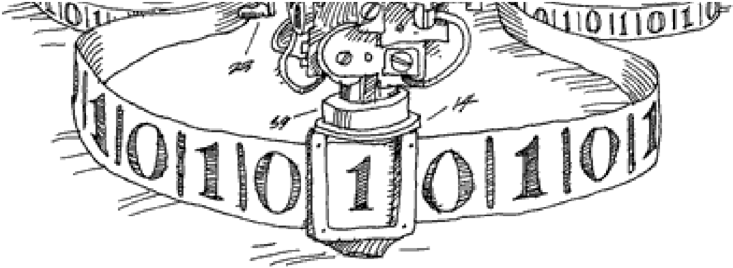
Karlsruher Institut für Technologie

Tutorium Theoretische Grundlagen der Informatik

Simon Bischof

Institut für Kryptographie und Sicherheit



Organisatorisches

- 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.

VL letzte Woche (VL-Folien/Skript)

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

Informationstheorie

Karlsruher Institut für Technologie

Rechenregeln für $\log$ und Wahrscheinlichkeiten

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

Rechenregeln für log und Wahrscheinlichkeiten

- $\log(a \cdot b) = \log a + \log b$, $\log(a^b) = b \log(a)$, 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 $X_1, X_2, \ldots, X_n$ stochastisch unabhängige ZV, so ist $p(X_1 = x_1, X_2 = x_2, \ldots, X_n = x_n) = p(X_1 = x_1) \cdot p(X_2 = x_2) \cdot \ldots \cdot p(X_n = x_n)$
- Erwartungswert: $\mathbb{E}(X) = \sum\limits_{x \in X} x \cdot p(x)$

Rechenregeln für log und Wahrscheinlichkeiten

- $\log(a \cdot b) = \log a + \log b$, $\log(a^b) = b \log(a)$, 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 $X_1, X_2, \ldots, X_n$ stochastisch unabhängige ZV, so ist $p(X_1 = x_1, X_2 = x_2, \ldots, X_n = x_n) = p(X_1 = x_1) \cdot p(X_2 = x_2) \cdot \ldots \cdot p(X_n = x_n)$
- Erwartungswert: $\mathbb{E}(X) = \sum\limits_{x \in X} x \cdot p(x)$
- Bedingte Wahrscheinlichkeit: $p(y|x) = \frac{p(x,y)}{p(x)}$

Eigenschaften von Information

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 $I_{(p_1 \cdot p_2)} = I_{p_1} + I_{p_2}$

Quellen, Information, Entropie

- Eine Quelle sendet Zeichen mit einer gewissen WK aus.

Quellen, Information, Entropie

Karlsruher Institut für Technologie

- Eine Quelle sendet Zeichen mit einer gewissen WK aus.
- Sie heißt gedächtnislos, falls die WK für ein Zeichen nicht von den vorigen Zeichen abhängt.

Quellen, Information, Entropie

- Eine Quelle sendet Zeichen mit einer gewissen WK aus.
- Sie heißt gedächtnislos, falls die WK für ein Zeichen nicht von den vorigen Zeichen abhängt.
- $I_p := \log_b \frac{1}{p} [= -\log_b p]$
- Hier immer $b = 2$, dadurch Einheit ”bit”

Quellen, Information, Entropie

- Eine Quelle sendet Zeichen mit einer gewissen WK aus.
- Sie heißt gedächtnislos, falls die WK für ein Zeichen nicht von den vorigen Zeichen abhängt.
- $I_p := \log_b \frac{1}{p} [= -\log_b p]$
- Hier immer $b = 2$, dadurch Einheit "bit"
- Entropie: $H(X) = \sum_{x \in X} p(x) \log \frac{1}{p(x)} = \mathbb{E} I(x)$

