Prof. Dr. Wolfgang Willems
David Lorch
Sebastian Thomas

SS 2009
25.08.2009

Codierungstheorie

Vorlesung 1

§0 Mathematische Probleme in der digitalen Datenübertragung

Sender → KANAL → Empfänger
KANÄLE: Atmosphäre, Telefonleitung, Speichermedium (magnetisches Band, CD, ...).

(a) Schutz der Daten bei der Übertragung gegen unerlaubtes Lesen oder Manipulieren

- passiv (Pay-TV, ...)
- aktiv (Homebanking, ...)

Idee: Verschlüsseln.

Theorie: Kryptographie.

Mathematik: (algebraische) Zahlentheorie, Komplexitätstheorie.

(b) Schutz der Daten gegen zufällige Fehler bei einem unsicher arbeitenden Kanal.

Idee: Man sendet zusätzliche Redundanz, mit welcher man Fehler korrigieren kann.

Theorie: Codierungstheorie.

Mathematik: Lineare Algebra, Kombinatorik, endliche Geometrie, algebraische Geometrie, Darstellungstheorie, Invariantentheorie.

Literatur

Einfach:

- W. Willems, *Codierungstheorie und Kryptographie*, Birkhäuser, 2008.

Weitergehend:

- J. Bierbrauer, *Introduction to Coding Theory*, Chapman/Hall, 2004.
- J. van Lint, *Introduction to Coding Theory*, Springer, 1998.
- Huffman, van Pless, *Fundamentals of error correcting codes*, Cambridge Press, 2003.

Bibel:

- Sloane, Mac Williams, *The theory of error-correcting codes*, North-Holland, 1988.

Überblick:

- Willems, *Mathematische Aspekte der Codierungstheorie*, Jahresberichte der DMV, 2007.

§1 Grundbegriffe

(1.1) Beispiel. Informationssymbol $\{0, 1\}$.

Information	Codierer	KANAL			Decodierer
00	00000			(4 Fehler)	
10	10110	$\rightsquigarrow$	10111	(1 Fehler)	$\rightsquigarrow 10110 \leftrightarrow 10$
01	01101			(3 Fehler)	
11	11011			(2 Fehler)	

Idee: Decodierer sucht das Codewort mit minimaler Anzahl von Fehlern.

(1.2) Definition. Sei K ein endlicher Körper mit q Elementen und $n \in \mathbb{N}$. Wir nennen einen linearen Unterraum von $K^n = \{(k_1, \ldots, k_n) \mid k_i \in K\}$ einen (*linearen*) *Code*, seine Elemente *Codewörter*. Schreibe: $C \leq K^n$.

Bemerkung. Das Alphabet muss kein Körper sein, ein Code muss nicht linear sein. $|A| = q$, $C \subseteq A^n$.

Endliche Körper:

- p Primzahl. $K = \mathbb{Z}/p\mathbb{Z}$ Körper mit p Elementen; $\operatorname{char} K = p$.
- $K_0 = \mathbb{Z}/p\mathbb{Z}$, $f \in K_0[x]$ irreduzibel vom Grad n (existiert!). $K = K_0[x]/fK_0[x]$, $|K| = p^n$.

(1.3) Definition.

(a) Für $u, v \in K^n$ definieren wir den *Hamming-Abstand* d durch $\mathrm{d}(u, v) = |\{i \in \{1, \ldots, n\} \mid u_i \neq v_i\}|$.

(b) Für $u \in K^n$ heißt $\mathrm{wt}(u) = \mathrm{d}(u, 0) = |\{i \in \{1, \ldots, n\} \mid u_i \neq 0\}|$ das *Gewicht* von u.

(c) Für $C \leq K^n$ heißt $\mathrm{d}(C) = \min\{d(c, c') \mid c, c' \in C, c \neq c'\}$ *Minimaldistanz* von C, falls $C \neq \{0\}$. Für $C = \{0\}$ setze $\mathrm{d}(C) = 0$.

(d) Für $C \leq K^n$ heißt $\mathrm{wt}(C) = \min\{\mathrm{wt}(c) \mid 0 \neq c \in C\}$ das *Minimalgewicht* von C, falls $C \neq \{0\}$. Ist $C = \{0\}$, so setzen wir $\mathrm{wt}(C) = 0$.

(1.4) Lemma.

(a) Der Hamming-Abstand d definiert eine translationsinvariante Metrik auf K^n.

- $\mathrm{d}(u, v) \geq 0$, $\mathrm{d}(u, v) = 0 \Leftrightarrow u = v$.
- $\mathrm{d}(u, v) = \mathrm{d}(v, u)$.
- $\mathrm{d}(u, v) \leq \mathrm{d}(u, w) + \mathrm{d}(w, v)$.
- translationsinvariant: $\mathrm{d}(u, v) = \mathrm{d}(u + w, v + w)$.

(b) $\mathrm{wt}(C) = \mathrm{d}(C)$. (Gilt nur für lineare Codes.)

