

- ▶ Ausgangssituation gegeben durch:  $(\Omega, P)$ , wobei
  - ▶  $\Omega$  : endliche Menge "Elementarereignisse"
  - ▶  $P : \Omega \rightarrow [0, 1]$  "Wahrscheinlichkeitsverteilung" mit

$$\sum_{\omega \in \Omega} P(\omega) = 1$$

- ▶  $P(\omega)$  : Wahrscheinlichkeit für das Eintreten des Ereignisses  $\omega$
- ▶  $(\Omega, P)$  : endlicher Wahrscheinlichkeitsraum
- ▶  $2^\Omega =$  Teilmengen von  $\Omega$  : "Ereignisse"
- ▶ Erweiterung zu einer Funktion  $P : 2^\Omega \rightarrow [0, 1]$

$$P(A) := \sum_{\omega \in A} P(\omega) \quad \text{für } A \subseteq \Omega$$

- ▶ Eigenschaften von  $P$ 
  - ▶  $P(\emptyset) = 0, P(\Omega) = 1$
  - ▶  $P(A \cup B) + P(A \cap B) = P(A) + P(B)$  für  $A, B \subseteq \Omega$

Beispiele:

- ▶ (fairer) Münzwurf:  $(\{H, T\}, P)$  mit  $P(H) = P(T) = 1/2$
- ▶ (allg.) Münzwurf :  $p \in [0, 1], (\{H, T\}, P)$  mit  $P(H) = p, P(T) = 1 - p$
- ▶ (fairer) Würfel:  $(\{1, 2, 3, 4, 5, 6\}, P)$  mit  $P(k) = 1/6$  für  $k = 1..6$
- ▶ Gleichverteilung ("uniform"):  $(\Omega, P^u)$  mit

$$P^u(\omega) = \frac{1}{\#\Omega} (\omega \in \Omega) \quad \text{also } P^u(A) = \frac{\#A}{\#\Omega}$$

- ▶  $\mathbb{B}^n$  mit Gleichverteilung mit  $P^u(\mathbf{a}) = 2^{-n}$  ( $\mathbf{a} \in \mathbb{B}^n$ )
- ▶  $\mathbb{B}^n$  mit Binomialverteilung für Parameter  $p \in [0, 1]$ :

$$\text{bin}_{n,p}(\mathbf{a}) = p^{|\mathbf{a}|} (1-p)^{n-|\mathbf{a}|} \quad (\mathbf{a} \in \mathbb{B}^n)$$

- ▶ Permutationen  $(\mathfrak{S}_n, P^u)$  mit  $P^u(\sigma) = 1/n!$  ( $\sigma \in \mathfrak{S}_n$ ).

Konstruktionen

- ▶ Teilmengen und bedingte Wahrscheinlichkeiten
  - ▶ Ist  $(\Omega, P)$  W.raum und  $A \subseteq \Omega$  mit  $P(A) > 0$  so ist

$$(A, P_A) \text{ mit } P_A : 2^A \rightarrow [0, 1] : B \mapsto \frac{P(B)}{P(A)}$$

W.raum ("Unterraum")

- ▶ In dieser Situation ist  $(\Omega, P(\cdot|A))$  mit

$$P(\cdot|A) : 2^\Omega \rightarrow [0, 1] : B \mapsto P(B|A) = \frac{P(A \cap B)}{P(A)}$$

eine W.raum: "durch A bedingte Wahrscheinlichkeiten".

Unabhängige Ereignisse

- ▶ Sind  $A, B$  Ereignisse mit  $P(A), P(B) > 0$  so ist

$$P(A|B) \cdot P(B) = P(A \cap B) = P(B|A) \cdot P(A)$$

(Formel von BAYES)

- ▶  $A, B \in 2^\Omega$  sind *unabhängig* in  $(\Omega, P)$ , falls

$$P(A \cap B) = P(A) \cdot P(B)$$

Es gilt dann:  $P(A|B) = P(A)$  und  $P(B|A) = P(B)$ .



