Wiederholung

Allgemeine Strategie für lineare Rekursionen

- Erzeugendenfunktion
- Ausnutzen Rekursionsgleichung
- Darstellung a_n als A(x)
- Geschlossene Form A(x)= g(x)/f(x)
- Formulierung von g(x)/f(x) als formale Potenzreihe
  - Partialbruchzerlegung von g(x)/f(x)
  - Formale Potenzreihe für $1/(1-ax)^k$
- Koeffizientenvergleich

Beispiele

- Fibonacci-Zahlen: $$F_n = \frac{1}{\sqrt{5}}(\phi^n - \phi'^n)$$
- Catalanzahlen: $$C_n = \frac{1}{n+1}\binom{2n}{n}$$

Wahrscheinlichkeitsraum

Def: Diskreter Wahrscheinlichkeitsraum

- Ergebnismenge $\Omega = \{\omega_1, \omega_2, \ldots\}$
  - ω_i sind Elementarereignisse
  - ω_i besitzten $Pr[\omega_i]$ mit $0 \leq Pr[\omega_i] \leq 1$
- Es gilt: $\sum_{\omega \in \Omega} Pr[\omega]=1$.

- Menge $E \subseteq \Omega$ heißt Ereignis.
- $Pr[E]:= \sum_{\omega \in E} Pr[\omega]$

Bsp.: Fairer Würfel

- $\Omega = \{1,2,3,4,5,6\}$
  - ω = i ist das Elementarereignis, dass i gewürfelt wird.
  - $Pr[\omega]=1/6$ für alle ω in Ω (Gleichverteilung, sogenanntes Laplace-Experiment)
- Offenbar: $\sum^{6}_{i=1} Pr[i] = 6*1/6 = 1$
- Sei E das Ereignis, dass eine durch 3 teilbare Zahl gewürfelt wird.
  D.h. $E=\{3,6\}$ und $Pr[E] = Pr[3] + Pr[6] = 1/3$

Bsp. Wahrscheinlichkeitsraum

Modellierung von Kartenspiel:

- Zwei Spieler erhalten je 10 aus 52 Karten.

- Definieren K={Karo, Herz, Pik, Kreuz} $\times$ {2,3,…,10,B,D,K,A}
- $\Omega = \{(X,Y) \subseteq K^2 \mid X \cap Y = \emptyset, |X|=|Y|=5\}$
  - Elementarereignisse $(X,Y) \in \Omega$ entsprechen Kartenverteilung
  - $Pr(\omega) = 1/|\Omega|$ für alle $\omega \in \Omega$ (Übungsaufgabe: Bestimme $|\Omega|$.)

- Ereignis, dass Spieler X vier Asse hat.
  - $E:=\{(X,Y) \in \Omega \mid \{(Karo,A), (Herz,A), (Pik,A), (Kreuz,A)\} \subseteq X\}$.
  - Oft vereinfachend:
    - E:=„Spieler X hat vier Asse.“
    - Pr[E] = Pr[„Spieler X hat vier Asse.“]

Unendlicher Wahrscheinlichkeitsraum

- Szenario: Eine Iteration eines Algorithmus liefert eine Ausgabe mit Wahrscheinlichkeit p, $0<p<1$.
- Frage: Wieviele Iterationen werden benötigt?

Modellierung Wahrscheinlichkeitsraum:

- $\Omega=\{\omega_1,\omega_2, \ldots\}$
- ω_i ist das Elementarereignis, das i Iterationen benötigt werden.
  - ω_i: Zunächst i-1 Misserfolge, dann Erfolg.

    $\Rightarrow \Pr[w_i] = (1-p)^{i-1}p$
- Definiert Wahrscheinlichkeitsraum

  $\sum_{\omega \in \Omega} \Pr[w] = \sum^{\infty}_{i=1} (1-p)^{i-1}p = p \sum^{\infty}_{i=0} (1-p)^{i} = p*1/(1-(1-p)) = 1.$

Nützliche Eigenschaften

1. $\Pr[\emptyset]=0$, $\Pr[\Omega]=1$

2. Sei $A \subseteq E$ und $\bar{A} = \Omega \setminus A$.
   - $\Pr[A] + \Pr[\bar{A}] = \Pr[A \cup \bar{A}] = \Pr[\Omega] = 1$
   - $\Rightarrow \Pr[\bar{A}] = 1 - \Pr[A]$

3. Additionssatz: $A_1, \ldots, A_n$ paarweise disjunkt, d.h. $A_i \cap A_j = \emptyset$:
   - $\Pr[\cup^n_{i=1} A_i] = \sum^n_{i=1} \Pr[A_i]$

4. Seien $A,B \subseteq \Omega$ mit $A \subseteq B$. Dann gilt $\Pr[A] \leq \Pr[B]$:
   - $\Pr[B] = \Pr[A \cup (B \cap \bar{A})] = \Pr[A] + \Pr[B \cap \bar{A}] \geq \Pr[A]$

5. Sei $A \subseteq \Omega$. Dann gilt $0 \leq \Pr(A) \leq 1$.
   - $0 \leq \Pr[\emptyset] \leq \Pr[A] \leq \Pr[\Omega] \leq 1$.

