Aufgabe 1

Aufgabe 1: Begriffe und Definition (3 Punkte)

Beschreiben Sie in Ihren eigenen Worten die Unterschiede und Gemeinsamkeiten der Themengebiete "Künstliche Intelligenz", "Machine Learning" und "Deep Learning".

Künstliche Intelligenz ist der Oberbegriff und definiert grundsätzlich den Einsatz diverser Technologien, um komplexe Probleme zu lösen und Handlungsempfehlungen aufgrund von Datenanalyse zu erstellen. Ziel ist es, selbstständig zu lernen und sich weiterzuentwickeln. Die Probleme sind oft schwierig formal zu beschreiben, für den Menschen jedoch einfach zu lösen (bspw. Bilderkennung). Es ist sozusagen das Gesamtkonzept mit verschiedensten Anwendungsmöglichkeiten.
Das Machine Learning ist eine Teilmenge der künstlichen Intelligenz und ist eine Anwendungsmöglichkeit im KI. Maschinelle Lernen wendet automatisiert Algorithmen an, um Daten selbstständig zu analysieren, sich zu verbessern und möglichst genaue Vorhersagen zu machen. Je mehr Daten zur Verfügung stehen, umso besser kann das Modell autonom lernen. Es müssen strukturierte Daten vorliegen. Die Muster werden durch den Menschen trainiert. Hierbei unterscheidet sich zwischen Supervised Learning und Unupervised Learning. Beim Unsupervised Learning bekommt der Algorithmus keine Beispielsdaten, sondern erkennt versteckte Muster selber. Im Supervised Learning wird das Modell anhand eines Training-datensatzes trainiert und mit einer Zielvariable trainiert.
Deep Learning ist wiederum ein Teilbereich des Machine Learnings und bedient sich dem Modell aus der Natur: neuronale Netze. Es verwendet künstlich erzeugte Neuronen, um Muster zu erkennen und den Algorithmus selbst zu optimieren. Deren Struktur ähnelt dem neuronalen Netzwerk im menschlichen Hirn. Es soll unteranderem komplexere Probleme lösen, für welche statistische Modelle an ihre Grenzen stossen, welche für den Meschen einfach zu lösen sind, jedoch formal schwierig anzuwenden sind (XOR-Problem). Der wesentliche Unterschied zu Machine Learning besteht in der Komplexität der sogenannten „hidden layers". Beim Deep Learning erkennt das System selbst nützliche Variablen und bindet sie in seinen Lernprozess ein.

Der Hauptunterschied zwischen Machine Learning und Deep Learning liegt in der Fähigkeit, durch künstliche neuronale Netzwerke, unstrukturierte Daten zu verarbeiten. Klassisches Machine Learning ist nicht in der Lage, diese unstrukturierten Daten selbstständig zu verarbeiten. Deep Learning löst sehr konkrete Probleme auch von unstrukturierten Daten. Algorithmen, die das vertiefte Lernen beherrschen, lernen mit jeder Berechnung besser, brauchen aber leistungsstärkere Computer und benötigen eine grössere Rechenlaufzeit. Hingegen sind Deep Learning Algorithmen schwer oder gar nicht interpretierbar. Dennoch haben beide das Ziel durch autonomes lernen und analysieren ein möglichst genaues Vorhersagemodell zu erstellen. Beide sind jedoch in der Künstlichen Intelligenz eingebettet und sind jeweils Sub-Kategorien voneinander.

Aufgabe 2: Verlustfunktion (6 Punkte)

Geben Sie drei Verlustfunktionen für Regression und Klassifikation an. Beschreiben Sie die jeweiligen Funktionen kurz.

Mean-Squared-Error (MSE): Der MSE beschreibt die mittlere quadratische Abweichung zwischen der Vorhersage und dem tatsächlichen Wert. Wird bei Regressionsproblemen verwendet.

Mean-Absolute-Error (MAE): Der MAE beschreibt die mittlere absolute Abweichung der Vorhersagen zum eigentlichen Target bei Regressionsanalysen.

Binary Cross-Entropy: Für binäre Klassifikationsprobleme (zwei Klassen) kann die Entropie verwendet werden, die den Informationsgehalt von Daten beschreibt. Eine Verlustfunktion, die den Fehler zwischen einer vorhergesagten Wahrscheinlichkeit und der Bezeichnung, die die tatsächliche Klasse darstellt, messen kann, wird als Cross-Entropy Verlustfunktion bezeichnet.

