Basics of Discrete Probability and Randomized Algorithms

Fahad Panolan

Indian Institute of Technology Hyderabad, India

27-Aug-2022

Slides from Prof. Chandra Chekuri (modified as needed)

Basics of Discrete Probability

Discrete Probability

Definition

A discrete probability space is a pair $(\Omega, \Pr)$ where

- Ω is a countable set, called the set of elementary events.
- $\Pr : \Omega \to [0,1]$ such that $\sum_{\omega\in\Omega} \Pr[\omega] = 1$.

Discrete Probability

Definition

A discrete probability space is a pair $(\Omega, \Pr)$ where

- Ω is a countable set, called the set of elementary events.
- $\Pr : \Omega \to [0, 1]$ such that $\sum_{\omega \in \Omega} \Pr[\omega] = 1$.

Examples

- An unbiased coin.

Discrete Probability

Definition

A discrete probability space is a pair $(\Omega, \Pr)$ where

- Ω is a countable set, called the set of elementary events.
- $\Pr : \Omega \to [0, 1]$ such that $\sum_{\omega \in \Omega} \Pr[\omega] = 1$.

Examples

- An unbiased coin. $\Omega = \{H, T\}$ and $\Pr[H] = \Pr[T] = 1/2$.

Discrete Probability

Definition

A discrete probability space is a pair $(\Omega, \Pr)$ where

- Ω is a countable set, called the set of elementary events.
- $\Pr : \Omega \to [0,1]$ such that $\sum_{\omega \in \Omega} \Pr[\omega] = 1$.

Examples

- An unbiased coin. $\Omega = \{H, T\}$ and $\Pr[H] = \Pr[T] = 1/2$.
- A 6-sided unbiased die.

Discrete Probability

Definition

A discrete probability space is a pair $(\Omega, \Pr)$ where

- Ω is a countable set, called the set of elementary events.
- $\Pr : \Omega \to [0, 1]$ such that $\sum_{\omega \in \Omega} \Pr[\omega] = 1$.

Examples

- An unbiased coin. $\Omega = \{H, T\}$ and $\Pr[H] = \Pr[T] = 1/2$.
- A 6-sided unbiased die. $\Omega = \{1, 2, 3, 4, 5, 6\}$ and $\Pr[i] = 1/6$ for all $i \in \Omega$.

Discrete Probability

Definition

A discrete probability space is a pair $(\Omega, \Pr)$ where

- Ω is a countable set, called the set of elementary events.
- $\Pr : \Omega \to [0, 1]$ such that $\sum_{\omega \in \Omega} \Pr[\omega] = 1$.

Examples

- An unbiased coin. $\Omega = \{H, T\}$ and $\Pr[H] = \Pr[T] = 1/2$.
- A 6-sided unbiased die. $\Omega = \{1, 2, 3, 4, 5, 6\}$ and $\Pr[i] = 1/6$ for all $i \in \Omega$.
- A pair of independent dice.

Discrete Probability

Definition

A discrete probability space is a pair $(\Omega, \Pr)$ where

- Ω is a countable set, called the set of elementary events.
- $\Pr : \Omega \to [0, 1]$ such that $\sum_{\omega \in \Omega} \Pr[\omega] = 1$.

Examples

- An unbiased coin. $\Omega = \{H, T\}$ and $\Pr[H] = \Pr[T] = 1/2$.
- A 6-sided unbiased die. $\Omega = \{1, 2, 3, 4, 5, 6\}$ and $\Pr[i] = 1/6$ for all $i \in \Omega$.
- A pair of independent dice. $\Omega = \{(i, j) \mid 1 \leq i \leq 6, 1 \leq j \leq 6\}$ and $\Pr[(i, j)] = 1/36$ for all $(i, j) \in \Omega$.

Events

Definition

Given a probability space $(\Omega, \Pr)$ an event is a subset of Ω. In other words an event is a collection of elementary events. The probability of an event A, denoted by $\Pr[A]$, is $\sum_{\omega \in A} \Pr[\omega]$.

