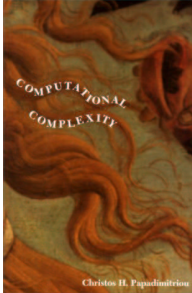





Literatur

C. Papadimitriou
UC Berkeley

Zum Komplexitätsbegriff

Strukturelle Komplexität

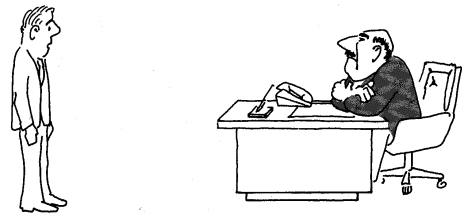
- Average Case Analyse
- Effiziente Algorithmen
- Logische Komplexität
- Beschreibungssprachen: SQL
- Kolmogorov Komplexität
- Komplexität = Programmgröße
- Axiomatische Komplexität
- Verallgemeinerte Komplexitätsmaße



Komplexitätstheorie

Einführung und Überblick
(Wiederholung)

Helmut Veith
Technische Universität München



"I can't find an efficient algorithm, I guess I'm just too dumb."

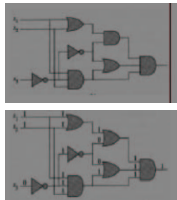
Garey & Johnson: Computers and Intractability

Time complexity function	Size n					
	10	20	30	40	50	60
n	.00001 second	.00002 second	.00003 second	.00004 second	.00005 second	.00006 second
n^2	.0001 second	.0004 second	.0009 second	.0016 second	.0025 second	.0036 second
n^3	.001 second	.008 second	.027 second	.064 second	.125 second	.216 second
n^4	.01 second	.16 seconds	.81 seconds	2.56 minutes	6.25 minutes	13.0 minutes
n^5	.0001 second	1.0 second	24.3 seconds	1024 minutes	17.7 centuries	35.7 centuries
2^n	.01 second	1.0 minutes	17.9 years	12.7 centuries	35.7 centuries	1.3×10^{13} centuries

Figure 1.2 Comparison of several polynomial and exponential time complexity functions.

The \$ 1.000.000 Problem

Existiert ein polynomieller Algorithmus für folgende Frage:
Kann ein Gatter eines kombinatorischen Schaltkreises je 1 werden ?



CIRCUIT SATISFIABILITY

NP Probleme

The \$ 1.000.000 Problem

Existiert ein polynomieller Algorithmus für folgende Frage:
Kann ein Gatter eines kombinatorischen Schaltkreises je 1 werden ?



CIRCUIT SATISFIABILITY

UNO Problem

Kann eine Gruppe n Delegierter so um einen runden Tisch platziert werden, dass keine Feinde nebeneinander zu sitzen kommen ?



Graphentheoretisch: Hamiltonian Cycle ?

Färbbarkeitsproblem

Kann eine Landkarte mit 3 Farben koloriert werden, sodass Nachbarstaaten unterschiedbar sind ?



4-Farbensatz

Kreuzwortproblem

Kann ein Kreuzworträtsel mit Wörtern einer Liste vollständig gefüllt werden ?



Cluster Workload Assignment

Kann eine Menge von Prozessen bekannter Workload auf N Prozessoren eingeteilt werden ?



Scheduling Problem

Kann eine Menge von n abhängigen Aufgaben innerhalb von t Zeitblöcken eingeteilt werden ?



... und tausende weitere Probleme.

Suchalgorithmen ?

Für die genannten Probleme sind nur exponentielle Algorithmen bekannt.

Aber: Die Eignung einer vorgeschlagenen Lösung kann effizient überprüft werden.

NP = Entscheidungsprobleme, die
(1) Lösungen polynomieller Grösse haben
(2) die Überprüfung von Lösungskandidaten in Polynomialzeit erlauben.

