Vorlesung Kap. 7

# Automatentheorie und Formale Sprachen – LV 4110 –

Kapitel 7

Lernziele

- Effizienz und Laufzeit von Programmen
- Herausstellen von Komplexitätsklassen
- Laufzeitkomplexität und Problemgröße
- Definitionen der Klassen P und NP
- Erläuterung und Einordnung des Knapsack-Problems
- Definition und Interpretation der NP-Vollständigkeit
- Erläuterung und Einordnung des Erfüllbarkeitsproblems (SAT)
- Lösungsalgorithmen für NP-harte Probleme

Kapitel 7 Gliederung

- 1. Intension in diesem Kapitel
- 2. Herausstellen von Komplexitätsklassen
- 3. Laufzeitkomplexität und O-Notation
- 4. Definitionen der Klassen P und NP
- 5. Erläuterung und Einordnung des Knapsack-Problems
- 6. NP-Vollständigkeit
- 7. Das Erfüllbarkeitsproblem (SAT und 3SAT)
- 8. NP-harte Probleme
- 9. Problemstellung der PARTITION

Kapitel 7 Gliederung

- 1. Intension in diesem Kapitel
- 2. Herausstellen von Komplexitätsklassen
- 3. Laufzeitkomplexität und O-Notation
- 4. Definitionen der Klassen P und NP
- 5. Erläuterung und Einordnung des Knapsack-Problems
- 6. NP-Vollständigkeit
- 7. Das Erfüllbarkeitsproblem (SAT und 3SAT)
- 8. NP-harte Probleme
- 9. Problemstellung der PARTITION

# Gibt es einen Effizienzgewinn beim Übergang zu "mächtigeren" Rechenmodellen als TM oder RAM bzw.

wie effizient kann ein Problem grundsätzlich gelöst werden ?

Kapitel 7 Gliederung

- 1. Intension in diesem Kapitel
- 2. Herausstellen von Komplexitätsklassen
- 3. Laufzeitkomplexität und O-Notation
- 4. Definitionen der Klassen P und NP
- 5. Erläuterung und Einordnung des Knapsack-Problems
- 6. NP-Vollständigkeit
- 7. Das Erfüllbarkeitsproblem (SAT und 3SAT)
- 8. NP-harte Probleme
- 9. Problemstellung der PARTITION

# Hintergründe:

- Wir haben Entscheidungsprobleme, Berechenbarkeitsprobleme, Approximationsprobleme, Erfüllbarkeitsprobleme, Aufzählungsprobleme, Suchprobleme bis hin zu Optimierungsproblemen zu lösen.
- Dazu stehen uns Erkennungsprozeduren, Such- und Findeprozeduren, Prüf- und Entscheidungsprozeduren sowie Verarbeitungsprozeduren zur Verfügung.
- In diesem Zusammenhang interessieren wir uns im allgemeinen für die Laufzeit von Algorithmen (Berechnungen) bzw. für die "Größe" von Problemen.

# Fragestellungen:

- In welchem Zusammenhang stehen Sprachen und Probleme? Gibt es überhaupt einen Zusammenhang?
- Gibt es eine Korrespondenz zwischen Entscheidungs-, Berechenbarkeits- und Optimierungsproblemen?
- Gibt es womöglich unterschiedliche Problemklassen?
- Gibt es für jedes Problem einen Lösungsalgorithmus bzw. existiert zu jedem Problem überhaupt eine Lösung?
- Gibt es ein Beweissystem (z. B. aus Axiomen und Schlussregeln), mit dem man feststellen kann, ob ein Problem algorithmisch (un)lösbar ist?

Hinter diesen Fragestellungen verbirgt sich eine der wichtigsten offenen Fragen der theoretischen Informatik:

Ist P≠NP?

# Mit anderen Worten:

- Besitzen deterministische Turing-Maschinen eine andere
   Zeitkomplexität als nicht deterministische Turing-Maschinen?
- Erzielen nicht deterministische Turing-Maschinen eine höhere Aussagekraft als deterministische Turing-Maschinen?

