

Informationstheorie – eine mathematische Theorie der Datenkompression und Datenübertragung

Erhard Aichinger

Institut für Algebra
Johannes Kepler Universität Linz

Tag der Mathematik, 23. November 2007, Johannes Kepler
Universität Linz

Outline

- 1 Ziele der Informations- und Codierungstheorie
- 2 Quellcodierung
- 3 Aufbereitung dieser Themen
- 4 Aufbereitung anderer Themen
- 5 Kanalcodierung

Ziele der Informations- und Codierungstheorie

Claude Elwood Shannon (1916 - 2001)

The fundamental problem of communication is that of reproducing at one point either exactly or approximately a message selected at another point.

Ziele der Informations- und Codierungstheorie

- Effizientes Darstellen einer Nachricht (Datenkompression)
- Zeitsparendes Schicken der Nachricht über einen Nachrichtenkanal
- Korrektur von Übertragungsfehlern

Ziele der Informations- und Codierungstheorie

Claude Elwood Shannon (1916 - 2001)

The fundamental problem of communication is that of reproducing at one point either exactly or approximately a message selected at another point.

Ziele der Informations- und Codierungstheorie

- Effizientes Darstellen einer Nachricht (Datenkompression)
- Zeitsparendes Schicken der Nachricht über einen Nachrichtenkanal
- Korrektur von Übertragungsfehlern

Ziele der Informations- und Codierungstheorie

Claude Elwood Shannon (1916 - 2001)

The fundamental problem of communication is that of reproducing at one point either exactly or approximately a message selected at another point.

Ziele der Informations- und Codierungstheorie

- Effizientes Darstellen einer Nachricht (Datenkompression)
- Zeitsparendes Schicken der Nachricht über einen Nachrichtenkanal
- Korrektur von Übertragungsfehlern

Ziele der Informations- und Codierungstheorie

Claude Elwood Shannon (1916 - 2001)

The fundamental problem of communication is that of reproducing at one point either exactly or approximately a message selected at another point.

Ziele der Informations- und Codierungstheorie

- Effizientes Darstellen einer Nachricht (Datenkompression)
- Zeitsparendes Schicken der Nachricht über einen Nachrichtenkanal
- Korrektur von Übertragungsfehlern

Ziele der Informations- und Codierungstheorie

Claude Elwood Shannon (1916 - 2001)

The fundamental problem of communication is that of reproducing at one point either exactly or approximately a message selected at another point.

Ziele der Informations- und Codierungstheorie

- Effizientes Darstellen einer Nachricht (Datenkompression)
- Zeitsparendes Schicken der Nachricht über einen Nachrichtenkanal
- Korrektur von Übertragungsfehlern

Ein Kommunikationssystem

Modell eines Kommunikationssystems

- Nachrichtenquelle
- Quellcodierer
- Kanalcodierer
- Kanal und Rauschen
- Kanaldecodierer
- Quelldecodierer
- Nachrichtensenke

Ein Kommunikationssystem

Modell eines Kommunikationssystems

- **Nachrichtenquelle**
- Quellcodierer
- Kanalcodierer
- Kanal und Rauschen
- Kanaldecodierer
- Quelldecodierer
- Nachrichtensenke

Ein Kommunikationssystem

Modell eines Kommunikationssystems

- Nachrichtenquelle
- Quellcodierer
- Kanalcodierer
- Kanal und Rauschen
- Kanaldecodierer
- Quelldecodierer
- Nachrichtensenke

Ein Kommunikationssystem

Modell eines Kommunikationssystems

- Nachrichtenquelle
- Quellcodierer
- Kanalcodierer
- Kanal und Rauschen
- Kanaldecodierer
- Quelldecodierer
- Nachrichtensenke

Ein Kommunikationssystem

Modell eines Kommunikationssystems

- Nachrichtenquelle
- Quellcodierer
- Kanalcodierer
- Kanal und Rauschen
- Kanaldecodierer
- Quelldecodierer
- Nachrichtensenke

