

Vorlesung WS 2014/2015

Ruhr-Universität Bochum

Algebraische Codierung für die sichere Datenübertragung

Dr.-Ing. Klaus Huber
Berlin

coding@klaus-huber.net

Die wichtigsten Bücher

E.Berlekamp: Algebraic Coding Theory,
Aegean Park Press, 1968/1984

Peterson, Weldon: Error-Correcting Codes,
MIT Press, second Edition 1972

MacWilliams, Sloane: The Theory of Error Correcting Codes, North
Holland 1977

Blahut: Theory and Practice of Error Control Codes,
Addison Wesley 1984

Pless, Huffman: Handbook of Coding Theory I, II,
North Holland 1998

McEliece: The Theory of Information and Coding,
Cambridge, 1977

Übersicht und Einführung

Grundlagen

Die wichtigsten Codeklassen

Decodierverfahren für die Hammingmetrik

Codes für andere Metriken

Das Kryptosystem von McEliece

Die MacWilliams Transformation

Übersicht und Einführung

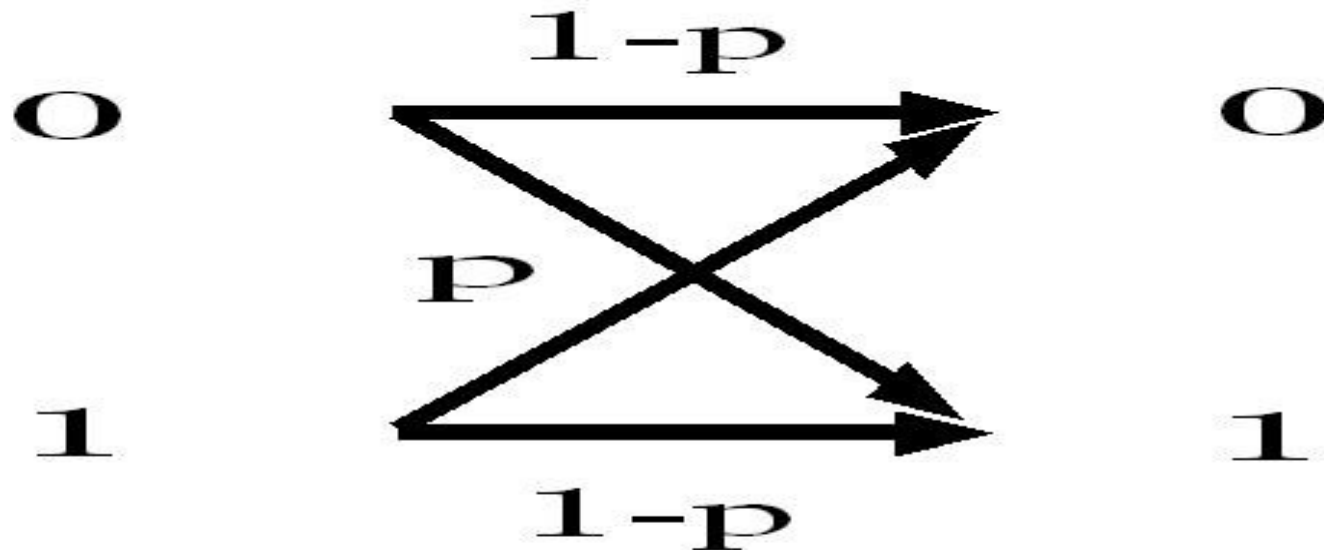


Kanalkapazität

Charakteristischer Parameter eines Kanals. Die **Kanalkapazität** gibt an mit welcher Datenrate man prinzipiell fehlerfrei (d.h. mit Fehlerwahrscheinlichkeit Null) Daten übertragen kann.

Die Kanalkapazität ist eine Obergrenze für das prinzipiell mit – Codierung - erreichbare. Sie geht auf Claude Shannon zurück. Bei Datenraten oberhalb der Kanalkapazität ist eine fehlerfreie Datenübertragung nicht möglich.

Beispiel: Binärer symmetrischer Kanal (BSC)



$$C = 1 + p \lg p + (1-p) \lg (1-p)$$

Beispiel: Bandbegrenzter Kanal mit Gaußschem weißen Rauschen

$$C = W \log \left(1 + \frac{S}{N} \right)$$

W: Bandbreite

S : Signalleistung

N: Rauschleistung

(AWGN-Kanal: Additive white Gaussian noise - channel)

Algebraische Codierung für die sichere Datenübertragung, K.Huber

Originalarbeiten zu speziellen Themen der Vorlesung

- V.D.Goppa, "A New Class of Linear Error-Correcting Codes", Probl. Peredach. Inform. Vol.6, No.3, pp. 24-30, 1970.
- E.R.Berlekamp, "Goppa Codes", IEEE Transactions on Information Theory, No.5, pp.590-592, 1973.
- Y.Sugiyama, M.Kasahara, S.Hirasawa, T.Namekawa, "A Method for Solving Key Equation for Decoding Goppa Codes", Information and Control, 27, 87-99, 1975.
- N.J.Patterson, "The Algebraic Decoding of Goppa Codes", IEEE Trans. on Inf. Theory, Vol.IT-21, No.2, March 1975, pp.203-207.
- K.Huber, "Note on Decoding Binary Goppa Codes", Electronics Letters, 18th January 1996, Vol. 32 No.2, pp. 102-103 (sowie verallgemeinert: K.Huber, "Taking p th roots modulo polynomials over finite fields", Designs, Codes and Cryptography, 28, pp. 303-311, 2003).
- R.Roth, "Introduction to Coding Theory", Cambridge University Press, 2006. (Chapter 10: Lee Metric)
- K.Huber, "Codes over Gaussian Integers", IEEE Transactions on Information Theory, Vol.40, No.1, pp. 207-216, 1994.