Dr. Th. Bouganis

Algebraische Codierungstheorie

Spezialvorlesung WS 2010-2011

Ort: INF288 HS 5 **Zeit:** Mi 14.00-16.00 Uhr **s.t.** **Beginn:** 13.10.2010

Motivation, das Problem der Codierungstheorie: (aus Prof. Matzats Buch [3]) Das Übertragen von (binären) Informationen über Telefonleitungen, Funk oder Satelliten verläuft oft nicht ungestört, da diese Informationen durch äußere Einflüsse wie schlechtes Wetter möglicherweise zerstört oder verändert werden. Auch das Auslesen von Speichermedien ist sehr fehleranfällig, da viele Bits durch hohe Auslesengeschwindigkeit oder diversen Verunreiningungen der Disketten verloren gehen können. Abhilfe dagegen verschafft man sich durch Einbau von Redundanzen, die mehrere Fehler auffangen können. Das Erweitern der Information mit Redundanzen nennt man *Codierung*, die Rückübersetzung der emfangenen Nachricht in den Klartext *Decodierung*.

Inhalt der Vorlesung: Algebraische Codierungstheorie stellt die Synthese aus Codierungstheorie und Algebra (oder sogar algebraischer Geometrie) dar. In der Tat kann man mit Hilfe von Methoden aus der Algebra sehr effiziente Codes definieren. In dieser Vorlesung werden wir wichtige Begriffe der algebraischen Codierungstheorie wie z.B lineare Codes, Dual Codes oder Schranken von Codes kennenlernen und interessante Beispiele (Reed-Solomon, Reed-Muller, elliptische Codes) betrachten. Als Hauptziel dieser Vorlesung setzen wir uns eine wichtige Klasse von Codes, die sogenannte Goppa-Codes oder algebraische geometriesche Codes zu definieren und ihre Eigenschaften zu studieren.

Im Laufe des Seminars sollen folgende Themen behandelt werden:

1. Einführung in die Codierungstheorie, Beschreibung des Hauptproblems und Motivation,
2. Definition von linearen Codes, Duale Codes und das Gewichtspolynom,
3. Pseudorationale Codes, Reed-Solomon Codes, Decodierung von Reed-Solomon Codes
4. Variationen von Codes (z.B. Direkte Summe, Verklebung, Tensorprodukt), Teilkörper-Codes,
5. Gruppen-Codes: Reed-Muller Codes,
6. Schranken für Codes: Singleton- und Plotkin-Schranke, Hamming- und Elias-Schranke und Gilbert-Varshomov Schranke,

7. Einführung in die Theorie der algebraischen Funktionenkörper (Primdivisoren, Bewertungsringe, das Geschlecht eines Funktionenkörpers),
8. Der Satz von Riemann-Roch,
9. Definition von Geometrischen Goppa Codes (Algebraiche Geometrische Codes), Berechnung der Dimension und Minimaldistanz mit Hilfe des Satzes von Riemann-Roch
10. Beispiele von Goppa-Codes: Rationale, Elliptische und Hyperelliptische Codes,
11. Decodierung von Goppa-Codes.

Fragen: Bei Thanasis Bouganis (Zi. 221, INF 288, email: bouganis@mathi.uni-heidelberg.de)

Literatur:

[1] J.H. van Lint, *Introduction to Coding Theory,* Graduate Texts in Mathematics 86, Springer 1986

[2] J.H. van Lint, G. van der Geer, *Introduction to Coding Theory and Algebraic Geometry,* DMV Seminar vol 12, Birkhäuser, Basel 1988

[3] B. Matzat, *Codierungtheorie,* Ausarbeitung von Th. Lagemann, IWR, Universität Heidelberg, 2007

[4] H. Stichtenoth, *Algebraic Function Fields and Codes,* Universitext, Springer-Verlag, 1993

Vorkenntnisse: Elementare Algebra.