

The background of the slide is a light gray circuit board pattern with white lines and nodes.

Machine Learning 101 – Workshop CCC Camp 2023

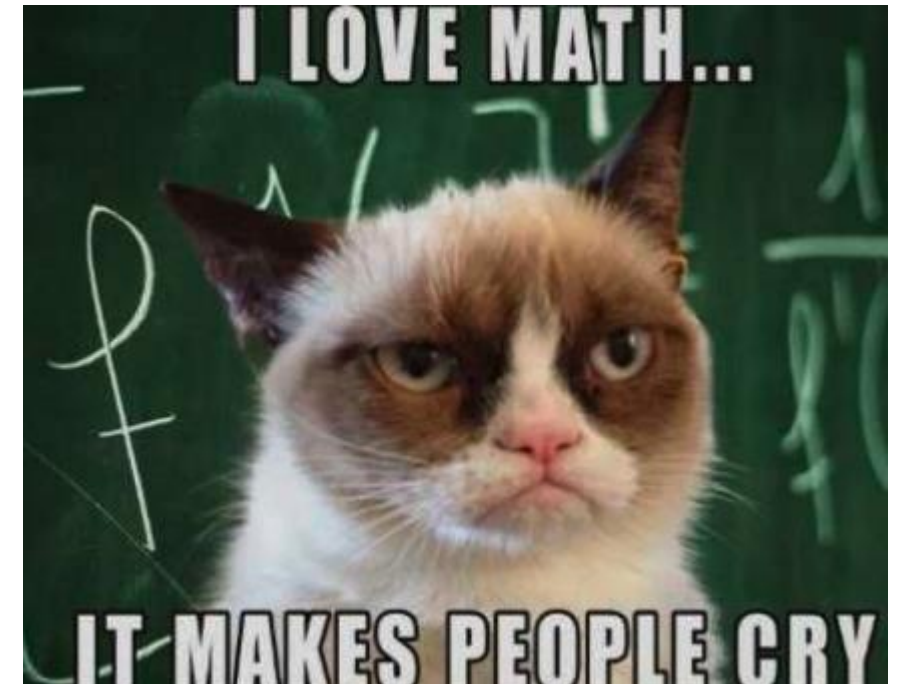
Jannes Quer <jannes@srlabs.de>



Jannes Quer

- Arbeitet bei bei SRLabs
- 2 Jahre Postdoc im Bereich ML in der Bioinformatik und der Moleküldynamik
- Erfahrung als Data Scientist bei einer Big Four Beratung
- Promotion an der Freien Universität Berlin im Bereich Moleküldynamik
- Studium Angewandte Mathematik in Lübeck mit dem Schwerpunkt Bildgebung

■ jannes@srlabs.de



Neuronale Netze versuchen das Gehirn durch angewandte Statistik zu imitieren

Künstliche Intelligenz (KI)

Computer imitieren menschliches Denken und Verhalten.

Machine Learning (ML)

Statistische Algorithmen ermöglichen Implementierung von KI durch Lernen aus Daten.

Deep Learning

Teilbereich des ML, der neuronale Netze verwendet.

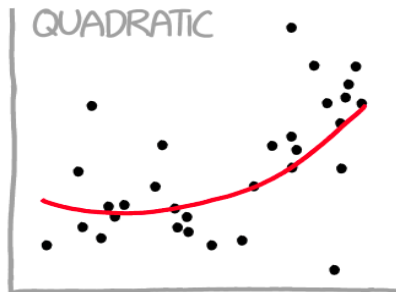
Generative KI hat viel mehr Spielraum, um gute Antworten zu produzieren

Spezialisierte KI

Spezialisierte KI kann nur Klassifikations- oder Regressionsprobleme lösen. Sie wird für eine einzelne Aufgabe trainiert und kann auch nur diese lösen.



