



### ARBEITSGRUPPE KRYPTOGRAPHIE UND KOMPLEXITÄTSTHEORIE

Prof. Dr. Marc Fischlin

Dr. Christian Janson

Patrick Harasser

Felix Rohrbach

Sommersemester 2020

Veröffentlicht: 24.04.2020, 14:00 Uhr MESZ

---

## P1 (Gruppendiskussion)

---

Nehmen Sie sich etwas Zeit, um die folgenden Fachbegriffe in einer Kleingruppe zu besprechen, sodass Sie anschließend in der Lage sind, die Begriffe dem Rest der Übungsgruppe zu erklären:

- (a) Algorithmus;
- (b) Sortieralgorithmen und InsertionSort;
- (c) Totale Ordnung;
- (d) Schleifeninvariante.

---

## P2 (Pseudocode schreiben)

---

Betrachten Sie folgende Probleme für ein nicht-leeres Array  $A$  ganzer Zahlen:

- (a) Berechnen Sie das Minimum der Werte in  $A$ .
- (b) Berechnen Sie den Mittelwert aller Einträge von  $A$ .
- (c) Gegeben sei eine feste Schranke  $x$ . Bestimmen Sie den größten Index  $idx$ , sodass  $\sum_{j=0}^{idx} A[j] \leq x$  gilt. Falls ein solcher Index  $idx$  zur gegebenen Schranke  $x$  nicht existiert, setzen Sie  $idx = -1$ .

Befolgen Sie für jedes dieser Probleme diese zwei Schritte:

- Formulieren Sie einen Algorithmus, der das Problem löst. Beschreiben Sie Ihren Algorithmus kurz und stellen Sie ihn in Pseudocode dar.
- Bestimmen Sie eine geeignete Schleifeninvariante und benutzen Sie diese, um die Korrektheit Ihres Algorithmus zu beweisen.

---

## P3 (Insertion-Sort)

---

- (a) In der Vorlesung haben Sie den Algorithmus InsertionSort kennengelernt, der die Elemente einer Liste in aufsteigender Reihenfolge sortiert. Schreiben Sie InsertionSort so um, dass der resultierende Algorithmus die Elemente in absteigender Reihenfolge sortiert, und begründen Sie Ihre Angabe. Beachten Sie, dass der neue Algorithmus weiterhin stabil sein soll.
- (b) Sortieren Sie mithilfe dieses Algorithmus das folgende Array von Strings nach ihrer Länge:

auf	Baum	Daten	Landesbibliothek	Haus	sortieren
-----	------	-------	------------------	------	-----------

Geben Sie dabei auch alle Zwischenschritte an, jeweils vor jedem Durchlauf der äußeren Schleife.

---

## P4 (Eigenschaften von Algorithmen)

---

Beschreiben Sie, für jeden der beiden Algorithmen unten, was dieser berechnet, und überprüfen Sie, welche Eigenschaften (Determiniertheit, Determinismus, Terminierung, Korrektheit, Effizienz) er erfüllt. Hierbei sind  $A$  ein Array ganzer Zahlen und  $n$  eine ganze Zahl.

Algorithm1( $A$ ):

```
11: len = length( $A$ )
12: while true do
13:   srtd = true
14:   for i = 0 to len - 2 do
15:     if  $A[i] < A[i + 1]$  then
16:       srtd = false
17:     if srtd = true then
18:       return  $A$ 
           // Waehle  $n_0, n_1$  zufaellig
           // mit  $0 \leq n_0, n_1 \leq len - 1$ 
19:    $n_1, n_2 \leftarrow \{0, \dots, len - 1\}$ 
20:   tmp =  $A[n_1]$ 
21:    $A[n_1] = A[n_2]$ 
22:    $A[n_2] = tmp$ 
```

Algorithm2( $n$ ):

```
31: if  $n \bmod 2 = 0$  then
32:   return false
33: i = 3
34: while i < n do
35:   if  $n \bmod i = 0$  then
36:     return false
37:   i = i + 2
38: return true
```

---

## P5\* (Türme von Hanoi)

---

Die *Türme von Hanoi* sind ein bekanntes Geduldspiel, dessen Regeln hier nochmal kurz erklärt werden.

Das Spiel besteht aus drei Stäben. Auf die Stäbe wird eine feste Anzahl  $n$  gelochter Scheiben gelegt, alle unterschiedlichen Größen. Zu Beginn liegen alle Scheiben auf einem Stab, der Größe nach geordnet, mit der größten Scheibe ganz unten. Ziel des Spiels ist es, alle Scheiben vom Ausgangsstab auf einen anderen Stab zu versetzen. Dabei müssen folgende Regeln befolgt werden:

- In jedem Spielzug darf immer nur eine Scheibe bewegt und auf einen anderen Stab gelegt werden;
- Während des gesamten Spieles darf niemals eine größere Scheibe über einer kleineren Scheibe liegen.

Als Beispiel finden Sie in der Abbildung unten zwei erlaubte (links) und zwei regelwidrige (rechts) Zustände, bei  $n = 4$  Scheiben:



- Geben Sie einen rekursiven Algorithmus an, der dieses Spiel löst, und berechnen Sie dessen Laufzeit. Begründen Sie Ihre Angaben.
- Zeigen Sie, dass Ihr Algorithmus "optimal" ist: Es gibt keinen korrekten Algorithmus, der es ermöglicht das Spiel in weniger Schritten zu lösen. (Falls dies nicht der Fall sein sollte, revidieren Sie Ihren Algorithmus aus (a).)
- Einer Legende zufolge gibt es tief im Dschungel in Südostasien, irgendwo bei Hanoi, einen Brahma-Tempel, in dem Mönche dieses Spiel seit uralten Zeiten mit 64 Scheiben aus purem Gold spielen. Die Legende besagt, dass die Welt in Schutt und Asche fallen wird, sobald die Mönche mit dem Spiel fertig sind. Angenommen, die Mönche verschieben eine Scheibe pro Sekunde und sie haben mit dem Spiel am Anfang der Zeit begonnen<sup>1</sup>, müssen wir uns über den "Weltuntergang durch die Türme von Hanoi" Gedanken machen?

<sup>1</sup>Unser Universum ist ca. 13,8 Milliarden Jahre alt.

---

## Hausübungen

---

In diesem Bereich finden Sie L<sup>A</sup>T<sub>E</sub>X-Hausübung von Blatt 1. Bitte beachten Sie, dass die Hausübung auf diesem Blatt nicht abgegeben und bewertet wird, und damit auch nicht Teil der Studienleistung ist.

---

<b>H1 (Dokumente schreiben)</b>	<b>(0 Punkte)</b>
---------------------------------	-------------------

---

Versuchen Sie, das beiliegende Dokument AuD20\_Dokument.pdf in L<sup>A</sup>T<sub>E</sub>X zu erstellen.

---

<b>H2 (Zeichnen)</b>	<b>(0 Punkte)</b>
----------------------	-------------------

---

Versuchen Sie, die Bäume im beiliegenden Dokument AuD20\_Baum.pdf in L<sup>A</sup>T<sub>E</sub>X zu erstellen.