

Proseminar im Sommersemester 2023: Codierungstheorie

Die Codierungstheorie betrachtet mathematische Konzepte und Verfahren zur Fehlersicherung bei der Übertragung von Nachrichten über durch Rauschen oder andere Einflüsse gestörte Kanäle. Die zu übertragende Information soll zum einen möglichst sparsam, also mit geringer Redundanz, übertragen werden. Zum anderen wird ein gewisses Maß an Redundanz bewusst in Kauf genommen, um etwaige Übertragungsfehler erkennen und gegebenenfalls korrigieren zu können. Die Codierungstheorie stellt Verfahren bereit, um die sich daraus ergebenden gegensätzlichen Anforderungen hinsichtlich Effizienz und Fehlerschutz miteinander in Einklang zu bringen.

Beispiel: Durch Anhängen eines „Paritätsbits“

$$(1, 1, 0, 0, 1) \in \mathbb{F}_2^5 \quad \rightsquigarrow \quad (1, 1, 0, 0, 1, 1) \in \mathbb{F}_2^6$$

lässt sich erkennen, ob, aber nicht an welcher Stelle, eine ungerade Anzahl (hier ein, drei oder fünf) von Übertragungsfehlern aufgetreten ist.

Die Codierungstheorie findet Anwendung in praktisch allen Bereichen der digitalen Informationsverarbeitung. Einige ausgewählte Anwendungsfelder, etwa bei QR-Codes, werden wir in diesem Proseminar kennenlernen.

Themenauswahl (zu jedem Themenblock sind ggf. mehrere Vorträge möglich):

- Grundlagen der Informationstheorie: Informationsgehalt, Entropie, Kanalkapazität, Shannons Kanalcodierungssatz
- Lineare Codes: endliche Körper, Erzeuger- und Prüfmatrixen, Syndromdecodierung, Singleton- und Kugelpackungsschranke
- Familien von linearen Codes: Hamming-, Golay-, und Reed-Solomon-Codes
- Zyklische Codes: Polynome über endlichen Körpern, Erzeuger- und Syndrompolynom, BCH-Schranke
- Low-Density-Parity-Check-Codes: Konstruktion von LDPC-Codes aus Graphen und *belief propagation*-Algorithmus
- Faltungscodes: Trellis-Diagramm, Viterbi-Algorithmus, Turbocodes

Literatur:

- [Man] O. Manz, Fehlerkorrigierende Codes. Konstruieren, Anwenden, Decodieren. Springer Vieweg, Wiesbaden (2017)

- [Roh] H. Rohling, Einführung in die Informations- und Codierungstheorie. Teubner Studienbücher Elektrotechnik. B. G. Teubner, Stuttgart (1995)
- [Rom] S. Roman, Coding and Information Theory. Graduate Texts in Mathematics **134**, Springer-Verlag Berlin, Heidelberg, New York (1992)
- [vLi] J. H. van Lint, Introduction to Coding Theory. Third Revised and Expanded Edition. Graduate Texts in Mathematics **86**, Springer-Verlag Berlin, Heidelberg (1998)

Organisatorische Hinweise:

Das Proseminar richtet sich an Studentinnen und Studenten in allen Bachelorstudiengängen der Mathematik und Informatik. Die erforderlichen Vorkenntnisse beschränken sich auf den Inhalt der Vorlesung Lineare Algebra I. Grundlagenkenntnisse aus der Algebra (z.B. endliche Körper, Polynomringe) sind hilfreich, werden aber nicht zwingend vorausgesetzt, sondern, soweit für das Thema erforderlich, im Proseminar erarbeitet.

Die Seminarvorträge können auf Deutsch oder auf Englisch gehalten werden. Jeder Vortrag soll in einer kurzen Ausarbeitung zusammengefasst werden.

Das Seminar findet ab 05.05.2023 i.d.R. **14-tägig freitags** von **14-17 Uhr** (c.t.) statt. Der Raum wird noch bekannt gegeben. Eine **Vorbesprechung** mit Vergabe der Vortragsthemen erfolgt per Videokonferenz nach individueller Vereinbarung mit den Teilnehmerinnen und Teilnehmern.

Die **Anmeldung** ist ab sofort über MÜSLI möglich (bitte zusätzliche Nachricht per Email an SWOBODA@MATHI.UNI-HEIDELBERG.DE). Bei Fragen können Sie sich gerne unter dieser Adresse an mich wenden.