Ein Kommunikationssystem

Modell eines Kommunikationssystems

- Nachrichtenquelle
- Quellcodierer
- Kanalcodierer
- Kanal und Rauschen
- Kanaldecodierer
- Quelldecodierer
- Nachrichtensenke

Ein Kommunikationssystem

Modell eines Kommunikationssystems

- Nachrichtenquelle
- Quellcodierer
- Kanalcodierer
- Kanal und Rauschen
- Kanaldecodierer
- Quelldecodierer
- Nachrichtensenke

Ein Kommunikationssystem

Modell eines Kommunikationssystems

- Nachrichtenquelle
- Quellcodierer
- Kanalcodierer
- Kanal und Rauschen
- Kanaldecodierer
- Quelldecodierer
- Nachrichtensenke

Quellcodierung

Ein Beispiel

Nachricht:

AAABAACAADBBAABAAAAABAAAAAABAADAAAAA . . .

- 60%A, 30%B, 5%C, 5%D.

Zeichenweise Codierung der Nachrichten als 0/1-Folgen

Zeichen	Vorschlag 1	Vorschlag 2	Vorschlag 3
<i>A</i>	00	0	0
<i>B</i>	01	10	10
<i>C</i>	10	110	110
<i>D</i>	11	01	111
	2	oje	1.5

Quellcodierung

Ein Beispiel

Nachricht:

AAABAACAADBBAABAAAAABAAAAAABAADAAAAA . . .

- 60%A, 30%B, 5%C, 5%D.

Zeichenweise Codierung der Nachrichten als 0/1-Folgen

Zeichen	Vorschlag 1	Vorschlag 2	Vorschlag 3
A	00	0	0
B	01	10	10
C	10	110	110
D	11	01	111
	2	oje	1.5

Quellcodierung

Ein Beispiel

Nachricht:

AAABAACAADBBAABAAAAABAAAAAABAADAAAAA . . .

- 60%A, 30%B, 5%C, 5%D.

Zeichenweise Codierung der Nachrichten als 0/1-Folgen

Zeichen	Vorschlag 1	Vorschlag 2	Vorschlag 3
A	00	0	0
B	01	10	10
C	10	110	110
D	11	01	111
	2	oje	1.5

Quellcodierung

Ziel der Quellcodierung

Ziel der Quellcodierung ist die Datenkompression.

Quellcodierung

Shannons Quellcodierungssatz - I

Wenn die Zeichen $A_1, A_2, \dots, A_n$ mit Wahrscheinlichkeiten $p_1, p_2, \dots, p_n$ auftreten, so braucht jedes Quellcodierungsverfahren, das für beliebig lange Dateien funktioniert, im Mittel zumindest

$$\sum_{i=1}^n p_i \cdot \log_2\left(\frac{1}{p_i}\right)$$

Bits pro Nachrichtenzeichen. Durch geeignete Codierungsverfahren kann man dieser Schranke beliebig nahe kommen. Für das obige Beispiel ist diese Schranke ungefähr 1.395 Bits pro Nachrichtenzeichen.

Die beste zeichenweise Codierung

Huffman-Algorithmus [Ash, 1990, p. 42], [MacKay, 2003, p.99]

Für gegebene Zeichen $A_1, A_2, \dots, A_n$ mit Wahrscheinlichkeiten $p_1, p_2, \dots, p_n$ produziert der Huffman-Algorithmus die beste zeichenweise Codierung von $A_1, A_2, \dots, A_n$ als 0/1-Folgen.

Unterlagen zur Informationstheorie

Aufbereitung der Informationstheorie

- Quellcodierung: Edith Lindenbauer, Diplomarbeit *Informationstheorie und Quellencodierung im Schulunterricht – Didaktische Aufbereitung der mathematischen Grundlagen*, 2005.
- Überblick, Quell- und Kanalcodierung: EA, Vorlesungsskriptum *Informations- und Codierungstheorie*, WS 06/07. pdf-Datei auf der Homepage.
- Die ganze Wahrheit: T.M. Cover, J.A. Thomas, *Elements of information theory*, Wiley, 2006.
- Die ganze Wahrheit und ein bisschen mehr: D.J.C. MacKay, *Information theory, inference and learning algorithms*, Cambridge UP, 2003. pdf-Datei öffentlich.

