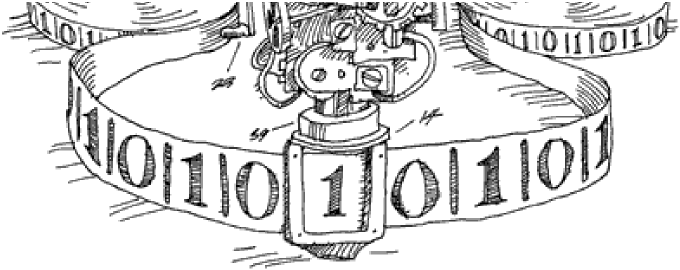
Karlsruher Institut für Technologie

# Theoretische Grundlagen der Informatik

## Tutorium 10

Institut für Kryptographie und Sicherheit



# Best of Übungsblatt 4

- Abgaben: 13 von 21 (61.9%)
- Mindestens 50% Punkte: 10 von 13 (76.92%)
- Durchschnittliche erreichte Punktzahl: 8.5
  - (nach Aufrunden auf halbe Punkte)

Aufgabenverteilung

Aufgabe 1: Gesamt: 23.75P (durchscnittlich 1.82)

Aufgabe 2: Gesamt: 36.25P (durchschnittlich 2.78)

Aufgabe 3: Gesamt: 14.25P (durchschnittlich 1.1)

Aufgabe 4: Gesamt: 35.25P (durchschnittlich 2.71)

# NP-Schwere

Wie zeige ich, dass $L$ NP-schwer ist?

- Formal: $\forall L' \in NP\colon L' \leq L$
  - Das sind ganz schön viele $L'$
- Wir nutzen Transitivität der Reduzierbarkeit in polynomieller Zeit
  - $\exists L_0 \forall L' \in NP\colon L' \leq L_0 \leq L \Rightarrow L' \leq L$
    - $L' \leq L_0$ gilt für alle NP-schweren $L_0$

Zu zeigen: $\exists L_0 \in NP\text{-schwer}\colon L_0 \leq L \Rightarrow L \in NP\text{-schwer}$

- Erinnerung: $NPC \subset NP\text{-schwer}$

# Reduzierung

Karlsruher Institut für Technologie

$L_0 \leq L$

$\Leftrightarrow$ Reduziere $L_0$ auf $L$

$\Leftrightarrow$ $L$ ist mindestens so schwer wie $L_0$

$\Leftrightarrow$ Ich kann eine Transformation $f\colon L_0 \to L$ mit folgenden Eigenschaften angeben:

- Die Lösung der erzeugten Instanz induziert eine Lösung der Eingabeinstanz
  - Bei Entscheidungsproblem bedeutet dies bspw. dass die erzeugte Instanz genau dann lösbar ist (ein sog. „Ja-Instanz“) wenn die Eingabeinstanz lösbar ist.
- Die f ist von geringerer Komplexität als die Probleme
  - Bei NP-Problemen darf die Transformation bspw. nur polynomiell Zeit benötigen und muss deterministisch sein.

# Bei Entscheidungsproblemen? Gibts noch mehr?

Die Meisten Entscheidungsprobleme existieren in 3 Formen:

- Enscheidungsproblem
  - Existiert eine Lösung für das Problem?
  - „Kann ich diesen Graphen mit 3 Farben färben?“
- Suchproblem
  - Suche eine Lösung für das Problem
  - „Wie sieht eine Dreifärbung für diesen Gaphen aus?“
- Optimierungsproblem
  - Welchen „Grad“ hat die beste Lösung für dieses Problem?
  - „Wie viele Farben benötige ich mindestens um den Graphen zu färben?“

- Umwandlung der Probleme zueinander in der Regel einfach
- In dieser Vorlesung hauptsächlich Entscheidungsprobleme

# 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 $\phi$ 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 **P** $\neq$ **NP** gelten.

# Aufgabe B10 A3

Karlsruher Institut für Technologie

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 $|V'| \geq n$, 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

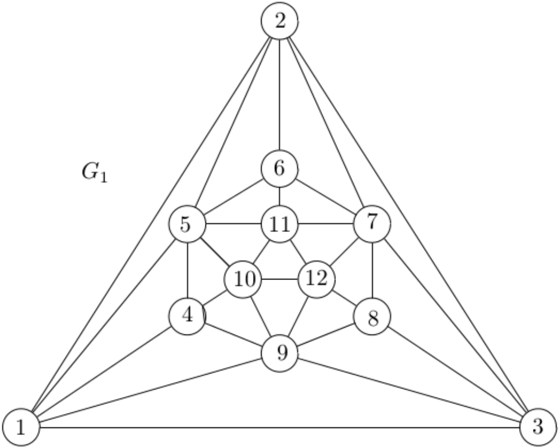
Enthält der gegebene Graph einen Kreis, d.h. gibt es einen Pfad der durch jeden Knoten exakt einmal geht und vom Startknoten wieder zum Startknoten führt (Start- und Endknoten wird nur einmal gezählt).