Quellen, Information, Entropie

- Eine Quelle sendet Zeichen mit einer gewissen WK aus.
- Sie heißt gedächtnislos, falls die WK für ein Zeichen nicht von den vorigen Zeichen abhängt.
- $I_p := \log_b \frac{1}{p} [= -\log_b p]$
- Hier immer $b = 2$, dadurch Einheit "bit"
- Entropie: $H(X) = \sum_{x \in X} p(x) \log \frac{1}{p(x)} = \mathbb{E} I(x)$
- Für Basis b gilt: $H_b(X) = \log_b 2 \cdot H(X)$

Quellen, Information, Entropie

Karlsruher Institut für Technologie

- Eine Quelle sendet Zeichen mit einer gewissen WK aus.
- Sie heißt gedächtnislos, falls die WK für ein Zeichen nicht von den vorigen Zeichen abhängt.
- $I_p := \log_b \frac{1}{p} [= -\log_b p]$
- Hier immer $b = 2$, dadurch Einheit "bit"
- Entropie: $H(X) = \sum_{x \in X} p(x) \log \frac{1}{p(x)} = \mathbb{E} I(x)$
- Für Basis b gilt: $H_b(X) = \log_b 2 \cdot H(X)$
- maximale Entropie bei n Zeichen: $\log n$; genau dann wenn alle Zeichen gleich wahrscheinlich sind (WK $\frac{1}{n}$)

Gemeinsame und bedingte Entropie

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

Gemeinsame und bedingte Entropie

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

Gemeinsame und bedingte Entropie

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

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

- Achtung: Es kann sein dass $H(X|Y) \neq H(Y|X)$!

Datenübertragung

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

Datenübertragung

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 Codes

- Sei Q ein Alphabet und $f : Q \longrightarrow \Sigma^*$ eine Kodierung.

Präfix Codes

- Sei Q ein Alphabet und $f : Q \longrightarrow \Sigma^*$ eine Kodierung.
- Achtung: Evtl. ist die Dekodierung nicht eindeutig!

Präfix Codes

- Sei Q ein Alphabet und $f : Q \to \Sigma^*$ eine Kodierung.
- Achtung: Evtl. ist die Dekodierung nicht eindeutig!
- Falls für alle Codewörter $c_1 c_2 \dots c_n \in f(Q)$ und für $k < n$ das Wort $c_1 c_2 \dots c_k$ kein Codewort ist, so heißt die Kodierung Präfix-Code.
- Präfix-Codes sind immer eindeutig.

Die Huffman-Kodierung

Karlsruher Institut für Technologie

- Die Huffman-Kodierung ist ein für gedächtnislose Quellen optimaler Präfix-Code.

Die Huffman-Kodierung

- Die Huffman-Kodierung ist ein für gedächtnislose Quellen optimaler Präfix-Code.

- Konstruktion: Für jedes Zeichen ein eigener Knoten. Häufigkeit dazuschreiben.

Die Huffman-Kodierung

Karlsruher Institut für Technologie

- Die Huffman-Kodierung ist ein für gedächtnislose Quellen optimaler Präfix-Code.

- Konstruktion: Für jedes Zeichen ein eigener Knoten. Häufigkeit dazuschreiben.
- Dann schrittweise einen Baum erstellen:
  Zwei (Wurzel-)Knoten aussuchen, dass Summe der Häufigkeiten minimal wird.
- Füge dann einen neuen Knoten als Vater dieser beiden Knoten hinzu und schreibe diese Summe dazu.

Die Huffman-Kodierung

- Die Huffman-Kodierung ist ein für gedächtnislose Quellen optimaler Präfix-Code.

- Konstruktion: Für jedes Zeichen ein eigener Knoten. Häufigkeit dazuschreiben.
- Dann schrittweise einen Baum erstellen:
  Zwei (Wurzel-)Knoten aussuchen, dass Summe der Häufigkeiten minimal wird.
- Füge dann einen neuen Knoten als Vater dieser beiden Knoten hinzu und schreibe diese Summe dazu.
- Am Ende: Wege nach links: 0, nach rechts: 1