

Die Macht der Algorithmen - technische Hintergründe, digitale Perspektiven und mögliche Handlungsempfehlungen

Prof. Dr. Ulrich Trottenberg

Interscience GmbH – Partner für Wissenschaft und Wirtschaft

Fraunhofer SCAI – Institut für Algorithmen und Wissenschaftliches Rechnen
Mathematisches Institut, Univ. zu Köln – Angewandte Mathematik

19.09.2018, Universität zu Köln

Digitale Schlagworte

- Industrie 4.0
- Internet der Dinge (IoT)
- Zukunftsstadt, Smart City
- Big Data
- Maschinelles Lernen
- Künstliche Intelligenz, Autonome Systeme

Auswirkungen auf

- Arbeitswelt, neue Berufszweige
- Wirtschaft, neue Branchen
- Wissenschaft, Medizin
- Politik, Verwaltung
- *Bildung, Kultur*
- Lebenswelt jedes Einzelnen
- ...

Technologieentwicklung

- Rechner
- Netze
- Daten
- *Algorithmen*

Rechner

- Moore's Law (1965):
Leistungssteigerung Faktor 2 in 18 Monaten
 - Faktor 10 in 5 Jahren
 - Faktor 1.000.000 in 30 Jahren

Netze

- E-Mail seit 1971
- Internet (http...) seit 1993
- Flächendeckende Glasfasernetze bis 2020
- € 5 Mrd. Infrastruktur-Ausbau für Schulen
- „Gigabit Gesellschaft“ 2025 (Giga = 1 Mrd.)

Heute:

- IPv4: $256^4=2^{32}$ = ca. 4.300.000.000 Adressen

Internet der Dinge:

- IPv6: 2^{128} = ca. 340.000.000.000.000.000.000.000.000.000.000.000.000.000 Adressen

Daten

- Datenexplosion : 5 ZettaByte (Zetta = 10^{21})
- (DVD Stapel, 4 x von der Erde bis zum Mond)

Beispiele:

- Google Suchanfragen: 4 Mill./min
- Facebook Einträge: 40 Mill./min
- Instagram Fotos: 50.000/min
- YouTube Videomaterial: 400 h/min

Algorithmen

Herkunft des Wortes:

- *Al-Chwarizmi* (780 – 840, Bagdad), Universalgelehrter

Definition:

- Eindeutige Handlungsvorschrift, die aus endlich vielen Einzelschritten besteht (und *terminiert*), zur Lösung eines Problems.

Alltägliche, nichtmathematische Beispiele

- Kochrezept, Wegbeschreibung, Anleitung zum Regalbau

Computerprogramme

Typen von Algorithmen

- Elementare
- Mathematische (Berechnung)
- Informatische (Daten)
- Interdisziplinäre, Kombinationen

Elementare Algorithmen

- Schriftliche Multiplikation
- Euklidischer Algorithmus (2300 Jahre alt, Berechnung des ggT. zweier ganzer Zahlen)
- 0/1 Codierung
- ...

„Mathematische“ Algorithmen

- Numerische Simulation: math. Modell + Berechnung
 - Numerik, Statistik, Optimierung, ...
- Anwendungen in
 - Natur-, Ingenieur-, Wirtschaftswissenschaften
- Beispiele:
 - Crash Simulationen
 - Wetter-, Klimaprognose
 - Optimierung
- „Schnelle“ Algorithmen: von $\sim N^2$ zu $\sim N$ Operationen

„Informatische“ (diskrete) Algorithmen

- Daten„verarbeitung“: Datenbanken
 - Suchen und Sortieren
- Datenkompression (mp3,...)
- Datenanalyse, insb. für BigData
 - Informationsextraktion, Knowledge Discovery
 - Data-Mining (Finden neuer Muster in Datenbeständen)
 - Maschinelles Lernen (z.B.: Klassifizierung, durch Training)
 - KI, Deep Learning (mit sog. Neuronalen Netzen)

Interdisziplinäre Algorithmen, Kombinationen

- GPS (Geographie, Relativitätstheorie)
- mp3 (Akustik)
- ...
- KI (Deep Blue 1996, AlphaGo 2016, Sprach-, Gesichts-, Stimmungserkennung usw.)
- Manifold Learning
- Deep Reinforcement Learning

- „Technological Singularity“ 2045? (Ray Kurzweil)
- ...

