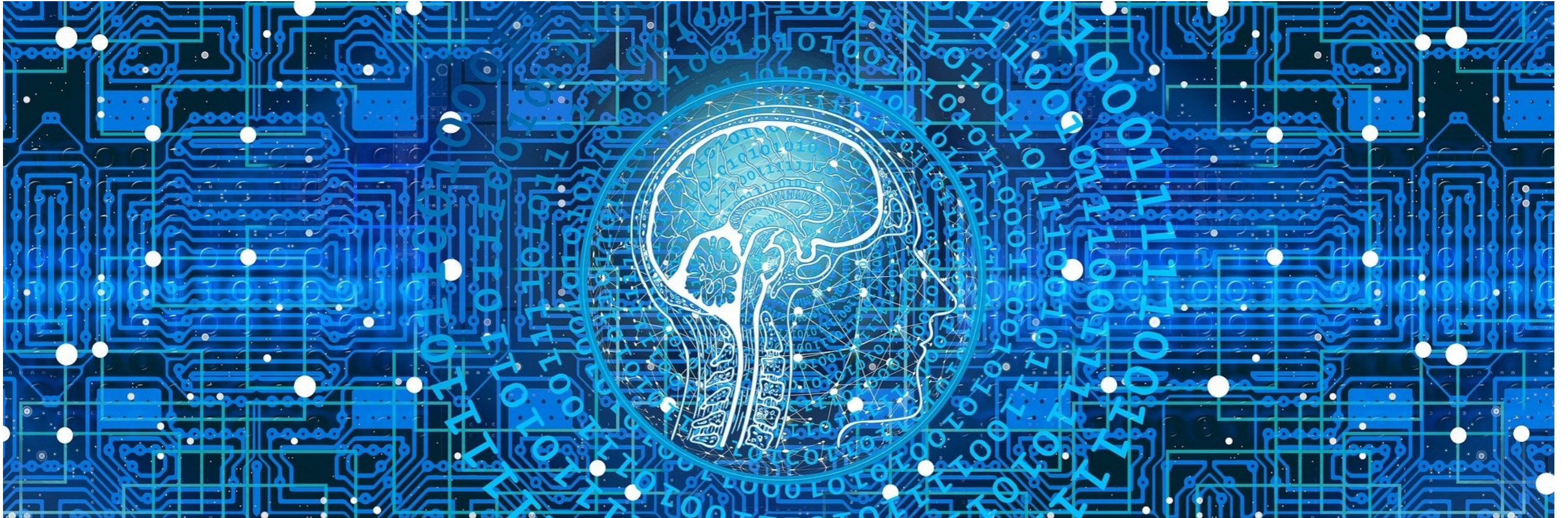


Einführung in die künstliche Intelligenz



Annika Liebgott, M.Sc.

28. Oktober 2021, Vortragsreihe „Künstliche Intelligenz“ VDE Kassel e.V.

Kurzvorstellung Annika Liebgott

- 2009 – 2016:** Studium der Elektrotechnik und Informationstechnik, Universität Stuttgart
- Seit 2016:** Promotion zum Thema „A comparative Study of Feature-based Machine Learning and Deep Learning for Medical Imaging Applications“, Universität Stuttgart
- 2016 – 2019:** Wiss. Mitarbeiterin in der Abteilung für Diagnostische und Interventionelle Radiologie, Universitätsklinikum Tübingen
- 2019 – 2021:** Wiss. Mitarbeiterin am Institut für Signalverarbeitung und Systemtheorie, Universität Stuttgart
- Seit 2020:** Lehrauftrag „Maschinelles Lernen“, Bachelor Informatik, DHBW Stuttgart
- Aktuell:** Elternzeit

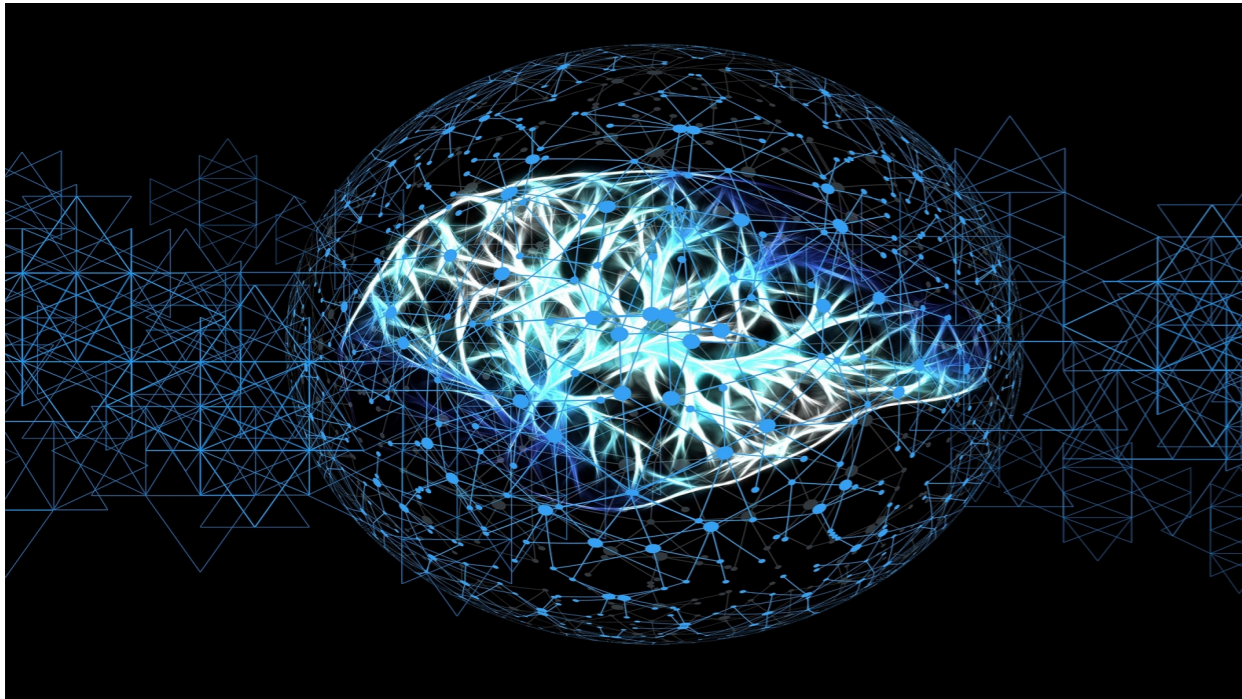


Künstliche Intelligenz und maschinelles Lernen

Was ist „künstliche Intelligenz“?

Als „künstliche Intelligenz“ oder „KI“ bezeichnet man

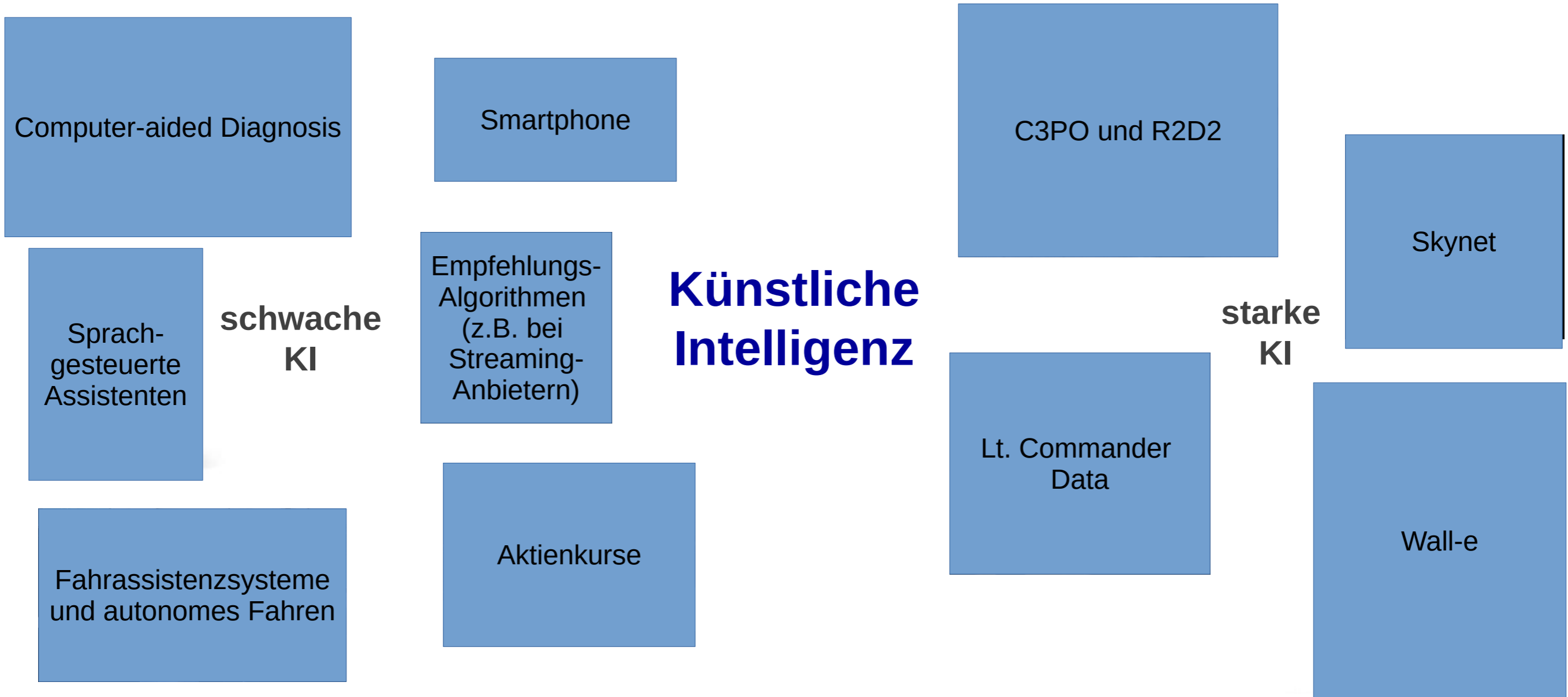
- Allgemein: Computerprogramme und Algorithmen, die menschliche Intelligenz imitieren
- In Filmen, Büchern etc. auch fortschrittliche, künstliche Lebensformen



Künstliche Intelligenz...

- wurde bereits Anfang des 20. Jahrhunderts von Forschern diskutiert
- konnte in frühen Formen schon in den 1950er Jahren realisiert werden (z.B. ELIZA, 1957)
- Ist heute längst auf vielfältige Weise in unseren Alltag integriert (z.B. Computerspiele, Social Media, Handykameras,...)