▶ Wesentliche Parameter einer Zufallsvariablen

- ▶  $E[X]$  Erwartungswert ("Mittelwert")

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

- ▶  $V(X)$  Varianz ("mittlere quadratische Abweichung vom Mittelwert")

$$V[X] := E[(X - E[X])^2] = E[X^2] - E[X]^2$$

- ▶ Linearität des Erwartungswertes: für  $X, Y : \Omega \rightarrow \mathbb{R}, a, b \in \mathbb{R}$

$$E[a \cdot X + b \cdot Y] = a \cdot E[X] + b \cdot E[Y]$$

- ▶ Folgerung (beachte  $E[X] \in \mathbb{R}$ )

$$\begin{aligned} V[X] &:= E[(X - E[X])^2] \\ &= E[X^2 - 2 \cdot X \cdot E[X] + E[X]^2] \\ &= E[X^2] - 2 \cdot E[X]^2 + E[X]^2 \\ &= E[X^2] - E[X]^2 \end{aligned}$$

Beispiele

- ▶ fairer Münzwurf mit  $X(H) = +1, X(T) = 0$

- ▶  $E[X] = \frac{1}{2} \cdot 1 + \frac{1}{2} \cdot 0 = \frac{1}{2}$
- ▶  $V[X] = \frac{1}{2} \cdot 1^2 + \frac{1}{2} \cdot 0^2 - (\frac{1}{2})^2 = \frac{1}{4}$

- ▶ fairer Würfel mit  $X(k) = k$  ( $1 \leq k \leq 6$ )

- ▶  $E[X] = \frac{1}{6}(1 + 2 + 3 + 4 + 5 + 6) = \frac{7}{3}$
- ▶  $V[X] = \frac{1}{6}(1^2 + 2^2 + 3^2 + 4^2 + 5^2 + 6^2) - (\frac{7}{3})^2 = \frac{91}{6} - (\frac{7}{3})^2 = \frac{175}{18}$

- ▶ Bitvektoren ( $\mathbb{B}^n, \text{bin}_{n,p}$ )
- ▶ Zufallsvariable  $X : \mathbb{B}^n \rightarrow \{0, 1, \dots, n\} : \mathbf{a} \mapsto \|\mathbf{a}\|$
- ▶  $\{X = k\} = \mathbb{B}_k^n, \text{bin}_{n,p}\{X = k\} = \binom{n}{k} p^k (1-p)^{n-k}$ 
  - ▶ Erwartungswert

$$\begin{aligned} E[X] &= \sum_{\mathbf{a} \in \mathbb{B}^n} \|\mathbf{a}\| \cdot \text{bin}_{n,p}(\mathbf{a}) = \sum_{k=0}^n k \cdot \binom{n}{k} p^k (1-p)^{n-k} \\ &= np \cdot \sum_{k=0}^{n-1} \binom{n-1}{k} p^k (1-p)^{n-1-k} = np \end{aligned}$$

- ▶ Varianz

$$\begin{aligned} V[X] &= E[X^2] - E[X]^2 = E[X(X-1)] + E[X] - E[X]^2 \\ &= \sum_{k=0}^n k(k-1) \cdot \binom{n}{k} p^k (1-p)^{n-k} + np - (np)^2 \\ &= n(n-1)p^2 - np - (np)^2 = np(1-p) \end{aligned}$$

- ▶ Permutationen  $(\mathfrak{S}_n, P^u)$  ( $\simeq$  Inversionsvektoren)
- ▶ Zufallsvariable: Anzahl der Inversionen

$$\text{inv} : \mathcal{L}_n \rightarrow \{0, 1, \dots, \binom{n(n-1)}{2}\} : (\ell_1, \ell_2, \dots, \ell_n) \mapsto \ell_1 + \dots + \ell_n$$