Inklusion/Exklusion

Additionsformel für nicht-disjunkte Ereignisse.

Satz: Seien $A_1, \ldots, A_n \subseteq \Omega$. Dann gilt:

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

Beweisen nur n=2: $\Pr[A_1 \cup A_2] = \Pr[A_1] + \Pr[A_2] - \Pr[A_1 \cap A_2]$

- Sei $B = A_1 \setminus A_2$.
  - B, $A_1 \cap A_2$ disjunkt

  $\Rightarrow \Pr[A_1] = \Pr[B \cup (A_1 \cap A_2)] = \Pr[B] + \Pr[A_1 \cap A_2]$

  $\Rightarrow \Pr[A_1 \cup A_2] = \Pr[B \cup A_2] = \Pr[B] + \Pr[A_2]$

  $= \Pr[A_1] - \Pr[A_1 \cap A_2] + \Pr[A_2]$

Allgemeines n: Per Induktion.

Boolsche Ungleichung

Korollar: Seien $A_1, \ldots, A_n \subseteq \Omega$. Dann gilt:

$Pr[\cup^n_{i=1} A_i] \leq \sum^n_{i=1} Pr[A_i]$.

Sei $B = \cup_{i=1}^{n} A_i$. Es gilt

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

Prinzip von Laplace: Setze $Pr[\omega]=1/|\Omega|$ für alle $\omega \in \Omega$.

$$\Rightarrow Pr(E) = \sum_{w \in E} Pr(w) = \sum_{w \in E} \frac{1}{|\Omega|} = \frac{|E|}{|\Omega|}.$$

"Günstige Ereignisse durch alle Ereignisse"

Zusätzliche Bedingungen

Würfelspiel (Laplace)

- E=„Augenzahl ist durch 3 teilbar“
  $\Rightarrow$ Pr(E)=|{3,6}|/|Ω| = 1/3

- Zusätzliche Information: F=„Augenzahl größer als 2“.
  - Wissen bereits, dass Ereignis F eingetreten ist.
  - Verändert Ω in Ω‘={3,4,5,6}
    $\Rightarrow$ Pr(E‘) = 2/4 = ½.

- Notation Pr(E‘) = Pr(E | F)
  - Sprechweise „E gegeben F“ oder „E unter der Bedingung F“

Beispiel aus Kryptographie: Klartext wird zu Chiffretext verschlüsselt

- Perfekte Sicherheit bedeutet:
  Pr[Klartext ist p] = Pr[Klartext ist p | Chiffretext ist c],
  d.h. der Chiffretext liefert keine Information über zugrundeliegenden Klartext.

Bedingte Wahrscheinlichkeiten

Def: Seien A,B Ereignisse mit Pr[B]>0. Dann gilt

$$\Pr[A|B] := \frac{\Pr[A \cap B]}{\Pr[B]}$$

Korollar: Pr[A ∩ B] = Pr[A|B] * Pr[B] = Pr[B|A] * Pr[A]

Eigenschaften:

- Pr[A|A] = Pr[A]/Pr[A] = 1 und Pr[A| $\bar{A}$] = Pr[∅]/Pr[A] = 0.
- Pr[A|Ω]=Pr[A]/Pr[Ω]=Pr[A]
- Neuer Wahrscheinlichkeitsraum für Ω:
  - Für $\omega \notin$ B: Pr[ω|B]=0.
  - Für $\omega \in$ B : Pr[ω|B]=Pr[ω]/Pr[B]. (d.h. Skalierung mit 1/Pr[B])

$$\sum_{\omega \in \Omega} \Pr[\omega|B] = \sum_{\omega \in \Omega} \frac{\Pr[\omega \cap B]}{\Pr[B]} = \sum_{\omega \in B} \frac{\Pr[\omega]}{\Pr[B]} = \frac{\Pr[B]}{\Pr[B]} = 1.$$

