

Randomisierte Algorithmen

Anhang: Konzepte aus der Wahrscheinlichkeitstheorie

Thomas Worsch

Fakultät für Informatik
Karlsruher Institut für Technologie

Wintersemester 2017/2018

Überblick

Wahrscheinlichkeitsräume

Zufallsvariablen

σ -Algebren

σ -Algebra (Ω, \mathcal{E})

- ▶ Ω Menge der *Ereignisraum* mit *Elementarereignissen*
- ▶ $\mathcal{E} \subseteq 2^\Omega$ Menge von *Ereignissen* mit
 1. $\emptyset \in \mathcal{E}$
 2. $E \in \mathcal{E} \implies \Omega \setminus E \in \mathcal{E}$
 3. $(\forall i \in \mathbb{N} : E_i \in \mathcal{E}) \implies \bigcup_{i \in \mathbb{N}} E_i \in \mathcal{E}$
- ▶ *diskrete* σ -Algebra: $\mathcal{E} = 2^\Omega$ und $|\Omega| \leq |\mathbb{N}|$

Wahrscheinlichkeitsmaße

(Ω, \mathcal{E}) eine σ -Algebra

- ▶ **Wahrscheinlichkeitsmaß:** $\mathbf{P} : \mathcal{E} \rightarrow \mathbb{R}_{\geq 0}$ mit
 1. $\mathbf{P}(\emptyset) = 0$ und
 2. **σ -Additivität:** für paarweise disjunkte $E_i \in \mathcal{E}$ gilt: $\mathbf{P}(\bigcup_i E_i) = \sum_i \mathbf{P}(E_i)$.
 3. $\mathbf{P}(\Omega) = 1$
- ▶ $(\Omega, \mathcal{E}, \mathbf{P})$ **Wahrscheinlichkeitsraum**

Einschluss-Ausschluss-Prinzip

Lemma

Sind E_1, \dots, E_k beliebige Ereignisse, dann gilt

$$\mathbf{P}(E_1 \cup E_2) = \mathbf{P}(E_1) + \mathbf{P}(E_2) - \mathbf{P}(E_1 \cap E_2)$$

und allgemeiner

$$\begin{aligned} \mathbf{P}\left(\bigcup_i E_i\right) &= \sum_i \mathbf{P}(E_i) - \sum_{i < j} \mathbf{P}(E_i \cap E_j) + \sum_{i < j < k} \mathbf{P}(E_i \cap E_j \cap E_k) - \dots \\ &\quad + (-1)^{l+1} \sum_{i_1 < i_2 < \dots < i_l} \mathbf{P}\left(\bigcap_{r=1}^l E_{i_r}\right) + \dots \end{aligned}$$

Bedingte Wahrscheinlichkeit

- ▶ *bedingte Wahrscheinlichkeit* von E_1 unter der Bedingung E_2 mit $\mathbf{P}(E_2) > 0$ ist

$$\mathbf{P}(E_1 \mid E_2) := \frac{\mathbf{P}(E_1 \cap E_2)}{\mathbf{P}(E_2)}$$

- ▶ falls $\mathbf{P}(E_2) = 0$, so sei $\mathbf{P}(E_1 \mid E_2) := 0$

Unabhängigkeit von Ereignissen

- ▶ Ereignisse $E_1, E_2 \in \mathcal{E}$ *unabhängig*, falls $\mathbf{P}(E_1 \cap E_2) = \mathbf{P}(E_1) \cdot \mathbf{P}(E_2)$.
- ▶ allgemeiner $\{E_i \mid i \in I\}$ *unabhängig*, falls für alle $S \subseteq I$ gilt:

$$\mathbf{P}\left(\bigcap_{i \in S} E_i\right) = \prod_{i \in S} \mathbf{P}(E_i)$$

- ▶ $\{E_i \mid i \in I\}$ *k-unabhängig*, wenn Gleichung für alle S mit $|S| \geq k$ gilt.

