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 $R(C) := \log_n(M)/n$. 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

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

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

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

Def.
- Man nennt einen Kanal einen **q-nären symmetrischen Kanal**, falls ein $p \in \mathbb{R}$ mit $0 < p < (q-1)/q$ existiert, sodass

$$\mathbb{P}(\beta \text{ empfangen} \mid \alpha \text{ gesendet}) = p/q-1$$

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

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

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

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 $R \leq R(C_n) < \kappa(q, p)$
- $\lim_{n \to \infty} (\mathbb{P}_{\text{err}}(C_n)) = 0$

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. Für $u \in Q^n$, $l \in \mathbb{N}$ sei $B_l(u) := \{x \in Q^n \mid d(x, x) \leq l\}$.

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
- $(t := \lfloor d-1/2 \rfloor)$-fehlerkorrigierend.

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

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

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

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 $C = \{(a, \dots, a) \mid a \in Q\} \subseteq Q^n$
- $d \leq d' \implies A_q(n, d) \geq A_q(n, d')$
- 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, $T = \{1 \leq t_1 < \dots < t_{|T|} \leq n\}$ und $\pi_T : C \to Q^{|T|}$, $c \mapsto (c_{t_1}, \dots, c_{t_{|T|}})$. 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

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

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

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, $\lambda_1, \dots, \lambda_{n-1} \in R$ Einheiten und $\lambda_n := -1$. Wir betrachten die Kontrollgleichung

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

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

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

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

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 $\{1, \dots, n\}$ und Permutationen $\sigma_1, \dots, \sigma_n$ auf Q, sodass

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

den Code C auf C' abbildet.

Bsp. $A_2(5, 3) = 4$ realisiert durch $\{00000, 11100, 00111, 11011\}$

Lem. Sei Q ein Alphabet, $u \in Q^n$. Dann gilt

$$|B_l(u)| = \sum_{j=0}^{l} \binom{n}{j} (|Q| - 1)^j.$$

Satz (**Kugelpackungsschranke** (KPS)). Sei $q \geq 2$, $n \geq 2$, $1 \leq d \leq n$, $t \coloneqq \lfloor \frac{d-1}{2} \rfloor$. Dann ist

$$A_q(n,d) \leq q^n / \sum_{j=0}^{t} \binom{n}{j} (q-1)^j.$$

Def. Ein q-närer (n, M, d)-Code C heißt **perfekt**, falls M gleich der Kugelpackungsschranke ist.

Bem. Die KPS kann zur **Johnsen-Schranke** verbessert werden. Zusammen mit dem letzten Beispiel liefert diese $A_2(6,3) = 8$.

Bsp. Für q=2, n=7, d=3 liefert die KGS genau $A_2(7,3) \leq 16$.

Bem. Zu jeder Primzahlpotenz $q = p^m \geq 2$ gibt es bis auf Isomorphie genau einen Körper $\mathbb{GF}_q = \mathbb{F}_q$ mit q Elementen. Die Charakteristik dieses Körpers ist p. Ist q keine Primzahlpotenz, so gibt es auch keinen Körper mit q Elementen.

Konstruktion. Sei $q = p^m$, p prim. Dann gibt es ein irreduzibles Polynom $g(x)$ in $\mathbb{Z}_p$ mit $\deg(g) = m$. Dann ist $\mathbb{F}_q \coloneqq \mathbb{Z}_p[x]/(g(x))$.

Def. Ein **$\mathbb{F}_q$-linearer Code** der Länge n ist ein $\mathbb{F}_q$-Teilraum $\mathbb{F}_q^n$.

Notation. Sei C ein $\mathbb{R}_q$-linearer Code. Sei $k \coloneqq \dim(C)$. Dann ist $|C| = q^k$, also C ein (n, q^k)-Code. Man sagt, C ist ein $[n,k]$-Code. Ist d der Minimalabstand von C, so: C ist ein $[n,k,d]$-Code.

Def. Sei C ein $\mathbb{F}_q$-linearer Code mit $\dim(C) \geq 1$. Das **Minimalgewicht** von C ist $\min\{\mathrm{wt}(c) \mid c \in C, c \neq 0\}$.

Lem. Sei C ein $\mathbb{F}_q$-linearer Code mit $\dim(C) \geq 1$. Dann:

$$\text{Minimalgewicht von } C = \text{Minimalabstand von } C.$$

Bsp. Folgender Code ist ein bin. $(6,8,3)$-Code bzw. $[6,3,3]$-Code:

$$\left\{ \begin{matrix} 000000, 100101, 010110, 001111, \\ 110011, 101010, 011001, 111100 \end{matrix} \right\} = \mathrm{span}\{100101, 010110, 001111\}$$

Problem. Gegeben sei $\mathbb{F}_q$, die Länge n und der Minimalabstand d. Gesucht ist $A_q^{\mathrm{lin}}(n,d)$, die bestmögliche Anzahl Wörter eines Codes mit diesen Parametern.

