

# Das **A''**alto

## Wörterbuch des Maschinellen Lernens

Alexander Jung and Konstantina Olioumtsevit

3. Juni 2025



please cite as: A. Jung and K. Olioumtsevit “The Aalto Dictionary of  
Machine Learning,” Aalto University, 2024.

### **Zusammenfassung**

Dieses Wörterbuch des Maschinellen Lernens entstand während der Entwicklung und Umsetzung der Kurse CS-E3210 **Machine Learning: Basic Principles**, CS-C3240 **Machine Learning**, CS-E4800 **Artificial Intelligence**, CS-EJ3211 **Machine Learning with Python**, CS-EJ3311 **Deep Learning with Python**, CS-E4740 **Federated Learning** und CS-E407507 **Human-Centered Machine Learning**. Diese Kurse wurden über die **Aalto-Universität** <https://www.aalto.fi/de>, über das **Finnish Institute of Technology (FITech)** <https://fitech.io> und die **Europäische Universitätsallianz Unite!** <https://www.aalto.fi/de/unite> angeboten.

## Glossar

**Daten** Ein Datensatz (Daten) besteht aus einem oder mehreren Datenpunkten und ist eine zentrale Komponente der meisten KI Anwendungen. Diese Anwendungen verwenden Datensätze zum Trainieren und Validieren von KI-Modellen. Verschiedene mathematische Modelle und formale Sprachen wurden entwickelt um Datensätze zu beschreiben und zu analysieren [?, ?, ?, ?]. Eines der am weitesten verbreiteten Datenmodelle ist das relationale Modell, das Daten in Tabellen (oder Beziehungen) organisiert [?]. Eine Tabelle besteht aus Zeilen und Spalten:

- Jede Zeile der Tabelle repräsentiert einen einzelnen Datenpunkt.
- Jede Spalte der Tabelle entspricht einem bestimmten Attribut (oder Merkmal) der Datenpunkte.

Tabelle 1 zeigt beispielsweise einen Datensatz mit Wetterbeobachtungen. Im relationalen Modell ist die Reihenfolge der Zeilen irrelevant und für jedes Attribut (Spalte) muss ein Wertebereich definiert sein. Diese Wertebereiche entsprechen dem Merkmalsraum der Datenpunkte. Während das relationale Modell ein nützliches Instrument für die Beschreibung und Analyse von KI System bietet, ist es unzureichend für die Dokumentation von vertrauenswürdiger KI. Moderne Ansätze wie Datenblätter für Datensätze bieten eine umfassendere Dokumentation, einschließlich Details zum Erfassungsprozess des Datensatzes und zur

FMI Station	Year	Month	Day	Time	Temp. [°C]
Kustavi Isokari	2023	4	1	00:00	-0.2
Kustavi Isokari	2023	4	2	00:00	-0.1
Kustavi Isokari	2023	4	3	00:00	-1.0
Kustavi Isokari	2023	4	4	00:00	-0.4
Kustavi Isokari	2023	4	5	00:00	0.9

Tabelle 1: Beobachtungen der Wetter-Station nahe der finnischen Gemeinde *Kustavi*.

beabsichtigten Verwendung [?].

**Diskrepanz** Consider an ?? application with ?? represented by an ??. ?? methods use a discrepancy measure to compare ?? maps from ??s at nodes  $i, i'$  connected by an edge in the ??.

**FedAvg** An ?? ?? using a server-client setting.

See also: ??, ??.

**FedGD** An ?? ?? that can be implemented as message passing across an ??.

See also: ??, ??, ??, ??.

**FedRelax** An ?? ??.

See also: ??, ??.

**FedSGD** An ?? ?? that can be implemented as message passing across an ??.

See also: ??, ??, ??, ??, ??.

**Klassifizierung** Klassifizierung bezeichnet ML Anwendungen die darauf abzielen, Datenpunkte in eine von mehreren vorgegebenen Kategorien oder Klassen einzuordnen.

