OPEN KNOWLEDGE

Workshop: MLOps Game

Wer wird Modellionär?

Hanna Lüschow & Oliver Zeigermann

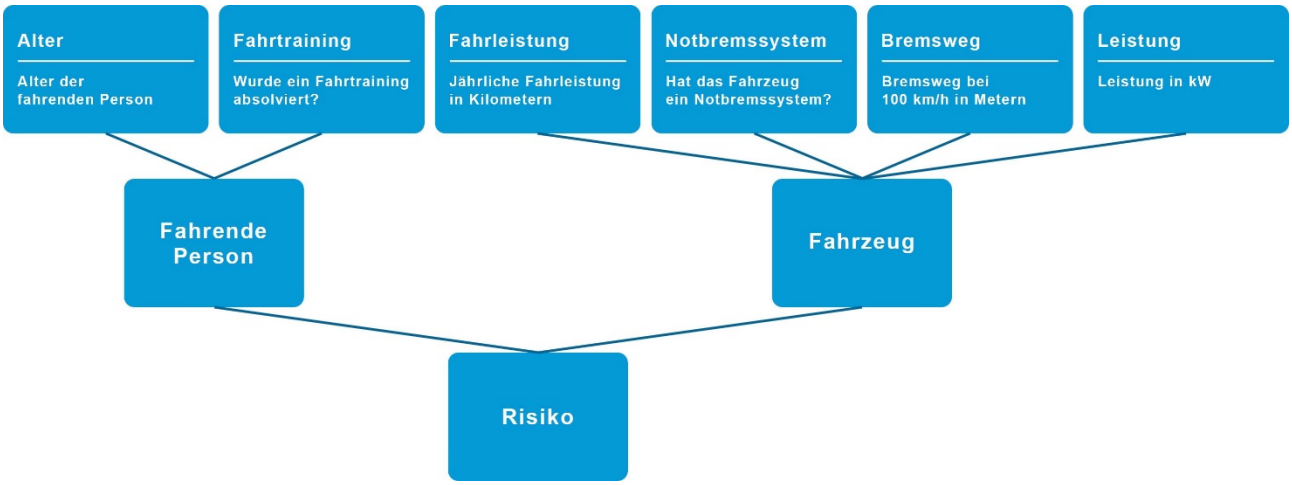
OPEN KNOWLEDGE GmbH

Stand: November 2022

Spielidee

Dieses Spiel soll euch die Prinzipien des Machine Learnings (ML) und des Betriebs eines Machine Learning-Systems (MLOps) näherbringen.
Ihr arbeitet für ein Unternehmen, das Kfz-Versicherungen anbietet. Eure Aufgabe ist es, einen Machine Learning-Ansatz für die Ermittlung des Versicherungsrisikos auszuwählen und über 5 Runden möglichst gut zu wirtschaften. Während des Spiels treten unterschiedliche Ereignisse auf, die an reale Probleme in Machine Learning-Projekten angelehnt sind. Am Ende gewinnt, wer am meisten Geld verdient hat.

Die folgende Grafik stellt die inhaltlichen Zusammenhänge der einzelnen Features dar. Diese zusammengenommen ergeben am Ende den Risikofaktor, der wiederum die Versicherungsbeiträge beeinflusst.



Spielvorbereitung

> Bildet Gruppen von 3-5 Personen.
> Denkt euch jeweils einen Namen für euer Unternehmen aus, ihr habt 2 Minuten Zeit.
> Jede Person bekommt ein Startkapital von **25 Geld**.
> Alle wählen für sich einen ML-Ansatz (siehe Steckbriefe). Beachtet die unterschiedlichen initialen Kosten und die Kosten und Erträge pro Runde.
> Berechnet für jede Person die folgenden initialen Kosten:
  Datenbeschaffung: **10 Geld** (für alle)
  ML-Design: **10 Geld** (Deep Learning) / **5 Geld** (KNN & Decision Tree)
  (Siehe Tabelle für initiale Kosten)
> Wer zuletzt einen Komplettausfall hatte, fängt an.

Hinweis zu den ML-Ansätzen:

Es kann passieren, dass ihr euren Ansatz im Laufe des Spiels aufgrund von unvorhergesehenen Ereignissen wechseln müsst.

Spielablauf

Das Spiel geht über 5 Runden, in denen ein ML-System in Produktion simuliert wird.
In jeder Runde würfelt ihr reihum und müsst auf Ereignisse reagieren und zum Beispiel euren Ertrag anpassen.

