Informatik III

Albert-Ludwigs-Universität Freiburg
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer

Christian Schindelhauer
Wintersemester 2006/07
19. Vorlesung
11.01.2007

Komplexitätstheorie - Zeitklassen

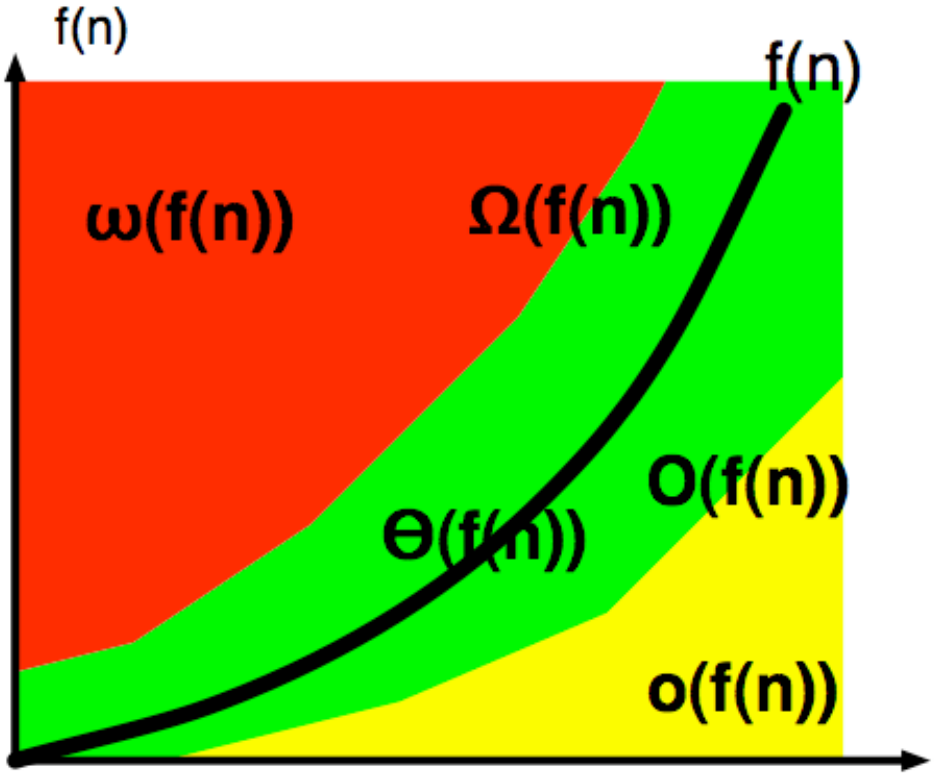
Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer

- **Die Komplexitätsklassen TIME**
  - DTIME, NTIME
  - P
  - NP
- **Das Cook-Levin-Theorem**
  - Polynomial-Zeit-Reduktion
  - Reduktionen zwischen 3SAT und Clique
  - NP-vollständigkeit
  - SAT ist NP-vollständig
- **Weitere NP-vollständige Probleme**
  - Knotenüberdeckung (Vertex-Cover)
  - Das Hamiltonsche Pfadproblem
  - Das ungerichtete Hamiltonsche Pfadproblem
  - Das Teilsummenproblem

