Probabilistic computing

Classical computation + coin flips

- Example 1: Matrix multiplication, Freivald's matrix multiplication checker
- Example 2: Primality testing
  - Input: n-bit integer
  - Output: YES if prime, NO otherwise.
  - Naive algorithm: $O(2^{n/2})$ steps
  - Miller 1976: Assuming extended Riemann hypothesis, $O(n^4)$ steps
  - Rabin 1980: Probabilistic twist on Miller's algorithm, $O(n^2)$ steps
  - Miller–Rabin algorithm used in https

Strongly believed

Every “compute a function” problem in P probabilistically is also in P deterministically

Upshot

Probabilistic computing

- Classical computation + one simple power “coin flip”
- Analyzing its complexity / efficiency requires probability theory
- Quintessential use: simulate something random
- Seems to give speedups over deterministic computing from one level of P efficiency to another level
- Strongly believed: doesn’t give speedups from exponential time to polynomial time for any “compute a function” task

- Typical probabilistic algorithm looks like:
  - Initialize array A of length n
  - For each i, $A[i]$:= coin flip 0 or 1
  - Do classical deterministic computing on A
- Now describe A’s state requires 2^n numbers (i.e. $\Pr(A = x) \forall x \in \{0,1\}^n$)

Looking forward

Quantum computing

- Classical computation + one simple power “rotate”
- Analyzing its complexity / efficiency requires probability theory + linear algebra
- Quintessential use: simulate something quantum
- Seems to give speedups over probabilistic computing from one level of P efficiency to another level
- Strongly believed: doesn’t give speedups from exponential time to polynomial time for any “compute a function” task

- Typical quantum algorithm looks like:
  - Initialize array A of n photons (qubits)
  - Run them through an obstacle course of mirror and prisms (quantum circuits)
- Now describe the state requires 2^n possibly negative numbers (amplitutdes)

Understanding and measuring one qubit

Comparison with classical computing

- In classical computer,
  - Logical bit 0 or 1
  - Physical bit low or high voltage
- In quantum computer,
  - Physically represented by photon polarization
  - A photon can be horizontally polarized ($|0\rangle$) or vertically polarized ($|1\rangle$)

Quantum mechanics

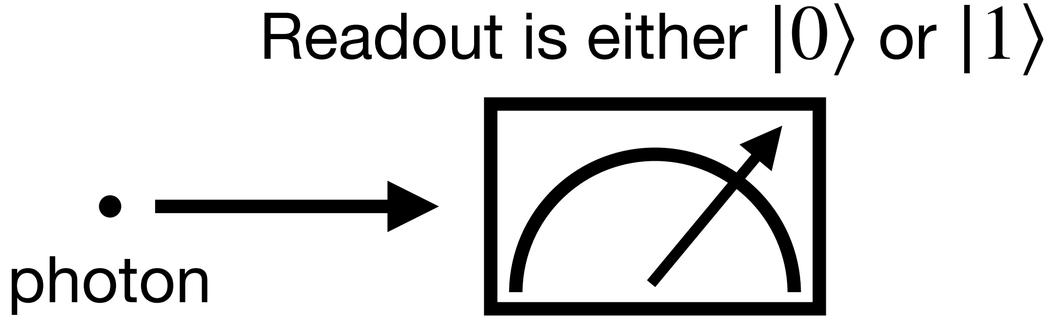
Law #1

- If a particle can be in one of the two basic states $|0\rangle$ or $|1\rangle$, then it can also be in a *superposition* state
  - α amplitude on $|0\rangle$ and β amplitude on $|1\rangle$
  - where α and β are complex numbers such that $|\alpha|^2 + |\beta|^2 = 1$
- Write the superposition state as $\alpha|0\rangle + \beta|1\rangle$

- A photon may have the following states.
  - Example 1: $0.8|0\rangle + 0.6|1\rangle$
  - Example 2: $0.8|0\rangle - 0.6|1\rangle$
  - Example 3: $1|0\rangle + 0|1\rangle$, write simply as $|0\rangle$
  - Example 4: $i|0\rangle + 0|1\rangle$

Measuring device

How can we extra information from a photon in superposition?



