

FH-Prof Dr. Lars Mehnen



Grenzen & Potentiale von künstlicher Intelligenz



Intro

Alles, was man heute unter künstlicher Intelligenz versteht ist

durch Algorithmen gesteuert,
und deswegen „keiner eigenen Einsicht“ fähig.

Diese Erkenntnis systematisch erarbeitet und sogar bewiesen zu haben ist ein Verdienst des britischen Mathematikers Roger Penrose. Viele kennen ihn auch als theoretischen Physiker.



Penrose

Heutige KI führt rein mechanisch Rechnungen durch, ohne selbst irgend etwas verstehen zu können. Sie nutzt lediglich das Verständnis ihrer Schöpfer, der Programmierer.

Diese Maschinen erscheinen nur deswegen so mächtig, weil sie unglaublich schnell und genau arbeiten.

Computer führen rasch und „fehlerfrei“ ihnen vorgegebene Rechenvorschriften aus und erreichen hier eine Perfektion, die die Fähigkeiten des Menschen weit übersteigt.

Zusammenfassend stellt Penrose fest:

Wo ein menschlicher Spieler sich immer wieder ein Urteil bildet, sinnvolle Pläne entwickelt und insgesamt versteht, worum es beim Spiel geht, punktet KI einfach nur mit ihrer Fähigkeit, in kürzester Zeit riesige Mengen von Daten erzeugen und nach gegebenen Kriterien als Lösung bzw. Nicht-Lösung klassifizieren zu können.

Fake

Was ist jetzt aber eine Lösung oder Nicht-Lösung.
Was ist Richtig und was ist Falsch.

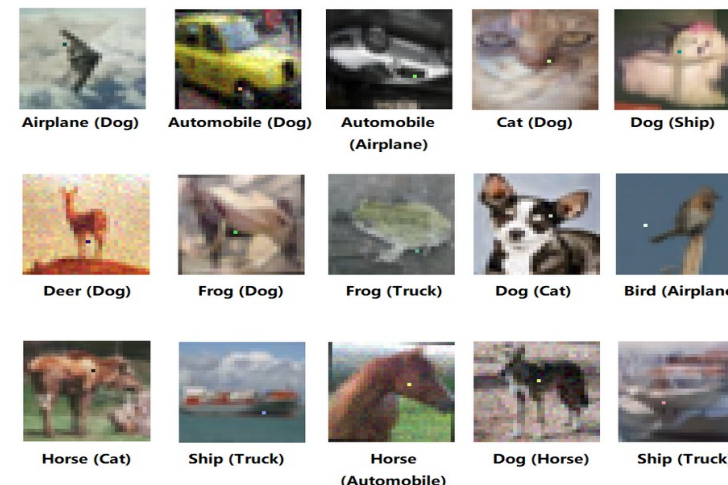


Fake

Fake hat häufig Zweck !

Warum ist das in der KI relevant ?

NN-Klassifizierer können
„leicht“ beeinflusst werden,
wie Adversarial Attacks on



Fake / Beispielp Probleme

Kopierer / Telekommunikation

Voice Cloning:

<https://www.youtube.com/watch?v=0sR1rU3gLzQ>

Deep Fakes (Face cloning / swapping):

<https://www.youtube.com/watch?v=aJq6ygTWdao>

<https://www.youtube.com/watch?v=duo-tHbSdMk>

Visual Microphones:

<https://www.youtube.com/watch?v=duo-tHbSdMk>

Isolate Speech Signals:

<https://www.youtube.com/watch?v=zL6ltnSKf9k>

Bildkompression: JBig2

Bild



Bild

Dieser Satz
kein Verb

Bild

ABCDEFGHIJK
LMNOPQRST
UVWXYZ

Bild

1 2 3 4 5 6 7 8 9 0
1 2 3 4 5 6 7 8 9 0

Bildkompression: JBig2, beides komprimiert



Dieser Satz
kein Verb

ABCDEFGHIJK
LMNOPQRST
UVWXYZ

1 2 3 4 5 6 7 8 9 0
1 2 3 4 5 6 7 8 9 0

Bildkompression: JBig2, mit Pattern Matching



↓ ↓
Dieser Satz
kein Verb
↑ ↑
ABCDEFGHIJK
LMNOPQRST
UVWXYZ

1 2 3 4 5 6 7 8 9 0
1 2 3 4 5 6 7 8 9 0

Bildkompression: JBig2, mit Pattern Matching



**Dieser Satz
kein Verb**

**ABCDEFGHIJK
LMNOPQRST
UVWXYZ**

**1 2 3 4 5 6 7 8 9 0
1 2 3 4 5 8 7 8 9 0**

Bildkompression: JBig2, mit Pattern Matching



Dieser Satz
kein Verb

ABCDEFGHIJK
LMNOPQRST
UVWXYZ

1 2 3 4 5 6 7 8 9 0
1 2 3 4 5 8 7 8 9 0

Fake or Fact ?

