Klassische Software vs. statistische KI

Rainer Fischbach

Macht der Technik — Macht durch Technik?

Berlin, 2. März 2024

Die Basis allen Rechnens: Die Natürlichen Zahlen

$\text{Zero} \varepsilon \text{Nat}$ (1)

$n \varepsilon \text{Nat} \rightarrow \text{Succ}(n) \varepsilon \text{Nat}$ (2)

$(n)\ \text{Zero} \neq \text{Succ}(n)$ (3)

$\text{Succ}(m) = \text{Succ}(n) \rightarrow m = n$ (4)

Die Konstruktion des ›Bodens‹ und der ›Leiter‹. Nichtzirkularität und Injektivität der Nachfolgerfunktion Succ.

$$\frac{P(\text{Zero}) \qquad P(n) \rightarrow P(\text{Succ}(n))}{(n)\ P(n)} \quad (5)$$

Die vollständige Induktion als Beweisschema

Von der vollständigen Induktion zur Rekursion

```
data Nat = Zero | succ(Nat)      {- rek. Typdefinition -}

add :: Nat -> Nat -> Nat         {- Typdeklaration -}
add Zero n     = n               {- Basisfall -}
add (Succ(m)) n = Succ(add m n)  {- Rekursionsschritt -}

ggt :: Nat -> Nat -> Nat         {- Typdeklaration -}
ggt x y
     | r == Zero   = y           {- Induktion über die -}
     | otherwise   = ggt y r     {- Reduktionsschritte -}
     where (_, r) = divmod x y
```

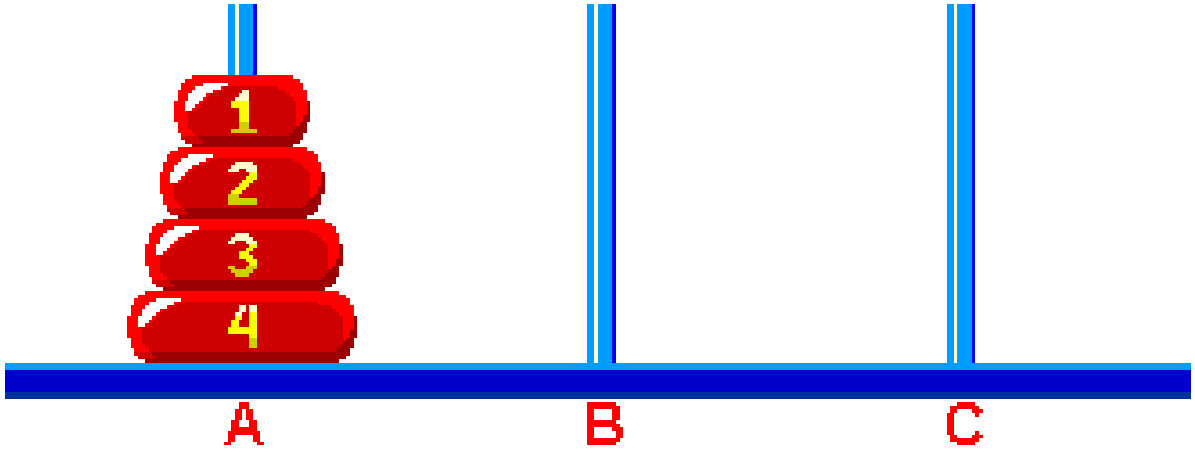
Rekursion über Strukturen (Induktion über Länge)

```
data Lst a = Empty | Cns(a, Lst a)  {- rek. Typdefinition -}

cnct :: Lst[a] -> Lst[a] -> Lst[a]
cnct Empty ls = ls                          {- Basisfall -}
cnct (Cns(x, lx)) ls = Cns(x, (cnct lx ls)

mpf :: (a -> b) -> Lst a -> Lst b
mpf f Empty          = Empty                {- Basisfall -}
mpf f (Cns(x, ls)) = Cns(f x, mpf f ls)

fldl :: (a -> b -> a) -> a -> Lst b -> a
fldl f v Empty          = v                 {- Basisfall -}
fldl f v (Cns(x, ls)) = fldl f (f v x) ls
```

Die Türme von Hanoi (Brahma)