Klassifikation

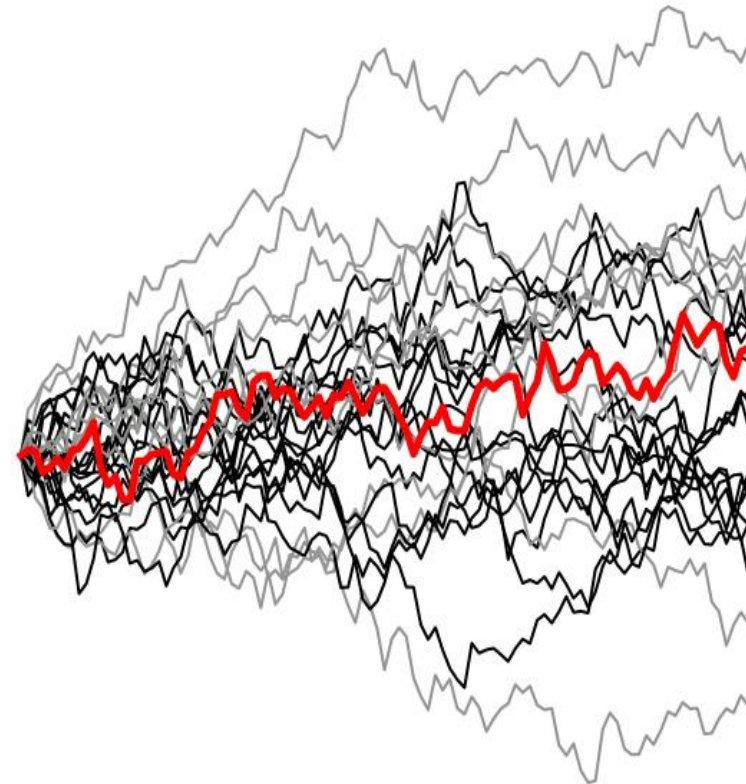


"I WANTED A CURVED
LINE, SO I MADE ONE
WITH MATH."

Regression

Generative KI

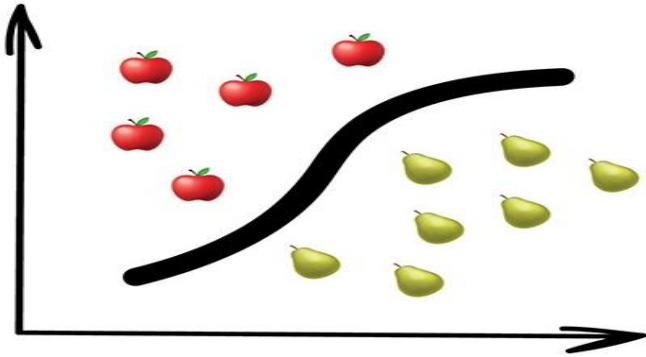
Generative KI hat sehr viele Möglichkeiten ein gutes und überzeugendes Ergebnis zu erzielen.



Gute und
überzeugende
Antwort

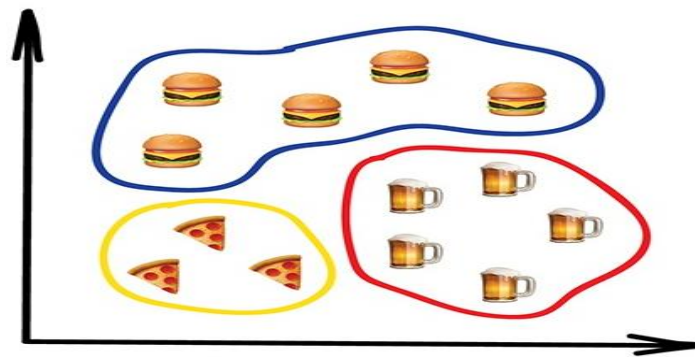
Es gibt drei unterschiedliche Arten des Machine Learnings

Supervised learning



- Label sind bekannt
- Ziel ist das Mapping von Input zu Output zu lernen
- Beispiel: Klassifikation, Regression

Unsupervised learning



- Label sind unbekannt
- Ziel ist es Muster und Gemeinsamkeiten in Daten zu lernen
- Beispiel: Recommender Systems