- Traue keinem Scan, den du nicht selbst gefälscht hast
- <https://www.youtube.com/watch?v=7FeqF1-Z1g0&t=114s>

Fake und Strategie

Da man beim Sammeln von Informationen teilweise absichtlich oder unabsichtlich verfälschte Informationen als Grundlage für Trainingsdatensätze bekommt, sollte man eine Meta-Ebene mit potentiellen Modifikatoren mit einbeziehen.

Dies wird am Beispiel von Kartenspielen gut verdeutlicht....

Schwierig wird es aber, wenn dynamische Strategiewechsel stattfinden.



Poker-face

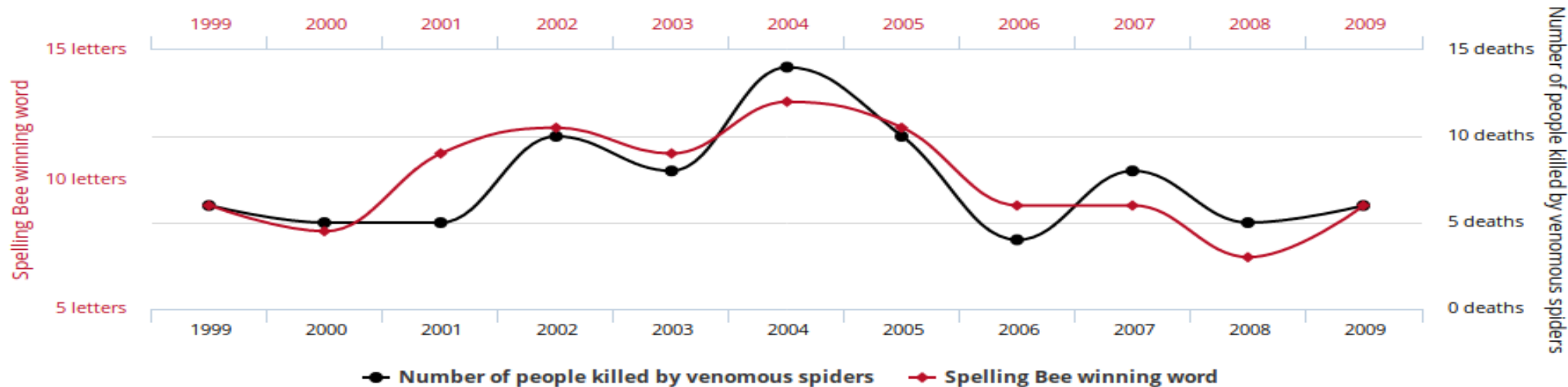
Correlation is NOT Causation

Letters in Winning Word of Scripps National Spelling Bee

correlates with

Number of people killed by venomous spiders

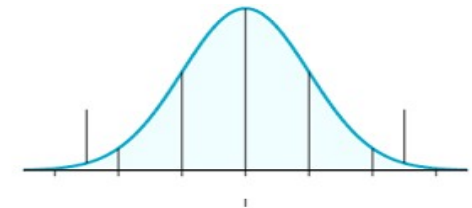
Correlation: 80.57% ($r=0.8057$)



Correlation is NOT Causation

In NN, CNN, RNN etc. werden Verfahren verwendet, die meist auf Korrelation oder ähnlichen Verfahren beruhen.

Korrelation funktioniert aber lediglich auf Datensätzen, die gewissen statistischen Bedingungen genügen.