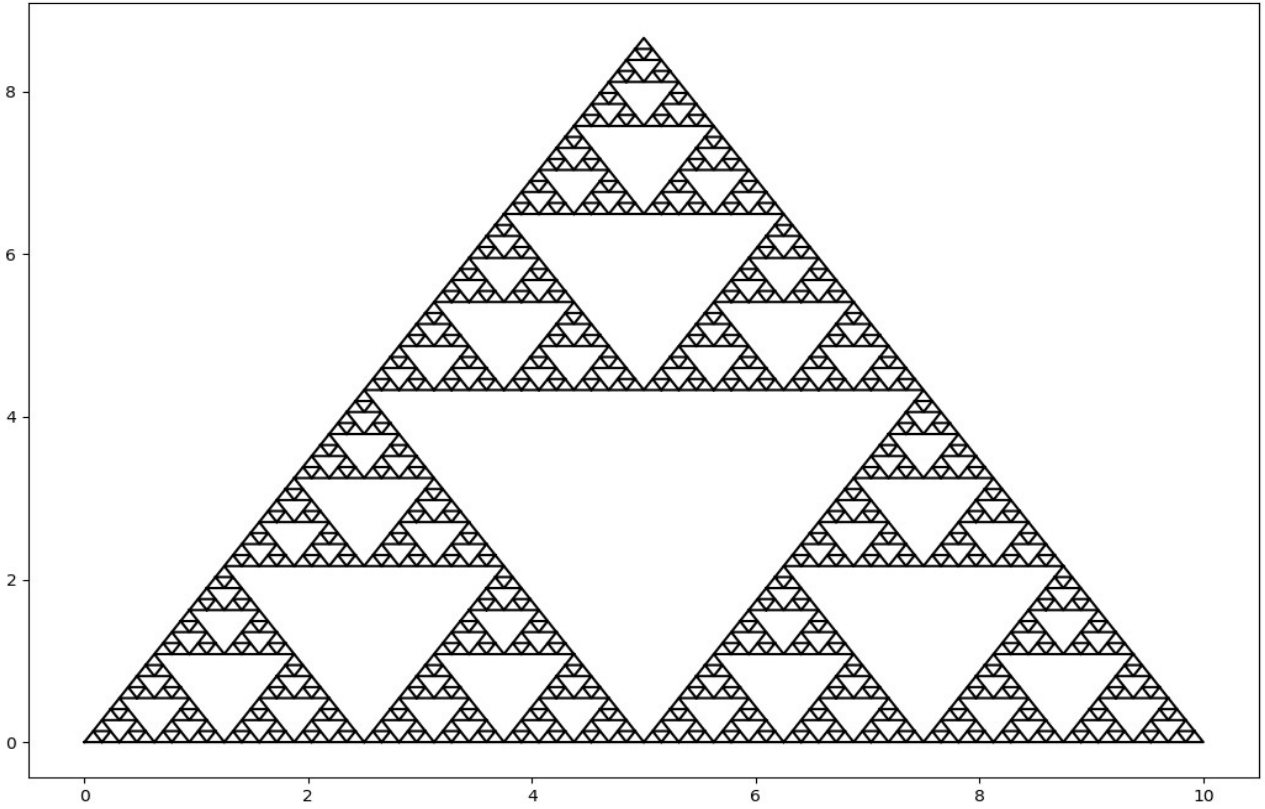
Versetze den Turm von A nach C, wobei nur eine Scheibe bewegt werden und nie eine größere über einer kleineren liegen darf.

Lösung durch Rekursion über die Höhe der Türme.

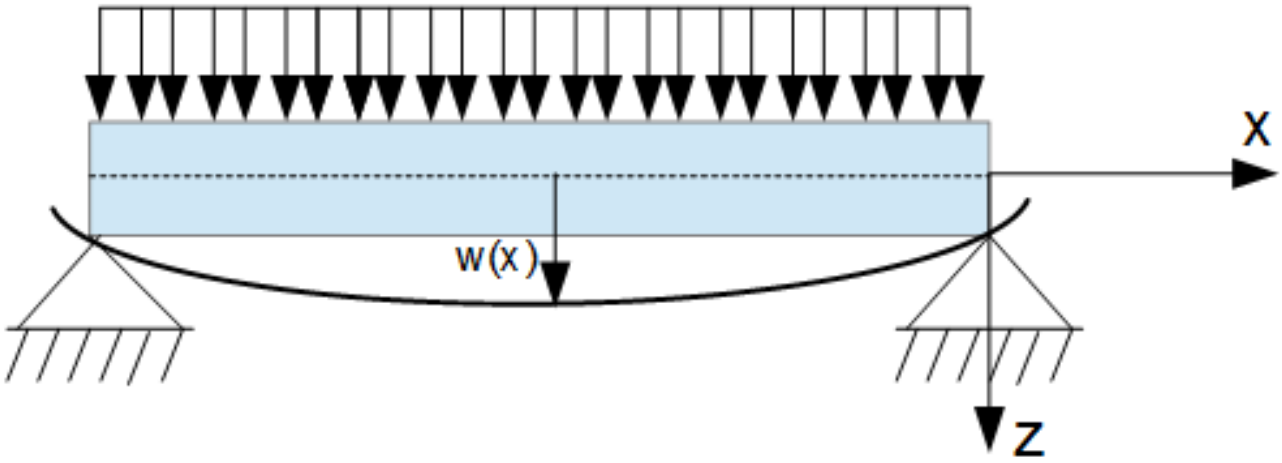


Die Lösung der Aufgabe durch einen Rechner bedarf eines Modells der Türme, der Scheiben und ihrer Bewegungen.

Eine fraktale (rekursive) Figur: das Sierpiński-Dreieck



Statisch bestimmt gelagerter Balken



Standardmodell (Kontinuumsmechanik): Der Versatz $w(x)$ des Balkens hängt von dessen Spannweite l, dem Flächenträgheitsmoment I seines Querschnitts, dem Elastizitätsmodul E seines Materials und der Last ab.

Quellen der Spezifikation

- Technik impliziert die Setzung von Normen.
- Wissenschaft kann Zusammenhänge aufklären,
- doch keine Normen setzen! *Don't follow the science*!
- Zielgrößen (zulässige Spannung und Verformung), Einflussgrößen (Lasten, Stoffparameter) sind wissenschaftlich informiert, doch normativ gesetzt.
- Funktionalität und Stabilität sind normative Begriffe!

