

Tutorium Theoretische Grundlagen der Informatik

Simon Bischof

Institut für Kryptographie und Sicherheit



- Abgabe ÜB 6 am Mo., 28.01
- Veröffentlichung ÜB 7 schon am Mo., 28.01
- Abgabe von ÜB 7 schon Fr., 01.02.
- Blatt 7: Nur 2 Aufgaben werden gewertet
- Zusätzlich Wiederholungsaufgaben: werden nicht gewertet. Ich werde diese Aufgaben dennoch korrigieren.

- $3SAT \leq_p HAMILTON-PATH$
- Fixed parameter tractability
- Average case complexity
- Impalazzos Welten
- Counting Classes und Probabilistische Klassen:
 $\#P, \mathcal{R}, co\mathcal{R}, ZPP, PP, BPP$

- $\log(a \cdot b) = \log a + \log b$, $\log(a^b) = b \log(a)$, insbesondere $\log \frac{1}{a} = -\log(a)$
- Hier: $0 \cdot \log 0 := 0$, $0 \cdot \log \frac{0}{0} = 0$, $a \cdot \log \frac{a}{0} = \infty$ ($a > 0$)

- $\log(a \cdot b) = \log a + \log b$, $\log(a^b) = b \log(a)$, insbesondere $\log \frac{1}{a} = -\log(a)$
- Hier: $0 \cdot \log 0 := 0$, $0 \cdot \log \frac{0}{0} = 0$, $a \cdot \log \frac{a}{0} = \infty$ ($a > 0$)
- Sind X_1, X_2, \dots, X_n stochastisch unabhängige ZV, so ist $p(X_1 = x_1, X_2 = x_2, \dots, X_n = x_n) = p(X_1 = x_1) \cdot p(X_2 = x_2) \cdot \dots \cdot p(X_n = x_n)$
- Erwartungswert: $\mathbb{E}(X) = \sum_{x \in X} x \cdot p(x)$

- $\log(a \cdot b) = \log a + \log b$, $\log(a^b) = b \log(a)$, insbesondere $\log \frac{1}{a} = -\log(a)$
- Hier: $0 \cdot \log 0 := 0$, $0 \cdot \log \frac{0}{0} = 0$, $a \cdot \log \frac{a}{0} = \infty$ ($a > 0$)
- Sind X_1, X_2, \dots, X_n stochastisch unabhängige ZV, so ist $p(X_1 = x_1, X_2 = x_2, \dots, X_n = x_n) = p(X_1 = x_1) \cdot p(X_2 = x_2) \cdot \dots \cdot p(X_n = x_n)$
- Erwartungswert: $\mathbb{E}(X) = \sum_{x \in X} x \cdot p(x)$
- Bedingte Wahrscheinlichkeit: $p(y|x) = \frac{p(x,y)}{p(x)}$

Information I_p für Zeichen der Wahrscheinlichkeit (WK) p

- $I_p \geq 0$
- $I_1 = 0$
- I ist stetig
- Sind zwei Ereignisse mit WK p_1, p_2 stochastisch unabhängig, dann
$$I_{(p_1 \cdot p_2)} = I_{p_1} + I_{p_2}$$

- $I_p := \log_b \frac{1}{p} [= -\log_b p]$; hier immer $b = 2$

- $I_p := \log_b \frac{1}{p} [= -\log_b p]$; hier immer $b = 2$
- Entropie: $H(x) = \sum_{x \in X} p(x) \log \frac{1}{p(x)} = \mathbb{E} I(x)$

- $I_p := \log_b \frac{1}{p} [= -\log_b p]$; hier immer $b = 2$
- Entropie: $H(x) = \sum_{x \in X} p(x) \log \frac{1}{p(x)} = \mathbb{E} I(x)$
- Für Basis b gilt: $H_b(X) = \log_b 2 H(X)$

- Gemeinsame Entropie: $H(X, Y) = \sum_{x \in X} \sum_{y \in Y} p(x, y) \log \frac{1}{p(x, y)}$

■ Gemeinsame Entropie: $H(X, Y) = \sum_{x \in X} \sum_{y \in Y} p(x, y) \log \frac{1}{p(x, y)}$

■ Bedingte Entropie: $H(Y|X) = \sum_{x \in X} H(Y|X = x) =$
 $-\sum_{x \in X} p(x) \sum_{y \in Y} p(y|x) \log(p(y|x)) = -\sum_{x \in X, y \in Y} p(x, y) \log(p(y|x))$

$\Rightarrow H((X, Y)|Z) = H(X|Z) + H(Y|X, Z)$

- Gemeinsame Entropie: $H(X, Y) = \sum_{x \in X} \sum_{y \in Y} p(x, y) \log \frac{1}{p(x, y)}$
 - Bedingte Entropie: $H(Y|X) = \sum_{x \in X} H(Y|X = x) =$
 $-\sum_{x \in X} p(x) \sum_{y \in Y} p(y|x) \log(p(y|x)) = -\sum_{x \in X, y \in Y} p(x, y) \log(p(y|x))$
- $\Rightarrow H((X, Y)|Z) = H(X|Z) + H(Y|X, Z)$
- Kettenregel: $H(X, Y) = H(X) + H(Y|X) = H(Y) + H(X|Y)$
 - Achtung: Es kann sein dass $H(X|Y) \neq H(Y|X)$!

Sei ein Kanal gegeben, der ein Symbol von X nach Y überträgt, und evtl. nicht fehlerfrei ist.

- $H(X, Y)$ heißt Totalinformation
- $H(X|Y)$ heißt Äquivokation
- $H(Y|X)$ heißt Fehlinformation/Irrelevanz

Sei ein Kanal gegeben, der ein Symbol von X nach Y überträgt, und evtl. nicht fehlerfrei ist.

- $H(X, Y)$ heißt Totalinformation
- $H(X|Y)$ heißt Äquivokation
- $H(Y|X)$ heißt Fehlinformation/Irrelevanz
- Transinformation: $I(X; Y) := H(X) - H(X|Y) = H(Y) - H(Y|X)$

Präfix-freie Codes

