Diskrete Strukturen

WiSe 2012/13 in Trier

Henning Fernau
Universität Trier
fernau@uni-trier.de

11. Januar 2013

Diskrete Strukturen Gesamtübersicht

- Organisatorisches und Einführung
- Mengenlehre
- Relationen und Funktionen
- Kombinatorik: Die Kunst des Zählens
- Grundbegriffe (algebraischer) Strukturen
- Graphen

Diskrete Stochastik: Anwendungen für Kombinatorik

. . . ist ein vornehmes Wort für die bekannte (?) Wahrscheinlichkeitsrechnung.

Im Gegensatz zur kontinuierlichen Stochastik legen wir fest:
Def.: Eine höchstens abzählbare Menge heißt auch *Ereignisraum*.
Die Elemente eines Ereignisraums heißen *elementare Ereignisse*.

Deutung: Ein *Zufallsexperiment* liefert ein Ergebnis, das nicht genau vorherzusagen ist. Jedes mögliche Ergebnis nennt man auch elementares Ereignis.

Diskrete Stochastik—Beispiele

Beispiel: Ein *Münzwurf* hat zwei elementare Ereignisse: “Kopf” (liegt oben) oder “Zahl” (liegt oben).

Beispiel: Der *Würfelwurf* hat sechs elementare Ereignisse.

Beispiel: Unter Vernachlässigung der Zusatzzahl sind elementare Ereignisse des Lottos “6 aus 49” alle 6-elementigen Teilmengen der natürlichen Zahlen zwischen 1 und 49.

Der Ereignisraum in den Beispielen (Münzwurf, Würfeln, Lotto) umfasst $2 = |\{\text{Kopf, Zahl}|$ bzw. $6 = |\{1, 2, 3, 4, 5, 6\}|$ bzw. $13983816 = \left(\begin{array}{c} 49 \\ 6 \end{array} \right)$ Elemente.

Ereignisse sind Teilmengen des Ereignisraums.

Beispiel: Der Ereignisraum des Würfelns mit zwei Würfeln umfasst $36 = |\{1, \ldots, 6\}^2|$ Elemente.
Das Ereignis, die Augensumme 7 zu würfeln, ist die Teilmenge:

$$\{(1,6), (2,5), (3,4), (4,3), (5,2), (6,1)\}.$$

Beispiel: Wie viele Elemente enthält das Ereignis, dass der Lotto-Tipp $\{2, 5, 6, 8, 12, 14\}$ genau fünf der gezogenen 6 Zahlen enthält ?

Wahrscheinlichkeitsdichte und -verteilung

Def.: Eine Funktion P, die jedem Elementarereignis $x \in S$ eine nichtnegative Zahl $P(x)$ zuordnet, heißt *Wahrscheinlichkeitsdichte* oder *Wahrscheinlichkeits-funktion*, falls $\sum_{x \in S} P(x) = 1$ gilt.

P lässt sich leicht auf Ereignisse verallgemeinern durch $P(A) = \sum_{x \in A} P(x)$ und wird dann auch als *Wahrscheinlichkeitsverteilung* angesprochen.

Eigenschaften

Es sei S ein Ereignisraum.

$1 \geq P(A) \geq 0$ für jedes Ereignis A.
$P(A \cup B) = P(A) + P(B)$ für disjunkte Ereignisse A, B.
$P(B \setminus A) = P(B) - P(A)$ und $P(A) \leq P(B)$ für $A \subseteq B$.
$P(\bar{A}) = P(S \setminus A) = 1 - P(A)$.
$P(\emptyset) = 0$.

Mit den bisherigen Festlegungen sind diese Eigenschaften elementar.
Im folgenden axiomatischen Zugang bedürfen sie aber “richtiger Beweise”.

Axiomatischer Zugang

Def.: Das Paar (S, P) heißt *diskreter Wahrscheinlichkeitsraum*, wenn gilt:

1. S ist eine höchstens abzählbare Menge (*Ereignisraum*).
2. $P : 2^S \to \mathbb{R}$ erfüllt:

(2a) $\forall A \subseteq S : P(A) \geq 0$ (*Nichtnegativität*)

(2b) $P(S) = 1$ (*Normiertheit*)

(2c) für jede Folge $(A_n)_{n\in\mathbb{N}}$ paarweise fremder Mengen aus S gilt:

$$P\Big(\bigcup_{n\in\mathbb{N}} A_n\Big) = \sum_{n\in\mathbb{N}} P(A_n) \qquad (\sigma\text{-}\textit{Additivität})$$

P heißt dann auch ein *(diskretes) Wahrscheinlichkeitsmaß*.