Bem. Klar ist $A_q^{\mathrm{lin}}(n,d) \leq A_q(n,d)$.

Lem.
- $A_q^{\mathrm{lin}}(n,1) = q^n = A_q(n,1)$
- $A_q^{\mathrm{lin}}(n,n) = q = A_q(n,n)$
- $d \leq d' \implies A_q^{\mathrm{lin}}(n,d) \geq A_q^{\mathrm{lin}}(n,d')$
- Für $n \geq 2$, $d \geq 2$ ist $A_q^{\mathrm{lin}}(n,d) \leq A_q^{\mathrm{lin}}(n-1,d-1)$.

Bem. Da die Parity-Check-Erweiterung durch eine lineare Abbildung geschieht, gilt:

Satz. $A_1^{\mathrm{lin}}(n,2) = q^{n-1} = A_q(n,2)$

Satz. Falls d ungerade, so ist $A_2^{\mathrm{lin}}(n,d) = A_2^{\mathrm{lin}}(n+1,d+1)$

Def. Sei C ein $[n,k]$-Code über $\mathbb{F}_q$, d. h. es gibt eine injektive Codierabbildung $E : \mathbb{F}_q^k \to \mathbb{F}_q^n$ mit $\mathrm{im}(E) = C$. Dann heißt für jede Basis $g^1, \ldots, g^k \in C$ von C die Matrix

$$G \coloneqq \begin{pmatrix} g^1 \\ \vdots \\ g^k \end{pmatrix} \in \mathbb{F}_q^{k \times n} \qquad \text{eine } \textbf{Generatormatrix} \text{ von } C.$$

Bem. Dann ist $E(u) = uG = \sum_{j=1}^{k} u_j g^j \in C$

Def. Zwei $[n,k]$-Codes $C, C' \subseteq \mathbb{F}_q^n$ heißen **linear äquivalent**, falls es $\gamma \in S_n$ und $\lambda_1, \ldots, \lambda_n \in \mathbb{F}_q^\times$ gibt, sodass die monomiale Transf.

$$\alpha : \mathbb{F}_q^n \to \mathbb{F}_q^n, \quad (x_1, \ldots, x_n) \mapsto (\lambda_1 x_{\gamma(1)}, \ldots, \lambda_n x_{\gamma(n)})$$

den Code C in C' überführt.

Def. Ein $[n,k]$-Code heißt **systematisch**, falls die ersten k Spalten seiner Generatormatrix die Standardbasisvektoren sind.

Notation. Sei $C \subset \mathbb{F}_q^n$ ein UVR. Für $x, y \in \mathbb{F}_q^n$ schreiben wir

$$x \equiv y \pmod{C} \quad :\iff x - y \in C.$$

Die zu $x \in V$ gehörende Kongruenzklasse modulo C ist $x + C$.

Def. Ein Repräsentantensystem $\mathcal{R}$ dieser Klassen heißt **gewichtsminimal**, falls $\mathrm{wt}(r) = \min_{c \in C} \mathrm{wt}(r+c)$ für alle $r \in \mathcal{R}$.

Satz. Sei C ein $[n,k]$-Code über $\mathbb{F}_q$, $\mathcal{R}$ ein gewichtsmin. Repräsentantensystem mod C. Zu $y \in \mathbb{F}_q^n$ sei $\mathcal{R}(y) \in \mathbb{R}$ mit $\mathcal{R}(y) + C = y + C$. Dann ist $D : \mathbb{F}_q^n \to C$, $y \mapsto y - \mathcal{R}(y)$ eine Decodierabbildung.

Bem. Sei $\mathbb{F}$ ein Körper, $n \in \mathbb{N}^*$. Das Standard-Skalarprodukt

$$(-|-) : \mathbb{F}^n \times \mathbb{F}^n \to \mathbb{F}, \quad (x,y) \mapsto \sum_{i=1}^{n} x_i y_i$$

ist eine nicht-ausgeartete, symmetrische Bilinearform.

Achtung. Es ist $\dim(U^\perp) = n - k$, im Allgemeinen gilt aber $U \cap U^\perp \neq 0$, z. B. ist $11011 \in \mathbb{F}_2^5$ senkrecht zu sich selbst.

Def. Sei C ein $[n,k]$-Code über $\mathbb{F}_q$. Dann heißt $C^\perp$ der zu C gehörende **duale Code**.

Def. Die Generatormatrix H von $C^\perp$ heißt **Kontrollmatrix** zu C.

