# Exercise Sheet 11:
# Randomised Computation and Quantum Computing

David Carral

February 5, 2020

# Exercise 1

Let $X_1, X_2, \ldots$ be a sequence of independent random variables such that, for all $i \in \mathbb{N}$, $X_i \in \{0,1\}$ and $P(X_i = 1) = p$ for some $0 < p < 1$. Using this sequence $X_1, X_2, \ldots$, describe a way to construct a sequence $Y_1, Y_2, \ldots$ such that, for all $i \in \mathbb{N}$, $Y_i \in \{0,1\}$ and $P(Y_i = 1) = P(Y_i = 0) = \frac{1}{2}$.

*Remark:* The construction may have a zero probability to fail.

**Solution.**

- We solve a simpler problem first. Namely, we describe a way to construct $Z_1, Z_2, \ldots$ such that $Z_i \in \{-1, 0, 1\}$ and $P(Z_i = 1) = P(Z_i = 0)$ for all $i \geq 1$.
- For all $i \geq 1$, let $Z_i = 1$ if $X_{2i} \neq X_{2i+1}$ and $X_{2i} = 1$, $Z_i = 0$ if $X_{2i} \neq X_{2i+1}$ and $X_{2i} = 0$, and $Z_i = -1$ if $X_{2i} = X_{2i+1}$.
- For all $i \geq 1$, $P(Z_i = 1) = P(X_{2i} = 1) \cdot P(X_{2i+1} = 0) = p \times (1 - p)$. Moreover, $P(Z_i = 0) = P(X_{2i+1} = 0) \cdot P(X_{2i} = 1) = (1 - p) \times p$.
- For all $i \geq 1$, let $Y_i$ be the $i$-th digit in $Z_1, Z_2, \ldots$ which is not a $-1$. That is, $Y_1, Y_2, \ldots$ is the string that results from removing every $-1$ from $Z_1, Z_2, \ldots$
- The bit $Y_i$ for some $i \geq 0$ may not be defined, but this event has 0 probability.

# Exercise 2

Consider the following alternative definition of $\mathrm{ZPP}$:
A language **L** is in $\mathrm{AZPP}$ if and only if there exists some polynomial time PTM $\mathcal{M}$ that answers Accept (A), Reject (R), or Inconclusive (I), and all of the following hold.

- For all $w \in \mathbf{L}$, $\mathcal{M}$ always returns A or I.
- For all $w \notin \mathbf{L}$, $\mathcal{M}$ always returns R or I.
- For all $w \in \Sigma^*$, $\Pr[\mathcal{M}(w) = \mathrm{I}] < \frac{1}{2}$.

**Solution.** We show that $\mathrm{ZPP} \subseteq \mathrm{AZPP}$.

1. Let **L** be some arbitrarily chosen language in $\mathrm{ZPP}$.
2. By (1), there is a PTM $\mathcal{M}$ that decides **L** and has expected runtime $p(n)$ with $p(n)$ a polynomial function.
3. Let $\mathcal{M}'$ be a TM that, on input $w$, simulates $\mathcal{M}$ for $3 \times p(|w|)$ steps. Then, if $\mathcal{M}$ accepts, return A; if $\mathcal{M}$ rejects, return R; and otherwise, return I.
4. By (2) and (3), $\mathcal{M}'$ always returns A or I for all $w \in \mathbf{L}$.
5. By (2) and (3), $\mathcal{M}'$ always returns R or I for all $w \notin \mathbf{L}$.
6. By (2) and (3), $\Pr[\mathcal{M}'(w) = \mathrm{I}] < \frac{1}{3}$ for all $w \in \Sigma^*$ (use Markov's inequality: $P(X > a) \leq \frac{E[X]}{a}$.).
7. By (3–6), $\mathbf{L} \in \mathrm{AZPP}$.

# Exercise 2

Consider the following alternative definition of $\mathrm{ZPP}$:
A language **L** is in $\mathrm{AZPP}$ if and only if there exists some polynomial time PTM $\mathcal{M}$ that answers Accept (A), Reject (R), or Inconclusive (I), and all of the following hold.

- For all $w \in \mathbf{L}$, $\mathcal{M}$ always returns A or I.
- For all $w \notin \mathbf{L}$, $\mathcal{M}$ always returns R or I.
- For all $w \in \Sigma^*$, $\Pr[\mathcal{M}(w) = \mathrm{I}] < \frac{1}{2}$.