Die asymptotischen Wachstumsklassen

Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer

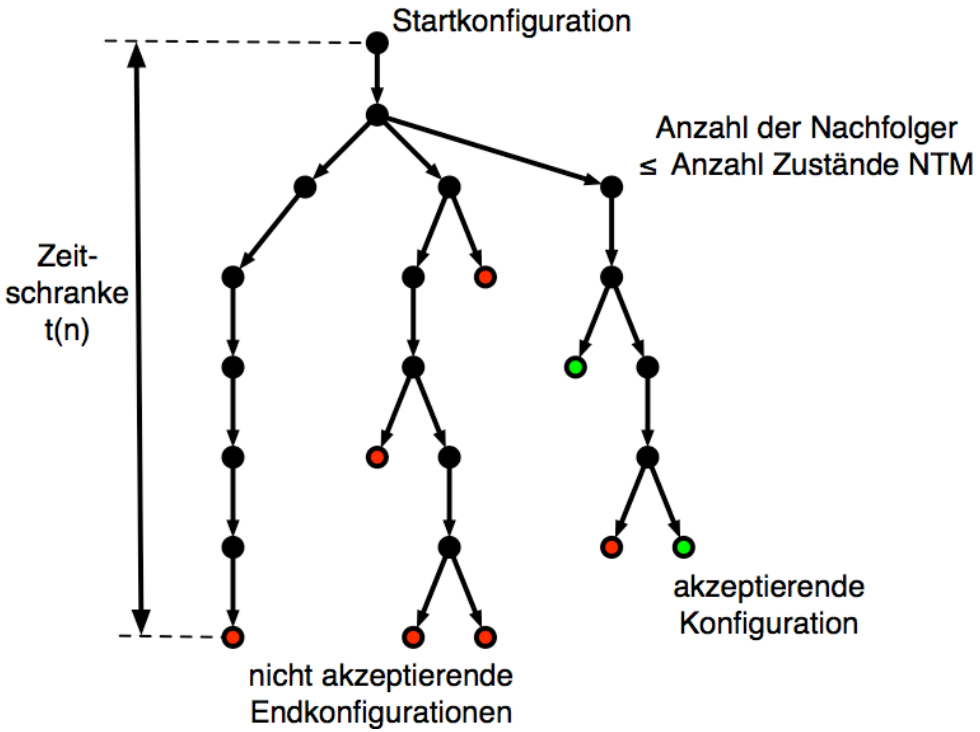
$$
\begin{aligned}
O(g) &:= \{f \mid \exists k \in \mathbb{R} \quad f \leq_{ae} k \cdot g\}, \\
o(g) &:= \{f \mid \forall k \in \mathbb{R}^+ \quad k \cdot f \leq_{ae} g\}, \\
\omega(g) &:= \{f \mid \forall k \in \mathbb{R}^+ \quad k \cdot g \leq_{ae} f\}, \\
\Omega(g) &:= \{f \mid \exists k \in \mathbb{R} \quad g \leq_{ae} k \cdot f\}, \\
\Theta(g) &:= O(g) \quad \cap \quad \Omega(g).
\end{aligned}
$$



Nichtdeterministische Zeitkomplexitätsklassen

Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer

- **Definition**
  - Eine NTM ist t-Zeit-beschränkt, wenn für eine Eingabe der Länge n jede nichtdeterministische Berechnung höchstens t(n) Schritte benötigt.
- **Definition**
  - Sei $t:N \rightarrow R^+$ eine Funktion.
  - Die Zeitkomplexitätsklasse **NTIME(t(n))** ist die Menge aller Sprachen,
    - die von einer **nicht**deterministischen O(t(n))-Zeit-Turing-Maschine entschieden werden.
  - Wird die Anzahl der Bänder auf k beschränkt, schreiben wir **$NTIME_{k\text{-}Band}(t(n))$** oder einfach **$NTIME_k(t(n))$.**



DTM versus NTM, k versus k' Bänder

Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer

- **Theorem: Für $k,k' \geq 1$, $t(n) = \Omega(n)$**

  - **$TIME_k(t(n)) \subseteq TIME_{k'}(t(n)^2)$**
    - Jede Berechnung einer t-Zeit-k-Band-DTM kann von einer $O(t(n)^2)$-Zeit-k'-Band-DTM berechnet werden.

  - **$NTIME_k(t(n)) \subseteq NTIME_{k'}(t(n)^2)$**
    - Jede Berechnung einer t-Zeit-k-Band-NTM kann von einer $O(t(n)^2)$-Zeit-k'-Band-NTM berechnet werden.

  - **$NTIME_k(t(n)) \subseteq TIME_{k'}(2^{O(t(n))})$**
    - Jede Berechnung einer t-Zeit-k-Band-NTM kann von einer $2^{O(t(n))}$-Zeit-k'-Band-DTM berechnet werden.