NP Probleme exponentiell lösbar

Angenommen, ein NP-Problem mit Eingabegrösse **N** hat Lösungen der Grösse **N^k** in Binärdarstellung.

Dann kann ein Suchalgorithmus in Zeit

$$2^{(N^k)}$$

alle Lösungen überprüfen.

Theorem $NP \subseteq EXPTIME$

Unentscheidbar

Entscheidbar

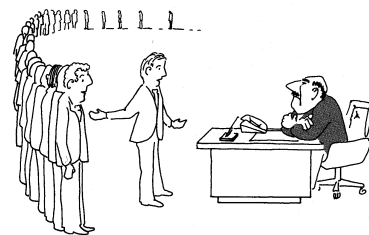
Exponentiell und höher

NP-vollständig

NP

PTIME

NP-Vollständigkeit




"I can't find an efficient algorithm, but neither can all these famous people."

Reduktionen

Cluster Workload Assignment

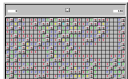
Kann eine Menge von Prozessen bekannter Workload auf N Prozessoren eingeteilt werden?




→

Minesweeper

Ist eine Spielsituation im Spiel Minesweeper konsistent?





Reduktion

Ein Algorithmus für Minesweeper kann mit polynomiellem Pre-Processing zum Lösen von Workload Assignment verwendet werden.

The \$ 1.000.000 Problem

Gibt es polynomielle Algorithmen für die Probleme in NP ?

NP Probleme

Das 4-Farben-Problem
Bekannt polynomieller Algorithmus, aber nicht für alle Graphen.

3SAT-Problem
Bekannt polynomieller Algorithmus, aber nicht für alle Formeln.

7-Farben-Problem
Bekannt polynomieller Algorithmus, aber nicht für alle Graphen.

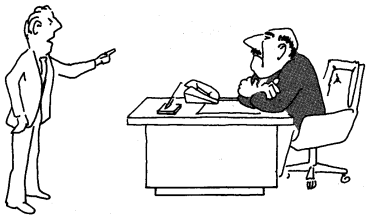
Knotenproblem
Bekannt polynomieller Algorithmus, aber nicht für alle Graphen.

Cluster Workload Assignment
Bekannt polynomieller Algorithmus, aber nicht für alle Graphen.

NP = PTIME ?

... und tausende weitere Probleme.

NP ≠ PTIME



"I can't find an efficient algorithm, because no such algorithm is possible!"



Komplexitätstheorie

NP-Vollständigkeit: Reduktionen

Helmut Veith
Technische Universität München

Probleme unter Bekannten

Gibt es K Studenten unter den N Anwesenden, die einander nicht kennen ?

INDEPENDENT SET

Reichen 3 Übungsgruppen, damit Studenten, die einander kennen, verschiedene Gruppen erhalten ?

3COLORABILITY

Reichen K Wanzen, um alle Telefongespräche zwischen Studenten abzuhören ?


VERTEX COVER

INDEPENDENT SET

Gibt es K Studenten unter den N Anwesenden, die einander nicht kennen ?

INSTANCE

Graph $G=(V,E)$; Zahl K.



QUERY

Hat G ein independent set I mit $|I| \geq K$?
d.h. ein I, sodass $\forall i,j \in I. (i,j) \notin E$

3COLORABILITY

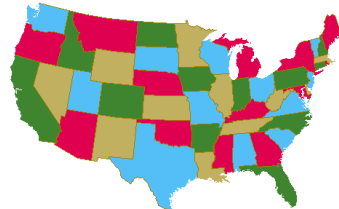
Reichen 3 Übungsgruppen, damit Studenten, die einander kennen, verschiedene Gruppen erhalten ?

INSTANCE
Graph $G=(V,E)$.

QUERY
Gibt es eine Funktion
 $F : V \rightarrow \{\text{red,green,blue}\}$
sodass benachbarte Knoten unterschiedlich gefärbt werden, d.h.
 $\forall (i,j) \in E . F(i) \neq F(j)$

Färbbarkeitsproblem

Kann eine Landkarte mit 3 Farben koloriert werden, sodass Nachbarstaaten unterscheidbar sind ?