Kapitel 7 Gliederung

- 1. Intension in diesem Kapitel
- 2. Herausstellen von Komplexitätsklassen
- 3. Laufzeitkomplexität und O-Notation
- 4. Definitionen der Klassen P und NP
- 5. Erläuterung und Einordnung des Knapsack-Problems
- 6. NP-Vollständigkeit
- 7. Das Erfüllbarkeitsproblem (SAT und 3SAT)
- 8. NP-harte Probleme
- 9. Problemstellung der PARTITION

# Hintergrund:

Ziel ist es, einen möglichst **effizienten Algorithmus** für ein bestimmtes Problem zu finden.

# <u>Definition</u> (Rechenzeit):

Sei **TM** eine deterministische Turingmaschine auf dem Eingabealphabet  $\Sigma$ . Dann ist die worst case Rechenzeit  $t_{TM}(n)$  die maximale Anzahl von Rechenschritten, die **TM** auf Eingaben aus  $\Sigma^n$  macht.

# <u>Definition</u> (Zeitkomplexitätsfunktion $T_{TM}(n) : IN \rightarrow IN$ ):

 $T_{TM}(n) = max{m}$ , so dass eine deterministische Turing-Maschine **TM** bei Eingabe  $\mathbf{x} \in \Sigma^n$  **m** Berechnungsschritte (Übergänge) benötigt, bis ein Endzustand erreicht wird.

# <u>Definition (O-Notation)</u>:

Für eine Funktion f : IN  $\rightarrow$  IN definieren wir

$$f(n) = O(g(n)) = \{ f : IN \rightarrow IN \mid \exists c, n_0 : \forall n \ge n_0 : f(n) \le c \cdot g(n) \}$$

und können so die Laufzeitfunktion f(n) durch eine asymptotische obere Schranke g(n) begrenzen  $\Rightarrow$  in Worten: f(n) wächst nicht schneller als g(n)

Die **Komplexität** eines Algorithmus ist O(g(n)), wenn die Laufzeit  $T_{TM}(n)$  in O(g(n)) ist, beispielsweise geschrieben als:  $f(n) = 2 \cdot n^2 + 4 \cdot n \in O(n^2)$ 

Dabei bezeichnen:

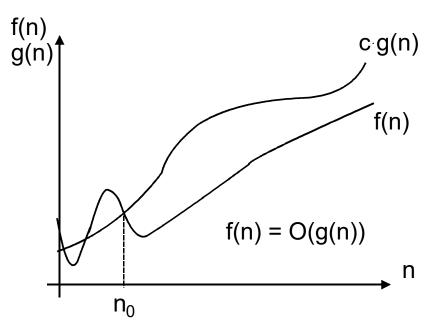
f(n), g(n) Zeitkomplexitätsfunktionen (positiv)

n Eingabelänge

c, n<sub>0</sub> positive Konstanten

# Algorithmen

# Verläufe und Beispiele:



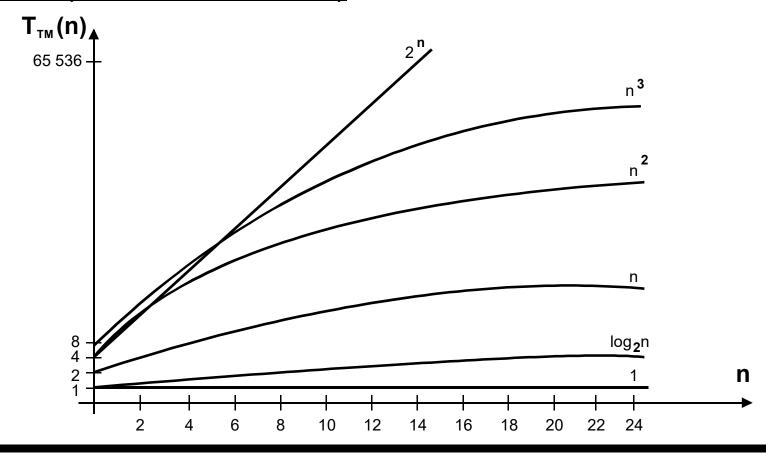
# Fehlerterm bei der Approximation:

 $e^{x} = 1 + x + x^{2} / 2 + O(x^{3})$  für  $\forall x \rightarrow 0$  drückt aus, dass die vernachlässigten Summanden höherer Ordnung kleiner sind als der konstante Wert  $x^{3}$ , wenn x nur klein genug ist.

