



# Deep Learning, Machine Learning und Künstliche Intelligenz – SS 26

Gelesen von Prof. Dr. Daniel Gaida

# Lernraum I: Wie wird ein Machine Learning Projekt durchgeführt?

- Künstliche Intelligenz im täglichen Leben
  - KI, Machine Learning und Deep Learning – Was ist der Unterschied?
  - Was ist und warum wird Machine Learning verwendet?
  - Anwendungsbeispiele für Machine Learning
  - Training von Machine Learning Modellen mit und ohne Menschliche Überwachung
  - Die wichtigsten Herausforderungen beim Machine Learning
- 
- Ein Machine Learning Projekt von A bis Z

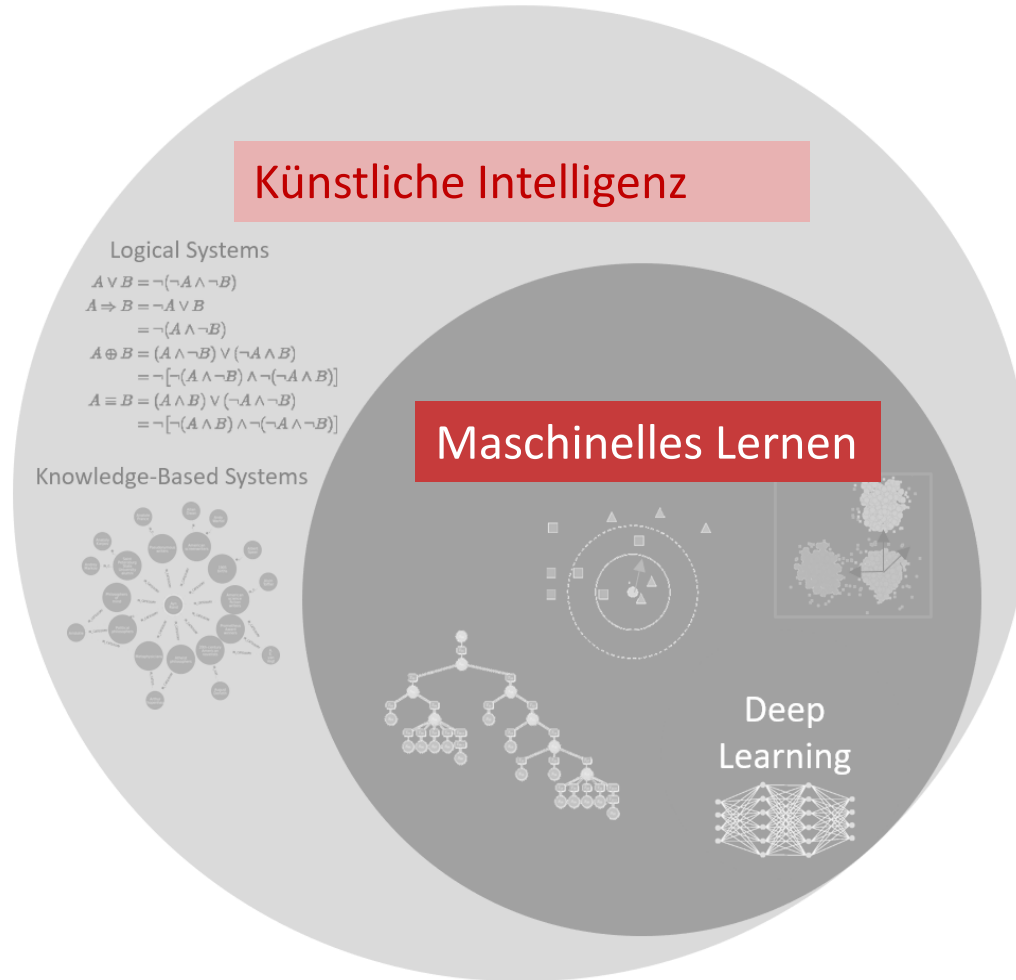
# Lernziele von heute und Fragen zur Überprüfung der Lernziele

Die Studierenden können für eine Aufgabenstellung bestimmen welche Art und ob Maschinelles Lernen hier erfolgreich eingesetzt werden kann, indem sie sagen können, ob überwachtes, unüberwachtes Lernen oder Reinforcement Learning eingesetzt werden kann und welche Herausforderungen es geben könnte, um später selbständig entscheiden zu können für welche Anwendungen sich Machine Learning eignet und wie grundlegend vorgegangen werden kann.

s. Übungsaufgaben von heute



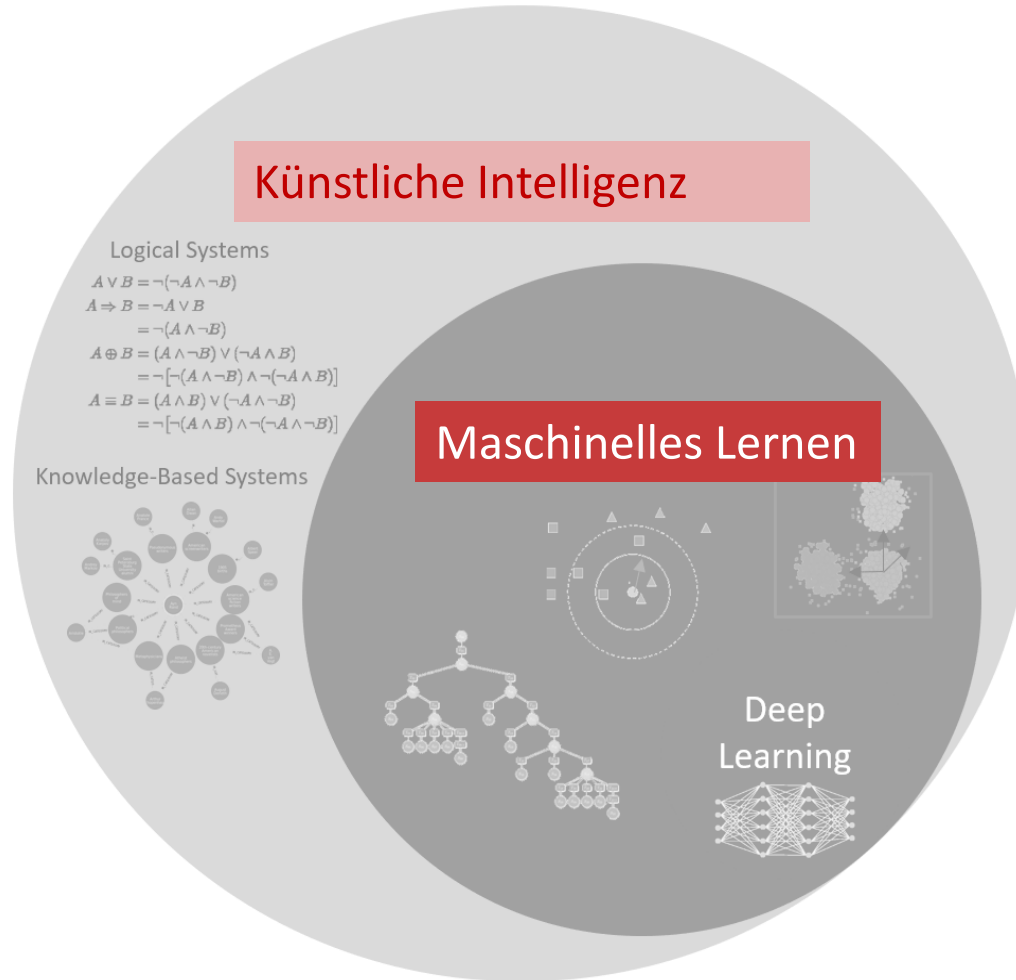
# KI, Machine Learning und Deep Learning – Was ist der Unterschied?



- Künstliche Intelligenz als Oberbegriff
  - Logisches Schließen, wissensbasierte Systeme
  - Optimierung
  - Statistische Analyse (maschinelles Lernen)

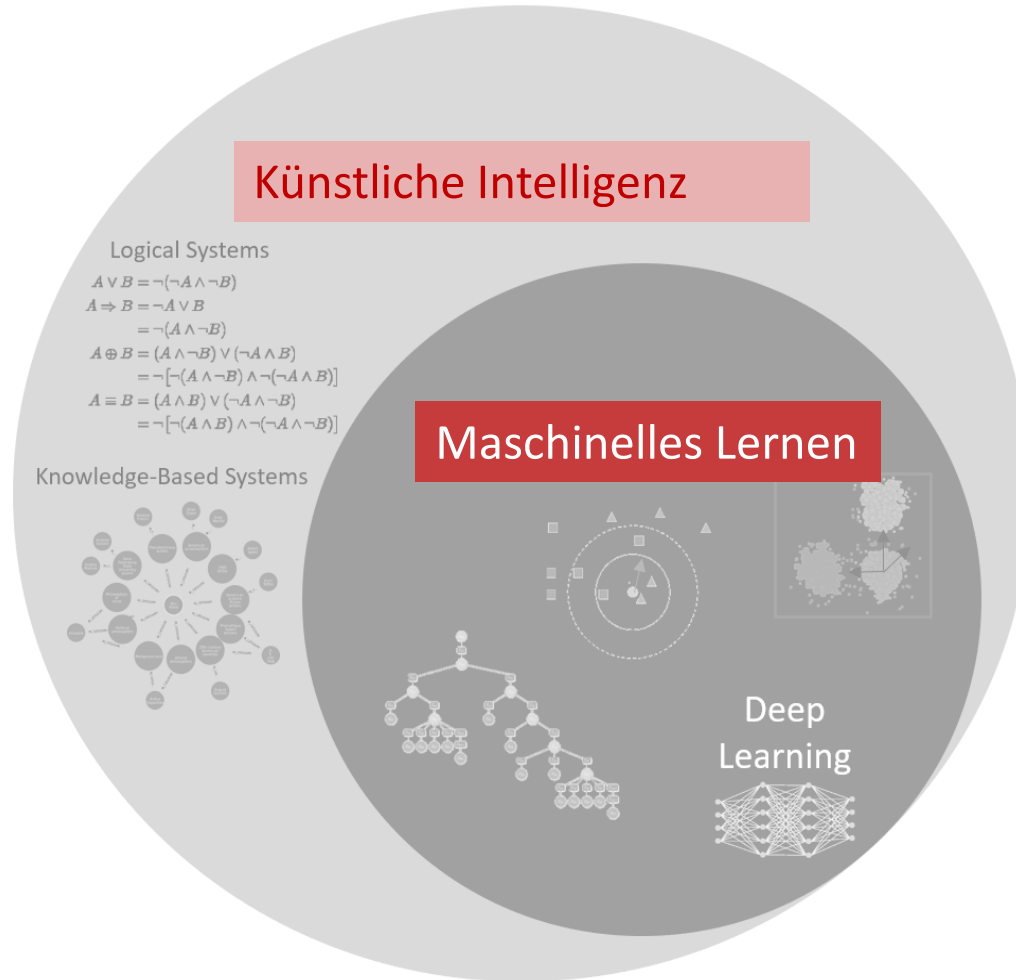
*Künstliche Intelligenz (KI) beschäftigt sich mit Methoden, die es einem Computer ermöglichen, solche Aufgaben zu lösen, die, wenn sie vom Menschen gelöst werden, Intelligenz erfordern.*

# KI, Machine Learning und Deep Learning – Was ist der Unterschied?



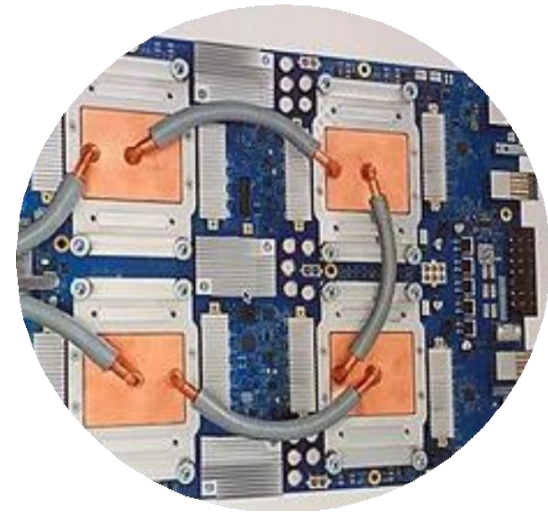
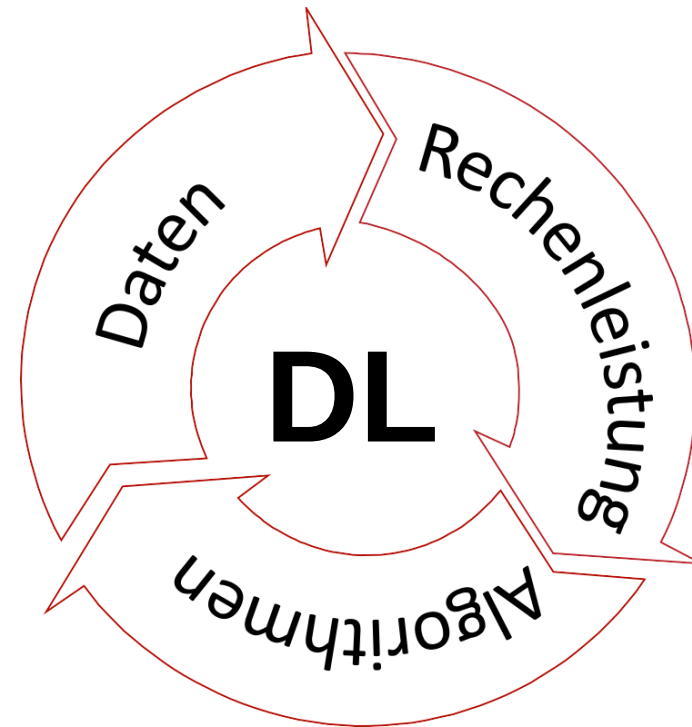
- Künstliche Intelligenz als Oberbegriff
  - Logisches Schließen, wissensbasierte Systeme
  - Optimierung
  - Statistische Analyse (maschinelles Lernen)
- Maschinelles Lernen
  - Systeme die aus Erfahrung & Beispielen lernen
  - Erkennen von Mustern in Daten
  - Eigenständiges Erlernen von Regeln

