Theoretische Grundlagen der Informatik
Tutorium XII & XIII (SR 301)

Tut Nr. 13 – Üb11, Informationstheorie

David Münch

Karlsruher Institut für Technologie
Institut für Informatik
IKS Müller-Quade

4. Februar 2010

Karlsruher Institut für Technologie

Inhaltsverzeichnis

1 Auftakt

Inhaltsverzeichnis

1. Auftakt
2. Lernziele

Inhaltsverzeichnis

1 Auftakt

2 Lernziele

3 Themen
- Übungsblatt 11
- Grundbegriffe der Informationstheorie
- Kanal
- Hamming-Code

Inhaltsverzeichnis

1. Auftakt
2. Lernziele
3. Themen
   - Übungsblatt 11
   - Grundbegriffe der Informationstheorie
   - Kanal
   - Hamming-Code
4. Abspann

Inhaltsverzeichnis

1. Auftakt
2. Lernziele
3. Themen
   - Übungsblatt 11
   - Grundbegriffe der Informationstheorie
   - Kanal
   - Hamming-Code
4. Abspann
5. Abspann

Organisatorisches

Email: muenchdavid@gmail.com

`https://www.stud.uni-karlsruhe.de/~uhbro/`

Tutorium 12: Donnerstags 8:00 Uhr - Raum 301
Tutorium 13: Donnerstags 9:45 Uhr - Raum 301

Übungsblattabgabe Mittwochs 12:00 Uhr.

Organisatorisches

44 Punkte sind notwendig für den Schein.

Das nächste und somit gleichzeitig auch das letzte Übungsblatt wird nicht korrigiert und gibt auch keine Punkte.

Organisatorisches

Nicht abgeholte Übungsblätter können ab sofort bei Nico Döttling R274 abgeholt werden.
`https://puck.iaks.uka.de/eiss/?id=167`

Wichtig!

Es gibt zum neuen Thema ein vorlesungsbegleitendes Skriptum unter: `https://puck.iaks.uka.de/eiss/fileadmin/User/Info_3/skript.pdf`.

Wichtig!

Die Onlineanmeldung für den Schein _und_ die Klausur nicht verpassen!

Was wollen wir heute erreichen?

Was wollen wir heute erreichen?

- Übungsblatt 11 besprechen

Was wollen wir heute erreichen?

- Übungsblatt 11 besprechen
- Wiederholung von Grundbegriffen der Informationstheorie

Was wollen wir heute erreichen?

- Übungsblatt 11 besprechen
- Wiederholung von Grundbegriffen der Informationstheorie
- Kanäle verstehen

Was wollen wir heute erreichen?

- Übungsblatt 11 besprechen
- Wiederholung von Grundbegriffen der Informationstheorie
- Kanäle verstehen
- Hamming-Code

Übungsblatt 11

Grundbegriffe der Informationstheorie

Kommunikationssystem

$$
\begin{array}{ccccccccc}
 & & & & \boxed{\textbf{Rauschen}} & & & & \\
 & & & & \downarrow & & & & \\
\boxed{\textbf{Quelle}} & \to & \boxed{\textbf{Codierer}} & \to & \boxed{\textbf{Kanal}} & \to & \boxed{\textbf{Decodierer}} & \to & \boxed{\textbf{Empfänger}}
\end{array}
$$

Die Informationstheorie versucht nun die einzelnen Blöcke durch ein mathematisches Modell zu bescheiben.

Zentrale Fragen der Informationstheorie

- Wieviel Information enthält eine Nachricht?

Zentrale Fragen der Informationstheorie

- Wieviel Information enthält eine Nachricht?
- Wieviel von der Nachricht ist überflüssig?

Zentrale Fragen der Informationstheorie

- Wieviel Information enthält eine Nachricht?
- Wieviel von der Nachricht ist überflüssig?
- Kann die Nachricht noch gelesen werden wenn Störungen auftreten?