Überblick

Wahrscheinlichkeitsräume

Zufallsvariablen

Die Borel-Mengen (von \mathbb{R})

- ▶ *Borel σ -Algebra* $\mathcal{B} = \mathcal{B}(\mathbb{R})$ ist die kleinste σ -Algebra, die für jedes $x \in \mathbb{R}$ das Intervall $(-\infty, x] = \{x' \in \mathbb{R} \mid x' \leq x\}$ enthält.
- ▶ Elemente von \mathcal{B} heißen *Borel-Menge*
- ▶ \mathcal{B} enthält dann auch für alle $x, y \in \mathbb{R}$ die Intervalle
 - ▶ $(-\infty, x)$
 - ▶ $[x, \infty)$
 - ▶ (x, ∞)
 - ▶ (x, y)
 - ▶ $(x, y]$
 - ▶ $[x, y)$
 - ▶ $[x, y]$
 - ▶ $\{x\}$
 - ▶ und viele viele andere Mengen ...

Zufallsvariablen

$(\Omega, \mathcal{E}, \mathbf{P})$ Wahrscheinlichkeitsraum

- ▶ *Zufallsvariable* $X : \Omega \rightarrow \mathbb{R}$, für die für jede Borelmenge $B \in \mathcal{B}$

$$X^{-1}(B) = \{\omega \mid X(\omega) \in B\} \in \mathcal{E}$$

- ▶ Schreibweisen
 - ▶ $\mathbf{P}(X \leq x)$ statt $\mathbf{P}(\{\omega \mid X(\omega) \leq x\})$
 - ▶ $\mathbf{P}(X = x)$ statt $\mathbf{P}(\{\omega \mid X(\omega) = x\})$
 - ▶ etc.

Zufallsvariablen

- ▶ Zufallsvariable X ist *diskret*, falls $\{X(\omega) \mid \omega \in \Omega\}$ endlich oder abzählbar unendlich
- ▶ *Indikatorvariable* für ein Ereignis E ist die diskrete ZV X mit

$$X(\omega) = \begin{cases} 1 & \text{falls } \omega \in E \\ 0 & \text{falls } \omega \notin E \end{cases}$$

Standardbeispiel: Würfeln

- ▶ $\Omega = \{\boxed{1}, \boxed{2}, \boxed{3}, \boxed{4}, \boxed{5}, \boxed{6}\}$
- ▶ $E = 2^\Omega$ diskret
 - ▶ z. B. $g = \{\boxed{2}, \boxed{4}, \boxed{6}\}$ «gerade Zahl gewürfelt»
- ▶ «fairer» Würfel:
 $\forall \omega \in \Omega : \mathbf{P}(\omega) = 1/6$
 - ▶ $\mathbf{P}(g) = 1/2$
 - ▶ allgemein: $\mathbf{P}(e) = |e|/6$
- ▶ $X(\omega) = \begin{cases} 0, & \text{falls } \omega \text{ Produkt zweier Primfaktoren} \\ 1, & \text{sonst} \end{cases}$
 - ▶ z. B. $\mathbf{P}(X = 1) = 2/3$

Erinnerung an W-Theorie (2)

- ▶ Zufallsvariable $X : \Omega \rightarrow \mathbb{R}$, nur abzählbar viele $X(\omega) \neq 0$
- ▶ *Erwartungswert* von X :
$$\mathbf{E}[X] = \sum_{x \in \mathbb{R}} x \cdot \mathbf{P}(X = x)$$

(falls das absolut konvergiert)
- ▶ immer: $\mathbf{E}[X + Y] = \mathbf{E}[X] + \mathbf{E}[Y]$
- ▶ *unabhängige* ZV: für alle $x, y \in \mathbb{R}$: $\mathbf{P}(X = x \wedge Y = y) = \mathbf{P}(X = x) \cdot \mathbf{P}(Y = y)$
- ▶ falls X, Y unabhängig: $\mathbf{E}[X \cdot Y] = \mathbf{E}[X] \cdot \mathbf{E}[Y]$
- ▶ *Indikator-ZV*: 0 und 1 einzig mögliche Funktionswerte

Standardbeispiel: Würfeln

- ▶ $\Omega = \{\boxed{1}, \boxed{2}, \boxed{3}, \boxed{4}, \boxed{5}, \boxed{6}\}$
- ▶ $E = 2^\Omega$
- ▶ Indikator-ZV $X(\omega) = 1$, falls ω prim
- ▶ Indikator-ZV $Y(\omega) = 1$, falls ω gerade
- ▶ X und Y *nicht* unabhängig:

$$\mathbf{P}(X = 1) = 1/2$$

$$\mathbf{P}(Y = 1) = 1/2$$

$$\mathbf{P}(X = 1) \cdot \mathbf{P}(Y = 1) = 1/4$$

$$\mathbf{P}(X = 1 \wedge Y = 1) = 1/6$$