Beweise der Eigenschaften (ausgehend von der Axiomatik)

Betrachte $A_0 = S$ und $A_n = \emptyset$ für $n \geq 1$. $\rightsquigarrow$

$$1 = P(S) = P(\bigcup_{n\in\mathbb{N}} A_n) = \sum_{n\in\mathbb{N}} P(A_n) = P(S) + P(\emptyset) + P(\emptyset) + \cdots = 1 + P(\emptyset) + \cdots + P(\emptyset)$$

$\rightsquigarrow P(\emptyset) = 0$.

Es seien A und B disjunkt. Betrachte $A_0 = A$, $A_1 = B$ und $A_n = \emptyset$ für $n \geq 2$. $\rightsquigarrow$

$$P(A \cup B) = P(\bigcup_{n\in\mathbb{N}} A_n) = \sum_{n\in\mathbb{N}} P(A_n) = P(A) + P(B) + P(\emptyset) + \cdots = P(A) + P(B) + 0$$

Also gilt: $P(A \cup B) = P(A) + P(B)$.

$1 = P(S) = P(A \cup \bar{A}) = P(A) + P(\bar{A}) \rightsquigarrow$ (1) $P(\bar{A}) = 1 - P(A) \rightsquigarrow$ (2) $P(A) \leq 1$ (wegen $P(\bar{A}) \geq 0$)

Für $A \subseteq B$ gilt: $B = (B \setminus A) \cup A$ (disjunkte Vereinigung)
$\rightsquigarrow$ (1) $P(B \setminus A) = P(B) - P(A)$ und (2) $P(A) \leq P(B)$ (wegen $P(B \setminus A) \geq 0$)

Wegen der σ-Additivität des Wahrscheinlichkeitsmaßes ist es durch die Festlegung der Wahrscheinlichkeiten der Elementarereignisse (also durch die Wahrscheinlichkeitsdichte) schon vollständig beschrieben.

Zusammenhang mit der Kombinatorik

Einfachster Fall: Alle elementaren Ereignisse sind gleichwahrscheinlich und der Ereignisraum ist endlich.
Dann gilt: $\forall x \in S : P(x) = 1/|S|$. (*Gleichverteilung*)

Für ein Ereignis $A \subseteq S$ gilt somit:

$$P(A) = \sum_{x \in A} P(x) = \frac{|A|}{|S|}.$$

Es kommt daher essentiell darauf an, die Elemente von A zu zählen.

Das Geburtstagsproblem

Wie viele Gäste muss man zu einer Party einladen, damit mit Wahrscheinlichkeit $\geq \frac{1}{2}$ zwei Gäste am selben Tag Geburtstag haben ?

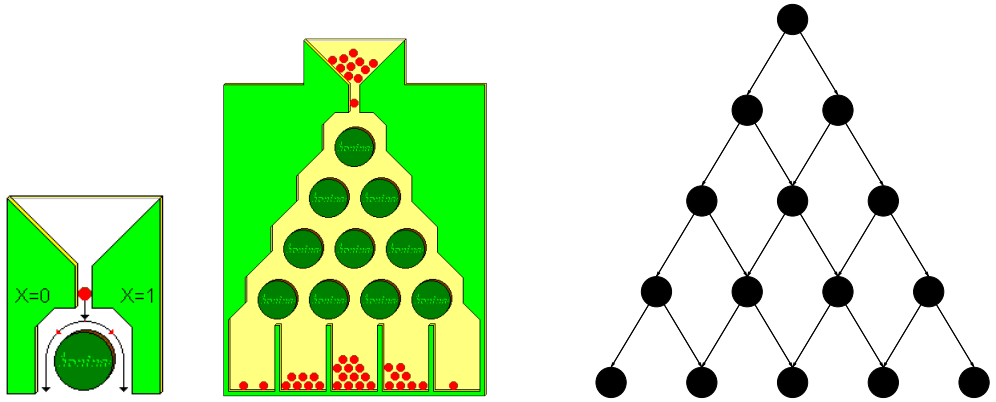
Vereinfachende Annahmen: Es gibt 365 Tage im Jahr und alle Tage seien für Geburten gleichwahrscheinlich; zudem sei unsere Gästeauswahl **nicht** z.B. auf Gäste konzentriert, die am 2.1. geboren wurden.