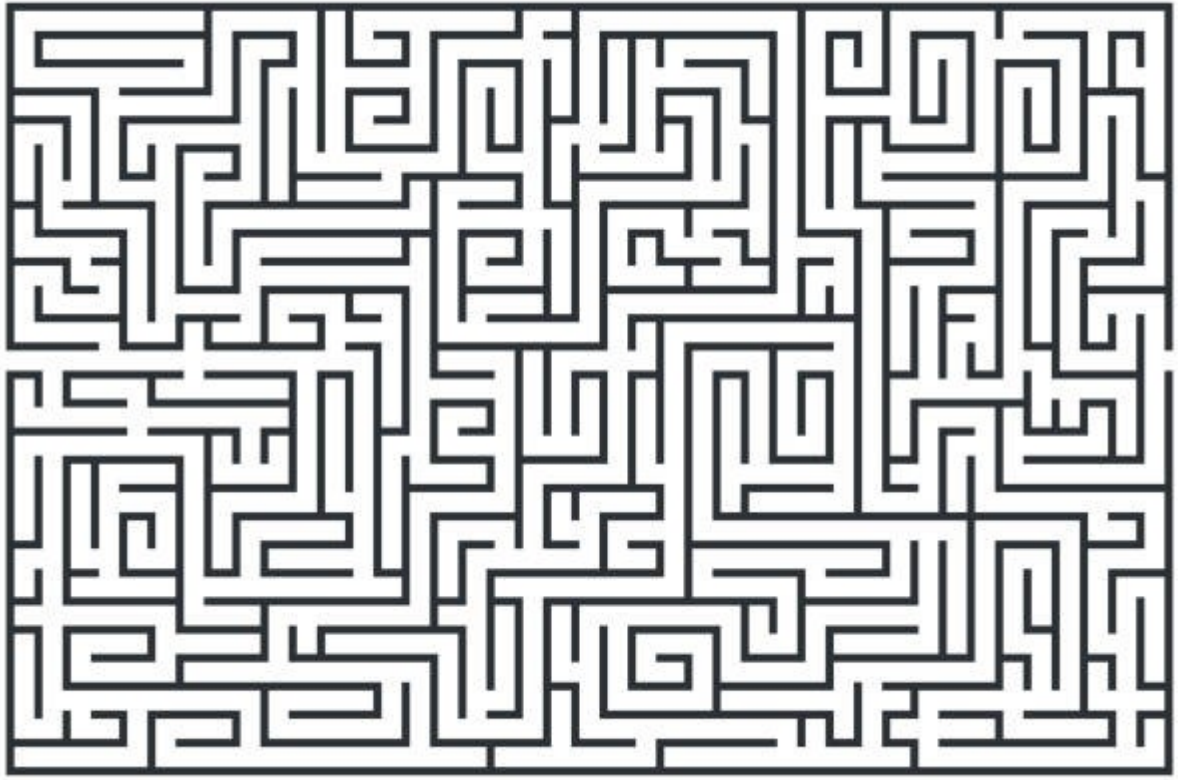
Klassische KI

- Einfache Spiele (Schach und Go blieben unerreicht),
- Optimierungsprobleme,
- Manipulation einfacher Kunstwelten (Bauklötzchen),
- Automatisierte Übersetzung auf Basis linguistischer Theorien (generative Grammatik) erwies sich trotz horrenden Aufwands als Fehlschlag,
- Expertensysteme mit beschränktem Erfolg auf klar explizit strukturierten Gebieten.

Expertensysteme (Knowledge-based Systems)

- Trennung von Inferenzmaschine und Wissensbasis, die
- als erweiterbares Modell in einer formalen Sprache vorliegt.
- Expertenwissen ist oft implizit oder intuitiv, d.h. nicht verbal und deshalb schwer oder nicht zu formalisieren.
- Viele Aufgaben sind nicht deduktiv, sondern abduktiv zu lösen: medizinische Differentialdiagnostik, Fehleranalyse und Reparatur in der Technik, Kriminalistik etc.
- Nichtmonotones Schließen bleibt kaum erreichbar.

Labyrinth



Eine KI-Aufgabe: Exploration eines Suchraums

- Das Labyrinth ist dafür ein bildhaftes Paradigma.
- Viele Aufgaben sind ähnlich (auch Spiele!).
- Es gibt zwei unverzichtbare Werkzeuge und zwei Strategien:
  - Ein Modell des Labyrinths in Form geeigneter Datenstrukturen.
  - Der Ariadnefaden: erinnere die begangenen Wege.
  - Tiefensuche: nimm den ersten Zweig und gehe nur zurück, wenn es nicht weitergeht, um den jeweils nächsten zu nehmen.
  - Breitensuche: gehe auf jedem Zweig einen Schritt und gehe dann zum ersten zurück, um die nächsten zu bearbeiten.

