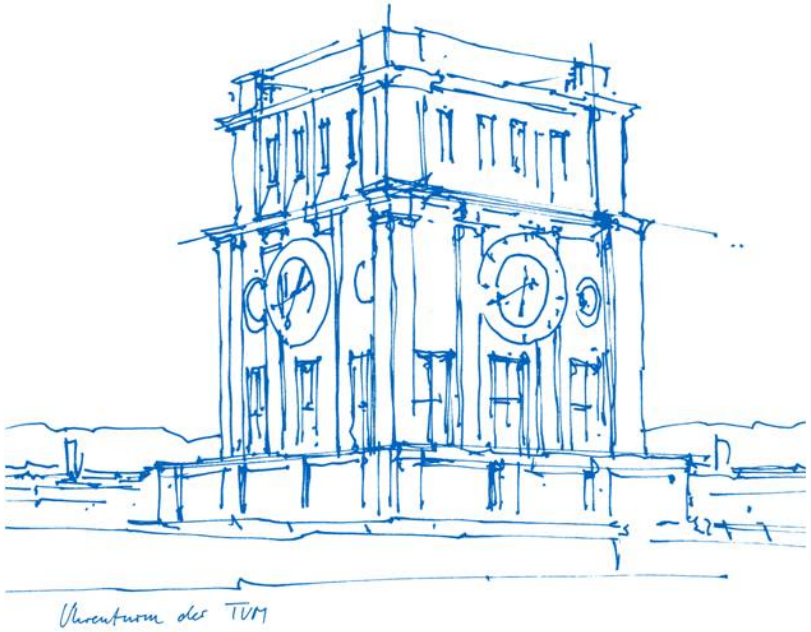
Lineare Algebra für Informatiker – Tutorium KW 21

Jeremias Bohn

Technische Universität München

Fakultät für Mathematik

Garching, 25. Mai 2020



Hausaufgabenbesprechung

- H7: Aus $U = \left\{ \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} \in \mathbb{R}^4 \;\middle|\; x_1 - 2x_2 + x_3 - x_4 \right\}$ folgt nicht $U = \left\langle \begin{pmatrix} 1 \\ -2 \\ 1 \\ -1 \end{pmatrix} \right\rangle$ oder dergleichen!
- H8 a): Der Schritt, wenn ihr $\lambda f \in U$ zeigen wollt, ist $(\lambda f)(x) = \lambda \cdot f(x) = \cdots$, damit erkenntlich ist, dass ihr λf berechnet
- H8 b): Für $\mathrm{G} + U$ reicht es nicht, die allgemeine Formel aufzuschreiben. Macht euch vorher Gedanken, wie eine Funktion, die darin liegt, aussehen könnte und zeigt dann, dass dieses Schema gilt.

Dimension

Die Dimension eines Raumes ist gegeben durch die Anzahl der Achsen, die ihn aufspannen

Allgemein gilt: Die Dimension eines Raumes ist die Mächtigkeit seiner Basis.

Für zwei Unterräume $U, W \subseteq V$ gilt zudem die Dimensionsformel

$$\dim(U + W) = \dim(U) + \dim(W) - \dim(U \cap W)$$

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^k 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 $\boldsymbol{e}$**-fehlerkorrigierend**, falls $d(C) = 2e + 1$ gilt und e-fehlerkorrigierend und $(\boldsymbol{e + 1})$-**fehlererkennend**, wenn $d(C) = 2(e + 1) = 2e + 2$ gilt.

Parity-Check-Matrix und Dekodierung

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

$$P \cdot G = 0$$

wobei 0 der Nullmatrix entspricht.

Daraus resultiert $\forall c \in C\colon\ P \cdot c = 0$.

Für eine Generatormatrix in Standardform

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

definieren wir die Parity-Check-Matrix als

$$P = (-A \quad I_{n-k}) \in K^{(n-k) \times n}$$

Dekodierung

Sei $c' \in K^n$ ein empfangenes Wort. Für $c \in C$, das ursprüngliche Codewort, heißt $f \coloneqq c' - c$ 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

$$f' = \underset{f, P \cdot f' = P \cdot c'}{\arg\min} w(f)$$

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

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