

Grundlagen

Unsupervised Learning hilft besonders beim Verständnis unbekannter Daten, und mit Long-Short-Term-Memory-Netzen lässt sich unter anderem Kundenverhalten vorhersagen. Reinforcement Learning gewinnt im produktiven Einsatz zunehmend an Bedeutung. Für alle ML-Anwendungen ist das Verständnis der Black Box wichtig, um Entscheidungen nachzuvollziehen.

ab Seite 6



Tools

Python Libraries wie NumPy und Pandas helfen bei der Aufbereitung von Daten. Bei den ML-Frameworks ist TensorFlow weiterhin der Platzhirsch, aber PyTorch etabliert sich ebenfalls in einigen Bereichen. Für die Versionierung von ML-Daten existieren Open-Source-Tools wie DVC. Und auch im mobilen und IoT-Umfeld lässt sich ML sinnvoll nutzen.

ab Seite 34

Grundlagen

- Unsupervised Learning: Methoden und Einsatz
- Experimente für Reinforcement Learning
- Long Short-Term Memory für Geschäftsanwendungen
- Erklärbarkeit und Fairness

Tools

- Ein Streifzug durch die PyData-IT-Landschaft
- TensorFlow 2.0 und Keras: Imperative Modellentwicklung
- PyTorch als Alternative zu TensorFlow
- Data Version Control im Team mit Open-Source-Werkzeugen
- Machine Learning für IoT und Mobile

Infrastruktur

- Vom Modell zum produktiven Einsatz
- Machine Learning as a Service
- Hardwarebeschleuniger für neuronale Netze
- Julia – eine differenzierbare Programmiersprache für ML

Praxis

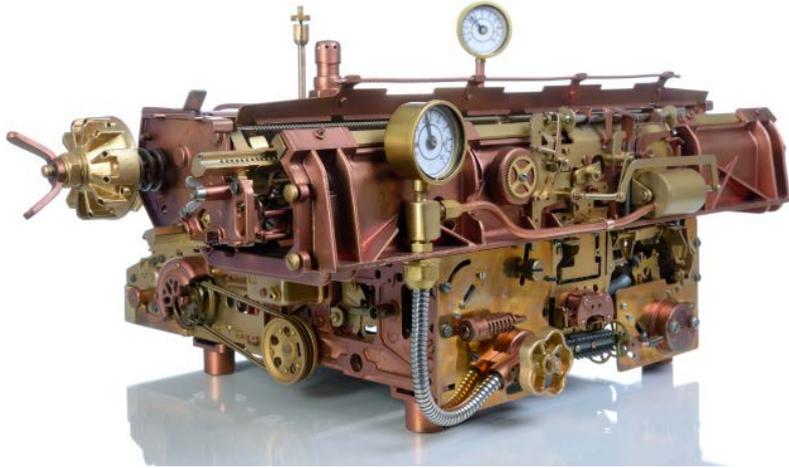
- 6 Word Embeddings: Theorie und Beispielanwendung 84
- 16 Textanalyse mit BERT 94
- 24 Methoden für Zeitreihenvorhersagen 100
- 30 Deep-Learning-Tutorial Bildanalyse:
 - Teil 1: Bilder für das Modelltraining aufbereiten 108
 - Teil 2: Trainieren des Modells 114
 - Teil 3: Einsatz auf der Zielhardware 120
- 34 Machine Learning zur Schadcode-Erkennung 126
- 40 Recommender-Systeme in der Praxis 129

Security und Recht

- 54 Gefahren durch Angriffe auf KI 137
- Neuronale Netze: Angriffe und Verteidigung 140
- Datenschutz und Urheberrecht bei der KI-Entwicklung 143

Sonstiges

- 60 Editorial 3
- 64 Impressum 89



Infrastruktur

Auf dem steinigen Weg vom Modell in den Produktivbetrieb helfen Open-Source-Tools wie ONNX und FastAPI. Die großen Cloud-Provider bieten derzeit vorkonfigurierte ML-Dienste an. Für den Betrieb im eigenen Unternehmen existieren unterschiedliche Hardwarebeschleuniger. Die Programmiersprache Julia bietet einige Konzepte, mit der sie Python als ML-Sprache herausfordern möchte.

ab Seite 60

Praxis

Die Textanalyse ist ein spannendes Feld, das in den letzten Jahren dank Verfahren wie BERT deutlich an Fahrt aufgenommen hat. Word Embeddings sind ein Standardverfahren, um Zusammenhänge in Texten zu erkennen. Ein dreiteiliges Tutorial führt in die Bildanalyse ein, und das Heft beleuchtet Zeitreihenanalyse, Recommender-Systeme und ML im Kampf gegen Hacking.

ab Seite 84



Security und Recht

ML-Systeme sind zunehmend Ziel unterschiedlicher Angriffe, und bei neuronalen Netzen findet ein regelrechter Wettlauf zwischen Angriffs- und Verteidigungsmethoden statt. Derzeit gilt es, beim Verwenden von Daten in ML-Anwendungen Datenschutz und Urheberrecht zu beachten.

ab Seite 137