# KI, Machine Learning und Deep Learning – Was ist der Unterschied?



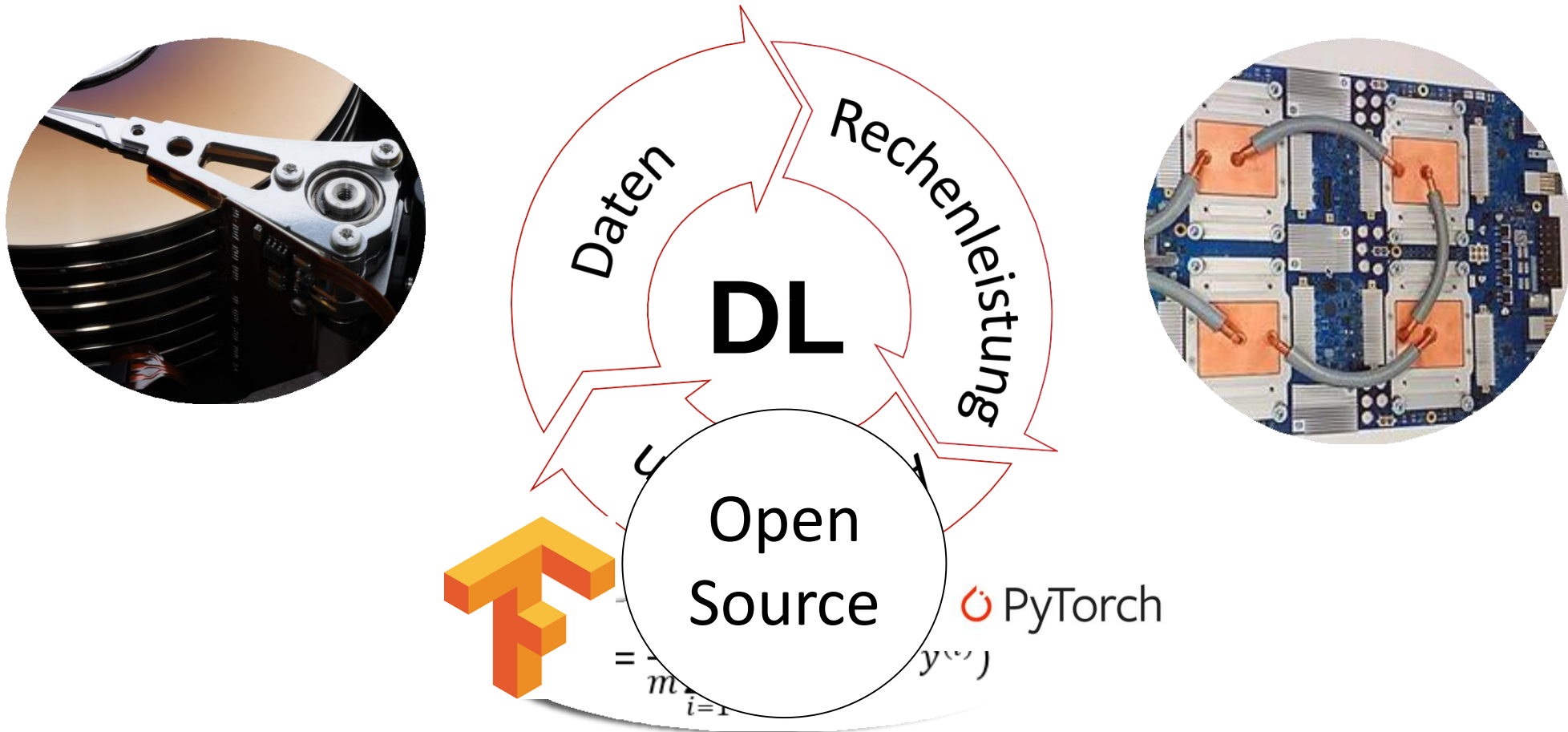
- Künstliche Intelligenz als Oberbegriff
  - Logisches Schließen, wissensbasierte Systeme
  - Optimierung
  - Statistische Analyse (maschinelles Lernen)
- Maschinelles Lernen
  - Systeme die aus Erfahrung & Beispielen lernen
  - Erkennen von Mustern in Daten
  - Eigenständiges Erlernen von Regeln
- Deep Learning
  - Ein Teilgebiet des maschinellen Lernens
  - Hype durch Erfolge in Bild- und Spracherkennung und Sprachverarbeitung

# Deep Learning – warum jetzt?



$$J(\theta) = \frac{1}{m} \sum_{i=1}^m (h_{\theta}(x^{(i)}) - y^{(i)})^2$$

# Deep Learning – warum jetzt?





# Was ist Maschinelles Lernen?

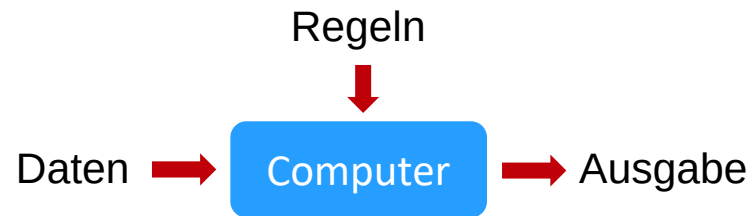
**„[Maschinelles Lernen ist das] Fachgebiet, das Computern die Fähigkeit zu lernen verleiht, ohne explizit programmiert zu werden.“**

Arthur Samuel, 1959

- Ein Spamfilter ist ein maschinelles Lernprogramm, das aus Beispielen für Spam-E-Mails (z.B. vom Nutzer markierten) und gewöhnlichen E-Mails (Nicht-Spam) lernt, Spam zu erkennen.
- Die vom Nutzer markierten Lernbeispiele nennt man den Trainingsdatensatz.
- Die Aufgabe besteht darin, neue E-Mails als Spam zu kennzeichnen.
- Maschinelles Lernen lernt diese Aufgabe aus dem Trainingsdatensatz, in dem es Muster/Zusammenhänge erkennt und wendet das erlernte Wissen auf neue E-Mails an, um Spam zu erkennen.

# Warum wird Maschinelles Lernen verwendet?

## Traditionelles Programmieren vs. Maschinelles Lernen



### Traditionelle Programmierung

- Alle Regeln werden explizit programmiert
- Jede Regel basiert auf einer logischen Grundlage
- Die Maschine gibt eine Ausgabe aus, die der logischen Anweisung folgt
- Komplexe Systeme benötigen viele Regeln

→ Instandhaltung kann schnell untragbar werden

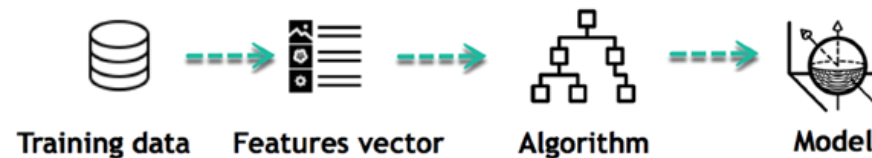


### Maschinelles Lernen

- Soll dieses Problem überwinden
- Regeln werden basierend auf der Korrelation zwischen Ein- & Ausgabe erlernt
- Regeln müssen nicht explizit geschrieben werden
- Algorithmen passen sich neuen Daten an

# Wie funktioniert Maschinelles Lernen?

Ziel des Maschinellen Lernens: **Lernen** und **Schlussfolgern**



## Lernphase

- Entdecken von Mustern/Korrelationen in Daten  
*Daten sind von entscheidender Bedeutung*
- Extrahieren von Merkmalen (**Feature-Vektor**)
- Überführen der Entdeckungen in ein Modell

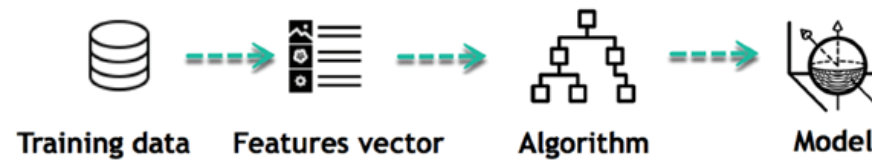


## Schlussfolgerung

- Testen der Performance auf neue und ungesehene Daten
- Extrahieren der Merkmale
- Modell liefert eine Vorhersage

# Wie funktioniert Maschinelles Lernen?

Einfaches Beispiel: Vorhersage des Umsatzes in einer Eisdiele



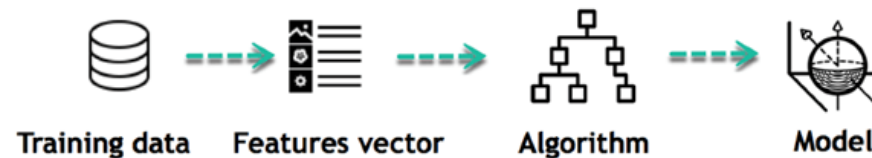
## Lernphase

- Daten: ?



# Wie funktioniert Maschinelles Lernen?

Einfaches Beispiel: Vorhersage des Umsatzes in einer Eisdiele

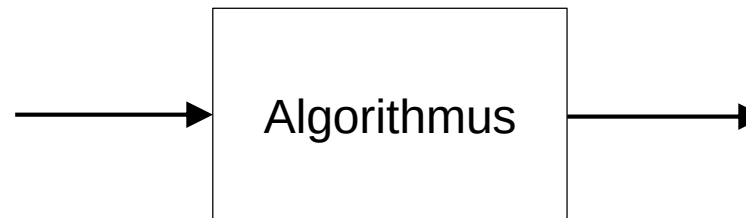
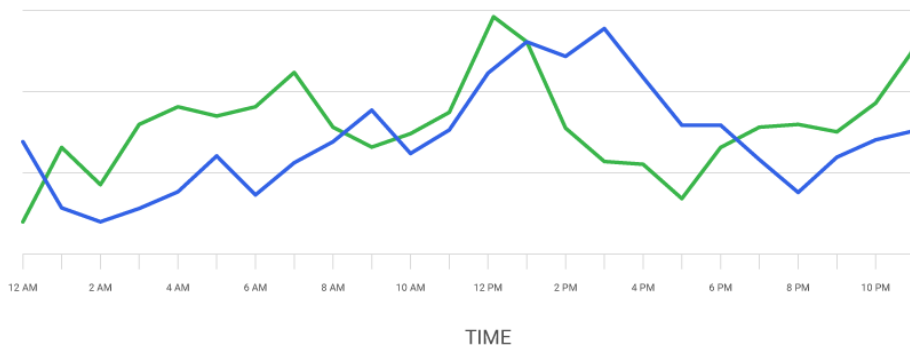


## Lernphase

- Daten: Wetter, Benzinpreis, Wochentag, Preis/Kugel, Jahreszeit, ...
- Algorithmus findet Muster zwischen Daten und Umsatz der letzten 6 Monate
- Überführen der Entdeckungen in ein Modell

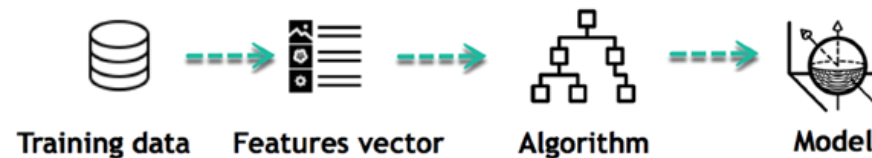
# Wie funktioniert Maschinelles Lernen?

Einfaches Beispiel: Vorhersage des Umsatzes in einer Eisdiele



# Wie funktioniert Maschinelles Lernen?

Einfaches Beispiel: Vorhersage des Umsatzes in einer Eisdiele



## Lernphase

- Daten: Wetter, Benzinpreis, Wochentag, Preis/Kugel, Jahreszeit, ...
- Algorithmus findet Muster zwischen Daten und Umsatz der letzten 6 Monate
- Überführen der Entdeckungen in ein Modell



## Schlussfolgerung

- Testen der Performance auf neue und ungesehene Daten
- Extrahieren der Merkmale
- Modell liefert eine Vorhersage

# Warum wird Maschinelles Lernen verwendet?

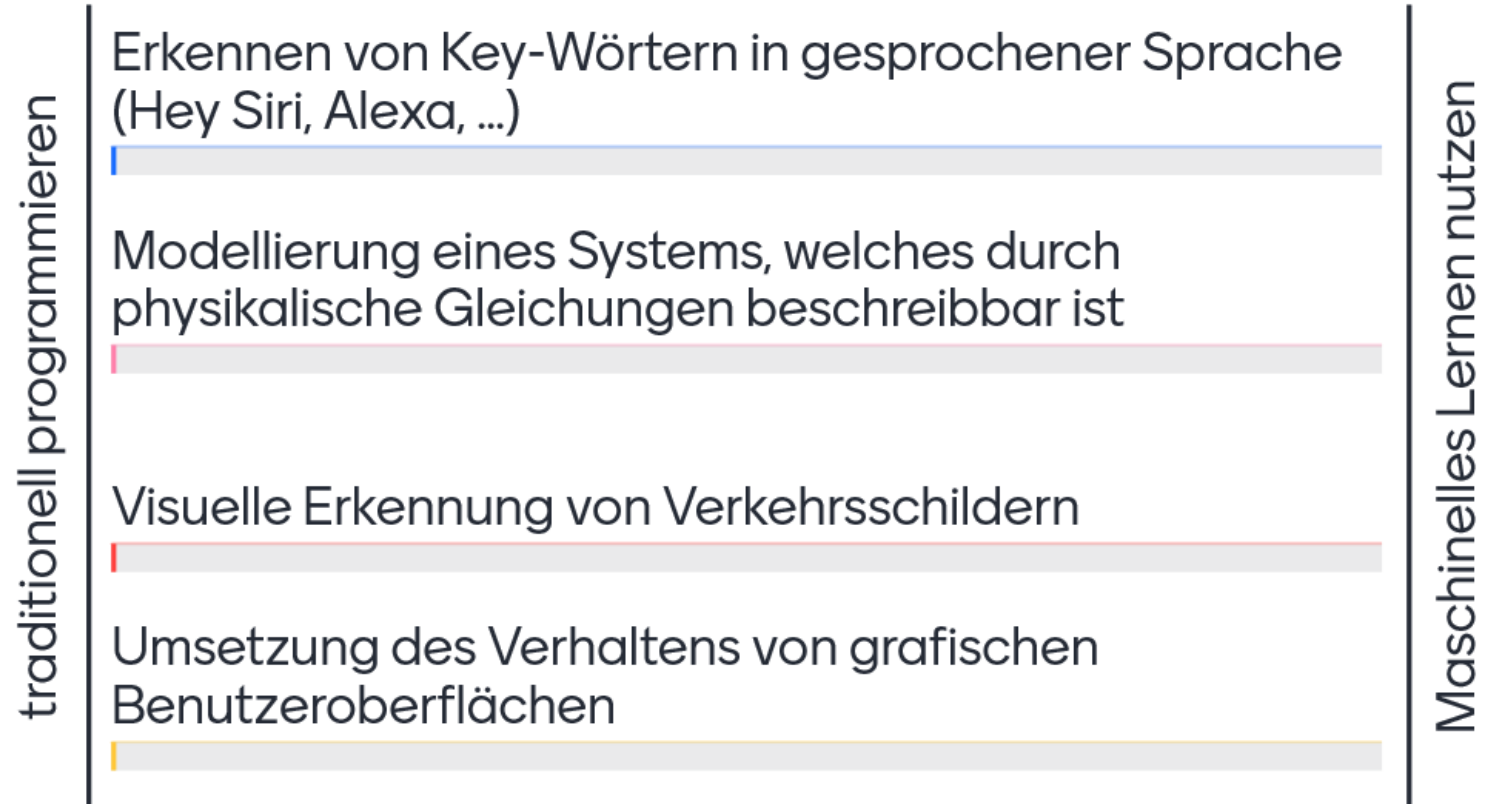
Situationen, in denen Maschinelles Lernen (ML) besser geeignet ist als traditionelle Programme:

- Probleme, für die bestehende Lösungen lange Listen von Regeln erfordern.
- Komplexe Probleme, für die ein traditioneller Ansatz keine gute Lösung liefert.
- Sich ändernde Umgebungen: ein ML-System kann sich an neue Daten anpassen.

