

ANALYSIS (MEHRDIMENSIONAL)

Gradient & Hesse-Matrix: Für $f: \mathbb{R}^n \rightarrow \mathbb{R}$:

- **Gradient:** $\nabla f(x) = (\partial_1 f, \dots, \partial_n f)^T$
- **Hesse-Matrix:** $H_f(x) = \left(\frac{\partial^2 f}{\partial x_i \partial x_j} \right)_{i,j}$

(Symmetrisch nach Satz von Schwarz)

Stationäre Punkte & Extrema

1. **Notwendig:** Berechne $\nabla f(x) = 0$. Löse LGS.
2. **Hinreichend:** Prüfe Definitheit von $H_f(x_0)$.

Definitheit der Hesse-Matrix $H_{f(x_0)}$:

- **Positiv definit** (> 0): **Lokales Minimum**
- **Negativ definit** (< 0): **Lokales Maximum**
- **Indefinit:** **Sattelpunkt**

Hurwitz-Kriterium (Definitheit)

Für symmetrische Matrix $A \in \mathbb{R}^{n \times n}$. Betrachte Hauptminoren D_k (Det. der oberen linken $k \times k$ Untermatrix).

- **Pos. Def.:** Alle $D_k > 0$ ($D_1 > 0, D_2 > 0, \dots$)
- **Neg. Def.:** Vorzeichenwechsel beginnend mit Minus ($- + - + \dots$), d.h. $D_1 < 0, D_2 > 0, D_3 < 0, \dots$
- **Indefinit:** $\det(A) \neq 0$, aber kein Muster oben passt.
- **Semidefinit:** Wenn $\det(A) = 0$ (Eigenwerte prüfen!).

Spezialfall 2×2 : $H_f = \begin{pmatrix} f_{xx} & f_{xy} \\ f_{yx} & f_{yy} \end{pmatrix}$

- $\det(H) > 0$ und $f_{xx} > 0 \Rightarrow$ Minimum.
- $\det(H) > 0$ und $f_{xx} < 0 \Rightarrow$ Maximum.
- $\det(H) < 0 \Rightarrow$ Sattelpunkt.

Richtungsableitung

Ableitung in Punkt x in Richtung v (v muss normiert sein!)
 $\|v\| = 1$):

$$\frac{\partial f}{\partial v}(x) = \nabla f(x) \cdot \frac{v}{\|v\|}$$

Konvexität

- f konvex $\Leftrightarrow H_{f(x)}$ positiv (semi-)definit für alle x .
- f konkav $\Leftrightarrow H_{f(x)}$ negativ (semi-)definit für alle x .
- S konvex: Verbindungslinie zweier Punkte liegt in S .

ZAHLENTHEORIE

Modulo-Rechnung

$\mathbb{Z}_n = \{0, \dots, n-1\}$. Rechnen mit Rest.

- **Einheiten $\mathbb{Z}_n^*$:** Elemente $a \in \mathbb{Z}_n$ mit $\text{ggT}(a, n) = 1$.
- **Euler $\varphi(n)$:** Anzahl der Einheiten.
 - p prim: $\varphi(p) = p-1$.
 - $n = p \cdot q$: $\varphi(n) = (p-1)(q-1)$.
 - $n = p^k$: $\varphi(p^k) = p^k - p^{k-1}$.

Wichtige Sätze

Kleiner Fermat: p prim, a kein Vielfaches:

$$a^{p-1} \equiv 1 \pmod{p}$$

Satz von Euler: $\text{ggT}(a, n) = 1$:

$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

- **Anwendung (Inverse):** In $\mathbb{Z}_n$ ist $a^{-1} = a^{\varphi(n)-1} \pmod{n}$.
- **Schnelle Exponentiation:**

Berechne $b^e \pmod{m}$.

1. Exponent e binär schreiben.
2. Quadrieren und bei 1 multiplizieren (Square & Multiply).
3. Oder: e reduzieren modulo $\varphi(m)$ (falls Basis b teilerfremd zu m !).

Euklidischer Algorithmus (ggT)

Zur Berechnung von $\text{ggT}(a, b)$ und s, t mit $\text{ggT}(a, b) = s \cdot a + t \cdot b$.

Beispiel $\text{ggT}(12, 7)$: $12 = 1 \cdot 7 + 5 \Rightarrow 5 = 12 - 1 \cdot 7$ $7 = 1 \cdot 5 + 2 \Rightarrow 2 = 7 - 1 \cdot 5 = 7 - (12 - 7) = 2 \cdot 7 - 1 \cdot 12$ $5 = 2 \cdot 2 + 1 \Rightarrow 1 = 5 - 2 \cdot 2 = (12 - 7) - 2(2 \cdot 7 - 1 \cdot 12) = 3 \cdot 12 - 5 \cdot 7 \Rightarrow 1 = 3 \cdot 12 + (-5) \cdot 7$. Inverse von 7 mod 12 ist -5 (=7).

