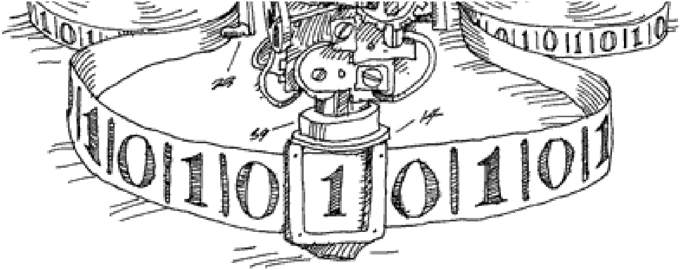
Theoretische Grundlagen der Informatik

Tutorium 10

Institut für Kryptographie und Sicherheit



Beweisprobleme

- $P \neq NP$ Beweise sind kompliziert
- Problem:
  $\exists A, B \in$ Orakel: $P^A = NP^A$ und $P^B \neq NP^B$
- Man braucht sog. nicht relativierende Beweise
  (Diagonalisirung und andere hier behandelte Methoden sind alle relativierend)
- $\implies$ Viele falsche $P \neq NP$ Beweise

Aufgabe B10 A2

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

- Durchlaufe für die gegebene Formel ϕ alle möglichen Belegungen der Variablen mit den Wahrheitswerten
- Akzeptiere ϕ, wenn eine der durchlaufenen Belegungen ϕ 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 **P** $\neq$ **NP** gelten.

Aufgabe B10 A3

1. Zeigen Sie, dass es unter der Voraussetzung $\mathbf{P} = \mathbf{NP}$ möglich ist, für eine aussagenlogische Formel ϕ 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 $|V'| \geq n$, bei der jeder Knoten eine Kante zu jedem anderen Knoten des Teilgraphs hat?

HALF-CLIQUE

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

Aufgabe B10 A1

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 $|V'| \geq |V|/2$

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

Hamiltonkreis

Kurzdefinition

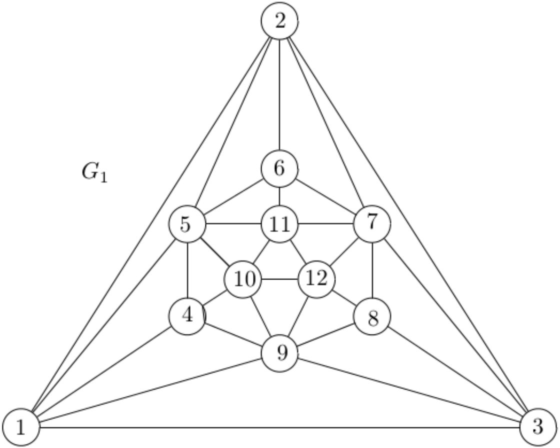
Enthält der gegebene Graph einen Kreis, d.h. gibt es einen Pfad der durch jeden Knoten exakt einmal geht und vom Startknoten wieder zum Startknoten führt (Start- und Endknoten wird nur einmal gezählt).

Formal

Gegeben: Ein ungerichteter Graph $G = (V, E)$.
Gesucht: Besitzt G einen Hamiltonkreis? (Dies ist eine Permutation π 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

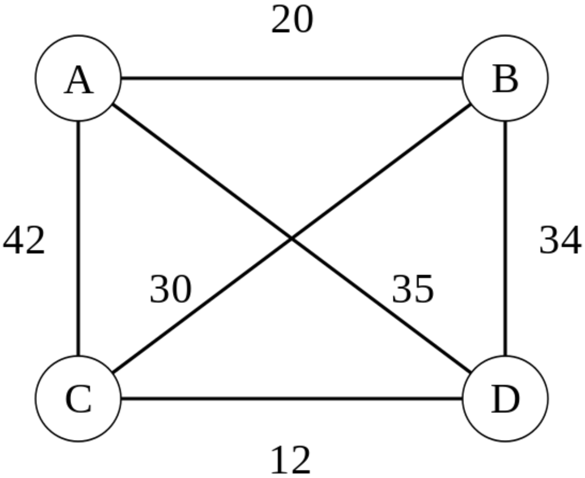
Geben sie einen Kreis des gegeben vollständig verbundenen Graphen mit Kantenlängen an, sodass dessen Gesamtkantenlänge minimal ist.

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?



Aufgabe B10 A4

Gegeben sind folgende Probleme:

Hamiltonkreisproblem:

Gegeben: Ein ungerichteter Baum $G = (V, E)$.
Gesucht: Besitzt G einen Hamiltonkreis? (Dies ist eine Permutation π 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 $\{v_{\pi(n)}, v_{\pi(1)}\} \in E$).

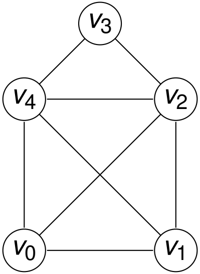
Travelling Salesman(TSP):

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.

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.

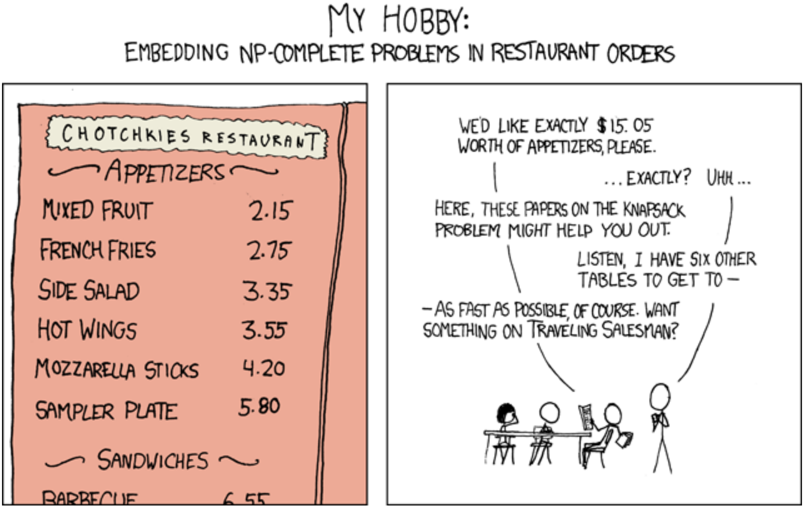
Aufgabe B10 A4

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!



Lizenzen