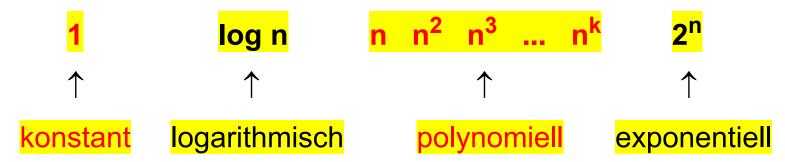
# **CPU Time eines Algorithmus:**

$$T_{TM}(n) = f(n) = 10 \log(n) + 5 (\log(n))^3$$
  
+ 7 n + 3 n<sup>2</sup> + 6 n<sup>3</sup>  
 $\Rightarrow f(n) = O(n^3)$ 

# Verläufe (Wachstumsraten):



Ein Beispiel für die Größenordnung bzw. Hierarchie ist die folgende Anordnung:



# Satz:

Sei **k** eine Konstante und **p** ein Polynom. Ein Algorithmus ist **polynomiell**, wenn seine Zeitkomplexität  $T_{TM}(n) \in O(n^k)$  ist. Ein Algorithmus ist dagegen **exponentiell**, wenn seine Laufzeit  $T_{TM}(n) \in O(2^{p(n)})$  ist.

Kapitel 7 Gliederung

- 1. Intension in diesem Kapitel
- 2. Herausstellen von Komplexitätsklassen
- 3. Laufzeitkomplexität und O-Notation
- 4. Definitionen der Klassen P und NP
- 5. Erläuterung und Einordnung des Knapsack-Problems
- 6. NP-Vollständigkeit
- 7. Das Erfüllbarkeitsproblem (SAT und 3SAT)
- 8. NP-harte Probleme
- 9. Problemstellung der PARTITION

# <u>Definition</u> (Klasse P):

P ist eine Klasse der Probleme, für die es eine deterministische Turingmaschine TM gibt, deren worst case Rechenzeit t™(n) polynomiell beschränkt ist, d. h. es existiert ein Polynom p mit

$$T_{TM}(n) \leq p(n)$$

# <u>Definition</u> (Klasse NP):

**NP** (nicht deterministisch polynomiell) ist die Klasse der Entscheidungsprobleme, für die es eine nicht deterministische Turingmaschine **NTM** gibt, deren worst case Rechenzeit **t**<sub>NTM</sub>(**n**) polynomiell beschränkt ist, d. h.

$$T_{NTM}(n) \leq p(n)$$

Das Entscheidungsproblem **PRIMES** besteht darin, zu entscheiden, ob es sich bei einer gegebenen natürlichen Zahl z > 1 um eine Primzahl handelt. Dabei sei die Zahl z zur Basis  $b \in IN$  dargestellt.

Die dazugehörige Sprache sei mit  $L_b = L[PRIMES, b]$  bezeichnet.

# Satz:

Sei L<sub>1</sub> := L[PRIMES, 1]. Erst 2002<sup>1)</sup> konnte gezeigt werden, dass gilt:

# L<sub>1</sub> liegt in P

- d. h. es gibt eine DTM, deren Laufzeit von der Ordnung **O(n³)** und damit polynomial beschränkt ist.
  - 1) Drei indische Mathematiker: M. Agrawal, N. Kayal und N. Saxena

Ein bedeutender Algorithmus ist der **Euklidische Algorithmus** zur Berechnung des größten gemeinsamen Teilers (kurz **ggT**(n, m)).

#### Satz:

Der Euklidische Algorithmus zur Berechnung des **ggT** zweier natürlicher Zahlen n und m ist **polynomial** und damit **effektiv berechenbar**.

Genauer gesagt gilt für seine Laufzeit:

$$T(n, m) = O((log_2 n + log_2 m)^2)$$

Liefert ein Entscheidungsalgorithmus zu der Frage, ob n zusammengesetzt (also beispielsweise  $n = p \cdot q$ ) ist, als Beleg der Antwort "JA" einen Faktor q von n, so lässt sich in polynomialer Zeit nachprüfen, ob  $q \mid n$ .