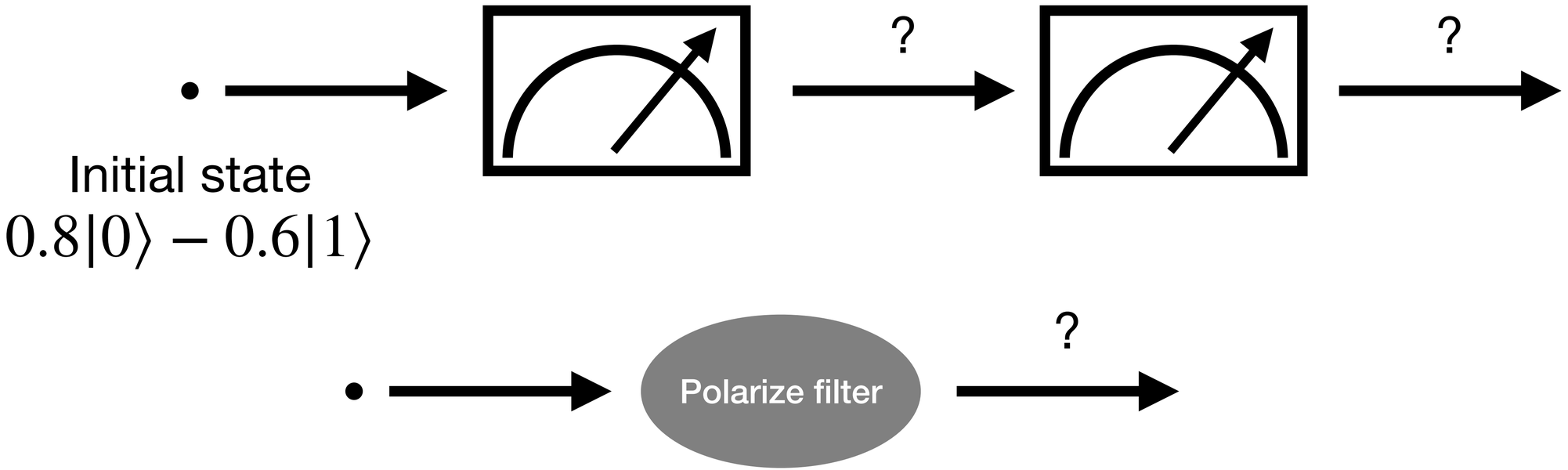
What's the readout of a photon in superposition?

Quantum mechanics

Law #2

- For a photon in the superposition state $\alpha|0\rangle + \beta|1\rangle$
- If you measure it, then the readout is
  - $|0\rangle$ with probability $|\alpha|^2$
  - $|1\rangle$ with probability $|\beta|^2$
- It makes sense because $|\alpha|^2 + |\beta|^2 = 1$
- After the measurement, the state “collapses” to $|0\rangle$ if the readout is $|0\rangle$
  and “collapses” to $|1\rangle$ if the readout is $|1\rangle$

Examples



Polarize filter first measures photon's state,
if $|0\rangle$, the photon flies through;
if $|1\rangle$, photon is converted into heat.

More photons

Joint state

- Two photons have 4 basic states $|00\rangle, |01\rangle, |10\rangle, |11\rangle$
- n photons have $N = 2^n$ basic states
  - $|00\ldots00\rangle, |00\ldots01\rangle, \ldots, |11\ldots11\rangle$ or equivalently $|0\rangle, |1\rangle, \ldots, |N-1\rangle$

Quantum mechanics

Law #1 and #2

- *Joint state* is $\sum_{s\in\{0,1\}^n} \alpha_s|s\rangle$ or equivalently $\sum_{s=0}^{N-1} \alpha_s|s\rangle$, where $\sum_s |\alpha_s|^2 = 1$
- Measurement: readout is $|s\rangle$ with probability $|\alpha_s|^2$, and the joint state collapses to $|s\rangle$ if the readout is $|s\rangle$