Chinesischer Restsatz (CRT)

Löse System: $x \equiv a_i \pmod{m_i}$ (moduli m_i paarweise teilerfremd).

$M = \prod m_i$, $M_i = \frac{M}{m_i}$. Löse $M_i y_i \equiv 1 \pmod{m_i}$ (Inverse von M_i).

Lösung: $x = \sum_i a_i M_i y_i \pmod{M}$.

LINEARE ALGEBRA: MATRIZEN

Matrizen & LGS

$A \in K^{m \times n}$. LGS $Ax = b$. **Gauß-Verfahren:** Auf Zeilenstufenform bringen.

- Rang r : Anzahl der Stufen (Nicht-Null-Zeilen).
- $r = n$: Eindeutige Lsg. (bei hom. nur 0).
- $r < n$: Unendlich viele Lsg. ($n-r$ Parameter frei).
- $r < m$: Lösbar nur wenn Nullzeilen rechts 0 sind.

Determinante (nur $n \times n$)

- $\det(A) \neq 0 \Leftrightarrow A$ invertierbar $\Leftrightarrow \text{Rang}(A) = n$.
- 2×2 : $\det \begin{pmatrix} a & b \\ c & d \end{pmatrix} = ad - bc$.
- 3×3 : Sarrus (Jägerzaun).
- $n \times n$: Laplace (Entwicklung nach Zeile/Spalte mit vielen 0).
- Regeln: $\det(AB) = \det A \det B$, $\det(A^T) = \det A$.
- $\det(\lambda A) = \lambda^n \det A$.

Inverse Matrix

A^{-1} existiert nur wenn $\det A \neq 0$.

- 2×2 : $A^{-1} = \frac{1}{\det A} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$.
- Allgemein: Gauß $(A \mid I_n) \rightarrow (I_n \mid A^{-1})$.

LINEARE ABBILDUNGEN

$\varphi: V \rightarrow W$ linear ($\varphi(v+w) = \varphi(v) + \varphi(w)$, $\varphi(cv) = c\varphi(v)$).

- **Bild:** Spaltenraum der Matrix A . $\dim(\text{Bild}) = \text{Rang}(A)$.
- **Kern:** Lösungsraum von $Ax = 0$.

Dimensionssatz:

$$\dim(V) = \dim(\text{Kern}(\varphi)) + \dim(\text{Bild}(\varphi))$$

$$n = \text{Anzahl freie Parameter} + \text{Rang}(A)$$

- **Injektiv:** $\text{Kern}(\varphi) = \{0\}$.
- **Surjektiv:** $\text{Bild}(\varphi) = W$ (Rang = Zeilenzahl).
- **Bijektiv:** $n = m$ und Determinante $\neq 0$.

Abbildungsmatrix

$M_B^{C(\varphi)}$: Matrix bzgl. Basis B (Start) und C (Ziel). Spalten sind Bilder der Basisvektoren von B , dargestellt in C .

$$\text{Spalte } j = \varphi(b_j)_C$$

Basiswechsel: $M_B^{C(1)}$ transformiert von B nach C . $A' = T^{-1}AT$ (wenn T Transformationsmatrix).

EIGENWERTE (EW) & DIAGONALISIERUNG

1. **Charakteristisches Polynom:** $P_{A(\lambda)} = \det(A - \lambda I) = 0$.
2. Nullstellen sind EW λ_i .
 - **Alg. Vielfachheit:** Potenz im Polynom.
 - **Geom. Vielfachheit:** $\dim(\text{Kern}(A - \lambda_i I)) = n - \text{Rang}(A - \lambda_i I)$.
3. **Eigenraum:** $E_\lambda = \text{Kern}(A - \lambda I)$ (LGS lösen).

Diagonalisierbar gdw:

1. P_A zerfällt komplett in Linearfaktoren.
2. Für jeden EW gilt: **Alg. VFH = Geom. VFH**.

Symmetrische Matrizen sind **immer** diagonalisierbar!

Matrix $D = S^{-1}AS$ (Diagonalmatrix mit EW). S : Spalten sind die Eigenvektoren.

Spektralsatz (Symmetrische Matrizen)

Ist $A = A^T$, dann:

- Alle EW sind reell.
- A ist orthogonal diagonalisierbar: $D = Q^T A Q$ mit $Q^T = Q^{-1}$.
- Eigenvektoren zu versch. EW sind **orthogonal**.

EUKLIDISCHE VEKTORRÄUME

Skalarprodukt & Norm

Standard $\mathbb{R}^n$: $\langle u, v \rangle = u^T v = \sum u_i v_i$.

- Norm: $\|u\| = \sqrt{\langle u, u \rangle}$.
- Winkel: $\cos \alpha = \frac{\langle u, v \rangle}{\|u\| \cdot \|v\|}$.
- Orthogonal: $\langle u, v \rangle = 0$.

Gram-Schmidt (ONB)

Aus Basis $v_1, \dots, v_n$ mache Orthonormalbasis $b_1, \dots, b_n$.

