



Repetition

Probability Theory

Algorithm Theory
WS 2015/16

Fabian Kuhn

Randomized Algorithms

- An algorithm that uses (or can use) **random coin flips** in order to make decisions
- **randomization** can be a **powerful tool** to make algorithms **faster** or **simpler**

First: Short Repetition of Basic Probability Theory

- We need: basic discrete probability theory
 - probability spaces, probability events, independence, random variables, expectation, linearity of expectation, Markov inequality
- Literature, for example
 - your old probability theory book / lecture notes / ...
 - Appendix C of book of Cormen, Rivest, Leiserson, Stein
 - <http://www.ti.inf.ethz.ch/ew/courses/APC15/material/ra.pdf>

Probability Space and Events

Definition: A **probability space** is a pair (Ω, \mathbb{P}) , where

- Ω : set of elementary events
- \mathbb{P} : assigns a probability to each $\omega \in \Omega$

$$\mathbb{P} : \Omega \rightarrow \mathbb{R}_{\geq 0} \quad \text{s. t.} \quad \sum_{\omega \in \Omega} \mathbb{P}(\omega) = 1$$

Definition: An **event** \mathcal{E} is a subset of Ω

- Event $\mathcal{E} \subseteq \Omega$: set of basic events
- Probability of \mathcal{E}

$$\mathbb{P}(\mathcal{E}) := \sum_{\omega \in \mathcal{E}} \mathbb{P}(\omega)$$

Example: Probability Space, Events



Example: Probability Space, Events



Independent Events

Definition: Events $\mathcal{A} \subseteq \Omega$ and $\mathcal{B} \subseteq \Omega$ are **independent** iff

$$\mathbb{P}(\mathcal{A} \cap \mathcal{B}) = \mathbb{P}(\mathcal{A}) \cdot \mathbb{P}(\mathcal{B})$$

Example:

Random Variables

Definition: A **random variable** X is a real-valued function on the elementary events Ω

$$X : \Omega \rightarrow \mathbb{R}$$

- We usually write X instead of $X(\omega)$
- We also write

$$\mathbb{P}(X = x) = \mathbb{P}(\{\omega \in \Omega : X(\omega) = x\})$$

Examples:

- X^{top} : $X^{top}(1) = 1, X^{top}(2) = 2, \dots, X^{top}(6) = 6$
- X^{bot} : $X^{bot}(1) = 6, X^{bot}(2) = 5, \dots, X^{bot}(6) = 1$
- Note that for all $\omega \in \Omega$, $X^{top}(\omega) + X^{bot}(\omega) = 7$
- To denote this, we write $X^{top} + X^{bot} = 7$

Indicator Random Variables

A random variable which only takes values 0 and 1 is called a **Bernoulli random variable** or an **indicator random variable**.

Independent Random Variables



Definition: Two random variables X and Y are called **independent** if

$$\forall \mathbf{x}, \mathbf{y} \in \mathbb{R} : \mathbb{P}(\mathbf{X} = \mathbf{x} \wedge \mathbf{Y} = \mathbf{y}) = \mathbb{P}(\mathbf{X} = \mathbf{x}) \cdot \mathbb{P}(\mathbf{Y} = \mathbf{y})$$

Independent Random Variables

Definition: A collection of random variables X_1, X_2, \dots, X_n on a probability space Ω is called **mutually independent** if

$\forall k \geq 2, 1 \leq i_1 < \dots < i_k \leq n, \forall x_{i_1}, \dots, x_{i_k} \in \mathbb{R} :$

$$\mathbb{P}(X_{i_1} = x_{i_1} \wedge \dots \wedge X_{i_k} = x_{i_k}) = \mathbb{P}(X_{i_1} = x_{i_1}) \cdot \dots \cdot \mathbb{P}(X_{i_k} = x_{i_k})$$

Expectation

Definition: The **expectation** of a random variable X is defined as

$$\mathbb{E}[X] := \sum_{x \in X(\Omega)} x \cdot \mathbb{P}(X = x) = \sum_{\omega \in \Omega} X(\omega) \cdot \mathbb{P}(\omega)$$

Example:

- recall: X^{top} is outcome of rolling a die

Expectation: Examples



Linearity of Expectation:

For random variables X and Y and any $c \in \mathbb{R}$, we have

$$\begin{aligned}\mathbb{E}[cX] &= c \cdot \mathbb{E}[X] \\ \mathbb{E}[X + Y] &= \mathbb{E}[X] + \mathbb{E}[Y]\end{aligned}$$

- holds also if the random variables are not independent

Product of Random Variables:

For two **independent** random variables X and Y , we have

$$\mathbb{E}[X \cdot Y] = \mathbb{E}[X] \cdot \mathbb{E}[Y]$$

Linearity of Expectation: Example

Sequence of coin flips: $C_1, C_2, \dots \in \{H, T\}$

- Stop as soon as the first H turns up

Random variable X : number of T before first H

Indicator random variable X_i ($i \geq 1$):

- $X_i = 1$: i^{th} coin flip happens and its outcome is T
 $X_i = 0$: otherwise

Markov's Inequality

Lemma: Let X be a nonnegative random variable.
Then for all $c > 0$

$$\mathbb{P}(X \geq c \cdot \mathbb{E}[X]) \leq \frac{1}{c}$$

Conditional Probabilities

For events $\mathcal{A} \subseteq \Omega$ and $\mathcal{B} \subseteq \Omega$, the **conditional probability** of \mathcal{A} given \mathcal{B} is defined as

$$\mathbb{P}(\mathcal{A}|\mathcal{B}) := \frac{\mathbb{P}(\mathcal{A} \cap \mathcal{B})}{\mathbb{P}(\mathcal{B})}$$

Conditioning on event \mathcal{B} defines a **new probability space** $(\Omega \setminus \mathcal{B}, \mathbb{P}')$

$$\forall \omega \in \Omega \setminus \mathcal{B} : \mathbb{P}'(\omega) = \frac{\mathbb{P}(\omega)}{\mathbb{P}(\mathcal{B})}.$$

Two events are **independent** iff $\mathbb{P}(\mathcal{A}|\mathcal{B}) = \mathbb{P}(\mathcal{A})$

Law of Total Probability / Expectation

Lemma: Let X and Y be two random variable on the same probability space (Ω, \mathbb{P}) . We then have

$$\forall x \in \mathbb{R} : \mathbb{P}(X = x) = \sum_{y \in Y(\Omega)} \mathbb{P}(X = x \mid Y = y) \cdot \mathbb{P}(Y = y).$$

$$\mathbb{E}[X] = \sum_{y \in Y(\Omega)} \mathbb{E}[X \mid Y = y] \cdot \mathbb{P}(Y = y)$$

Important Discrete Prob. Distributions

Bernoulli Random Variable $X : \Omega \rightarrow \{0, 1\}$

$$\mathbb{P}(X = 1) = p, \mathbb{P}(X = 0) = 1 - p, \quad \mathbb{E}[X] = p$$

Binomial Random Variable $X \sim \text{Bin}(n, p)$

$$\forall k \in \{0, \dots, n\} : \mathbb{P}(X = k) = \binom{n}{k} p^k (1 - p)^{n-k}, \quad \mathbb{E}[X] = np$$

- measures number of ones in n independent biased coin flip

Geometric Random Variables $X \sim \text{Geom}(p)$

$$\forall k \geq 1 : \mathbb{P}(X = k) = p(1 - p)^{k-1}, \quad \mathbb{E}[X] = \frac{1}{p}$$

- measures number independent biased coin flips are necessary to get one “heads”

Happy Holidays!