The complement event of an event $A \subseteq \Omega$ is the event $\Omega \setminus A$ frequently denoted by $\bar{A}$.

Events

Definition

Given a probability space $(\Omega, \Pr)$ an event is a subset of Ω. In other words an event is a collection of elementary events. The probability of an event A, denoted by $\Pr[A]$, is $\sum_{\omega \in A} \Pr[\omega]$.

The complement event of an event $A \subseteq \Omega$ is the event $\Omega \setminus A$ frequently denoted by $\bar{A}$.

Example

A pair of independent dice. $\Omega = \{(i, j) \mid 1 \leq i \leq 6, 1 \leq j \leq 6\}$.
Let A be the event that the sum of the two numbers on the dice is even.
Then $A = \{(i, j) \in \Omega : (i + j) \text{ is even}\}$.
$\Pr[A] = |A|/36 = 1/2$.

Independent Events

Definition

Given a probability space $(\Omega, \Pr)$ and two events A, B are independent if and only if

$$\Pr[A \cap B] = \Pr[A]\Pr[B].$$

Otherwise they are dependent. In other words A, B independent implies one does not affect the other.

Independent Events

Definition

Given a probability space $(\Omega, \Pr)$ and two events A, B are independent if and only if

$$\Pr[A \cap B] = \Pr[A] \Pr[B].$$

Otherwise they are dependent. In other words A, B independent implies one does not affect the other.

Example

Two coins. $\Omega = \{HH, TT, HT, TH\}$ and $\Pr[HH] = \Pr[TT] = \Pr[HT] = \Pr[TH] = 1/4$.

- A is the event that the first coin is heads and B is the event that second coin is tails.

Independent Events

Definition

Given a probability space $(\Omega, \Pr)$ and two events A, B are independent if and only if

$$\Pr[A \cap B] = \Pr[A] \Pr[B].$$

Otherwise they are dependent. In other words A, B independent implies one does not affect the other.

Example

Two coins. $\Omega = \{HH, TT, HT, TH\}$ and $\Pr[HH] = \Pr[TT] = \Pr[HT] = \Pr[TH] = 1/4$.

- A is the event that the first coin is heads and B is the event that second coin is tails. A, B **are independent**.

Independent Events

Definition

Given a probability space $(\Omega, \Pr)$ and two events A, B are independent if and only if

$$\Pr[A \cap B] = \Pr[A] \Pr[B].$$

Otherwise they are dependent. In other words A, B independent implies one does not affect the other.

Example

Two coins. $\Omega = \{HH, TT, HT, TH\}$ and $\Pr[HH] = \Pr[TT] = \Pr[HT] = \Pr[TH] = 1/4$.

- A is the event that the first coin is heads and B is the event that second coin is tails. A, B **are independent**.
- A is the event that both are not tails and B is event that second coin is heads.

Independent Events

Definition

Given a probability space $(\Omega, \Pr)$ and two events A, B are independent if and only if

$$\Pr[A \cap B] = \Pr[A] \Pr[B].$$

Otherwise they are dependent. In other words A, B independent implies one does not affect the other.

Example

Two coins. $\Omega = \{HH, TT, HT, TH\}$ and $\Pr[HH] = \Pr[TT] = \Pr[HT] = \Pr[TH] = 1/4$.

- A is the event that the first coin is heads and B is the event that second coin is tails. A, B **are independent**.
- A is the event that both are not tails and B is event that second coin is heads. A, B **are dependent**.

Union bound

The probability of the union of two events, is no bigger than the probability of the sum of their probabilities.

Lemma

For any two events A and B, we have that

$$\Pr[A \cup B] \leq \Pr[A] + \Pr[B].$$

Random Variables and Expectation

Random Variable

Given a probability space $(\Omega, \Pr)$ a random variable X over Ω is

$$X : \Omega \to \mathbb{R}.$$

Random Variables and Expectation

Random Variable

Given a probability space $(\Omega, \Pr)$ a random variable X over Ω is

$$X : \Omega \to \mathbb{R}.$$

Expectation

For a random variable X over a probability space $(\Omega, \Pr)$ the <u>expectation</u> of X is defined as

$$\sum_{\omega \in \Omega} \Pr[\omega] X(\omega).$$

In other words, the expectation is the average value of X according to the probabilities given by $\Pr[\cdot]$.