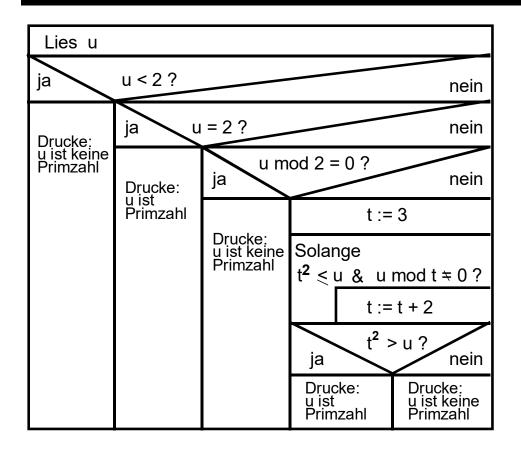
Es gilt nämlich:  $q \mid n \mid gdw \mid (\exists k \in \mathbf{Z}) : n = k \cdot q \iff ggT(q, n) = |q|$ 

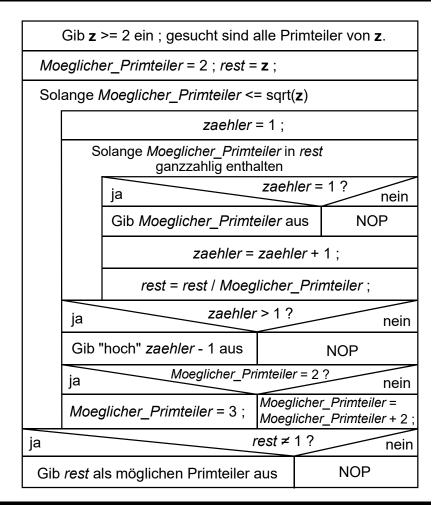
Das **Faktorisierungsproblem** (d. h. die Zerlegung von n in ihre Primfaktoren) ist also in **NP**, aber man weiß <u>nicht</u>, ob es in **P** ist.

#### Satz:

Die Klasse **NP** besteht aus denjenigen Entscheidungsalgorithmen, bei denen es einen Algorithmus gibt, der im Falle einer **JA**-Antwort durch den Algorithmus des Entscheidungsproblems die Korrektheit der Antwort in polynomialer Zeit testet (d. h. Antwort plus Beleg).

Algorithmen Komplexität





Kapitel 7 Gliederung

- 1. Intension in diesem Kapitel
- 2. Herausstellen von Komplexitätsklassen
- 3. Laufzeitkomplexität und O-Notation
- 4. Definitionen der Klassen P und NP
- 5. Erläuterung und Einordnung des Knapsack-Problems
- 6. NP-Vollständigkeit
- 7. Das Erfüllbarkeitsproblem (SAT und 3SAT)
- 8. NP-harte Probleme
- 9. Problemstellung der PARTITION

# <u>Definition</u> (KNAPSACK **KP**):

Gegeben sei ein Rucksack und **n** Objekte mit Gewichten  $g_1, g_2, ..., g_n \in IN$  sowie eine Gewichtsschranke **G**. Zusätzlich seien  $a_1, a_2, ..., a_n \in IN$  die Nutzenwerte für die Objekte. Bei  $x_i = 1$  wird ein Objekt i eingepackt und bei  $x_i = 0$  nicht.

<u>Variante 1</u>: Gibt es zu einem gegebenen Nutzenwert **A** eine Bepackung des Rucksackes, die das Gewichtslimit **G** respektiert und mindestens den Nutzen **A** erreicht?

Also ob:  $a_1 \cdot x_1 + a_2 \cdot x_2 + ... + a_n \cdot x_n \ge \mathbf{A}$ 

unter der Nebenbedingung:  $g_1 \cdot x_1 + g_2 \cdot x_2 + ... + g_n \cdot x_n \leq \mathbf{G}$ 

Variante 2: Berechne den größten erreichbaren Nutzen A!

Variante 3: Berechne eine optimale Bepackung des Rucksackes!

#### Satz:

Die Entscheidungsvarianten 1 bis 3 von KP sind in NP.

# Satz:

Trivialerweise gilt:

$$P \subseteq NP$$

#### Satz:

Für jede Sprache L ∈ **NP** gibt es ein Polynom **p** und eine **deterministische** Turingmaschine **TM**, so dass **TM** die Sprache L in

exponentieller Zeit 2<sup>p(n)</sup> akzeptiert.

Dabei ist:

n = Länge der Eingabesymbole (aus Σ<sup>n</sup>)

Sprachen Knapsack (2)

#### Satz:

# KP ist NP-vollständig<sup>1)</sup>.

1) also mindestens so komplex, wie jedes andere Problem in NP.