Der Ereignisraum S_k, der sich durch Einladen von k Gästen ergibt, lässt sich durch $\{1,\ldots,365\}^k$ beschreiben, d.h., $|S_k| = 365^k$ nach der Potenzregel.
Wir nummerieren die Gäste behelfsweise durch.
Der erste Gast kann an einem beliebigen Tag Geburtstag haben, ohne dass zwei Gäste am selben Tag Geburtstag haben. Der erste Gast "blockiert" aber einen Tag für den zweiten Gast, der nur noch an einem der anderen 364 Tage geboren sein darf, ohne dass zwei Gäste am selben Tag Geburtstag haben.
Schließlich "blockieren" die ersten $k-1$ Gäste $k-1$ Tage für den k-ten Gast, der nur noch an einem der nicht-blockierten $365-(k-1)$ Tage geboren sein darf, ohne dass zwei Gäste am selben Tag Geburtstag haben.

Für das fragliche Ereignis E_k gilt also: $|E_k| = 365\cdot 364\cdots(365-k+1)$, $\rightsquigarrow P(E_k) = \frac{365\cdot 364\cdots(365-k+1)}{365^k}$.
$\rightsquigarrow$ 23 Gäste genügen !
PS: Auf dem Mars mit 669 Tagen müsste man 31 Gäste einladen.

Wiederholte Münzwürfe

Ein Münzwurf lässt sich auch durch den Weg einer Kugel in folgendem Diagramm (einfachstes *Galton-Brett*) von oben nach unten veranschaulichen.



Sind wir nur an der Zahl j der Zahl-oben-Ereignisse bei einem wiederholten Münzwurfexperiment interessiert, so entspricht dies der Zahl der Kugeln im j-ten Fach des n-fach kaskadierten Galtonbretts. n über j von insgesamt 2^n Möglichkeiten (elementaren Ereignissen) beinhaltet dieses Ereignis.

Bernoulli-Experimente: Münzwürfe mit Wahrscheinlichkeit p für "Zahl"

$b(k; n, p)$: Wahrscheinlichkeit, bei n unabhängigen Wiederholungen eines Bernoulli-Versuches mit Wahrscheinlichkeit p für "Zahl" genau k mal "Zahl" zu werfen.