Reinforcement learning

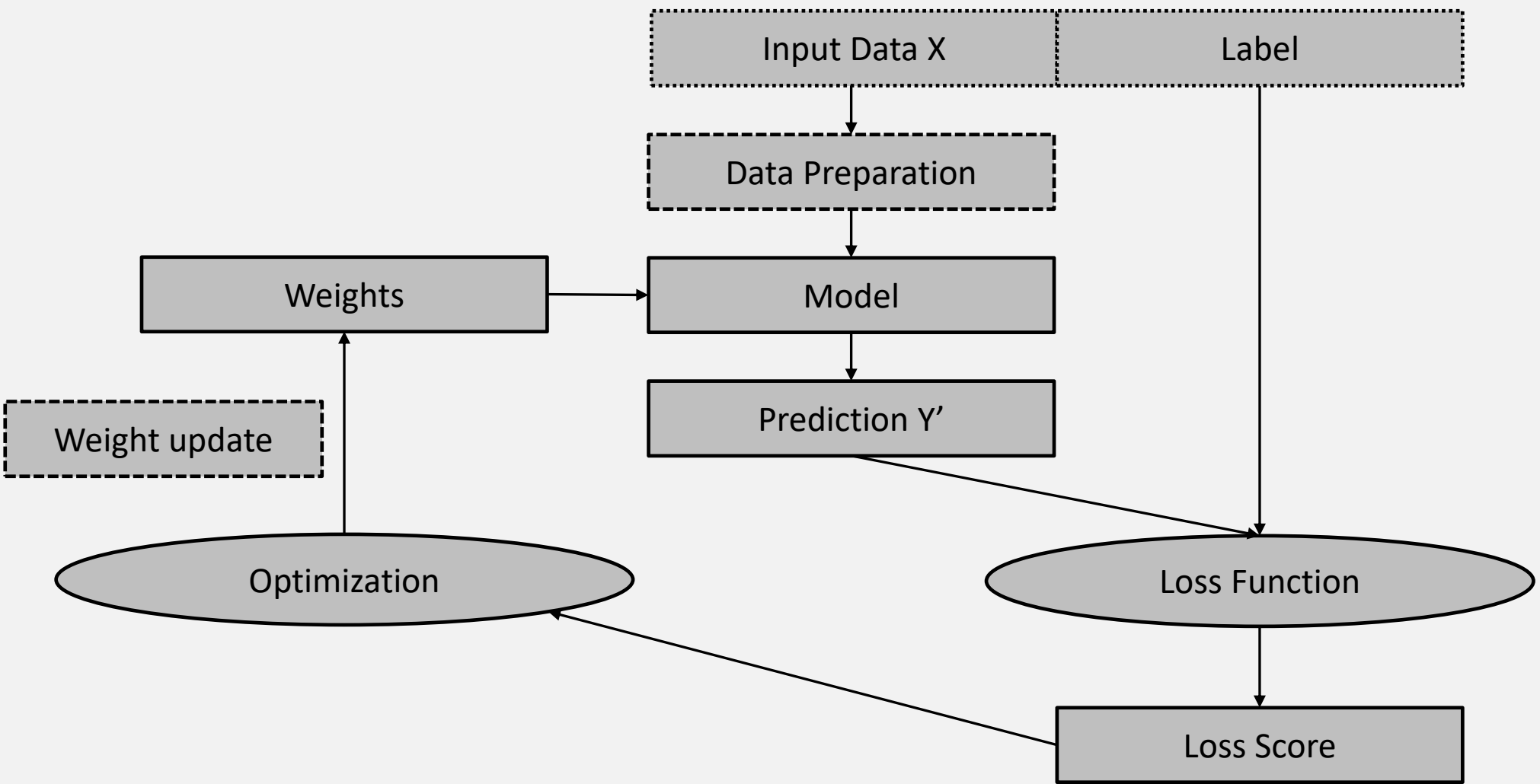


- Daten werden erzeugt
- Ziel ist es ein Verhalten in einer Umgebung zu lernen
- Beispiel: Alpha Go

Ziel des Lernens ist immer eine mathematische Funktion zu lernen, die von Input auf Output abbildet.

„Lernen“ ist ein iterativer Algorithmus

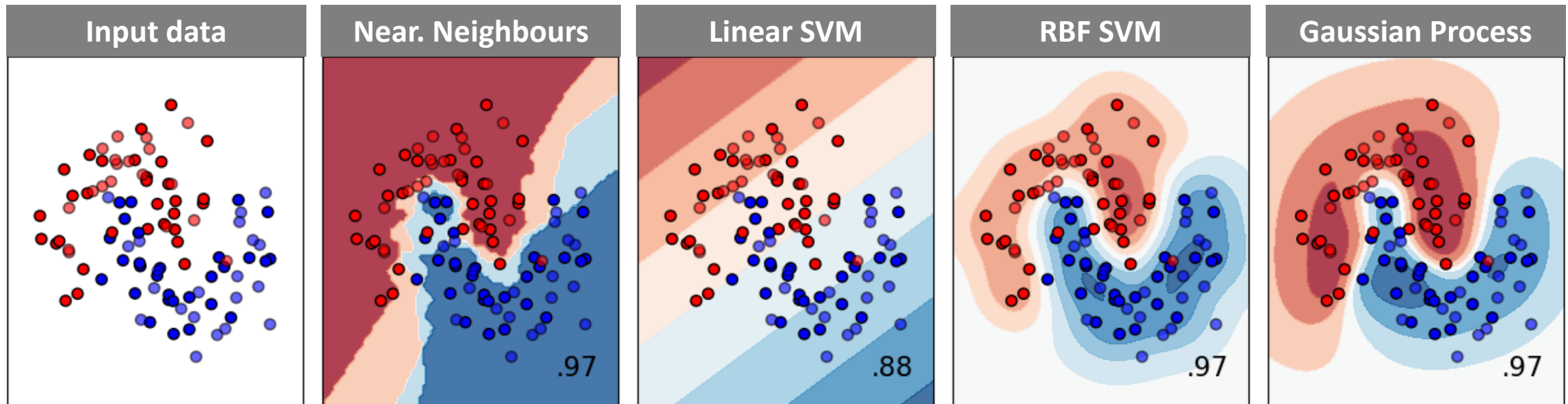
Beispiel: Supervised Learning



Es gibt viele unterschiedliche Modelle, die jeweils ihre Vor- und Nachteile haben