Immer wenn du an der Reihe bist, führst du diese Schritte nacheinander aus:

- Berechne dein Geld auf Basis von deinen Kosten und Erträgen.
- Bist du mit deinem gewählten Modell nicht mehr zufrieden, kannst du es jetzt wechseln. Du musst dabei keine neuen Daten beschaffen, es fallen jedoch die Kosten für das ML-Design an (siehe Tabelle initiale Kosten). Deine laufenden Kosten und Erträge werden an die Startwerte des neuen Modells angepasst.
- Würfele (je nach Ereignis evtl. mehrfach)
- Berechne auf Basis des Ereignisses dein Geld, deine Kosten und deinen Ertrag neu.

Wichtig:

Solltest du jemals unter **0 Geld** fallen, scheidest du aus dem Spiel aus! Beachte dies, wenn du z. B. deinen ML-Ansatz wechselst.

Spielende

Das Spiel endet nach der 5. Runde. Ihr berechnet ein letztes Mal euer Geld anhand eurer Kosten und Erträge. Wer am meisten Geld hat, gewinnt das Spiel und ist Modellionär.
Es gibt einen Gleichstand? Dann teilt ihr euch den Sieg.

Kosten und Erträge

Die Kosten und Erträge der einzelnen Modelle sind unterschiedlich.

Initiale Kosten:

	Daten beschaffen *(initial)*	Daten beschaffen *(später im Spiel)*	ML-Ansatz designen
Deep Learning	10	5	10*
K-Nearest Neighbors (KNN)	10	5	5
Decision Tree	10	5	5
Regelsystem	10	5	0**

* Jede Iteration braucht länger und benötigt bessere Hardware.

** Der Aufwand zur Erstellung des Regelsystems ist im Vergleich zu einem ML-Ansatz vernachlässigbar. Aufgrund dessen fallen hierfür keine weiteren Kosten an.

Laufende Kosten und Erträge:

Die laufenden Kosten berechnen sich aus dem Ressourcenbedarf, der Ertrag ergibt sich aus der Genauigkeit des gewählten Modells.

	Kosten pro Runde (−)	Erträge pro Runde (+)
Deep Learning	4	12
K-Nearest Neighbors (KNN)	5	7
Decision Tree	2	8
Regelsystem	1	4

Ereignisse

Die Last verändert sich.

Würfele nochmal:

Die Last steigt, es werden mehr Ressourcen benötigt.	Die Kosten verdoppeln sich. (Maximum: 10)
Die Last sinkt, es werden weniger Ressourcen benötigt.	Die Kosten halbieren sich. (Minimum: 1)

Ein übles Ereignis tritt ein.

Würfele nochmal:

Die Kunden fordern Erklärung.
Hast du ein Modell mit guter oder schlechter Erklärbarkeit?

Bei schlechter Erklärbarkeit:
Notabschaltung und Fallback auf Regelsystem

Investigativer Journalismus
Bias, in diesem Fall Altersdiskriminierung
Nutzt du das Alter für deine Berechnung? Dann musst du es aus den Features entfernen. Dies bleibt bis zum nächsten Ansatzwechsel.
Hast du jetzt noch mehr als ein anderes Feature für deine Berechnung?

Mehr als ein anderes Feature:
Dein Modell hat eine geringere Genauigkeit. Dein Gewinn reduziert sich um **2 Geld**.
Nur ein anderes Feature:
Notabschaltung und Fallback auf Regelsystem

Adversarial Attack
Angreifer wollen die Vorhersage manipulieren.
Hast du eine hohe oder niedrige innere Komplexität?

Bei niedriger Komplexität:
Der Angriff ist erfolgreich. Du musst einen anderen ML-Ansatz wählen. Zahle dafür die „ML-Ansatz designen“ Kosten.

Hackerangriff
Hast du Kundendaten in Produktion?
Von den vier angegebenen ML-Ansätzen hat nur KNN Kundendaten in Produktion.

Kundendaten in Produktion:
Die Marketingabteilung muss den Schaden ausbügeln, das kostet dich **10 Geld**.
Um im Geschäft zu bleiben, musst du außerdem einen neuen ML-Ansatz wählen. Zahle dafür die „ML-Ansatz designen“ Kosten.

Ein gutes Ereignis tritt ein.

Würfele nochmal:

Es hat sich ein Investor gefunden, der dir deine Firma abkaufen will. Würfele noch einmal. Diese Zahl multipliziert mit 10 ist das Angebot. Wenn du es annimmst, ist das Spiel für dich beendet. Für dein Endergebnis zählt nur der Verkaufspreis, nicht dein bisheriges Kapital.

Dein Modell hat wegen [hier guten Grund ausdenken] an Relevanz gewonnen.	Dein Gewinn verdoppelt sich.

Die Welt ändert sich und ein Drift setzt ein.

Du musst neue Daten beschaffen, zahle **5 Geld**.
Wenn du das Regelsystem nutzt, fallen keine weiteren Kosten an. Ansonsten würfele nochmal:

Das Modell performt mit den neuen Daten immer noch hervorragend.