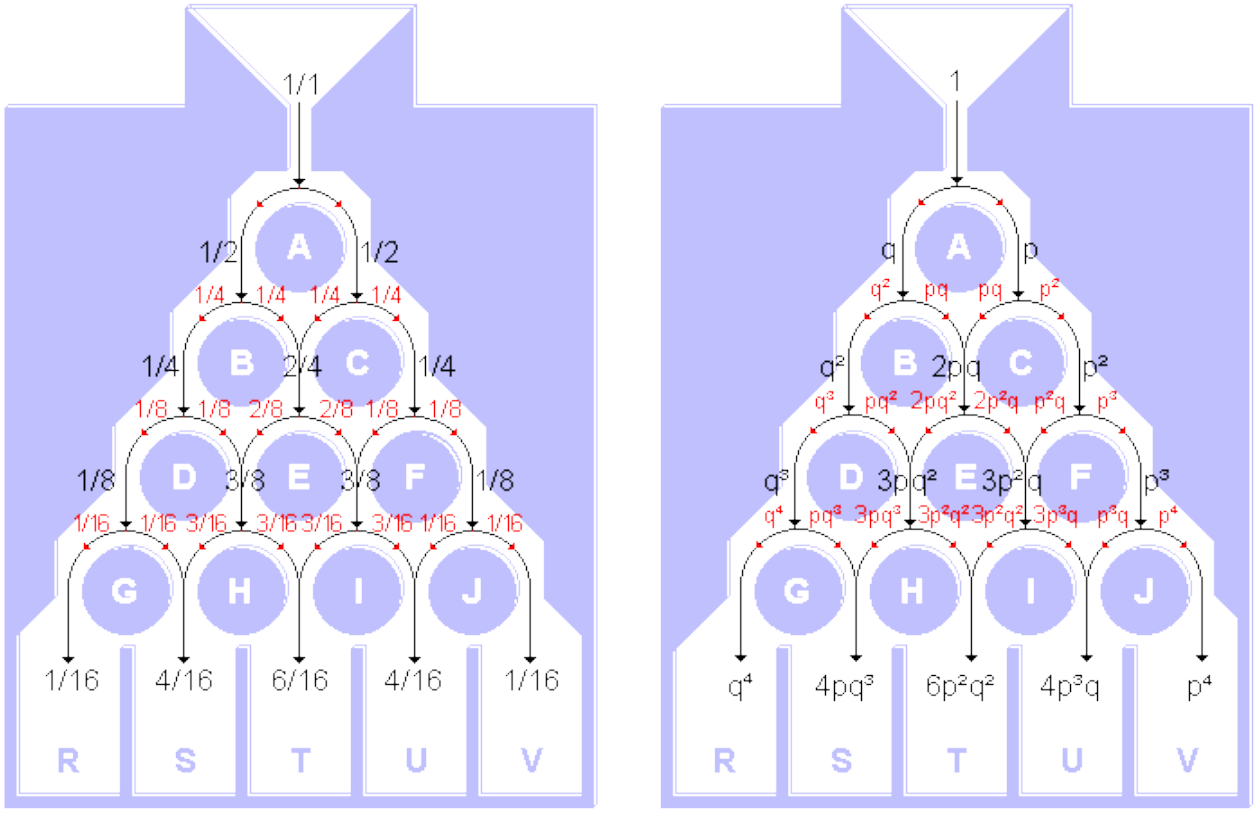
Satz: (*Binomialverteilung*) $b(k; n, p) = \left(\begin{array}{c} n \\ k \end{array} \right) \cdot p^k (1-p)^{n-k}$.

Beweis: durch Induktion über n:
IA: $n = 1$ ✓
IV: Die Behauptung gelte für $n = m$.
IB: Die Behauptung gilt für $n = m + 1$.
Es gibt zwei Möglichkeiten, mit $m + 1$ Versuchen genau k Zahlen zu werfen.
1. Im $m + 1$. Versuch wird "Kopf" geworfen, aber in den vorigen m Versuchen genau k-mal Zahl.
2. Im $m + 1$. Versuch wird "Zahl" geworfen und in den vorigen m Versuchen genau $(k - 1)$-mal Zahl.

$$\begin{aligned} b(k; m+1, p) &= b(k; m, p)(1-p) + b(k-1; m, p)p \\ &= \binom{m}{k} \cdot p^k (1-p)^{m-k}(1-p) + \binom{m}{k-1} \cdot p^{k-1}(1-p)^{m-k+1}p \\ &= \left(\binom{m}{k} + \binom{m}{k-1}\right) p^k (1-p)^{m-k+1} \\ &= \binom{m+1}{k} p^k (1-p)^{(m+1)-k} \end{aligned}$$

Die letzte Gleichung folgt mit dem bekanntesten Satz über das Pascalsche Dreieck.

Ergänzung: Den Zusammenhang mit dem binomischen Lehrsatz (mit $q = 1 - p$) veranschaulicht das Galton-Brett:



Bedingte Wahrscheinlichkeit

Es sei S ein Ereignisraum mit Wahrscheinlichkeitsfunktion $P : S \to \mathbb{R}$.

Def.: Die *bedingte Wahrscheinlichkeit* von Ereignis $A \subseteq S$ unter der Voraussetzung, dass Ereignis $P(B) \neq 0$ eintritt, ist definiert als:

$$P(A|B) = \frac{P(A \cap B)}{P(B)}.$$

Beobachte: $P(A|B) = P(A'|B)$ gdw. $P(A \cap B) = P(A' \cap B)$; dies ist insbesondere dann der Fall, wenn $A \cap B = A' \cap B$ gilt.
$\rightsquigarrow$ nur die Wahrscheinlichkeitsverteilung "im Bereich B" ist von Interesse
Tatsächlich definiert $P_B(x) := P(x)/P(B)$ für $x \in B$ eine Wahrscheinlichkeitsfunktion auf dem Ereignisraum B.
Beweis: $\sum_{x \in B} P_B(x) = \sum_{x \in B} P(x)/P(B) = 1$.
Diese Deutung der bedingten Wahrscheinlichkeit ist oft bequem.