Künstliche Intelligenz – Science Fiction vs. Realität

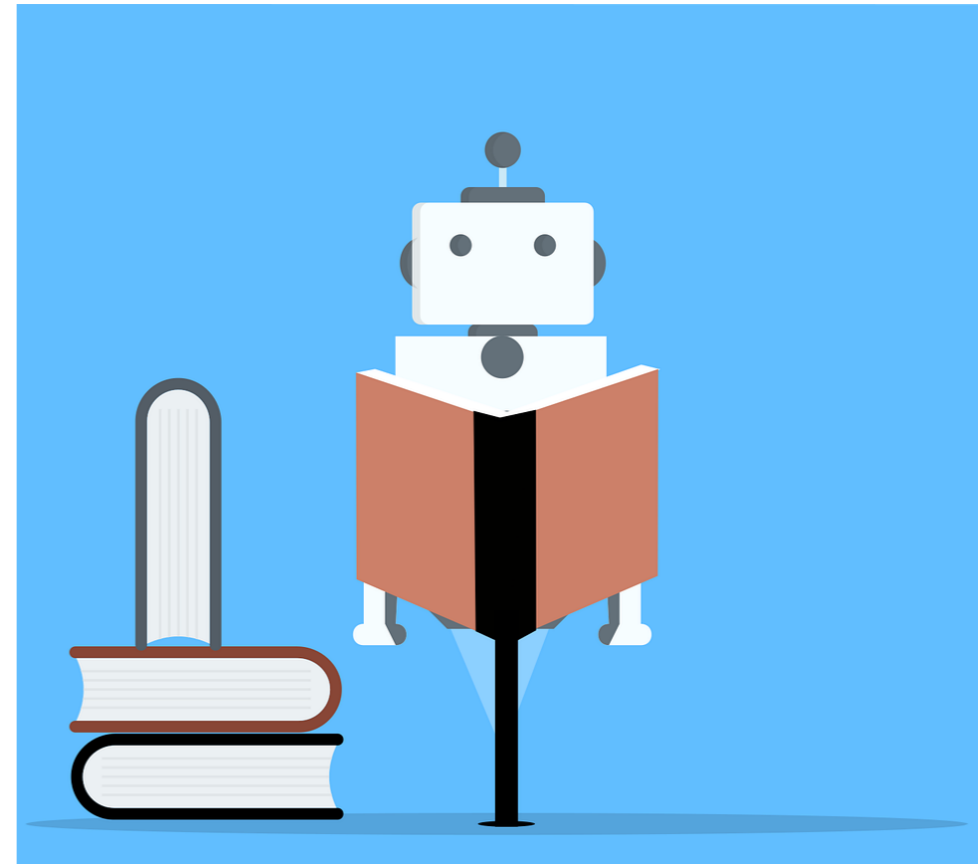


Maschinelles Lernen

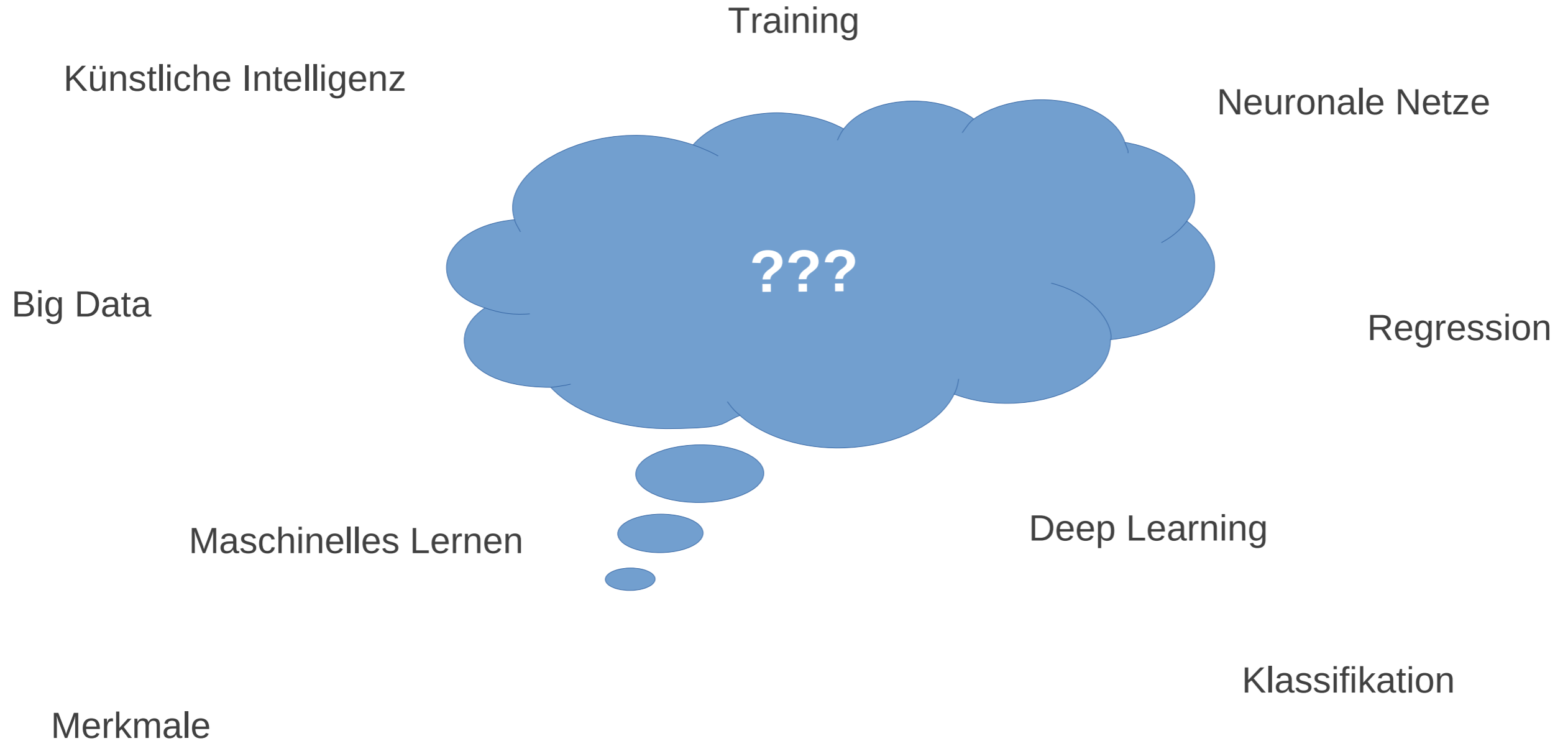
Was versteht man unter maschinellem Lernen (ML)?

- Teilgebiet der Mathematik, Informatik und Signalverarbeitung
- Algorithmen, mit deren Hilfe Computermodellen das selbstständige Lösen bestimmter Aufgaben beigebracht werden kann
- Hintergrund: aus Daten (z.B. Bildern) relevante Informationen gewinnen und diese verarbeiten

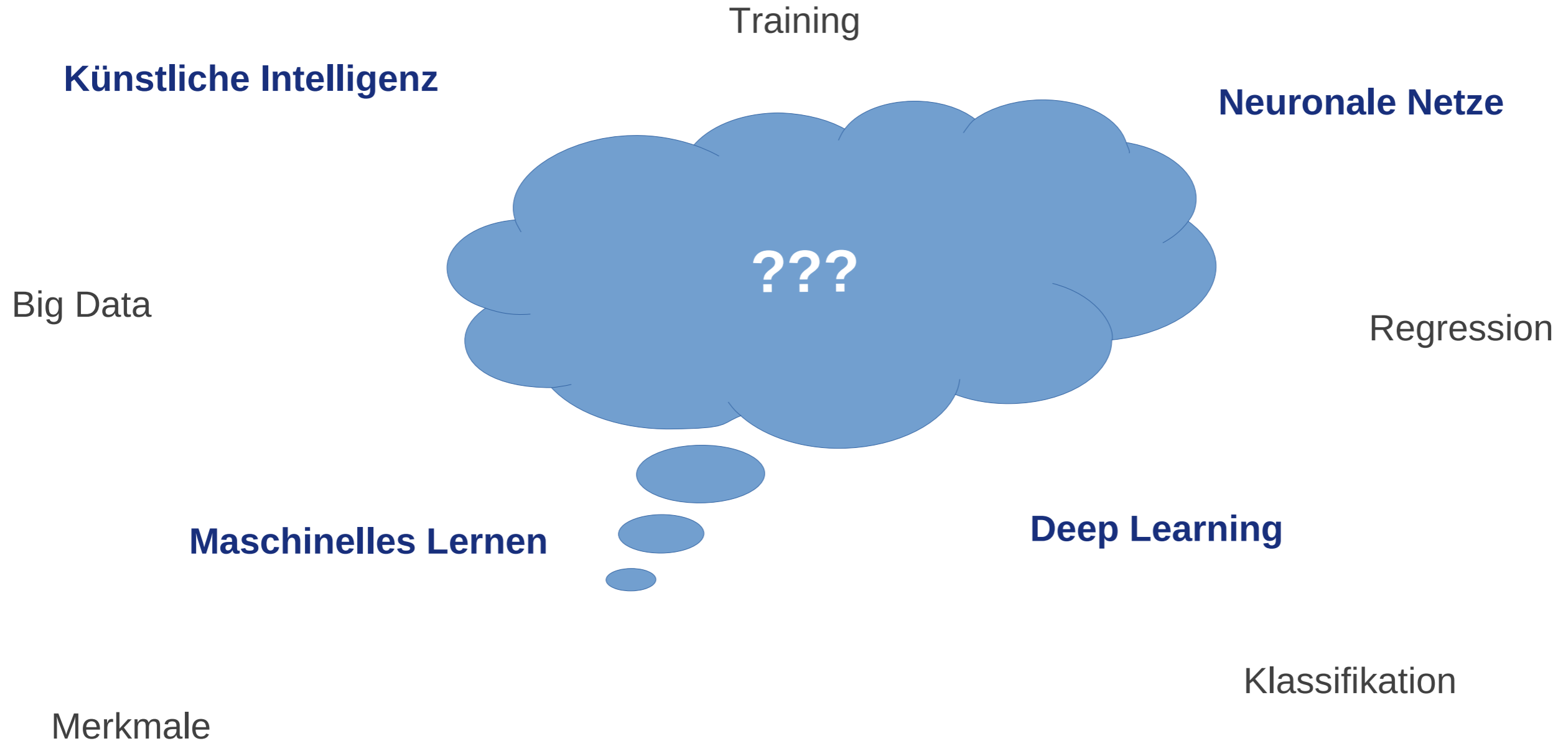
➔ **Werkzeug, um KI in der Praxis umzusetzen**



KI und maschinelles Lernen



KI und maschinelles Lernen



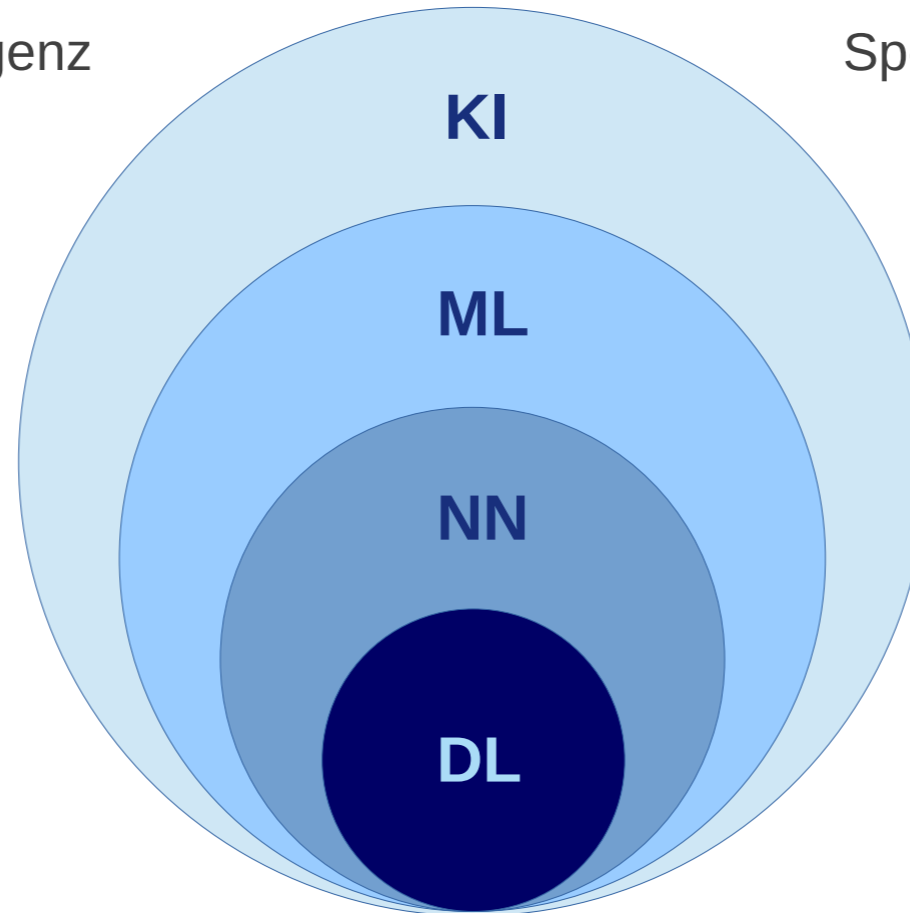
Zusammenhang KI/ML

Künstliche Intelligenz (KI)

Nachahmung menschlicher Intelligenz

(künstliche) neuronale Netze (NN)

Spezielle Methodenfamilie im ML



Maschinelles Lernen (ML)

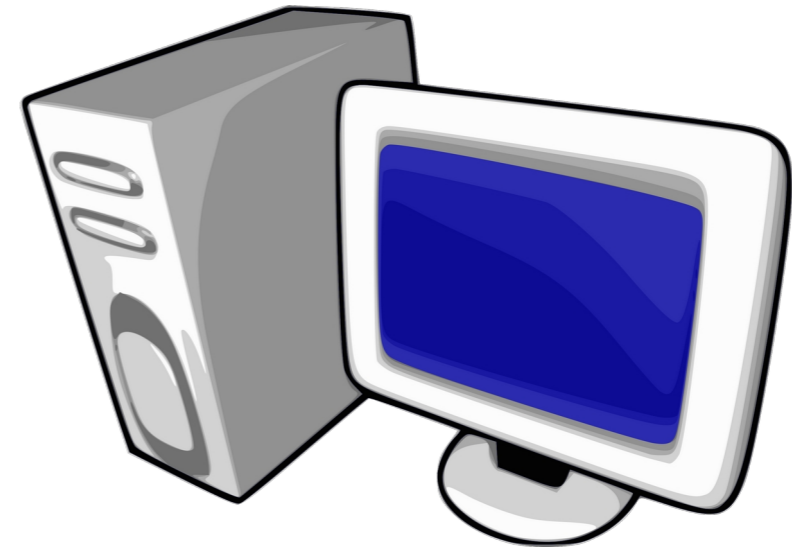
Algorithmen, mit denen KI realisiert werden kann

Deep Learning (DL)

Wichtigstes Teilgebiet der NN-Algorithmen

Wie lernt eine Maschine?

Hund oder Katze?



Der Klassifikator

Was ist ein Klassifikator?

- Ein Algorithmus bzw. Computermmodell im Bereich des maschinellen Lernens
- Kann darauf trainiert werden, Daten zu charakterisieren
- Lernt, eine stark begrenzte Menge an Aufgaben durchzuführen
 - ➔ z.B.: Erkennung eines Objekts, Unterscheidung verschiedener Objekte



Verschiedene Typen von ML-Systemen

Maschinelles Lernen = einem Computermodell beibringen, bestimmte Daten anhand bestimmter Eigenschaften zu erkennen

Mathematisch ausgedrückt: Optimierung einer Zielfunktion, z.B. Minimierung einer Loss-Funktion

Klassifikation

Der Algorithmus ordnet jedem Datenpunkt ein *diskretes Klassenlabel* zu

Beispiel: Covid-19 oder kein Covid-19?