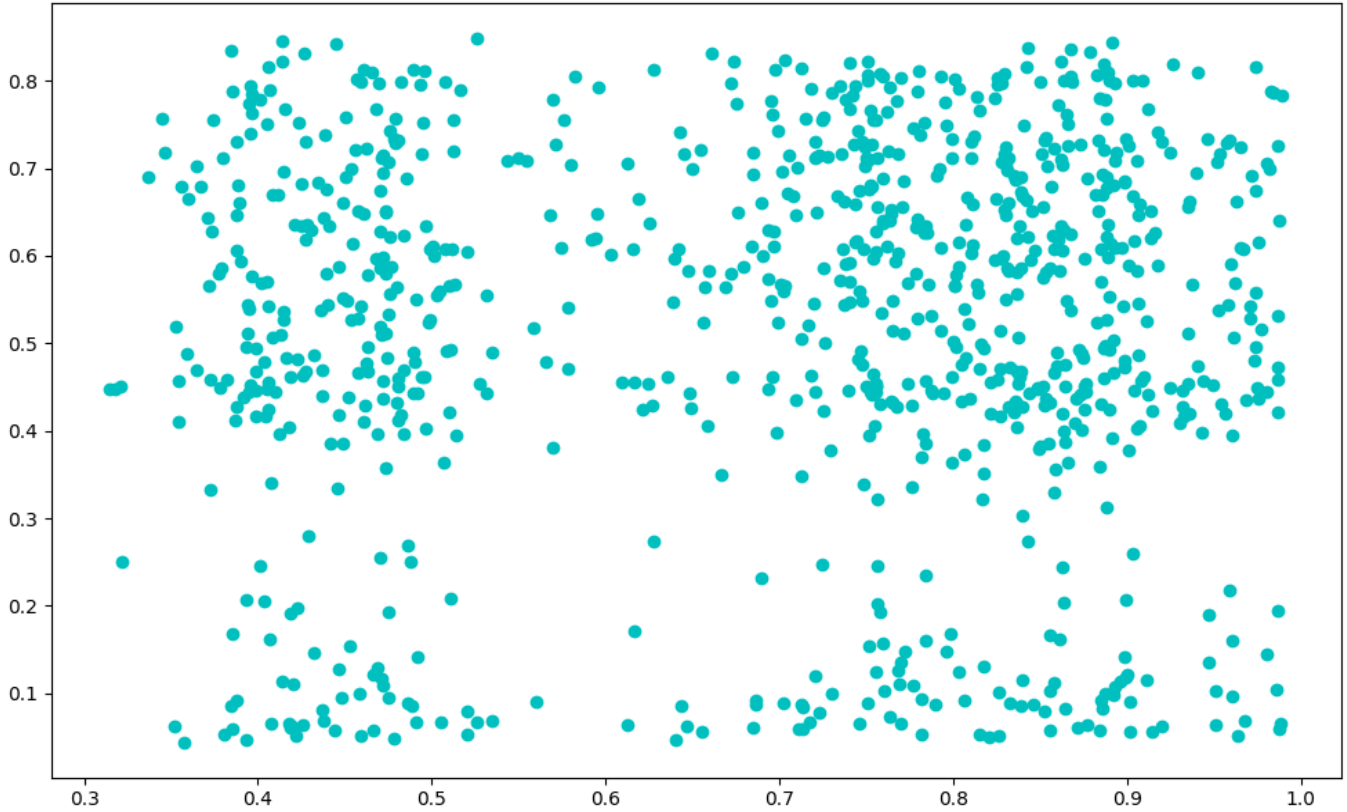
Aufgaben und Methoden der statistischen KI

- Vorhersage, Mustererkennung und Klassifizierung.
- »Maschinenlernen« mittels Beispieldaten zur Bestimmung der Systemparameter ist aufwendig und energieintensiv.
- Techniken:
  - Partitionierung: finde ähnliche Gruppen im Datenraum.
  - Extrapolation durch Regression (linear, multilinear, nichtlinear).
  - Bedingte Wahrscheinlichkeit (Bayes) und Entscheidungsbäume.
  - Künstliche Neuronale Netze (KNN) plus Backpropagation.