PLANAR 3COLORABILITY

PLANAR 3COLORABILITY

Reichen 3 Übungsgruppen, damit Studenten, die einander kennen, verschiedene Gruppen erhalten ?

INSTANCE
Planarer Graph $G=(V,E)$.

QUERY
Gibt es eine Funktion
 $F : V \rightarrow \{\text{red,green,blue}\}$
sodass benachbarte Knoten unterschiedlich gefärbt werden, d.h.
 $\forall (i,j) \in E . F(i) \neq F(j)$

VERTEX COVER

Reichen K Wanzen, um alle Telefongespräche zwischen Studenten abzuhoeren ?

INSTANCE
Graph $G=(V,E)$; Zahl K .



QUERY
Hat G ein Vertex Cover C mit $|C| \leq K$?
d.h. ein $C \subseteq V$, sodass $\forall (i,j) \in E . i \in C \vee j \in C$

HAMILTONIAN CYCLE

INSTANCE Graph $G=(V,E)$.

QUERY Hat G einen Hamiltonschen Kreis ?

UNO Problem

Kann eine Gruppe n Delegierter so um einen runden Tisch platziert werden, dass keine Feinde nebeneinander zu sitzen kommen ?



Graphentheoretisch:
Hamiltonian Cycle ?

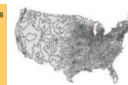
TSP

INSTANCE Graph $G=(V,E)$, Zahl K
und Gewichtsfunktion $f: E \rightarrow \mathbb{N}$

QUERY Hat G einen Zyklus mit
Gesamtgewicht $\leq K$?

Travelling Salesperson

Kann ein Vertreter n Städte besuchen, und dabei nicht mehr als K Kilometer zurücklegen ?



BIN PACKING

INSTANCE $N; a_1, \dots, a_M; b$

QUERY Können M Jobs mit Workloads a_i auf N Prozessoren mit maximaler Workload b aufgeteilt werden ?

Cluster Workload Assignment

Kann eine Menge von Prozessen bekannter Workload auf N Prozessoren eingeteilt werden?



RUCKSACK

INSTANCE $a_1, \dots, a_M; W$

QUERY Kann eine Teilmenge der a_i in Summe exakt W ergeben ?

Rucksackproblem

Gegeben eine Menge von Wertobjekten unterschiedlichen Gewichts und Wertes. Kann ein Dieb mit einem Rucksack mit Maximalgewicht M den Wert W erzielen ?



CLIQUE

Gibt es K Studenten unter den N Anwesenden, die einander kennen ?

INSTANCE

Graph $G=(V,E)$; Zahl K .



QUERY

Hat G ein independent set I mit $|I| \geq K$?
d.h. ein I , sodass $\forall i,j \in I. (i,j) \in E$

Boolesche Bedingungen

INSTANCE

C Source Code der Form

`if (f) p;`

wobei f aus Booleschen Variablen, $\&\&$, $\|\|$, $!$ besteht.

QUERY

Ist f eine erfüllbare Bedingung ?

d.h. gibt es eine Belegung der Variablen, sodass p ausgeführt wird ?

SAT

INSTANCE

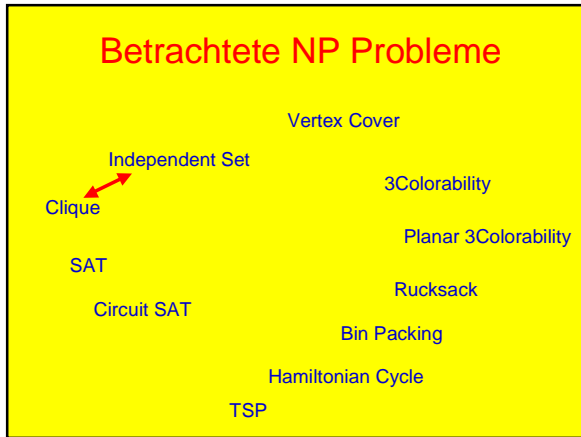
Boolesche (aussagenlogische) Formel f

QUERY

Gibt es eine Belegung der Variablen, sodass f wahr wird ?