Regression

Der Algorithmus ordnet jedem Datenpunkt ein *kontinuierliches Klassenlabel* zu

Beispiel: Wahrscheinlichkeit, zu erkranken

Supervised Learning

Der Algorithmus *kennt das wahre Klassenlabel* von jedem Datenpunkt im Trainingsset

→ Modell *lernt Beziehung* zwischen Datenpunkten und den zugehörigen Klassenlabels

Unsupervised Learning

Der Algorithmus *kennt das wahre Klassenlabel* von jedem Datenpunkt im Trainingsset *nicht*

→ Modell *sucht selbstständig nach Mustern* in den Trainingsdaten

Trainingsphase vs. Produktivbetrieb

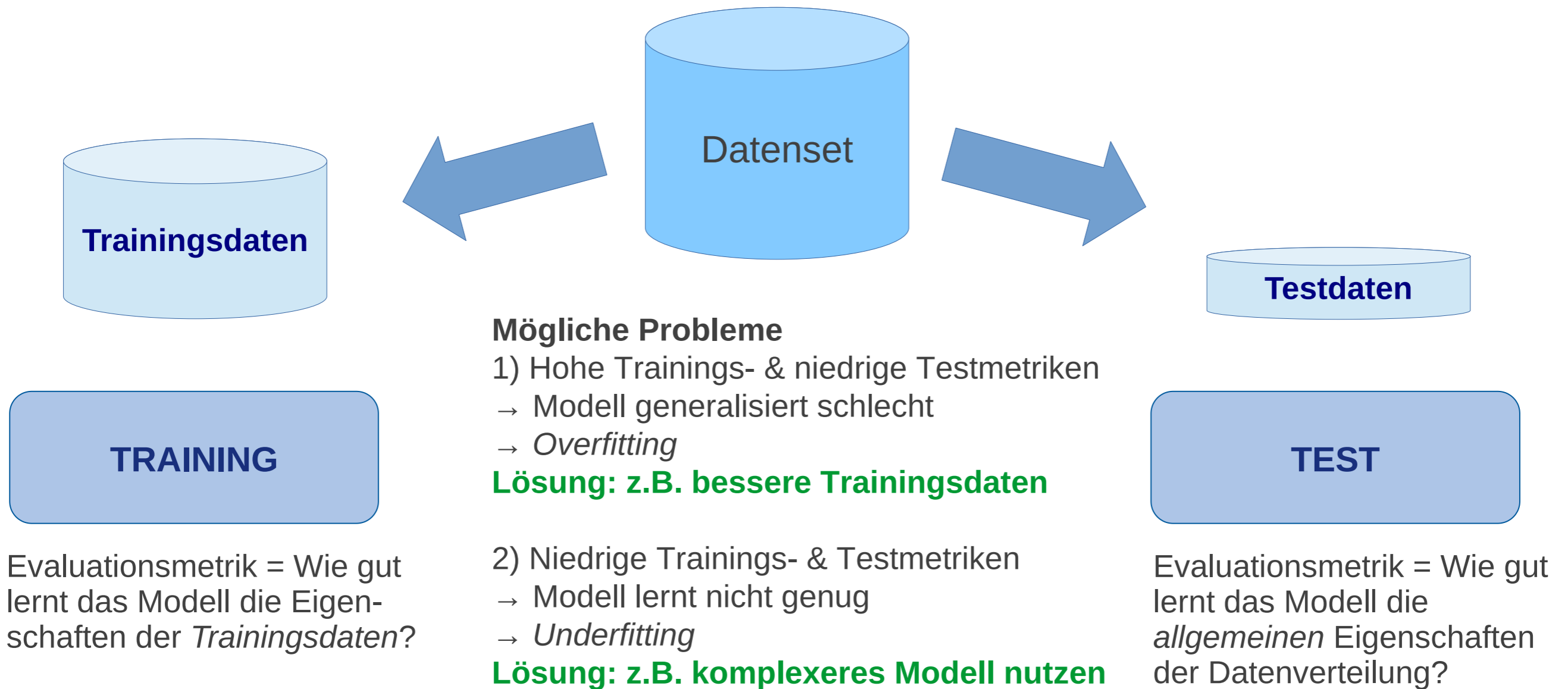
Trainingsphase



Produktivbetrieb

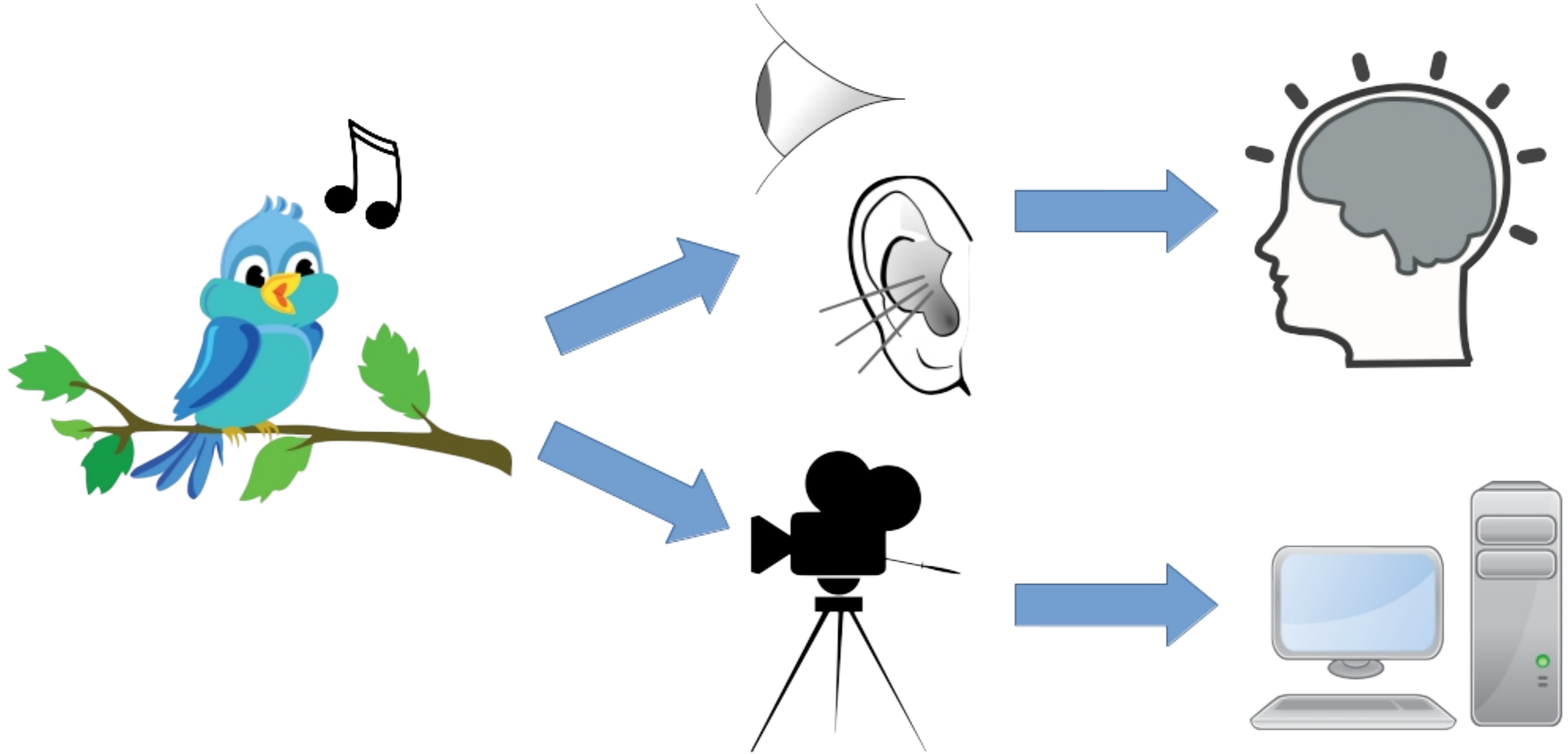


Überprüfen des trainierten Modells



Merkmalsbasiertes maschinelles Lernen

Merkmale erkennen und verarbeiten



Merkmale aus Sicht des Menschen

Ein Mensch...

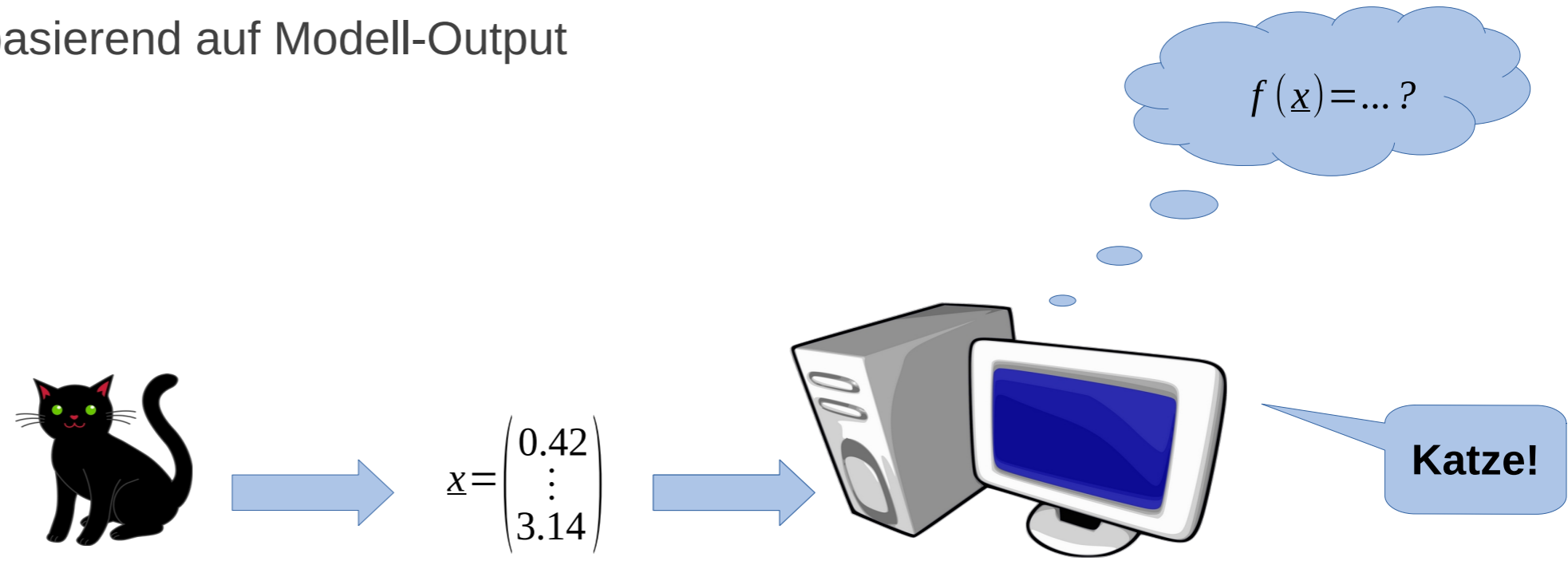
- sieht ein Objekt an
- erkennt automatisch wichtige Eigenschaften
- ruft in seinem Gedächtnis Wissen über ähnliche Objekte ab
- identifiziert das Objekt basierend auf seiner gesamten Erfahrung



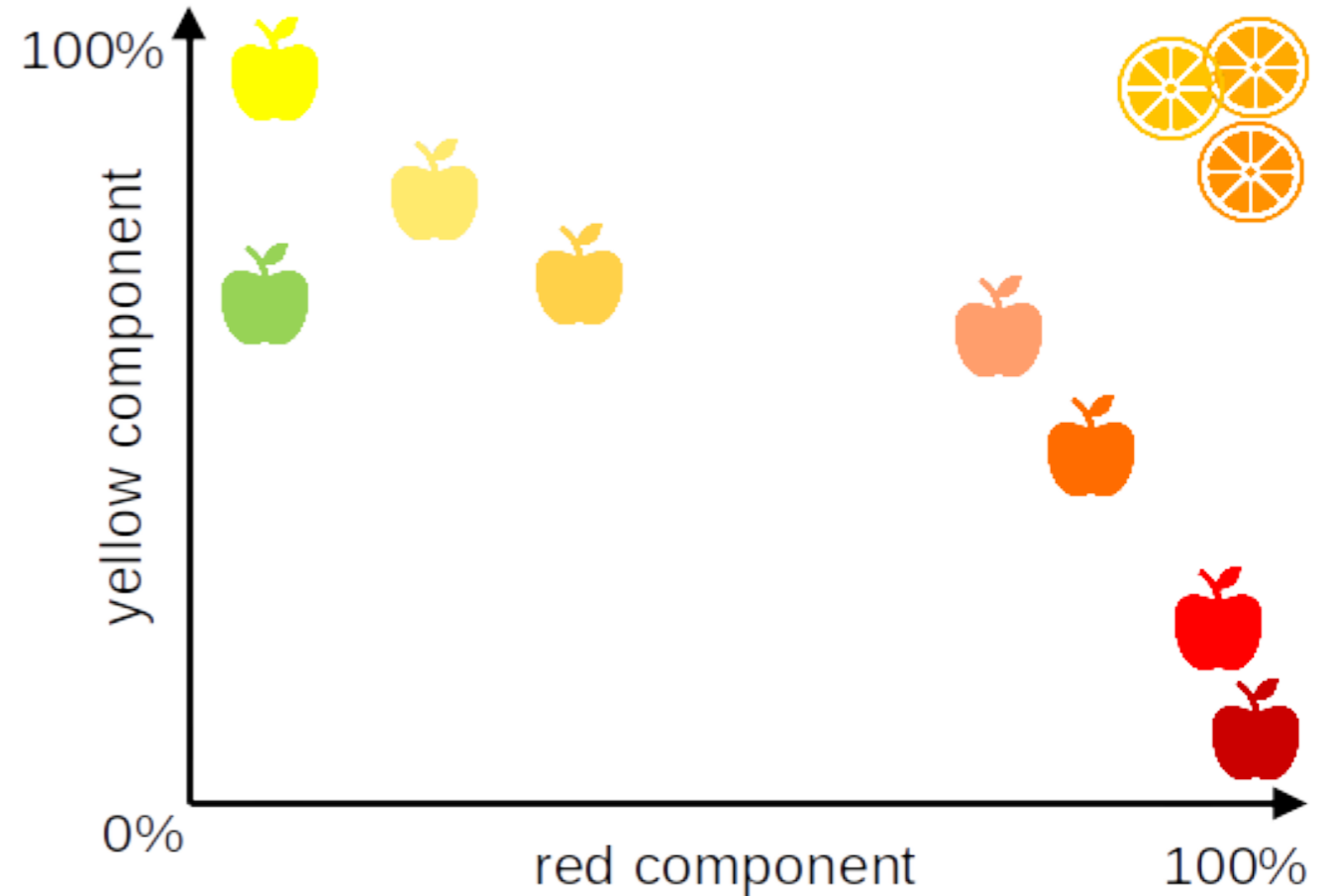
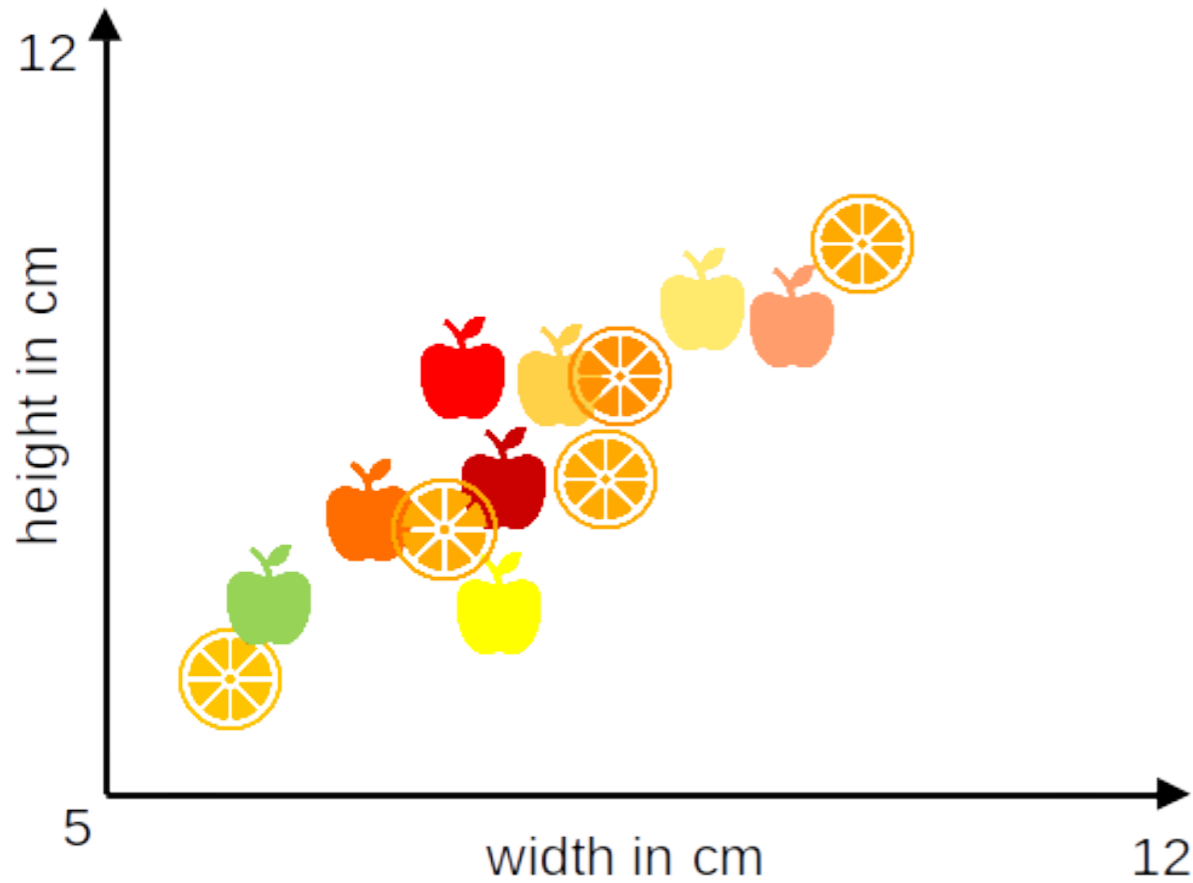
Merkmale aus Sicht des Computermodells