# Warum wird Maschinelles Lernen verwendet?

## Quiz – traditionell programmieren oder ML?

Mentimeter Code: 1741 3121



# Fragen?



# Lernraum I: Wie wird ein Machine Learning Projekt durchgeführt?

- Künstliche Intelligenz im täglichen Leben
- KI, Machine Learning und Deep Learning – Was ist der Unterschied?
- Was ist und warum wird Machine Learning verwendet?
- Anwendungsbeispiele für Machine Learning
- Training von Machine Learning Modellen mit und ohne Menschliche Überwachung
- Die wichtigsten Herausforderungen beim Machine Learning

# Projektteil (10 CPs) als Teil von WASP I

- Wer möchte ein Projekt machen?

# Infos für Masterstudierende

- Prüfungsform: Mündliche Prüfung
  - Termin in Prüfungswoche oder eine Woche danach (muss noch abgesprochen werden)
  - Aktuell ist keine Anmeldung über PSSO/CAMS-EXA notwendig
    - Anmeldung erfolgt per Mail an [daniel.gaida@th-koeln.de](mailto:daniel.gaida@th-koeln.de) (weitere Infos folgen)

# Kurze Pause?

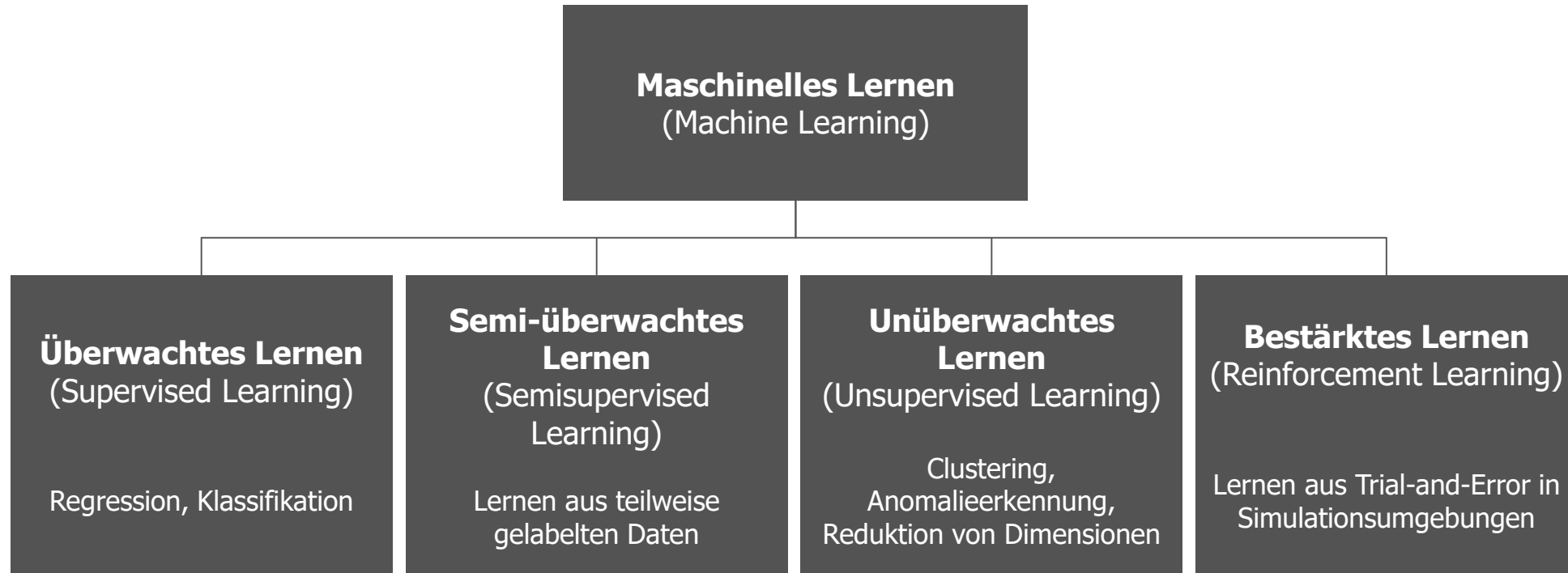
- Ja, 5 Minuten
- Ja, 10 Minuten
- Nein

# Anwendungsbeispiele für Maschinelles Lernen

- Vorhersage der Stromproduktion und -nachfrage
  - Berücksichtigung der Wettervorhersage (erneuerbare Energie)
  - Berücksichtigung des täglichen Profils der Stromnachfrage
- Vorausschauende Wartung
  - Wann wird Komponente X in Maschine Y ausfallen?
- Aufdeckung von Betrug
  - Beispiel: Ermittlung typischer Muster für Kreditkartenbetrug.
- Kreditwürdigkeitsprüfung
  - Ermittlung von Kriterien für die Kreditwürdigkeit von Kunden
- Vorhersage der Nachfrage
  - Wie viele Einheiten von Produkt X werden wir in Woche 42 verkaufen?



# Training von Machine Learning Modellen mit und ohne Überwachung

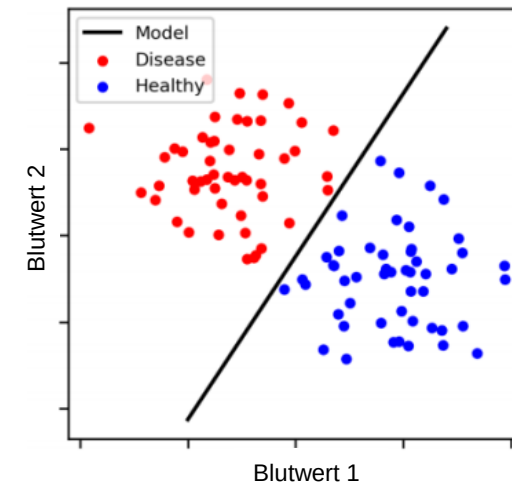
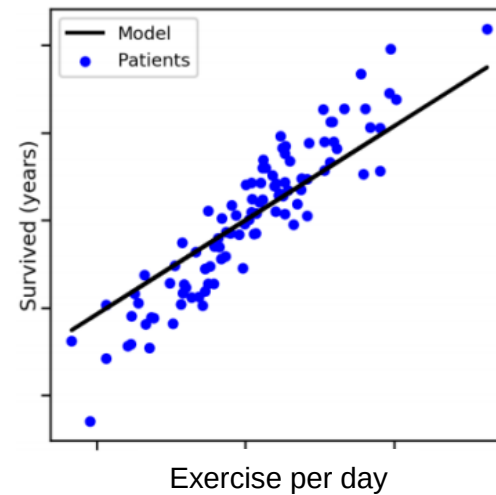


# Training von ML Modellen mit und ohne Überwachung

## Überwachtes Lernen: Regression vs. Klassifikation

- Trainingsdaten sind gelabelt

|            | Regression                   | Klassifikation               |
|------------|------------------------------|------------------------------|
| Vorhersage | Numerische Werte (geordnet)  | Klassen (ungeordnet)         |
| Beispiel   | Alters- oder Preisvorhersage | Gesund/krank, Spam/kein Spam |

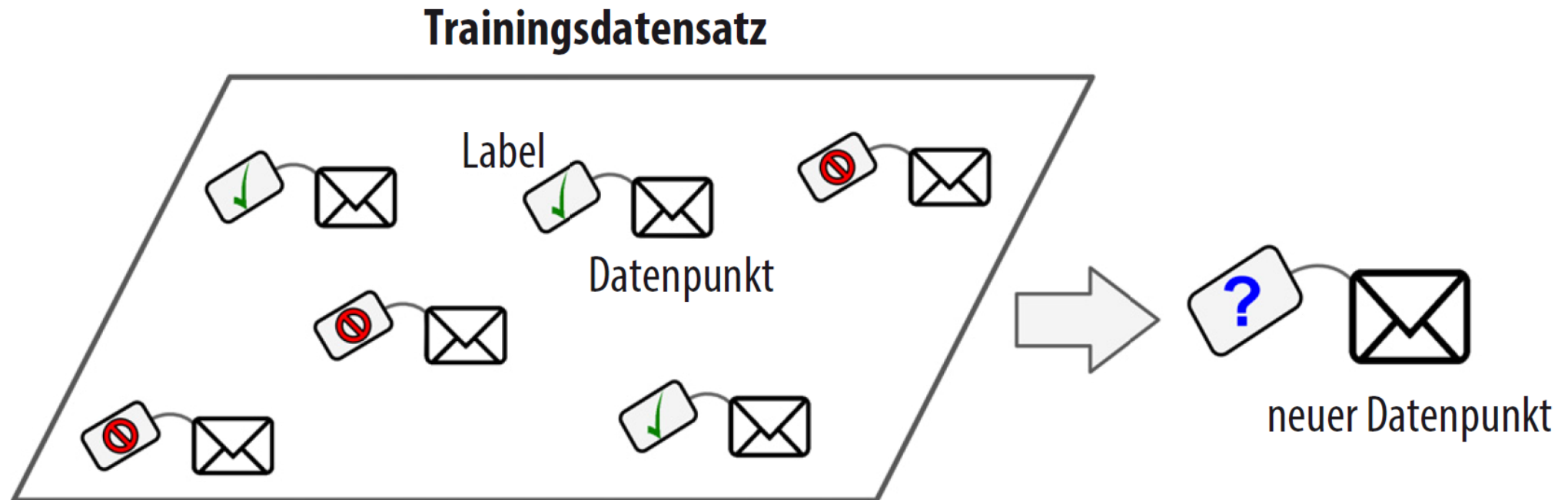




# Training von ML Modellen mit und ohne Überwachung

## Überwachtes Lernen

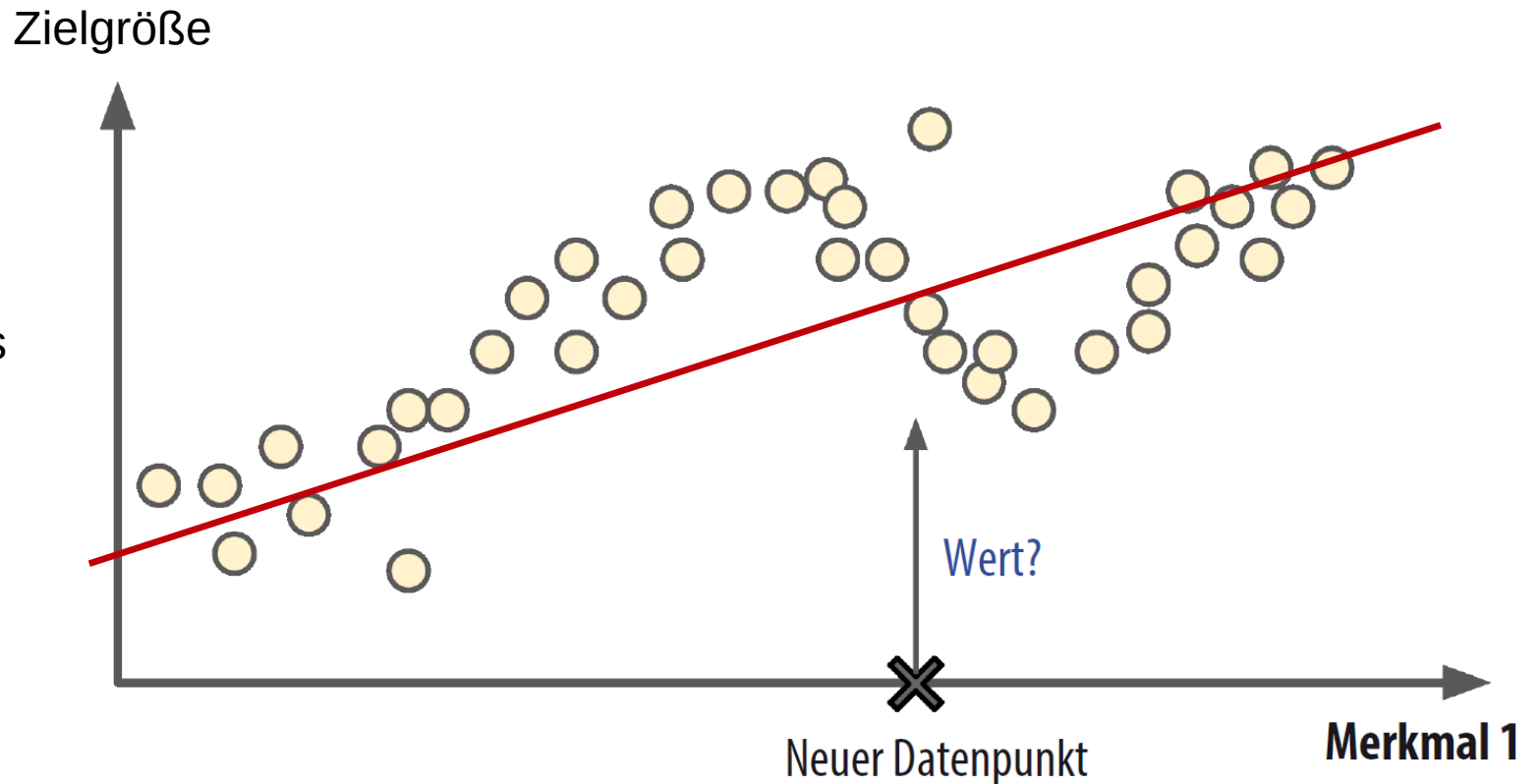
- Klassifikation: Beispiel Spamerkennung
- Weitere Beispiele für Klassifikationsprobleme?