Ein Beispiel Münzwurf mit zwei (fairen) Münzen

Ereignisraum $S = \{(\text{Kopf}, \text{Kopf}), (\text{Kopf}, \text{Zahl}), (\text{Zahl}, \text{Kopf}), (\text{Zahl}, \text{Zahl})\}$

Wie groß ist die Wahrscheinlichkeit, dass zwei Münzwürfe beide “Kopf” ergeben, wenn man sicher weiß, dass mindestens einer der Würfe “Kopf” ergibt ?

$A = \{(\text{Kopf}, \text{Kopf})\}$
$B = \{(\text{Kopf}, \text{Kopf}), (\text{Kopf}, \text{Zahl}), (\text{Zahl}, \text{Kopf})\}$.

$P(A|B) = \frac{P(A \cap B)}{P(B)} = \frac{P(A)}{P(B)} = \frac{1/4}{3/4} = \frac{1}{3}$
oder: $P_B((\text{Kopf}, \text{Kopf})) = 1/3$ direkt, da $(\text{Kopf}, \text{Kopf})$ Elementarereignis der Gleichverteilung über B ist.

Unabhängigkeit

Def.: Zwei Ereignisse A und B heißen *unabhängig*, gdw. $\mathrm{P}(\mathrm{A} \cap \mathrm{B}) = \mathrm{P}(\mathrm{A}) \cdot \mathrm{P}(\mathrm{B})$.

Beispiel: Wir betrachten wieder zwei Münzwürfe.
A bedeute: Der erste Wurf ergibt “Kopf”.
B bedeute: Die beiden Würfe sind verschieden.
C bedeute: Beide Würfe ergeben “Kopf”.

$\mathrm{A} \cap \mathrm{B}$ heißt: Der erste Wurf ergibt Kopf und der zweite “Zahl”.
$\mathrm{A} \cap \mathrm{C}$ heißt: Beide Würfe ergeben “Kopf” (also wie C).
$\mathrm{B} \cap \mathrm{C}$ ist das leere Ereignis.

Daher sind A und B unabhängig, aber nicht A und C oder B und C.

Der Satz von Bayes

Hinweis: Gilt $P(B) \neq 0$, so folgt: A und B sind unabhängig gdw. $P(A|B) = P(A)$.
Dies motiviert: Setze $P(A|B) = P(A)$, falls $P(B) = 0$.

Dann gilt (auch für $P(B) = 0$): $P(A \cap B) = P(B) \cdot P(A|B)$
sowie symmetrisch: $P(A \cap B) = P(A) \cdot P(B|A)$

$\rightsquigarrow$ Satz: (Bayes):

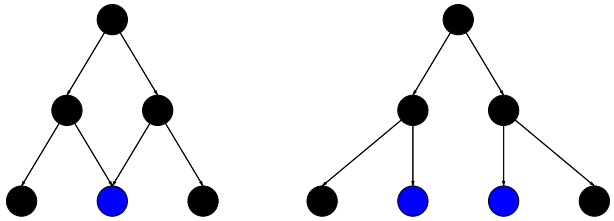
$$P(A|B) = \frac{P(A) \cdot P(B|A)}{P(B)}.$$

In der Anwendung oft nützlich:

$$P(B) = P(B \cap A) + P(B \cap \bar{A}) = P(A) \cdot P(B|A) + P(\bar{A}) \cdot P(B|\bar{A}).$$

Eine Anwendung: Das Galton-Brett

Betrachte das (kleine) Brett für Würfe mit nur zwei Münzen.
Dem entspricht die folgende graphische Darstellung, links nach Galton, rechts als Entscheidungsbaum:



Die blau gezeichneten Knoten geben jeweils das Ereignis B "genau einmal Kopf und einmal Zahl" wieder.
Da die Münzwürfe unabhängig sind, ist das Erreichen jedes Knotens auf der unteren Ebene des Entscheidungsbaums gleichwahrscheinlich, genauer beträgt sie $0,25 = 0,5 \cdot 0,5$.
Die Wahrscheinlichkeit, in einen der blauen Knoten des Entscheidungsbaums zu gelangen, ist daher $0,5 = 0,25 + 0,25$.
Wenn A bedeuten soll, dass im ersten Wurf "Kopf" oben war, so gilt außerdem:
$\mathrm{P}(\mathrm{B}) = \mathrm{P}(\mathrm{B} \cap \mathrm{A}) + \mathrm{P}(\mathrm{B} \cap \bar{\mathrm{A}}) = \mathrm{P}(\mathrm{A}) \cdot \mathrm{P}(\mathrm{B}|\mathrm{A}) + \mathrm{P}(\bar{\mathrm{A}}) \cdot \mathrm{P}(\mathrm{B}|\bar{\mathrm{A}}) = 0,5 \cdot 0,5 + 0,5 \cdot 0,5 = 0,5,$
denn "$\mathrm{B}|\mathrm{A}$" bedeutet: "Zahl im zweiten Wurf" und "$\mathrm{B}|\bar{\mathrm{A}}$" bedeutet: "Kopf im zweiten Wurf".

Eine Anwendung mit (un)fairen Münzen

Wir haben eine faire Münze und eine unfaire, die immer “Kopf” liefert. Das folgende Zufallsexperiment wird ausgeführt: “Wähle eine der beiden Münzen zufällig (fair) aus und wirf sie zweimal.”
Wie groß ist die Wahrscheinlichkeit dafür, die unfaire Münze ausgewählt zu haben, falls zweimal “Kopf” erscheint ?

A entspricht: die unfaire Münze wurde ausgewählt.
B heißt: Beide Münzwürfe liefern “Kopf”.
Wir fragen also nach: $P(A|B)$.
Bekannt: $P(A) = 1/2$; $P(B|A) = 1$; $P(B) = P(A) \cdot P(B|A) + P(\bar{A}) \cdot P(B|\bar{A}) = 5/8$.
Bayes $\rightsquigarrow$ $P(A|B) = 4/5$.

Die Bayes’sche Regel wird in der Praxis in ähnlicher Weise zur Bestimmung von Wahrscheinlichkeiten für nur indirekt beobachtete Ereignisse verwendet.

Zufallsvariablen

Def.: Eine *Zufallsvariable* (ZV), auch *Zufallsgröße* genannt, ist eine Abbildung aus einem Ereignisraum S in die reellen Zahlen.

Beispiel: Eine übliche ZV X_1 für ein Würfelexperiment mit einem Würfel liefert die Augenzahl. Beim Würfeln mit zwei Würfeln ergeben sich mehrere natürliche Möglichkeiten von ZV, z.B.: Minimum $X_{\min}$ / Maximum $X_{\max}$ / Summe der Augenzahlen $X_{\sum}$.

Es sei S ein Ereignisraum mit Wahrscheinlichkeitsfunktion P und einer ZV X. Die Wahrscheinlichkeit, dass X den Wert r annimmt, ist:

$$P[X = r] = \sum_{e \in X^{-}(r)} P(e).$$

Zufallsvariablen und Erwartungswert

Beispiel: Bestimme $P[X_{max} = 3]$:
$X_{max}(e) = 3$ für $e \in \{(1,3),(2,3),(3,3),(3,2),(3,1)\}$.
$\rightsquigarrow P[X_{max} = 3] = \frac{5}{36}$.

Satz: $P_X(r) = P[X = r]$ definiert eine Wahrscheinlichkeitsdichte auf $X(S)$.

Def.: Der *Erwartungswert* von X ist gegeben durch:

$$E[X] = \sum_{r \in X(S)} r \cdot P[X = r].$$

Beispiel: $E[X_1] = 3,5$.
Beispiel: $E[X_{max}] = \frac{1*1+2*3+3*5+4*7+5*9+6*11}{36} = \frac{1+6+15+28+45+66}{36} = \frac{40}{9} \approx 4,44$.