Zurück zum Würfelbeispiel

- E=„Augenzahl ist durch 3 teilbar“
- F=„Augenzahl größer als 2“

Pr[E ∩ F] = |{3,6}|/|Ω|=1/3
Pr[F] = |{3,4,5,6}|/|Ω| = 2/3 (Skalierungsfaktor)

$$\Pr[E|F] := \frac{\Pr[E \cap F]}{\Pr[F]} = \frac{\frac{1}{3}}{\frac{2}{3}} = \frac{1}{2}$$

Zweikinderproblem

- Laplace-Annahme: Geburt von Junge oder Mädchen mit Ws 1/2
- Familie besitzt zwei Kinder.
- Frage: Mit welcher Ws tritt folgendes Ereignis A ein?
  - A=„Beide Kinder sind Mädchen.“
- Zusätzliche Information: Es gilt folgendes Ereignis
  - B=„Eines der Kinder ist ein Mädchen.“

- Müssen Pr[A|B] bestimmen.
- Wahrscheinlichkeitsraum Ω={mm, jm, mj, jj} (sortiert nach Alter)
  - Jedes der Elementarereignisse hat Ws ¼.
- $Pr[A \cap B] = Pr[A] = |\{mm\}|/|\Omega| = ¼$
- $Pr[B] = |\{mm, jm, mj\}|/|\Omega| = ¾$
  $\Rightarrow Pr[A|B] = 1/4 * 4/3 = 1/3$
- Für das Ereignis B‘=„Das ältere Kind ist ein Mädchen“ gilt:
  Pr[B‘] = ½ und damit Pr[A|B‘] = ½

- ABER: Anderer Wahrscheinlichkeitsraum Ω={mm, jm, jj} (unsortiert) liefert:
  Pr[B] = ½ und damit Pr[A|B] = ½.

Multiplikationssatz

Satz: Seien A_1, …, A_n Ereignisse mit $Pr[A_1 \cap \ldots \cap A_n] > 0$.
Dann gilt:
$Pr[A_1 \cap \ldots \cap A_n] = Pr[A_1] * Pr[A_2|A_1] * Pr[A_3|A_1 \cap A_2] * \ldots * Pr[A_n|A_1 \cap \ldots \cap A_{n-1}]$.

- Es gilt $0 < Pr[A_1 \cap \ldots \cap A_n] \leq Pr[A_1 \cap \ldots \cap A_{n-1}] \leq \ldots \leq Pr[A_1]$.
- n-malige Anwendung der Def. für bedingte Wahrscheinlichkeiten:

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

- Kürzen liefert $Pr[A_1 \cap \ldots \cap A_n]$.

Geburtstagsproblem

- Gegeben: m Personen
- Gesucht: Ws p, dass 2 Personen am selben Tag Geburtstag haben

- Bälle in Urnen: Werfe nacheinander m Bälle in n=365 Urnen.
- Bestimmen 1-p:
  Keine zwei Personen haben am selben Tag Geburtstag.
  - Gesucht: Ws für A=„Alle Bälle liegen allein in einer Urne.“
  - Sei A_i=„Ball i kommt in einen leeren Korb.“
  - $Pr[A] = Pr[A_1 \cap \ldots \cap A_m]$
    $= Pr[A_1] * Pr[A_2|A_1| * \ldots * Pr[A_m \mid A_1 \cap \ldots A_{m-1}]$.
  - $Pr[A_j \mid A_1 \cap \ldots \cap A_{j-1}] = (n-(j-1))/n = 1- (j-1)/n$
    - j-ter Ball landet in einem der noch freien n-(j-1) Urnen

Abschätzen von p

- Erhalten 1-p = Pr[A] = $\prod^{m}_{j=1}$ Pr[A_j | $A_1 \cap \ldots A_{j-1}$]
- Nutzen 1-x $\leq$ e^{-x}:

$$\Pr[A] = \prod_{j=1}^{m} \left(1 - \frac{j-1}{n}\right) \leq \prod_{j=2}^{m} e^{-\frac{j-1}{n}} = e^{-\frac{1}{n}\sum_{j=1}^{m-1} j} = e^{-\frac{m(m-1)}{2n}}$$

$$\Rightarrow p \geq 1 - e^{-\frac{m(m-1)}{2n}}.$$

- D.h. wir erhalten eine konstante Ws. p für $m = \Theta(\sqrt{n})$ (sogenanntes Geburtstagsparadoxon)

Anwendung bei kryptographischen Hashfunktionen $H:\{0,1\}^* \rightarrow \{0,1\}^n$
Falls die Bilder von H zufällig in $\{0,1\}^n$ verteilt sind:

- Werten H für verschiedene Urbilder $x_1, \ldots, x_m$ aus.
- Benötigen $m = \Theta(\sqrt{n})$ für Kollision $x_i \neq x_j$ mit $H(x_i) = H(x_j)$.