Fun Facts

- Ein Modell ist eine **parametrische Repräsentation** einer mathematischen Funktion
- Die Wahl eines Modells führt **immer implizit Annahmen** mit ein
- Beispiel: Lineare Regression $f(\mathbf{x}, \mathbf{a}) = \sum_{i=1}^N a_i x_i$
- Logistische Regression, Entscheidungsbäume, Random Forest, Support Vector Machines, ...



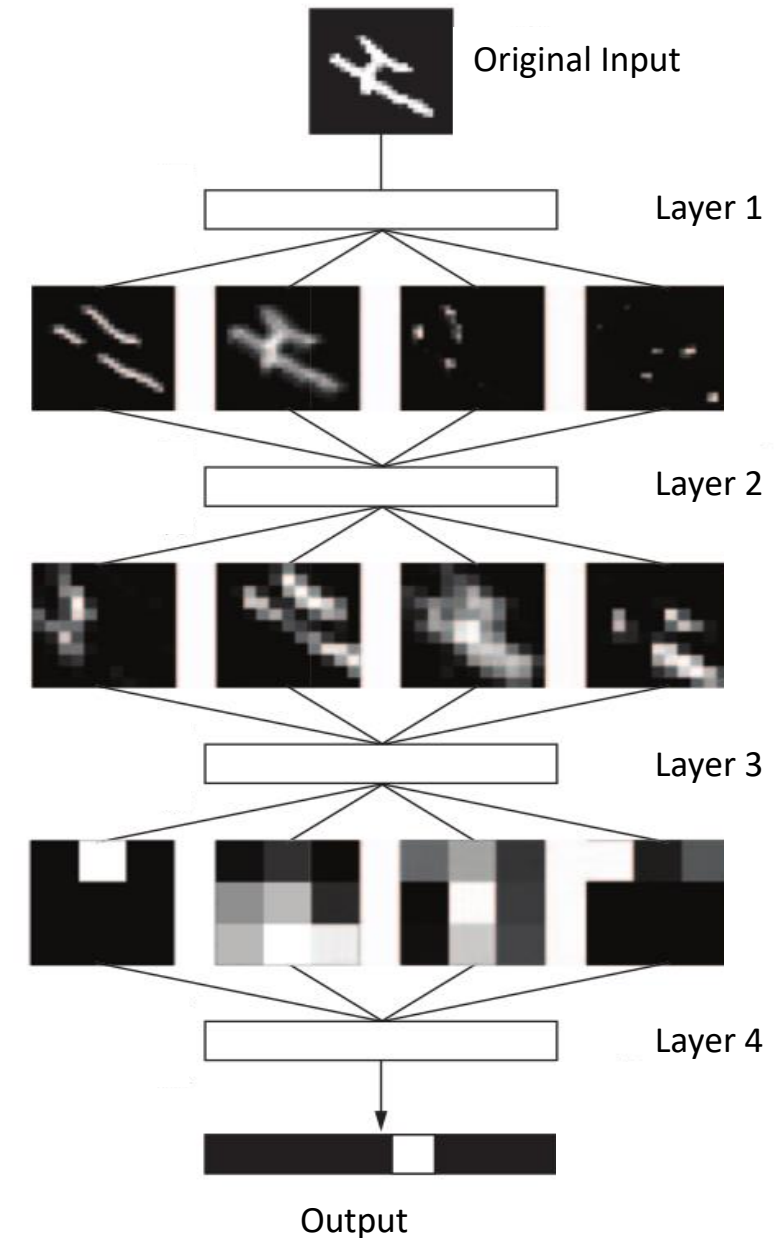
Deep Learning ist das Lernen mit tiefen neuronalen Netzen

