping

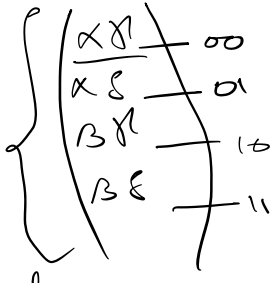
Question 12: What is your favorite interpretation of quantum mechanics?



Multiple Qubits

$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$
$|\varphi\rangle = \gamma|0\rangle + \delta|1\rangle$

$\Big\}$ $|\psi\rangle \otimes |\varphi\rangle = \alpha\gamma|00\rangle + \alpha\delta|01\rangle + \beta\gamma|10\rangle + \beta\delta|11\rangle$



n Qubits

Assume they have this decomposition.

$|\psi\rangle = (\alpha_1|0\rangle + \beta_1|1\rangle) \otimes (\alpha_2|0\rangle + \beta_2|1\rangle) \otimes \cdots \otimes (\alpha_n|0\rangle + \beta_n|1\rangle)$

admit this decomposition

If $|\psi\rangle$ is separable, then we only need $O(n)$ (linear memory) for keeping track OR storing the qtm state.