

# Theoretische Grundlagen der Informatik

**Tutorium 10** 

Institut für Kryntographie und Sicherheit



# Beweisprobleme



- $P \neq NP$  Beweise sind kompliziert
- Problem:

 $\exists A, B \in \text{Orakel: } P^A = NP^A \text{ und } P^B \neq NP^B$ 

- Man braucht sog. nicht relativierende Beweise (Diagonalisirung und andere hier behandelte Methoden sind alle relativierend)
- $\blacksquare$   $\Longrightarrow$  Viele falsche  $P \neq NP$  Beweise





Finden Sie den Fehler im folgenden "Beweis" für  $P \neq NP!$  Betrachten Sie folgenden Algorithmus für SAT:

- Durchlaufe für die gegebene Formel  $\phi$  alle möglichen Belegungen der Variablen mit den Wahrheitswerten
- Akzeptiere  $\phi$ , wenn eine der durchlaufenen Belegungen  $\phi$  erfüllt

Dieser Algorithmus hat eine mit der Anzahl der Variablen exponentiell wachsende Laufzeit. Daher hat das Problem SAT einen exponentiellen Aufwand und kann nicht in **P** liegen. Weil aber SAT in **NP** liegt, muß also  $\mathbf{P} \neq \mathbf{NP}$  gelten.



1. Zeigen Sie, dass es unter der Voraussetzung  $\mathbf{P} = \mathbf{NP}$  möglich ist, für eine aussagenlogische Formel  $\phi$  in polynomieller Zeit eine erfüllende Belegung der Variablen zu finden, falls eine solche Belegung existiert!



## **HALF-CLIQUE**



Wiederholung: CLIQUE

Enthält der Graph G = (V, E) einen Teilmenge  $V' \subseteq V$  mit  $|V'| \ge n$ , bei der jeder Knoten eine Kante zu jedem anderen Knoten des Teilgraphs hat?

HALF-CLIQUE

Enthält der Graph G = (V, E) eine CLIQUE mit  $|V'| \ge |V|/2$ ?



Gegeben ist das folgende Problem:

HALF-CLIQUE:

*Gegeben:* Ein ungerichteter Graph G = (V, E)

*Gesucht:* Gibt es eine Teilmenge  $V' \subseteq V$ 

 $mit \ \forall \ v, w \in V', v \neq w : (v, w) \in E \ und \ |V'| \ge |V|/2$ 

Beweisen Sie, dass HALF-CLIQUE NP-vollständig ist!

Zur Erinnerung:

Das als **NP**-vollständig bekannte Problem CLIQUE ist definiert durch:

CLIQUE:

*Gegeben:* Ein ungerichteter Graph G = (V, E) und  $k \in \mathbb{N}$ 

Gesucht: Gibt es eine Teilmenge  $V' \subseteq V$ 

 $\mathsf{mit} \ \forall \ \mathsf{v}, \mathsf{w} \in \mathsf{V}', \mathsf{v} \neq \mathsf{w} : (\mathsf{v}, \mathsf{w}) \in \mathsf{E} \ \mathsf{und} \ |\mathsf{V}'| \geq \mathsf{k}$ 



## **Hamiltonkreis**



#### Kurzdefinition

Enthält der gegebene Graph einen Kreis, d.h. gibt es einen Pfad der durch jeden Knoten exakt einmal geht und vom Startknoten wieder zum Startknoten führt (Start- und Endknoten wird nur einmal gezählt).

### Formal

Gegeben: Ein ungerichteter Graph G = (V, E).

Gesucht: Besitzt G einen Hamiltonkreis? (Dies ist eine Permutation  $\pi$  der Knotenindizes  $(v_{\pi(1)}, v_{\pi(2)}, ..., v_{\pi(n)})$ , sodass für i = 1, ..., n-1 gilt:

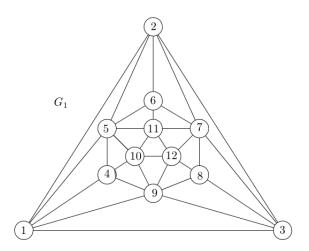
$$\{v_{\pi(i)}, v_{\pi(i+1)}\} \in E$$
) und außerdem  $\{v_{\pi(n)}, v_{\pi(1)}\} \in E$ ).



