Mathematische Grundlagen der digitalen Signalverarbeitung

(Sommersemester 2016)

Grundaufgabe der Signalverarbeitung:

Informationen aus einem physikalischen / gemessenen Signal (wieder-) gewinnen.

Das Gebiet hat sehr viele wissenschaftliche Facetten und noch mehr konkrete Anwendungsbereiche.
In dieser Vorlesung werden wir uns auf 3 Aspekte beschränken; wir nehmen auch an, dass das Signal digital vorliegt und so unmittelbar per Computer weiter verarbeitet werden kann.

A) Codierungstheorie ($\rightsquigarrow$ Kombinatorik, Algebra) ~50%

B) Compressive Sensing ($\rightsquigarrow$ Analysis, Stochastik, Opt.) ~25%

C) Maschinelles Lernen ($\rightsquigarrow$ Stochastik, Opt.) ~25%

Teil A Codierungstheorie

Kapitel 1 Grundlagen

§ 1 Auf geht's

Was ist eine Code?

Sei Q ein Alphabet mit q verschiedenen Symbolen. Eine Teilmenge $C \subseteq Q^n$ heißt Blockcode der Länge n.

Seien $x, y \in Q^n$. Die (Hamming)-Distanz zwischen x und y ist definiert als

$$d(x,y) = |\{ i \in \{1, \ldots, n\} : x_i \neq y_i \}|.$$

Das (Hamming)-Gewicht von x ist

$$w(x) = d(x, 0^n) \quad , \quad \text{falls } 0 \in Q.$$

R. W. Hamming (1915 - 1998): Begründer der algebraischen Codierungstheorie, Originalarbeit "Error Detecting and Error Correcting Code" (1950).

Lemma Die Hamming-Distanz ist eine Metrik auf Q^n.

Bew.: unmittelbares Nachprüfen.

Def.: Die Minimaldistanz eines Blockcodes $C \subseteq Q^n$ ist

$$d(C) = \inf\{d(x,y) : x, y \in C,\ x \neq y\}.$$

Das Minimalgewicht von C ist

$$w(C) = \inf\{d(x, 0^n) : x \in C,\ x \neq 0^n\}, \quad \text{falls } 0 \in Q.$$

C heißt (n, M, d)-Code, falls n die Blocklänge von C ist, falls $M = |C|$ ist, und $d(C) \geq d$ gilt.

Die Informationsrate von C ist

$$R(C) = \frac{\log_q |C|}{n}.$$

Def.: Für $\varrho \in \mathbb{N}$ und $x \in Q^n$ definiere die (Hamming-) Kugel

$$B(x, \varrho) = \{y \in Q^n : d(x,y) \leq \varrho\}$$

um x mit Radius ϱ.

Lemma $|B(x,\varrho)| = \sum_{i=0}^{\varrho} \binom{n}{i} (q-1)^i$.

Bew.: klar.

Satz (Hamming-Schranke / Kugelpackungsschranke)

Sei $C \subseteq Q^n$ ein (n, M, d)-Code. Setze $\varrho = \lfloor \frac{d-1}{2} \rfloor$. Dann gilt

$$M \sum_{i=0}^{\varrho} \binom{n}{i} (q-1)^i \leq q^n. \qquad (*)$$

Bew.: Die Kugeln $B(x,\varrho)$ mit $x \in C$ sind paarweise disjunkt und enthalten $|B(x,\varrho)| = \sum_{i=0}^{\varrho} \binom{n}{i}(q-1)^i$ viele Elemente.

Def.: Ein Code C heißt perfekt, falls in $(*)$ Gleichheit gilt.

Wozu werden Codes verwendet?

C.E. Shannon (1916–2001): Begründer der Informationstheorie. "A Mathematical Theory of Communication" (1948):

The fundamental problem of communication is that of reproducing at one point either exactly or approximately a message selected at another point.