Unterlagen zur Informationstheorie

Aufbereitung der Informationstheorie

- Quellcodierung: Edith Lindenbauer, Diplomarbeit *Informationstheorie und Quellencodierung im Schulunterricht – Didaktische Aufbereitung der mathematischen Grundlagen*, 2005.
- Überblick, Quell- und Kanalcodierung: EA, Vorlesungsskriptum *Informations- und Codierungstheorie*, WS 06/07. pdf-Datei auf der Homepage.
- Die ganze Wahrheit: T.M. Cover, J.A. Thomas, *Elements of information theory*, Wiley, 2006.
- Die ganze Wahrheit und ein bisschen mehr: D.J.C. MacKay, *Information theory, inference and learning algorithms*, Cambridge UP, 2003. pdf-Datei öffentlich.

Unterlagen zur Informationstheorie

Aufbereitung der Informationstheorie

- Quellcodierung: Edith Lindenbauer, Diplomarbeit *Informationstheorie und Quellencodierung im Schulunterricht – Didaktische Aufbereitung der mathematischen Grundlagen*, 2005.
- Überblick, Quell- und Kanalcodierung: EA, Vorlesungsskriptum *Informations- und Codierungstheorie*, WS 06/07. pdf-Datei auf der Homepage.
- Die ganze Wahrheit: T.M. Cover, J.A. Thomas, *Elements of information theory*, Wiley, 2006.
- Die ganze Wahrheit und ein bisschen mehr: D.J.C. MacKay, *Information theory, inference and learning algorithms*, Cambridge UP, 2003. pdf-Datei öffentlich.

Unterlagen zur Informationstheorie

Aufbereitung der Informationstheorie

- Quellcodierung: Edith Lindenbauer, Diplomarbeit *Informationstheorie und Quellencodierung im Schulunterricht – Didaktische Aufbereitung der mathematischen Grundlagen*, 2005.
- Überblick, Quell- und Kanalcodierung: EA, Vorlesungsskriptum *Informations- und Codierungstheorie*, WS 06/07. pdf-Datei auf der Homepage.
- Die ganze Wahrheit: T.M. Cover, J.A. Thomas, *Elements of information theory*, Wiley, 2006.
- Die ganze Wahrheit und ein bisschen mehr: D.J.C. MacKay, *Information theory, inference and learning algorithms*, Cambridge UP, 2003. pdf-Datei öffentlich.

Unterlagen zur Informationstheorie

Aufbereitung der Informationstheorie

- Quellcodierung: Edith Lindenbauer, Diplomarbeit *Informationstheorie und Quellencodierung im Schulunterricht – Didaktische Aufbereitung der mathematischen Grundlagen*, 2005.
- Überblick, Quell- und Kanalcodierung: EA, Vorlesungsskriptum *Informations- und Codierungstheorie*, WS 06/07. pdf-Datei auf der Homepage.
- Die ganze Wahrheit: T.M. Cover, J.A. Thomas, *Elements of information theory*, Wiley, 2006.
- Die ganze Wahrheit und ein bisschen mehr: D.J.C. MacKay, *Information theory, inference and learning algorithms*, Cambridge UP, 2003. pdf-Datei öffentlich.

Aufbereitung anderer Themen

Aufbereitung anderer Themen

- Public-Key-Verschlüsselung: Angelika Gahleitner, Diplomarbeit *Das RSA-Verfahren im Schulunterricht – Didaktische Aufbereitung der mathematischen Grundlagen*, 2003.
- Formale Begriffsanalyse nach Wille: Elisabeth Steinmair, Diplomarbeit *Wissensverarbeitung durch Formale Begriffsanalyse – Theorie und Arbeitsblätter für den Unterricht*, 2002.
- Stefan Leitner, Diplomarbeit *Authentifikation und Identifikation mit Hilfe kryptographischer Algorithmen*, 2002.