# **Beispiel**



## Gibt es in diesem Graphen einen Hamiltonkreis?





## **Travelling Salesman**



#### Kurzdefinition

Geben sie einen Kreis des gegeben vollständig verbundenen Graphen mit Kantenlängen an, sodass dessen Gesamtkantenlänge minimal ist.

## Formal

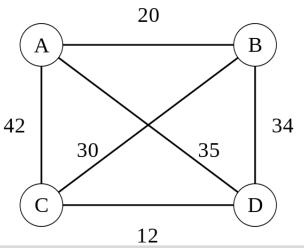
Gegeben: Ein Graph  $G = (V, V \times V)$ 

Gesucht: Ein einfacher Kreis  $C = (v_1, v_2, ..., v_n, v_1)$ , sodass n = |V| und  $\sum_{(u,v)\in C} d(u,v)$  minimiert wird, wobei d(u,v) die Entfernung zwischen den Knoten u und v ist.

# **Beispiel**



Wie lang ist die kürzeste Route und durch welche Kanten geht sie?





## Gegeben sind folgende Probleme:

## Hamiltonkreisproblem:

*Gegeben:* Ein ungerichteter Baum G = (V, E).

Gesucht: Besitzt G einen Hamiltonkreis? (Dies ist eine Permutation  $\pi$ der Knotenindizes ( $v_{\pi(1)}, v_{\pi(2)}, ..., v_{\pi(n)}$ ), sodass für i = 1, ..., n-1 gilt:  $\{v_{\pi(i)}, v_{\pi(i+1)}\} \in E$ ) und außerdem  $\{v_{\pi(n)}, v_{\pi(1)}\} \in E$ ).

## Travelling Salesman(TSP):

*Geaeben:* Ein Graph  $G = (V, V \times V)$ 

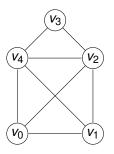
Gesucht: Ein einfacher Kreis  $C = (v_1, v_2, ..., v_n, v_1)$ , sodass n = |V|und  $\sum_{(u,v)\in C} d(u,v)$  minimiert wird, wobei d(u,v) die Entfernung

zwischen den Knoten u und v ist.

Zeigen Sie, dass TSP NP-Vollständig ist, wobei das Hamiltonkreisproblem auch NP-Vollständig ist. Benutzen Sie für den Beweis die Reduktion Hamiltonkreisproblem $\leq_p$ TSP. 4 ₱ ▶ 4 **=** ▶ 40 Q (>



Gegeben sei folgender Graph:



Gibt es einen Hamiltonkreis? Wandeln Sie hierzu das Problem in ein TSP um und finden Sie eine optimale Rundtour.



## Bis zum nächsten Mal!



## MY HOBBY: EMBEDDING NP-COMPLETE PROBLEMS IN RESTAURANT ORDERS



WE'D LIKE EXACTLY \$ 15, 05 WORTH OF APPETIZERS, PLEASE. ... EXACTLY? UHH ... HERE, THESE PAPERS ON THE KNAPSACK PROBLEM MIGHT HELP YOU OUT. LISTEN. I HAVE SIX OTHER TABLES TO GET TO -- AS FAST AS POSSIBLE OF COURSE. WANT SOMETHING ON TRAVELING SALESMAN?

Tutoriumsmaterial von Michael Fuerst

## Lizenzen





Dieses Werk ist unter einem "Creative Commons Namensnennung-Weitergabe unter gleichen Bedingungen 3.0 Deutschland"-Lizenzvertrag lizenziert. Um eine Kopie der Lizenz zu erhalten, gehen Sie bitte zu http://creativecommons.org/licenses/by-sa/3.0/de/ oder schreiben Sie an Creative Commons, 171 Second Street, Suite 300, San Francisco, California 94105, USA.

Davon ausgenommen sind das Titelbild, welches aus der März-April 2002 Ausgabe von American Scientist erschienen ist und ohne Erlaubnis verwendet wird, sowie das KIT Beamer Theme. Hierfür gelten die Bestimmungen der jeweiligen Urheber.