Ein Computermodell...

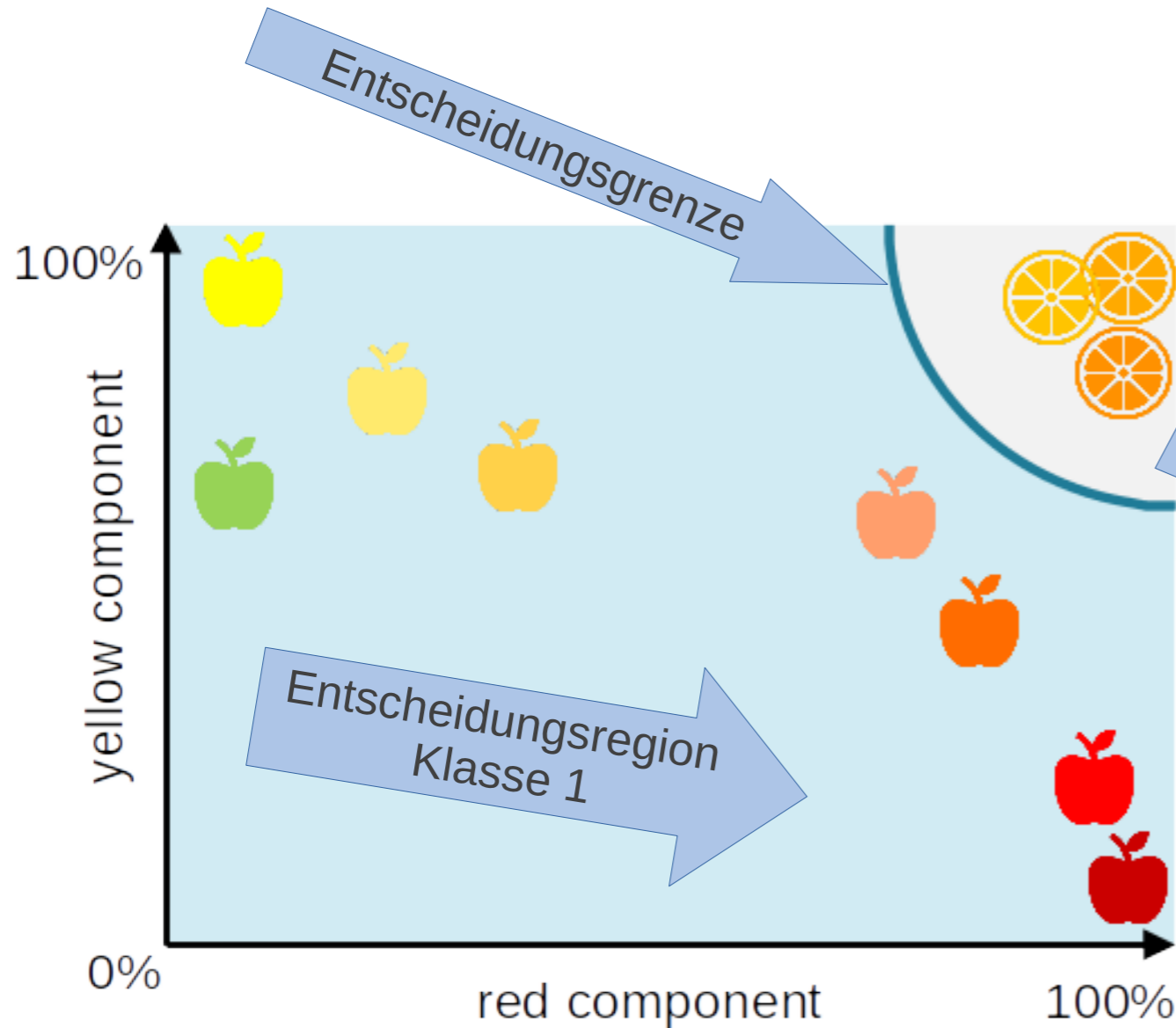
- sieht eine numerische Repräsentation des Objekts
- benötigt eine **numerische Repräsentation der Eigenschaften** \longrightarrow **Merkmale im ML**
- wendet ein Modell an, das mit Objekten mit ähnlichen Eigenschaften trainiert wurde
- identifiziert das Objekt basierend auf Modell-Output



Gute und schlechte Merkmale



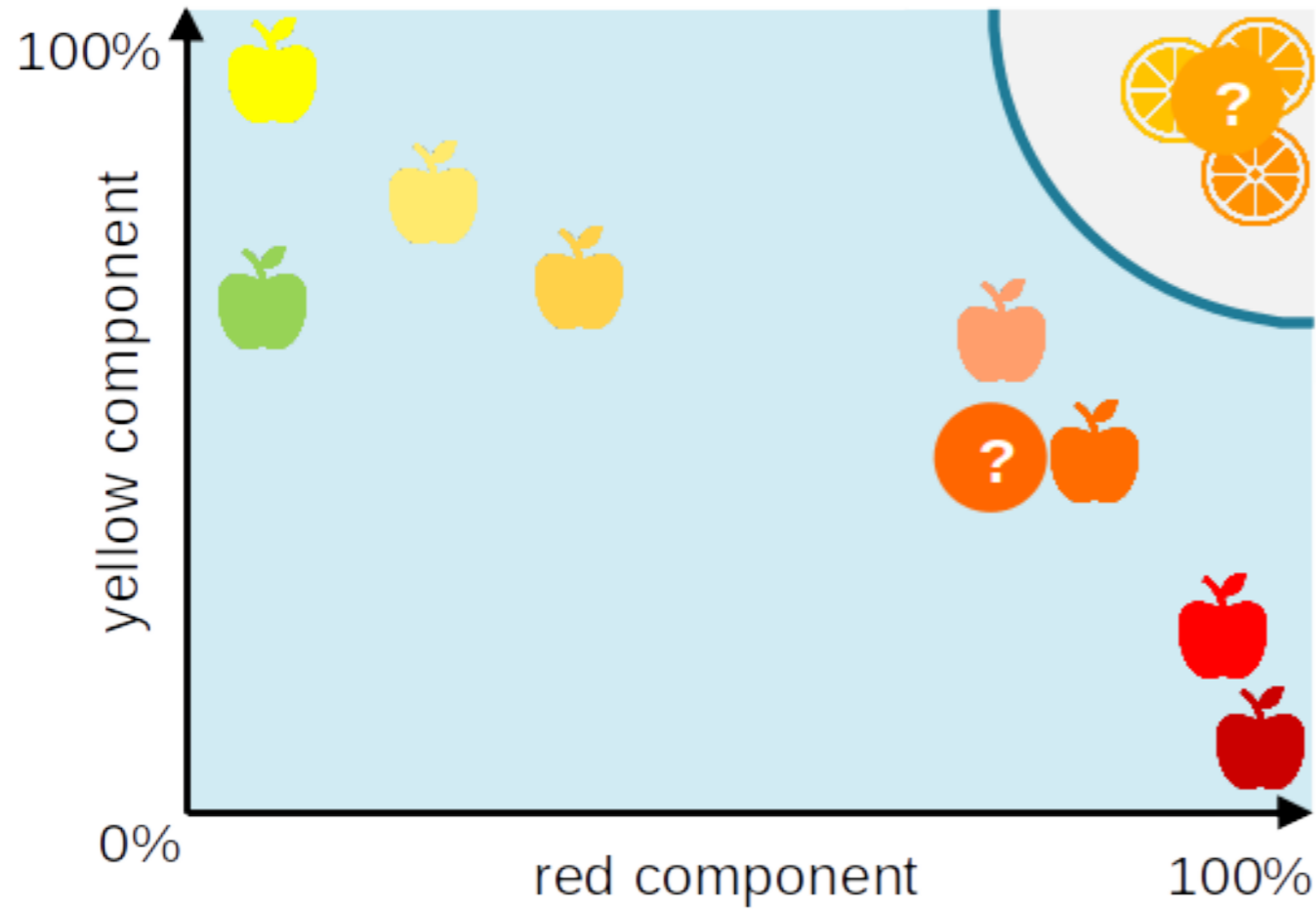
Und nach dem Training?



Der Klassifikator hat gelernt...

- wo im Merkmalsraum die Äpfel liegen und wo die Orangen
- wo er eine sinnvolle Grenze zwischen beiden „Obsträumen“ ziehen kann

Klassifikation neuer Daten



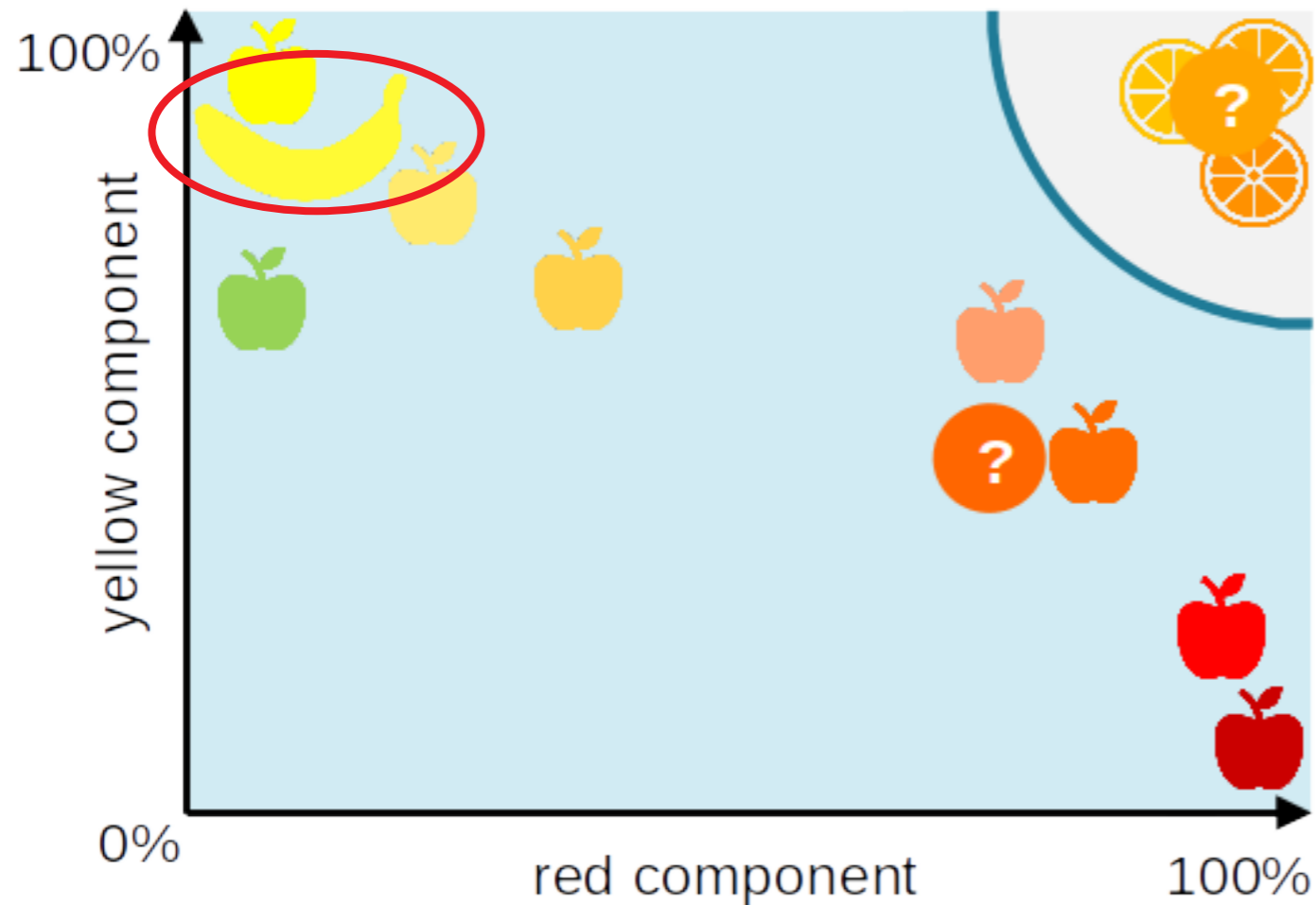
Wie werden neue Daten verarbeitet?

