Université
franco-allemande
Deutsch-Französische
Hochschule

ZUSAMMENFASSUNG:

Die Codierungstheorie beschäftigt sich mit fehlererkennenden und -korrigierenden Codes, welche bei der Speicherung (z.B. auf CDs und DVDs oder Flash-Memories) und bei der ¨Übertragung von digitalen Daten zum Schutz gegen auftretende Fehler angewandt werden. Viele Grundlagen der Codierungstheorie entstammen der Algebra. Neben mathematischen Methoden werden auch Techniken der Informatik und Elektrotechnik verwendet.

Meine Dissertation umfasst zwei Themenbereiche der algebraische Codierungstheorie. Der erste Teil ist der effiziente Decodierung (mit und ohne Kanalzustandsinformationen) von verallgemeinerten Reed–Solomon Codes über endlichen Körpern in Hamming-Metrik gewidmet. Die Motivation für dieses mehr als 50 Jahre alte Problem wurde durch die Entdeckung eines interpolationsbasierten Decodierprinzips mit polynomieller Laufzeit bis zum Johnson- Radius durch Guruswami und Sudan am Ende des 20. Jahrhunderts erneuert. Die ersten syndrombasierten Fehler- und Auslöschungs-Decodieralgorithmen von Berlekamp–Massey und Sugiyama–Kasahara–Hirasawa–Namekawa für verallgemeinerte Reed–Solomon Codes werden durch eine Schlüsselgleichung, d.h., eine algebraische Darstellung des Decodierproblems, ausgedrückt. Die Beschreibung des neuen interpolationsbasierten Verfahren durch Schlüsselgleichungen ist ein zentraler Bestandteil dieser Dissertation. Die Darstellung beinhaltet zahlreiche Aspekte von Schlüsselgleichungen für die Decodierung von verallgemeinerte Reed–Solomon Codes ohne Kanalzustandsinformationen (Guruswami–Sudan Prinzip) als auch für die Decodierung unter Berücksichtigung der Kanalzustandsinformationen (Kötter–Vardy Prinzip). Das hergeleitete homogene Gleichungssystem ist strukturiert und ein effizienter Decodieralgorithmus wurde entwickelt.

Der zweite Themenbereich der Dissertation beinhaltet neue untere Schranken für die minimale Hamming-Distanz von linearen zyklischen Block-Codes ¨über endlichen Körpern und Decodierverfahren bis zu diesen Schranken. Ein Kernkonzept ist hierbei die Einbettung des gegebenen zyklischen Codes in einen zyklischen (verketteten) Produkt-Code, weshalb deren Grundlagen ausführlich beschrieben werden. Wir definieren zyklische verkettete Produkt-Codes und zeigen wie diese zur Herleitung von unteren Schranken genutzt werden können. Notwendige und hinreichende Bedingungen für niederratige nicht-primitive binäre zyklische Codes mit Mindestdistanz zwei und drei werden hergeleitet und ihre Bedeutung für die Einbettungs-Technik werden beschrieben. Des Weiteren entwickeln wir syndrombasierte Fehler- und Auslöschung- Decodieralgorithmen mit quadratischer Laufzeit, die in der Lage sind, bis zu den neuen hergeleiteten Schranken zu decodieren.