Orthogonalität

Erinnerung:

Zwei Vektoren eines euklidischen Vektorraumes $(V, \langle\cdot,\cdot\rangle)$ heißen **orthogonal**, falls $\langle\vec{u},\vec{v}\rangle = 0$ gilt.

Schreibweise: $\vec{u} \perp \vec{v}$.

Ein Vektor $\vec{v}$ heißt **orthogonal zu einem Unterraum** U von V, falls für alle $\vec{u} \in U$ gilt:

$$\langle\vec{u},\vec{v}\rangle = 0.$$

Schreibweise: $\vec{v} \perp U$.

Das **orthogonale Komplement** eines Unterraumes U von V ist die Menge

$$U^{\perp} := \{\vec{v} \in V \mid \vec{v} \perp U\}\ .$$

<u>Theorem 31:</u> Zu jedem Unterraum U von V ist $U^{\perp}$ wieder ein Unterraum von V.

Anwendung: Linearcodes

Nachrichtenmenge: $\mathbb{K}^k$ ... k-dimensionaler Vektorraum über dem Körper $\mathbb{K}$.

Ein (n,k)-Linearcode ist

eine injektive lineare Abbildung $f_c : \mathbb{K}^k \to \mathbb{K}^n$

bzw. der zugehörige k-dimensionale Unterraum $C := f_c(\mathbb{K}^k)$ von $\mathbb{K}^n$.

f_c wird durch eine $(n \times k)$-Matrix A (Standardmatrix) beschrieben:

$$A \begin{pmatrix} v_1 \\ \vdots \\ v_k \end{pmatrix} = \begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix} \quad \text{bzw.} \quad \underbrace{(c_1 \ \dots \ c_n) = (v_1 \ \dots \ v_k) A^T}_{\textit{Wortschreibweise}}$$

$G := A^T$ heißt **Generatormatrix** des Linearcodes C.

Anwendung: Linearcodes

Betrachten das Skalarprodukt $\quad (c_1 \ \dots \ c_n) \bullet (d_1 \ \dots \ d_n) = \sum_{k=1}^{n} c_k \cdot d_k \ .$

Es hat auf einem beliebigen Körper i.a. nur die Eigenschaften (S1) und (S2).
(Der Begriff wird auch teilweise ohne Eigenschaft (S3) definiert.)

Für das orthogonale Komplement $C^\perp$ des Linearcodes $C \subset \mathbb{K}^n$ gilt dann

- $C^\perp$ ist ein Unterraum von $\mathbb{K}^n$.
- $\dim C^\perp = n - k$.
- $C^\perp$ kann als $(n, n-k)$-Linearcode aufgefasst werden.

$\Rightarrow$ Es gibt eine $(n - k \times n)$-Generatormatrix H von $C^\perp$, und:

$$\forall \ \underline{c} = (c_1 \ \dots \ c_n) \in C : \quad \underline{c} H^T = 0.$$

H heißt **Kontrollmatrix** zum Linearcode C.

Orthogonale Mengen

Es sei $(V, \langle \cdot, \cdot \rangle)$ ein euklidischer Vektorraum über $\mathbb{R}$.

Eine Menge von Vektoren $\{\vec{u}_1, \ldots, \vec{u}_k\}$ aus V heißt **orthogonal**, falls

$$\langle \vec{u}_i, \vec{u}_j \rangle = 0 \qquad \text{für alle } i \neq j,\ i, j \in \{1, \ldots, k\}.$$

Eine Menge von Vektoren $\{\vec{u}_1, \ldots, \vec{u}_k\}$ aus V heißt **orthonormal**, falls

- sie orthogonal ist und
- $\|\vec{u}_j\| = \sqrt{\langle \vec{u}_j, \vec{u}_j \rangle} = 1$ für $j = 1, \ldots, k$.

<u>Theorem 32:</u> Jede orthogonale Menge von Nichtnull-Vektoren $\{\vec{u}_1, \ldots, \vec{u}_k\}$ eines euklidischen Vektorraumes $(V, \langle \cdot, \cdot, \rangle)$ ist linear unabhängig.

Eine **Orthogonalbasis** eines euklidischen Vektorraumes $(V, \langle \cdot, \cdot, \rangle)$ ist eine Basis von V, die eine orthogonale Menge ist.

