Aufbau

1. Einführung – 1 Seite
   1. Aktuelle Situation (keine Beispiele)
   2. Problematik (abstrakt)
   3. Aufbau der Arbeit / Problemlösung
2. Grundlage – 4 Seite
   1. KI
      1. Neuronale Netze
         1. „Was sieht die KI?“
            1. 3D
            2. Gewichte
            3. Features
         2. <https://www.capgemini.com/de-de/2017/09/artifical-intelligence-machine-learning-und-data-science-same-same-but-different/>
      2. Konzentration auf Deep Learning
         1. Mensch entscheidet, ob Training in Richtige Richtung geht
      3. Loss-Funktion
         1. Performanz berechnen
         2. <https://www.ai-united.de/arbeitsweise-eines-neuronalen-netzwerkes-algorithmen-training-aktivierungs-und-verlustfunktionen/>
      4. Informationsverlust zwischen Schichten
         1. 1. Schicht verbunden mit letzter Schicht
            1. Eingabe hoher Einfluss auf Endergebnis
         2. Jede Schicht nur Verbindung zu der Nächsten
            1. Hohe Informationsverlust
   2. Bias
      1. Erklärung des Wortes -> in unserem Use-Case
   3. Neuronen und Features
   4. Daten
      1. Datenaufbereiten
         1. Daten sollen Generalisiert sein
            1. Beispiel Bilder

Sammeln

Drehen

Spiegeln

Verzerren

Etc.

* + 1. Under- / Overfitting
       1. <https://medium.com/greyatom/what-is-underfitting-and-overfitting-in-machine-learning-and-how-to-deal-with-it-6803a989c76>
    2. Daten müssen zur Architektur passen oder anders rum 😊
       1. Je Komplexer mehr Neuronen
       2. Mehrfälle desto Fehleranfälliger = mehr Bias
  1. Architekturen
     1. Arten
        1. Full Connected
        2. CNN
        3. ResNet
        4. Natural Network Connection
        5. Dropout
        6. …
  2. Lernarten
     1. Supervised
     2. Unsupervised
     3. Controlevisional
     4. Reinforcement

1. Probleme Beschreibung – 3 Seiten
   1. Unvollständigkeit der Daten
   2. Ähnlichkeit der Daten
      1. Selbst für Menschen auf ersten Blick schwierig zu differenzieren
      2. Bild Croissant vs Katze
      3. <https://distill.pub/2019/activation-atlas/>
   3. Bias in Daten
      1. iPhone Gesichtserkennung (keine Asiaten in Daten)
   4. Falsches Ziel ( menschlicher Fehler )
   5. KI lernt einfachste Unterschiede
      1. Nicht Unterscheid zwischen Auto und Boot sondern Untergrund(Wasser/Land)
      2. Sehr Fehleranfällig z.B. Auto fährt durch flaches Wasser (KI -> Boot)
   6. Falsche Architektur
      1. Auto ML
         1. Rechenaufwändig
      2. Beispiel handgeschriebene Zahlen erkennen (Architektur ohne XOR)
   7. Angriff auf Netz
      1. Adversarial Attacks
      2. <https://www.inovex.de/blog/machine-perception-face-recognition/>
2. Sicherheitsprobleme (Beispiele) – 3 Seiten
   1. Gefahr für Maschinen
      1. Google Kühlung von Maschinen
   2. Gefahr für Menschen
      1. Tesla Autopilot
      2. Evtl DeepFake
      3. Etc.
3. Prävention – 2 Seiten
   1. Passende Architektur zu Daten
   2. Nur ein Ziel
      1. Viele Ziele = Komplex -> Fehleranfällig -> Bias
      2. Beispiel: Baidu Gesichtserkennung (erkennt nur Asiaten)
   3. Verfahren zum Validieren
      1. Unterschiedliche Personen
      2. An echte Daten Testen
         1. Beispiel Polizei Berlin Gesichtserkennung bei Überwachungskamera
            1. 3 verschiedene KIs
   4. Test-/Trainingsdaten Aufbereitung
      1. Vollständigkeit
         1. Fehler hier = Bias
      2. Ohne Bias in Daten
4. Fazit – 1 Seite
   1. Thema ist größer als hier beschreibbar
   2. Evtl. Deep Fake

Generell:

* Abstrakter
* Überschriften:
  + Keine Fragen
  + Knapp

<http://iphome.hhi.de/samek/pdf/LapNCOMM19.pdf>

<https://ujjwalkarn.me/2016/08/11/intuitive-explanation-convnets/>