Homework 1 things

Basic probability

Def: A discrete probability space is a pair $\langle \Omega, \Pr \rangle$ where Ω is a nonempty set (the sample space, elements of Ω are called outcomes, subsets of Ω are called events), and

$$\Pr : \underbrace{\mathcal{P}(\Omega)}_{\text{set of all events}} \to \mathbb{R}$$

such that

1. $\underbrace{\Pr[E]}_{\text{"the probability of event } E\text{"}} \geq 0$ for all $E \subseteq \Omega$

2. $\Pr[\Omega] = 1$ — Ω is the certain event

3. For any events $A_1, A_2, \dots \subseteq \Omega$ that are pairwise disjoint,

$$\Pr\left[\bigcup_i A_i\right] = \sum_i \Pr[A_i] \quad //$$

An elementary event is an event $\{x\}$ for some $x \in \Omega$

$\Pr(x) = \Pr[\{x\}] =: p(x)$

Then $\forall A \subseteq \Omega$,

$$\Pr[A] = \sum_{x \in A} p(x)$$

[$A = \{x_1, \dots, x_n\}$, then $\{x_1\}, \dots, \{x_n\}$ are disjoint and $A = \bigcup_{x \in A} \{x\}$. Then use (axiom 3).]

In particular,

$$1 = \Pr[\Omega] = \sum_{x \in \Omega} p(x)$$

So, for any $A \subseteq \Omega$,

$$0 \leq \Pr[A] = \sum_{x \in A} p(x) \leq \sum_{x \in \Omega} p(x) = 1$$

$\therefore \quad 0 \leq P[A] \leq 1$

A random experiment is just a probability space.

Important: $\Pr$ is completely determined by the probabilities $p(x)$ $(x \in \Omega)$

Have: $p(x) \geq 0 \quad \forall x$

$$\sum_{x \in \Omega} p(x) = 1$$

p is a probability distribution which we will call any vector $(p_1, \dots)$ such that $p_i \geq 0 \quad \forall i$ & $\sum_i p_i = 1$.

$A \subseteq \Omega$, define

$$\overline{A} := \Omega - A$$

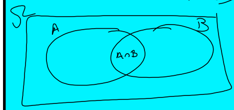
so

$$\Pr[\overline{A}] = 1 - \Pr[A]$$

[$A \setminus B$ means $A - B$
$= \{x : x \in A \text{ \& } x \notin B\}$]

Given $A, B \subseteq \Omega$ such that $\Pr[B] > 0$, Define the (<u>conditional</u>) probability of A <u>given B</u> as

$$P[A \mid B] \doteq \frac{\Pr[A \cap B]}{\Pr[B]}$$



<u>Chain Rule</u>: Let $A_1, \ldots, A_n$ be events in Ω.

$$\Pr[A_1 \cap \cdots \cap A_n] =$$

$$\Pr[A_1] \cdot \Pr[A_2 \mid A_1] \cdot \Pr[A_3 \mid A_1 \cap A_2] \cdots \Pr[A_n \mid A_1 \cap \cdots \cap A_{n-1}]$$

$$= \prod_{i=1}^{n} \Pr[A_i \mid A_1 \cap \cdots \cap A_{i-1}]$$

[an empty intersection is Ω by convention & $P[A_1] = \Pr[A_1 \mid \Omega]$]

(Useful for Ex 1.25)

<u>Ex 1.25</u>: Given uniformly random $n \times n$ matrix A over $\mathbb{Z}_2 = \{0,1\}$, what is the prob that A is nonsingular (invertible)?

A is invertible iff

1. It's first row is nonzero vector (prob $= 1 - 2^{-n}$)
2. For $i := 2, \ldots, n$, the first i rows of A are lin indep, given that the first $i-1$ rows are lin indep.

By the chain rule, the answer is the product of all these (conditional) probabilities.

How to calculate 2?

Given $i-1$ rows lin indep, They span a subspace of dimension $i-1$, so size 2^{i-1}. The whole n-dim space over $\mathbb{Z}_2$ has size 2^n. Row i is lin indep from the prev $i-1$ rows iff it is not in the span of the previous $i-1$ rows.

So prob is $2^{-n}(2^n - 2^{i-1})$

$$= 1 - \frac{2^{i-1}}{2^n} = \cdots$$

Hint for Ex 1.13:

Consider $\ell(A+B, A+B)$ & use properties of ℓ.