Ein längeres Beispiel: Multiple Choice

Bei einer Prüfung mit “Multiple-Choice-Fragen” werden drei Fragen gestellt, wobei für jede der drei Fragen zwei Antworten zur Auswahl vorliegen, von denen jeweils genau eine richtig ist. Die Antworten werden von einem nicht vorbereiteten Prüfling rein zufällig und unabhängig voneinander angekreuzt (Gleichverteilung). Sei Z die Zufallsvariable, welche die Anzahl der richtigen Antworten angibt.

Wie viele richtige Antworten liefert ein Prüfling “im Mittel”, wenn er “rein zufällig” seine Antworten wählt ?

Ein längeres Beispiel: Multiple Choice (Forts.)

Wie müssen wir den Wahrscheinlichkeitsraum wählen ?

$S = \{r, f\}^3$, wobei r für "richtig" und f für "falsch" stehe.

Ohne Vorkenntnisse gilt: $P(\{x\}) = 1/8$ für $x \in \{r, f\}^3$.

$Z(S) = \{0, 1, 2, 3\}$.

$P[Z = 0] = P((f, f, f)) = 1/8$

$P[Z = 1] = P(\{(r, f, f), (f, r, f), (f, f, r)\}) = 3/8$

$P[Z = 2] = P(\{(r, r, f), (f, r, r), (r, f, r)\}) = 3/8$

$P[Z = 3] = P((r, r, r)) = 1/8$

$E[Z] = \sum_{r \in [3]} rP[Z = r] = \frac{0*1+1*3+2*3+3*1}{8} = 1,5$

Erwartungswert Rechenregeln

Satz: Der Erwartungswert ist ein *lineares Funktional*.

Das heißt: $E[aX + bY] = aE[X] + bE[Y]$ für Zahlen a, b und ZV X, Y.

Beweis: elementar

Satz: (Ungleichung von Markoff)
Sei $c > 0$ und X eine ZV mit nichtnegativen Werten. $\rightsquigarrow$

$$P[X \geq c] \leq \frac{E[X]}{c}.$$

Beweis: $P[X \geq c] = \sum_{r \geq c} P[X = r] \leq \sum_{r \geq c} \frac{r}{c} \cdot P[X = r] \leq \sum_{r \geq 0} \frac{r}{c} \cdot P[X = r] = \frac{E[X]}{c}$.

Binomialverteilung als ausführliches Beispiel

Erinnerung: $b(k;n,p) = \left(\begin{array}{c} n \\ k \end{array} \right) \cdot p^k (1-p)^{n-k}$.

ZV X: Anzahl der "Erfolge" bei "Erfolgswahrscheinlichkeit" p.
$\rightsquigarrow P[X = k] = b(k;n,p)$.

$$
\begin{aligned}
E[X] &= \sum_{k \in [n+1]} k \cdot b(k;n,p) = \sum_{k \in [n+1]} k \cdot \left(\begin{array}{c} n \\ k \end{array} \right) \cdot p^k (1-p)^{n-k} \\
&= \sum_{k=1}^{n} k \cdot \frac{n}{k} \cdot \left(\begin{array}{c} n-1 \\ k-1 \end{array} \right) \cdot p^k (1-p)^{n-k} = n \cdot p \cdot \sum_{k=1}^{n} \left(\begin{array}{c} n-1 \\ k-1 \end{array} \right) \cdot p^{k-1} (1-p)^{n-k} \\
&= n \cdot p \cdot \sum_{k=0}^{n-1} \left(\begin{array}{c} n-1 \\ k \end{array} \right) \cdot p^k (1-p)^{n-1-k} = n \cdot p \cdot \sum_{k=0}^{n-1} b(k;n-1,p) = n \cdot p
\end{aligned}
$$

Geometrische Verteilung — ein weiteres Beispiel

Wir werfen wiederum wiederholt mit einer Münze, die mit Wahrscheinlichkeit p "Kopf" zeigt.

Wie oft muss man werfen, bis das erst Mal "Kopf" erscheint ?

X: ZV, die die Anzahl der nötigen Würfe beschreibt.
Definitionsbereich von X: Menge der endlichen Folgen von Münzwürfen.
$X(e)$ ist dann der Index der ersten Stelle, die "Kopf" ist.
Beispiel: $X((\text{Zahl}, \text{Zahl}, \text{Zahl}, \text{Kopf}, \text{Zahl}, \text{Kopf})) = 4$.
Wertebereich von X: Menge der positiven ganzen Zahlen.