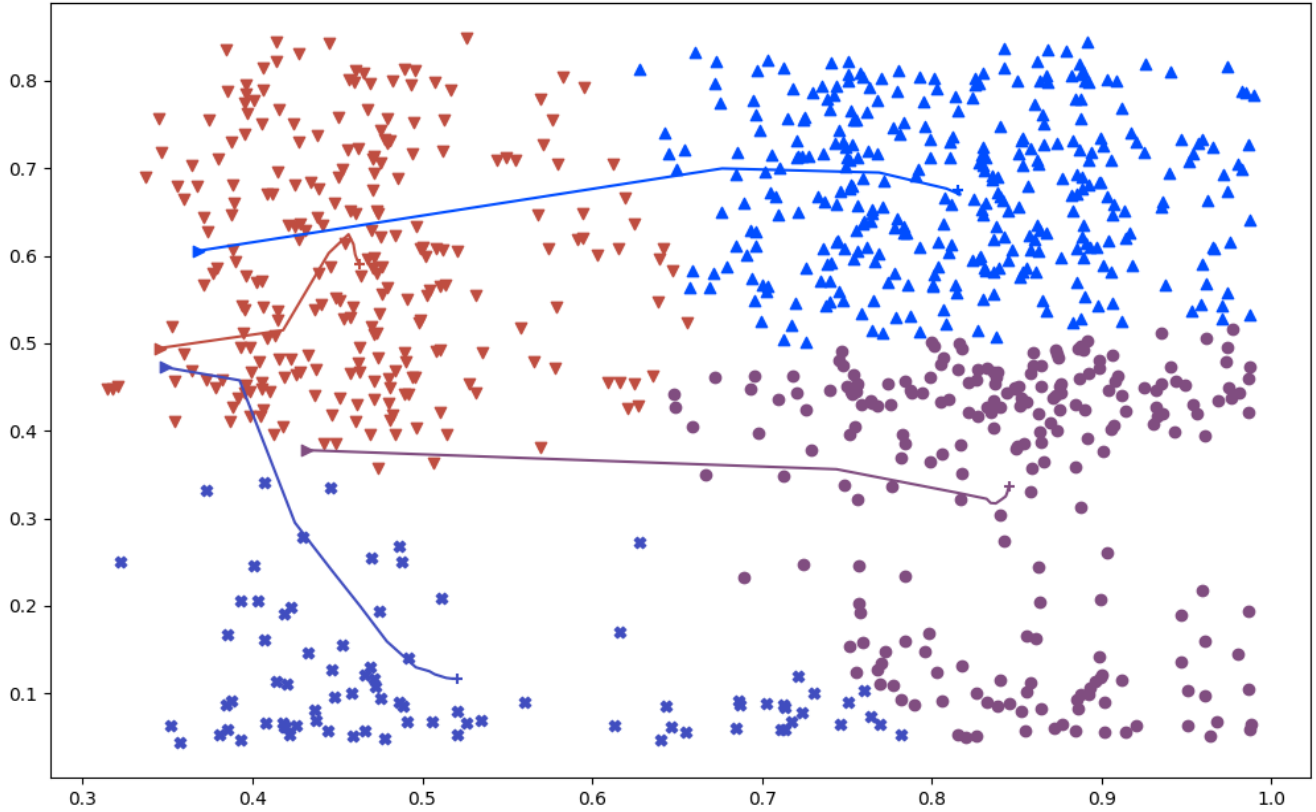
Anwendungen statistischer KI

- Spamfilter,
- Muster- bzw. Bilderkennung, z.B.
  - in der Medizin (Röntgen, MRT, Ultraschall),
  - in fahrerlosen Automobilen (mit ernsten Problemen),
  - in der Fernerkundung (Geowissenschaften, Geheimdienste ...),
  - in Betriebsdaten für vorausschauende Wartung,
- automatische Übersetzung (mit beschränkter Qualität),
- Generative KI (LLMs ...).