# Training von ML Modellen mit und ohne Überwachung

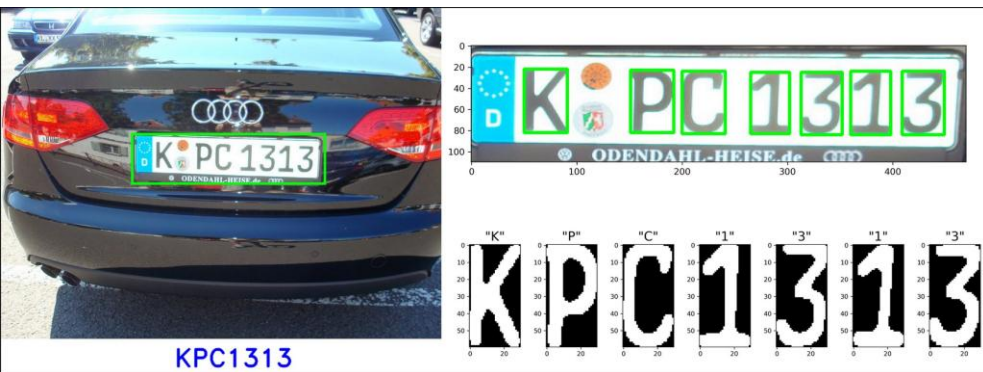
## Überwachtes Lernen

- Regression
  - Vorhersage einer numerischen Zielgröße aus **Merkmalen**
  - Bspw. Preis eines Gebrauchtwagens auf Basis von gefahrene Kilometer, Alter, Marke, ...
  - Gefahrene Kilometer, Alter, Marke, ... sind **Merkmale (Features)**
- Beispiel:
  - Lineare Regression



# Quiz – Regression oder Klassifikation

Mentimeter Code: 1741 3121



Quelle: <https://www.analyticsvidhya.com/blog/2021/03/license-plate-character-recognition-using-knn-and-cnn/>

Klassifikation

Preisvorhersage an der Tankstelle auf Basis des Ölpreises, weltweite Krisen, Monat, Ort

Erkennung von Nummernschildern mit einer Kamera

Detektion von gesprochenen Key-Wörtern wie Alexa, Hey Siri, ...

Schätzung der Oberflächentemperatur eines Sees auf Basis der Sonnenscheindauer und Außentemperatur

Regression

# Training von ML Modellen mit und ohne Überwachung

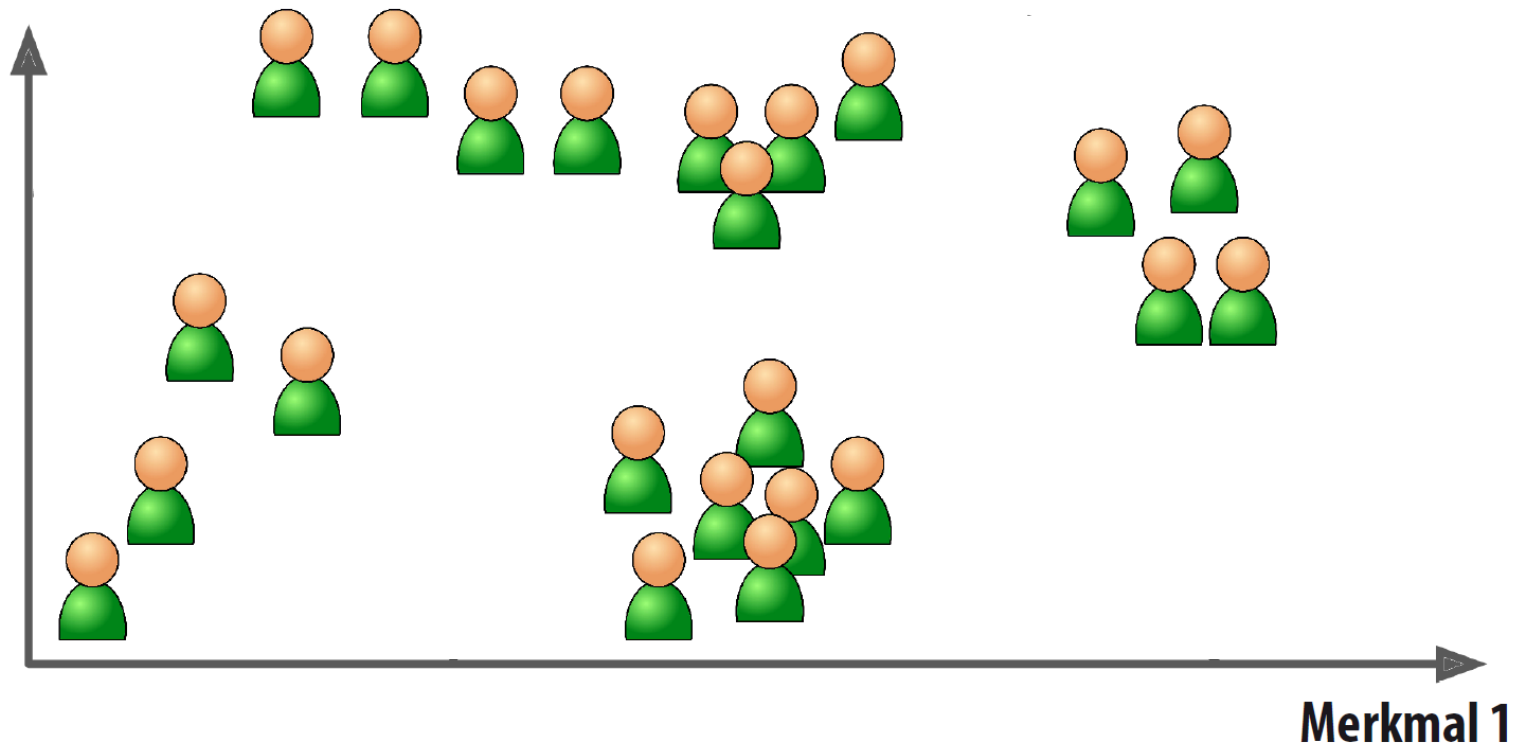
## Unüberwachtes Lernen

- Beispiel:
  - Empfehlungssysteme

- Was wären Beispiele für Merkmale?
- Bsp. Videofilm
  - Merkmal 1: Spannung
  - Merkmal 2: Action

- Clustering
- Wie viele Cluster sehen Sie?

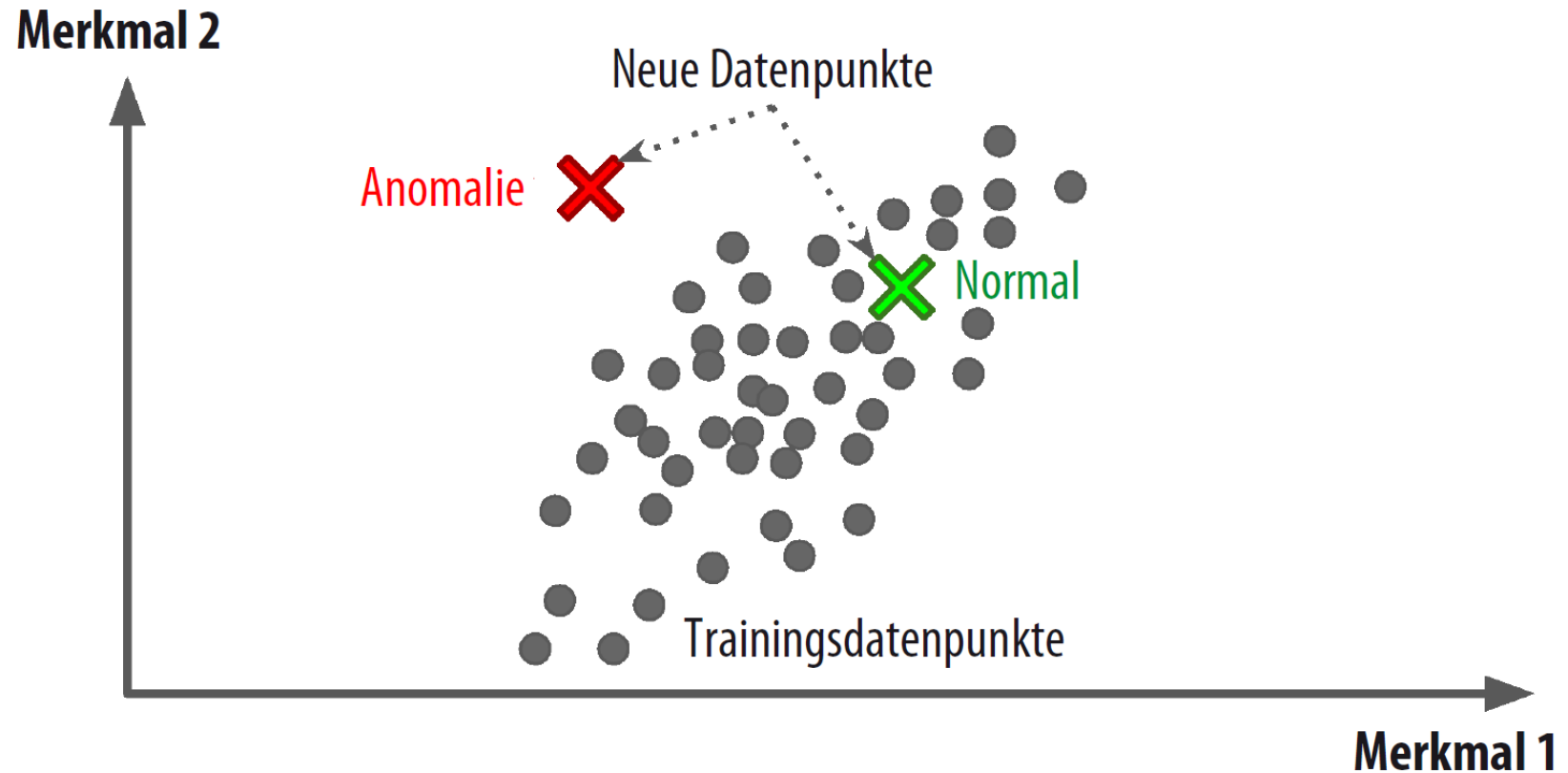
**Merkmal 2**



# Training von ML Modellen mit und ohne Überwachung

## Unüberwachtes Lernen

- Anomalieerkennung
- Beispiel:
  - Ungewöhnliche Transaktionen auf Kreditkarten
  - Produktionsfehler
  - Messfehler
  - Sensordefekt
- Merkmale?
  - Merkmal 1: Temperatur
  - Merkmal 2: Durchfluss



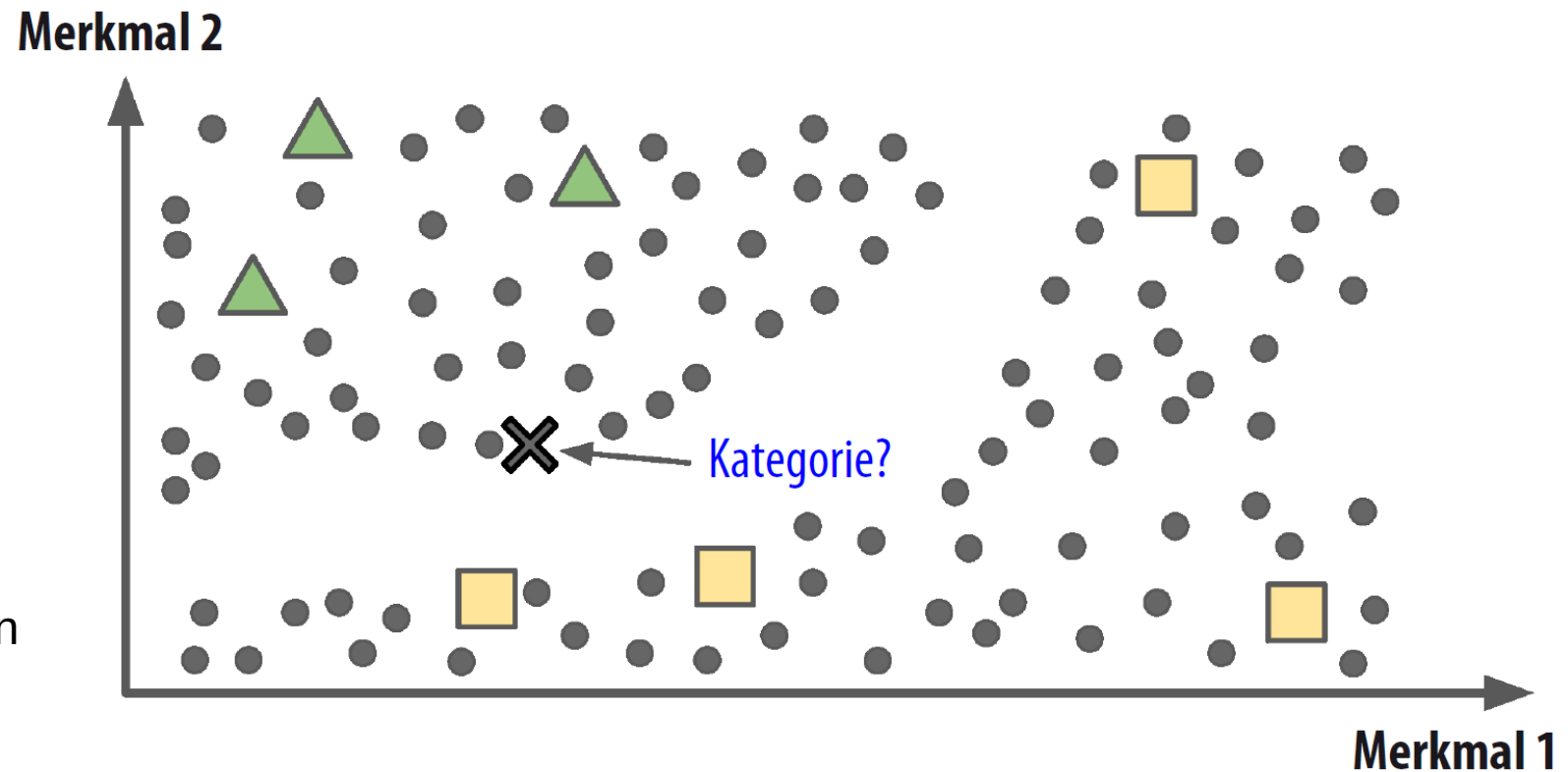
# Training von ML Modellen mit und ohne Überwachung

## Semi-Überwachtes Lernen

- Quadrat- und Dreieckklasse
- Teilweise gelabelter Datensatz, da Labeling teuer und zeitaufwändig