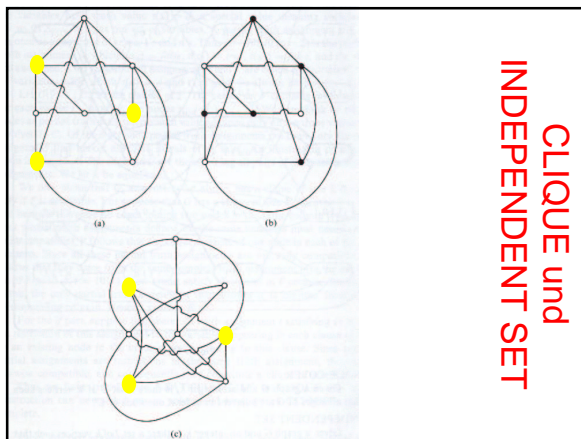
Betrachtete NP Probleme

Vertex Cover
Independent Set
3Colorability
Clique
Planar 3Colorability
SAT
Rucksack
Circuit SAT
Bin Packing
Hamiltonian Cycle
TSP



CLIQUE und INDEPENDENT SET

Lemma
 Graph $G = (V,E)$ und S Teilmenge V .
 Dann gilt:
 S ist ein Independent Set in G
 gdw
 S ist eine Clique im Komplement von G



CLIQUE und INDEPENDENT SET

Lemma
 Graph $G = (V,E)$ und S Teilmenge V .
 Dann gilt:
 S ist eine Clique in G
 gdw
 S ist ein Independent Set im Komplement von G .

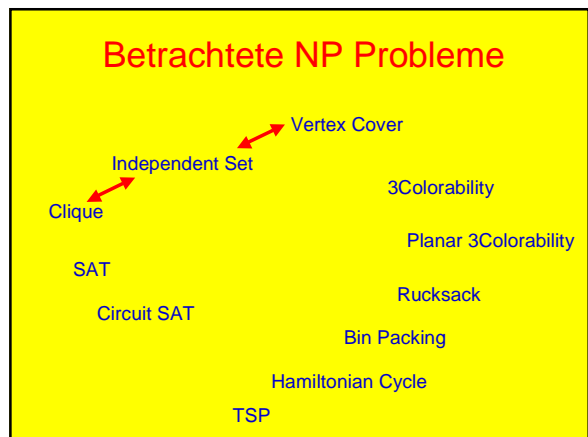
Algorithmische Reduktion zwischen CLIQUE und INDEPENDENT SET:
Berechne das Komplement des Graphen.
 $R: (V,E) \rightarrow (V, V \times V - E)$

CLIQUE und INDEPENDENT SET

CLIQUE(V,E): Algorithmus f. Clique

➔ **Algorithmus f. Independent Set:**

Independent_Set(V,E)
 $E' = V \times V - E;$
CLIQUE(V, E');



CLIQUE und INDEPENDENT SET

Lemma

Graph $G = (V, E)$ und S Teilmenge V .

Dann gilt:

