Partialbruchzerlegung

Beispiel: Partialbruchzerlegung

- Seien $g(x) = x$ und $f(x) = 1 - x - x^2$.
- $f^R(x) = x^2 - x - 1$ besitzt die beiden Nullstellen $\frac{1}{2} \pm \sqrt{\frac{1}{4} + 1}$, d.h.

$$\phi = \tfrac{1+\sqrt{5}}{2} \text{ und } \bar{\phi} = \tfrac{1-\sqrt{5}}{2}.$$

- Damit gilt $f(x) = (1 - \phi x)(1 - \bar{\phi} x)$.
- Wir erhalten den Partialbruchansatz $\frac{x}{(1-\phi x)(1-\bar{\phi} x)} = \frac{a}{1-\phi x} + \frac{b}{1-\bar{\phi} x}$.
- Multiplikation mit f liefert $x = (1 - \bar{\phi} x)a + (1 - \phi x)b$.
- Koeffizientenvergleich ergibt $\left| \begin{array}{rcl} -\bar{\phi} a - \phi b & = & 1 \\ a + b & = & 0 \end{array} \right|$.
- Dies impliziert $a = \frac{1}{\phi - \bar{\phi}} = \frac{1}{\sqrt{5}} = -b$.

Fibonacci-Rekursion

Satz Formel für Fibonacci-Zahlen

Sei $F_0 = 0, F_1 = 1$ und $F_n = F_{n-1} + F_{n-2}$ für $n \geq 2$. Dann gilt

$$F_n = \frac{1}{\sqrt{5}} \left(\phi^n - \bar{\phi}^n \right).$$

Beweis:

- Einsetzen von $F(x) = \sum_{n \geq 0} F_n x^n$ in die Rekursionsgleichung
  $F(x) = F_0 + F_1 x + \sum_{n \geq 2} F_n x^n = x + \sum_{n \geq 2} (F_{n-1} + F_{n-2}) x^n.$
- Wir stellen die Summen wieder durch $F(x)$ dar.
  $$\begin{aligned} F(x) &= x + x \sum_{n \geq 1} F_n x^n + x^2 \sum_{n \geq 0} F_n x^n \\ &= x + x(F(x) - F_0) + x^2 F(x) = x + F(x)(x + x^2). \end{aligned}$$
- Auflösen nach $F(x)$ ergibt $F(x) = \frac{x}{1 - x - x^2}$.
- Partialbruchzerlegung $F(x) = \frac{1}{1 - \phi x} + \frac{b}{1 - \bar{\phi} x}$ mit $a = (-b) = \frac{1}{\sqrt{5}}$.
- Partialbruchlemma liefert $F(x) = a \sum_{n \geq 0} (\phi x)^n + b \sum_{n \geq 0} (\bar{\phi} x)^n$.
- Durch Koeffizientenvergleich erhalten wir $F_n = \frac{1}{\sqrt{5}} \left(\phi^n - \bar{\phi}^n \right)$.

Wahrscheinlichkeitsraum

Definition Wahrscheinlichkeitsraum

Seien $\omega_1, \omega_2, \ldots$ Elementareignisse mit Wahrscheinlichkeiten $0 \leq \Pr[\omega_1], \Pr[\omega_2], \ldots \leq 1$. Wir bezeichnen $\Omega = \{\omega_1, \omega_2, \ldots\}$ als *Ergebnismenge*. Ω definiert einen diskreten *Wahrscheinlichkeitsraum* falls $\sum_{\omega \in \Omega} \Pr[\omega] = 1$.

Eine Teilmenge $E \subseteq \Omega$ heißt Ereignis mit $\Pr[E] := \sum_{\omega \in E} \Pr[\omega]$.

Beispiel: Fairer Würfel

- $\omega_i = i, i \in [6]$ bezeichnen die Elementarereignis, i zu würfeln.
- Der Ergebnisraum ist $\Omega = \{1, 2, 3, 4, 5, 6\}$.
- Bei einem fairen Würfel gilt $\Pr[i] = \frac{1}{6}$ für alle $i \in [6]$.
- D.h. $\sum_{i \in \Omega} \Pr[i] = 1$. Damit definiert Ω einen Wsraum.
- Sei $E = \{3, 6\}$, d.h. es wird eine durch 3 teilbare Zahl gewürfelt.
- Dann gilt $\Pr[E] = \Pr[3] + \Pr[6] = \frac{1}{3}$.