Layer

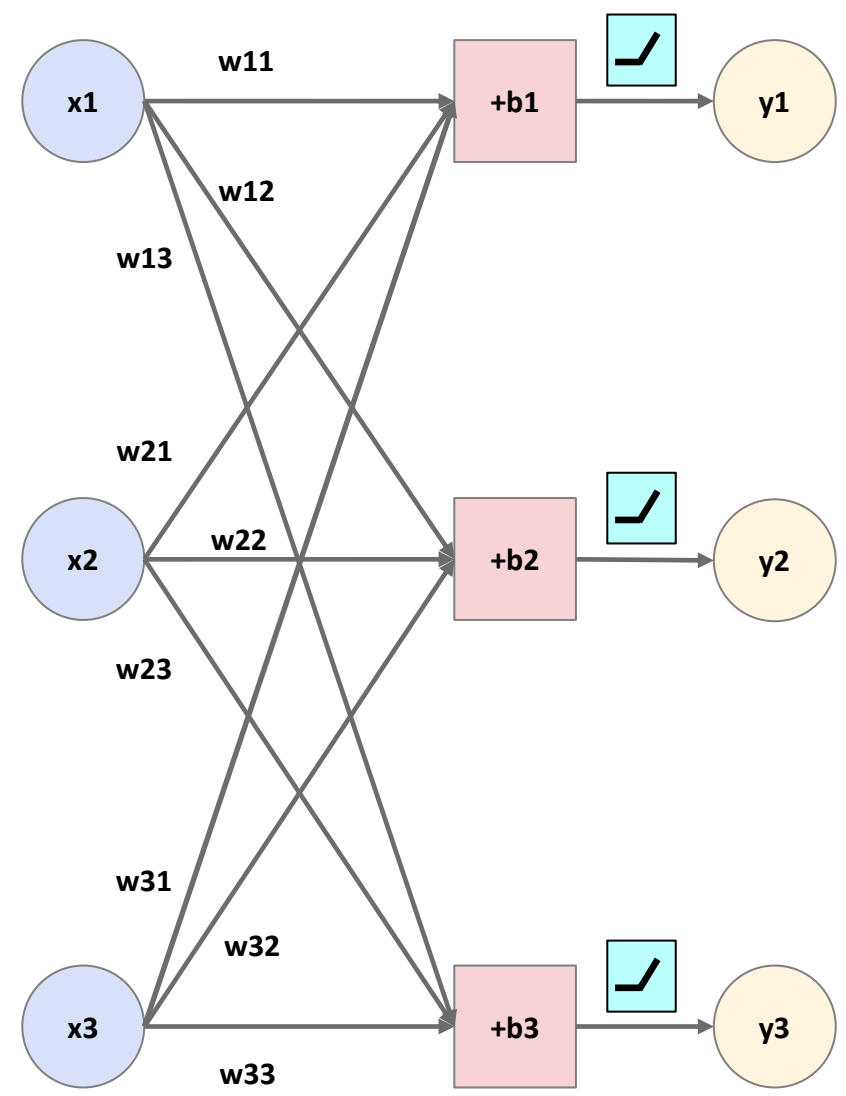
- Deep Learning heißt so, weil **viele Layer hintereinander** gesetzt werden
- Der Aufbau und die Verknüpfung der Layer heißt **Architektur**
- Layer **transformieren** die eingehenden Daten

Features

- **Feature Engineering** wird **nicht** mehr **benötigt**
- In jedem Layer iterative eine zunehmend **aussagekräftigen Darstellung** gelernt
- Es ist mehr oder **weniger möglich** die **gelernten Features zu verstehen**



Ein Neuronales Netz lässt sich auch als mathematische Formel darstellen



The diagram shows the mathematical representation of the neural network's output for each node, where the input vector is multiplied by the weight matrix and the bias is added. Each hidden node's output is passed through an activation function (represented by a cyan box with a black line graph).

Node 1:

$$= \text{Activation Function} \left(w_{11}x_1 + w_{21}x_2 + w_{31}x_3 + b_1 \right)$$

Node 2:

$$= \text{Activation Function} \left(w_{12}x_1 + w_{22}x_2 + w_{32}x_3 + b_2 \right)$$

Node 3:

$$= \text{Activation Function} \left(w_{13}x_1 + w_{23}x_2 + w_{33}x_3 + b_3 \right)$$

Das Lernen ist eine stochastische Optimierung

1

Vorbereitung

- Festlegen von Modell und Architektur
- Vorinitialisieren der Gewichte

2

Lossfunktion (Bsp: Empirisches Risiko)