Sollen neue Früchte klassifiziert werden:

- Rot- und Gelbanteil der neuen Früchte wird berechnet
- Die Lage der Früchte im Merkmalsraum wird mit den gelernten Räumen und der Entscheidungsgrenze verglichen
- Entscheidung fällt für die Obstsorte, in deren „Obsträum“ sich die neue Frucht befindet

➡ Funktioniert gut für diese beiden Obstsorten

Grenzen des trainierten Klassifikators



Frage 1: Was passiert, wenn wir eine Banane klassifizieren möchten?

Der Klassifikator wird sich eindeutig für einen Apfel entscheiden

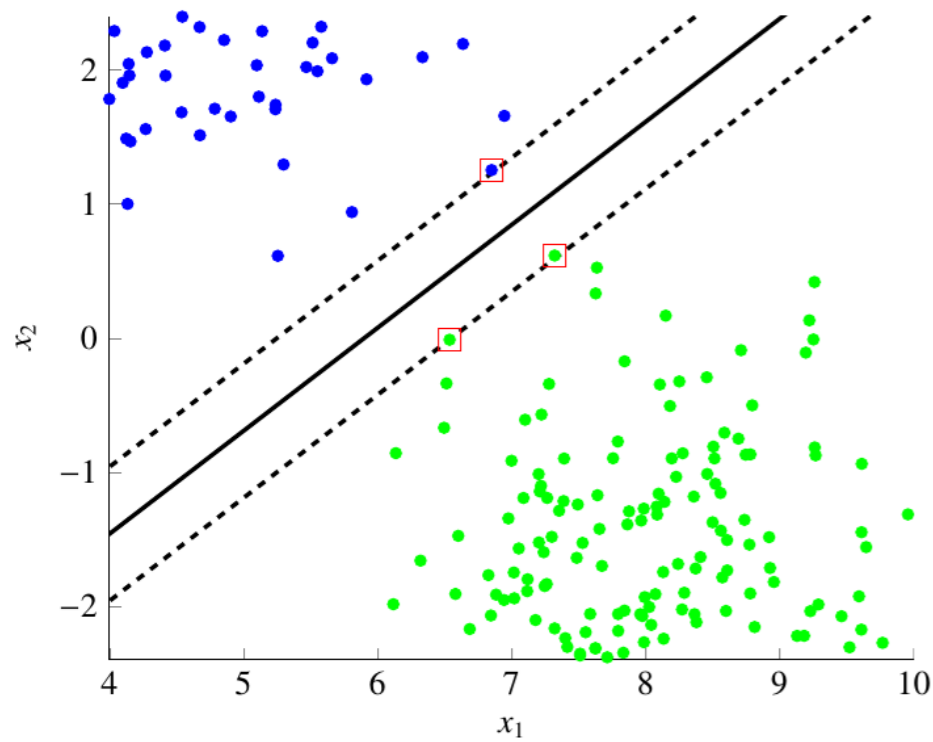
Frage 2: Was könnte man tun, um zusätzlich zu Orangen und Äpfeln auch Bananen zu erkennen?

Ein weiteres Merkmal, wie z.B. die Länge der Frucht mit dazu nehmen

➡ Aber: zur Erkennung weiterer Klassen muss in der Regel neu trainiert werden!

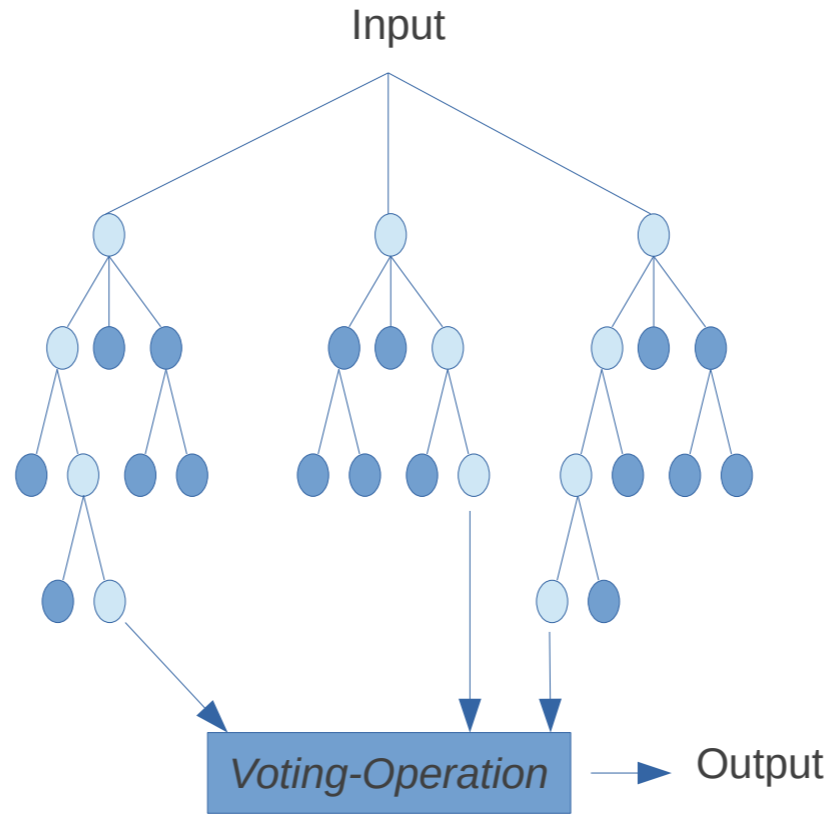
Beliebte merkmalsbasierte Klassifikatoren

Support Vector Machine



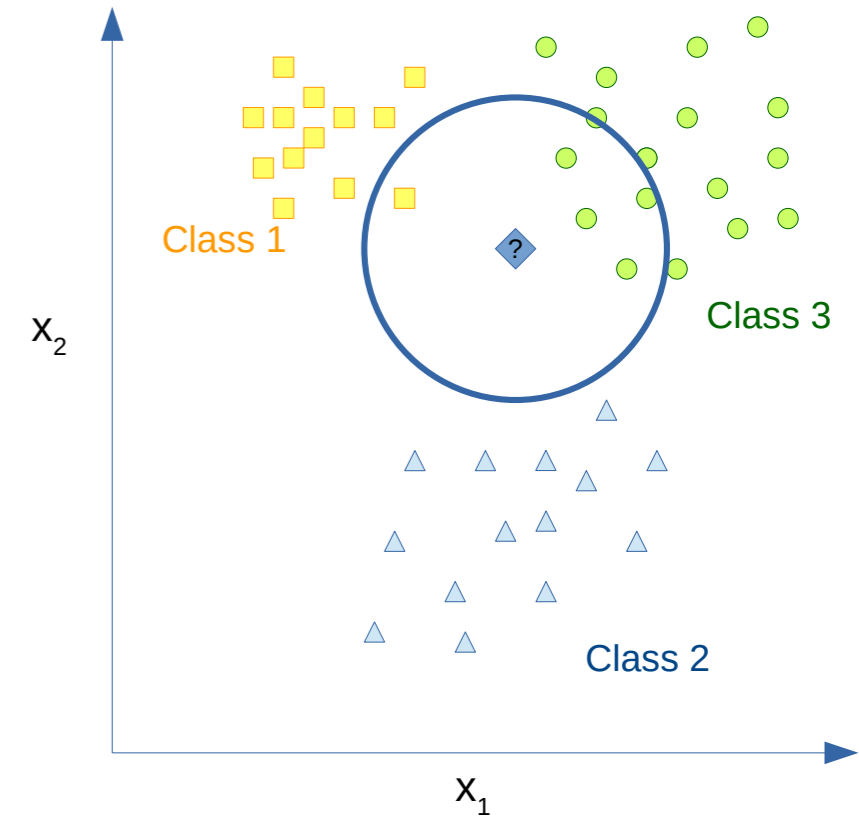
- Supervised Training
- Versucht, eine optimale Hyperebene zwischen zwei Klassen zu lernen

Random Forest



- Supervised Training
- Entscheidungsbaum-Ensemble
- Finaler Output basiert auf Mehrheits-Voting

k-Nearest Neighbor



- Supervised Training
- Klassifikator entscheidet für die Klasse, zu der die meisten Nachbardatenpunkte gehören

Neuronale Netze

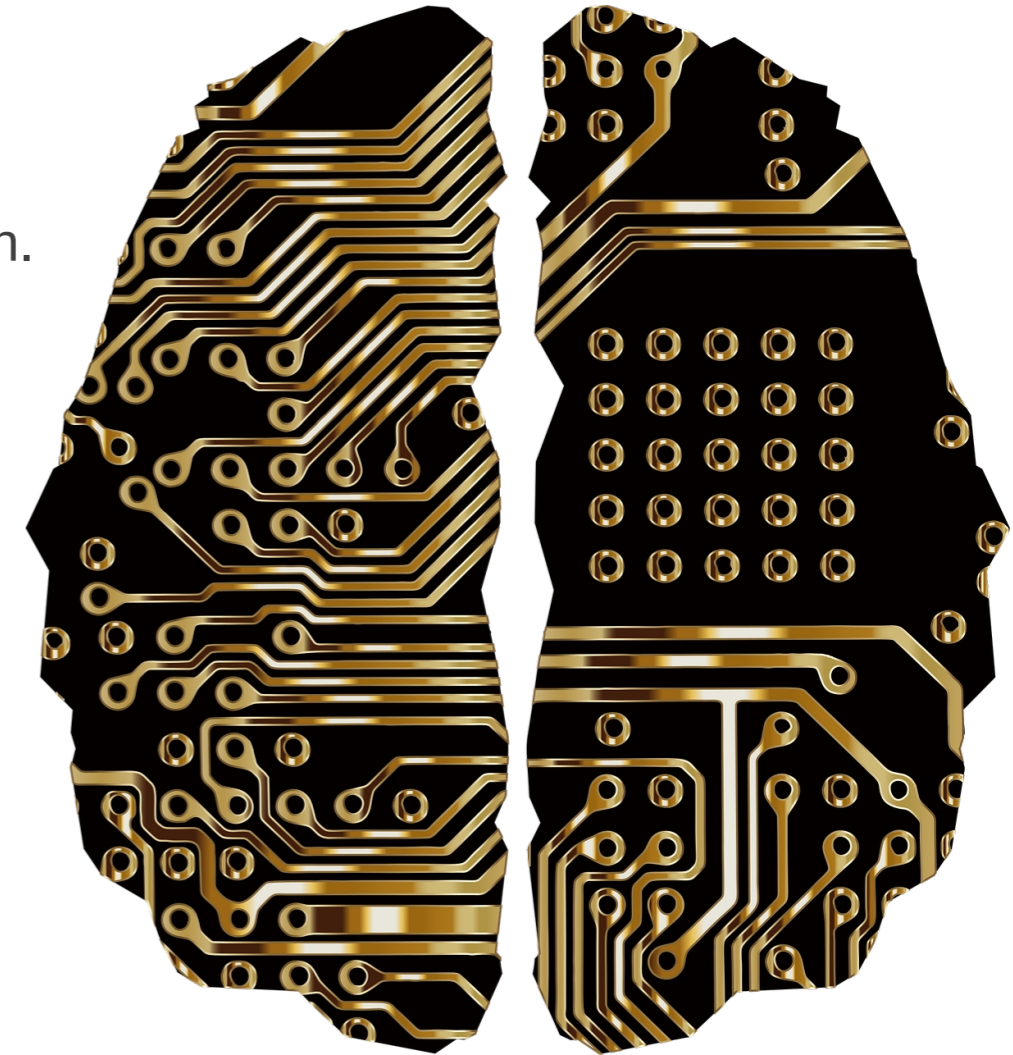
Biologische und künstliche neuronale Netze

