Zusammenfassung Codierungstheorie

© BY: Tim Baumann, http://timbaumann.info/uni-spicker

$$\text{Datenquelle} \xrightarrow{\text{senden}} \text{Kanal} \xrightarrow{\text{empfangen}} \text{Senke}$$

Die Daten liegen bereits digitalisiert vor. Mit dem Problem wie Daten wie bspw. natürliche Sprache möglichst effizient codiert werden, befasst sich die Informationstheorie. In dieser Vorlesung soll es darum gehen, Daten mit einer Kanalcodierung so zu übersetzen, dass Fehler, die bei einer Übertragung über einen fehlerhaften Kanal, korrigiert oder zumindest bemerkt werden.

$$\text{Datenquelle} \xrightarrow[E]{\text{codieren}} \text{Code} \xrightarrow{\text{senden}} \text{Kanal} \xrightarrow{\text{empfangen}} \square$$
$$\xrightarrow[D]{\text{decodieren}} \text{Code} \xrightarrow[E^{-1}]{} \text{Senke}$$

Def. Ein **Alphabet** ist eine Menge Q mit $q > 1$ Elementen, typischerweise $\{0, 1, \dots, q-1\} \cong \mathbb{Z}_q$.

Bem. $\mathbb{Z}_q$ trägt die Struktur eines Ringes. Falls q eine Primzahlpotenz ist, so gibt es einen Körper $\mathbb{F}_q$ mit q Elementen.

Def. Sei $n \geq 1$. Eine nichtleere Menge $C \subseteq Q^n$ mit $q = |Q|$ heißt **Blockcode** der Länge n über Q oder **q-närer Code** der Länge n. Jedes $c = (c_1, \dots, c_n) \in C$ heißt ein **Codewort**. Falls $M = |C|$, so nennt man C einen **(n, M)-Code** über Q.

Def. Die **Informationsrate** von C ist dann $R(C) \coloneqq \log_n(M)/n$. Falls $|M| = q^k$, dann ist $R(C) = k/n$.

Bem. Ist $Q \cong \mathbb{F}_q$, dann ist Q^n ein $\mathbb{F}_q$-VR. Falls C ein Unterraum von Q^n ist, so ist $R(C) = \dim_{\mathbb{F}_q}(C)/n$.

Def. Der **Hamming-Abstand** von $u, v \in Q^n$ ist

$$d(u, v) \coloneqq |\{i = 1, \dots, n \mid u_i \neq v_i\}|.$$

Lem. Der Hamming-Abstand ist eine Metrik auf Q^n.

Notation. Es sei $C \subseteq Q^n$ ein Code und $y \in Q^n$. Wenn y empfangen wurde, so geht man davon aus, dass das gesendete Wort dasjenige des Codes mit den wenigsten Unterschieden zu y ist, also ein Wort, welches den **Hamming-Abstand** $d(y, C) \coloneqq \min_{c \in C} d(y, c)$ von y zu C realisiert. Es existiert i. A. kein eindeutiges solches Element, sondern eine Menge

$$N_c(y) \coloneqq \{\overline{c} \mid d(y, C) = d(y, \overline{c})\}.$$

Def.
- Man nennt einen Kanal einen **q-nären symmetrischen Kanal**, falls ein $p \in \mathbb{R}$ mit $0 < p < (q-1)/q$ existiert, sodass
$$\mathbb{P}(\beta \text{ empfangen} \mid \alpha \text{ gesendet}) = \tfrac{p}{q-1}$$
für alle $\beta \neq \alpha \in Q$, also $\mathbb{P}(\alpha \text{ empfangen} \mid \alpha \text{ gesendet}) = 1 - p$.
- Man nennt einen Kanal **gedächtnislos**, falls
$$\mathbb{P}(y \text{ empfangen} \mid c \text{ gesendet}) = \prod_{i=1}^{n} \mathbb{P}(y_i \text{ empfangen} \mid c_i \text{ gesendet})$$
für alle Wörter $x, y \in Q^n$ gilt.

Def (Maximum-Likelihood-Prinzip). Gegeben sei ein Code $C \subseteq Q^n$ und $y \in Q^n$. Gesucht ist $\hat{c} = \arg\max_{c \in C} \mathbb{P}(y \mid c)$.

Satz. Es seien ein q-närer symm, gedächtnisloser Kanal und ein Code $C \subseteq Q^n$ gegeben. Sei $y \in Q^n$ und $\hat{c} \in C$. Dann sind äquivalent:
- $\mathbb{P}(y \mid \hat{c}) = \max_{c \in C} \mathbb{P}(y \mid c)$
- $\hat{c} \in N_c(y)$