

Bild 6.8: Orthogonale Projektion $\mathbf{u} = \text{proj}_U(\mathbf{x})$ von \mathbf{x} auf U .

zufolge hat. Damit lässt sich jeder Vektor $\mathbf{x} \in V$ *eindeutig* als Summe

$$\mathbf{x} = \mathbf{u} + \mathbf{w} \quad \text{mit } \mathbf{u} \in U \text{ und } \mathbf{w} \in U^\perp$$

darstellen. Der Vektor $\mathbf{u} = \mathbf{x} - \mathbf{w}$ heißt dann die *Projektion* (oder *orthogonale Projektion*) von \mathbf{x} auf U und wird mit $\mathbf{u} = \text{proj}_U(\mathbf{x})$ bezeichnet (siehe Bild 6.8).

Beispiel 6.28: Projektionen und die Kommunikationskomplexität

Zwei weit entfernt lebende Spieler besitzen zwei große Datenbanken (zwei lange Vektoren) $\mathbf{v}_1, \mathbf{v}_2 \in \mathbb{R}^n$ und wollen bestimmen, ob $\mathbf{v}_1 = \mathbf{v}_2$ gilt. Eine Möglichkeit wäre, dass der erste Spieler seinen ganzen Vektor \mathbf{v}_1 verschickt. Die Kommunikation ist aber teuer: Für jede verschickte reelle Zahl muss man, sagen wir, 1 € zahlen. Deshalb ist diese Lösung sehr teuer: Man müsste insgesamt n € bezahlen. (Man kann zeigen, dass es in einer solchen Situation, in der nur zwei Spieler vorhanden sind, auch nicht billiger geht.) Wir nehmen deshalb an, dass es noch einen dritten Spieler gibt, der die Projektion $\text{proj}_U(\mathbf{v}) = (\mathbf{x}, \mathbf{x})$ von $\mathbf{v} = (\mathbf{v}_1, \mathbf{v}_2)$ auf den Vektorraum $U = \{(\mathbf{u}, \mathbf{u}) : \mathbf{u} \in \mathbb{R}^n\}$ erhält.

Wie sieht denn die Projektion $\text{proj}_U(\mathbf{v})$ aus? Ein Vektor (\mathbf{y}, \mathbf{z}) gehört zu U^\perp genau dann, wenn $\langle (\mathbf{u}, \mathbf{u}), (\mathbf{y}, \mathbf{z}) \rangle = 0$ und somit auch $\langle \mathbf{u}, \mathbf{z} \rangle = -\langle \mathbf{y}, \mathbf{u} \rangle$ für *alle* Vektoren $\mathbf{u} \in \mathbb{R}^n$ gilt. Da dies insbesondere auch für die Einheitsvektoren $\mathbf{e}_i = (0, \dots, 0, 1, 0, \dots, 0)$ gelten muss, besteht der Orthogonalraum U^\perp aus allen Vektoren $(\mathbf{y}, -\mathbf{y})$ mit $\mathbf{y} \in \mathbb{R}^n$. Daher ist $(\mathbf{v}_1, \mathbf{v}_2) = (\mathbf{x}, \mathbf{x}) + (\mathbf{y}, -\mathbf{y})$ für ein $\mathbf{y} \in \mathbb{R}^n$. Der Vektor \mathbf{y} ist aber keinem der Spieler bekannt: Der erste Spieler kennt nur $\mathbf{v}_1 = \mathbf{x} + \mathbf{y}$, der zweite Spieler kennt nur $\mathbf{v}_2 = \mathbf{x} - \mathbf{y}$, und der dritte Spieler kennt nur \mathbf{x} . Sie müssen also entscheiden, ob $\mathbf{y} = \mathbf{0}$ gilt. Es ist interessant, dass nun 6 € völlig ausreichen: Nur die Zahlen $\|\mathbf{v}_1\|$, $\|\mathbf{v}_2\|$ und $\|\mathbf{x}\|$ müssen kommuniziert werden! Es gilt nämlich

$$\|\mathbf{x}\| = \|\mathbf{x} - \mathbf{y}\| = \|\mathbf{x} + \mathbf{y}\| \iff \mathbf{y} = \mathbf{0}.$$

Beweis: Die Richtung (\Leftarrow) ist trivial. Nehmen wir nun an, dass $\|\mathbf{x}\| = \|\mathbf{x} - \mathbf{y}\| = \|\mathbf{x} + \mathbf{y}\|$ gilt. Dann gilt auch

$$\begin{aligned} \|\mathbf{x}\|^2 &= \|\mathbf{x} - \mathbf{y}\|^2 = \langle \mathbf{x} - \mathbf{y}, \mathbf{x} - \mathbf{y} \rangle = \|\mathbf{x}\|^2 - 2\langle \mathbf{x}, \mathbf{y} \rangle + \|\mathbf{y}\|^2, \\ \|\mathbf{x}\|^2 &= \|\mathbf{x} + \mathbf{y}\|^2 = \langle \mathbf{x} + \mathbf{y}, \mathbf{x} + \mathbf{y} \rangle = \|\mathbf{x}\|^2 + 2\langle \mathbf{x}, \mathbf{y} \rangle + \|\mathbf{y}\|^2. \end{aligned}$$

Aufaddiert erhalten wir $2\|\mathbf{x}\|^2 = 2\|\mathbf{x}\|^2 + 2\|\mathbf{y}\|^2$, woraus $\|\mathbf{y}\| = 0$ und somit auch $\mathbf{y} = \mathbf{0}$ folgt, da \mathbb{R}^n ein euklidischer Vektorraum ist. \square

Der euklidische Abstand zwischen zwei Vektoren \mathbf{x} und \mathbf{y} wird als $\|\mathbf{x} - \mathbf{y}\|$ definiert.