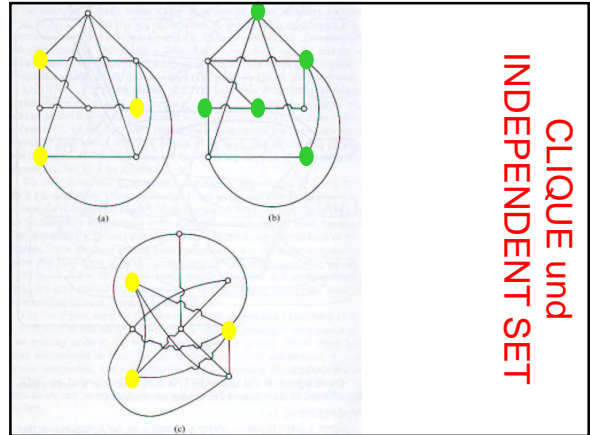
S ist eine Clique in G

gdw

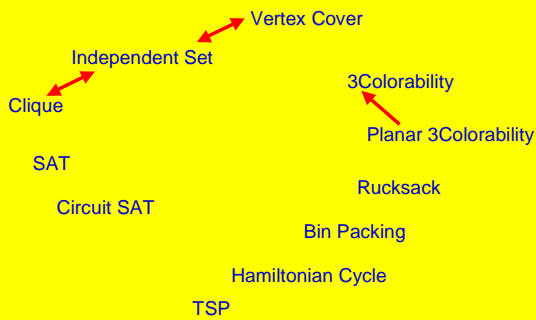
S ist ein Independent Set im Komplement von G

gdw

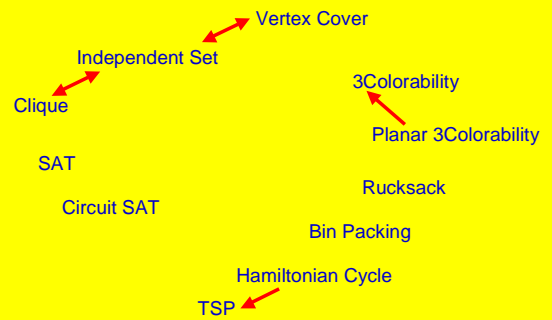
$V-S$ ist ein Vertex Cover von G .



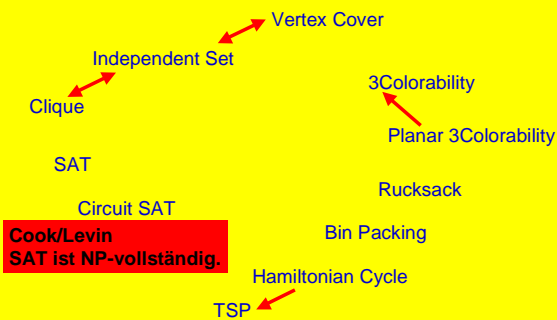
Betrachtete NP Probleme



Betrachtete NP Probleme



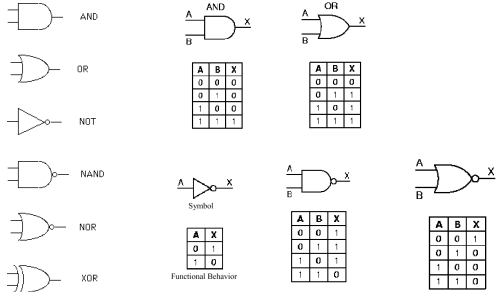
Betrachtete NP Probleme



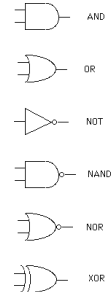
Exkurs: Boolesche Funktionen

- Boolesche Funktionen
- Funktionale Vollständigkeit
- Formeln
- CNF
- DNF
- Schaltkreise
- Boolesche Algebra
- Auswertungsalgorithmen
- Alternative Beschreibungen

