Concrete Codes for Communication

Adrian Sieler, 25.Juni.2015

Definition: Sei $\mathcal{X}$ ein endliches Alphabet, $0 \in \mathcal{X}$ und $x, x' \in \mathcal{X}^n$:

- $d(x) = |\{i \in \{1, ..., n\} \mid x_i \neq 0\}|$ *"Hamming weight"*
- $d(x - x') = |\{i \mid x_i \neq x'_i\}|$ *"Hamming distance"*
- $\{x' \in \mathcal{X} \mid d(x - x') \leq r\}$ *"Hamming ball" mit Radius r um x*

Definition: *Sei* $C \subseteq \mathcal{X}^n$:

- $R(C) := \frac{\log(|C|)}{\log(|\mathcal{X}^n|)}$ bezeichnet die *"Rate"* eines Codes.
- $d(C) := \min\limits_{c,c' \in C \ \wedge \ c \neq c'} d(c - c')$ bezeichnet die *"Distanz"* und $\frac{d(C)}{n}$ die *"relative Distanz"* eines Codes.

Lemma: Ein Code mit Distanz d erlaubt

1. $\lfloor \frac{d-1}{2} \rfloor$ *Fehler*,
2. $(d-1)$ *Auslöschungen* zu korrigieren.

Definition: Sei $\mathcal{X}$ ein Körper und $C \subseteq \mathcal{X}^n$ ein Untervektorraum, dann wird C "linearer Code" genannt.

Definition:

- $G \in GF(q)^{n \times k}$ wird als *"Generatormatrix"* für einen linearen Code $C \subseteq GF(q)^n$ bezeichnet, wenn die Spalten von G eine Basis von C bilden.
- C wird als "$[n, k] - Code$" oder "$[n, k, d] - Code$" bezeichnet, wenn $d(C) = d$.

Lemma: Für jeden linearen Code $C \subseteq GF(q)^n$ gilt

$$d(C) = \min_{c \in C \setminus \{0\}} d(c)$$

Definition: Eine Generatormatrix $G \in GF(q)^{n \times k}$ liegt in systematischer Form vor, wenn $G = (\mathbb{1}_k \ P)^t$ mit $P \in GF(q)^{k \times (n-k)}$.
Das Kodieren $x \to Gx$ wird dann als "systematisch" bezeichnet.

Proposition: Sei $G = (\mathbb{1}_k \ P)^t$ die Generatormatrix eines linearen Codes $C \subseteq GF(q)^n$. Dann gilt $\forall c \in GF(q)^n$:

$$c \in C \iff Mc = 0 \text{ mit } M := (-P^t \ \mathbb{1}_{n-k})$$

M wird als *"parity check matrix"* bezeichnet.

Proposition (Hamming-Schranke):
Sei $C \subseteq \mathcal{X}^n$ ein Code mit $q := |\mathcal{X}|$, Distanz $d := d(C)$ und $m := \lfloor \frac{d-1}{2} \rfloor$, dann gilt:

$$|C| \leq \frac{q^n}{V(q,n,m)} \text{ mit } V(q,n,m) := \sum_{i=0}^{m} \binom{n}{k}(q-1)^i$$

Ein Code für den die *Hamming-Schranke* mit Gleichheit erfüllt ist, wird als *"perfekt"* bezeichnet.

Definition (Reed-Solomon-Codes):
Für $1 \leq k < n \leq q$ und $\alpha \in GF(q)^n$ mit unterschiedlichen Komponenten wird

$$C := \{p(\alpha) \in GF(q)^n \mid p \textit{ ist Polynom } \text{über } GF(q) \textit{ mit Grad} < k\}$$

als *"Reed-Solomon-Code"* ($[n,k] - RS$ *code*) bezeichnet.

Kodierung (Reed-Solomon-Codes):

- Identifizieren der Nachricht $m \in GF(q)^k$ mit dem Polynom

  $$p_m(x) := \sum_{l=0}^{k-1} m_{l+1} x^l$$

  das Codewort ist dann $p_m(\alpha) = (p(\alpha_1), p(\alpha_2), \ldots, p(\alpha_n))$

- $p_m(\alpha) = Gm$ mit $G \in GF(q)^{n \times k}$ ist eine *"Vandermonde Matrix"* mit $G_{xy} = \alpha_x^{y-1}$
  $\implies$ RS-Codes sind linear

Literatur

[1] Robert J. McEliece, *The Theory of Information and Coding*, Cambridge University Press, Second edition, 2002.

[2] David MacKay, *Information Theory, Inference, and Learning Algorithms* Cambridge University Press, First edition, 2003

[3] Michael Wolf, *http://www-m5.ma.tum.de/Allgemeines/MA5103_2012W*, 2012