Digitale Bildung (gesamte Bildungskette)

- Digitales Basiswissen
- *Algorithmisches Verständnis*
- Erlernen einer Programmiersprache
- Calliope, Roberta Light, Erlebe IT,...

Repräsentative Algorithmen (für Schule und Lehreraus- und fortbildung)

- MINT-Kinderzimmer, Dynamische Labyrinth (KiTa, Grundschule)
- Schriftliche Rechenverfahren (elementares Rechnen; Grundschule)
- **0/1-Darstellung beliebiger Dezimalzahlen (elementares Rechnen; Grundschule)**
- Euklidischer Algorithmus (elementare Zahlentheorie; Grundschule)
- Gaußscher Algorithmus (lineare Algebra, elementare Numerik; Sek I)
- Matrixmultiplikation (lineare Algebra; Sek I)
- Iterative Lösung linearer Gleichungssysteme (elementare Numerik; Sek I)
- Schnelle Lösung linearer Gleichungssysteme (Analysis, Numerik; Sek II)
- Elementare Verschlüsselung, z.B. „Caesar“ (elementare Kryptographie; Grundschule)
- **RSA-Verschlüsselung (elementare Zahlentheorie; Sek I/II)**
- Suchen und Sortieren (Sek I)
- **Kürzeste Wege, z.B. „Christofides-Heuristik“ (elementare Optimierung; Sek I)**
- TSP (Optimierung, P/NP-Problematik; Sek I/II)
- Simplex-Verfahren (lineare Optimierung; Sek II)
- Verkehrs-/Stausimulation, zelluläre Automaten etc.; (Sek I/II)
- Absorb. Markow-Ketten (elementare Wahrscheinlichkeitsrechnung; Sek I/II)
- **mp3 (Analysis, Fouriertransformation, Akustik etc.; Sek I/II)**
- Datencodierung, -kompression (Grundschule; Sek I/II)
- **GPS (Analysis, Relativitätstheorie, Sek I/II)**
- Interpolation: Polynom-, Spline-Interpol. etc. (Analysis, Numerik; Sek I/II)
- Wavelets (Analysis, Numerik; Sek II)
- **Google Page Ranking (lineare Algebra, Analysis; Sek II)**
- SVM (Klassifizierung, Statistik, Informatik; Sek II)
- **PCA, SVD (multivariate Statistik; Sek II)**
- Lernen mit Kernen (maschinelles Lernen; Sek II)
- **Deep Learning (mehrschichtige Neuronale Netze; Sek II)**
- Quantum Computing (Sek II)

Risiken, Bedrohungen - *und algorithmische Antworten?*

- Ausspähung, Datenschutz?, *Verschlüsselung!*
- Persönlichkeitsrechte, Kontrolle über eigene Daten?, Löschung?

- Hackerangriffe, „Darknet“, *Cybersicherheit*
- Programmierfehler, *Verifikation*

- Algorithmische Entscheidungen (ADM)
 - Bewerberselektion, Bankkredite, Versicherungsbedingungen,...
 - Börsenhandel (HFT)

- Fake News, Verschwörungstheorien

- **Fehlende digitale Aufklärung der Öffentlichkeit, Leichtfertigkeit**

Fazit

- Was wollen wir? Was wollen wir nicht?
- **Gestaltung** der digitalen Entwicklungen
- Gesellschaft, Presse, Politik und Technologie

- **Digitale Aufklärung und Bildung**

- *Digitale Bildung und „Medienkompetenz“ ohne algorithmisches Verständnis bleibt substanzlos.*

Vielen Dank für Ihr Interesse
und Ihre Aufmerksamkeit.