Diskrete Mathematik
Wintersemester 2012/2013

Steffen Reith
Steffen.Reith@hs-rm.de

Hochschule RheinMain

10. Oktober 2012

Termine

Vorlesung:

Mittwoch 14^{15} - 15^{45} im Hörsaal UDE-D11

Übung:

Mittwoch 16^{00} - 17^{30} im Hörsaal UDE-D11

Bemerkung:
Die Übung am 17.10.2012 fällt aus. Es wird ein Übungsblatt und (später) eine Musterlösung geben.

Über den Dozenten

- Prof. Dr. Steffen Reith, geboren 1968, verheiratet
- Seit Sommersemester 2006 an der FH Wiesbaden
- Vorher tätig als Softwareentwickler für kryptographische und mathematische Algorithmen für tief eingebettete System in KFZs.
- Spezialgebiete: Komplexitätstheorie, Logik in der Informatik und Kryptographie (Computational Number Theory)
- Masterarbeiten: Kryptographie, Kryptographie für eingebettete Systeme, paralleles Rechnen, Komplexitätstheorie, Logik in der Informatik

EMail:
`Steffen.Reith@hs-rm.de`

Büro:
Raum C202

Weitere Informationen zur Vorlesung

Webseite: `http://www.cs.hs-rm.de/~reith`

Literatur:

- Werner Struckmann und Dietmar Wätjen, Mathematik für Informatiker - Grundlagen und Anwendungen, Spektrum Akademischer Verlag, 2007
- Rod Haggarty, Diskrete Mathematik für Informatiker, Pearson Studium, 2004
- Christoph Meinel und Martin Mundhenk, Mathematische Grundlagen der Informatik, Teubner, 2006
- Ronald L. Graham, Donald E. Knuth und Oren Patashnik, Concrete Mathematics - A Foundation for Computer Science, Addison-Wesley, 1994

Weitere Informationen zur Vorlesung (II)

Ersatztermine:
Werden Dienstags stattfinden

Skript:
Wird in unregelmäßigen Abständen auf der Webseite der Vorlesung veröffentlicht (muss noch erstellt/verbessert werden).

Folien:
Einzelne (kleine) Teile der Vorlesung werden in Folienform zur Verfügung stehen. Folien die vom Skript abweichen, werden auf der Webseite (nachträglich) zur Verfügung stehen.

Eine eigene Mitschrift sollte *angefertigt* werden!

Ein roter Faden

In der Vorlesung werden die folgenden Themen untersucht:

1. Einleitung - Einige Beispiele (Überabzählbarkeit)
2. Zählen
3. Permutationen, Zyklendarstellung, Satz von Cayley
4. Algebraische Strukturen und elementare Gruppentheorie
5. Elementare Zahlentheorie, Konkruenzen
6. Umwandlung rekursiver in explizite Gleichungen

Spielregeln

- *Rechner* und Handys sind zu Beginn der Veranstaltung *aus*
- Wir (Dozent + Hörer) sind *pünktlich*
- Es *redet nur eine Person*
- Bei Fragen und Problemen *sofort melden / fragen*
- Es wird Eigeninitiative und selbstständiges Arbeiten erwartet
- Eine Vorlesung ist keine (wöchentliche) Fernsehserie
  - Eine Vorlesung wird von *den Hörern* und vom Dozenten *gestaltet*
  - aktive Mitarbeit erwünscht und erforderlich
  - Der Dozent will motiviert werden
  - Umfangreiche Vor- und Nachbereitung notwendig
  - Lernen kurz vor der Klausur ist tötlich! (kontinuierliches Lernen)
- Vergessen Sie den (angeblichen) Konflikt von Theorie und Praxis

Was wünschen Sie sich?

Diskrete Mathematik - Einleitung

Informatik ist die Wissenschaft der (systematischen) Verarbeitung von Informationen.
Für ein tieferes Verständnis von Soft- und Hardwareentwicklung und dem Design von Algorithmen spielen

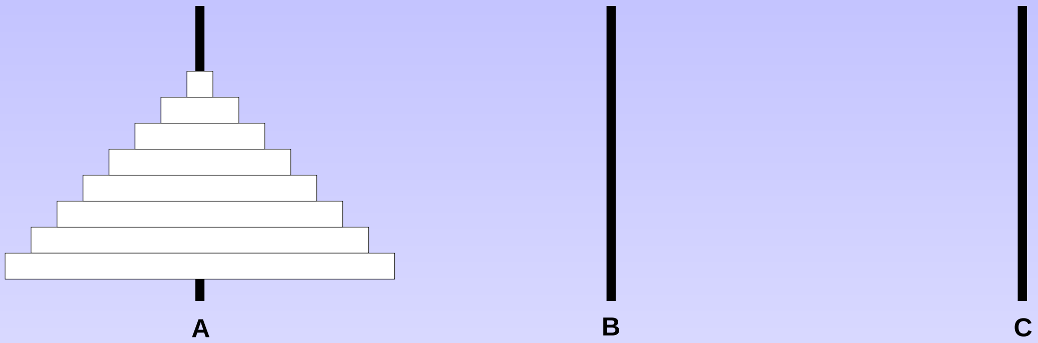
- mathematische Methoden (z.B. Induktion) und
- formale Beschreibungen und Modelle eine große Rolle.