#### Algorithmus:

Die Lösung des KP-Problems führt auf die sog. Bellmansche Optimalitätsgleichung.

#### Satz:

Das Rucksack-Problem (KP) kann in der Zeit (→ pseudopolynomiell)

# O(nG)

gelöst werden (n = Anzahl der Objekte, G = Gewichtsschranke).

Kapitel 7
Gliederung

- 1. Intension in diesem Kapitel
- 2. Herausstellen von Komplexitätsklassen
- 3. Laufzeitkomplexität und O-Notation
- 4. Definitionen der Klassen P und NP
- 5. Erläuterung und Einordnung des Knapsack-Problems
- 6. NP-Vollständigkeit
- 7. Das Erfüllbarkeitsproblem (SAT und 3SAT)
- 8. NP-harte Probleme
- 9. Problemstellung der PARTITION

<u>Definition</u> (Polynomiell reduzierbar):

Es seien L<sub>1</sub> und L<sub>2</sub> Sprachen über  $\Sigma_1$  bzw.  $\Sigma_2$ . Dann heißt L<sub>1</sub> polynomiell auf L<sub>2</sub> reduzierbar,

Notation:

L<sub>1</sub> ≤p L<sub>2</sub> (p steht für polynomiell)

wenn es eine polynomielle Transformation von L<sub>1</sub> nach L<sub>2</sub> gibt, d. h. wenn es eine von einer deterministischen Turingmaschine **TM** in polynomieller Zeit **berechenbare** Funktion

$$\mathbf{f}: \Sigma^{*}_{1} \to \Sigma^{*}_{2}$$

gibt, so dass für alle  $w \in \Sigma^{*}_{1}$  gilt:

$$w \in L_1 \Leftrightarrow f(w) \in L_2$$

Seien L<sub>1</sub> die Sprache der ungeraden Zahlen in Dezimaldarstellung über  $\Sigma_1 = \{0, 1, ..., 9\}$  und L<sub>2</sub> die Sprache der Wörter gerader Länge über dem Alphabet  $\Sigma_2 = \{a, b\}$ .

Dann kann L₁ polynomial in L₂ transformiert werden, d. h. L₁ ≤p L₂.

#### Beweisidee:

Sei f :  $\Sigma_1^* \to \Sigma_2^*$  definiert als

$$f(z) := \begin{cases} \mathbf{aa}, & \text{falls z ungerade} \\ \mathbf{a}, & \text{sonst} \end{cases}$$

Dann kann f von einer DTM berechnet werden.

#### Fortsetzung der Beweisidee:

Eine solche DTM erhält als Eingabe eine Dezimalzahl z. Zunächst löscht sie alle Zeichen der Eingabe bis auf das Letzte. Wenn das letzte Zeichen der Eingabe ungerade ist, schreibt sie aa, ansonsten a auf das Band. Die Laufzeit der DTM ist hierbei im Wesentlichen logarithmisch in der Größe der Eingabe. Damit ist die Laufzeit polynomial beschränkt.

Sei  $z \in \Sigma_1^*$ . Dann ist  $f(z) \in L_2 \Leftrightarrow f(z) = aa \Leftrightarrow z$  ist ungerade  $\Leftrightarrow z \in L_1$ .

Damit ist f eine polynomiale Transformation von L<sub>1</sub> in L<sub>2</sub>.

# <u>Definition</u> (NP-Vollständigkeit):

Eine Sprache L heißt NP-vollständig, wenn L ∈ NP ist und für alle L' ∈ NP gilt:

# **Interpretation:**

L ist also NP-vollständig, wenn L selber zu NP gehört und jedes Problem in NP bzgl. ≤p nicht schwieriger als L ist. NP-vollständige Probleme müssen also selber in NP enthalten sein.

# **NP-**vollständig ⊆ **NP**

NP-vollständige Probleme sind also mindestens so komplex, wie jedes andere Problem in NP.

