

Randomisierte Algorithmen

1. Einleitung

Thomas Worsch

Fakultät für Informatik
Karlsruher Institut für Technologie

Wintersemester 2019/2020

Überblick

Organisatorisches

Grundsätzliches

Schlagwörter

Geschichtliches

Literatur

Allgemeine Informationen

- ▶ Termin 1: jede Woche
jeweils Donnerstag, 11:30 – 13:00 in Raum 236
- ▶ Termin 2: alle zwei Wochen
jeweils Montag, 11:30 – 13:00 in HS -101
erstmalig erst am Montag, **4. November!**
- ▶ Unterlagen zu Vorlesungen und Übungen:
<http://liinwww.ira.uka.de/~thw/vl-rand-alg/>
- ▶ die Vorlesung ist prüfbar
 - ▶ Termine bitte rechtzeitig vereinbaren

Überblick

Organisatorisches

Grundsätzliches

Schlagwörter

Geschichtliches

Literatur

Sichtweisen für randomisierte Algorithmen

Erweiterung des klassischen Begriffs eines deterministischen Algorithmus:

Sichtweisen für randomisierte Algorithmen

Erweiterung des klassischen Begriffs eines deterministischen Algorithmus:

- ▶ neuer *algorithmischer Elementarschritt*
Beschaffung eines zufälligen Wertes
- ▶ „*quantifizierter Nichtdeterminismus*“
mit (schönen!) Wahrscheinlichkeiten gewichtete Auswahl
für den nächsten Elementarschritt
- ▶ *zufällige „uneigentliche“ Eingabe* (neben der „normalen“)
zufällige Auswahl eines deterministischen Algorithmus

Die fundamentale Neuerung

Mehrere Ausführungen

des *gleichen* randomisierten Algorithmus
für die *gleiche* Eingabe

können verschieden sein,
insbesondere verschiedene Ergebnisse liefern!

Zufallsvariablen überall

Selbst für eine einzelne Eingabe sind

- ▶ die benötigte Laufzeit
- ▶ der benötigte Speicherplatz
- ▶ das berechnete Ergebnis

Zufallsvariablen.

Algorithmen mit unbekannter Laufzeit

- ▶ Will man das?
- ▶ «Wie unbekannt?»
 - ▶ *Quantifizierung?*

Algorithmen, die «variierende Ausgaben» liefern

- ▶ vielleicht erträglich bei Optimierungsproblemen
 - ▶ *Quantifizierung?*
- ▶ Erzeugung «zufälliger Objekte»
 - ▶ *Eigenschaften?*

Algorithmen, die «falsche Ausgaben» liefern

- ▶ Will man das?
- ▶ Schlägt in diesem Hörsaal gleich ein Meteorit ein?
- ▶ Ist $2^{400} - 593$ die größte Primzahl kleiner als 2^{400} ?
- ▶ Soll die Ampel jetzt auf grün schalten?

- ▶ *Fehlerwahrscheinlichkeit?*

Vorteile randomisierter Algorithmen

Sie sind manchmal

- ▶ leichter zu formulieren und zu implementieren
- ▶ schneller
- ▶ besser
- ▶ die einzige Möglichkeit

Vorteile randomisierter Algorithmen

Sie sind manchmal

- ▶ leichter zu formulieren und zu implementieren
- ▶ schneller
- ▶ besser
- ▶ die einzige Möglichkeit

Aber: Man zahlt einen Preis!

Nicht in dieser Vorlesung

probabilistische Analyse deterministischer Algorithmen

Überblick

Organisatorisches

Grundsätzliches

Schlagwörter

Geschichtliches

Literatur

Wie kann Zufall helfen?

Wie kann Zufall helfen?

- ▶ Symmetriebrechung
- ▶ Balancierung
- ▶ zufälliges Auswählen und Umordnen
- ▶ Vereitelung «gegnerischer Angriffe»
- ▶ Fingerabdrücke
- ▶ Überfluss an Zeugen
- ▶ schnelles Mischen
- ▶ ...

Weitere Aspekte

- ▶ die *probabilistische Methode*
- ▶ randomisierte Komplexitätsklassen
- ▶ Zufall als Berechnungsressource
- ▶ Elimination von Zufall

Überblick

Organisatorisches

Grundsätzliches

Schlagwörter

Geschichtliches

Literatur

Manche Ideen sind alt

- ▶ Omar Khayyam Moore (1957)
Divination—a new perspective
American Anthropologist 59, pp. 69-74.

Manche Ideen sind alt

- ▶ Omar Khayyam Moore (1957)
Divination—a new perspective
American Anthropologist 59, pp. 69-74.
- ▶ zitiert von
J. Shallit (1992)
Randomized algorithms in “primitive” cultures or
what is the oracle complexity of a dead chicken.
ACM SIGACT News 23(4), pp. 77–80.

Entwicklung in der Informatik

- 1955: de Leeuw: probabilistische Maschinen
- 1963: Rabin: probabilistische endliche Automaten
- 1977: Gill: probabilistische Turingmaschinen
- 1976: Rabin: randomisierter Primzahltest
- 1977: Solovay/Strassen: randomisierter Primzahltest

Überblick

Organisatorisches

Grundsätzliches

Schlagwörter

Geschichtliches

Literatur

Bücher zum Thema

- ▶ Motwani/Raghavan (1995)
Randomized Algorithms
Cambridge University Press.
- ▶ Hromkovič (2004)
Randomisierte Algorithmen: Methoden zum Entwurf von zufallsgesteuerten Systemen für Einsteiger Teubner-Verlag.
- ▶ Borodin/El-Yaniv (1998)
Online Computation and Competitive Analysis
Cambridge University Press.

Weitere Bücher, Aufsätze und Online-Dokumente

sind im Skript aufgeführt.