Zusammenfassung Codierungstheorie

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 $\{0, 1, \ldots, q-1\} \cong \mathbb{Z}_q$.

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 $c = (c_1, \ldots, c_n) \in C$ heißt ein **Codewort**. Falls $M = |C|$, so nennt man C einen **(n, M)-Code** über Q.

Def. Die **Informationsrate** von C ist dann $R(C) := \log_n(M)/n$. 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

$$d(u, v) := |\{i = 1, \ldots, n \,|\, u_i \neq v_i\}|.$$

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** $d(y, C) := \min\limits_{c \in C} d(y, c)$ von y zu C realisiert. Es existiert i. A. kein eindeutiges solches Element, sondern eine Menge

$$N_c(y) := \{\overline{c} \,|\, d(y, C) = d(y, \overline{c})\}.$$

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 $\hat{c} = \arg\max\limits_{c \in C} \mathbb{P}(y \mid c)$.

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:
- $\mathbb{P}(y \mid \hat{c}) = \max\limits_{c \in C} \mathbb{P}(y \mid c)$
- $\hat{c} \in N_c(y)$

Def. $D : Q^n \to C$ heißt **vollständige Decodierabbildung**, falls

$$\forall\, y \in Q^n \;:\; D(y) \in N_C(y).$$

Def. Die **Kanalkapazität** eines q-nären symmetrischen Kanal ist

$$\kappa(q, p) := \log_2(q) + p \cdot \log_2(\tfrac{p}{q-1}) + (1-p) \cdot \log_2(1-p).$$

Sie ist ein Maß für die maximale Information, die über den Kanal übertragen werden kann. Die **Entropiefunktion** ist

$$H(q, p) := 1 - \kappa(q, p).$$

Def. Sei C ein Code und D sei eine zugehörige (vollständige) Decodierabbildung. Die **Restfehlerwahrscheinlichkeit** zu (C, D):

$$\mathbb{P}_{\text{err}}(C) := \max_{y \in Q^n, c \in C} \mathbb{P}(D(y) \neq c \mid c \text{ gesendet, } y \text{ empfangen})$$

Satz (**Shannon**)**.** Sei $0 < R < \kappa(q, p)$. Dann gibt es eine Folge $(C_n)_{n \in \mathbb{N}}$ von Codes und zugehörigen Decodierabbildungen D_n mit:
- C_n ist ein (n, M_n)-Code mit Informationsrate $R \leq R(C_n) < \kappa(q, p)$
- $\lim\limits_{n \to \infty} (\mathbb{P}_{\text{err}}(C_n)) = 0$

Def. Der **Minimalabstand** eines (n, M)-Codes C über Q ist

$$d := d(C) := \min_{c, c' \in C, c \neq c'} d(c, c').$$

Man sagt dann, C ist ein q-närer (n, M, d)-Code.

Notation. Zu $u \in Q^n$ und zu $l \in \mathbb{N}$ sei $B_l(u) := \{x \in Q^n \,|\, d(x, x) \leq l\}$.

Def.
- Ein Code C heißt **l-fehlerkorrigierend**, falls $B_l(c) \cap B_{l'}(c') = \emptyset$ für alle $c, c' \in C$ mit $c \neq c'$.
- C heißt **m-fehlererkennend**, wenn $B_m(c) \cap C = \{c\}$ f. a. $c \in C$.
- C heißt **genau l-fehlerkorrigierend/-erkennend**, falls C m-fehlerkorr./-erkennend für $m := l$ aber nicht $m := l + 1$ ist.

Satz. Jeder (n, M, d)-Code C ist genau
- $(d-1)$-fehlererkennend und
- $(t := \lfloor \frac{d-1}{2} \rfloor)$-fehlerkorrigierend.

Bsp. $C = \{000, 111\}$ ist ein binärer $(3, 2, 3)$-Code.

Problem. Gegeben: q, Länge n, Minimalabstand d. Gesucht:

$$A_q(n, d) := \max\{M \,|\, \exists\, (n, M, d)\text{-Code}\}$$

Def. Ein (n, M, d)-Code heißt **optimal**, falls $M = A_q(n, d)$.