Zwei wichtige Komplexitätsklassen

Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer

P & NP

Zwei wichtige Komplexitätsklassen

Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer

- **Definition:**
  - $\mathrm{P} = \bigcup_k \mathrm{TIME}(n^k)$
  - $\mathrm{NP} = \bigcup_k \mathrm{NTIME}(n^k)$
- **Noch mal:**
  - P: Klasse aller Sprachen, die von einer Polynom-Zeit DTM entschieden werden
  - NP: Klasse aller Sprachen, die von einer Polynom-Zeit NTM entschieden werden können.

NP und P

Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer

- **Definition:**

$$\mathrm{NP} = \bigcup_k \mathrm{NTIME}(n^k)$$

- **Theorem**

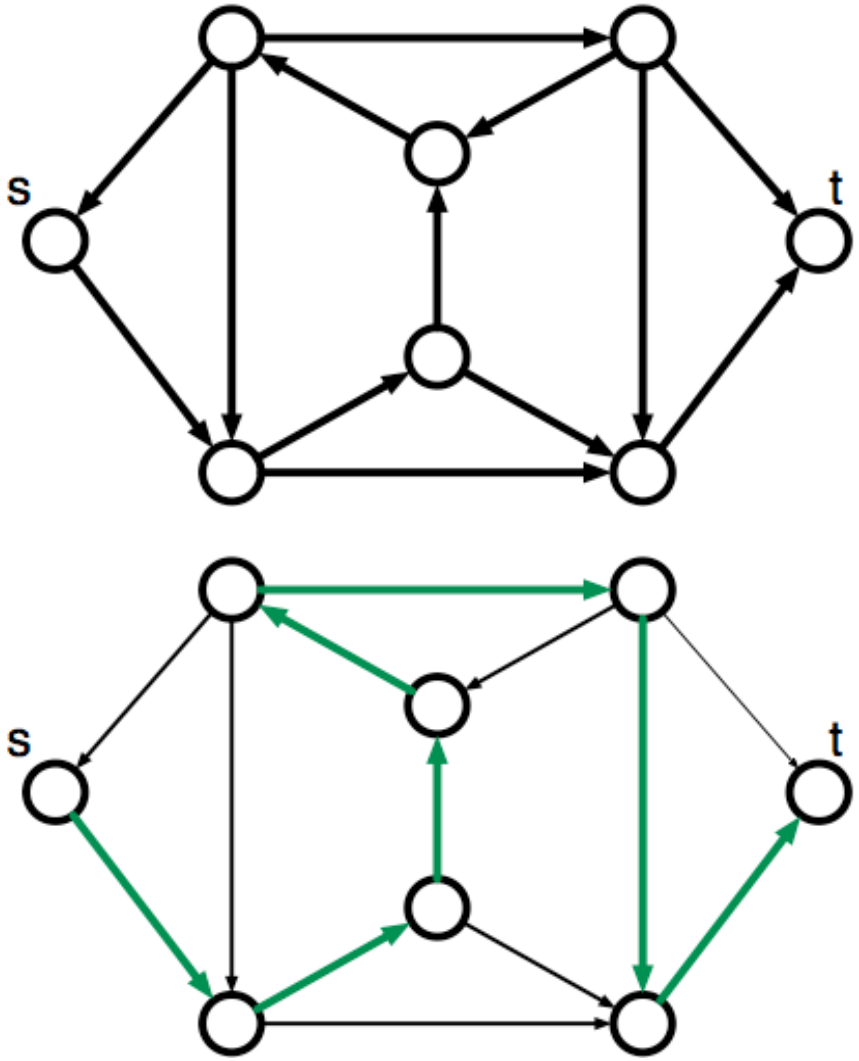
$$\mathrm{P} \subseteq \mathrm{NP}$$

- **Alles was in P ist, ist auch in NP**

Hamiltonsche Pfade

Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer

- **Definition:** *HAMPATH*
  - Das Hamiltonsche Pfadproblem
    - Geg.:
      - ein gerichteter Graph
      - Zwei Knoten s,t
    - Ges.: existiert ein Hamitonscher Pfad von s nach t
      - d.h. ein gerichteter Pfad, der alle Knoten besucht, aber keine Kante zweimal benutzt
- **Algorithmus für Hamiltonscher Pfad:**
  - Rate eine Permutation $(s,v_1,v_2,...,v_{n-2},t)$
  - Teste, ob Permutation ein Pfad ist
    - falls ja, akzeptiere
    - falls nein, verwerfe
- **Also: HamPath ∈ NP**