- Auswahl ist abhängig vom Problem

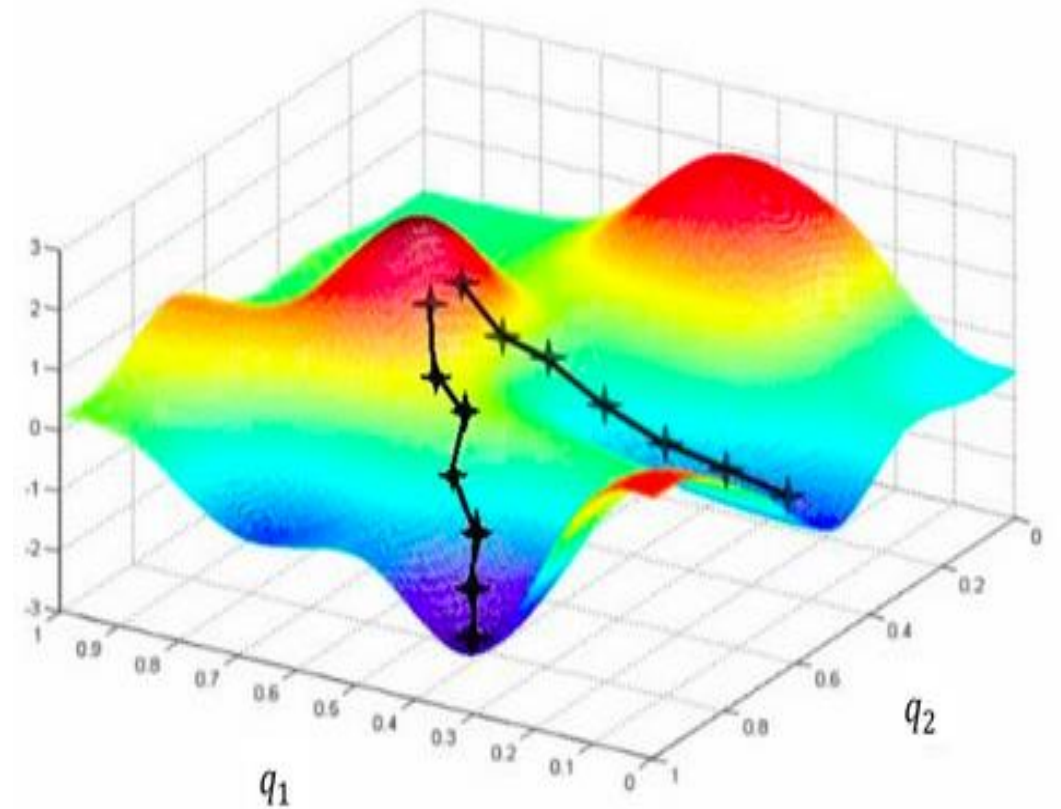
$$J(x, y, \alpha) = \frac{1}{2} \sum (y_i - \varphi(x_i, \alpha))^2$$

3

Gradientenabstieg

- Gradient der Lossfunktion (Ableitung) ist einfach zu berechnen
- Gradient zeigt in Richtung der größten Veränderung

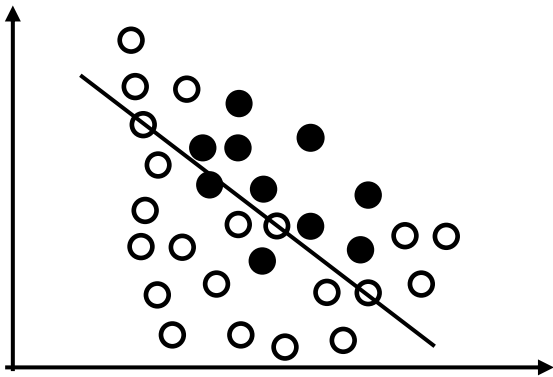
$$\alpha_{new} = \alpha_{old} - \varepsilon \nabla J(x, y, \alpha)$$



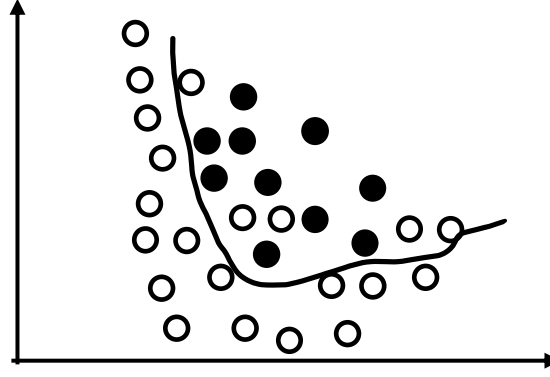
Güte eines Modells

- Das Training ist immer ein **Trade-off** zwischen **Overfitting** und **Underfitting**
- Ein **Modell** wird meistens **nicht 100% korrekt** sein
- Die **Anwendung** bestimmt darüber **welcher Fehler akzeptierbar ist** und welcher nicht
- Welches **Modell das Beste** ist, ist mathematisch **nicht zu beweisen**

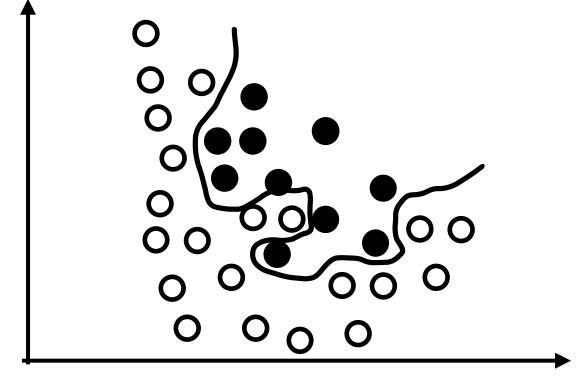
Underfitting



Bestes Model?!?