- ▶ Erwartungswert

$$E[\text{inv}] = \frac{n(n-1)}{4}$$

- ▶ Varianz

$$V[\text{inv}] = \frac{n(n-1)(2n+5)}{72}$$

- ▶ Permutationen  $(\mathfrak{S}_n, P^u)$  ( $\simeq$  Inversionsvektoren)
- ▶ Zufallsvariable: Anzahl der Links-Rechts-Maxima

$$\text{lrm} : \mathcal{L}_n \rightarrow \{1, 2, \dots, n\} : (\ell_1, \ell_2, \dots, \ell_n) \mapsto \#_k(\ell_1, \dots, \ell_n)$$

- ▶ Erwartungswert

$$E[\text{lrm}] = H_n$$

- ▶ Varianz

$$V[\text{lrm}] = H_n - H_n^{(2)}$$

- ▶ Zufallsvariablen  $X, Y : (\Omega, P) \rightarrow \mathbb{N}$  sind *unabhängig*, wenn für alle  $k, \ell \in \mathbb{N}$  die Ereignisse  $\{X = k\}$  und  $\{Y = \ell\}$  unabhängig sind, d.h.

$$P(\{X = k\} \cap \{Y = \ell\}) = P\{X = k\} \cdot P\{Y = \ell\} \quad (k, \ell \in \mathbb{N})$$

d.h.

$$P_{(X,Y)}(k, \ell) = P_X(k) \cdot P_Y(\ell)$$

- ▶ Analog definiert man Unabhängigkeit für mehrere Zufallsvariable

- ▶ Folgerungen: für unabhängige Zufallsvariablen  $X, Y$  gilt

- ▶  $E[X \cdot Y] = E[X] \cdot E[Y]$

$$\begin{aligned} E[X \cdot Y] &= \sum_{k \in \mathbb{N}} k \cdot P\{X \cdot Y = k\} \\ &= \sum_{\ell, m \in \mathbb{N}} \ell \cdot m \cdot P\{X = \ell\} \cdot P\{Y = m\} \\ &= \sum_{\ell \in \mathbb{N}} \ell \cdot P\{X = \ell\} \cdot \sum_{m \in \mathbb{N}} m \cdot P\{Y = m\} = E[X] \cdot E[Y] \end{aligned}$$

- ▶  $V[X + Y] = V[X] + V[Y]$

$$\begin{aligned} V[X + Y] &= E[(X + Y)^2] - E[X + Y]^2 \\ &= E[X^2 + 2X \cdot Y + Y^2] - (E[X] + E[Y])^2 \\ &= E[X^2] + 2E[X \cdot Y] + E[Y^2] - E[X]^2 - 2E[X] \cdot E[Y] - E[Y]^2 \\ &= E[X^2] - E[X]^2 + E[Y^2] - E[Y]^2 = V[X] + V[Y] \end{aligned}$$

- ▶ Inversionsvektoren  $(\mathbb{B}^n, \text{bin}_{n,p})$
- ▶ betrachte Zufallsvariable  $X_1, X_2, \dots, X_n$  mit

$$X_k : \mathbb{B}^n \rightarrow \{0, 1\} : \mathbf{a} \mapsto a_k \quad (1 \leq k \leq n)$$

- ▶ Diese Zufallsvariablen sind unabhängig und es ist

$$E[X_k] = p \quad V[X_k] = p(1-p)$$

- ▶ Für  $X : \mathbf{a} \mapsto \|\mathbf{a}\|$  gilt  $X = X_1 + X_2 + \dots + X_n$ , also

$$E[X] = n \cdot E[X_1] = np$$

$$V[X] = n \cdot V[X_1] = np(1-p)$$

- ▶ Inversionsvektoren  $(\mathcal{L}_n, P^u)$
- ▶ Für Links-Rechts-Maxima in Permutationen betrachte Zufallsvariable  $X_1, X_2, \dots, X_n$  mit

$$X_k : \mathcal{L}_n \rightarrow \{0, 1\} : \ell = (\ell_1, \dots, \ell_n) \mapsto \chi_{\ell_k=0} \quad (1 \leq k \leq n)$$