Die Nicht-Primzahlen

Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer

- **Definition:** *COMPOSITES*
  - Geg.: x (als Binärzahl)
  - Ges.: Gibt es ganze Zahlen p,q>1
    - so dass x = p q

COMPOSITES
:= {x | x = p q, für ganze Zahlen p,q>1}

- **NTM für** *COMPOSITES* **:**
  - Rate p,q>1
  - Berechne p q
  - Akzeptiere, falls p q = x
  - Verwerfe sonst

- **Also ist** *COMPOSITES* ∈ **NP**

Raum für eigene Notizen

Der Verifizierer

Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer

- **Definition**
  - Ein **Verifizierer** für eine Sprache A ist eine DTM V, wobei
    - A = {w | V akzeptiert <w,c> für ein Wort c}
  - Ein **Polynom-Zeit-Verifizierer** hat eine Laufzeit die durch ein Polynom $|w|^k$ beschränkt ist.
  - Eine Sprache ist in **Polynom-Zeit verifizierbar**, falls sie einen Polynom-Zeit-Verifizierer hat.

- **Theorem**
  - NP beschreibt genau die Sprachen, die in Polynom-Zeit verifiziert werden können.

Verifizierbare Sprachen sind in NP

Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer

- Ein Polynom-Zeit-Verifizierer für eine Sprache A ist eine DTM V, wobei
  - A = {w | V akzeptiert <w,c> für ein Wort c}
  - und V mit Polynom-Laufzeit $O(|w|^k)$ beschränkt ist.

- **Theorem**
  - NP beschreibt genau die die Sprachen, die in Polynom-Zeit verifiziert werden können.
- **Beweis:**
  - 1. Teil: Die Sprachen, die in Polynom-Zeit verifiziert werden können, sind in NP.

- **Konstruiere NTM M die A in Polynom-Zeit akzeptiert:**

- **M = "Auf Eingabe w,**
  - Rate ein Wort c der Länge $\leq |w|^k$
  - Führe Berechnung von V auf Eingabe <w,c> durch
  - Akzeptiere, wenn V akzeptiert"
- **M akzeptiert genau die Worte in A**
  - da V nur Worte <w,c> der Länge $|w|^k$ bearbeiten kann, wird auch das relevante Wort c berücksichtigt, wenn V auf <w,c> akzeptiert.
- **M rechnet in Polynom-Zeit:**
  - Laufzeit für Raten $\leq |w|^k$
  - Laufzeit für Verifizieren $\leq |w|^k$

Alle Sprachen in NP sind verifizierbar

Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer

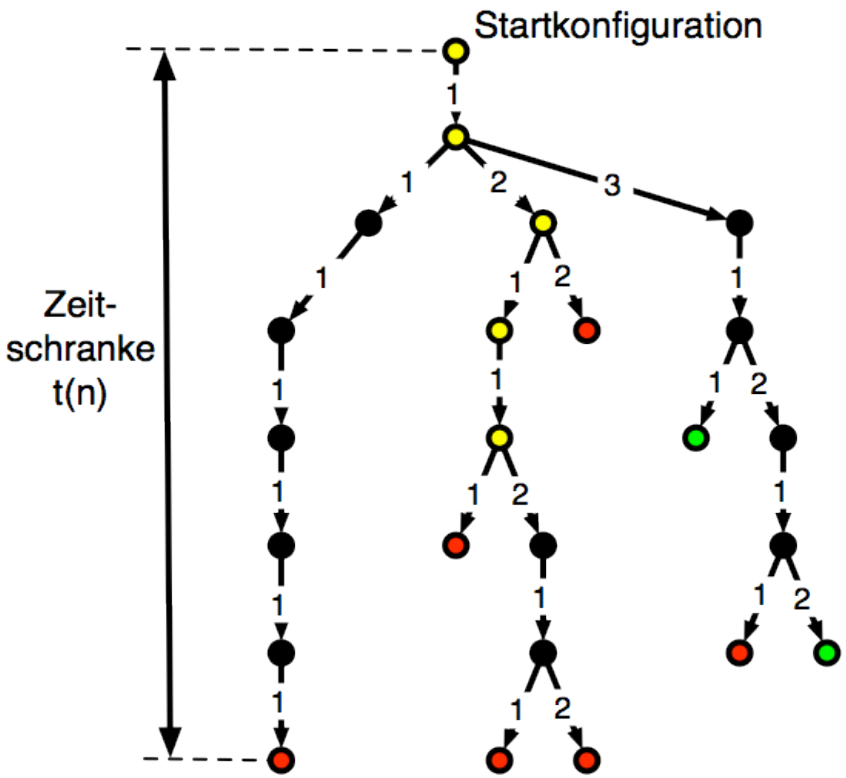
- Ein Polynom-Zeit-Verifizierer für eine Sprache A ist eine DTM V, wobei
  - A = {w | V akzeptiert <w,c> für ein Wort c}
  - und V mit Polynom-Laufzeit $O(|w|^k)$ beschränkt ist.

