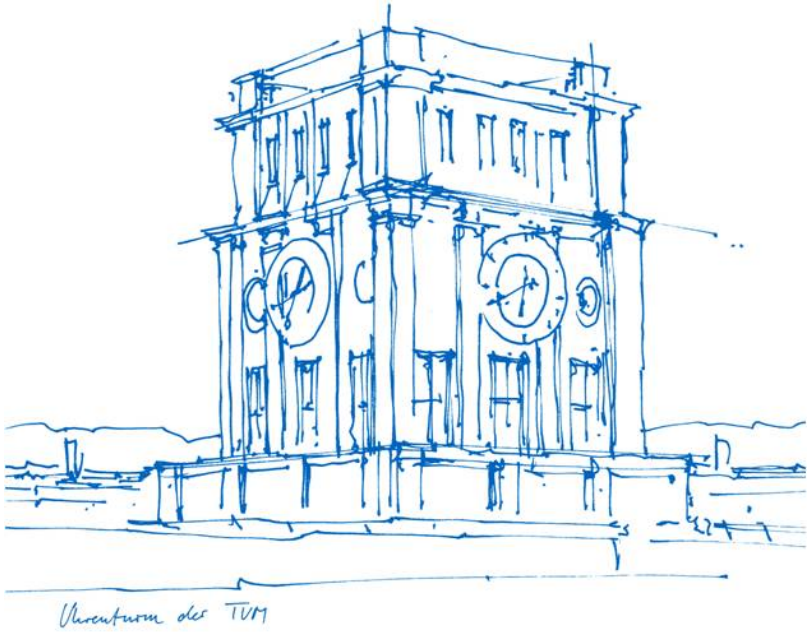
Lineare Algebra für Informatiker – Tutorium KW 21

Jeremias Bohn

Technische Universität München

Fakultät für Mathematik

Garching, 20./21. Mai 2021



Quiz

https://jeremias-bohn.de/la/21/quiz/?quizid=621748855

Lineare Kodierungen

Eine lineare Kodierung wird durch eine Funktion, die **Kodierungsvorschrift**, vorgegeben. Sie bildet einen **Informationswort** auf ein **Codewort** ab. Die Kodierungsvorschrift kann dabei als Matrix geschrieben werden, die sogenannte **Generatormatrix** G.

In der Regel bezeichnen wir die Länge des Informationswortes mit k, die des Codewortes mit n. Eine Kodierung, die solch eine Transformation durchführt, wird auch als $(\boldsymbol{n}, \boldsymbol{k})$**-Code** bezeichnet.

Wichtige Eigenschaften von solchen Codes sind die **Informationsrate** $\frac{k}{n}$ und die **Redundanz** $n - k$.

$C \coloneqq \left\{ G \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_k \end{pmatrix} \middle| \begin{pmatrix} x_1 \\ \vdots \\ x_k \end{pmatrix} \in K^k \right\}$ ist der Unterraum von K^n aller Codewörter beschrieben durch Generatormatrix G.

Hamming-Gewicht und -Abstand

Seien $c, c' \in K^n$ Codewörter.

- Das Hamming-Gewicht eines Codewortes wird beschrieben durch $w(c) \coloneqq |\{i \in \{1, \dots, n\} \mid c_i \neq 0\}|$.
- Der Hamming-Abstand zweier Codewörter ist $d(c, c') \coloneqq |\{i \in \{1, \dots, n\} \mid c_i \neq c_i'\}|$, für den gesamten Raum C $d(C) = \min\{d(c, c') \mid c, c' \in C,\ c \neq c'\}$, also der minimale Abstand zweier Codewörter.

Ein Code heißt ***e*-fehlerkorrigierend**, falls $d(C) = 2e + 1$ gilt und ***e*-fehlererkennend**, wenn $d(C) = e + 1$ gilt.

Parity-Check-Matrix

Sei P die Parity-Check-Matrix zu einem Code definiert durch die Generatormatrix G. Dann gilt:

$$P \cdot G = 0$$

Daraus resultiert $\forall c \in C\colon\ P \cdot c = 0$, denn $\forall c\ \exists x\colon c = G \cdot x$ und damit $P \cdot c = P \cdot G \cdot x = 0 \cdot x = 0$

Für eine Generatormatrix in Standardform

$$G = \begin{pmatrix} I_k \\ A \end{pmatrix} \in K^{n \times k}, A \in K^{(n-k) \times k}$$

definieren wir die Parity-Check-Matrix als

$$P = \begin{pmatrix} -A & I_{n-k} \end{pmatrix} \in K^{(n-k) \times n}$$

Dekodierung

Sei $c' \in K^n$ ein empfangenes Wort. Für $c \in C$, das ursprüngliche Codewort, heißt $f := c' - c$ der **Fehlervektor**. Weiterhin sei das **Syndrom** des empfangenen Wortes c' gegeben durch

$$P \cdot c' = P \cdot (c + f) = 0 + P \cdot f = P \cdot f$$

- Wir suchen nun für die Dekodierung den Fehlervektor mit kleinstmöglichem Hamming-Gewicht (und damit den wahrscheinlichsten):

$$f' = \arg\min_f \{w(f) \mid P \cdot f = P \cdot c'\}$$

- Das wahrscheinliche Codewort ist dann $c'' = c' - f'$, das wahrscheinliche Informationswort die Lösung für

$$G \cdot x = c''$$