**Solution.** We show that $\mathrm{AZPP} \subseteq \mathrm{ZPP}$.

1. Let **L** be some arbitrarily chosen language in $\mathrm{AZPP}$.
2. By (1), there is a PTM $\mathcal{M}$ bounded by some polynomial $p(n)$ that satisfies the above restrictions.
3. Let $\mathcal{M}'$ be the TM that simulates $\mathcal{M}$ repeatedly until one of these simulations outputs A or R.
4. By (3), $L(\mathcal{M}') = \mathbf{L}$.
5. By (3), the expected runtime of $\mathcal{M}'$ is $2 \times p(n)$.
   - Worst case expected runtime of $\mathcal{M}'$: $\frac{1}{2} \times p(n) + \frac{1}{4} \times 2 \times p(n) + \frac{1}{8} \times 3 \times p(n) + \ldots$
   - $p(n) \times \Sigma_{i=1}^{\infty} \frac{i}{2^i} = 2 \times p(n)$.
6. By (3–5), $\mathbf{L} \in \mathrm{ZPP}$.

# Exercise 3

Prove Theorem 23.7 (see slide 18 of lecture 23).

**Theorem.** Consider a language **L** and a polynomially time-bounded PTM $\mathcal{M}$ for which there is some $c > 0$ such that, for every word $w \in \Sigma^*$,

- if $w \in \mathbf{L}$ then $\Pr[\mathcal{M} \text{ accepts } w] \geq \frac{1}{|w|^c}$
- if $w \notin \mathbf{L}$ then $\Pr[\mathcal{M} \text{ accepts } w] = 0$

Then, for every $d > 0$, there is a polynomially time-bounded PTM $\mathcal{M}'$ such that

- if $w \in \mathbf{L}$ then $\Pr[\mathcal{M}' \text{ accepts } w] \geq 1 - \frac{1}{2^{|w|^d}}$
- if $w \notin \mathbf{L}$ then $\Pr[\mathcal{M}' \text{ accepts } w] = 0$.

# Exercise 3

**Theorem.** Consider a language **L** and a polynomially time-bounded PTM $\mathcal{M}$ for which there is some $c > 0$ such that, for every word $w \in \Sigma^*$,

- if $w \in \mathbf{L}$ then $\Pr[\mathcal{M} \text{ rejects } w] \leq 1 - \frac{1}{|w|^c}$
- if $w \notin \mathbf{L}$ then $\Pr[\mathcal{M} \text{ accepts } w] = 0$

Then, for every $d > 0$, there is a polynomially time-bounded PTM $\mathcal{M}'$ such that

- if $w \in \mathbf{L}$ then $\Pr[\mathcal{M}' \text{ rejects } w] \leq \frac{1}{2^{|w|^d}}$
- if $w \notin \mathbf{L}$ then $\Pr[\mathcal{M}' \text{ accepts } w] = 0$.

**Solution.**

- Let $\mathcal{M}$ be the TM defined above.
- For every $w \in \mathbf{L}$, $\Pr[\mathcal{M} \text{ rejects } w] \leq 1 - \frac{1}{|w|^c}$
- Let $\mathcal{M}_k$ be the TM that, on input $w$, simulates $|w|^k$-times the computation of $\mathcal{M}$ on $w$. If any of these simulations accept, then $\mathcal{M}_k$ *accepts*. Otherwise, reject.
- $\mathcal{M}_k$ is poly-time bounded.
- For every $w \notin \mathbf{L}$, $\Pr[\mathcal{M}_k \text{ accepts } w] = 0$.
- For every $w \in \mathbf{L}$, $\Pr[\mathcal{M}_k \text{ rejects } w] \leq (1 - \frac{1}{|w|^c})^{|w|^k}$.
- Let $c, d > 0$. Choose $k$ such that $(1 - \frac{1}{|w|^c})^{|w|^k} \leq \frac{1}{2^{|w|^d}}$ for all $w \in \Sigma^*$.
- Let $c, d > 0$. Choose $k$ such that $(1 - \frac{1}{n^c})^{n^k} \leq \frac{1}{2^{n^d}}$ for all $n \in \mathbb{N}$.

# Exercise 3

**Solution.**
Let $c, d > 0$. Choose $k$ such that $(1 - \frac{1}{n^c})^{n^k} \leq \frac{1}{2^{n^d}}$ for all $n \in \mathbb{N}$.