1. Unüberwachtes Training, um Cluster zu finden
2. Überwachtes Finetuning, um Cluster zu verfeinern und zu labeln

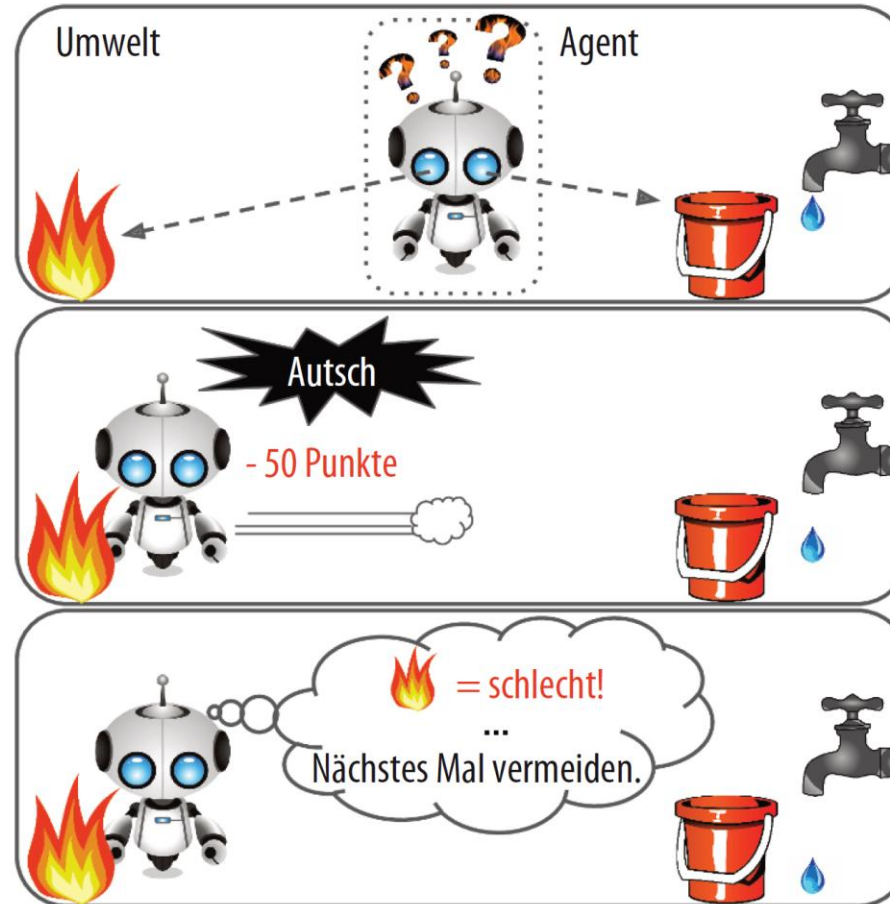
- Bspw. Personenidentifikation in Fotosammlung



# Training von ML Modellen mit und ohne Überwachung

## Reinforcement Learning

- Agent lernt durch Interaktion mit Umgebung (führt Aktionen aus)
- Erhält Belohnungen
- Maximierung der Summe der Belohnungen über die Zeit
- Policy definiert, welche Aktion Agent in welcher Situation auswählt
- Beispiele:
  - Roboter
  - Spiele (AlphaGo)



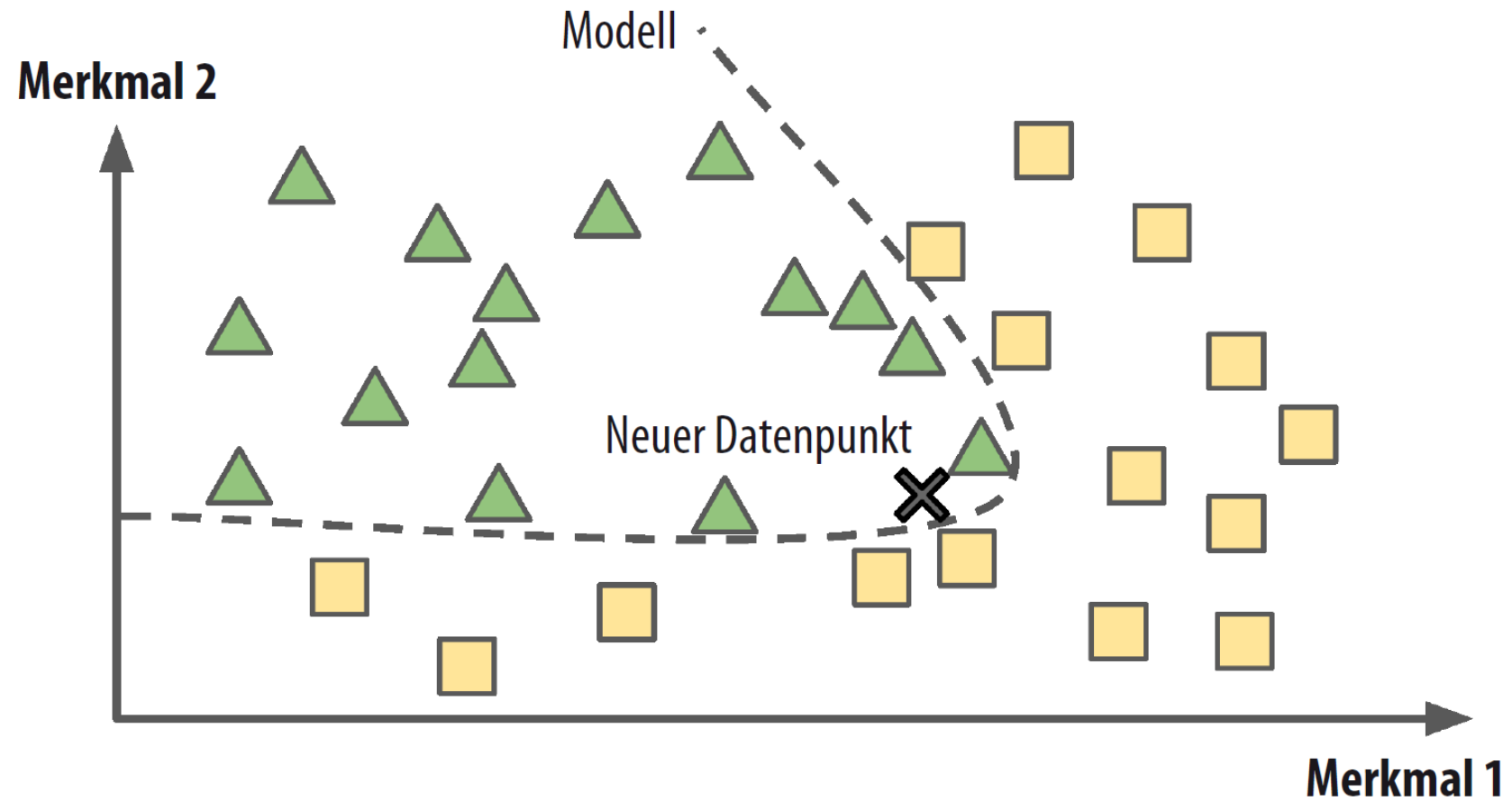
- 1 Beobachten
- 2 Aktion nach einer Policy auswählen
- 3 Aktion durchführen!
- 4 Belohnung oder Strafe erhalten
- 5 Policy aktualisieren (Lernschritt)
- 6 Wiederholen bis zum Finden einer optimalen Policy

# Umfrage zu Training von Machine Learning Modellen mit und ohne Überwachung

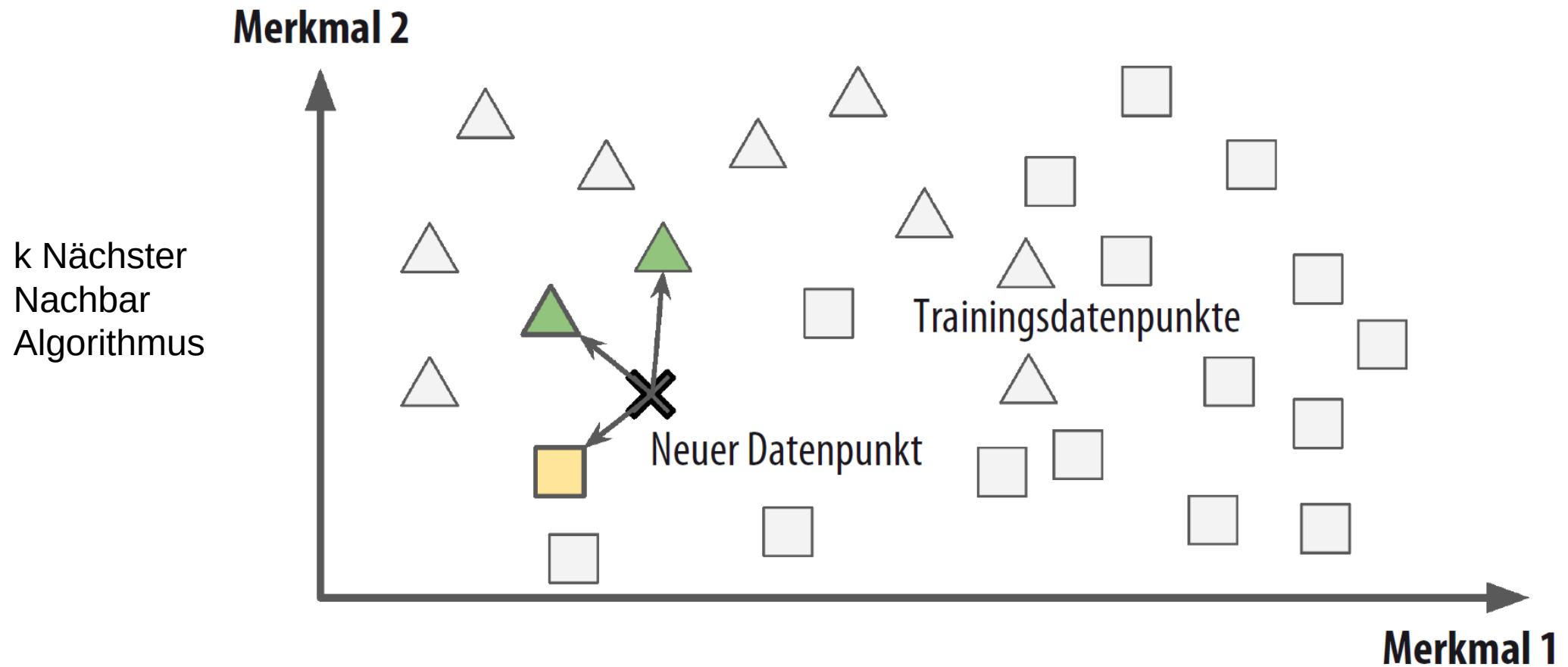
- Vorhersage eines Aktienkurses
  - Die Kreditwürdigkeit eines Bankkunden vorhersagen
  - Vorhersage der Biogasproduktion einer Biogasanlage auf Basis von Sensordaten
  - Gruppieren ähnlicher Systemzustände einer chemischen Anlage auf Basis von Sensordaten
  - Training eines Agenten für einen Ego-Shooter
  - Erkennung ob ein Text ein Thema aus der Wirtschaft, dem Sport oder Kultur beschreibt
- 
- Antwortmöglichkeiten:
    - Überwachtes Lernen (Regression, Klassifikation)
    - Unüberwachtes Lernen
    - Reinforcement Learning



# Instanzbasiertes vs. Modellbasiertes Lernen



# Instanzbasiertes vs. Modellbasiertes Lernen



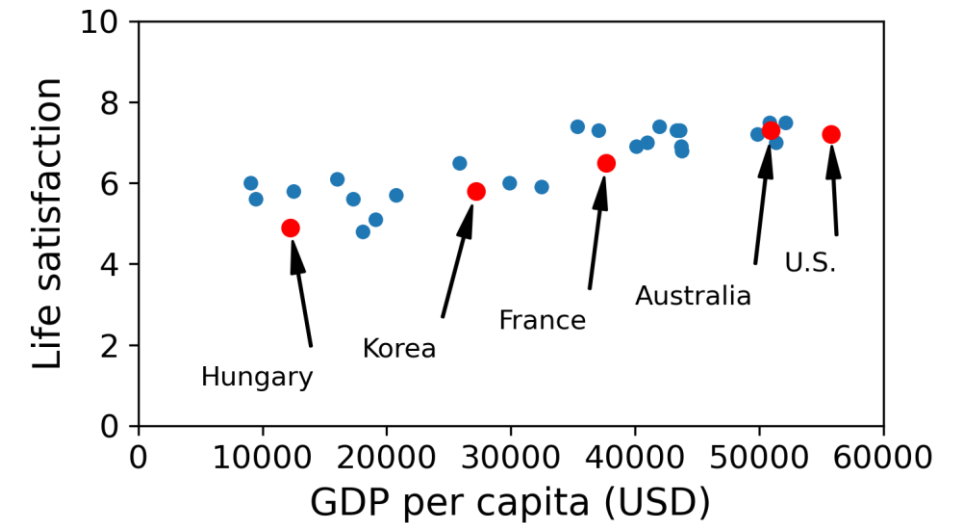
# Modellbasiertes Lernen - Einfaches Beispiel

## Macht Geld glücklich?

- Lebenszufriedenheit vs. Bruttoinlandsprodukt (BIP)
- Sehen Sie hier einen Trend?
- Ist dieser linear, quadratisch, logarithmisch?
- Modellannahme:

*Formel 1-1: Ein einfaches lineares Modell*

$$\text{Zufriedenheit} = \theta_0 + \theta_1 \times \text{BIP\_pro\_Kopf}$$



# Einfaches Beispiel

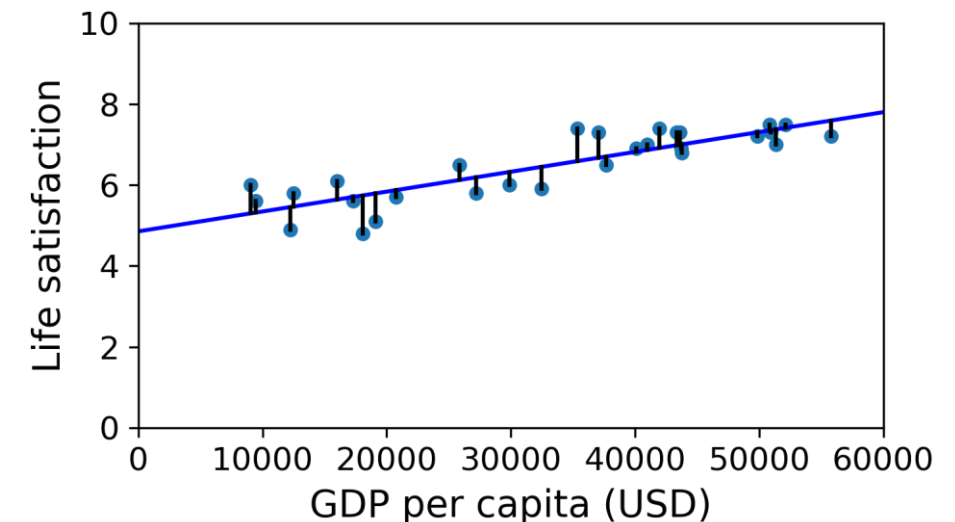
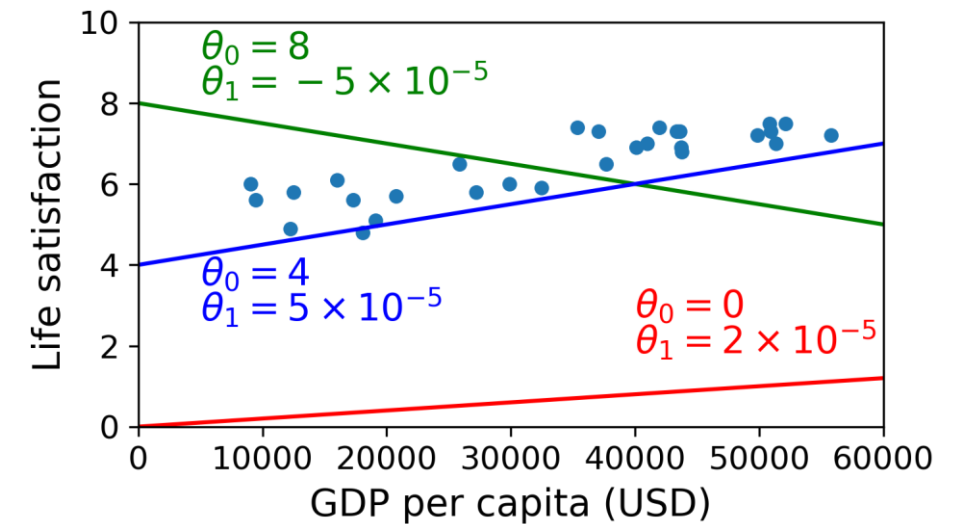
## Macht Geld glücklich?

