Seminarprogramm

Lineare Codierungstheorie

Universität Duisburg-Essen, Wintersemester 2014/15

Veranstalter: Prof. Dr. J. Kohlhaase, Dr. A. Pal
Ort und Zeit: WSC N-U-4.05, Di 12–14
Vorbesprechung: 16.09.2014, 12 c.t., WSC S-U-3.03

Inhalt: Bei der Übermittlung von Informationen treten oftmals Fehler auf, etwa durch atmosphärische Störungen beim Funkverkehr oder durch Materialfehler beim Schreiben auf Festplatten. Die Codierungstheorie stellt Methoden bereit, um solche Übertragungsfehler zu erkennen und zu korrigieren. Die grundlegende Idee ist hierbei, die gewünschten Informationen redundant zu übertragen. Dadurch wird allerdings der Informationsfluss langsamer und teurer. Gesucht sind daher besonders geschickte Codierungsverfahren.

In der linearen Codierungstheorie werden Verfahren dieser Art mit Hilfe der linearen Algebra über endlichen Körpern konstruiert. Im Rahmen des Seminars werden wir uns sowohl mit der entsprechenden Theorie als auch mit zahlreichen für die alltägliche Praxis wichtigen Beispielen auseinandersetzen.

Behandelte Themen: Aufgaben und Probleme der Codierungstheorie, Paritäts- und Wiederholungscodes, lineare Codes, Äquivalenz linearer Codes, Fehlerkorrektur und Maximum-Likelihood Decodierung, Syndromdecodierung, perfekte Codes, Hamming-Codes, Beispiele von BCH-Codes, duale Codes, erzeugende Funktionen, Reed-Muller-Codes, Hadamard-Codes, binäre Golay-Codes, zyklische Codes

1. Das Grundproblem der Codierungstheorie [14.10.]: Aufgaben und Probleme der Codierungstheorie (vgl. Einleitungen der unten stehenden Quellen); Codierung und Decodierung für den binären Paritätscode (vgl. [3], §0.2 aber mit beliebiger Wortlänge); erläutern Sie, inwiefern er 1-fehlererkennend ist; Codierung und Decodierung für den binären $(2e+1)$-Wiederholungscode (vgl. [2], Example 1.0.3 mit $k = 1$); inwiefern ist er e-fehlerkorrigierend?

2. Lineare Codes und Codierung [21.10.]: Codes und lineare Codes (vgl. [3], Definition 1.1.1 (1) und (2)); erläutern Sie den Begriff Blocklänge; Erzeugermatrix (vgl. [3], S. 16); Erzeugermatrix und Codierung (vgl. [1], Bemerkung 5.7 (a) und [2], §4.7); Kontrollmatrix (zur Existenz vgl. [1], Satz 5.10); erkennen von Codewörtern mit Hilfe der Kontrollmatrix; erläutern Sie alle Begriffe anhand des linearen Codes in [3], §0.3 (vgl. auch [3], S. 17/18)

3. Äquivalenz von Codes [28.10.]: Erzeugermatrizen in reduzierter Form; Äquivalenz linearer Codes (vgl. [3], S. 16); beweisen Sie [3], Lemma 1.1.4 (vgl. [1], Satz 5.31); behandeln Sie [1], Beispiel 5.32; Informations- und Kontrollsymbole; beweisen Sie [3], Lemma

1.1.5; (unvollständige) Decodierungsregeln (vgl. [3], Definition 1.1.1 (6)); Informationsrate eines Codes (vgl. [3], Definition 1.1.1 (7); welche Intuition steckt dahinter?)