Biologische neuronale Netze

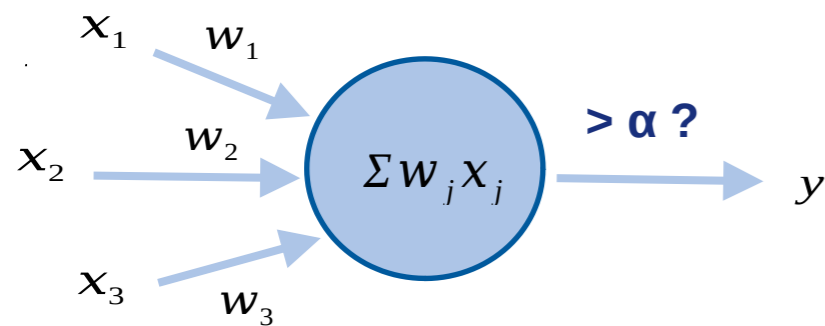
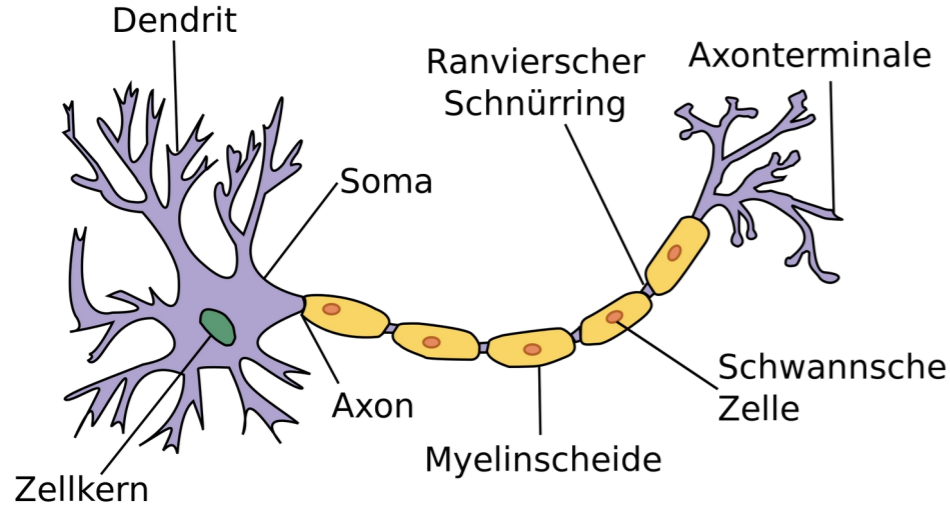
- Biologisches Neuron: Nervenzelle
- bestehen aus hochgradig vernetzten biologischen Neuronen
- sehr lernfähig, kann ausgezeichnet abstrahieren und sich anpassen.
- Biologisches neuronales Netz im Menschen: Gehirn

Künstliche neuronale Netze

- Künstliches Neuron: elektronische Schaltung oder Software
- versuchen, das Funktionsprinzip biologischer neuronaler Netze zu imitieren
- Großer Vorteil: sie können selbstständig relevante Merkmale in Daten suchen und erkennen
- Herzstück auf dem Weg zu stärkerer künstlicher Intelligenz



Ein künstliches Neuron



biologisch

künstlich

Dentriten: nehmen Eingangssignal auf gewichten Eingangssignal

$x_{1,2,3}$

$w_{1,2,3}$

Soma: summiert die gewichteten Eingangssignale

$\sum w_j x_j$

Axon: "feuert" wenn bestimmter Schwellwert überschritten wird

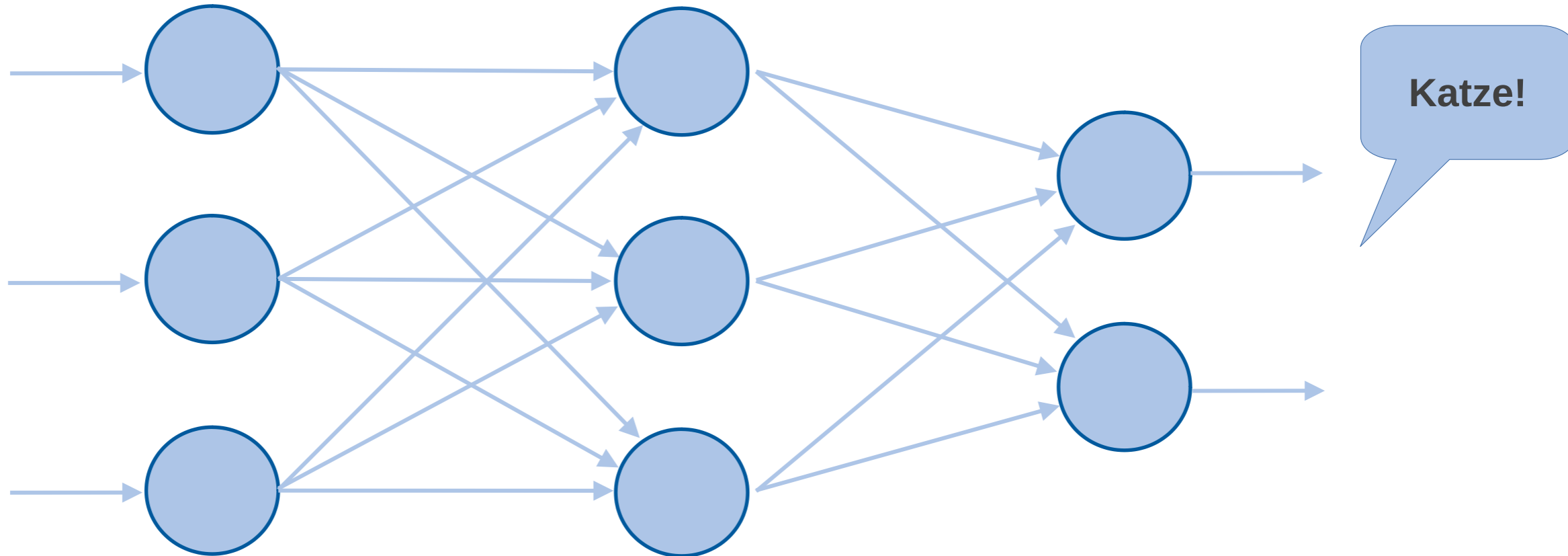
$> \alpha ?$

Axonterminale: geben Signal an andere Zellen weiter

y

➡ Künstliche Neuronen bilden biologische mit einfachen mathematischen Berechnungen nach

Aufbau eines neuronalen Netzes



Input
z.B. Bilder

Eingabeschicht
„Übersetzt“ die Daten
für das neuronale Netz

Versteckte Schicht
Lernt Eigenschaften
der Daten

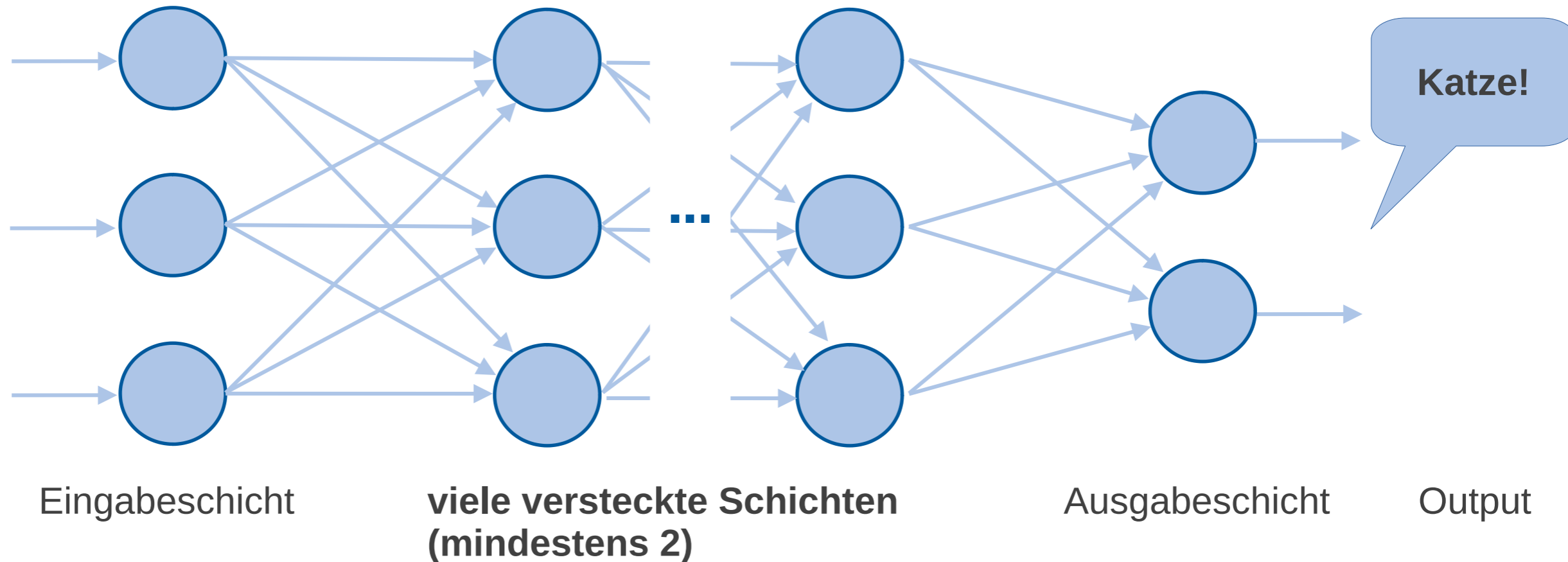
Ausgabeschicht
Verknüpft gelernte
Eigenschaften mit
der zu lösenden
Aufgabe

Output
z.B. Klasse

Deep Learning

Deep Learning (dt. „Tiefes Lernen“): Maschinelles Lernen mithilfe von tiefen neuronalen Netzen

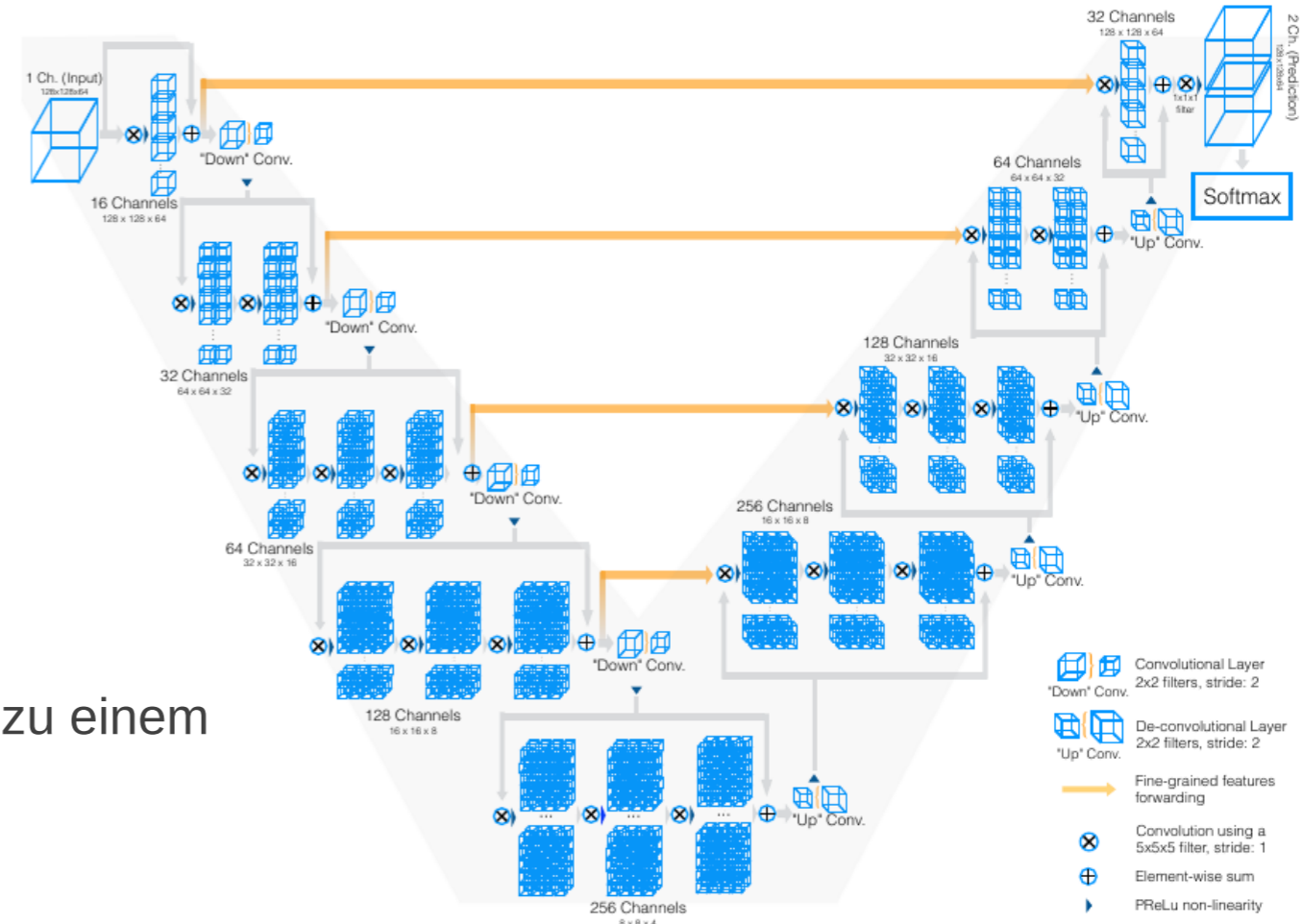
➔ Momentan wichtigstes und am schnellsten wachsendes ML-Teilgebiet



Deep-Learning-Architekturen

Netzwerk-Architekturen:

- Struktur eines neuronalen Netzwerks
 - Wie viele Neuronen?
 - Wie viele Schichten?
 - Welche Arten von Schichten?
 - Wie sind die Schichten miteinander verknüpft?
 - ...
- Herzstück eines jeden DL-Modells
- Die richtige Architektur auszuwählen ist der Schlüssel zu einem erfolgreichen DL-Modell!



Beispiel: V-Net-Architektur zur 3D-Bildverarbeitung (Milletari et al., ArXiv 2018)

Welche Architektur sich eignet, hängt von den zu verarbeitenden Daten ab!