- Lebenszufriedenheit vs. BIP

*Formel 1-1: Ein einfaches lineares Modell*

$$\text{Zufriedenheit} = \theta_0 + \theta_1 \times \text{BIP\_pro\_Kopf}$$

- Gesucht sind die Werte für die Modellparameter, die zu einer Vorhersage führen, die einen möglichst kleinen Prädiktionsfehler hat
- Wie messen wir den Prädiktionsfehler?
  - Definition einer Kostenfunktion
- Beispiele für Kostenfunktionen:
  - Quadratischer Fehler, Absoluter Fehler, ...



# Einfaches Beispiel

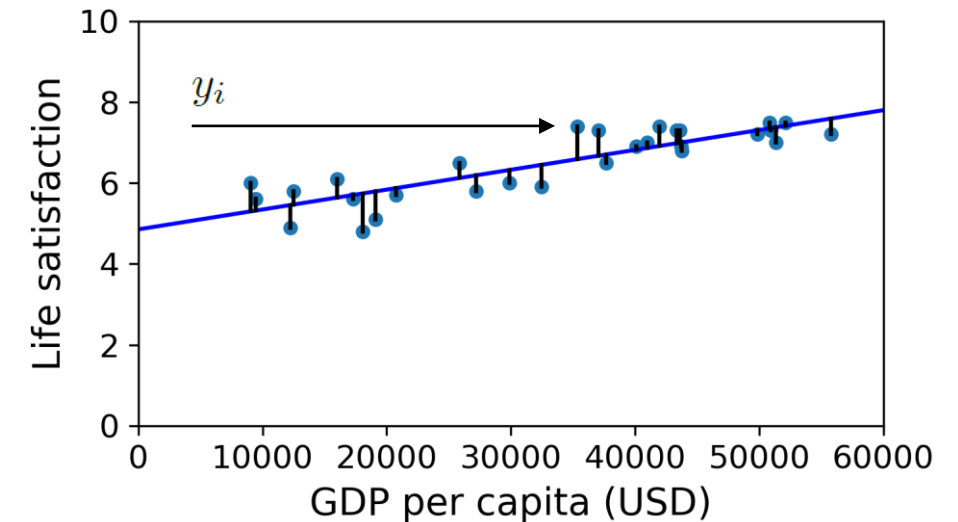
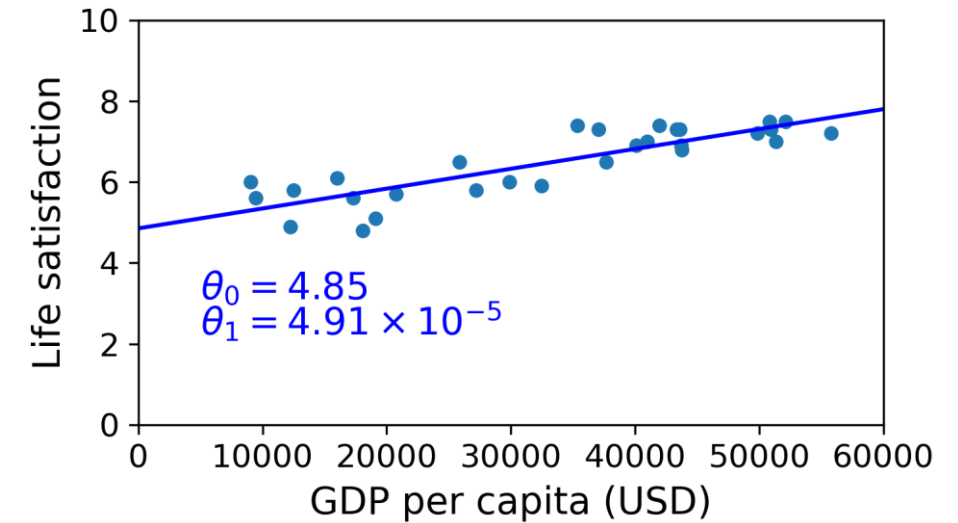
## Macht Geld glücklich?

- Algorithmus Lineare Regression:
- Training des Modells:
  - Minimierung der Kostenfunktion durch Variation der Modellparameter
  - Hier: Minimierung des RMSE-Prädiktionsfehlers auf den Trainingsdaten

*Formel 1-1: Ein einfaches lineares Modell*

Zufriedenheit =  $\theta_0 + \theta_1 \times \text{BIP\_pro\_Kopf}$

$$RMSE = \sqrt{\sum_{i=1}^n \frac{(\hat{y}_i - y_i)^2}{n}}$$



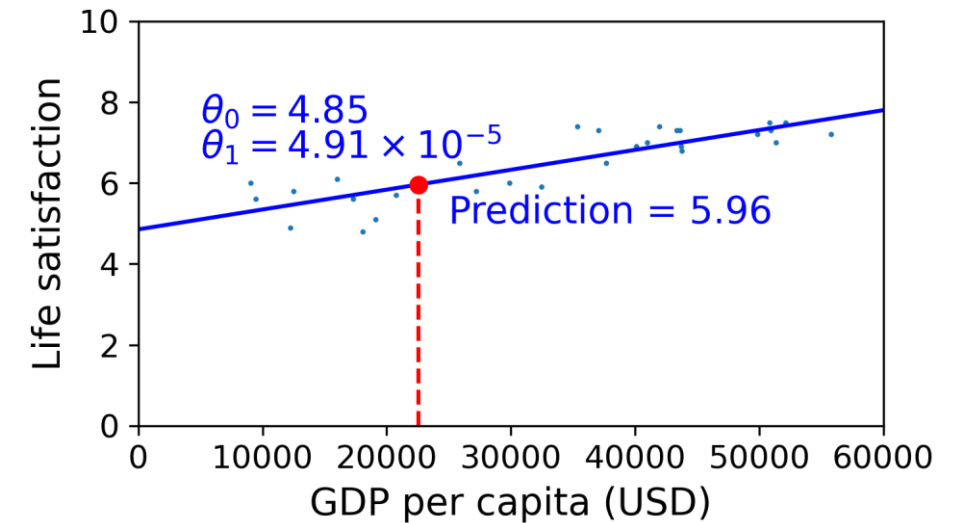
# Einfaches Beispiel

## Macht Geld glücklich?

- Test des Modells:
  - Für ein neues Land (hier: Zypern) BIP nehmen und Lebenszufriedenheit mit trainiertem Modell vorhersagen

*Formel 1-1: Ein einfaches lineares Modell*

$$\text{Zufriedenheit} = \theta_0 + \theta_1 \times \text{BIP\_pro\_Kopf}$$



# Fragen?

# Kurze Pause?

- Ja, 5 Minuten
- Ja, 10 Minuten
- Nein



# Die wichtigsten Herausforderungen beim Machine Learning

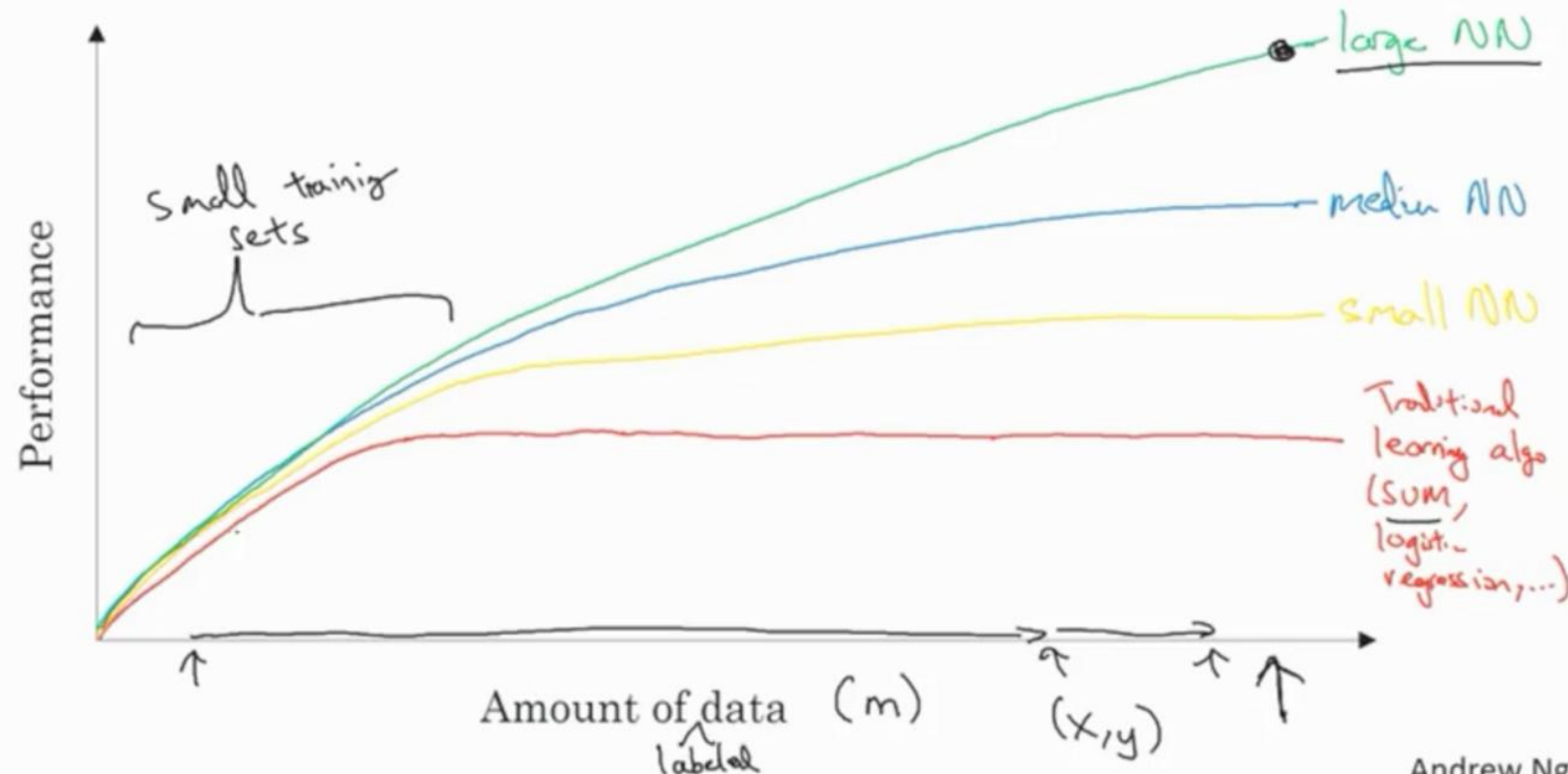
- Unzureichende Menge an Trainingsdaten
- Nicht repräsentative Daten
- Minderwertige Daten
- Irrelevante Merkmale
- Overfitting der Trainingsdaten
- Underfitting der Trainingsdaten

# Die wichtigsten Herausforderungen beim Machine Learning

## Unzureichende Menge an Trainingsdaten

- Um Machine Learning Modelle zu trainieren, werden sehr viele Trainingsdaten benötigt
- Ein Deep Learning Modell, das ein Fahrzeug visuell erkennen soll, muss viele Bilder von Fahrzeugen gesehen haben

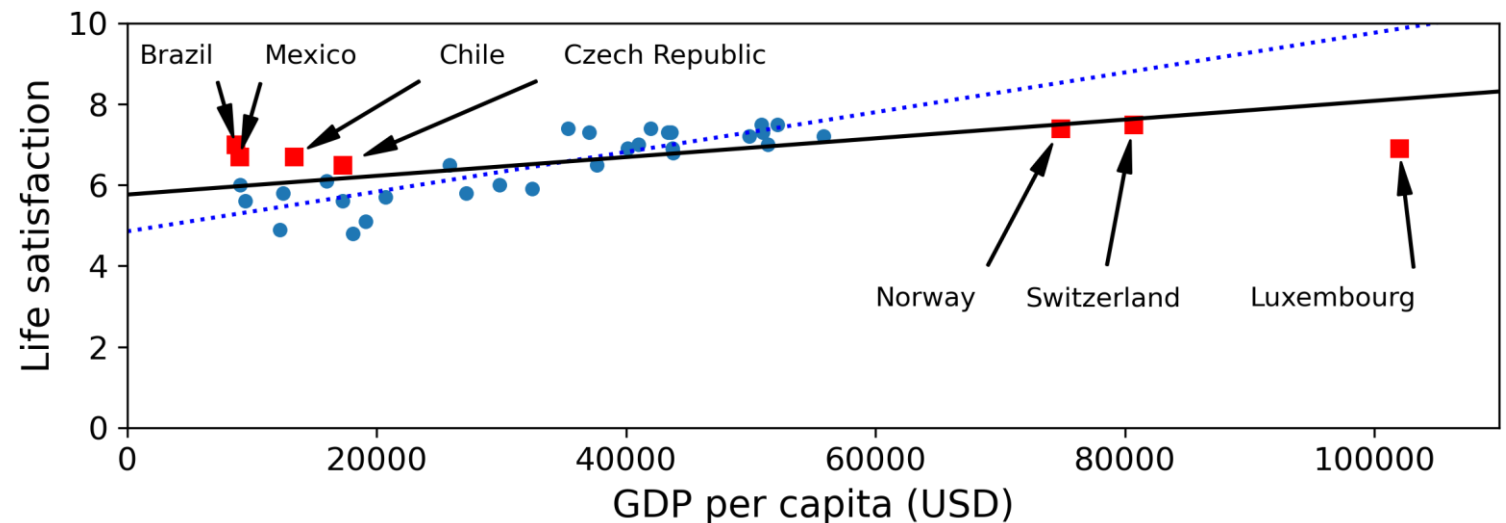
### Scale drives deep learning progress



# Die wichtigsten Herausforderungen beim Machine Learning

## Nicht repräsentative Daten

- Die vorhin genutzten Trainingsdaten waren nicht repräsentativ
- Für sehr arme und sehr reiche Länder macht das trainierte Modell keine genauen Vorhersagen