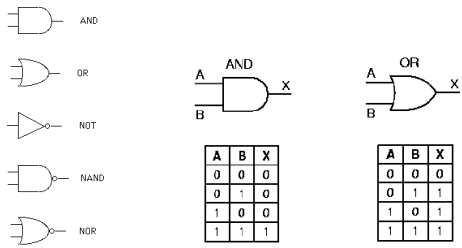
Schaltkreise



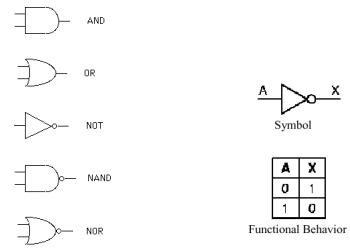
Schaltkreise



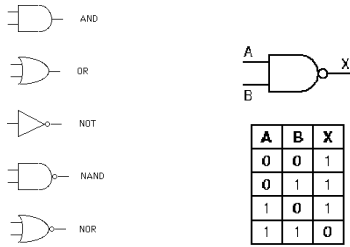
Schaltkreise



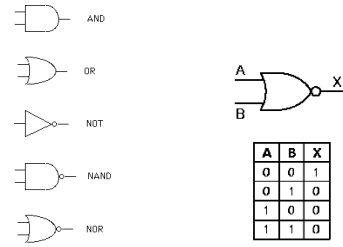
Schaltkreise



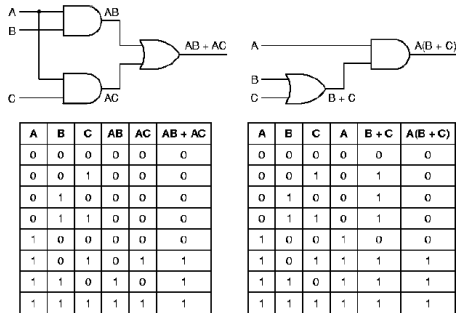
Schaltkreise



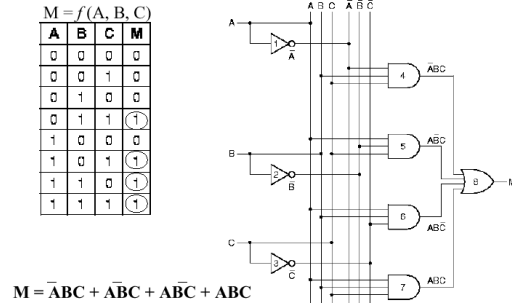
Schaltkreise



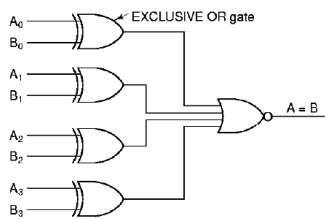
Schaltkreise



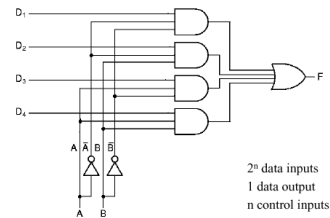
Schaltkreise



Schaltkreise



Schaltkreise



Uniforme Schaltkreise

Theorem

Zu jedem polynomialen Algorithmus (PTIME Algorithmus) A mit binären Eingaben gibt es eine Familie von Schaltkreisen C_1, C_2, \dots , sodass

- (1) C_i in Zeit i konstruiert werden kann.
- (2) Für alle Eingaben der Länge n C_i dasselbe Ergebnis wie A liefert.

Exkurs: Boolesche Funktionen

Boolesche Funktionen
 Funktionale Vollständigkeit
 Formeln
 CNF
 DNF
 Schaltkreise
 Boolesche Algebra
 Auswertungsalgorithmen
 Alternative Beschreibungen

SAT-Probleme

CIRCUIT SAT Ist ein Schaltkreis erfüllbar ?

SAT Ist eine Formel erfüllbar ?

CNF SAT Ist eine CNF Formel erfüllbar ?

3SAT Ist eine CNF Formel mit maximal 3 Literalen pro Klausel erfüllbar ?

DNFSAT Ist eine DNF Formel erfüllbar ?

HORN SAT Ist eine Horn Formel erfüllbar ?

SAT-Probleme

CIRCUIT SAT Ist ein Schaltkreis erfüllbar ?

SAT Ist eine Formel erfüllbar ?