- Let $k = d + c$
- $(1 - \frac{1}{n^c})^{n^{c+d}} \leq (\frac{1}{2})^{n^d}$
- $(1 - \frac{1}{n^c})^{\frac{n^{c+d}}{n^d}} \leq \frac{1}{2}$
- $(1 - \frac{1}{n^c})^{n^c} \leq \frac{1}{2}$

Note that, $\left(1 - \frac{1}{x}\right)^x$ for all $x \geq 1$ is monotonic and

$$\lim_{x \to \infty} \left(1 - \frac{1}{x}\right)^x = \lim_{x \to \infty} e^{\ln\left(1 - \frac{1}{x}\right)^x} = e^{-1} = \frac{1}{e}$$

Detailed explanation for the above: `https://socratic.org/questions/how-do-you-find-the-limit-of-1-1-x-x-as-x-approaches-infinity`

# Exercise 4

Let **UPath** be the set of all tuples $\langle G, s, t \rangle$ with $G$ an undirected graph, and $s$ and $t$ are two connected vertices in $G$. Show that **UPath** $\in \mathrm{RL}$.

**Theorem.** Let $G$ be some undirected graph and let $s$ and $t$ be some vertices in $G$. If $s$ is connected to $t$, then the expected number of steps it takes for a walk from $s$ to hit $t$ is at most $10n^4$.

**Solution.**

- *Markov's inequality:* $P(X > a) \leq \frac{E[X]}{a}$. Hence, $P(X > 100n^4) \leq \frac{10n^4}{100n^4} = \frac{1}{10}$.
- Let $\mathcal{M}$ be the PTM that, on input $\langle G, s, t \rangle$, performs the following computation:
  - Initialise a counter with $100n^4$.
  - Take a random walk of $100n^4$ steps.
  - If we encounter $t$ during this walk, *accept*. Otherwise, *reject*.
- For all $w \notin$ **UPath**, $\mathcal{M}$ rejects $w$.
- For all $w \in$ **UPath**, $\Pr[\mathcal{M}(w) = 1] \geq \frac{9}{10}$.

# Exercise 5

Review the updated slides from Lecture 24, and especially slides 13–18 on calculating the odds in a quantum-based game strategy.

1. Can Bob use the experiment to learn about Alice's choice, possibly by repeating the experiment with many pairs of entangled particles? Compute the chances of Bob measuring 0 in each case considered on the slides.
2. Suppose Alice measures her bit without any rotation happening before. Specify the possible states of Bob's remaining 1-qubit system after this.
3. Consider the case $x = 0$ and $y = 1$, and the following order of events: Alice measures, Bob rotates, Bob measures. What is the probability of the game being won in this case.

# Exercise 5

Two players, Alice and Bob, are in physically separated locations:

- The game master throws two coins: $x, y \in \{0, 1\}$
- The value of $x$ is communicated to Alice, the value of $y$ to Bob
- Alice must answer with a bit $a \in \{0, 1\}$, and Bob with a bit $b \in \{0, 1\}$
- The players win if $a \oplus b = x \wedge y$.

*A strategy that uses Quantum Mechanics:*

- Alice and Bob create an entangled quantum state $\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$
- Alice takes the first bit (particle); Bob the second.
- Alice's strategy: if $x = 1$, rotate the first bit by $\pi/8$ (22.5 degrees), otherwise do nothing; then measure the first bit and answer with its value
- Bob's strategy: if $y = 1$, rotate the second bit by $-\pi/8$ (-22.5 degrees), otherwise do nothing; then measure the second bit and answer with its value

# Exercise 5

Can Bob use the experiment to learn about Alice's choice, possibly by repeating the experiment with many pairs of entangled particles? Compute the chances of Bob measuring 0 in each case considered on the slides.

Case 1: $x = 0$ and $y = 0$.
None of them rotate.

$$\begin{pmatrix} \frac{1}{\sqrt{2}} \\ 0 \\ 0 \\ \frac{1}{\sqrt{2}} \end{pmatrix} \begin{array}{l} \text{corresponds to } |00\rangle \\ \text{corresponds to } |01\rangle \\ \text{corresponds to } |10\rangle \\ \text{corresponds to } |11\rangle \end{array}$$

The players win if $a \oplus b = x \wedge y$. That is, they win if $a = b$.
The probability of this happening is $(\frac{1}{\sqrt{2}})^2 + (\frac{1}{\sqrt{2}})^2 = 1$.

The probability of Bob's bit (i.e., the second bit) being 0 is $(\frac{1}{\sqrt{2}})^2 = \frac{1}{2}$.

# Exercise 5

Can Bob use the experiment to learn about Alice's choice, possibly by repeating the experiment with many pairs of entangled particles? Compute the chances of Bob measuring 0 in each case considered on the slides.