- **Theorem**
  - NP beschreibt genau die die Sprachen, die in Polynom-Zeit verifiziert werden können.
- **Beweis:**
  - 2. Teil: Die Sprachen in NP können in Polynom-Zeit verifiziert werden

- **Gegeben:**
  - NTM M mit Polynom-Laufteit $|w|^k$
  - Konstruiere Polynom-Zeit-Verifizierer
- **Beschreibe c den Pfad eines Berechnungsbaums von M**
- **V = “Auf Eingabe <w,c>,**
  - Führe Berechnung von M auf Eingabe w durch
  - Falls M in Schritt t nichtdeterministisch verzweigt, gibt der Buchstabe c_t an, welcher Folgezustand von A genommen wird.
  - Akzeptiere, wenn M akzeptiert”
- **V verifiziert genau die Worte in L(M)**
  - da M nur $|w|^k$ Schritte rechnen kann, kann auch der Berechnungspfad beschrieben von c von V eingelesen werden, für den M auf w akzeptert (wenn M jemals akzeptiert)
- **V rechnet in Polynom-Zeit:**
  - da M in Polynom-Zeit rechnet

Alle Sprachen in NP sind verifizierbar

Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer



- **Gegeben:**
  - NTM M mit Polynom-Laufteit $|w|^k$
  - Konstruiere Polynom-Zeit-Verifizierer
- **Beschreibe c den Pfad eines Berechnungsbaums von M**
- **V = "Auf Eingabe <w,c>,**
  - Führe Berechnung von M auf Eingabe w durch
  - Falls M in Schritt t nichtdeterministisch verzweigt, gibt der Buchstabe c_t an, welcher Folgezustand von A genommen wird.
  - Akzeptiere, wenn M akzeptiert"
- **V verifiziert genau die Worte in L(M)**
  - da M nur $|w|^k$ Schritte rechnen kann, kann auch der Berechnungspfad beschrieben von c von V eingelesen werden, für den M auf w akzeptert (wenn M jemals akzeptiert)
- **V rechnet in Polynom-Zeit:**
  - da M in Polynom-Zeit rechnet

Das Teilsummenproblem (Subset-Sum-Problem)

Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer

- **Definition SUBSET-SUM:**
  - Gegeben:
    - Menge von natürlichen Zahlen $S = \{x_1,..., x_k\}$
    - Eine natürliche Zahl t
  - Gesucht:
    - Gibt es eine Teilmenge $\{y_1,...,y_m\} \subseteq \{x_1,..., x_k\}$ so dass $\sum_{i=1}^{m} y_i = t$
- **Theorem**
  - Das Teilsummenproblem ist in NP
- **Beweis**
  - Betrachte
    $A=\{<x_1,..., x_k,t> \mid$ es gibt $\{y_1,...,y_m\} \subseteq \{x_1,..., x_k\}$ und $\sum_{i=1}^{m} y_i = t$
  - Verifizierer testet, ob die Teilmengenbeziehung gilt und ob die Summe der Teilmenge t entspricht
  - Laufzeit: O(n log n)

Ende der 19. Vorlesung

Albert-Ludwigs-Universität Freiburg
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer

Christian Schindelhauer

Wintersemester 2006/07

19. Vorlesung

11.01.2007