Beispiel Wsraum

Beispiel: Wsraum

- Wir modellieren 2 Kartenspieler mit je 10 aus 52 Karten.
- Karten $K = \{\text{Karo, Herz, Pik, Kreuz}\} \times \{2, \ldots, 10, B, D, K, A\}$.
- Ergebnismenge $\Omega = \{(X, Y) \subseteq K^2 \mid X \cap Y = \emptyset, |X| = |Y| = 10\}$.
- Elementareignisse $(X, Y) \in \Omega$ entsprechen Kartenverteilungen.
- Es gilt $\Pr(\omega) = \frac{1}{|\Omega|}$ für alle $\omega \in \Omega$. (Übung: Bestimmen Sie $|\Omega|$.)
- Das Ereignis, das Spieler X vier Asse besitzt, ist

  $$E = \{(X, Y) \in \Omega \mid \{(\text{Karo,A}),(\text{Herz,A}), (\text{Pik,A}), (\text{Kreuz,A})\} \subset X\}.$$
- Für bessere Lesbarkeit schreiben wir oft $E =$“Spieler X besitzt 4 Asse.” und analog $\Pr[E] = \Pr[\text{“Spieler X besitzt vier Asse”}]$.

Unendlicher Wsraum

Problem Laufzeit von probabilistischen Las-Vegas Algorithmen

Gegeben: Algorithmus, der in jeder Iteration eine Ausgabe mit Ws von $p \in (0,1)$ liefert.

Gesucht: Ws, dass genau i Iterationen durchgeführt werden.

Modellierung als unendlicher Wsraum

- Sei w_i, $i \in \mathbb{N}$ das Elementarereignis, das genau i Iterationen des Algorithmus durchgeführt werden.
- Die Ergebnismenge $\Omega = \{\omega_1, \omega_2, \ldots\}$ ist unendlich.
- Für ω_i benötigt man zunächst $i-1$ Misserfolge, dann Erfolg.
- D.h. $\Pr[\omega_i] = (1-p)^{i-1}p$. Damit definiert Ω einen Wsraum, denn $\sum_{\omega\in\Omega} \Pr[\omega] = \sum_{i\geq 1}(1-p)^{i-1}p = p\sum_{i\geq 1}(1-p)^i = p\cdot\frac{1}{1-(1-p)} = 1$.

Additionslemma und Gegenereignis

Lemma Additionslemma

Sei Ω ein Wsraum. Für paarweise disjunkte $A_1, \ldots, A_n \subseteq \Omega$ gilt $\Pr[\bigcup_{i=1}^{n} A_i] = \sum_{i=1}^{n} \Pr[A_i]$.

Beweis:

- $\Pr[\bigcup_{i=1}^{n} A_i] = \sum_{a \in A_1} \Pr[a] + \ldots + \sum_{a \in A_n} \Pr[a] = \sum_{i=1}^{n} \Pr[A_i]$.

Lemma Gegenereignis

Sei Ω ein Wsraum. Sei $A \subseteq \Omega$ mit Gegenereignis $\bar{A} = \Omega \setminus A$. Dann gilt $\Pr[\bar{A}] = 1 - \Pr[A]$.

Beweis:

- $\Pr[A] + \Pr[\bar{A}] = \Pr[A \cup \bar{A}] = \Pr[\Omega] = 1$.
- Daraus folgt $\Pr[\bar{A}] = 1 - \Pr[A]$.

Teilereignisse

Lemma Teilereignis

Sei Ω ein Wsraum und $A, B \subseteq \Omega$ mit $A \subseteq B$. Dann gilt $\Pr[A] \leq \Pr[B]$.

Beweis:

- $\Pr[B] = \Pr[A \cup (B \cap \bar{A})] = \Pr[A] + \Pr[B \cap \bar{A}] \geq \Pr[A]$.

Inklusion/Exklusion für nicht-disjunkte Ereignisse

Satz Additionsformel

Sei Ω ein Wsraum mit Ereignissen $A_1, \ldots, A_n$. Dann gilt

$$\Pr[\bigcup_{i=1}^{n} A_i] = \sum_{i=1}^{n} \Pr[A_i] - \sum_{1 \le i_1 < i_2 \le n} \Pr[A_{i_1} \cap A_{i_2}] + \ldots + (-1)^{n-1} \Pr[A_1 \cap \ldots A_n].$$

Beweis:

- Wir zeigen nur $n = 2$, für allg. n folgt der Beweis per Induktion.
- D.h. zu zeigen ist $\Pr[A_1 \cup A_2] = \Pr[A_1] + \Pr[A_2] - \Pr[A_1 \cap A_2]$.
- Sei $B = A_1 \setminus A_2$. Dann sind B und $A_1 \cap A_2$ disjunkt.
- Damit gilt $\Pr[A_1] = \Pr[B \cup (A_1 \cap A_2)] = \Pr[B] + \Pr[A_1 \cap A_2]$.
- Es folgt

$$\begin{aligned} \Pr[A_1 \cup A_2] &= \Pr[B \cup A_2] = \Pr[B] + \Pr[A_2] \\ &= \Pr[A_1] - \Pr[A_1 \cap A_2] + \Pr[A_2]. \end{aligned}$$