Case 2: $x = 0$ and $y = 1$.
Bob rotates; Alice does not do anything.

$$\begin{pmatrix} \cos\frac{\pi}{8} & \sin\frac{\pi}{8} & 0 & 0 \\ -\sin\frac{\pi}{8} & \cos\frac{\pi}{8} & 0 & 0 \\ 0 & 0 & \cos\frac{\pi}{8} & \sin\frac{\pi}{8} \\ 0 & 0 & -\sin\frac{\pi}{8} & \cos\frac{\pi}{8} \end{pmatrix} \begin{pmatrix} \frac{1}{\sqrt{2}} \\ 0 \\ 0 \\ \frac{1}{\sqrt{2}} \end{pmatrix} = \begin{pmatrix} \frac{1}{\sqrt{2}}\cos\frac{\pi}{8} \\ -\frac{1}{\sqrt{2}}\sin\frac{\pi}{8} \\ \frac{1}{\sqrt{2}}\sin\frac{\pi}{8} \\ \frac{1}{\sqrt{2}}\cos\frac{\pi}{8} \end{pmatrix} \begin{matrix} \text{corresponds to } |00\rangle \\ \text{corresponds to } |01\rangle \\ \text{corresponds to } |10\rangle \\ \text{corresponds to } |11\rangle \end{matrix}$$

The players win if $a \oplus b = x \wedge y$. That is, they win if $a = b$.
The probability of this happening is $2(\frac{1}{\sqrt{2}}\cos\frac{\pi}{8})^2 = (\cos\frac{\pi}{8})^2 > 0.853$

The probability of Bob's bit (i.e., the second bit) being 0 is $(\frac{1}{\sqrt{2}}\cos\frac{\pi}{8})^2 + (\frac{1}{\sqrt{2}}\sin\frac{\pi}{8})^2 = \frac{1}{2}$.

# Exercise 5

Can Bob use the experiment to learn about Alice's choice, possibly by repeating the experiment with many pairs of entangled particles? Compute the chances of Bob measuring 0 in each case considered on the slides.

Case 3: $x = 1$ and $y = 0$.
Alice rotates; Bob does not do anything.

$$\begin{pmatrix} \cos\frac{\pi}{8} & 0 & -\sin\frac{\pi}{8} & 0 \\ 0 & \cos\frac{\pi}{8} & 0 & -\sin\frac{\pi}{8} \\ \sin\frac{\pi}{8} & 0 & \cos\frac{\pi}{8} & 0 \\ 0 & \sin\frac{\pi}{8} & 0 & \cos\frac{\pi}{8} \end{pmatrix} \begin{pmatrix} \frac{1}{\sqrt{2}} \\ 0 \\ 0 \\ \frac{1}{\sqrt{2}} \end{pmatrix} = \begin{pmatrix} \frac{1}{\sqrt{2}}\cos\frac{\pi}{8} \\ -\frac{1}{\sqrt{2}}\sin\frac{\pi}{8} \\ \frac{1}{\sqrt{2}}\sin\frac{\pi}{8} \\ \frac{1}{\sqrt{2}}\cos\frac{\pi}{8} \end{pmatrix} \begin{matrix} \text{corresponds to } |00\rangle \\ \text{corresponds to } |01\rangle \\ \text{corresponds to } |10\rangle \\ \text{corresponds to } |11\rangle \end{matrix}$$

The players win if $a \oplus b = x \wedge y$. That is, they win if $a = b$.
The probability of this happening is $2(\frac{1}{\sqrt{2}}\cos\frac{\pi}{8})^2 = (\cos\frac{\pi}{8})^2 > 0.853$

The probability of Bob's bit (i.e., the second bit) being 0 is $(\frac{1}{\sqrt{2}}\cos\frac{\pi}{8})^2 + (\frac{1}{\sqrt{2}}\sin\frac{\pi}{8})^2 = \frac{1}{2}$.

# Exercise 5

Case 4: $x = 1$ and $y = 1$.
Bob rotates.

$$\begin{pmatrix} \cos\frac{\pi}{8} & \sin\frac{\pi}{8} & 0 & 0 \\ -\sin\frac{\pi}{8} & \cos\frac{\pi}{8} & 0 & 0 \\ 0 & 0 & \cos\frac{\pi}{8} & \sin\frac{\pi}{8} \\ 0 & 0 & -\sin\frac{\pi}{8} & \cos\frac{\pi}{8} \end{pmatrix} \begin{pmatrix} \frac{1}{\sqrt{2}} \\ 0 \\ 0 \\ \frac{1}{\sqrt{2}} \end{pmatrix} = \begin{pmatrix} \frac{1}{\sqrt{2}}\cos\frac{\pi}{8} \\ -\frac{1}{\sqrt{2}}\sin\frac{\pi}{8} \\ \frac{1}{\sqrt{2}}\sin\frac{\pi}{8} \\ \frac{1}{\sqrt{2}}\cos\frac{\pi}{8} \end{pmatrix} \begin{matrix} \text{corresponds to } |00\rangle \\ \text{corresponds to } |01\rangle \\ \text{corresponds to } |10\rangle \\ \text{corresponds to } |11\rangle \end{matrix}$$