Aufbereitung anderer Themen

Aufbereitung anderer Themen

- Public-Key-Verschlüsselung: Angelika Gahleitner, Diplomarbeit *Das RSA-Verfahren im Schulunterricht – Didaktische Aufbereitung der mathematischen Grundlagen*, 2003.
- Formale Begriffsanalyse nach Wille: Elisabeth Steinmair, Diplomarbeit *Wissensverarbeitung durch Formale Begriffsanalyse – Theorie und Arbeitsblätter für den Unterricht*, 2002.
- Stefan Leitner, Diplomarbeit *Authentifikation und Identifikation mit Hilfe kryptographischer Algorithmen*, 2002.

Aufbereitung anderer Themen

Aufbereitung anderer Themen

- Public-Key-Verschlüsselung: Angelika Gahleitner, Diplomarbeit *Das RSA-Verfahren im Schulunterricht – Didaktische Aufbereitung der mathematischen Grundlagen*, 2003.
- Formale Begriffsanalyse nach Wille: Elisabeth Steinmair, Diplomarbeit *Wissensverarbeitung durch Formale Begriffsanalyse – Theorie und Arbeitsblätter für den Unterricht*, 2002.
- Stefan Leitner, Diplomarbeit *Authentifikation und Identifikation mit Hilfe kryptographischer Algorithmen*, 2002.

Aufbereitung anderer Themen

Aufbereitung anderer Themen

- Public-Key-Verschlüsselung: Angelika Gahleitner, Diplomarbeit *Das RSA-Verfahren im Schulunterricht – Didaktische Aufbereitung der mathematischen Grundlagen*, 2003.
- Formale Begriffsanalyse nach Wille: Elisabeth Steinmair, Diplomarbeit *Wissensverarbeitung durch Formale Begriffsanalyse – Theorie und Arbeitsblätter für den Unterricht*, 2002.
- Stefan Leitner, Diplomarbeit *Authentifikation und Identifikation mit Hilfe kryptographischer Algorithmen*, 2002.

Kanalcodierung

Binärer symmetrischer Kanal

Der binäre symmetrische Kanal überträgt pro Durchgang ein Bit. Jedes Bit wird mit Wahrscheinlichkeit $1 - f$ richtig übertragen. (f ist die **Fehlerwahrscheinlichkeit** des Kanals).

Beispiel für Kanalkodierung

Beispiel für Kanalkodierung

- 1 Wir wollen die Bitfolge $x_1x_2x_3x_4 \dots$ übertragen.
- 2 Der **Kanalcodierer** fügt Kontrollstellen dazu und transformiert $x_1x_2x_3x_4 \dots$ zu $y_1y_2y_3y_4y_5y_6 \dots$
- 3 $y_1y_2y_3y_4y_5y_6 \dots$ wird über den Kanal gesendet. Die Folge $z_1z_2z_3z_4z_5z_6 \dots$ kommt an.
- 4 Der **Kanaldecodierer** versucht jene Folge $x_1x_2x_3x_4 \dots$ zu finden, die am wahrscheinlichsten gesendet wurde. Er produziert eine Folge $u_1u_2u_3u_4 \dots$

Beispiel für Kanalkodierung

Beispiel für Kanalkodierung

- 1 Wir wollen die Bitfolge $x_1x_2x_3x_4 \dots$ übertragen.
- 2 Der **Kanalcodierer** fügt Kontrollstellen dazu und transformiert $x_1x_2x_3x_4 \dots$ zu $y_1y_2y_3y_4y_5y_6 \dots$
- 3 $y_1y_2y_3y_4y_5y_6 \dots$ wird über den Kanal gesendet. Die Folge $z_1z_2z_3z_4z_5z_6 \dots$ kommt an.
- 4 Der **Kanaldecodierer** versucht jene Folge $x_1x_2x_3x_4 \dots$ zu finden, die am wahrscheinlichsten gesendet wurde. Er produziert eine Folge $u_1u_2u_3u_4 \dots$