Beispiel Bildverarbeitung - besonders erfolgreich: Convolutional Neural Networks (CNNs), nutzen Faltungsoperationen zur Merkmalsextraktion

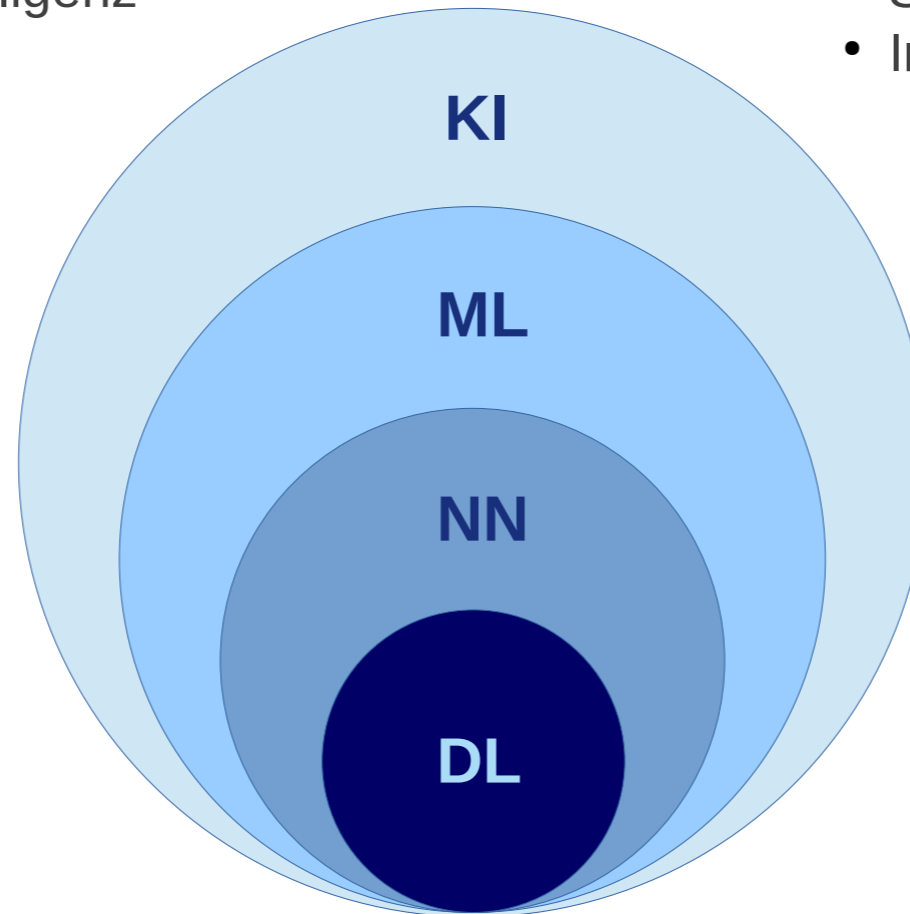
Zusammenfassung

Künstliche Intelligenz (KI):

- Nachahmung menschlicher Intelligenz
- Heute: schwache KI
- Zukunft: starke KI?

Maschinelles Lernen (ML):

- Algorithmen, mit denen KI realisiert werden kann
- Computermodelle lernen von Trainingsdaten wichtige Eigenschaften
- Modelle können dann Aussagen zu unbekanntem Daten mit ähnlichen Eigenschaften treffen



(künstliche) neuronale Netze (NN):

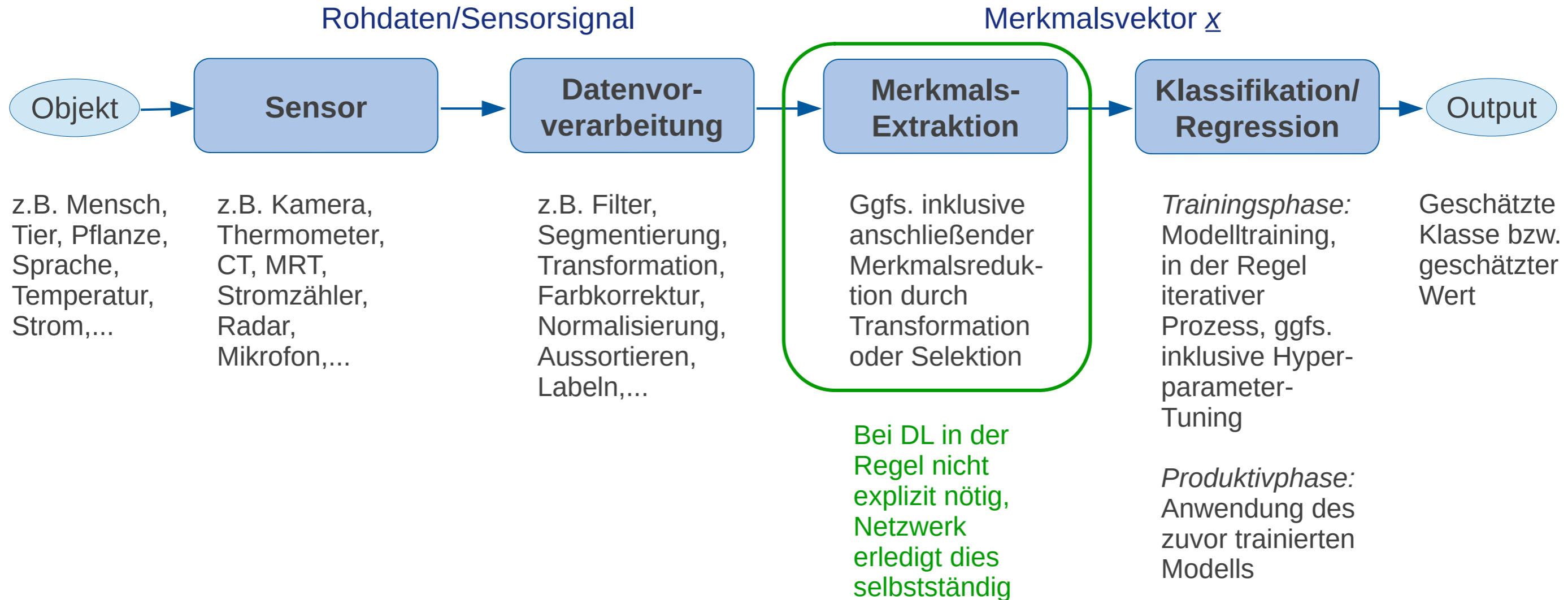
- Spezielle Methodenfamilie im ML
- Inspiriert durch menschliches Gehirn:
 - Künstliche Neuronen
 - Neuronen sind in vernetzten Schichten angelegt

Deep Learning (DL):

- Tiefe neuronale Netze
- Wichtigstes Teilgebiet der NN-Algorithmien
- Mindestens 2 versteckte Neuronen-Schichten zwischen Eingabe- und Ausgabeschicht

Überlegungen zum praktischen Einsatz von maschinellem Lernen

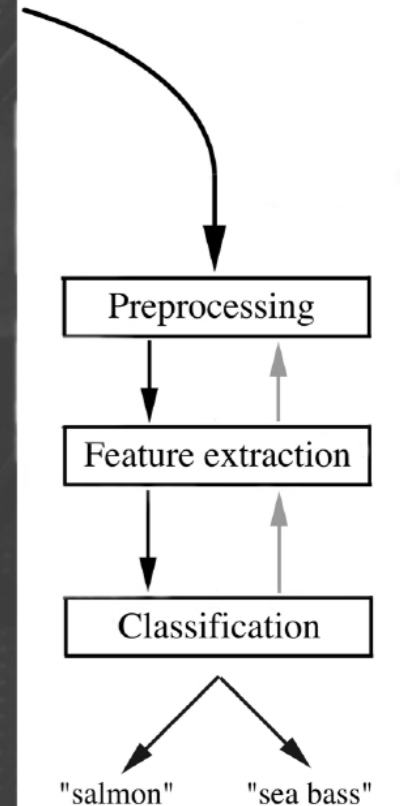
Zusammenfassung: Allgemeiner Aufbau von ML-Systemen



Beispiel: Automatisierte Fisch-Sortierung

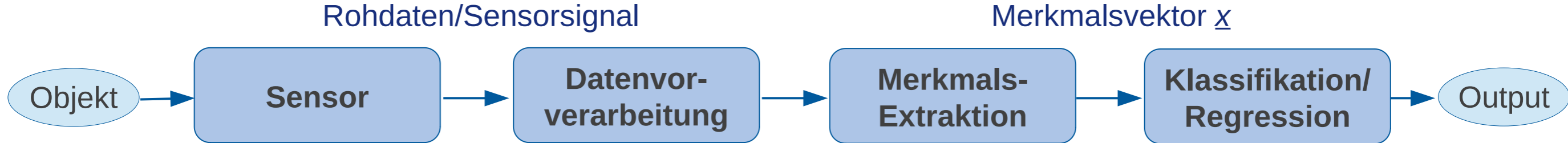
Beispiel aus Standardwerk „Pattern Classification“¹:

Fiktive Fisch-Sortieranlage, die auf Basis von Kamera-Aufnahmen automatisch zwischen gefangenen Lachsen und Seebarschen unterscheiden soll



¹Richard O. Duda, Peter E. Hart, David G. Stork: „Pattern Classification“, Wiley-Verlag

Beispiel: Automatisierte Fisch-Sortierung



- **Objekt:** Fisch unbekannter Spezies
- **Sensor:** Kamera
- **Rohdaten:** Bild
- **Datenvorverarbeitung:** Segmentierung, Farbkorrektur, Skalierung, Rotation
- **Merkmalsextraktion:** verschiedene Eigenschaften, z.B. Länge, Breite, Anzahl Flossen, Farbton,...
- **Merkmalsvektor:** numerische Repräsentation oben genannter Eigenschaften
- **Modell:** binäres Klassifikationsmodell
- **Output:** Klassenlabel, das Spezies des Fisches repräsentiert

Was muss berücksichtigt werden?

Daten

Zu klärende Fragen:

- Wie ist die *Qualität* meiner Daten?
- Ist mein Datenset *repräsentativ*?
- Habe ich *genug* Daten?

Labels

Merke: Ein Klassifikator kann *nur* so gut sein, *wie die Qualität der verwendeten Klassenlabels!*

Wenn die Labels der Trainingsdaten auf der *subjektiven Meinung* eines Experten beruhen:
Mehr als eine Meinung einholen

ML-Modell

Bei der Modell-Auswahl sollte berücksichtigt werden:

- Das Datenset – Größe, Verfügbarkeit von Klassenlabels,...
- Die Fragestellung – Klassifikation oder Regression? Binäre oder multi-class Klassifikation?
- Die Anwendung – weichen reale Daten eventuell leicht von den Trainingsdaten ab?
Könnten zusätzliche Klassen hinzukommen?
- Die verfügbaren Ressourcen – sind Schnelligkeit oder Recheneffizienz wichtig?

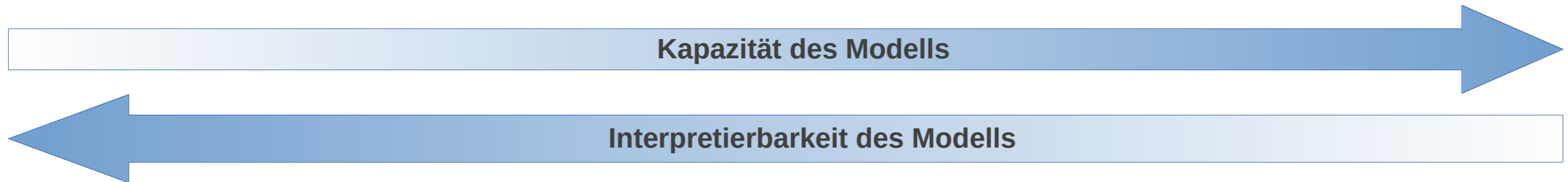
Merkmalsbasiertes ML vs. Deep Learning

Merkmalsbasiertes ML

- + bessere Interpretierbarkeit
- + Algorithmen teilweise sehr schnell (ohne GPU)
- + kann auch mit kleineren Datensets funktionieren (unter den passenden Umständen)
- Wahl der passenden Merkmale ist essenziell
- nicht notwendigerweise robust
- generelle Einschränkungen in Bezug auf Komplexität der lösbaren Probleme

Deep Learning

- + höhere Modell-Kapazitäten möglich
- + keine explizite Merkmalsextraktion nötig
- + keine explizite Merkmals-Selektion nötig
- + höchst innovatives Forschungsgebiet
- Ergebnisse oft schwerer zu interpretieren
- mehr Trainingsdaten nötig
- Training und Einsatz eines Modells meist Ressourcen-intensiver



Zusammenfassung: 7 Schritte zu erfolgreichem ML

1. Die Aufgabe verstehen und eine klare Problemstellung definieren
2. Literaturrecherche betreiben und einen ML-Ansatz wählen, der zu *diesem* Problem passt
3. Sorgfältige Datenvorverarbeitung betreiben (z.B. Labeling durch Experten)
4. Im merkmalsbasierten Fall: *sinnvolle und informative* Merkmale extrahieren
5. ML-Modell trainieren und optimieren
6. Das trainierte Modell anhand neuer Daten evaluieren
7. Das ML-Modell erst dann in den Produktiveinsatz übergeben, wenn man sicher ist, dass es robust ist

Wo wird KI schon heute erfolgreich eingesetzt?

