Computing With Linear Algebra (pt. 2)

CSE 490Q: Quantum Computation

Probabilistic Computing

- States are vectors of non-negative numbers that sum to 1
- Operations are stochastic matrices
  - columns of non-negative numbers that sum to 1
- Dirac notation for linear algebra:
  - makes clear what is a vector, matrix, and number
  - eliminates the need for inventing some names

$|x\rangle$ $|x\rangle\langle x|$

e_1 e_2

$|1\rangle$ $|2\rangle$

Combining Outcomes

Two bits: 00 01 10 11 (4)

One bit, die: 01 02 ... 06 (12)
11 12 ... 16

n outcomes → m outcomes

nm outcomes

Two Bits

Two bits: 00 01 10 11

Ex: $0.2|00\rangle + 0.3|01\rangle + 0.3|10\rangle + 0.2|11\rangle$

$|0,0\rangle \Rightarrow |00\rangle$.

$|5,5\rangle$

n values, m outcomes

basis vectors are $|i,j\rangle$

$i \to n$, $j \to m$

$|11\rangle$

Combining States

First — Second

$$\left(\underbrace{\tfrac{1}{3}|0\rangle}_{x} + \underbrace{\tfrac{2}{3}|1\rangle}_{y}\right) \otimes \left(\underbrace{\tfrac{1}{2}|0\rangle + \tfrac{1}{2}|1\rangle}_{z}\right)$$

$$= \underbrace{\tfrac{1}{3}|0\rangle}_{z} \otimes \left(\underbrace{\tfrac{1}{2}|0\rangle}_{x} + \underbrace{\tfrac{1}{2}|1\rangle}_{y}\right) + \tfrac{2}{3}|1\rangle \otimes \left(\tfrac{1}{2}|0\rangle + \tfrac{1}{2}|1\rangle\right)$$

$$= \tfrac{1}{3}|0\rangle \otimes \tfrac{1}{2}|0\rangle + \tfrac{1}{3}|0\rangle \otimes \tfrac{1}{2}|1\rangle + \tfrac{2}{3}|1\rangle \otimes \tfrac{1}{2}|0\rangle + \tfrac{2}{3}|1\rangle \otimes \tfrac{1}{2}|1\rangle$$

$$= \tfrac{1}{6}|0\rangle \otimes |0\rangle + \tfrac{1}{6}|0\rangle \otimes |1\rangle + \tfrac{1}{3}|1\rangle \otimes |0\rangle + \tfrac{1}{3}|1\rangle \otimes |1\rangle$$

$$\Rightarrow = \tfrac{1}{6}|00\rangle + \tfrac{1}{6}|01\rangle + \tfrac{1}{3}|10\rangle + \tfrac{1}{3}|11\rangle$$

Tensor Products

$$(a|x\rangle) \otimes |y\rangle = a(|x\rangle \otimes |y\rangle)$$

$$|x\rangle \otimes (a|y\rangle) = a(|x\rangle \otimes |y\rangle).$$

$$(|x\rangle + |y\rangle) \otimes |z\rangle = |x\rangle \otimes |z\rangle + |y\rangle \otimes |z\rangle$$

$$|z\rangle \otimes (|x\rangle + |y\rangle) = |z\rangle \otimes |x\rangle + |z\rangle \otimes |y\rangle$$

Notation: $|x\rangle \otimes |y\rangle \longrightarrow |x, y\rangle$.

Kronecker Products

Just saw $\underset{|x\rangle}{\begin{bmatrix} a \\ b \end{bmatrix}} \otimes \underset{|y\rangle}{\begin{bmatrix} c \\ d \end{bmatrix}} = \begin{bmatrix} ac \\ ad \\ bc \\ bd \end{bmatrix}$

$= \begin{bmatrix} a|y\rangle \\ b|y\rangle \end{bmatrix}$

first 2nd

$\left.\begin{matrix} 00 \\ 01 \\ 10 \\ 11 \end{matrix}\right\}$

Tensor Products of Operations

F^{1st} $\quad G^{\text{2nd}}$ $\quad \otimes \longrightarrow$ "$F \otimes G$"

$$\underbrace{(F|x\rangle) \otimes (G|y\rangle)}_{4\text{ elem}} = (F \otimes G)(|x\rangle \otimes |y\rangle)$$

Kronecker Products of Operations

$$F = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \qquad G = \begin{bmatrix} e & f \\ g & h \end{bmatrix}$$

$$F \otimes \underline{G} = \begin{bmatrix} aG & bG \\ cG & dG \end{bmatrix} = \begin{bmatrix} ae & af & be & bf \\ ag & ah & bg & bh \\ ce & cf & de & ef \\ cg & ch & dg & dh \end{bmatrix}$$

Example Operations

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \qquad F_1 = \begin{bmatrix} 0 & 0 \\ 1 & 1 \end{bmatrix}$$

$$(X \otimes F_1)|1,0\rangle = X|1\rangle \otimes F_1|0\rangle$$

$$= |0\rangle \otimes |1\rangle = \underline{|01\rangle}$$

$$\begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \end{bmatrix} \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix}$$

$$\begin{array}{l} 00 \\ \rightarrow 01 \\ 10 \\ 11 \end{array}$$

Size of Probabilistic States

- An n-bit state requires 2^n numbers to describe
- An n-bit operation requires $2^n \times 2^n$ numbers to write down

$2 \cdot 2 = 4$

8

16

- For even n = 1000, these are too large to write down!

$\overbrace{I \otimes \cdots \otimes I}^{99} \otimes F_1$

- Does that mean that probabilistic computing is not possible?
- Certainly not!

Implementing Probabilistic Computing

- We cannot write down the full distribution on 1000 bits
- To generate a random bit, we flip a fair coin and record its value as 0 or 1
  - rather than the distribution on 2^n values, we just record one value
  - that requires only n bits
- Deterministic operations take us from one specific value to another
  - stochastic operations are a combination of coin flips and deterministic ops

Sampling

- Output is not the distribution but a *sample* from that distribution
- If we were to run it many times, we should find that each output arises the fraction of times indicated by the distribution
- For decision problems (BPP), the output is just {0, 1} and we need only a 67% probability of sampling the correct answer

Meaning of Probabilistic States

- Probabilistic states represent our knowledge of the system
  - state $[0.6, 0.4]^T$ means that 60% of these situations would give a 0
- However, the actual bit really is a 0 or 1!

2^n

- This will not be true for quantum states.
  - that is the crux of why quantum systems are hard to simulate

Sampling of Quantum States

- For quantum computation, the output will also be a random sample
- The fact that we cannot write down the states of that computation does not rule out the possibility that we can generate the samples another way
  - some probabilistic computation could produces the same distribution
- For most problems of simulating quantum systems, we expect that is not possible
- But in general, the burden of proof is on us to show that it cannot be done
  - for some problems (e.g., factoring) the evidence is fairly strong