Beispiel für Kanalkodierung

Beispiel für Kanalkodierung

- 1 Wir wollen die Bitfolge $x_1x_2x_3x_4 \dots$ übertragen.
- 2 Der **Kanalcodierer** fügt Kontrollstellen dazu und transformiert $x_1x_2x_3x_4 \dots$ zu $y_1y_2y_3y_4y_5y_6 \dots$
- 3 $y_1y_2y_3y_4y_5y_6 \dots$ wird über den Kanal gesendet. Die Folge $z_1z_2z_3z_4z_5z_6 \dots$ kommt an.
- 4 Der **Kanaldecodierer** versucht jene Folge $x_1x_2x_3x_4 \dots$ zu finden, die am wahrscheinlichsten gesendet wurde. Er produziert eine Folge $u_1u_2u_3u_4 \dots$

Beispiel für Kanalkodierung

Beispiel für Kanalkodierung

- 1 Wir wollen die Bitfolge $x_1x_2x_3x_4 \dots$ übertragen.
- 2 Der **Kanalcodierer** fügt Kontrollstellen dazu und transformiert $x_1x_2x_3x_4 \dots$ zu $y_1y_2y_3y_4y_5y_6 \dots$
- 3 $y_1y_2y_3y_4y_5y_6 \dots$ wird über den Kanal gesendet. Die Folge $z_1z_2z_3z_4z_5z_6 \dots$ kommt an.
- 4 Der **Kanaldecodierer** versucht jene Folge $x_1x_2x_3x_4 \dots$ zu finden, die am wahrscheinlichsten gesendet wurde. Er produziert eine Folge $u_1u_2u_3u_4 \dots$

Beispiel für Kanalkodierung

Beispiel für Kanalkodierung

- 1 Wir wollen die Bitfolge $x_1x_2x_3x_4 \dots$ übertragen.
- 2 Der **Kanalcodierer** fügt Kontrollstellen dazu und transformiert $x_1x_2x_3x_4 \dots$ zu $y_1y_2y_3y_4y_5y_6 \dots$
- 3 $y_1y_2y_3y_4y_5y_6 \dots$ wird über den Kanal gesendet. Die Folge $z_1z_2z_3z_4z_5z_6 \dots$ kommt an.
- 4 Der **Kanaldecodierer** versucht jene Folge $x_1x_2x_3x_4 \dots$ zu finden, die am wahrscheinlichsten gesendet wurde. Er produziert eine Folge $u_1u_2u_3u_4 \dots$

Bitfehlerrate und Übertragungsrate

Definition (Bitfehlerrate)

Die **mittlere Bitfehlerrate** b dieser Prozedur ist die Wahrscheinlichkeit dafür, dass $x_i \neq u_i$.

Definition (Übertragungsrate)

Die **Übertragungsrate** r ist die Anzahl der Quellbits pro gesendetem Kanalbit.

Bitfehlerrate und Übertragungsrate

Definition (Bitfehlerrate)

Die **mittlere Bitfehlerrate** b dieser Prozedur ist die Wahrscheinlichkeit dafür, dass $x_i \neq u_i$.

Definition (Übertragungsrate)

Die **Übertragungsrate** r ist die Anzahl der Quellbits pro gesendetem Kanalbit.

Shannons Kanalkodierungssatz

Die Frage

Wir haben einen Kanal mit Fehlerrate f , und eine Übertragungsrate r vorgegeben. Welche Bitfehlerrate können wir bei Verwendung dieses Kanals mit Übertragungsrate r bestenfalls erreichen?

Shannons Kanalcodierungssatz

Theorem (Shannons Kanalcodierungssatz)

Sei C der binäre symmetrische Kanal mit Fehlerrate f .

- 1 Wenn die Übertragungsrate r die Ungleichung

$$r < 1 + f \cdot \log_2(f) + (1 - f) \cdot \log_2(1 - f),$$

erfüllt, und $\varepsilon > 0$ gilt, dann gibt es eine Übertragungsprozedur mit Übertragungsrate r , sodass die Bitfehlerrate $< \varepsilon$ ist.