- Beispiele:
  - Daten aus Umfragen (Personen, die keine Umfragen mögen (kein Telefon haben), haben nicht teilgenommen, sind also nicht repräsentiert im Trainingsdatensatz)
  - Maschinendaten einer Maschine sind nicht repräsentativ für alle Maschinen eines Herstellers

# Die wichtigsten Herausforderungen beim Machine Learning

## Minderwertige Daten

- Trainingsdaten mit vielen Fehlern, Ausreißern, hohem Messrauschen, fehlenden Datenpunkten, ...
- Machine Learning Modell hat Schwierigkeiten die richtigen Muster in den Daten zu erkennen
- Säubern von Daten ist sehr zeitaufwändig
  - Ausreißer/Fehler beheben oder entfernen
  - Datenlücken beheben
  - ...
- Beispiele:
  - Maschinendaten mit fehlerhaften oder falsch kalibrierten Sensoren
  - Wichtige Informationen fehlen (bspw. welches Material wurde bearbeitet, ...)
  - Sehr wenig gelabelte Daten

# Die wichtigsten Herausforderungen beim Machine Learning

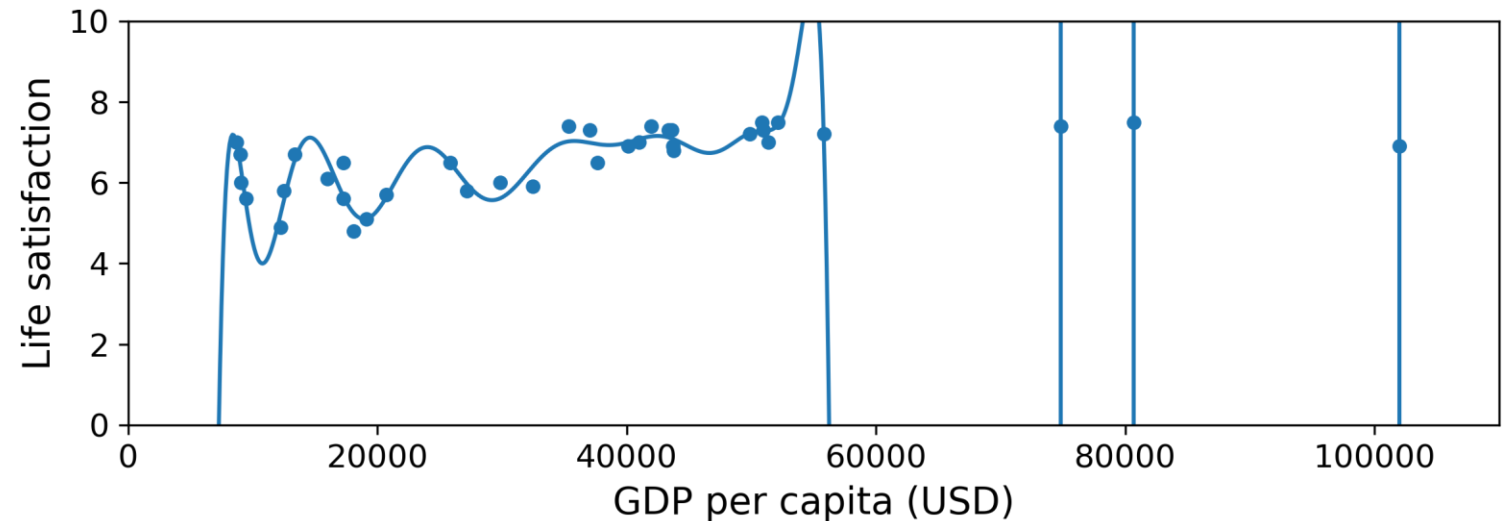
## Irrelevante Merkmale

- Müll rein, Müll raus
- Nicht alle Merkmale sind relevant
- Lösungsansätze:
  - Auswahl der relevanten Merkmale
  - Berechnung von relevanteren Merkmalen aus mehreren vorhandenen Merkmalen
    - Merkmal „BIP pro Einwohner“ ist besser als
    - 2 Merkmale:  
BIP, Anzahl Einwohner

# Die wichtigsten Herausforderungen beim Machine Learning

## Overfitting der Trainingsdaten

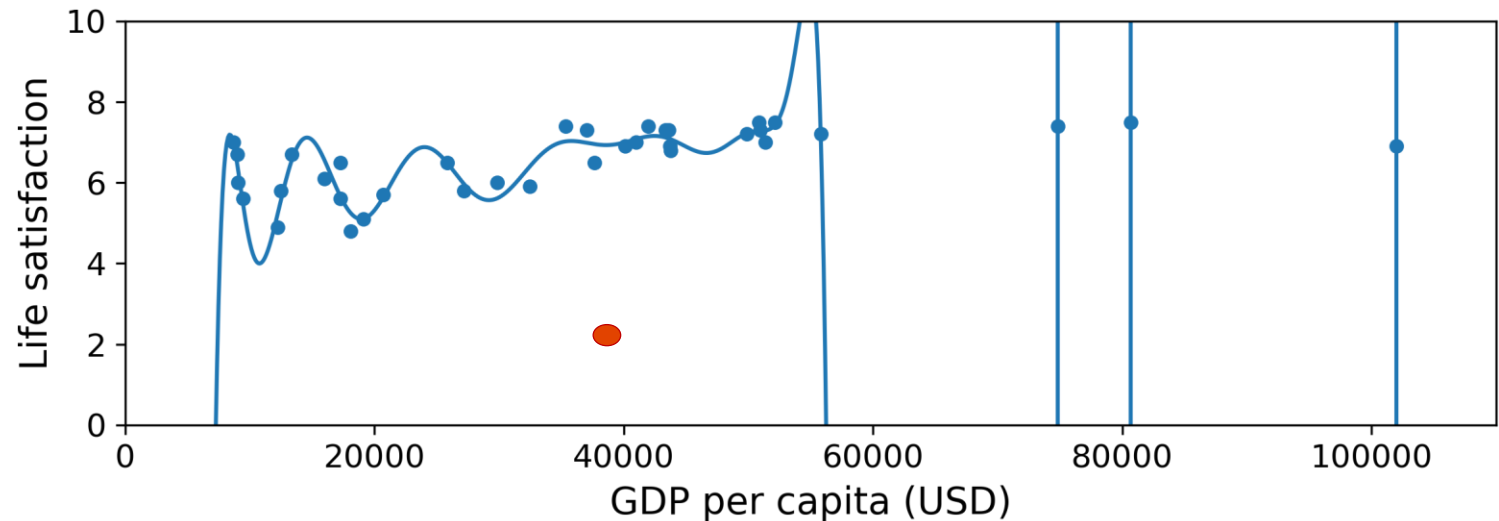
- Gewähltes Modell ist zu komplex für Daten
- Polynomiales Modell (30ter Ordnung): Lebenszufr. =  $\theta_0 + \theta_1 \cdot \text{BIP} + \theta_2 \cdot \text{BIP}^2 + \theta_3 \cdot \text{BIP}^3 + \dots$
- Lösungen?



# Die wichtigsten Herausforderungen beim Machine Learning

## Overfitting der Trainingsdaten

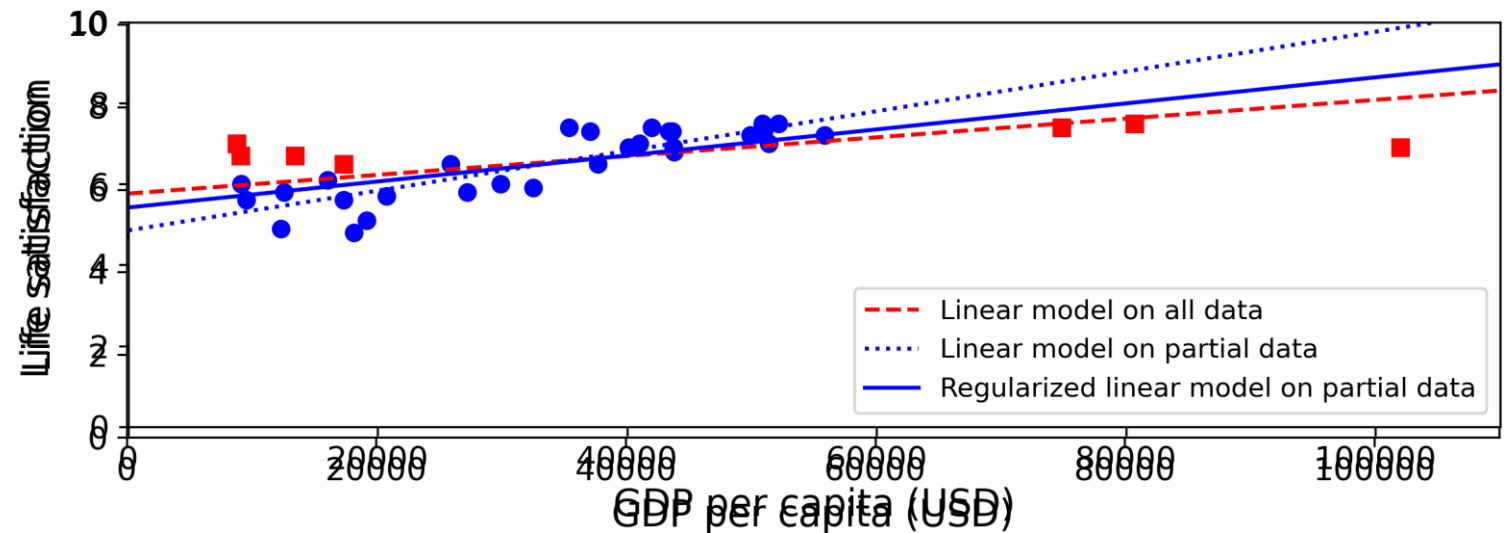
- Gewähltes Modell ist zu komplex für Daten
- Polynomiales Modell (30ter Ordnung):  $\text{Lebenszufr.} = \theta_0 + \theta_1 \cdot \text{BIP} + \theta_2 \cdot \text{BIP}^2 + \theta_3 \cdot \text{BIP}^3 + \dots$
- Lösungen:
  - Einfacheres Modell nutzen
    - Weniger Parameter
    - Weniger irrelevante Merkmale
  - Mehr Trainingsdaten sammeln
  - Fehler in Trainingsdaten beheben (Ausreißer entfernen)



# Die wichtigsten Herausforderungen beim Machine Learning

## Overfitting der Trainingsdaten

- Regularisierung
- Begrenzung des Wertebereichs der Modellparameter

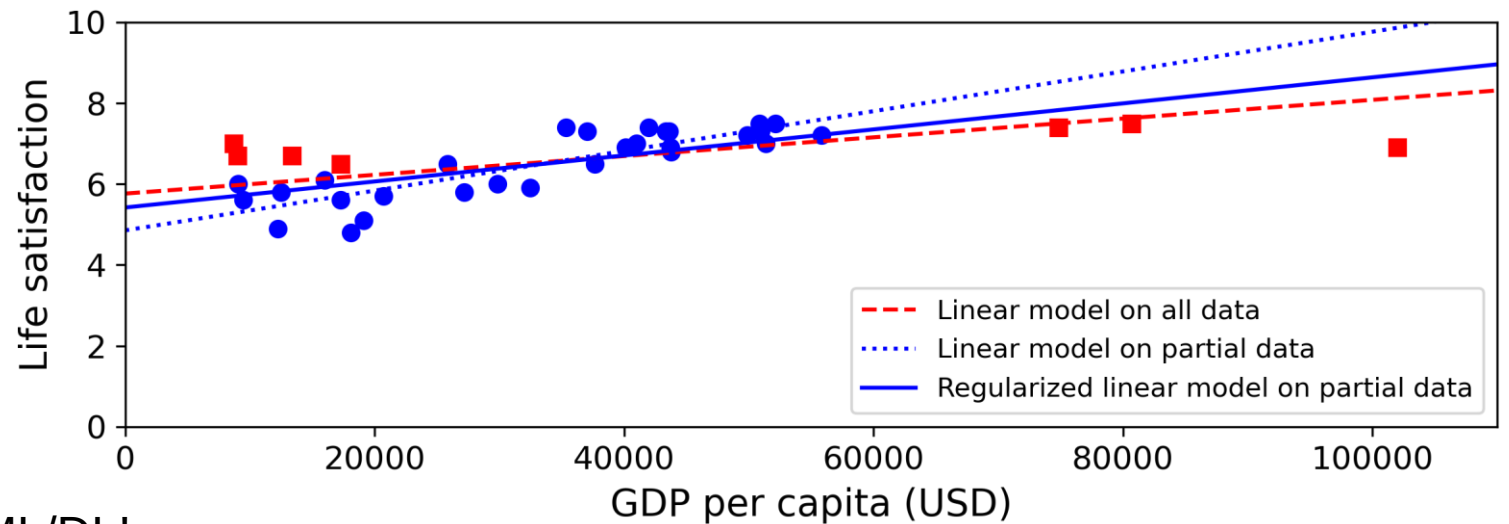




# Die wichtigsten Herausforderungen beim Machine Learning

## Overfitting der Trainingsdaten

- Regularisierung
  - Begrenzung des Wertebereichs der Modellparameter
  - Allgemeiner: Einschränkung der Freiheitsgrade des Modells