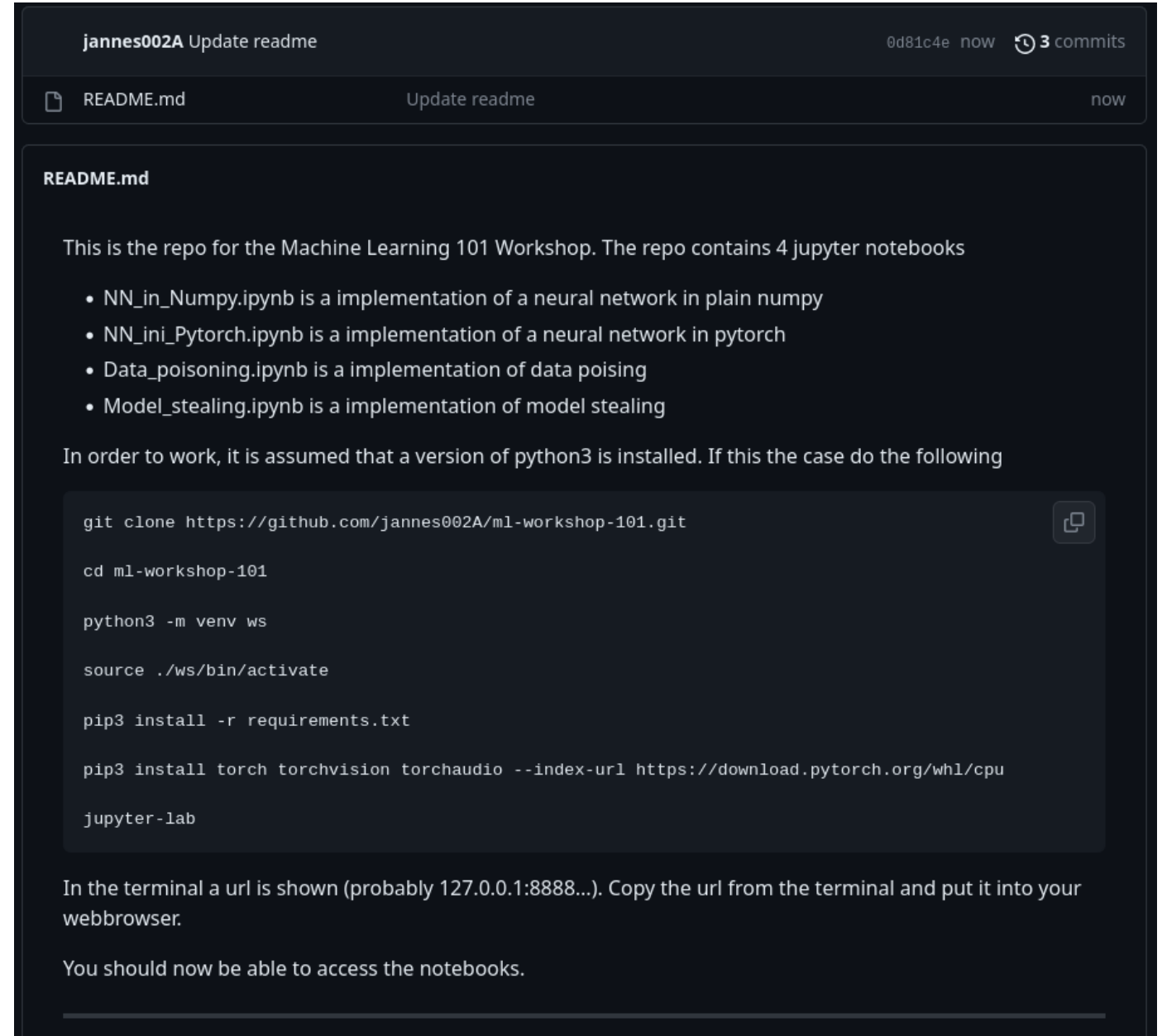
Overfitting



Lets do it!!!

