Karlsruher Institut für Technologie

Fakultät für Mathematik
Institut für Algebra und Geometrie
Prof. Dr. Frank Herrlich
Verena Möhler

Programm für das Proseminar
CODIERUNGSTHEORIE
im Sommersemester 2018
Donnerstag, 09:45-11:15, Seminarraum -1.009

Hauptquelle für die Vorträge ist das Buch von Willems [1]. Sie dürfen vor allem in einem Punkt ausgesprochen gerne von der Vorlage abweichen: Bitte verwenden Sie den Plural „Codewörter" anstelle des in [1] verwendeten „Codeworte".

Das Buch von Lütkebohmert [2] ist zwar nur in Vortrag 8 als explizite Quelle angegeben, kann aber für viele weitere Vorträge als ergänzende Literatur genutzt werden.

Teil 1: Einführung und lineare Codes

1. Grundbegriffe und erste Beispiele ([1] 1.1 bis Bsp. 1.1.17)
19.4., Raphaela Vana
Wir machen uns mit der Problemstellung und den Begrifflichkeiten der Codierungstheorie vertraut und sehen erste Beispiele für Codes.

2. Schranken für Codes und Lineare Codes I ([1] Def. 1.1.18 bis Bsp. 1.2.9)
26.4., Annika Schütz
Wir lernen Schranken an die Parameter von Codes kennen und beginnen mit dem Studium der linearen Codes, die uns in unserem Proseminar sehr viel beschäftigen werden.

3. Lineare Codes II ([1] Bsp. 1.2.10 und Def. 1.2.15 bis Bsp. 1.2.24)
3.5., Luisa Gebhardt
Wir lernen die Reed-Solomon-Codes kennen und betrachten Isometrien von Codes. Wir gehen auf das Problem der Fehlerbündel ein und betrachten als Beispiel die Codierung, die bei Audio-CDs verwendet wird.

4. Lineare Codes III ([1] Lemma 1.2.12 bis Bem. 1.2.14 und Def. 1.2.25 bis Ende 1.2)
17.5., Jonas Welsch
Wir lernen die Reed-Muller-Codes kennen und zeigen zwei weitere Schranken speziell für lineare Codes. Die Griesmer-Schranke wird von bestimmten Reed-Muller-Codes erreicht.

Teil 2: Algebraische Grundlagen

Für mehr Informationen zu einem Vortrag aus diesem Teil oder für eine andere Darstellung der Thematik können Sie gerne ein Algebra-Buch Ihrer Wahl zu Rate ziehen, z. B. das von Bosch [3].

5. Gruppenaktionen und abelsche Gruppen ([3] 5.1 und [1] 2.1)
24.5., Theresa Meier
Wir erhalten eine kurze Übersicht über Gruppenaktionen und klassifizieren dann die zyklischen sowie die endlichen abelschen Gruppen.

6. Endliche Körper ([1] 2.2 bis Def. 2.2.16)
7.6., Lena Biehl
Wir erweitern unser Wissen über endliche Körper und zeigen insbesondere, dass es zu jeder Primzahlpotenz $q = p^n$ genau einen Körper mit q Elementen gibt.

7. Galoistheorie endlicher Körper ([1] Def. 2.2.17 bis Ende 2.2)
14.6., Miriam Goetze
Wir zeigen den Hauptsatz der Galois-Theorie im Rahmen von endlichen Körpern und lernen Eigenschaften der Spurabbildung und primitive Einheitswurzeln kennen.

Teil 3: Wichtige Klassen von Codes

8. Dualität ([1] 3.1 (ohne Satz 3.1.8) und 3.2 bis Satz 3.2.2 / [2] Satz 1.4.5)
21.6., Sebastian Anhalt
Wir beschäftigen uns mit dem Konzept der Dualität, das auch in der Codierungstheorie ein wichtiges Hilfsmittel ist. Insbesondere betrachten wir Zusammenhänge zwischen einem Code und seinem dualen Code.

9. Unterkörper-Teilcodes ([1] 4.2)
28.6., Michael Zündorf
Wir wenden unser Wissen über endliche Körper an und lernen Unterkörper-Teilcodes kennen. Beispielsweise sind Hamming-Codes Unterkörper-Teilcodes von verallgemeinerten Reed-Solomon-Codes.

10. Zyklische Codes ([1] 6.1)
5.7., Janina Krüger
Wir erhalten mehr algebraische Struktur für unsere Codes, indem wir Codewörter als (Restklassen von) Polynome(n) auffassen. Zyklische Codes besitzen ein besonders schönes Erzeugerpolynom (die Idempotente) und können Fehlerbündel gut erkennen.

11. BCH-Codes ([1] 6.2)
12.7., Erik Genze
Wir lernen eine wichtige Klasse zyklischer Codes, die BCH-Codes, kennen und berechnen ihre Minimaldistanz.

Teil 4: Decodierung

12. Decodierung ([1] 9.1 und 9.2)
19.7., Freya Ebert
Wir lernen zwei Verfahren zur Decodierung kennen, den Peterson-Gorenstein-Zierler-Decodierer und ein Verfahren, das auf dem euklidischen Algorithmus basiert.

Literatur

[1] W. Willems. *Codierungstheorie*. De Gruyter 1999.

[2] W. Lütkebohmert. *Codierungstheorie*. Vieweg 2003.

[3] S. Bosch. *Algebra*. Springer 2009.