## Formal

Gegeben: Ein ungerichteter Graph $G = (V, E)$.
Gesucht: Besitzt $G$ einen Hamiltonkreis? (Dies ist eine Permutation $\pi$ der Knotenindizes $(v_{\pi(1)}, v_{\pi(2)}, \ldots, v_{\pi(n)})$, sodass für $i = 1, \ldots, n-1$ 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

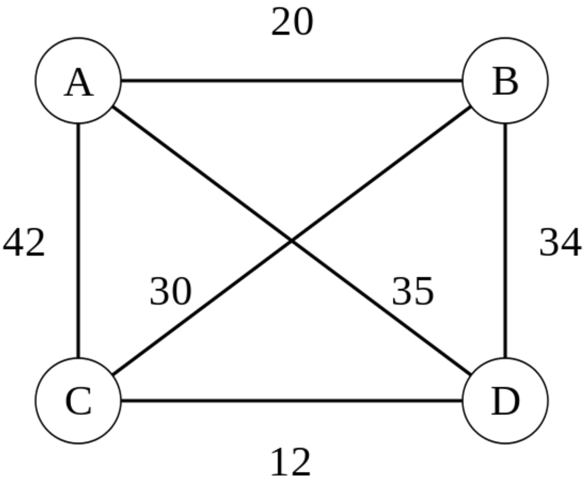
Geben sie einen Kreis des gegeben vollständig verbundenen Graphen mit Kantenlängen an, sodass dessen Gesamtkantenlänge minimal ist.

## Formal

Gegeben: Ein Graph $G = (V, V \times V)$, eine Gewichtungsfunktion $d : V \times V \rightarrow \mathbb{N}$ und ein Parameter $k$
Gesucht: Besitzt $G$ einen einfacher Kreis $C = (v_1, v_2, ..., v_n, v_1)$, sodass $n = |V|$ und $\sum_{(u,v) \in C} d(u, v) \leq k$.

# Beispiel

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



# Aufgabe B10 A4

Gegeben sind folgende Probleme:

## Hamilton-Kreis

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 $\{v_{\pi(n)}, v_{\pi(1)}\} \in E$).

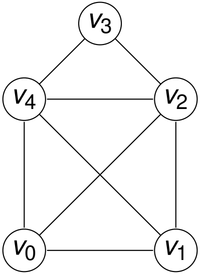
## TSP Enscheidungsproblem

Gegeben: Ein Graph $G = (V, V \times V)$, eine Gewichtungsfunktion $d : V \times V \to \mathbb{N}$ und ein Parameter $k$
Gesucht: Besitzt $G$ einen einfacher Kreis $C = (v_1, v_2, ..., v_n, v_1)$, sodass $n = |V|$ und $\sum_{(u,v)\in C} d(u, v) \leq k$.

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:



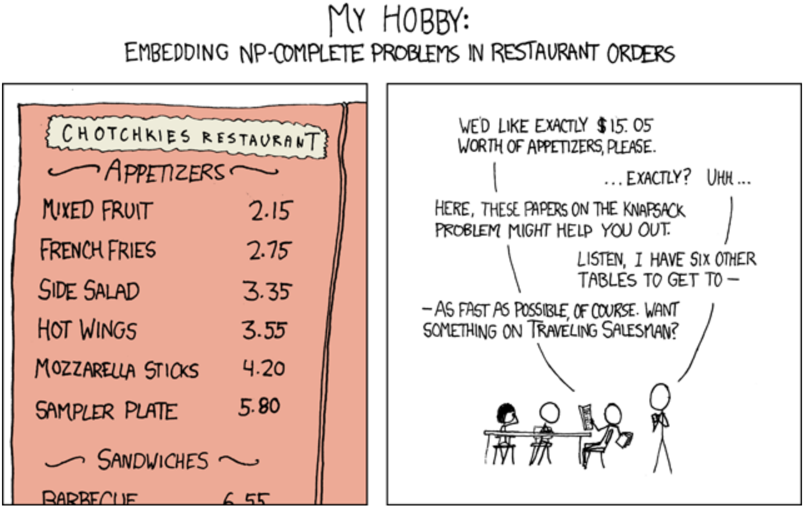

Gibt es einen Hamiltonkreis? Wandeln Sie hierzu das Problem in ein TSP um und finden Sie eine optimale Rundtour.

# Immer hilfreich: Mehr Probleme

Karlsruher Institut für Technologie

- NP-Probleme
  - Sat
  - n-Sat ($n \geq 3$)
  - n-Color ($n \geq 3$)
  - Partition
  - Clique
  - Bin-Packing
  - Traveling Salesman (TSP)
  - Knapsack
  - Vertex Cover
  - Dominating Set
  - Independent Set
  - Hamilton Kreis
  - Super Mario Bros.

# Bis zum nächsten Mal!



# Lizenzen