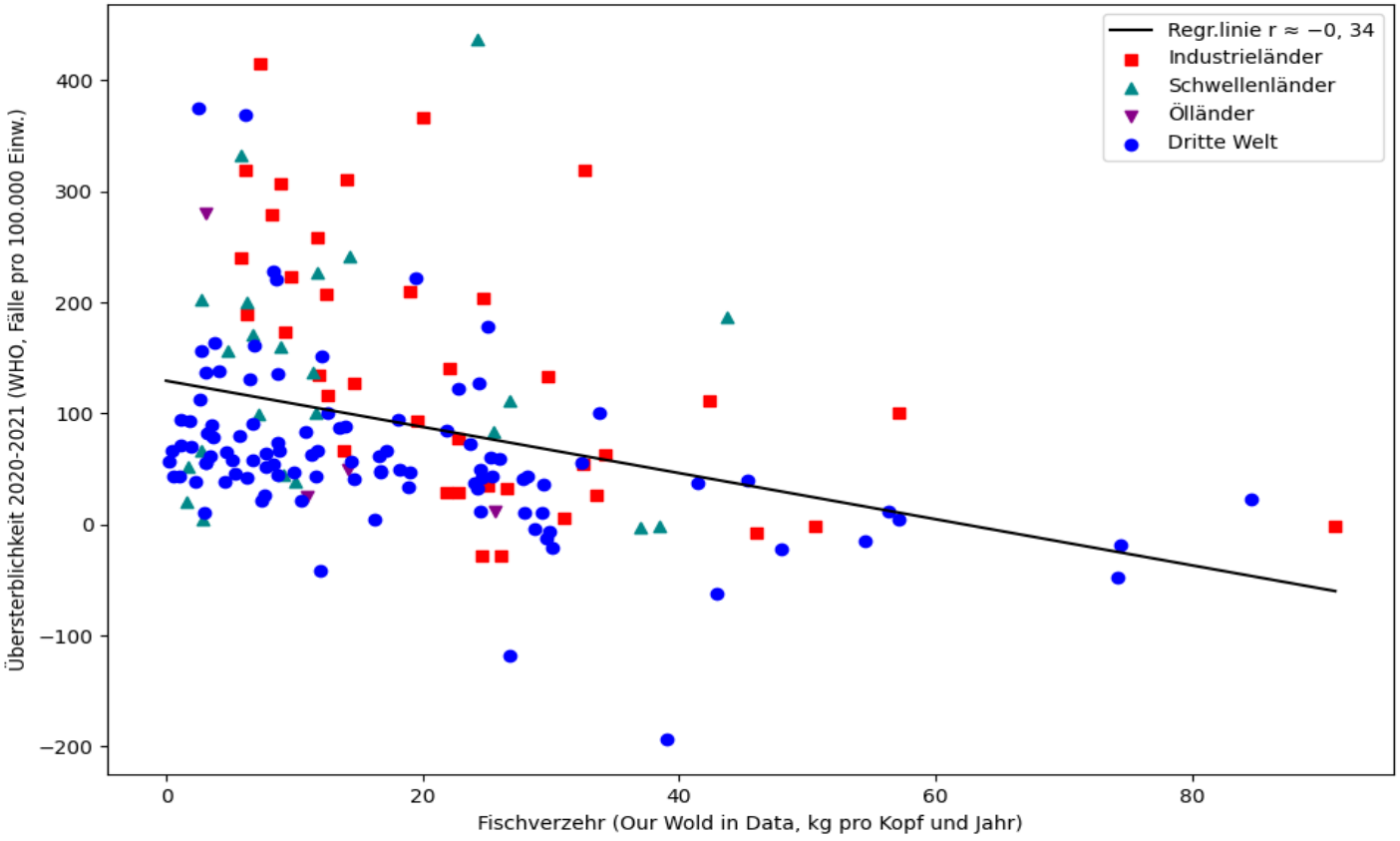
Partitionierung: Ausgangssituation



Unsupervised Learning: Partition mit k-Means



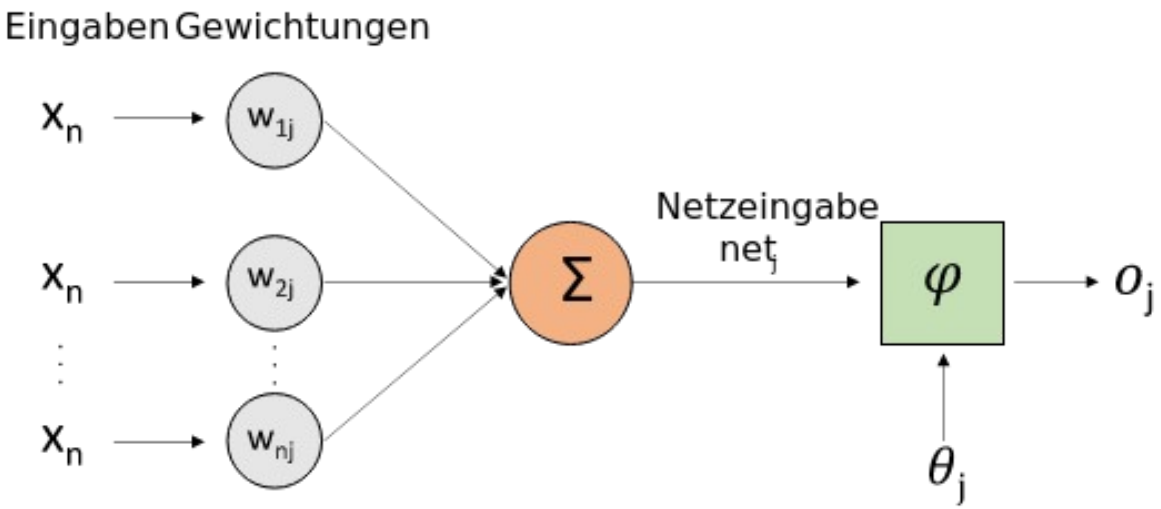
Regression: Übersterblichkeit und Fischverzehr



Probleme der Regression

- Naheliegende Proxy-Variable verdecken die realen Faktoren.
- Die realen Faktoren sind mangels Daten oft nicht greifbar.
- Variablen von Interesse sind oft selbst statistische Artefakte, wie Übersterblichkeit, Exposition gegen Strahlung, Umweltgifte etc.
- Mangelnde Qualität der erhobenen Daten durch uneinheitliche Auflösung der Datenpunkte, inadäquate Messverfahren etc.
- Beschränkter Umfang der Samples.
- Täuschung durch zufällige Korrelationen ($\rightarrow$ Overfitting)