Lem. Seien $q, n \in \mathbb{N}$, $q \geq 2$, $n \geq 1$.
- $A_q(n, 1) = q^n$, realisiert durch $C = Q^n$.
- $A_q(n, n) = q$, realisiert durch $C = \{(a, \ldots, a) \,|\, a \in Q\} \subseteq Q^n$
- $d \leq d' \implies A_q(n, d) \geq A_q(n, d')$
- Sei $n \geq 2$ und $d \geq 2$. Dann gilt $A_q(n, d) \leq A_q(n-1, d-1)$.

Kor (**Singletonschranke**)**.** $A_q(n, d) \leq q^{n-d+1}$

Def. Ein Code, der die Singletonschranke mit Gleichheit erfüllt, heißt ein **MDS-Code** (MDS = maximum distance separable).

Bem. Sei $C \subseteq Q^n$ ein (n, M, d)-Code, $T = \{1 \leq t_1 < \ldots < t_{|T|} \leq n\}$ und $\pi_T : C \to Q^{|T|}$, $c \mapsto (c_{t_1}, \ldots, c_{t_{|T|}})$. Ist C ein MDS-Code, so ist π_T bijektiv für alle T mit $|T| = n - d + 1$.

Satz. $A_q(n, 2) = q^{n-1}$, realisiert durch einen Code mit Prüfziffer

Def. Sei $(G, +, 0)$ eine kommutative Gruppe. Das **Hamming-Gewicht** von $x \in G^n$ ist

$$\text{wt}(x) := |\text{supp}(x)|, \quad \text{wobei} \quad \text{supp}(x) := \{i \,|\, x_i \neq 0\}.$$

Lem. Sei G wie oben, $x, y \in G^n$. Dann wt$(x - y) = d(x, y)$.

Satz. $A_q(n, 2) = q^{n-1}$ für alle $q \geq 2$ und alle $n \geq 2$.

Beweis. Wir konstruieren einen $(n, q^{n-1}, 2)$-Code. Sei R ein kommutativer Ring mit q Elementen, $\lambda_1, \ldots, \lambda_{n-1} \in R$ Einheiten und $\lambda_n := -1$. Wir betrachten die Kontrollgleichung

$$\kappa : R^n \to R, \quad z \mapsto \lambda_1 z_1 + \ldots + \lambda_n z_n.$$

Dann ist $C := \ker(\kappa)$ ein 1-fehlererkennender Code. $\square$

Lem. Falls $\lambda_2 - \lambda_1, \ldots, \lambda_n - \lambda_{n-1}$ ebenfalls Einheiten sind, so sind Nachbarvertauschungen als Fehler erkennbar.

Bspe.
- Für $q = 2, R = \mathbb{Z}_2, \lambda_1 = \ldots = \lambda_{n-1} = 1$ heißt $C := \ker(\kappa)$ **Parity-Check-Erweiterung**.
- Beim ISBN-Code ist $R = \mathbb{Z}_{11}$, $\lambda_1 = 1, \ldots, \lambda_9 = 9$, also $\kappa(z) = \sum\limits_{i=1}^{10} i z_i$.

Bem. Es gilt $A_q(4, 3) = q^2 \iff$ es gibt ein Paar orthogonaler lateinischer Quadrate der Größe $q \iff q \neq 2$ oder $q \neq 6$.

Lem. Für $x, y \in \mathbb{Z}_2^n$ gilt $d(x, y) = \text{wt}(x) + \text{wt}(y) - 2 \cdot \text{wt}(x \cdot y)$.

Satz. Für alle $n \geq 1$ und d ungerade gilt $A_2(n, d) = A_2(n+1, d+1)$, realisiert durch die Parity-Check-Erweiterung.

Def. Zwei (n, M)-Codes C, C' über Q heißen **äquivalent**, falls gilt: Es gibt eine Permutation γ auf $\{1, \ldots, n\}$ und Permutationen $\sigma_1, \ldots, \sigma_n$ auf Q, sodass

$$\alpha : Q^n \to Q^n, \quad (x_1, \ldots, x_n) \mapsto (\sigma_1(x_{\gamma(1)}), \ldots, \sigma_n(x_{\gamma(n)}))$$

den Code C auf C' abbildet.