- ▶ Diese Zufallsvariable sind unabhängig und es gilt

$$E[X_k] = \frac{1}{k} \quad V[X_k] = \frac{1}{k} - \left(\frac{1}{k}\right)^2$$

- ▶ Für  $X : \mathcal{L}_n \rightarrow \{1, \dots, n\} : \ell \mapsto \#0\ell$  gilt  $X = X_1 + X_2 + \dots + X_n$ , also

$$E[X] = \sum_{k=1}^n E[X_k] = H_n$$

$$V[X] = \sum_{k=1}^n V[X_k] = H_n - H_n^{(2)}$$

- ▶ Inversionsvektoren  $(\mathcal{L}_n, P^u)$
- ▶ Für Anzahl Inversionen in Permutationen betrachte Zufallsvariable  $X_1, X_2, \dots, X_n$  mit

$$X_k : \mathcal{L}_n \rightarrow \{0, 1\} : \ell = (\ell_1, \dots, \ell_n) \mapsto \ell_k \quad (1 \leq k \leq n)$$

- ▶ Diese Zufallsvariable sind unabhängig und es gilt

$$E[X_k] = \frac{k-1}{2}, \quad V[X_k] = \frac{(k-1)(2k-1)}{6} - \left(\frac{k-1}{2}\right)^2 = \frac{(k-1)(k+1)}{12}$$

- ▶ Für  $X : \mathcal{L}_n \rightarrow \{1, \dots, \binom{n}{2}\} : \ell \mapsto \ell_1 + \ell_2 + \dots + \ell_n$  gilt  $X = X_1 + X_2 + \dots + X_n$ , also

$$E[X] = \sum_{k=1}^n E[X_k] = \sum_{k=1}^n \frac{k-1}{2} = \frac{n(n-1)}{4}$$

$$V[X] = \sum_{k=1}^n V[X_k] = \sum_{k=1}^n \frac{(k-1)(k+1)}{12} = \frac{n(n-1)(2n-5)}{72}$$

- ▶ Ist  $X : (\Omega, P) \rightarrow \mathbb{N}$  eine ZV, so definiert man das *erzeugende Polynom*, indem man jedem Ereignis  $\omega \in \Omega$  das Monom  $z^{X(\omega)}$  zuordnet und aufsummiert:

$$p_X(z) = \sum_{k \in \mathbb{N}} P\{X = k\} z^k = \sum_{\omega \in \Omega} z^{X(\omega)}$$

- ▶ Dann gilt
  - ▶ Erwartungswert

$$E[X] = [p_X(z)']_{z=1} = p'(1)$$

- ▶ Varianz

$$V[X] = [p_X(z)''']_{z=1} + [p_X(z)']_{z=1} - [p_X(z)']_{z=1}^2$$

$$= p_X''(1) + p_X'(1) - p_X'(1)^2$$

- ▶ Faltungsformel für unabhängige ZVen  $X, Y$ :

$$p_{X+Y}(z) = p_X(z) \cdot p_Y(z)$$





- ▶ Mittels der MARKOV-Ungleichung für  $Z$  erhält man

$$\begin{aligned} P\{X - np \geq \delta\} &= P\{Z \geq e^{\alpha\delta}\} \\ &\leq E[Z] \cdot e^{-\alpha\delta} \\ &\leq e^{\alpha^2(1-p)n/2 - \alpha\delta} \end{aligned}$$

- ▶ Man kann  $\alpha$  so wählen, dass der Ausdruck auf der rechten Seite so klein wie möglich wird: das führt auf  $\alpha = \frac{\delta}{n(1-p)}$ . Setzt man dies ein, erhält man die Behauptung.