Beweis. Übung. □

(1.5) Definition. Sei $C \leq K^n$. Ist $\dim C = k \leq n$ und $d = \mathrm{d}(C)$ die Minimaldistanz von C, so heißt C ein $[n, k, d]$-Code über K.

(1.6) Beispiel. $K = \mathbb{F}_2$. $C = \{c \in K^7 \mid c_1 + c_4 + c_6 + c_7 = 0, c_2 + c_4 + c_5 + c_7 = 0, c_3 + c_5 + c_6 + c_7 = 0\} \leq K^7$.

$$H = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}.$$

Dann $C = \{c \in K^7 \mid Hc^{\mathrm{T}} = 0\}$. $\dim C = \dim(\operatorname{Kern} H) = n - \dim(\operatorname{Bild} H) = n - \operatorname{rg} H = 7 - 3 = 4$.
Was ist $\mathrm{d}(C)$? $\begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 0 \end{pmatrix} \in C \Rightarrow \mathrm{d}(C) = \mathrm{wt}(C) \leq 3$. $\mathrm{d}(C) \neq 1$, $\mathrm{d}(C) \neq 2$ erkennt man an H. $\Rightarrow$ C ist ein $[7, 4, 3]$-Code (*Hamming-Code*).

(1.7) Definition. Sei C ein $[n, k, d]$-Code über K. Ist $H \in (K)_{n-k,n}$ und $C = \operatorname{Kern} H$, so heißt H eine *Kontrollmatrix* für C. Ist $G \in (K)_{k,n}$, so dass die Zeilen von G den Code C aufspannen (Zeilen sind dann Basis), so heißt G eine *Erzeugermatrix*.

(1.8) Lemma. Sei C ein $[n, k]$-Code mit $k \geq 1$ und Kontrollmatrix H. Dann gilt:

$$\begin{aligned} \mathrm{d}(C) &= \min\{r \in \mathbb{N} \mid \text{es existieren } r \text{ linear abhängige Spalten von } H\} \\ &= \max\{r \in \mathbb{N} \mid \text{je } r - 1 \text{ Spalten von } H \text{ sind linear unabhängig}\}. \end{aligned}$$

Beweis. $H = \begin{pmatrix} h_1 & \ldots & h_n \end{pmatrix}$. Die Spalten $h_1, \ldots, h_n$ sind linear abhängig, da $C \neq \{0\}$. Sei w minimal gewählt, so dass $h_{i_1}, \ldots, h_{i_w}$ linear abhängig. Also $\sum_{j=1}^{w} c_{i_j} h_{i_j} = 0$ ($c_{i_j} \neq 0$ für alle j). Setze $c = \begin{pmatrix} c_1 & \ldots & c_n \end{pmatrix}$ mit

$$c_k = \begin{cases} c_{i_j}, & \text{falls } k = i_j, \\ 0, & \text{sonst.} \end{cases}$$

Also $Hc^{\mathrm{T}} = 0$ und damit $c \in C$. $\mathrm{d}(C) = \mathrm{wt}(C) \leq \mathrm{wt}(c) = w$.
Angenommen, es gibt ein $c' \in C$ mit $\mathrm{wt}(c') = w' < w$. $0 = Hc'^{\mathrm{T}}$, d.h. w' Spalten von H sind linear abhängig, Widerspruch. □

(1.9) Definition. Sei $0 \leq r \in \mathbb{R}$, $u \in K^n$. $\mathrm{B}_r(u) = \{v \in K^n \mid \mathrm{d}(v,u) \leq r\}$ *Kugel* um u vom Radius r.

(1.10) Lemma. Ist $|K| = q$, so ist

$$|\mathrm{B}_r(u)| = |\mathrm{B}_r(0)| = \sum_{j=0}^{\lfloor r \rfloor} \binom{n}{j} (q-1)^j$$

für alle $u \in K^n$.

Beweis. Übung. □

(1.11) Anwendung in der Datenübertragung. Nachricht = Folge von Nachrichteneinheiten.
Nachrichteneinheiten $\leftrightarrow$ Codeworte in einem $[n,k,d]$-Code über $K = \mathbb{F}_q$. $\mathbb{N} \ni e \leq \lfloor \frac{d-1}{2} \rfloor$. $|K^n| = q^n$.
$e \leq \lfloor \frac{d-1}{2} \rfloor \Rightarrow \mathrm{B}_e(c) \cap \mathrm{B}_e(c') = \emptyset$, falls $c, c' \in C$, $c \neq c'$.
Annahme: Im Kanal passieren bei der Übertragung höchstens e Fehler.
$c \in C$ gesendet, $v \in K^n$ empfangen. Decodierer sucht die Kugel, in der v liegt und decodiert zum Mittelpunkt der Kugel.
Fazit: Ein $[n,k,d]$-Code kann bis zu $\frac{d-1}{2}$ Fehler korrigieren.

Problem. Gegeben n, k, q. Suche $C \leq K^n$ mit $\dim C = k$ und $\mathrm{d}(C)$ größtmöglich.
$K = \mathbb{F}_2$, $n = 72$. Wie viele Codes der Dimension 36 gibt es?