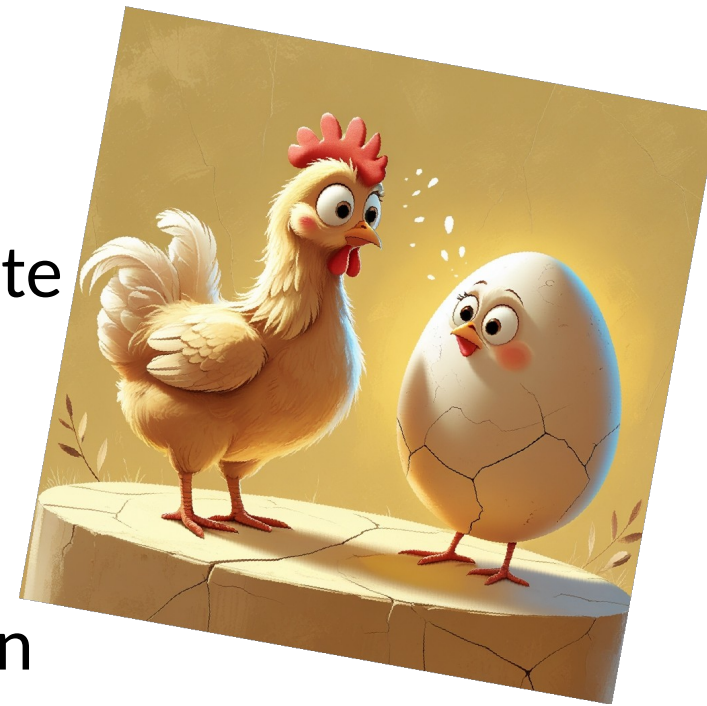


Wenn diese dann für die Klassifizierung herangezogenen Bedingungen z.B. nicht genügend einer Normal Verteilung ähnelt, sind Aussagen, die Aufgrund der Varianz getroffen werden nicht besonders aussagekräftig.

Correlation is NOT Causation

Dies ist in den meisten Fällen unproblematisch, da Messwerte aus einfachen Umgebungen meist lediglich Resultate aus Additiven oder Multiplikativen Prozessen sind, die der Normalverteilung nicht viel anhaben können.

Sind die Parameter aber Ergebnisse aus rekursiven Prozessen oder Umordnungen (Sortierung / Priorisierung) so werden die Verteilungen geändert und Aussagen oft unbrauchbar.



Correlation is NOT Causation

Wenn man klassische Korrelationen verwendet,
wirft dies zusätzlich noch eine Problematik auf.

Der Korrelations-Wert ist ein ungerichtetes Maß.

Die Aussage gilt also für beide Richtungen, was in
der Realität oft nicht stimmt.



Fact

Fakt: Bedeutungen:

Tatsächlich bestehender Umstand, unumstößliche Tatsache, d.h. etwas wirklich Vorhandenes, Existierendes.



Hier wird leider der Umstand „**warum**“ etwas existiert nicht betrachtet – ein Fakt hat also „keine“ Bedeutung da er in keinem Zusammenhang steht.

Causal Inference

Um die meisten modernen KI-Werkzeuge benutzen zu können, müssen Zusammenhänge aber analysiert, erkannt und bewertet werden.

Geschieht dies nicht, können und werden falsche Schlussfolgerungen gezogen.



Causal Inference

Dies wird sehr gut anhand einiger Statistischer Bias-Typen klar:

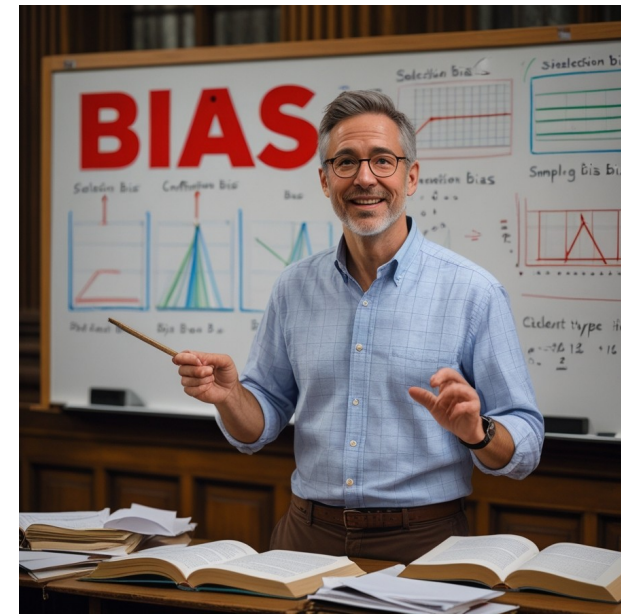
Selection bias Self-selection bias

Recall bias Observer bias

Survivorship bias Omitted variable bias

Cause-effect bias Funding bias

Cognitive bias



Causal Inference

this statement is false.

Einige sehr bekannte Statistische Paradoxi,
die auf Abhängigkeiten beruhen sind z.B.

- 1) Das Monty Hall Problem (unsymmetrische Bedingung)
- 2) Berkson's Paradox (Collider Bias)
- 3) Simpsons Paradox (Direkte und Indirekte Abhängigkeiten)

Causal Inference

Dies ist insbesondere Wichtig, handelt es sich um ein:

- Front-Door Problem
(Direkte und Indirekte Abhängigkeiten)
- Back-Door Problem
(Abhängigkeiten von „Input“ Parametern)
- Rekursives Problem (Abhängigkeiten auf sich selbst)



Causal Inference

Glücklicherweise können heutzutage diese Abhängigkeiten geprüft und in „einfachen Fällen“ gelöst werden.

Die Forschung in der Statistik auf diesem Gebiet fängt leider gerade erst an populär zu werden.

Leider werden diese Statistischen-Werkzeuge noch nicht häufig verwendet.



Es gibt viel zu tun...