$P[X = k] = (1-p)^{k-1}p$
$P[X = \cdot]$ ist Wahrscheinlichkeitsdichte wegen geometrischer Reihe:
$\sum_{k=1}^{\infty} P[X = k] = \sum_{k=1}^{\infty}(1-p)^{k-1}p = p \cdot \frac{1}{1-(1-p)} = 1.$
$E[X] = \sum_{k=1}^{\infty} k \cdot (1-p)^{k-1}p = \frac{p}{1-p}\sum_{k=0}^{\infty} k(1-p)^k = \frac{p}{1-p} \cdot \frac{1-p}{p^2} = \frac{1}{p}$;
erinnere dazu aus der Analysis: $\sum_k \frac{dx^k}{dx} = \frac{d\sum_k x^k}{dx}$.

Noch ein Beispiel (Fasching I)

Es werden wiederholt “zufällig” Bonbons an r Kinder verteilt.
Der Versuch eines Kindes, einen geworfenen Bonbon zu fangen, ist ein Bernoulli-Versuch. Jedes der Kinder fängt (in diesem einfachen Modell) mit derselben Wahrscheinlichkeit einen Bonbon; die Erfolgswahrscheinlichkeit jedes Kindes ist daher $p = 1/r$.

Wie groß ist die Wahrscheinlichkeit, dass ein bestimmtes Kind von n geworfenen Bonbons genau k fängt ?
Definiere dazu ZV X, deren Wert die Anzahl der von diesem speziellen Kind gefangenen Bonbons beschreibt.
$P[X = k] = b(n; k, 1/r)$ (Binomialverteilung)
$\rightsquigarrow E[X] = n/r$. d.h.; “im Mittel fängt ein Kind n/r Bonbons”.

Noch ein Beispiel (Fasching II)

Wie viele Bonbons müssen geworfen werden, bis dieses spezielle Kind einen Bonbon gefangen hat ?

Definiere dazu ZV Y, die die Nummer des ersten Wurfs angibt, bei dem das Kind ein Bonbon gefangen hat.

$P[Y = k] = (1 - 1/r)^{k-1} 1/r$ (geometrische Verteilung)

$\rightsquigarrow E[Y] = r$, d.h.,

"im Mittel muss ein Kind $r - 1$ Würfe warten, bis es ein Bonbon bekommt".

Noch ein Beispiel (Fasching III)

Wie viele Bonbons müssen geworfen werden, bis jedes Kind einen Bonbon gefangen hat ?

Definiere ZV X_i wie folgt: Wenn bereits $i-1$ Kinder mindestens einen Bonbon gefangen haben, gebe X_i die Zahl der Würfe an, die noch gemacht werden müssen, bis das i-te Kind einen Bonbon fängt.

Die Misserfolgswahrscheinlichkeit dieses Versuchs ist $(i-1)/r$.

Alle X_i sind untereinander unabhängig (warum?) und unterliegen jeweils der geometrischen Verteilung. Also gilt:

$$E[X_i] = \frac{1}{1-\frac{i-1}{r}} = \frac{r}{r-i+1}.$$

Für die ZV Z, die angibt, wie viele Versuche unternommen wurden, damit jedes Kind einen Bonbon gefangen hat, gilt: $Z = X_1 + X_2 + \cdots + X_r$. Also ist:

$$E[Z] = \sum_{i=1}^{r} E[X_i] = \sum_{i=1}^{r} \frac{r}{r-i+1} = r \cdot \sum_{i=1}^{r} \frac{1}{i}.$$

Man kann zeigen: Dies “in etwa gleichbedeutend mit” $r\ln(r)$ vielen Versuchen.

Abschließende Bemerkungen

Grundlegende Kenntnisse in der Wahrscheinlichkeitsrechnung werden sich insbesondere bei Kryptologie-Veranstaltungen als notwendig erweisen.

Wahrscheinlichkeitsrechnung ist in den meisten Schul-Curricula fester Bestandteil des Mathematik-Unterrichts.

Sollten Sie hier Lücken verspüren: Es gibt zahlreiche einfach gehaltene Einführungen, z.B. von Karl Bosch, Vieweg, 1986.