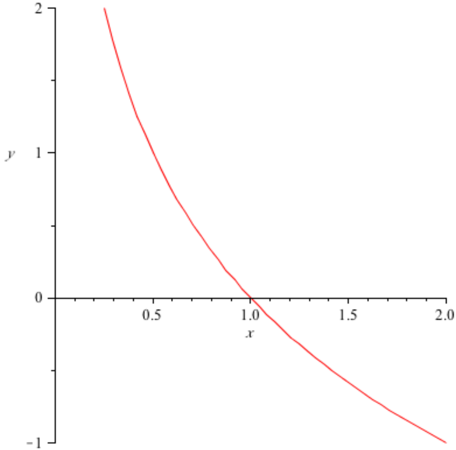
Beispiel:
Sendet man statt einer Eins n Einsen, dann kann man für $n \to \infty$ die Fehlerwahrscheinlichkeit beliebig klein machen auf Kosten der Übertragungsgeschwindigkeit.

Entropie

Definition:

Sei X eine Zufallsvariable mit den unabhängigen Ereignissen $x_1, ..., x_m$ und sei $p_i = p(x_i) = P(X = x_i)$ die Wahrscheinlichkeit eines Ereignisses x_i, das mit der Unsicherheit (Information) $h(x_i)$ behaftet ist.
Eine Ereignissfolge $x_i x_j$ tritt mit der Wahrscheinlichkeit $p_{ij} = p(x_i x_j) = p_i \cdot p_j$ auf und hat die Unsicherheit $h(p_{ij}) = h(p_i) + h(p_j)$.
U.a. daraus folgt, dass die Unsicherheitsfunktion (oder Information eines Zeichens) von der Gestalt $h(p) = -\log_b p$ sein muss.

Entropie



Entropie

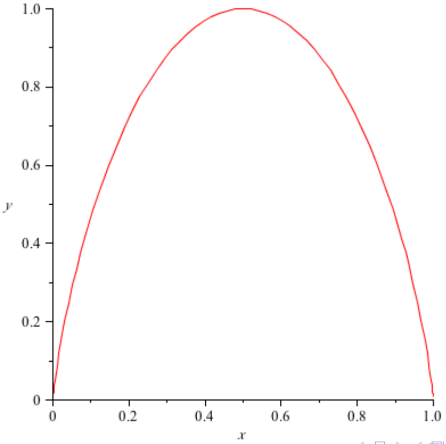
Definition: Entropie

Die Entropie (Informationsgehalt) einer Zufallsvariablen X ist $H(X) = H(p_1, ..., p_m) = -\sum_{i=1}^{m} p_i \log p_i$

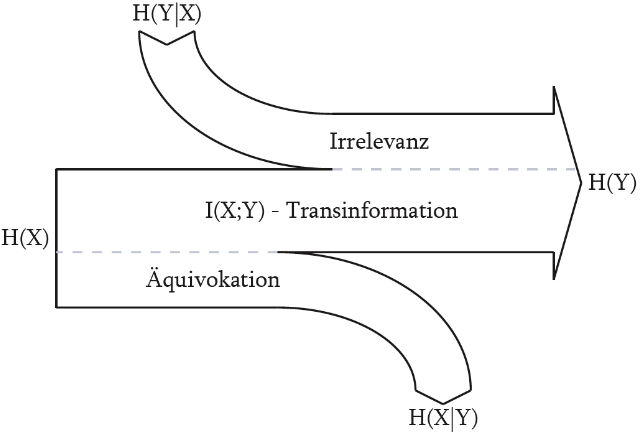
Die Entropie ist die Information pro Zeichen, die wir erwarten.
Oder: Die Entropie ist die durchschnittliche Anzahl von Entscheidungen (bits), die benötigt werden, um ein Zeichen aus einer Zeichenmenge zu identifizieren oder zu isolieren.

Entropie

Beispiel: Entropie von Münzen: $H(p, 1-p)$



Übertragungskanal



Zusammenfassung

Transinformation: $I(X|Y) = H(X) - H(X|Y) = I(Y|X)$

Zusammenfassung

Transinformation: $I(X|Y) = H(X) - H(X|Y) = I(Y|X)$
Äquivokation: $H(X|Y) = H(X) - I(X|Y)$

Zusammenfassung

Transinformation: $I(X|Y) = H(X) - H(X|Y) = I(Y|X)$
Äquivokation: $H(X|Y) = H(X) - I(X|Y)$
Irrelevanz: $H(Y|X) = H(Y) - I(X|Y)$

Zusammenfassung

Transinformation: $I(X|Y) = H(X) - H(X|Y) = I(Y|X)$
Äquivokation: $H(X|Y) = H(X) - I(X|Y)$
Irrelevanz: $H(Y|X) = H(Y) - I(X|Y)$
Totalinformation: $H(Y|X) + I(X|Y) + H(X|Y)$