Then Alice rotates.

$$\begin{pmatrix} \cos\frac{\pi}{8} & 0 & -\sin\frac{\pi}{8} & 0 \\ 0 & \cos\frac{\pi}{8} & 0 & -\sin\frac{\pi}{8} \\ \sin\frac{\pi}{8} & 0 & \cos\frac{\pi}{8} & 0 \\ 0 & \sin\frac{\pi}{8} & 0 & \cos\frac{\pi}{8} \end{pmatrix} \begin{pmatrix} \frac{1}{\sqrt{2}}\cos\frac{\pi}{8} \\ -\frac{1}{\sqrt{2}}\sin\frac{\pi}{8} \\ \frac{1}{\sqrt{2}}\sin\frac{\pi}{8} \\ \frac{1}{\sqrt{2}}\cos\frac{\pi}{8} \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} (\cos\frac{\pi}{8})^2 - (\sin\frac{\pi}{8})^2 \\ -2\cos\frac{\pi}{8}\sin\frac{\pi}{8} \\ 2\cos\frac{\pi}{8}\sin\frac{\pi}{8} \\ (\cos\frac{\pi}{8})^2 - (\sin\frac{\pi}{8})^2 \end{pmatrix} = \begin{pmatrix} \frac{1}{2} \\ -\frac{1}{2} \\ \frac{1}{2} \\ \frac{1}{2} \end{pmatrix}$$

The players win if $a \oplus b = x \wedge y$. That is, they win if $a \neq b$.
The probability of this happening is $(-\frac{1}{2})^2 + (\frac{1}{2})^2 = \frac{1}{2}$.

The probability of Bob's bit (i.e., the second bit) being 0 is $(\frac{1}{2})^2 + (\frac{1}{2})^2 = \frac{1}{2}$.

# Exercise 5

Suppose Alice measures her bit without any rotation happening before. Specify the possible states of Bob's remaining 1-qubit system after this.

$$\begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} \quad \text{or} \quad \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

corresponds to $|00\rangle$
corresponds to $|01\rangle$
corresponds to $|10\rangle$
corresponds to $|11\rangle$

# Exercise 5

Consider the case $x = 0$ and $y = 1$, and the following order of events: Alice measures, Bob rotates, Bob measures. What is the probability of the game being won in this case.

Case 1: Alice reads a 0.

$$\begin{pmatrix} \cos\frac{\pi}{8} & \sin\frac{\pi}{8} & 0 & 0 \\ -\sin\frac{\pi}{8} & \cos\frac{\pi}{8} & 0 & 0 \\ 0 & 0 & \cos\frac{\pi}{8} & \sin\frac{\pi}{8} \\ 0 & 0 & -\sin\frac{\pi}{8} & \cos\frac{\pi}{8} \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} \cos\frac{\pi}{8} \\ -\sin\frac{\pi}{8} \\ 0 \\ 0 \end{pmatrix} \quad \begin{array}{l} \text{corresponds to } |00\rangle \\ \text{corresponds to } |01\rangle \\ \text{corresponds to } |10\rangle \\ \text{corresponds to } |11\rangle \end{array}$$

Alice and Bob win the game if $a = b$.
The probability of this happening is $(\cos\frac{\pi}{8})^2 > 0.853$.

# Exercise 5

Consider the case $x = 0$ and $y = 1$, and the following order of events: Alice measures, Bob rotates, Bob measures. What is the probability of the game being won in this case.

Case 2: Alice reads a 1.

$$\begin{pmatrix} \cos\frac{\pi}{8} & \sin\frac{\pi}{8} & 0 & 0 \\ -\sin\frac{\pi}{8} & \cos\frac{\pi}{8} & 0 & 0 \\ 0 & 0 & \cos\frac{\pi}{8} & \sin\frac{\pi}{8} \\ 0 & 0 & -\sin\frac{\pi}{8} & \cos\frac{\pi}{8} \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \sin\frac{\pi}{8} \\ \cos\frac{\pi}{8} \end{pmatrix} \begin{array}{l} \text{corresponds to } |00\rangle \\ \text{corresponds to } |01\rangle \\ \text{corresponds to } |10\rangle \\ \text{corresponds to } |11\rangle \end{array}$$

Alice and Bob win the game if $a = b$.
The probability of this happening is $(\cos\frac{\pi}{8})^2 > 0.853$.