1. $u_1 = v_1$, dann $b_1 = \frac{u_1}{\|u_1\|}$.
2. $u_2 = v_2 - \langle v_2, b_1 \rangle b_1$, dann $b_2 = \frac{u_2}{\|u_2\|}$.
3. $u_k = v_k - \sum_{j=1}^{k-1} \langle v_k, b_j \rangle b_j$.
4. $b_k = \frac{u_k}{\|u_k\|}$.

Orthogonale Matrizen Q

$Q^T Q = I$ ($Q^{-1} = Q^T$). Spalten bilden ONB. Längentreu ($\|Qx\| = \|x\|$) und winkeltreu. Determinante ist ± 1 .

- **Drehmatrix (2D):** $\begin{pmatrix} \cos \alpha & -\sin \alpha \\ \sin \alpha & \cos \alpha \end{pmatrix}$.
- **Drehmatrix (3D):** Drehung um Achse a . Ein EW ist 1 (Achse). Spur ist $1 + 2\cos(\alpha)$.

KODIERUNGSTHEORIE

Lineare Codes $C \subset \mathbb{R}^n$ (meist $\mathbb{F}_2, \mathbb{F}_3, \mathbb{F}_5$). Parameter $[n, k, d]$: Länge n , Dimension k , Minimaldistanz d .

Erzeugermatrix G ($k \times n$)

Zeilen bilden Basis von C . G in Stufenform bringen um Dimension zu sehen. Standardform: $G = (I_k | A)$. Codierung: $x \rightarrow xG$.

Prüfmatrix H ($(n-k) \times n$)

Es gilt: $GH^T = 0$. Wenn $G = (I_k | A)$, dann $H = (-A^T | I_{n-k})$. (Im Binären ist $-A = A$, also $H = (A^T | I_{n-k})$). Code ist Kern von H : $c \in C \Leftrightarrow Hc^T = 0$.

Minimaldistanz & Fehler

- **Hamming-Gewicht** $w(x)$: Anzahl Einträge $\neq 0$.
- **Minimaldistanz** $d_{\min} = \min\{w(c) \mid c \in C, c \neq 0\}$.
- $d_{\min}$ ist auch das minimale Gewicht der Spalten von H , die linear abhängig sind (oft die kleinste Anzahl linear abh. Spalten).

Erkennung: $d-1$ Fehler erkennbar. **Korrektur:** $e = \lfloor \frac{d-1}{2} \rfloor$ Fehler korrigierbar. ($d=3 \Rightarrow 1$ Fehler, $d=5 \Rightarrow 2$ Fehler)

Dekodierung (Syndrom)

Empfangenes Wort $r = c + e$ (Code + Fehler).

1. Berechne **Syndrom** $S = Hr^T$.
2. Wenn $S = 0 \Rightarrow$ kein Fehler.
3. Wenn $S \neq 0$: Suche Spalte in H , die Vielfaches von S ist.
 - Position der Spalte = Position des Fehlers.
 - Wert des Fehlers aus Faktor bestimmen.

ALGEBRAISCHE STRUKTUREN

Gruppen $(G, \cdot)$: Assoziativ, Neutrales e , Inverses a^{-1} .

- **Abelsch:** + Kommutativ.
- **Zyklisch:** Ein Erzeuger g generiert ganze Gruppe (g^k). $\mathbb{Z}_n$ ist zyklisch (Erzeuger 1).
- **Ordnung:** $|G|$ Anzahl Elemente. Satz von Lagrange: $|U|$ teilt $|G|$.

Untergruppen: Teilmenge, abgeschlossen bzgl. Op. und Inverse. **Isomorphie:** $\mathbb{Z}_{nm} \cong \mathbb{Z}_n \times \mathbb{Z}_m$ gdw. $\text{ggT}(n, m) = 1$.

Körper $(K, +, \cdot)$: $(K, +)$ abelsche Grp, $(K \setminus \{0\}, \cdot)$ abelsche Grp, Distributiv. Beispiele: $\mathbb{R}, \mathbb{Q}, g, \mathbb{Z}_p$ (p prim). $\mathbb{Z}_n$ ist kein Körper wenn n nicht prim (Nullteiler!).

Polynomring $K[x]$: Division mit Rest möglich.

DIVERSES & TIPPS

- **LGS lösen:** Immer Gauß. Nie Cramer (zu langsam).
- **Komplexe Zahlen:** $i^2 = -1$. $z = a + bi$. $\overline{z} = a - bi$. $|z|^2 = z \overline{z} = a^2 + b^2$. Polarkoordinaten $re^{i\varphi}$.
- **Nilpotent:** $A^k = 0$. Einziger EW ist 0. Spur ist 0. Nicht invertierbar.
- **Äquivalenzrelation:** Reflexiv ($x \sim x$), Symmetrisch ($x \sim y \Rightarrow y \sim x$), Transitiv ($x \sim y, y \sim z \Rightarrow x \sim z$). Äquivalenzklassen bilden Partition.
- **Injektiv:** Kern = $\{0\}$. **Surjektiv:** Bild = Zielraum.