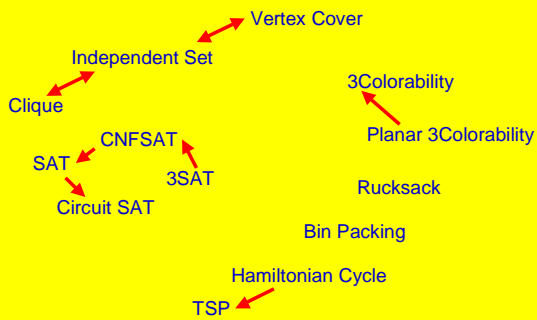
CNF SAT Ist eine CNF Formel erfüllbar ?

3SAT Ist eine CNF Formel mit maximal 3 Literalen pro Klausel erfüllbar ?

DNFSAT Ist eine DNF Formel erfüllbar ?

HORN SAT Ist eine Horn Formel erfüllbar ?

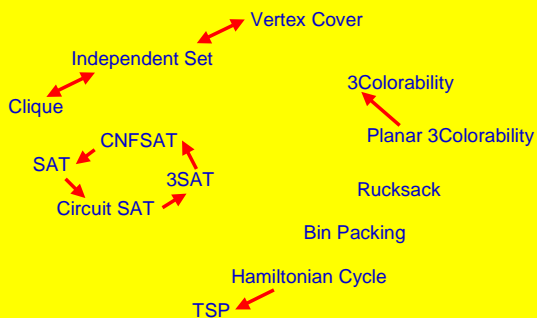
Betrachtete NP Probleme



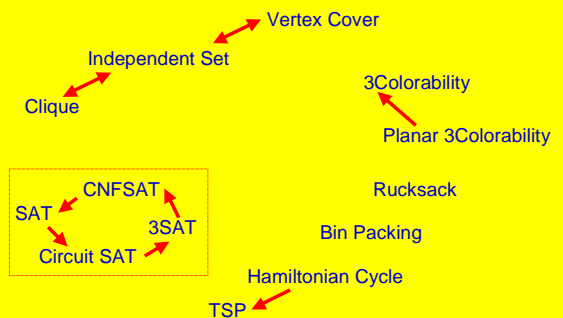
CIRCUIT SAT → 3SAT

