Programm des Seminar
CODIERUNGSTHEORIE
im Wintersemester 2019/20
Montage 14.10.2019 bis 27.01.2020,
Zeit: 12:00 bis 14:00, **Seminarraum:** D.13.11

Die Haupttext für die Vorträge ist Teil I des Buch von Willems.

1. Grundbegriffe und Beispiele ([1] Abschnitt 1) 21.10.19 und 28.10.19

1. Beispiele: Paritätscheck-Code und Wiederholungscode ([1] S. 4 (a), (b))
2. Definition: Code, Codewort, Hamming-Abstand ([1] S. 5)
3. Lemma: ([1] S. 5)
4. Definition: q -när symmetrische Kanäle ([1] S. 6)
5. Bemerkung: Die ML-Decodierung ([1] S. 6, 7).
6. Definition: Minimaldistanz, (n, M, d) -Code, Kugeln, perfekt, t -fehlererkennend, t -fehlerkorrigierend ([1] S. 8, 9, 12)
7. Satz: Hamming- und Singleton-Schranke([1] S. 12, 14)
8. Definition: MDS-Codes ([1] S. 14)
9. Beispiel ([1] S. 13)

2. Lineare Codes ([1] Abschnitt 2) 21.10.19 und 28.10.19

1. Definition: Lineare Codes, $[n, k, d]$ -Code über K ([1] S. 16)
2. Beispiel: ([1] S. 16)
3. Definition: Gewichtsfunktion, Minimalgewicht ([1] S. 16)
4. Lemma: $d(C) = wt(C)$ ([1] S. 16)
5. Definition: Erzeuger- und Kontrollmatrizen ([1] S. 17)
6. Beispiel: ([1] S. 17)
7. Satz: $d(C)$ kann mittels einer Kontrollmatrix berechnet sein([1] S. 18)
8. Definition: monomiale Matrizen, äquivalente Codes ([1] S. 25)
9. Satz: ([1] Aufgabe 11 S. 25)
10. Bemerkung: Die Syndrom-Decodierung ([1] S. 18)

3. Körper und der Polynomring ([1] Abschnitt 22) 4.11.19 und 11.11.19

1. Definition: Gruppe, Ring, Körper, Charakteristik ([1] S. 125)
2. Lemma: Charakteristik ist entweder 0 oder eine Primzahl ([1] S. 125)
3. Satz: K endlicher Körper. Dann gilt $|K| = p^n$ für eine Primzahl p . ([1] S. 125)
4. Satz: Die multiplikative Gruppe eines endlichen Körper ist zyklisch. ([1] S. 126)
5. Definition: $K[x]$, Grad, irreduzibel, Quotient $K[x]/(fK[x])$. ([1] S. 126)
6. Satz: f irreduzibel $\implies K[x]/(fK[x])$ ist ein Körper ([1] S. 127)
7. Beispiel: $\mathbb{R}[x]/((x^2 + 1)\mathbb{R}[x]) \cong \mathbb{C}$
8. Satz (ohne Beweis): $|K| = p^n$. Dann ist K isomorph zum Körper $\mathbb{Z}_p[x]/(f\mathbb{Z}_p[x])$. ([1] S. 128)

4. Duale Codes ([1] Abschnitt 5) 18.11.19

1. Erinnerung: Definition symmetrische, nicht ausgeartete K -Bilinearform.
2. Bemerkung: $\langle v, v \rangle = 0$ für $v \neq 0$, wenn K^n nicht euklidisch. z.B $v = (1, 1) \in \mathbb{F}_2^2$ ([1] S. 36)
3. Definition: dualer Code und selbstdual ([1] S. 36)
4. Lemma: Für V eine Untervektorraum in K^n , gilt $\dim_K(V^\perp) = n - \dim_K(V)$ und $(V^\perp)^\perp = V$. (Aufgabe 26 S. 40)
5. Satz: ([1] S. 36)
6. Satz: Der duale Code eines MDS-Code ist auch ein MDS-Code ([1] Aufgabe 32 S. 41)
7. Beispiel: binärer Golay-Code ([1] S. 39)
8. Definition: r -dividierbar ([1] S. 37)
9. Lemma: Dividierbarkeitslemma ([1] S. 38)
10. Lemma: ([1] Aufgabe 27 S. 41)

5. Besondere Codes ([1] 4.11.19 und 11.11.19

1. Beispiel: Hamming-Codes ([1] S. 19)
2. Definition: Simplex-Codes ([1] S. 37).
3. Lemma: Parameter-Simplex-Codes und Gewichte ([1] S. 37)
4. Beispiele: Die Reed-Solomon-Codes ([1] S. 20) und die Erzeugermatrix ([1] Aufgabe 13 S. 25)
5. Lemma: Der duale Code eines Reed-Solomon-Code ([1] Aufgabe 33 S.41)
6. Beispiele: Die Reed-Muller-Codes ([1] S. 21-22)
7. Lemma: Der duale Code eines Reed-Muller-Code
8. Satz: Parameter Reed-Muller-Codes ([1] S. 22)

6. LDPC-Codes ([1] Abschnitt 4)

1. Definition: bipartite Graphen
2. Bemerkung: bipartite Graphen von binären Code ([1] S. 31)
3. Definition: (l, r) -regulär binären Codes ([1] S. 32)
4. Bemerkung: Die Kontrollmatrix eines (l, r) -regulär binären Code. ([1] S. 32)
5. Definition: $(n, l, r, \alpha, \delta)$ -Expander, Expander-Code ([1] S. 32)
6. Beispiele: ([1] S. 32)
7. Satz: Minimaldistanz und Fehlerkorrektur beim Expander-Code ([1] S. 33)
8. Bemerkung: Iteratives Decodierverfahren ([1] S. 33)
9. Beispiel: ([1] S. 34)

7. Zyklische Codes ([1] Abschnitt 7)

1. Definition: zyklischer Code ([1] S. 47)
2. Beispiel: ([1] S. 47)

3. Bemerkung: Codewörter als Polynome in $K[x]$ modulo $x^n - 1$ ([1] S. 47, 48)
4. Satze: ([1] S. 48, 49)
5. Bemerkung: der zu einem zyklischen Code duale Code ist zyklisch ([1] S. 49)
6. Beispiel: CRC-Codes and zyklische Reed-Solomon Codes ([1] S. 49/50)
7. Satz: BCH-Schranke ([1] S. 51)
8. Beispiele: [7,4,3]-Code und [11,6,5] ([1] S. 52)

8. Schranken und Lineare Optimierung ([1])

9. Decodierung von BCH-Codes ([1])

Literatur

[1] W. Willems. *Codierungstheorie und Kryptographie*. Birkhäuser, 2008 (e-book)

Voraussetzungen : Lineare Algebra I and II