Kapitel 7 Gliederung

- 1. Intension in diesem Kapitel
- 2. Herausstellen von Komplexitätsklassen
- 3. Laufzeitkomplexität und O-Notation
- 4. Definitionen der Klassen P und NP
- 5. Erläuterung und Einordnung des Knapsack-Problems
- 6. NP-Vollständigkeit
- 7. Das Erfüllbarkeitsproblem (SAT und 3SAT)
- 8. NP-harte Probleme
- 9. Problemstellung der PARTITION

#### Bemerkungen:

Falls irgendwann jemand einen polynomiellen Lösungsalgorithmus für ein NP-vollständiges Problem L finden würde, dann hätte man einen polynomiellen Lösungsalgorithmus für jedes Problem in NP.

Es würde dann gelten, dass

#### P = NP

(eines der z. Z. größte offene Problem der theoretischen Informatik!)

Obwohl man bisher noch **nicht** nachweisen konnte, dass es <u>keinen</u> polynomiellen Lösungsalgorithmus für **NP**-vollständige Probleme gibt, konnte man für eine Reihe wichtiger Probleme zeigen, dass sie **NP**-vollständig sind.

Das bekannteste Beispiel ist das **Erfüllbarkeitsproblem**, kurz **SAT**. (**SAT** = **Sat**isfiability)

# **Definition** (SAT):

Sei  $X = \{x_1, x_2, ..., x_m\}$  eine Menge von **booleschen** Variablen  $\{x_i \text{ und } \overline{x}_i\}$  heißen auch **Literale**). Eine **Wahrheitsbelegung** von X ist eine Funktion

$$\mathbf{f}: \mathbf{X} \to \{ \text{ wahr, falsch } \}.$$

Eine Klausel k ist ein boolescher Ausdruck der Form

$$y_{k1} \vee y_{k2} \vee ... \vee y_{ks}$$

(d. h. Disjunktion von Literalen) mit

$$y_{ki} \in \{x_1, x_2, ..., x_m\} \cup \{\bar{x}_1, \bar{x}_2, ..., \bar{x}_m\} \cup \{\text{ wahr, falsch}\}.$$

Dann ist **SAT** wie folgt definiert:

Existiert eine Wahrheitsbelegung von X, so dass alle Klauseln (k = 1, 2, ... n) den Wahrheitswert wahr annehmen?

Gegeben seien eine Menge von Variablen  $X = \{x_1, x_2\}$  und eine Menge von Klauseln  $C = \{c_1, c_2\}$  über X gegeben mit

$$c_1 = x_1 \vee \overline{x}_2$$
 und  $c_2 = \overline{x}_1 \vee x_2$ .

Mit der Wahrheitsbelegung

$$f(x_1) = f(x_2) = wahr$$

(d. h.  $x_1 = x_2 = 1$ ) wird **C** erfüllt.

Satz (von Steven Cook, 1971):

**SAT** ist **NP**-vollständig.

# **Definition** (3SAT):

Gegeben: Eine Menge X von Variablen und eine Menge C von Klauseln

C, wobei jede Klausel genau drei Literale enthält.

Frage: Existiert eine erfüllende Wahrheitsbelegung für C?

Satz:

Das Problem **3SAT** ist **NP**-vollständig.

# Anmerkung:

Um zu zeigen, dass ein Problem NP-vollständig ist, wird häufig 3SAT auf das Problem reduziert.

# Beispiel (3SAT):

Gegeben seien eine Menge von Variablen  $\mathbf{X} = \{x_1, x_2, x_3\}$  und eine Menge von Klauseln  $\mathbf{C} = \{c_1, c_2, c_3, c_4\}$  über  $\mathbf{X}$ , wobei  $\mathbf{m} = |\mathbf{X}| = 3$  und  $\mathbf{n} = |\mathbf{C}| = 4$ .

$$C_1 = X_1 \lor X_2 \lor X_3$$
 $C_2 = X_1 \lor \bar{X}_2 \lor X_3$ 
 $C_3 = X_1 \lor \bar{X}_2 \lor \bar{X}_3$ 
 $C_4 = \bar{X}_1 \lor \bar{X}_2 \lor \bar{X}_3$ 

# Mit der Wahrheitsbelegung

$$f(x_1) = f(x_2) = wahr und f(x_3) = falsch,$$

d. h.  $(x_1, x_2, x_3) = (1, 1, 0)$ , wird **C** erfüllt.