Und los

- Gehe zu github.com/jannes002A/ml-workshop-101 and clone das Repo
- Alles weitere steht im README
- **Bei Fragen einfach melden!**



The screenshot shows a GitHub repository page for 'jannes002A Update readme'. At the top, it says '0d81c4e now 3 commits'. Below the repository name, there's a file named 'README.md' with a button 'Update readme' and 'now'. The main content area shows the 'README.md' file. It starts with 'This is the repo for the Machine Learning 101 Workshop. The repo contains 4 jupyter notebooks'. Then it lists four notebooks: 'NN_in_Numpy.ipynb' (neural network in plain numpy), 'NN_ini_Pytorch.ipynb' (neural network in pytorch), 'Data_poisoning.ipynb' (data poisoning), and 'Model_stealing.ipynb' (model stealing). Below this, it says 'In order to work, it is assumed that a version of python3 is installed. If this the case do the following'. Then there's a code block with the following commands:

```
git clone https://github.com/jannes002A/ml-workshop-101.git
cd ml-workshop-101
python3 -m venv ws
source ./ws/bin/activate
pip3 install -r requirements.txt
pip3 install torch torchvision torchaudio --index-url https://download.pytorch.org/whl/cpu
jupyter-lab
```

 Below the code block, it says 'In the terminal a url is shown (probably 127.0.0.1:8888...). Copy the url from the terminal and put it into your webbrowser.' and 'You should now be able to access the notebooks.'

Where to start

Workshop @ Camp

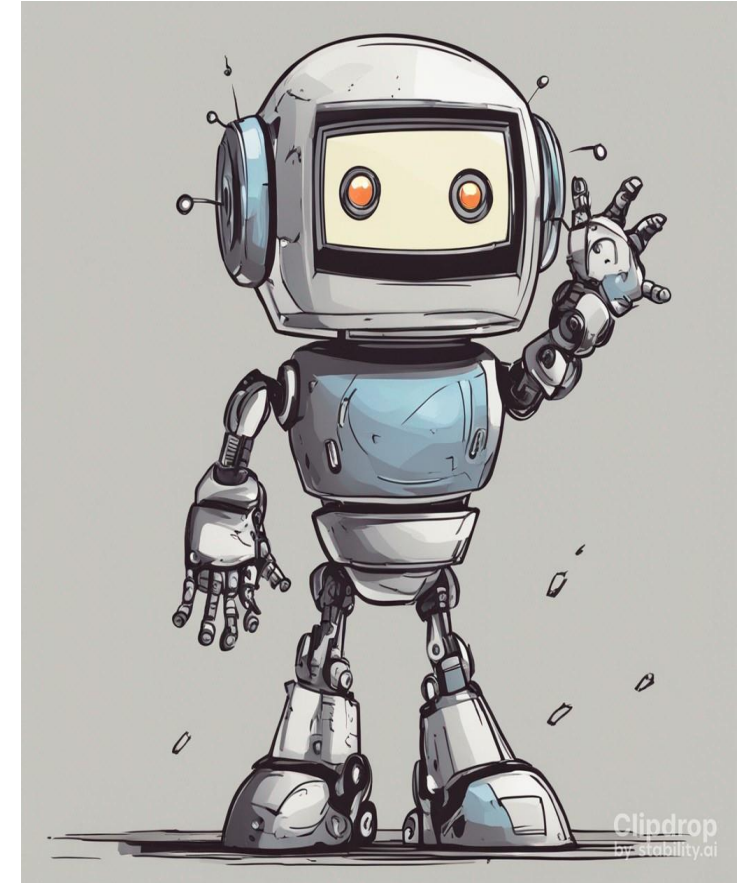
- Workshop @jugend hackt Machine Learning 101
2023-08-19 14h
- Email: jannes@srlabs.de

Kaggle

<https://www.kaggle.com/>

Bücher

- Deep Learning with Python, F. Challet
- M. P. Deisenroth et al
<https://mml-book.github.io/book/mml-book.pdf>
- I. Goodfellow et al.
<https://www.deeplearningbook.org/>



**Security
Research
Labs**

Quellen

- [1,13] Stable Diffusion
- [2] <https://www.pinterest.com/pin/237916792788104970/>
- [3] https://www.reddit.com/r/ich_iel/comments/xi8fs8/ichiel/
- [5] <https://www.freecodecamp.org/news/chihuahua-or-muffin-my-search-for-the-best-computer-vision-api-cbda4d6b425d/>
- [6] <https://noeliagorod.com/2019/05/21/machine-learning-for-everyone-in-simple-words-with-real-world-examples-yes-again/>
- [3,6,8,11] Deep Learning with Python, Francois Challet
- [7] <https://scikit-learn.org/>
- [9] <https://www.heise.de/select/ix/2017/9/1504455013673842>
- [10] [shashank-ojha.github.io/ParallelGradientDescent](https://github.com/shashank-ojha/ParallelGradientDescent)