Kanaleigenschaften

- deterministisch: $H(Y|X) = 0$

Kanaleigenschaften

- deterministisch: $H(Y|X) = 0$
- verlustfrei: $H(X|Y) = 0$

Kanaleigenschaften

- deterministisch: $H(Y|X) = 0$
- verlustfrei: $H(X|Y) = 0$
- störungsfrei: $H(X|Y) = H(Y|X) = 0$

Kanaleigenschaften

- deterministisch: $H(Y|X) = 0$
- verlustfrei: $H(X|Y) = 0$
- störungsfrei: $H(X|Y) = H(Y|X) = 0$
- nutzlos: $I(X|Y) = 0$

Kanaleigenschaften

- deterministisch: $H(Y|X) = 0$
- verlustfrei: $H(X|Y) = 0$
- störungsfrei: $H(X|Y) = H(Y|X) = 0$
- nutzlos: $I(X|Y) = 0$

Die Zufallsvariablen X und Y sind genau dann stochastisch unabhängig, wenn der Kanal nutzlos ist.
$H(X,Y) = H(X) + H(Y)$

Kanalkapazität

Definition: Kanalkapazität

$C = max_{P(X)}\{I(X|Y)\}$
C ist die höchste Informationsmenge, die unter allen möglichen Quellenverteilungen über den Kanal übertragen werden kann.

Aufgabe

Gegeben sei folgender binärer, asymetrischer Kanal über den Alphabeten $\mathcal{X} = \mathcal{Y} = \{0, 1\}$:

$$\begin{array}{cc} P(0|0) = 1 - \beta & P(1|0) = \beta \\ P(0|1) = 0 & P(1|1) = 1 \end{array}$$

a) Für welches β hat der Kanal maximale Kapazität?

Aufgabe

Gegeben sei folgender binärer, asymetrischer Kanal über den Alphabeten $\mathcal{X} = \mathcal{Y} = \{0, 1\}$:

$$\begin{array}{cc} P(0|0) = 1 - \beta & P(1|0) = \beta \\ P(0|1) = 0 & P(1|1) = 1 \end{array}$$

a) Für welches β hat der Kanal maximale Kapazität?

b) Für welches $H(X)$ wird bei gegebener Wahrscheinlichkeitsverteilung β der Wert von $H(Y)$ maximal?

Aufgabe

Gegeben sei folgender binärer, asymetrischer Kanal über den Alphabeten $\mathcal{X} = \mathcal{Y} = \{0, 1\}$:

$$\begin{array}{cc} P(0|0) = 1 - \beta & P(1|0) = \beta \\ P(0|1) = 0 & P(1|1) = 1 \end{array}$$

a) Für welches β hat der Kanal maximale Kapazität?

b) Für welches $H(X)$ wird bei gegebener Wahrscheinlichkeitsverteilung β der Wert von $H(Y)$ maximal?

c) Berechne Irrelevanz, Äquivokation und Transinformation für $\beta = 0.9$ und Gleichverteilung auf X.

Hamming-Code

Quellen

Pajor - Informatik 4 Tutorium SS2007

Prautzsch - Skript Informatik 4 SS2008

Ash: Information Theory. Dover 1990. ISBN 0-486-66521-6
http://www.ubka.uni-karlsruhe.de/hylib-bin/suche.cgi?opacdb=UBKA_OPAC&nd=9866904

Reflexion

Was haben wir heute gelernt?

Reflexion

Was haben wir heute gelernt?

- Übungsblatt 11 besprochen

Reflexion

Was haben wir heute gelernt?

- Übungsblatt 11 besprochen
- Grundbegriffe der Informationstheorie wiederholt

Reflexion

Was haben wir heute gelernt?

- Übungsblatt 11 besprochen
- Grundbegriffe der Informationstheorie wiederholt
- Übertragungskanal behandelt

Reflexion

Was haben wir heute gelernt?

- Übungsblatt 11 besprochen
- Grundbegriffe der Informationstheorie wiederholt
- Übertragungskanal behandelt
- Hammingcode

Noch Fragen?

Vorschau

Vorschau

- Klausurwiederholung, bitte konkrete Wünsche per Email!

Bis zum letzten Mal