Kapitel 7
Gliederung

- 1. Intension in diesem Kapitel
- 2. Herausstellen von Komplexitätsklassen
- 3. Laufzeitkomplexität und O-Notation
- 4. Definitionen der Klassen P und NP
- 5. Erläuterung und Einordnung des Knapsack-Problems
- 6. NP-Vollständigkeit
- 7. Das Erfüllbarkeitsproblem (SAT und 3SAT)
- 8. NP-harte Probleme
- 9. Problemstellung der PARTITION

Sprachen NP hart (1)

#### Vorbemerkung:

Wenn auch bislang der Versuch eines Beweises für **N = NP** nicht gelungen ist, so konnte man in der Vergangenheit für manche Probleme jedoch schon zeigen, dass man damit jedes andere Problem in **NP** lösen kann. Offensichtlich gelang es dabei aber noch nicht zu zeigen, dass diese Probleme selbst auch in **NP** sind.

Für diese Klasse von Problemen führte man die Bezeichnung NP hart ein.

Sprachen NP hart (2)

#### <u>Definition</u> (NP hart):

Eine Sprache L heißt NP-hart, wenn für alle L' ∈ NP gilt:

#### **Interpretation:**

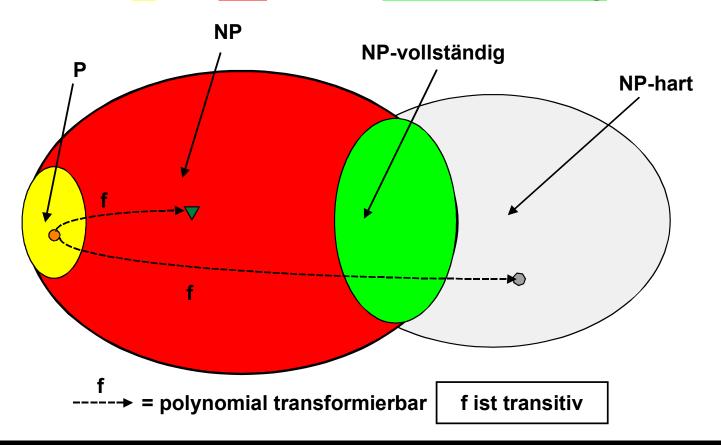
Ein Problem, das **NP** hart ist, muss selbst <u>nicht</u> notwendigerweise in **NP** enthalten sein. Wir nennen ein Problem **NP** hart, wenn es **mindestens** so schwer ist, wie alle **NP**-vollständigen Probleme.

Klar ist dagegen, dass ein NP-vollständiges Problem immer auch NP hart ist.

**NP vollständig** ⊆ **NP** hart

Sprachen NP hart (3)

<u>Zusammenhänge</u>: P ⊆ NP und NP-vollständig ⊆ NP-hart



Kapitel 7 Gliederung

- 1. Intension in diesem Kapitel
- 2. Herausstellen von Komplexitätsklassen
- 3. Laufzeitkomplexität und O-Notation
- 4. Definitionen der Klassen P und NP
- 5. Erläuterung und Einordnung des Knapsack-Problems
- 6. NP-Vollständigkeit
- 7. Das Erfüllbarkeitsproblem (SAT und 3SAT)
- 8. NP-harte Probleme
- 9. Problemstellung der PARTITION

Sprachen Partition (1)

# **Definition** (PARTITION):

Gegeben sind  $b_1, b_2, ..., b_n \in IN$ . Gibt es eine Teilmenge  $K \subseteq \{1, 2, ..., n\}$ , so dass die Summe aller  $b_k, k \in K$ , gleich der Summe aller  $b_j, j \notin K$  ist?

#### Satz:

# PARTITION ist NP-vollständig.

#### Beweis:

PARTITION ∈ **NP**, da wir **K** raten können. Das vollständige Raten (vollständige Aufzählung) entspricht dabei dem **Nicht-Determinismus**.

Sprachen Partition (2)

#### **Beispiel** (PARTITION):

Gegeben sei die Zahlenmenge ( $b_1$ ,  $b_2$ , ...,  $b_8$ ) = (2, 4, 5, 6, 7, 9, 10, 13). Die gesuchte Teilmenge  $\mathbf{K} \subseteq \{1, 2, ..., 8\}$  ist dann gleich  $\{1, 2, 4, 5, 6\}$ ,

weil:

$$b_1 + b_2 + b_4 + b_5 + b_6 = b_3 + b_7 + b_8 = 28$$