Es muss mit neuen Daten trainiert werden.
Hast du ein stabiles oder ein instabiles Modell?

Bei stabilem Modell:
Zahle **2 Geld**
Bei instabilem Modell:
Zahle **4 Geld**

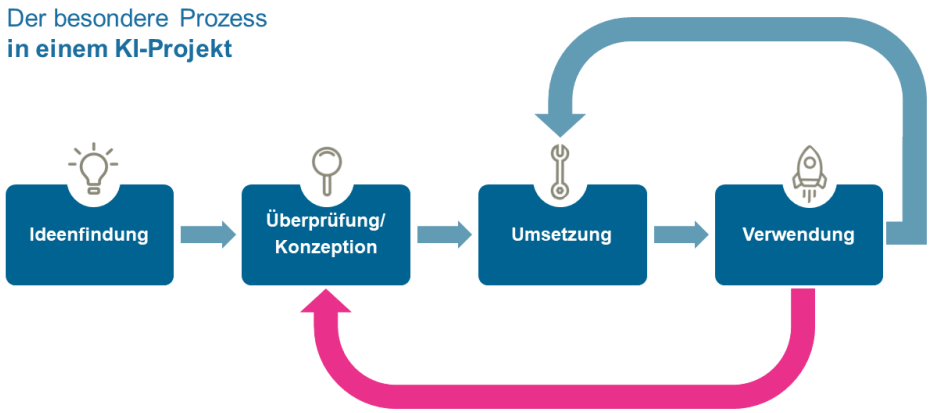
Du brauchst eine neue Modell-Architektur, erreichst aber die ursprüngliche Performance mit vertretbarem Aufwand.

Zahle **5 Geld**, um deinen ML-Ansatz erneut zu designen.

Es läuft alles rund. ☺

Glossar

Der KI-Prozess besteht aus 4 Phasen, an denen sich auch dieses Spiel orientiert. In der Konzeptionsphase wählst du ein Modell aus, das du in der Umsetzung designst. Danach folgt die Verwendungsphase, die den größten Teil des Spielablaufs abbildet.

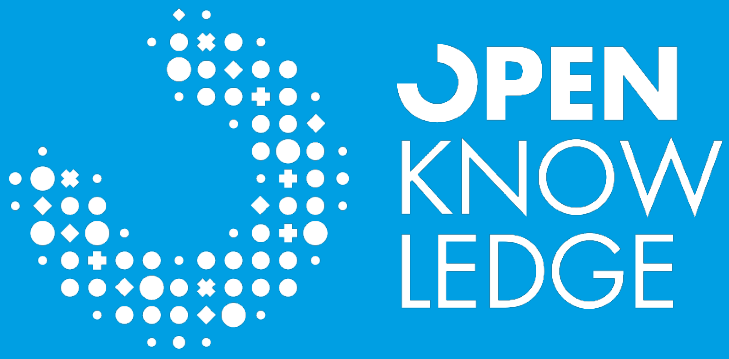


Eigenschaften von Ansätzen

- **Features:** Features sind Eingaben in das Vorhersage-System, z.B. Alter, Leistung, etc.
- **Erklärbarkeit:** Eine gute Erklärbarkeit bedeutet, dass einem (nicht technikaffinen) Kunden die Schlussfolgerungen und Entscheidungen des Systems verständlich aufgezeigt werden können.
- **Genauigkeit:** Die Genauigkeit bildet die Anzahl der korrekten Vorhersagen des Modells bei einer Test-Menge ab.
- **Stabilität:** Bei einem stabilen Modell bleiben die Vorhersagen für alle Bereiche, die nicht von neuen Daten betroffen sind, gleich.
- **Ressourcenbedarf:** Der Ressourcenbedarf setzt sich aus dem Aufwand und den Kosten für den Betrieb des Modells zusammen.
- **Innere Komplexität:** Die innere Komplexität beschreibt die Nachvollziehbarkeit der Funktionsweise des Modells für technikaffine Menschen.

Ereignisse

- **Drift:** Die Welt ändert sich und dein Modell passt möglicherweise nicht mehr.
- **Adversarial Attack:** Nutzer haben die interne Funktionsweise deines Systems durchschaut. Sie machen sich dieses Wissen zu Nutze und passen ihre Angaben so an, dass sie einen Vorteil erhalten.



Kontakt

OPEN KNOWLEDGE GmbH
Poststraße 1, 26122 Oldenburg
Tel.: +49 441 – 4082-0
Fax: +49 441 – 4082-111

Autoren
Hanna Lüschow
hanna.lueschow@openknowledge.de

Oliver Zeigermann
oliver.zeigermann@openknowledge.de