Boolesche Ungleichung

Satz Boolesche Ungleichung

Sei Ω ein Wsraum mit Ereignissen $A_1, \ldots, A_n$. Dann gilt

$$\Pr[\bigcup_{i=1}^{n} A_i] \leq \sum_{i=1}^{n} \Pr[A_i].$$

Beweis:

- Sei $B = \bigcup_{i=1}^{n} A_i$. Dann folgt

$$\Pr[B] = \sum_{\omega \in B} \Pr[\omega] \leq \sum_{i=1}^{n} \sum_{\omega \in A_i} \Pr[\omega] = \sum_{i=1}^{n} \Pr[A_i].$$

Prinzip von Laplace

Definition Prinzip von Laplace

Sei Ω eine Ergebnismenge. Beim *Prinzip von Laplace* setzen wir $\Pr[\omega] = \frac{1}{|\Omega|}$ für alle $\omega \in \Omega$.

Anmerkung:

- Das Prinzip von Laplace liefert eine Gleichverteilung.
- Für alle $E \subseteq \Omega$ gilt $\Pr(E) = \sum_{\omega \in E} \Pr(\omega) = \sum_{\omega \in E} \frac{1}{|E|} = \frac{|E|}{|\Omega|}$.
- D.h. wir erhalten die Faustformel “Günstige durch Mögliche”.

Bedingte Wahrscheinlichkeit

Definition Bedingte Wahrscheinlichkeit

Sei Ω ein Wsraum mit $A, B \subseteq \Omega$ und $\Pr[B] > 0$. Dann definieren wir die *bedingte Wahrscheinlichkeit* $\Pr[A|B] := \frac{\Pr[A \cap B]}{\Pr[B]}$.

Anmerkungen:

- $\Pr[A|B]$ bezeichnet die Wahrscheinlichkeit, dass Ereignis A eintrifft unter der Bedingung dass Ereignis B eintrifft.
- Es folgt $\Pr[A \cap B] = \Pr[A|B] \cdot \Pr[B] = \Pr[B|A] \cdot \Pr[A]$.
- Ferner gilt $\Pr[A|A] = 1$ und $\Pr[A|\bar{A}] = 0$.
- Es gilt $\Pr[\omega|B] = \begin{cases} 0 & \text{für } \omega \notin B \\ \frac{\Pr[\omega]}{\Pr[B]} & \text{für } \omega \in B \end{cases}$.
- D.h. für $\omega \in B$ wird der Wsraum mit dem Faktor $\frac{1}{\Pr[B]}$ skaliert.
- Dies liefert einen Wsraum, denn
$$\sum_{\omega \in \Omega} \Pr[\omega|B] = \sum_{\omega \in \Omega} \frac{\Pr[\omega \cap B]}{\Pr[B]} = \frac{1}{\Pr[B]} \sum_{\omega \in B} \Pr[\omega] = \frac{\Pr[B]}{\Pr[B]} = 1.$$

Beispiel bedingte Wahrscheinlichkeiten

Beispiel:

- Wir betrachten einen Laplace-Würfel mit Wsraum $\Omega = [6]$.
- Sei $A =$"Augenzahl ist durch 3 teilbar".
- Sei $B =$"Augenzahl ist größer als 2".
- $\Pr[A \cap B] = \frac{|\{3,6\}|}{|\Omega|} = \frac{1}{3}$ und $\Pr[B] = \frac{|\{3,4,5,6\}|}{|\Omega|} = \frac{2}{3}$.
- Damit folgt $\Pr[A|B] = \frac{\Pr[A \cap B]}{\Pr[B]} = \frac{1}{3} \cdot \frac{3}{2} = \frac{1}{2}$.
- Der Skalierungsfaktor $\frac{1}{\Pr[B]}$ ist $\frac{3}{2}$.
- Alternativ können wir $\Pr[A|B]$ wie folgt bestimmen.
- Falls B eintritt, verändert dies den Wsraum zu $\Omega' = \{3, 4, 5, 6\}$.
- Damit gilt $\Pr[A|B] = \frac{|\{3,6\}|}{|\Omega'|} = \frac{1}{2}$.

- Wir betrachten ein weiteres Beispiel aus der Kryptographie.
- Perfekte Sicherheit wird in der Kryptographie definiert als

  $$\Pr[\text{Klartext ist } p] = \Pr[\text{Klartext ist } p \mid \text{Chiffretext ist } c].$$
- D.h. c liefert keine Information über das zugrundeliegende p.