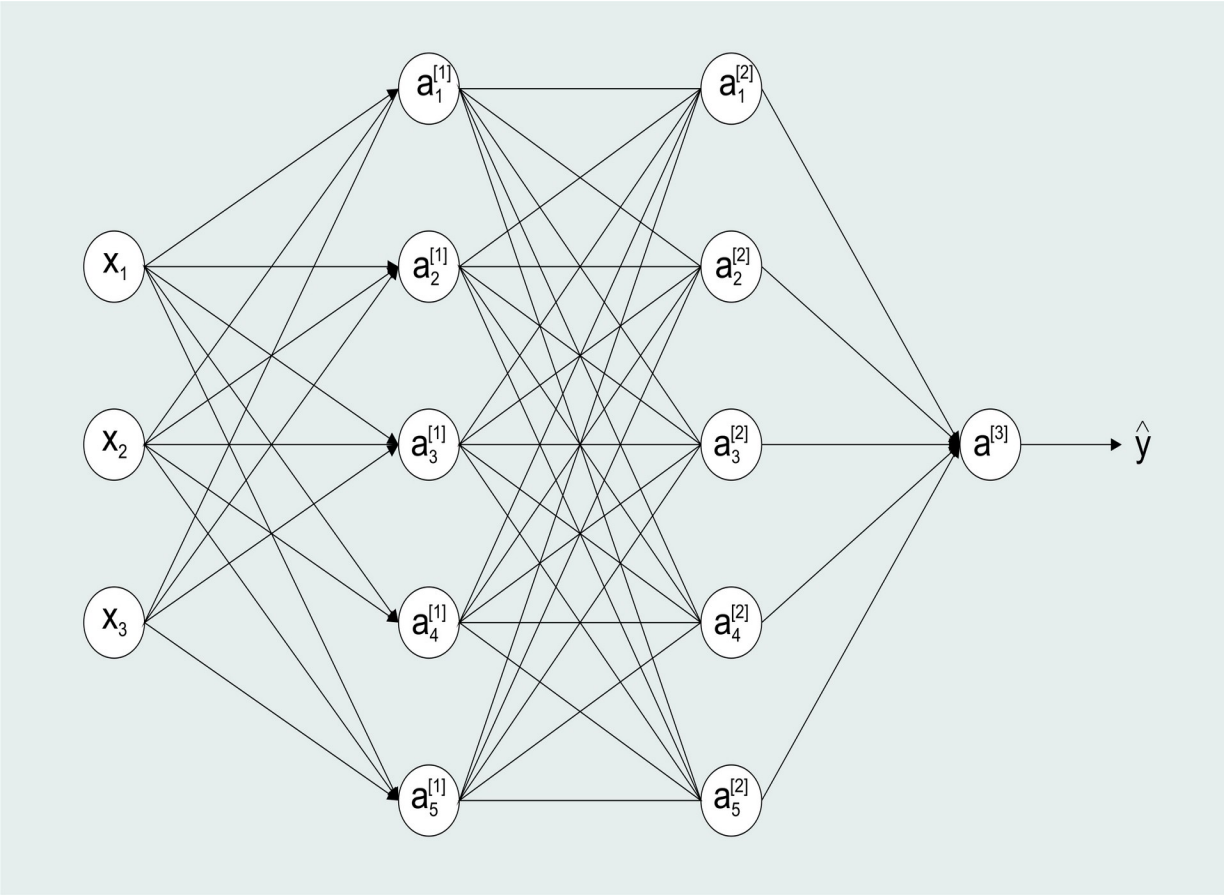
Künstliche Neuronale Netze (KNN): Knotensicht



Die Inputs x_i werden mit Gewichten w_i multipliziert, addiert, um eine Konstante erhöht und darauf die Aktivierungsfunktion φ angewandt. Liegt deren Wert über der Schwelle θ, ›feuert‹ das Neuron. KNN können in Schichten übereinander angeordnet werden (Tiefe KNN).

Das ›Lernen‹ von KNN erfolgt, indem die Gewichte w_i, von Zufallswerten ausgehend, gezielt variiert werden, um die Differenz der Ausgabe zu den den Sollwerten zu minimieren. Leitend ist dabei die Ableitung der Netzfunktion nach den Gewichten (Backpropagation).

Künstliche Neuronale Netze (KNN): Netzsicht



Die Ausgaben der tieferen Schicht (links) werden zu den Eingaben der darüber liegenden. Die Anzahl der Schichten und der Knoten darin ist von der Aufgabenstellung abhängig. Der Aufwand für das ›Lernen‹ steigt mit der Anzahl der Knoten und Schichten.

Supervised Learning: was hat die Maschine gelernt?

x_1	x
x_2	x
x_3	x
...	...
x	?

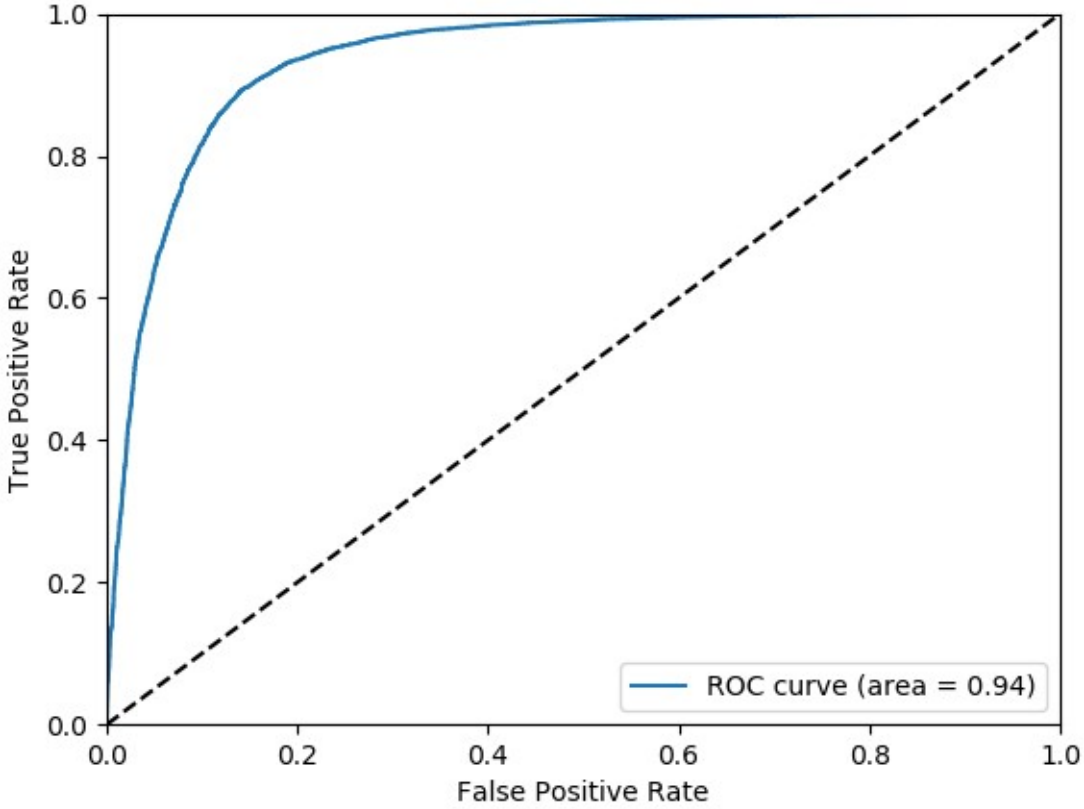
U x	x
U x	x
U x	x
...	...
x	?

x	x
x	x
x	x
...	...
U x	?