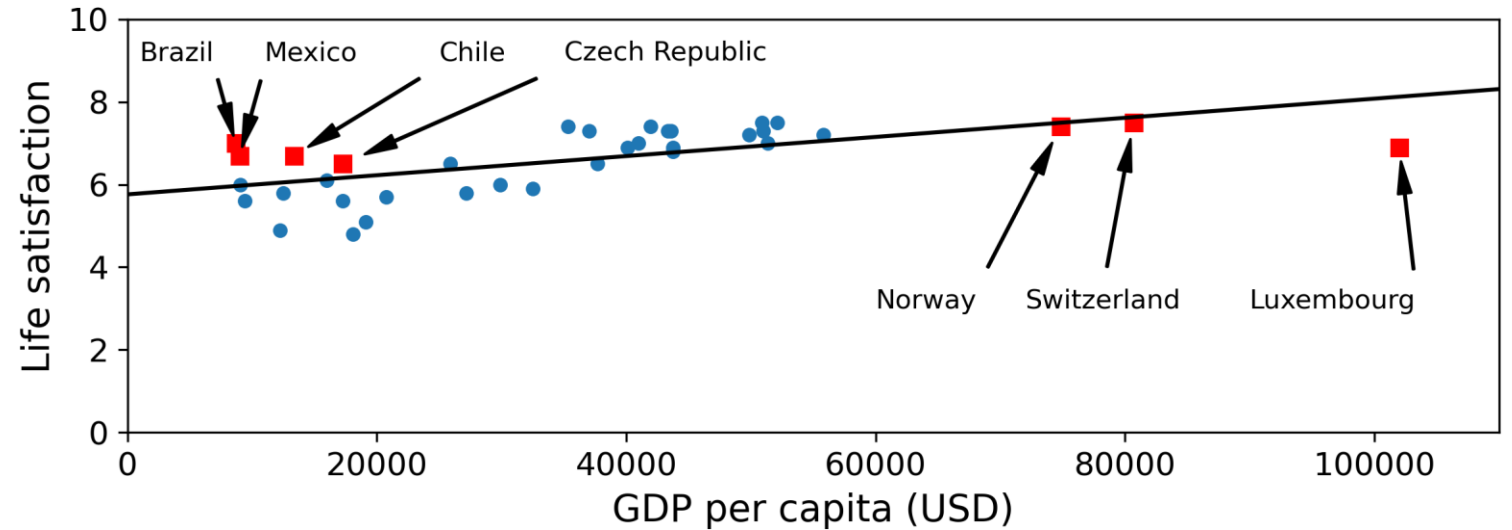


- SEHR wichtiges Konzept in ML/DL!
- Werden wir in Vorlesung sehr häufig sehen

# Die wichtigsten Herausforderungen beim Machine Learning

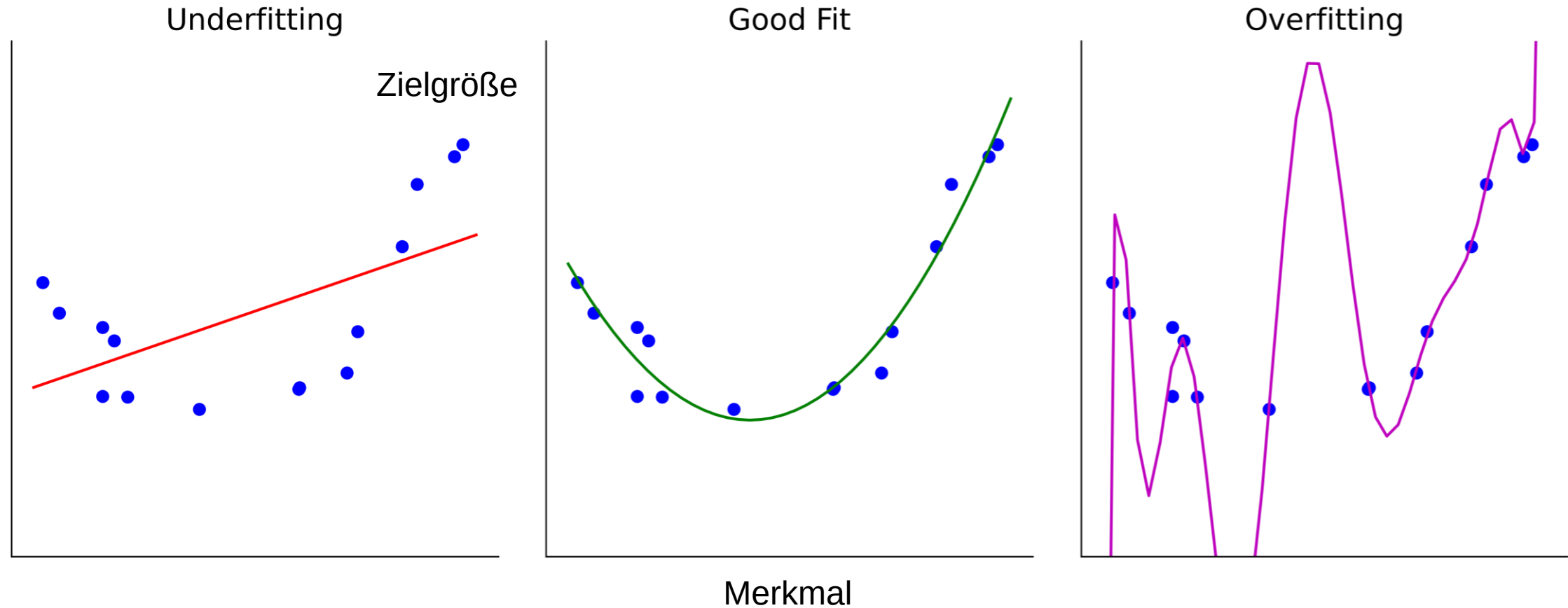
## Underfitting der Trainingsdaten

- Gegenteil von Overfitting
- Unser lineares Modell underfittet die Trainingsdaten
- Lösungen?
  - Ein komplexeres Modell mit mehr Parametern wählen
  - Mehr relevante Merkmale messen/berechnen
  - Auswirkung der Regularisierung verkleinern



# Die wichtigsten Herausforderungen beim Machine Learning

## Over- und Underfitting der Trainingsdaten



# Machine Learning Grundlagen

## Zusammenfassung und Fragen

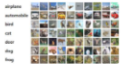
- Beim Machine Learning geht es darum, Maschinen bei der Lösung einer Aufgabe zu verbessern, indem sie aus Daten lernen, anstatt explizit definierte Regeln zu erhalten.
- In einem ML-Projekt sammeln Sie Daten in einem Trainingsdatensatz und speisen diesen in einen Lernalgorithmus ein. Wenn der Algorithmus auf einem Modell basiert, tut er einige Parameter, um das Modell an die Trainingsdaten anzupassen (d.h., um gute Vorhersagen auf den Trainingsdaten selbst zu treffen). Danach ist es hoffentlich in der Lage, auch für neue Daten gute Vorhersagen zu treffen. Wenn der Algorithmus instanzbasiert ist, lernt er die Beispiele einfach auswendig und verallgemeinert auf neue Instanzen durch ein Ähnlichkeitsmaß, um sie mit den bekannten Instanzen zu vergleichen.
- Wenn der Trainingsdatensatz zu klein ist oder die Daten nicht repräsentativ, verrauscht oder durch irrelevante Merkmale verunreinigt sind, wird das System keine hohe Leistung erbringen (Müll rein, Müll raus). Schließlich darf Ihr Modell weder zu einfach (dann underfittet es) noch zu komplex sein (dann overfittet es).

# Recherche von Veröffentlichungen (und Datensätzen)

- scholar.google.de
- paperswithcode.com
- semanticscholar.org

🔔 Share your dataset with the ML community!

7859 dataset results



**CIFAR-10**  
The CIFAR-10 dataset (Canadian Institute for Advanced Research, 10 classes) is a subset of the Tiny Images dataset and consists of 60000 32x32 color images. The images are labelled with...  
10,753 PAPERS • 68 BENCHMARKS



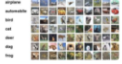
**ImageNet**  
The ImageNet dataset contains 14,197,122 annotated images according to the WordNet hierarchy. Since 2010 the dataset is used in the ImageNet Large Scale Visual Recognition Challenge...  
10,256 PAPERS • 98 BENCHMARKS



**COCO (Microsoft Common Objects in Context)**  
The MS COCO (Microsoft Common Objects in Context) dataset is a large-scale object detection, segmentation, key-point detection, and captioning dataset. The dataset consists of 328K...  
7,315 PAPERS • 80 BENCHMARKS



**MNIST**  
The MNIST database (Modified National Institute of Standards and Technology database) is a large collection of handwritten digits. It has a training set of 60,000 examples, and a test set of...  
5,980 PAPERS • 50 BENCHMARKS



**CIFAR-100**  
The CIFAR-100 dataset (Canadian Institute for Advanced Research, 100 classes) is a subset of the Tiny Images dataset and consists of 60000 32x32 color images. The 100 classes in the...  
5,434 PAPERS • 44 BENCHMARKS



**Cityscapes**

Google Scholar

federated learning

Ungefähr 8.970 Ergebnisse (0,05 Sek.)

Artikel

Beliebige Zeit

Seit 2021

Seit 2020

Seit 2017

Zeitraum wählen...

Nach Relevanz sortieren

Nach Datum sortieren

Beliebige Sprache

Seiten auf Deutsch

Alle Typen

☐ Patente einschließen

☒ Zitate einschließen

Übersichtsarbeiten

☒ Alert erstellen

**[HTML] Federated learning for healthcare informatics**  
[J Xu](#), [BS Glicksberg](#), [C Su](#), [P Walker](#), [J Bian](#) ... - Journal of Healthcare ..., 2021 - Springer  
With the rapid development of computer software and hardware technologies, more and more healthcare data are becoming readily available from clinical institutions, patients, insurance companies, and pharmaceutical industries, among others. This access provides ...  
☆ 99 Zitiert von: 121 Ähnliche Artikel Alle 7 Versionen

**Secureboost: A lossless federated learning framework**  
[K Cheng](#), [T Fan](#), [Y Jin](#), [Y Liu](#), [T Chen](#) ... - IEEE Intelligent ..., 2021 - ieeexplore.ieee.org  
The protection of user privacy is an important concern in machine learning, as evidenced by the rolling out of the General Data Protection Regulation (GDPR) in the European Union (EU) in May 2018. The GDPR is designed to give users more control over their personal ...  
☆ 99 Zitiert von: 142 Ähnliche Artikel Alle 9 Versionen

**Ditto: Fair and robust federated learning through personalization**  
[T Li](#), [S Hu](#), [A Beirami](#), [V Smith](#) - ... on Machine Learning, 2021 - proceedings.mlr.press  
Fairness and robustness are two important concerns for federated learning systems. In this work, we identify that robustness to data and model poisoning attacks and fairness, measured as the uniformity of performance across devices, are competing constraints in ...  
☆ 99 Zitiert von: 12 Ähnliche Artikel Alle 3 Versionen

**Communication-efficient federated learning**  
[M Chen](#), [N Shlezinger](#), [HV Poor](#) ... - Proceedings of the ..., 2021 - National Acad Sciences  
Federated learning (FL) enables edge devices, such as Internet of Things devices (eg, sensors), servers, and institutions (eg, hospitals), to collaboratively train a machine learning (ML) model without sharing their private data. FL requires devices to exchange their ML ...  
☆ 99 Zitiert von: 13 Ähnliche Artikel Alle 6 Versionen

[HTML] springer.com

[PDF] ieee.org

[PDF] mlr.press

[PDF] weizmann.ac.il

SEMANTIC SCHOLAR

A free, AI-powered research tool for scientific literature

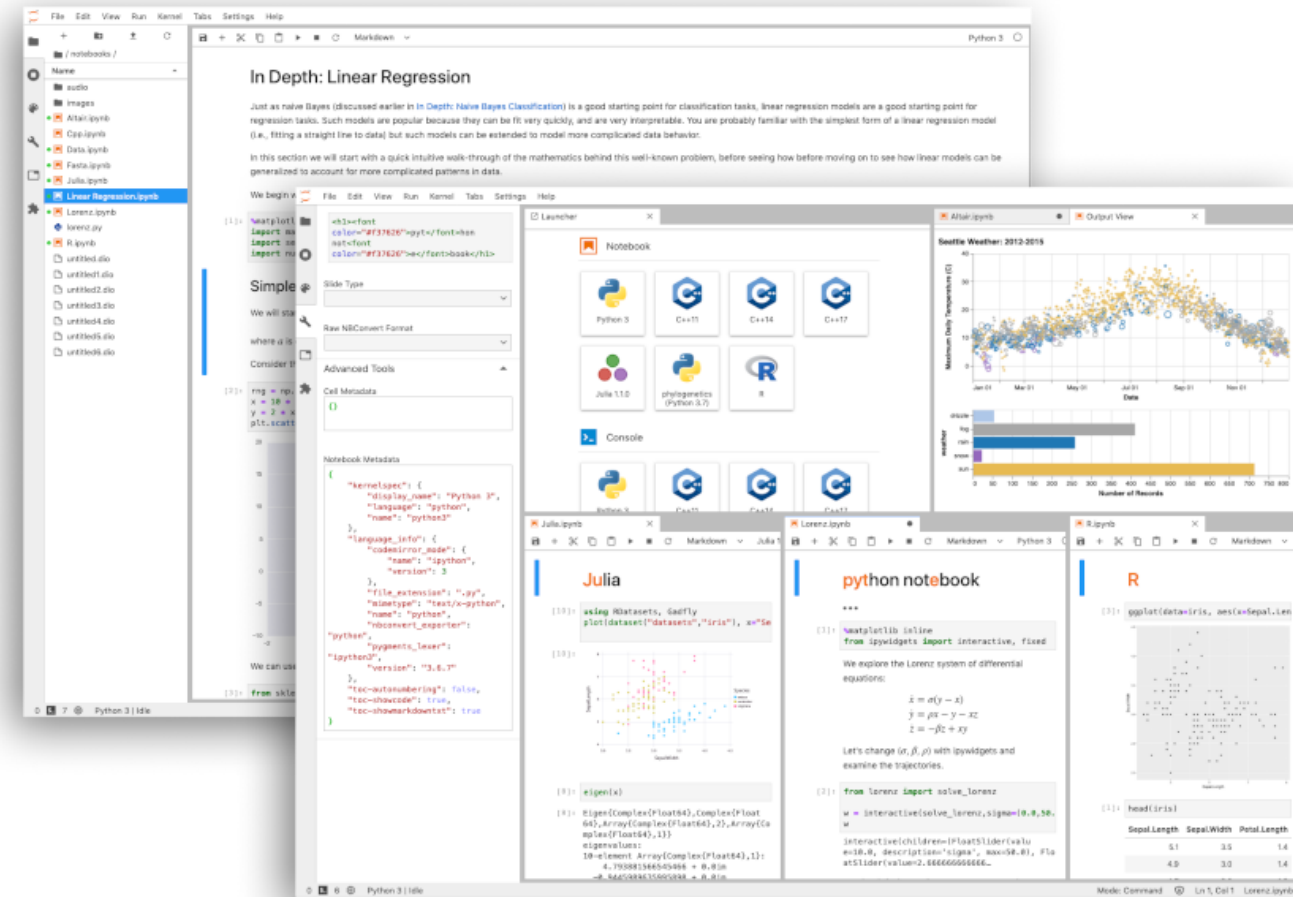
Search 211.634.114 papers from all fields of science

Search

Try: [G. Lang Farmer](#) • [Vikings](#) • [Brownian Motion](#)

# Hausaufgabe

- Lokale Installation:
  - Anaconda (oder Miniconda),  
<https://www.anaconda.com/products/individual>
    - Enthält Python und viele Standard Bibliotheken
    - Jupyter Notebook oder Jupyter Lab
    - Pandas, Scikit-learn, Matplotlib
    - Später: TensorFlow
  - environment.yml in ILU
- Cloud Umgebung:
  - Google Colab



# Nächste Vorlesung und Fragen

- Ein Machine Learning Projekt von A bis Z
- Fragen?