Die meisten diese Begriffe beschäftigen sich mathematischen Strukturen, die abzählbar unendlich oder endlich sind.
Zur diskreten Mathematik gehören (Teile) der:

- Mathematische Logik
- Mengentheorie
- Graphentheorie
- Kombinatorik
- Zahlentheorie
- Kodierungstheorie
- Kryptographie

Ein Beispiel

Die „Türme von Hanoi“ (nach Edouard Lucas, 1883): Gegeben ist ein Turm mit acht Scheiben auf drei Stäben:



Aufgabe: Bewege die Scheiben von A nach C, wobei nie eine größere über einer kleineren Scheibe liegen darf.

Die Türme von Hanoi

Angeblich gibt es eine Legende:

Es gibt einen Turm mit 64 *Scheiben aus Gold, die auf Stäben aus Diamant ruhen*

Priester bewegen jeden Tag eine Scheibe nach folgenden Schema:

„Wenn Du den Turm der Höhe n von X über Y nach Z bewegen sollst, dann

- *gib Deinem ältesten Lehrling den Auftrag einen Turm der Höhe $n - 1$ von X über Z nach Y zu bewegen,*
- *verschiebe die letzte Scheibe von X nach Z und*
- *gib Deinem ältesten Lehrling den Auftrag einen Turm der Höhe $n - 1$ von Y über X nach Z zu bewegen.“*

Ist die Arbeit vollständig getan, dann geht die Welt unter.

Wie lange haben wir noch zu leben?

Idee: Analysiere das Problem allgemein für n Scheiben und ermittle wieviele Bewegungen notwendig sind.

Idee: Probiere für kleine n die Anzahl der Scheibenbewegungen einfach aus.

Abkürzung: $[n, \mathrm{X}, \mathrm{Y}, \mathrm{Z}]$ bedeutet „bewege einen Turm der Höhe n von X über Y nach Z.

n	# Bewegungen
n = 0	0
n = 1	1
n = 2	3
n = 3	7

Sei $T : \mathbb{N} \to \mathbb{N}$, dann ist $T(n)$ die Anzahl der notwendigen Bewegungen bei einer Turmhöhe von n.

Anzahl der Scheibenbewegungen

Klar: $T(0) = 0$, $T(1) = 1$, $T(2) \leq 3$ und $T(3) \leq 7$.
Mit der „Arbeitsbeschreibung“ ergibt sich:

$$T(n) \leq 2\,\underbrace{T(n-1)}_{\text{“Lehrling“}} + 1, \; n > 0$$

Unklar: $T(n) \stackrel{?}{=} 2T(n-1) + 1$ (bessere Strategie?)
Aber es sind mindestens

- eine Scheibenbewegung durch den Meister
- und zweimal $T(n-1)$ Bewegungen durch den Lehrling notwendig.

Also gilt

$$T(n) = 2T(n-1) + 1 \text{(„Rekurrenzgleichung“)}.$$

Test: T(3) = 2 T(2) + 1 = 4 T(1) + 3 = 8 T(0) + 7

Anzahl der Scheibenbewegungen (II)

Theorem

Die Türme von Hanoi mit n Scheiben benötigen $T(n) = 2^n - 1$ Bewegungen zur Lösung.

Induktion über *n*.

(IA) Wenn $n = 0$, dann $T(0) = 2^0 - 1 = 0$
(IV) $T(n) = 2^n - 1$
(IS) $n \to n + 1$:

$$\begin{aligned} T(n+1) &= 2 \cdot T(n) + 1 \\ &\overset{\textbf{(IV)}}{=} 2 \cdot (2^n - 1) + 1 \\ &= 2 \cdot 2^n - 1 \end{aligned}$$

$\square$

Fazit

Die Welt geht also in

$$\begin{aligned} 2^{64} + 1 \text{ Tagen} &\approx 1.84 \cdot 10^{19} \text{ Tagen} \\ &\approx 5.05 \cdot 10^{16} \text{ Jahren} \end{aligned}$$

unter.

Wir haben noch genug Zeit für die Vorlesung!