Anwendung vs. Lernen. Linke Spalte: Datensatz mit Merkmal. Rechte Spalte: vergebenes Label bzw. nicht erkanntes Merkmal.

Datensätze werden mit Kennzeichnungen versehen. Entsprechende Merkmale sollen in neuen Datensätzen erkannt werden. Was durch unvollständige oder verschmutzte Daten scheitern kann.

Die ROC-Kurve: Sensitivität vs. Spezifität



Jede Steigerung der True Positive Rate (TPR) durch Senkung des Schwellenwertes führt auch zu einer Erhöhung der False Positive Rate (FPR) um wachsende Beträge.

ChatGPT, LLMs etc.

- LLMs betten Tokens (Worte bzw. Wortteile) und Phrasen in Vektorräume von zig Tausenden Dimensionen ein.
- Eine Konfiguration mehrerer tiefer KNN schlägt mögliche Fortsetzungen angefangener Texte vor, aus denen die Auswahl durch gesteuerten Zufall erfolgt.
- LLMs sind statistisch gesteuerte Vollidioten.
- Sie verstehen nichts und produzieren deshalb öfters kompletten Unsinn.

Summa

- Mit statistischen Verfahren lassen sich eng umrissene Probleme bearbeiten.
- Klare Problemdefinition, Datenqualität und saubere Methodik sind essentiell.
- Das konkurrierende Verhältnis von Sensitivität und Spezifität erschwert anspruchsvolle Anwendungen.
- Die fehlende Rückverfolgbarkeit bzw. das Risiko von Fehlklassifizierungen machen Anwendungen riskant.

Im Kontext des Stoffwechsels mit der Natur

- Die Entmaterialisierung durch IT und KI bleibt eine Illusion.
- IT hat Voraussetzungen in Form von Infrastruktur:
  - Rechenzentren, Vermittlungsknoten, Übertragungswege
  - Energieversorgung für Betrieb und Herstellung,
  - kritische Rohstoffe (Kupfer, Wolfram, Kobalt Seltene Erden ...),
  - qualifizierte Arbeit.
- KI verbleibt im Kontext der Industriegesellschaft.

Im Kontext gesellschaftlicher Macht

- Verfügung über IT-Infrastruktur und Softwaresysteme bedeutet Macht über kritische Ressourcen.
- Sie impliziert Macht zur Bewegung von Stoff, Energie, menschlicher Arbeit, politischen Entscheidungen.
- Doch auch epistemische Macht — nämlich Macht
  - zur Definition von Wirklichkeit durch ihre Modellierung,
  - zur Einteilung von Menschen und Dingen in Klassen,
  - zur selektiven Gewährung des Zugangs zu Ressourcen.

Beispiele kritischer Bereiche

- Smart City:
  - Google wird zum Souverän, indem es das Land kartiert.
  - Google, Uber, Amazon etc. entwerfen die Stadt neu.
- Digitale Medizin:
  - der Patient wird zum Datensatz
  - Genanalyse macht ihn zum asymptomatisch Erkrankten.
- Wissenschaft: Krise der Reproduzierbarkeit und der Masse.
- Kultur: Enteignung von Sprache und Urteilskraft.

Innovations/Technologiepolitik

- Orientierung an den großen Spielern (USA, China) ist fatal!
- Durch *more and bigger Big Data* sind keine entscheidenden Fortschritte zu erwarten!
- Anspruchsvolle wissenschaftliche, medizinische und industrielle Anwendungen sind durch Clickwork und Datenmassen aus dem Netz *nicht* zu erstellen.
- Sie setzen qualifizierte Arbeit (IT und Anwendung) und eine sorgfältige organisatorische Integration voraus.

Die größte Gefahr besteht nicht im Aufkommen einer Superintelligenz, die die Menschheit beherrschen oder gar eliminieren könnte, sondern in der Projektion von Fähigkeiten in eine KI, die über sie nicht verfügt.

Die Übergabe von kritischen Aufgaben an solche Systeme (z.B. Programmierung von lebenswichtigen Systemen, politisch-militärische und wirtschaftliche Entscheidungen, medizinische Diagnose und Intervention) hat tatsächlich Katastrophenpotential.

THIS IS YOUR MACHINE LEARNING SYSTEM?
YUP! YOU POUR THE DATA INTO THIS BIG PILE OF LINEAR ALGEBRA, THEN COLLECT THE ANSWERS ON THE OTHER SIDE.
WHAT IF THE ANSWERS ARE WRONG?
JUST STIR THE PILE UNTIL THEY START LOOKING RIGHT.
DATA
ANSWERS