Lem. $x \in C \iff Hx^T = 0$

Algorithmus. Sei C ein $[n,k]$-Code, $H \in \mathbb{F}_q^{n-k \times n}$ die Kontrollmatrix. Dann ist

$$\psi_H : \mathbb{F}_q^n \to \mathbb{F}_q^{n-k}, \quad x \mapsto Hx^T$$

eine surjektive lineare Abbildung mit $\ker(\psi_H) = C$.

- Sei $c \in C$ gesendet, $y \in \mathbb{F}_q^n$ empfangen, etwa $y = c + e$. Wir als Empfänger kennen jedoch c und e nicht, nur y. Trotzdem können wir das **Syndrom** $s \coloneqq \phi_H(y) = Hc^T + He^T = He^T \in \mathbb{F}_q^{n-k}$ berechnen.
- Wahrscheinlich ist e ein gewichtsminimaler Repräsentant von y. Sei also $\mathcal{R}$ ein minimales Repräsentantensystem. Dann ist $\psi \coloneqq \psi_H|_{\mathcal{R}} : \mathcal{R} \to \mathbb{F}_q^{n-k}$ bijektiv. Dann definiert $D(y) \coloneqq y - \psi^{-1}(s)$ eine Decodierabbildung.

Satz. Sei C ein linearer $[n,k,d]$-Code über $\mathbb{F}_q$, H eine Kontrollmatrix zu C. Dann gilt:

$$\begin{aligned} d &= 1 + \max\{a \in \mathbb{N}^* \mid \text{je } a \text{ Spalten von } H \text{ sind lineare unabhängig}\} \\ &= \min\{m \in \mathbb{N}^* \mid \text{es gibt } m \text{ linear abhängige Spalten in } H\} \end{aligned}$$

Def. Sei C ein linearer Code der Länge n über $\mathbb{F}_q$. Die **Gewichtsverteilung von C** ist $A = A_C \in \mathbb{N}^{\{0,1,\ldots,n\}}$ mit

$$A(i) \coloneqq \{w \in C \mid \mathrm{wt}(w) = i\}, \quad 0 \leq i \leq n.$$

Bem. Es gilt $A_0 = 1$ und $A_1 = A_2 = \ldots = A_{d-1} = 0$, falls d das Minimalgewicht von C ist.

Def. $A_C(Z) \coloneqq \sum_{i=0}^{k} A_i Z^k \in \mathbb{C}[Z]$ heißt **Gewichtszählpolynom**,

$$A_C^{\mathrm{hom}}(X,Y) \coloneqq \sum_{i=0}^{n} A_i X^{n-i} \cdot Y^i \in \mathbb{C}[X,Y]$$

heißt **homogenes Gewichtszählpolynom**.

Bem.
- $A_C(Z) = A_C^{\mathrm{hom}}(1,Z)$
- $A_C^{\mathrm{hom}}(X,Y) = X^n \cdot A_C(\frac{Y}{X})$
- Aus $A_C(X,Y)$ erhält man durch die sogenannte Mac-Williams-Transformation $A_{C^\perp}(X,Y)$

Lem. Sei C ein perfekter (n, M, d)-Code. Dann ist d ungerade.

Bem. Wir betrachten nun perfekte Codes C mit $t = 1$, also $d = 3$. Es gilt dann $|C| = q^n / 1+n(q-1)$, es ist also $1 + n(q-1)$ ein Teiler von q^n. Beispielsweise ist für $q \geq 2$ und $n = q + 1$ die Zahl $1 + n(q-1) = q^2$ ein Teiler von q^n. Diese Teilbarkeit ist eine notwendige, aber nicht hinreichende Bedingung für die Existenz eines perfekten $(n, M, 3)$-Codes über Q mit $q = |Q|$.

Lem. Seien $p, u, v \in \mathbb{N}$, $p \geq 2$. Dann gilt $u|v \iff p^u - 1 | p^v - 1$.

Prop. Sei C perfekt mit $t = 1$ über Q, wobei $|Q| = q$ eine Primzahlpotenz ist. Dann ist $|C|$ eine q-Potenz.

Bem. Sei nun $q \geq 2$ eine Primzahlpotenz, C ein q-närer perfekter $(n, M, 3)$-Code. Dann ist

$$q^k = |C| = M = q^n / 1+n(q-1) \iff n = (q^{n-k} - 1) / q-1$$

Wie viele Lösungspaare (n,k) gibt es bei festem q? Wir setzen $m \coloneqq n - k$. Dann ist $k(m) \coloneqq n - m$ und $n(m) \coloneqq \frac{q^m - 1}{q-1}$. Die Lösungspaare hängen damit nur noch vom Parameter m ab.