- 2 Wenn $r > 1 + f \cdot \log_2(f) + (1 - f) \cdot \log_2(1 - f)$, dann gibt es ein $b > 0$, sodass die Bitfehlerrate jedes Übertragungssystems mit Rate r zumindest b ist.

Shannons Kanalcodierungssatz

Theorem (Shannons Kanalcodierungssatz)

Sei C der binäre symmetrische Kanal mit Fehlerrate f .

- 1 Wenn die Übertragungsrate r die Ungleichung

$$r < 1 + f \cdot \log_2(f) + (1 - f) \cdot \log_2(1 - f),$$

erfüllt, und $\varepsilon > 0$ gilt, dann gibt es eine Übertragungsprozedur mit Übertragungsrate r , sodass die Bitfehlerrate $< \varepsilon$ ist.

- 2 Wenn $r > 1 + f \cdot \log_2(f) + (1 - f) \cdot \log_2(1 - f)$, dann gibt es ein $b > 0$, sodass die Bitfehlerrate jedes Übertragungssystems mit Rate r zumindest b ist.

Shannons Kanalcodierungssatz

Theorem (Shannons Kanalcodierungssatz)

Sei C der binäre symmetrische Kanal mit Fehlerrate f .

- ① Wenn die Übertragungsrate r die Ungleichung

$$r < 1 + f \cdot \log_2(f) + (1 - f) \cdot \log_2(1 - f),$$

erfüllt, und $\varepsilon > 0$ gilt, dann gibt es eine Übertragungsprozedur mit Übertragungsrate r , sodass die Bitfehlerrate $< \varepsilon$ ist.

- ② Wenn $r > 1 + f \cdot \log_2(f) + (1 - f) \cdot \log_2(1 - f)$, dann gibt es ein $b > 0$, sodass die Bitfehlerrate jedes Übertragungssystems mit Rate r zumindest b ist.

Recommended Literature

- R. B. Ash. *Information theory*. Dover Publications Inc., New York, 1990. Corrected reprint of the 1965 original.
- T. M. Cover and J. A. Thomas. *Elements of information theory*. Wiley-Interscience [John Wiley & Sons], Hoboken, NJ, second edition, 2006.
- D. J. C. MacKay. *Information theory, inference and learning algorithms*. Cambridge University Press, New York, 2003.
The book can be viewed at
<http://www.inference.phy.cam.ac.uk/mackay/itprnn/book.html> .

Recommended Literature

- R. B. Ash. *Information theory*. Dover Publications Inc., New York, 1990. Corrected reprint of the 1965 original.
- T. M. Cover and J. A. Thomas. *Elements of information theory*. Wiley-Interscience [John Wiley & Sons], Hoboken, NJ, second edition, 2006.
- D. J. C. MacKay. *Information theory, inference and learning algorithms*. Cambridge University Press, New York, 2003.
The book can be viewed at
<http://www.inference.phy.cam.ac.uk/mackay/itprnn/book.html> .

Recommended Literature

- R. B. Ash. *Information theory*. Dover Publications Inc., New York, 1990. Corrected reprint of the 1965 original.
- T. M. Cover and J. A. Thomas. *Elements of information theory*. Wiley-Interscience [John Wiley & Sons], Hoboken, NJ, second edition, 2006.
- D. J. C. MacKay. *Information theory, inference and learning algorithms*. Cambridge University Press, New York, 2003.
The book can be viewed at
<http://www.inference.phy.cam.ac.uk/mackay/itprnn/book.html> .



Ash, R. B. (1990).

Information theory.

Dover Publications Inc., New York.

Corrected reprint of the 1965 original.



MacKay, D. J. C. (2003).

Information theory, inference and learning algorithms.

Cambridge University Press, New York.

The book can be viewed at

<http://www.inference.phy.cam.ac.uk/mackay/itprnn>