**Optimismus im Angesicht der Unsicherheit** ML-Methoden verwenden ein Leistungsmaß  $\bar{f}(\mathbf{w})$  um Modell-Parameter  $\mathbf{w}$  zu lernen. Allerdings haben sie in der Regel keinen direkten Zugriff auf  $\bar{f}(\mathbf{w})$ , sondern nur auf eine Schätzung (oder Annäherung)  $f(\mathbf{w})$ . Zum Beispiel verwenden herkömmliche ML Methoden einen Trainingsfehler als Schätzung für den erwarteten Verlust. Mit einem probabilistischen Modell lässt sich ein Konfidenzintervall  $[l^{(\mathbf{w})}, u^{(\mathbf{w})}]$  für jede Wahl von Modellparametern konstruieren. Eine einfache Konstruktion hierfür ist  $l^{(\mathbf{w})} := f(\mathbf{w}) - \sigma/2$ ,  $u^{(\mathbf{w})} := f(\mathbf{w}) + \sigma/2$ , wobei  $\sigma$  ein Maß für die (erwartete) Abweichung von  $f(\mathbf{w})$  zu  $\bar{f}(\mathbf{w})$  ist. Es können auch andere Konstruktionen für dieses Intervall verwendet werden, solange sie sicherstellen, dass mit ausreichend hoher Wahrscheinlichkeit  $\bar{f}(\mathbf{w}) \in [l^{(\mathbf{w})}, u^{(\mathbf{w})}]$  gilt. Als Optimist wählen wir  $\mathbf{w}$  gemäß dem günstigsten – aber dennoch plausiblen – Wert  $\tilde{f}(\mathbf{w}) := l^{(\mathbf{w})}$  des Leistungsmaßes. Zwei Beispiele für diese Konstruktion findet man in der strukturellen Risikominimierung [?, Kap. 11] sowie bei Methoden für die sequentielle Entscheidungsfindung [?, Abschnitt 2.2].

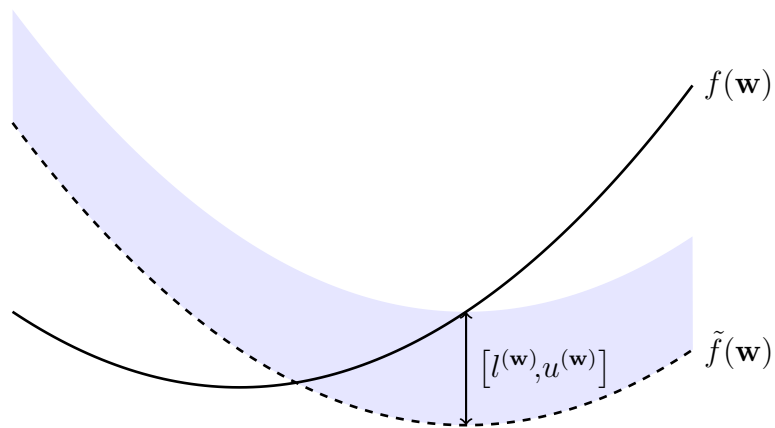


Abbildung 1: Wir verwenden eine Schätzung  $f(\mathbf{w})$  für das Leistungsmaß  $\tilde{f}(\mathbf{w})$  um ein Konfidenzintervall  $[l^{(\mathbf{w})}, u^{(\mathbf{w})}]$  zu konstruieren. Ein Optimist im Angesicht der Unsicherheit wählt Modellparameter  $\mathbf{w}$  gemäß dem günstigsten – aber dennoch plausiblen – Wert  $\tilde{f}(\mathbf{w}) := l^{(\mathbf{w})}$ .

# Index

Daten, 2

discrepancy, 3

FedAvg, 3

FedGD, 3

FedRelax, 3

FedSGD, 3

Klassifizierung, 4

Optimismus im Angesicht der

Unsicherheit, 4