Lecture 4

A considerable part of this class will study randomized computation for two reasons:

1. quantum computation can be used to perform randomized computation (essentially because complex numbers are a superset of non-negative numbers–probabilities): in fact, many quantum algorithms, such as Shor's, have some non-trivial randomized (but non-quantum) component.

2. we want to argue that quantum computers can be *strictly faster* than randomized computers, so we need to study the limitations of the latter.

Basics of randomized information processing

Before quantum, let's understand randomized information processing better first.

Definition 1 (Randomized state)**.** A *randomized state* of n bits is described by a column vector of length 2^n:

$$\vec{p} := [p_{0^n}, p_{0^{n-1}1}, \ldots, p_{1^n}]^\top \tag{9}$$

such that

1. non-negativity: $p_x \geq 0$ for all $x \in \{0,1\}^n$,

2. normalization $\sum_{x\in\{0,1\}^n} p_x = 1$.

Vectors $\vec{p}$ of the above form are also referred to as probability vectors or probability distributions.

If exactly one of the p_xs is non-zero, then the randomized state can also be referred to as a *deterministic state.*

For example, the state \$0 (recall, \$ denotes a fair coin toss) is represented by the column vector

$$[1/2, 0, 1/2, 0]^\top \tag{10}$$

where the indexing is

(11)

00	01	10	11
1/2	0	1/2	0

Suppose I XORed the first bit onto the second bit (this operation sometimes goes under the name CNOT or $\text{CNOT}_{1\to 2}$ or $\text{CNOT}_{1,2}$ to be more precise), what happens? Well, $00 \mapsto 00$, $01 \mapsto 01$, $10 \mapsto 11$, and $11 \mapsto 10$. Suppose I then flipped the first bit (denote as NOT here or NOT_1), what happens? Well, $00 \mapsto 10$, $01 \mapsto 11$, $10 \mapsto 00$, and $11 \mapsto 01$.

(12)

	00	01	10	11
	1/2	0	1/2	0
$\text{CNOT}_{1,2}$	1/2	0	0	1/2
then NOT_1	0	1/2	1/2	0

Let's think about doing the operations in a different order.

(13)

	00	01	10	11
	1/2	0	1/2	0
NOT_1	1/2	0	1/2	0
then $\text{CNOT}_{1,2}$	1/2	0	0	1/2

A key message:

Doing operations in different orders can change the outcome.

Quiz: can doing these operations in different orders change the outcome if we started in a deterministic state? Yes (in fact, in this case, the outcomes changes for all deterministic states)! This message carries over into the quantum case. Why? Again, because quantum is a generalization of randomized, which is a generalization of deterministic.

Puzzle 1. *We just saw that the order matter when the initial state is* $[1/2, 0, 1/2, 0]^\top$ *(and a deterministic state), but are there initial states for which the order doesn't matter? If so, can we characterize them as a set?*

Comment: pause for an example, but note that the set of answers could be larger, at least apriori
To answer this question, useful to adopt a more sophisticated view of operations.

$$\text{CNOT} = \begin{array}{c|cccc} & 00 & 01 & 10 & 11 \\ \hline 00 & 1 & 0 & 0 & 0 \\ 01 & 0 & 1 & 0 & 0 \\ 10 & 0 & 0 & 0 & 1 \\ 11 & 0 & 0 & 1 & 0 \end{array} \tag{14}$$

Comment: Check that CNOT carries 10 to 11 by matrix multiplication.

$$\text{NOT} = \begin{array}{c|cccc} & 00 & 01 & 10 & 11 \\ \hline 00 & 0 & 0 & 1 & 0 \\ 01 & 0 & 0 & 0 & 1 \\ 10 & 1 & 0 & 0 & 0 \\ 11 & 0 & 1 & 0 & 0 \end{array} \tag{15}$$

Then what we observed before is that

$$\text{NOT}_1 \cdot \text{CNOT}_{1,2} \begin{pmatrix} 1/2 \\ 0 \\ 1/2 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1/2 \\ 1/2 \\ 0 \end{pmatrix} \neq \begin{pmatrix} 1/2 \\ 0 \\ 0 \\ 1/2 \end{pmatrix} = \text{CNOT}_{1,2} \cdot \text{NOT}_1 \begin{pmatrix} 1/2 \\ 0 \\ 1/2 \\ 0 \end{pmatrix} \tag{16}$$