4. Maximum-Likelihood Decodierung [04.11.]: Hamming-Abstand und Hamming-Norm (vgl. [3], S. 13/14); Minimaldistanz, e-fehlerkorrigierend, e-fehlererkennend und $[n, k, d]$-Codes (vgl. [3], Definition 1.1.1 (3)–(5) und [1], Definition 2.4 (c)); beweisen Sie [1], Satz 5.13; Maximum-Likelihood Decodierung (vgl. [3], Definition 1.1.2 und [1], Bemerkung nach Definition 2.4); berechnen Sie die Minimaldistanz für den in [3], §0.3 angegebenen linearen Code und zeigen Sie, dass die dortige Decodierungsregel der Maximum-Likelihood Bedingung genügt

5. Syndromdecodierung [11.11.]: Wiederholen Sie Nebenklassen von Untervektorräumen (vgl. [1], S. 37); erläutern Sie, wieso bei Maximum-Likelihood Decodierung Nebenklassenrepräsentanten minimaler Hamming-Norm von Bedeutung sind; erklären Sie ausführlich die Syndromdecodierung nach [3], 1.1.7/8 bzw. [1], §5.21 (vgl. auch [2], §4.8.3); führen Sie [1], Beispiel 5.22 vor

6. Perfekte Codes [18.11.]: [3], Definition 1.2.1; Eindeutigkeit der Maximum-Likelihood Decodierung (vgl. [3], Notiz 1.2.1 (a)); die Gleichung $d(\mathcal{C}) = 2e + 1$ (vgl. [1], Satz 4.2); Hamming-Schranke und Charakterisierung perfekter Codes (vgl. [3], Notiz 1.2.2 (b)&(c); für den Beweis vgl. [1], Lemma 4.3 und Satz 4.4); zeigen Sie, dass die binären Wiederholungscodes $\mathcal{R}_{2m+1}$ perfekt sind (vgl. [3], S. 19); führen Sie [1], Beispiel 4.5 vor

7. Hamming-Codes [25.11.]: [3], Definition 1.2.3; Konstruktion von Hamming-Codes (vgl. [3], Bemerkung 1.2.4 (a)&(b) und [1], §5.18); geben Sie in den Fällen $(q, r) = (2, 3)$ und $(q, r) = (3, 2)$ die Erzeugermatrix eines Hamming-Codes an; Perfektheit von Hamming-Codes (vgl. [3], Satz 1.2.6 und [1], S. 35 unten); erklären und beweisen Sie, wie die Maximum-Likelihood Decodierung von Hamming-Codes aussieht (vgl. [3], Bemerkung 1.2.7)

8. BCH-Codes [02.12.]: erläutern Sie ausführlich die Konstruktion des in [3], §1.3 vorgestellten BCH-Codes; zeigen Sie, dass bei Verwendung der Funktion $f(x) = x^3$ ein Fehlervektor mit Hamming-Norm 2 eindeutig durch sein Syndrom festgelegt ist; beweisen Sie die Eigenschaften des BCH-Codes in [3], Satz 1.3.1; erläutern Sie das unvollständige Maximum-Likelihood Decodierungsverfahren in [3], Notiz 1.3.2

9. Duale Codes [09.12.]: kanonische Paarung und orthogonale Komplemente (vgl. [3], Lemma 1.4.1 und [1], Satz 6.4 (a)&(b)); definieren Sie duale und selbstduale Codes; Erzeuger- und Kontrollmatrizen unter Dualität (vgl. [3], Notiz 1.4.3 und [1], Satz 6.4 (c)&(d)); zeigen Sie, dass in den dualen Hamming-Codes alle von Null verschiedenen Codewörter dieselbe Hamming-Norm haben (vgl. [1], Beispiel 6.5)

10. Erzeugende Funktionen [16.12.]: definieren Sie die erzeugende Funktion eines Codes (vgl. [3], S. 27); beweisen Sie die MacWilliams-Identität für duale Codes (vgl. [3], Satz 1.4.5 und Lemma 1.4.6); bestimmen Sie hiermit die erzeugenden Funktionen der binären

Hamming-Codes (vgl. [1], Beispiel 6.8)

11. Reed-Muller-Codes I [13.01.]: die $(u, u+v)$-Konstruktion (vgl. [3], Definition 1.5.1); beweisen Sie [3], Satz 1.5.2; binäre Reed-Muller-Codes (vgl. [3], Definition 1.5.3); beweisen Sie die Eigenschaften der Reed-Muller-Codes in [3], Satz 1.5.4; zeigen Sie, dass $\mathcal{R}(0, m)$ der binäre Wiederholungscode und $\mathcal{R}(m-1, m)$ der Paritätscode ist; referieren Sie über die Anwendung der Reed-Muller-Codes in der Raumfahrt (vgl. [3], Bemerkung 1.5.9 und [1], Beispiel 7.3 (d))