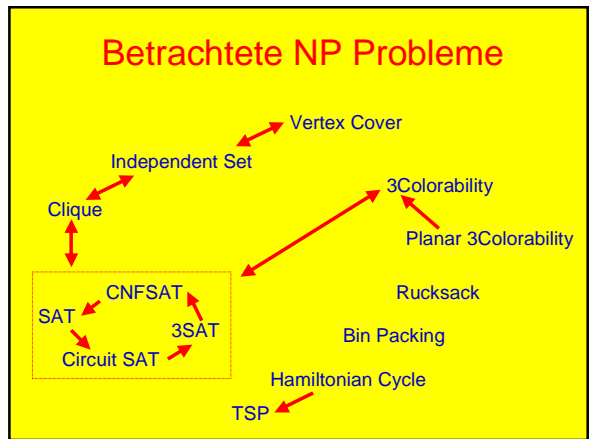
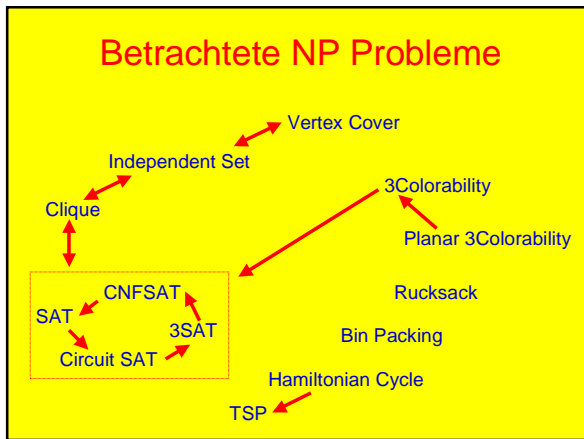
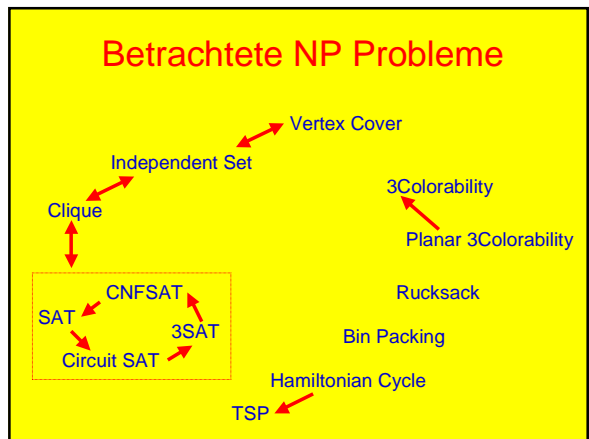
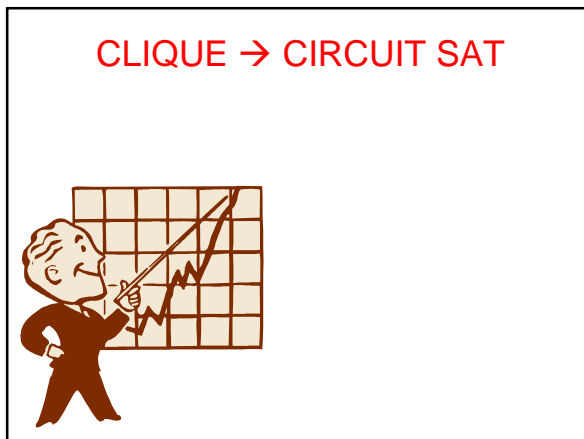
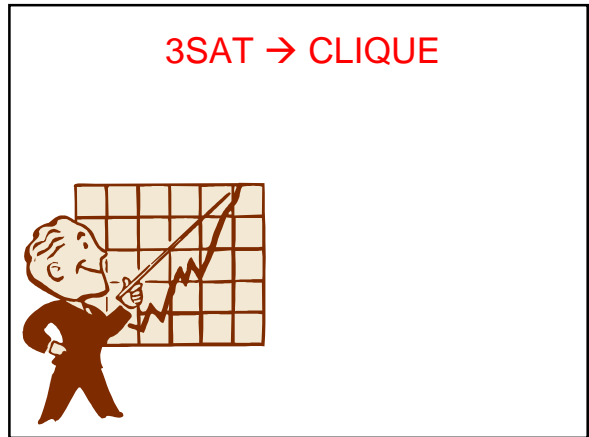
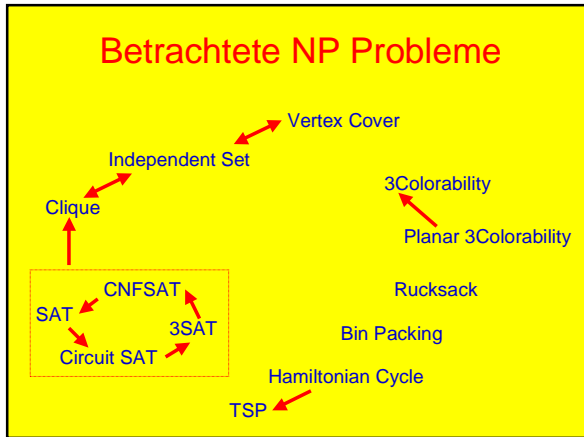


Betrachtete NP Probleme

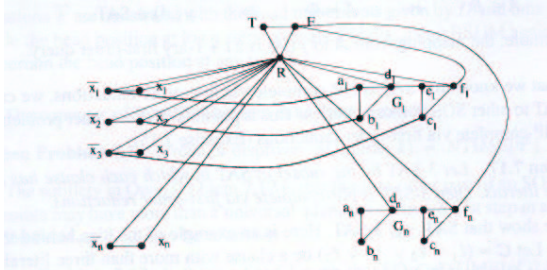


Betrachtete NP Probleme





3SAT \rightarrow 3COL



Danke für Ihre
Aufmerksamkeit