Expectation: examples

Example

A 6-sided unbiased die. $\Omega = \{1, 2, 3, 4, 5, 6\}$ and $\Pr[i] = 1/6$ for $1 \leq i \leq 6$.

- $X : \Omega \to \mathbb{R}$ where $X(i) = i \mod 2$. Then

$$\mathbf{E}[X] = \sum_{i=1}^{6} \Pr[i] \cdot X(i) = \frac{1}{6} \sum_{i=1}^{6} X(i) = 1/2.$$

Expectation: examples

Example

A 6-sided unbiased die. $\Omega = \{1, 2, 3, 4, 5, 6\}$ and $\Pr[i] = 1/6$ for $1 \le i \le 6$.

- $X : \Omega \to \mathbb{R}$ where $X(i) = i \mod 2$. Then

$$\mathbf{E}[X] = \sum_{i=1}^{6} \Pr[i] \cdot X(i) = \frac{1}{6} \sum_{i=1}^{6} X(i) = 1/2.$$

- $Y : \Omega \to \mathbb{R}$ where $Y(i) = i$. Then

$$\mathbf{E}[Y] = \sum_{i=1}^{6} \frac{1}{6} \cdot i = 3.5.$$

Probabilistic Inequalities

Markov's Inequality

Let X be a **non-negative** random variable over a probability space $(\Omega, \Pr)$. For any $a > 0$,

$$\Pr[X \geq a] \leq \frac{\mathbf{E}[X]}{a}.$$

In other words, for any $t > 0$, $\Pr[X \geq t\mathbf{E}[X]] \leq \frac{1}{t}$.

Markov's Inequality

Let X be a **non-negative** random variable over a probability space $(\Omega, \Pr)$. For any $a > 0$,

$$\Pr[X \geq a] \leq \frac{\mathbf{E}[X]}{a}.$$

In other words, for any $t > 0$, $\Pr[X \geq t\mathbf{E}[X]] \leq \frac{1}{t}$.

Proof:

$$\begin{aligned}
\mathbf{E}[X] &= \textstyle\sum_{\omega \in \Omega} X(\omega) \Pr[\omega] \\
&= \textstyle\sum_{\omega,\ 0 \leq X(\omega) < a} X(\omega) \Pr[\omega] + \sum_{\omega,\ X(\omega) \geq a} X(\omega) \Pr[\omega] \\
&\geq \textstyle\sum_{\omega \in \Omega,\ X(\omega) \geq a} X(\omega) \Pr[\omega] \\
&\geq a \textstyle\sum_{\omega \in \Omega,\ X(\omega) \geq a} \Pr[\omega] \\
&= a \Pr[X \geq a]
\end{aligned}$$

Variance

Variance

Given a random variable X over probability space $(\Omega, \Pr)$, variance of X is the measure of how much does it deviate from its mean value. Formally,

$$Var(X) = \mathbf{E}[(X - \mathbf{E}[X])^2] = \mathbf{E}[X^2] - \mathbf{E}[X]^2.$$

Variance

Variance

Given a random variable X over probability space $(\Omega, \Pr)$, variance of X is the measure of how much does it deviate from its mean value. Formally,

$$Var(X) = \mathbf{E}[(X - \mathbf{E}[X])^2] = \mathbf{E}[X^2] - \mathbf{E}[X]^2.$$

Derivation

Define $Y = (X - \mathbf{E}[X])^2 = X^2 - 2X\mathbf{E}[X] + \mathbf{E}[X]^2$.