Categorical-Cross-Entropy: Analog zur binären Entropie gibt es auch die allgemeine Form, die auch für beliebig viele Klassen verwendet werden kann.

Aufgabe 3: Deep Learning Anwendungen (4 Punkte)

Finden Sie 3 Anwendungen für Deep Learning:

- **Beschreiben Sie jedes Anwendungsgebiet kurz und wo und wie Deep Learning zum Einsatz kommt, insbesondere neuronale Netze.**
- **Wo stossen die verwendeten neuronalen Netze in dem jeweiligen Anwendungsgebiet an ihre Grenzen und warum?**

1. Bilderkennungen (z.B. Google+) basieren auf Deep Learning, indem sie das Bild zuerst Schritt für Schritt analysiert. In der ersten Layer prüft das neuronale Netz beispielsweise die verwendeten Farben der Pixel (hierbei wird jedes Pixel über ein einzelnes Neuron verarbeitet) und so weiter. Durch die Vielzahl an Operatoren ist das Modell schliesslich in der Lage, ein Bild auf unterschiedliche Kategorien zuzuordnen (z.B. ist es ein Hund oder eine Katze?). Das Training wird zuerst durch den Menschen korrigiert, bis der Algorithmus sich selbst durch die Anpassungen der Gewichtungen der Variablen so verbessert hat, dass es immer genauer wird. Je mehr Bildmaterial vorhanden ist, umso mehr kann er lernen. Genau dies ist das Problem, da die Bilder so individuell sind und selten Generalisierbar sind. Es braucht eine grosse Menge an Daten, um ein Bilderkennungstool dem Menschen ebenbürtig zu machen. Zudem sind die Algorithmen im Gegensatz zum Menschen nicht darauf trainiert, auf Plausibilität zu prüfen.

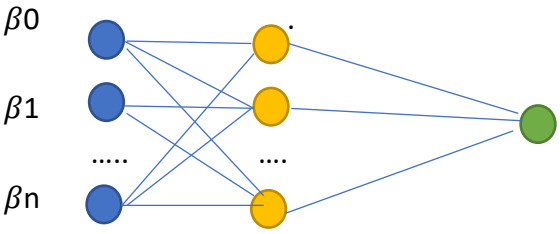
2. Spracherkennungen wie z.B. Siri oder Übersetzungen basieren auf Deep Learning. Bei der Spracherkennung stellen die einzelnen Sprachen auf der Welt als Lerninhalte dar. Je mehr Sprachen eine Maschine mit Deep Learning ausgesetzt wird, desto besser kann es diese auch verstehen, erkennen und beispielsweise in andere Sprachen übersetzen. Das grösste Problem ist zu verstehen, wie Sprachsignale in Text umgewandelt werden können. Die Charakteristika der realen Sprache wie Akzente, Hintergrundgeräusche und Mehrdeutigkeit machen es jedoch schwierig, eine perfekte Lösung zu finden.

3. Ein weiterer Anwendungsbereich ist die Cybersecurity. KI-Systeme mit Deep Learning sind durch ihr eigenständiges und kontinuierliches Lernen besonders geeignet, um Unregelmäßigkeiten in Systemaktivitäten festzustellen. Sie können so auf mögliche Hackerangriffe aufmerksam machen. Problem: durch Verunreinigung von Inputdatensätzen beispielsweise sorgen Hacker dafür, dass funktionierende Systeme fehlerhafte Ergebnisse und nicht der Realität entsprechende Bilder der Datenlage produzieren.

Aufgabe 4: Deep Learning Regression (6 Punkte)

Zeichnen Sie ein neuronales Netz für eine Regressionsanwendung. Beschreiben Sie die jeweiligen Komponenten.

Für $p\ X = \beta 0 + \beta 1X + \ldots. \beta nX$



In der Eingabeschicht werden wie Inputs der Variablen der Regression angewendet. Jede Variable hat einen eigenen Knoten im neuronalen Netz. Hier in diesem Beispiel sind dies $\beta 0$, $\beta 1$ bis βn.
Die Hidden layers können auch mehrere Schichten aufweisen und sind die Zwischenschicht zwischen In- und Output, die eine nicht-lineare Funktion auf Basis der Inputvariablen berechnen. Hier werden die Gewichtungen trainiert und angepasst, um das Modell zu verbessern.
Der Output zeigt die Vorhersage der Regression nach der Verarbeitung aller hidden layers. Die Ausgabe ist eine kontinuierliche Variable.