12. Reed-Muller-Codes II [20.01.]: erläutern Sie ausführlich die Struktur der Booleschen Algebra A (vgl. [3], Bemerkung 1.5.6 (i)–(v)); beweisen Sie [3], Satz 1.5.7 über die alternative Konstruktion der Reed-Muller-Codes; führen Sie die für die Formulierung von [3], Satz 1.5.8 notwendigen Bezeichnungen ein und erklären Sie ohne Beweis das Decodierungsverfahren für Reed-Muller-Codes

13. Hadamard-Codes [27.01.]: punktierte und erweiterte Codes (vgl. [3], Einleitung zu Kapitel 2); Hadamard-Matrizen (vgl. [3], Definition 2.1.1); Konstruktion und Eigenschaften von Hadamard-Matrizen (vgl. [3], Bemerkung 2.1.2); die Hadamard-Codes im Fall $n = 2^m$ (vgl. [3], Konstruktion 2.1.4 inklusive Beweis der Minimaldistanzen); führen Sie die Konstruktion im Fall $m = 2$ mit Hilfe der Matrix H_4 aus [3], Beispiel 2.1.3 explizit vor; Nachweis der Linearität; zeigen Sie, dass die binären Reed-Muller-Codes $\mathcal{R}(1, m)$ stets Hadamard-Codes sind (vgl. [3], Beispiel 2.1.6)

14. Binäre Golay-Codes [03.02.]: erläutern Sie schrittweise die Konstruktion des binären Golay-Codes $\mathcal{G}_{24}$ (vgl. [3], S. 42); beweisen Sie, dass $\mathcal{G}_{24}$ ein linearer Code der Dimension 12 ist; definieren Sie den binären Golay-Code $\mathcal{G}_{23}$; beweisen Sie so ausführlich wie möglich die Eigenschaften der binären Golay-Codes in [3], Notiz 2.2.2 (vgl. auch [2], §5.3.3))

15. Zyklische Codes [10.02.]: [3], Definition 3.1.1; geben Sie Beispiele (nicht) zyklischer Codes an; zeigen Sie, dass für einen zyklischen Code auch der duale Code zyklisch ist; wiederholen Sie Division mit Rest im Polynomring $\mathbb{F}_q[X]$; erklären Sie, wie man den Quotientenring $\mathbb{F}_q[X]/(X^n - 1)$ mit $\mathbb{F}_q^n$ identifiziert und wie sich die Multiplikation beschreiben lässt (vgl. [3], S. 47/48 oder [2], §7.1); definieren Sie, was ein Ideal in einem Ring ist und beweisen Sie die Charakterisierung zyklischer Codes in [3], Notiz 3.1.3 (vgl. auch [2], Theorem 7.2.1)

Literatur

[1] P. Hauck: *Codierungstheorie*, Vorlesungsskriptum, Universität Tübingen, Wintersemester 2005/06, online erhältlich unter `http://dm.inf.uni-tuebingen.de/skripte/Codierungstheorie/`

[2] S. Ling, C. Xing: *Coding Theory – a First Course*, Cambridge University Press, 2004

[3] W. Lütkebohmert: *Codierungstheorie – Algebraisch-geometrische Grundlagen und Algorithmen*, Vieweg, 2003

[4] B.H. Matzat: *Codierungstheorie*, Vorlesungsskriptum, Universität Heidelberg, Wintersemester 2003/04, online erhältlich unter `http://www.iwr.uni-heidelberg.de/~Heinrich.Matzat/PDF/`

[5] R.H. Schulz: *Codierungstheorie – Eine Einführung*, 2. Auflage, Vieweg, 2003

Die oben angegenen Referenzen enthalten Hinweise auf weitere Literaturquellen. Die Bücher [2], [3] und [5] liegen in meinem Büro aus und können zum Kopieren entliehen werden.