$$\begin{aligned} Var(X) &= \mathbf{E}[Y] \\ &= \mathbf{E}[X^2] - 2\mathbf{E}[X]\mathbf{E}[X] + \mathbf{E}[X]^2 \\ &= \mathbf{E}[X^2] - \mathbf{E}[X]^2 \end{aligned}$$

Variance

Variance

Given a random variable X over probability space $(\Omega, \Pr)$, variance of X is the measure of how much does it deviate from its mean value. Formally,

$$Var(X) = \mathbf{E}[(X - \mathbf{E}[X])^2] = \mathbf{E}[X^2] - \mathbf{E}[X]^2.$$

Variance

Variance

Given a random variable X over probability space $(\Omega, \Pr)$, variance of X is the measure of how much does it deviate from its mean value. Formally,

$$Var(X) = \mathbf{E}[(X - \mathbf{E}[X])^2] = \mathbf{E}[X^2] - \mathbf{E}[X]^2.$$

Independence

Random variables X and Y are called mutually independent if

$$\forall x, y \in \mathbb{R},\ \Pr[X = x \land Y = y] = \Pr[X = x]\Pr[Y = y]$$

Variance

Variance

Given a random variable X over probability space $(\Omega, \Pr)$, variance of X is the measure of how much does it deviate from its mean value. Formally,

$$Var(X) = \mathbf{E}[(X - \mathbf{E}[X])^2] = \mathbf{E}[X^2] - \mathbf{E}[X]^2.$$

Independence

Random variables X and Y are called mutually independent if

$$\forall x, y \in \mathbb{R},\ \Pr[X = x \wedge Y = y] = \Pr[X = x] \Pr[Y = y]$$

Lemma

If X and Y are independent random variables then $Var(X + Y) = Var(X) + Var(Y)$.

Chebyshev's Inequality

If $Var(X) < \infty$, then for any $a \geq 0$,

$$\Pr[|X - \mathbf{E}[X]| \geq a] \leq \frac{Var(X)}{a^2}.$$

This implies $\Pr[X \leq \mathbf{E}[X] - a] \leq \frac{Var(X)}{a^2}$ AND $\Pr[X \geq \mathbf{E}[X] + a] \leq \frac{Var(X)}{a^2}$

Chebyshev's Inequality

If $Var(X) < \infty$, then for any $a \geq 0$,

$$\Pr[|X - \mathbf{E}[X]| \geq a] \leq \frac{Var(X)}{a^2}.$$

This implies $\Pr[X \leq \mathbf{E}[X] - a] \leq \frac{Var(X)}{a^2}$ AND $\Pr[X \geq \mathbf{E}[X] + a] \leq \frac{Var(X)}{a^2}$

Proof.

$Y = (X - \mathbf{E}[X])^2$ is a non-negative random variable. Apply Markov's Inequality to Y for a^2.

$$\begin{aligned} \Pr[Y \geq a^2] \leq \frac{\mathbf{E}[Y]}{a^2} \quad &\Leftrightarrow \quad \Pr[(X - \mathbf{E}[X])^2 \geq a^2] \leq \frac{Var(X)}{a^2} \\ &\Leftrightarrow \quad \Pr[|X - \mathbf{E}[X]| \geq a] \leq \frac{Var(X)}{a^2} \end{aligned}$$

$\square$

Chernoff Bound

Let $X_1, \dots, X_k$ be k independent random variables such that, for each $i \in \{1, \dots, k\}$, X_i equals 1 with probability p_i, and 0 with probability $(1 - p_i)$. Let $X = \sum_{i=1}^{k} X_i$ and $\mu = \mathbf{E}[X] = \sum_i p_i$. For any $0 < \varepsilon < 1$, it holds that:

- $\Pr[|X - \mu| \geq \varepsilon\mu] \leq 2e^{\frac{-\varepsilon^2\mu}{3}}$
- $\Pr[X \geq (1+\varepsilon)\mu] \leq e^{\frac{-\varepsilon^2\mu}{3}}$
- $\Pr[X \leq (1-\varepsilon)\mu] \leq e^{\frac{-\varepsilon^2\mu}{2}}$

Thank You.