<u>Def</u>: $\langle \Omega, \Pr \rangle$ prob space, $A, B \subseteq \Omega$ are <u>independent</u> if $\Pr[A \cap B] = \Pr[A]\Pr[B]$

(equiv. $\Pr[A \mid B] = \Pr[A]$
$\Pr[B \mid A] = \Pr[B]$)

A few more rules:

$\Pr[\emptyset] = 0$

$A \subseteq B \Rightarrow \Pr[A] \le \Pr[B]$

$\Pr[A \cup B] = \Pr[A] + \Pr[B] - \Pr[A \cap B]$

$\Pr[A] = \Pr[A \cap B] + \Pr[A \setminus B]$

Ex 1.15: Any $n \times n$ matrix A.

$$\operatorname{tr} A = \sum_{i=1}^{n} [A]_{ii}$$

Properties: (1) $\operatorname{tr}(AB) = \operatorname{tr}(BA)$

$\therefore \operatorname{tr}(ABC) = \operatorname{tr}(CAB) = \operatorname{tr}(BCA)$

(cyclic property of the trace).

(2a) $\operatorname{tr}(aA) = a \operatorname{tr}(A)$

(2b) $\operatorname{tr}(A+B) = \operatorname{tr} A + \operatorname{tr} B$

(linearity)

(3) $\operatorname{tr} I = n$ ($n \times n$ identity matrix)

Recall: $e_i := \begin{bmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix} \leftarrow i\text{th place}$

$$\forall i,j,\quad E_{ij} := \underbrace{e_i e_j^T}_{\text{any scalar field}} = \underbrace{e_i e_j^*}_{\text{for } \mathbb{C}\text{-spaces}}$$

$$= \begin{array}{c} \\ \\ \\ i \rightarrow \\ \\ \\ \end{array} \underbrace{\begin{bmatrix} 0 \\ \vdots \\ 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix}}_{e_i} \underbrace{\begin{array}{c} \qquad\qquad j\text{th} \downarrow \\ \begin{bmatrix} 0 \cdots 0 & 1 & 0 \cdots 0 \end{bmatrix} \end{array}}_{e_j^T}$$

$$= \begin{array}{c} \\ i\text{th row} \rightarrow \\ \\ \end{array} \begin{bmatrix} & & \\ & 1 & \\ & & \end{bmatrix}$$
$$\qquad \uparrow j\text{th column}$$

zeros everywhere else.

Any matrix ($m \times n$, say)

$$A = \sum_{i=1}^{m} \sum_{j=1}^{n} [A]_{ij} E_{ij}.$$

---

tr is linear means tr is completely determined by its behavior on the $\{E_{ij}\}$ basis

Suffices to show then, that $\operatorname{tr} E_{ij} = \delta_{ij}$

$$= \begin{cases} 1 & \text{if } i=j \\ 0 & \text{o.w} \end{cases}$$

<u>How?</u> Also useful: $\forall i,j,k,l$

$$E_{ij} E_{kl} = \delta_{jk} E_{il} = \begin{cases} E_{il} & \text{if } j=k \\ 0 & \text{if } j \ne k. \end{cases}$$

<u>Hint</u>: Consider $\operatorname{tr}(E_{ij} E_{kl})$

$= \operatorname{tr}(E_{kl} E_{ij})$ (by axiom (1))

for various i,j,k,l.

[$\operatorname{tr} 0 = 0$ by linearity axioms 2a, 2b]

<u>Qubit geometry</u>

An arbitrary single qubit state is

$$|\psi\rangle = e^{i\psi}\left(\cos\frac{\theta}{2}\begin{bmatrix}1\\0\end{bmatrix} + e^{i\varphi}\sin\frac{\theta}{2}\begin{bmatrix}0\\1\end{bmatrix}\right)$$

where $0 \le \theta \le \pi$

$0 \le \varphi, \psi < 2\pi$.

An arbitrary single qubit state is

$$|\psi\rangle = e^{i\psi}\left(\cos\frac{\theta}{2}\begin{bmatrix}1\\0\end{bmatrix} + e^{i\varphi}\sin\frac{\theta}{2}\begin{bmatrix}0\\1\end{bmatrix}\right)$$

where $0 \le \theta \le \pi$

$0 \le \varphi, \psi < 2\pi$.

ψ is physically irrelevant and can be any value ($\psi = 0$, say)

$$|\psi\rangle = \cos\frac{\theta}{2}\begin{bmatrix}1\\0\end{bmatrix} + e^{i\varphi}\sin\frac{\theta}{2}\begin{bmatrix}0\\1\end{bmatrix}$$

Spherical (in $\mathbb{R}^3$) coordinates

$$\underbrace{(x, y, z)}_{\text{cartesian coords}} = \underbrace{(\cos\varphi\sin\theta, \sin\varphi\sin\theta, \cos\theta)}_{\text{spherical coords}}$$