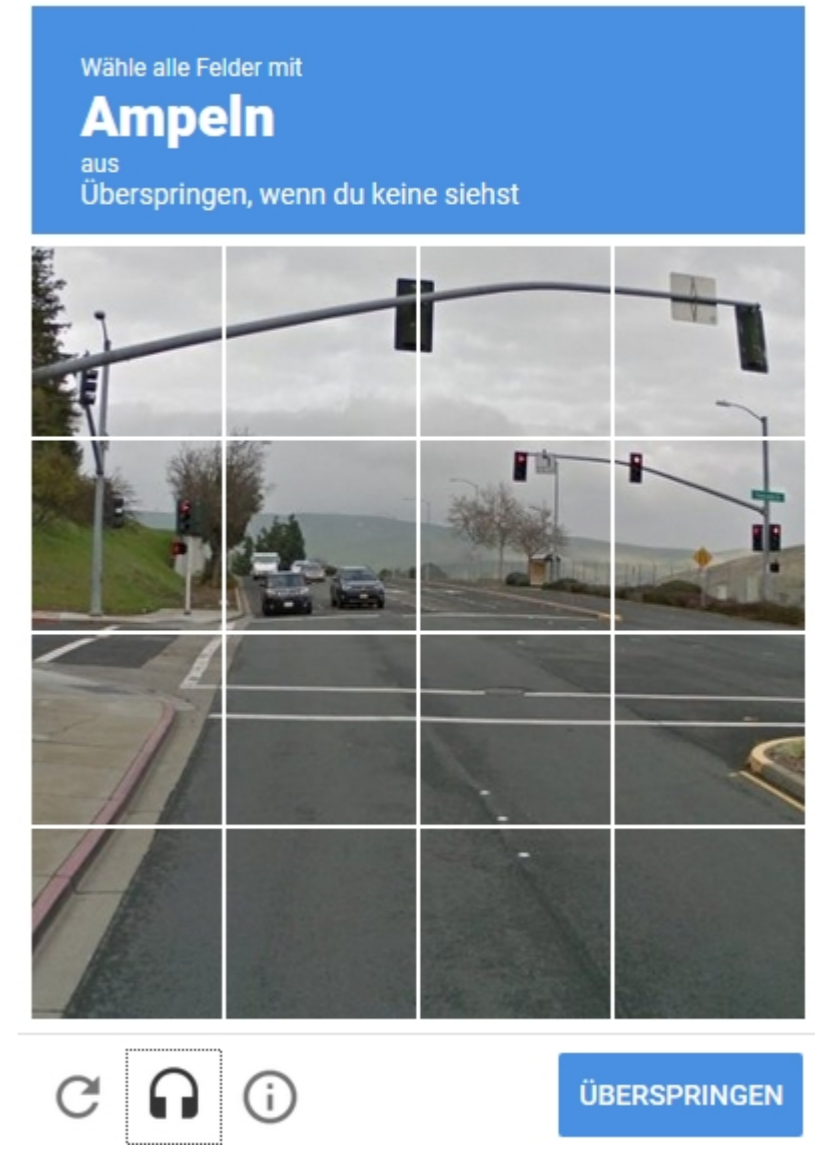
Captchas

Was haben Captchas mit ML zu tun?

- User werden gebeten, Wörter zu identifizieren oder, aktuell häufiger, in Bildern Objekte zu identifizieren
- Funktion 1: Spam bzw. Bots verhindern
- Funktion 2: Aufbereitung von Trainingsdaten für Google

Hintergrund

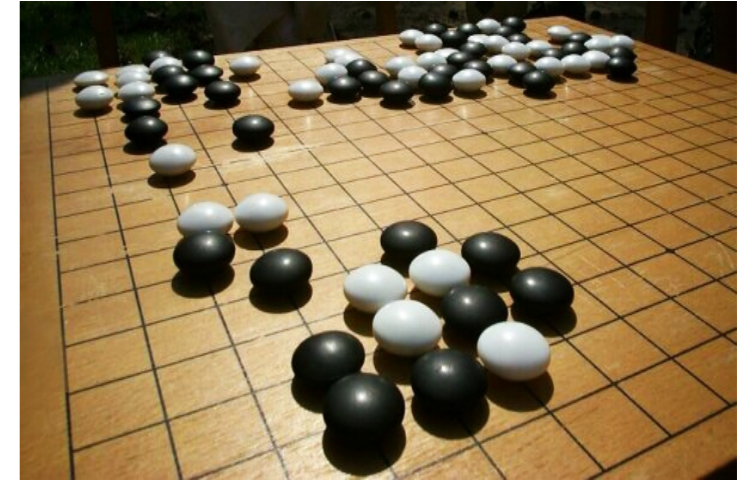
Trainingsdaten labeln ist sehr zeitaufwändig und oft teuer. Durch Captchas lässt Google auf clevere Weise Millionen von Menschen diese Arbeit erledigen – kostenlos.



AlphaGo

Go:

- ältestes chinesisches Brettspiel (über 2.500 Jahre alt)
- Einfache Regeln, komplexe Strategien: Zu Spielbeginn existieren mehr Möglichkeiten, als Atome im Universum



Bildquelle: Go board, Donarreiskoffer, CC BY-SA 3.0, via Wikimedia Commons

Wieso machte AlphaGo weltweite Schlagzeilen?

Google DeepMind trainierte NN auf Basis vieler menschlicher Go-Partien:

- 2015: Professioneller Go-Spieler Fan Hui wird geschlagen (Modell AlphaGo Fan)
- 2017: Ke Jie, amtierender Go-Weltmeister, wird mit 3:0 geschlagen (Modell AlphaGo Master)
- Auch 2017: AlphaGo Zero wird ohne Vorkenntnisse, nur anhand Partien gegen AlphaGo, trainiert.
 - ➔ Nach 21 Tagen: AlphaGo Zero erreicht Level von AlphaGo Master, unerreichbar für Menschen

➔ Demonstration des Potenzials von KI: weniger als 1 Monat Training schlägt 2.500 Jahre menschlicher Erfahrung...

TikTok

Fakten:

- TikTok war 2018-2020 die App mit den am schnellsten wachsenden Downloadzahlen
- Durchschnittlicher TikTok-User nutzt die App täglich 46-52 Minuten (Stand 2019, d.h. vor Corona)
- Deutlich höhere Nutzungsdauer als andere Social-Media-Plattformen

Warum fällt es Usern so schwer, die App wieder zu schließen?

App nutzt ausgefeiltes, KI-basiertes Empfehlungssystem für den ForYou-Feed mit Berücksichtigung von

- Interesse bzw. Desinteresse des Users für Content (werden Videos zu ende geschaut?)
- Interaktionen der User (Kommentare, Likes, Shares,...)
- Video-Daten (Hashtags, Sounds, Captions,...)
- User-Informationen (Spracheinstellung, Art des Endgeräts, Standortdaten,...)

Musik und Kunst

KI vervollständigt Schuberts unbeendete Symphonie Nr. 8

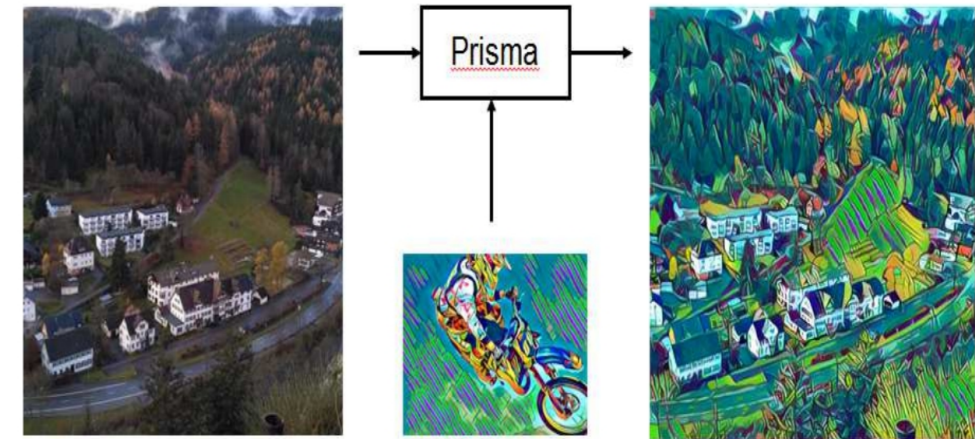
- Schubert komponierte die Symphonie 1822, aber nur 2 Sätze vollendet
- Huawei trainiert neuronales Netzwerk, generiert 3. und 4. Satz
- Uraufführung Februar 2019 in London, viel Lob von Experten



Pressefoto der Uraufführung am 14. Februar 2019, London

Style-Transfer (Image-to-image-Translation)

- Modell wird auf Imitation des Stils von z.B. bestimmtem Künstler trainiert
- Modell „übersetzt“ z.B. Fotos in gelernten Stil
- Prominentes, täglich genutztes Beispiel: Instagram-Filter



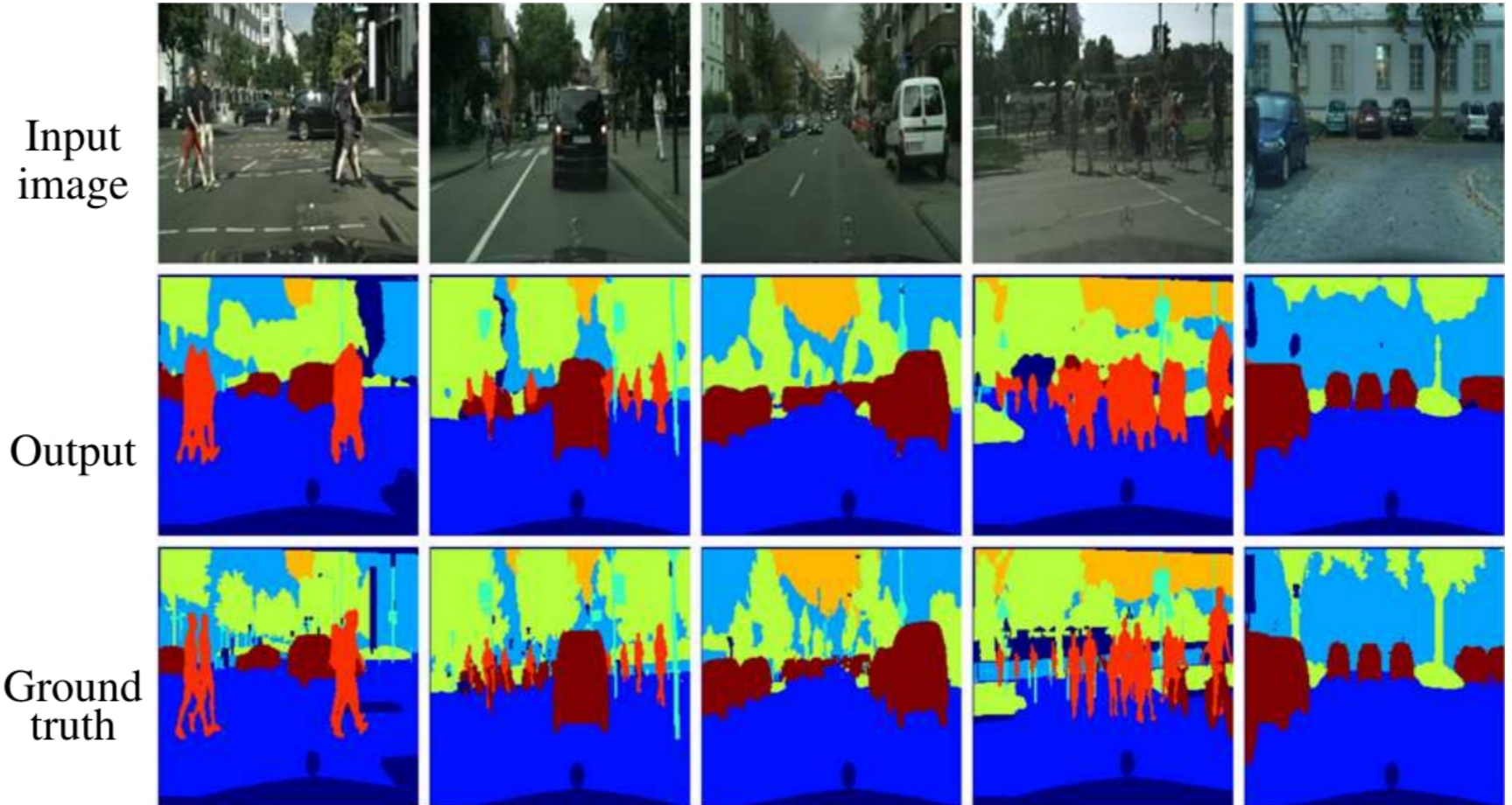
Gatys et al.: „A neural algorithm of artistic style“, ArXiv 2015

➡ 2 Beispiele für den Einsatz von KI, die auf sog. *generativen Modellen* basiert

Autonomes Fahren/Fahrassistenzsysteme

Vielfältige Anwendung von KI:

- Fahrerzustandserkennung (z.B. Müdigkeitserkennung)
- Spurhalteassistentz
- Adaptive Cruise Control
- Notbrems-Assistentz
- Umgebungserkennung
- Objektdetektion und -Lokalisation
- Hindernis-Klassifikation
- „Vorausschauendes Fahren“ des autonomen Fahrzeugs
- ...



Beispiel: Detektion und Segmentierung von Umgebungsobjekten im städtischen Fahrumfeld (Wang et al.: "On semantic image segmentation using deep convolutional neural network with shortcuts and easy class extension", IPTA, 2016)

Weitere Anwendungsgebiete

KI wird bereits heute standardmäßig eingesetzt für bestimmte Aufgaben in

- zielorientierter Werbung
- Computerspielen (z.B. KI-Gegner, Landschaftsgenerierung,...)
- Natural Language Processing (NLP, z.B. Sprachassistenten wie Amazon Alexa, Siri,...)
- Smart Home (z.B. individualisierte Temperaturanpassungen,...)
- Aktienhandel (z.B. Kursvorhersagen)
- Sicherheitsanwendungen (z.B. Gesichtserkennung, Sturzdetektion,...)
- Medizin (Vortrag am 04.11.)
- Energieversorgung (Vortrag am 11.11.)
- Automatisierungs- und Produktionstechnik (Vortrag am 18.11.)
- ...