Mathematically…

Linear algebra

- Joint state is a unit (column) vector in $\mathbb{C}^d$
- Example: $0.8|0\rangle - 0.6|1\rangle$ is just $\begin{bmatrix} 0.8 \\ -0.6 \end{bmatrix}$, a point on the unit circle
- Recall, for $u, v \in \mathbb{C}^d$, $\langle u, v \rangle = u_1^* v_1 + \ldots u_d^* v_d = u^\dagger v$ (dagger, or conjugate transpose)
- Recall, if $z = x + yi$, then $z^* = x - yi$
- Check: $\|v\|^2 = \sum_k |v_k|^2$ for $v \in \mathbb{C}^d$

Dirac's notation

Bra-Ket

- High school: $i = \begin{bmatrix}1\\0\\0\end{bmatrix}, j = \begin{bmatrix}0\\1\\0\end{bmatrix}, k = \begin{bmatrix}0\\0\\1\end{bmatrix}, 3i + 5j - 2k = \begin{pmatrix}3\\5\\-2\end{pmatrix}$
- College: $e_1 = \begin{bmatrix}1\\0\\\vdots\\0\end{bmatrix}, e_2 = \begin{bmatrix}0\\1\\\vdots\\0\end{bmatrix}, \ldots, e_d = \begin{bmatrix}0\\0\\\vdots\\1\end{bmatrix}$
- Quantum: $|0\rangle, \ldots, |d-1\rangle$
- Qubit state: $\begin{bmatrix}\alpha\\\beta\end{bmatrix} = \alpha|0\rangle + \beta|1\rangle,$

Dirac’s notation

Bra-Ket

- Ket $|\text{blah}\rangle$ signifies a column vector
- Bra $\langle\text{blah}|$ signifies a row vector
- Connection: $\langle\text{blah}| = |\text{blah}\rangle^\dagger$
- Inner product: $u^\dagger v = \langle u||v\rangle = \langle u \mid v\rangle$

Dirac's notation

Examples

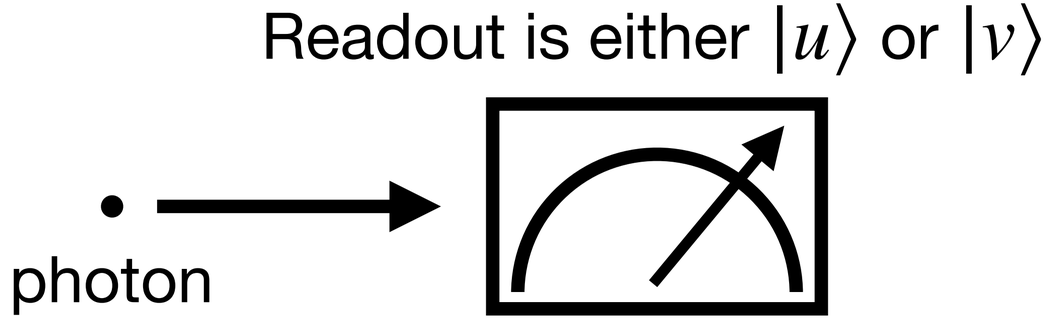
- $|+\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$
- $|-\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$

- What happens when a photon in $|+\rangle$ state is measured?

Measuring in a different basis

For one qubit

- Standard measuring device measures in $|0\rangle, |1\rangle$ basis
- For any orthonormal basis $|u\rangle, |v\rangle$, can build a measuring device for this basis.



- It makes sense for $\alpha|u\rangle + \beta|v\rangle$, the readout is $|u\rangle$ with probability $|\alpha|^2$, and the readout is $|v\rangle$ with probability $|\beta|^2$

Measuring in a different basis

For one qubit

- Given $|\varphi\rangle \in \mathbb{C}^2$, how to write it as $\alpha|u\rangle + \beta|v\rangle$?
- Theorem: If $|u\rangle, |v\rangle$ form an orthonormal basis, then $|\varphi\rangle = \langle u \mid \varphi\rangle|u\rangle + \langle v \mid \varphi\rangle|v\rangle$
- Theorem: Measure $|\varphi\rangle \in \mathbb{C}^2$ in the $|u\rangle, |v\rangle$ basis. The readout is $|u\rangle$ with probability $|\langle u \mid \varphi\rangle|^2$, and the readout is $|v\rangle$ with probability $|\langle v \mid \varphi\rangle|^2$.
- Example: Measure $|0\rangle$ in the $|+\rangle, |-\rangle$ basis