Eine **Orthonormalbasis** von V ist eine Basis von V, die eine orthonormale Menge ist.

Darstellung in Koordinaten einer Orthogonalbasis

Theorem 33: Es sei $\mathcal{B} = \{\vec{u}_1, \ldots, \vec{u}_n\}$ eine Orthogonalbasis von $(V, \langle \cdot, \cdot, \rangle)$.

Dann hat jeder Vektor $\vec{v} \in V$ in $\mathcal{B}$ die eindeutige Koordinatendarstellung

$$\vec{v} = c_1 \vec{u}_1 + \ldots + c_n \vec{u}_n \qquad \text{mit} \qquad c_j = \frac{\langle \vec{v}, \vec{u}_j \rangle}{\langle \vec{u}_j, \vec{u}_j \rangle}, \quad j = 1, \ldots, n\,.$$

Ist $\mathcal{B} = \{\vec{u}_1, \ldots, \vec{u}_n\}$ sogar eine Orthonormalbasis, so gilt

$$c_j = \langle \vec{v}, \vec{u}_j \rangle, \; j = 1, \ldots, n\,.$$

In diesem Fall ist $\langle \vec{v}, \vec{u}_j \rangle$ gerade die **orthogonale Projektion** von $\vec{v}$ in Richtung des Vektors $\vec{u}_j$.

Best-Approximation

Es sei U ein Unterraum eines euklidischen Vektorraumes $(V, \langle \cdot, \cdot, \rangle)$.

Theorem 34: (Orthogonale Zerlegung)

Jeder Vektor $\vec{y} \in V$ kann eindeutig zerlegt werden in

$$\vec{y} = \hat{\vec{y}} + \vec{z}$$

mit $\hat{\vec{y}} \in U$ und $\vec{z} \in U^{\perp}$.

Bezeichnung: $\mathbf{proj}_{\boldsymbol{U}}(\vec{\boldsymbol{y}}) := \hat{\vec{\boldsymbol{y}}}$ heißt **orthogonale Projektion von $\vec{\boldsymbol{y}}$ auf $\boldsymbol{U}$**.

Bestapproximation:

Für jedes $\vec{y} \in V$ ist $\mathrm{proj}_U(\vec{y})$ der zu $\vec{y}$ nächstgelegene Punkt in U bzgl. der zugeordneten euklidischen Norm:

$$\|\vec{y} - \mathrm{proj}_U(\vec{y})\| \leq \|\vec{y} - \vec{u}\| \quad \text{für alle } \vec{u} \in U\,.$$

Der Gram-Schmidt-Prozess

Algorithmus, der aus einer gegebenen Basis eines Unterraumes U eines euklidischen Vektorraumes $(V, \langle\cdot,\cdot,\rangle)$ eine orthogonale Basis konstruiert.

Es sei $\{\vec{b}_1, \ldots, \vec{b}_k\}$ eine Basis von U.

Schrittweise Konstruktion einer Orthogonalbasis $\{\vec{u}_1, \ldots, \vec{u}_k\}$ von U:

- $\vec{u}_1 := \vec{b}_1$ $\qquad W_1 := \mathrm{Span}(\{\vec{u}_1\})$
- $\vec{u}_2 := \vec{b}_2 - \mathrm{proj}_{W_1}(\vec{b}_2)$ $\qquad W_2 := \mathrm{Span}(\{\vec{u}_1, \vec{u}_2\})$

$\vdots \qquad \vdots$

- $\vec{u}_{k-1} := \vec{b}_{k-1} - \mathrm{proj}_{W_{k-2}}(\vec{b}_{k-1})$ $\qquad W_{k-1} := \mathrm{Span}(\{\vec{u}_1, \ldots, \vec{u}_{k-1}\})$
- $\vec{u}_k := \vec{b}_k - \mathrm{proj}_{W_{k-1}}(\vec{b}_k)$

$$= \vec{b}_k - \frac{\langle\vec{b}_k,\vec{u}_1\rangle}{\langle\vec{u}_1,\vec{u}_1\rangle}\,\vec{u}_1 - \ldots - \frac{\langle\vec{b}_k,\vec{u}_{k-1}\rangle}{\langle\vec{u}_{k-1},\vec{u}_{k-1}\rangle}\,\vec{u}_{k-1}$$