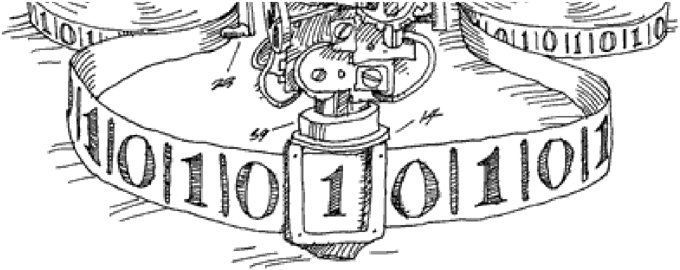
Karlsruher Institut für Technologie

Theoretische Grundlagen der Informatik

Tutorium 7

Institut für Theoretische Informatik



Allgemeines zu $\mathcal{NP}$-Vollständigkeitsbeweisen

Karlsruher Institut für Technologie

In der Regel ist es schwer zu zeigen, dass ein Problem $\mathcal{NP}$-schwer ist, aber leicht zu zeigen, dass ein Problem in $\mathcal{NP}$ liegt.

Da man üblicherweise ein $\mathcal{NP}$-vollständiges Problem als Voraussetzung für die Reduktion benötigt (Ausnahme: Satz von Cook), lohnt es sich einige kennen zu lernen.

SAT (SATisfiability = Erfüllbarkeitsproblem)

Karlsruher Institut für Technologie

Problem

Gegeben: Formel in konjunktiver Normalform

- Menge *U* von Variablen
- Menge *C* von Klauseln (Disjunktionen) über *U*

$$\underbrace{(\overset{\text{Literale}}{\overset{\downarrow}{a}} \vee \overset{\downarrow}{b} \vee \overset{\downarrow}{\overline{c}})}_{\text{Klausel}} \wedge \underbrace{(b \vee c)}_{\text{Klausel}} \wedge \underbrace{(\overline{a} \vee \overline{b} \vee \overline{c})}_{\text{Klausel}}$$

Frage: Existiert eine (alle Klauseln) erfüllende Variablenbelegung?

- *Das* Standardproblem.
- „Erstes" $\mathcal{NP}$-vollständiges Problem (Satz von Cook)
- Es gibt viele hochoptimierte „SAT-Solver". Steht man in der Praxis vor einem $\mathcal{NP}$-Problem, kann eine Transformation auf *SAT* sinnvoll sein.

SAT (SATisfiability = Erfüllbarkeitsproblem)

Problem

Gegeben: Formel in konjunktiver Normalform

- Menge U von Variablen
- Menge C von Klauseln (Disjunktionen) über U

Literale

$$\underbrace{(\overset{\downarrow}{a} \vee \overset{\downarrow}{b} \vee \overset{\downarrow}{\overline{c}})}_{\text{Klausel}} \wedge \underbrace{(b \vee c)}_{\text{Klausel}} \wedge \underbrace{(\overline{a} \vee \overline{b} \vee \overline{c})}_{\text{Klausel}}$$

Frage: Existiert eine (alle Klauseln) erfüllende Variablenbelegung?

- *Das* Standardproblem.
- „Erstes“ $\mathcal{NP}$-vollständiges Problem (Satz von Cook)
- Es gibt viele hochoptimierte „SAT-Solver“. Steht man in der Praxis vor einem $\mathcal{NP}$-Problem, kann eine Transformation auf *SAT* sinnvoll sein.

3SAT

Karlsruher Institut für Technologie

Problem

Gegeben:

- Menge *U* von Variablen
- Menge *C* von Klauseln über *U*
  Jede Klausel enthält genau *genau 3* Literale

$$C = \{(x_1 \vee x_2 \vee x_3), (x_1 \vee \overline{x_2} \vee \overline{x_3}), (\overline{x_1} \vee x_2 \vee x_3)\}$$

Frage: Existiert eine erfüllende Wahrheitsbelegung von *C*?

- Bietet sich bei Reduktion eher an als SAT, da übersichtlicher

MAX2SAT

Problem

Gegeben:

- Menge U von Variablen
- Menge C von Klauseln über U, wobei jede Klausel genau zwei Literale enthält
- Zahl $K \in \mathbb{N}$

Frage: Existiert eine Wahrheitsbelegung, die mindestens K Klauseln erfüllt?

- $MAX2SAT$ ist $\mathcal{NP}$-vollständig, aber $2SAT$ ist in $\mathcal{P}$.

Aufgabe

Haben die folgenden SAT-Instanzen eine Lösung? Gib eine erfüllende Wahrheitsbelegung an oder zeige, dass keine existieren kann.

1. $\{(a \lor b \lor \overline{c}), (b \lor c), (\overline{a} \lor \overline{b} \lor \overline{c})\}$
2. $\{(\overline{a} \lor b), (\overline{b} \lor a), (a \lor b \lor \overline{c}), (\overline{a} \lor c), (\overline{a} \lor \overline{b} \lor \overline{c}), (\overline{c} \lor \overline{b}), (a \lor b \lor c)\}$

Komplementsprachen

Karlsruher Institut für Technologie

Definition

Zu einer Sprache $L \subseteq \Sigma^*$ definieren wir co-L als das Komplement der Sprache, also co-$L := \Sigma^* \setminus L$.

Für eine Klasse von Sprachen wie $\mathcal{P}$ definieren wir die „co"-Klasse (wie z.B. co-$\mathcal{P}$) als Menge der Komplemente (und nicht etwa als Komplement der Klasse – warum?).

Beispiel: co-3SAT: Die aussagenlogischen Formeln mit 3 Variablen pro Klausel, die nicht erfüllbar sind.

Aufgabe: Beschreibe co-CLIQUE.

Aufgabe: Gelten folgende Behauptungen?

- $\mathcal{P} =$ co-$\mathcal{P}$?
- $\mathcal{NP} =$ co-$\mathcal{NP}$?

Komplementsprachen

Definition

Zu einer Sprache $L \subseteq \Sigma^*$ definieren wir co-L als das Komplement der Sprache, also co-$L := \Sigma^* \setminus L$.

Für eine Klasse von Sprachen wie $\mathcal{P}$ definieren wir die „co"-Klasse (wie z.B. co-$\mathcal{P}$) als Menge der Komplemente (und nicht etwa als Komplement der Klasse – warum?).

Beispiel: co-3SAT: Die aussagenlogischen Formeln mit 3 Variablen pro Klausel, die nicht erfüllbar sind.

Aufgabe: Beschreibe co-CLIQUE.

Aufgabe: Gelten folgende Behauptungen?

- $\mathcal{P} =$ co-$\mathcal{P}$?
- $\mathcal{NP} =$ co-$\mathcal{NP}$?

Komplementsprachen

Definition

Zu einer Sprache $L \subseteq \Sigma^*$ definieren wir co-L als das Komplement der Sprache, also co-$L := \Sigma^* \setminus L$.

Für eine Klasse von Sprachen wie $\mathcal{P}$ definieren wir die „co"-Klasse (wie z.B. co-$\mathcal{P}$) als Menge der Komplemente (und nicht etwa als Komplement der Klasse – warum?).

Beispiel: co-3SAT: Die aussagenlogischen Formeln mit 3 Variablen pro Klausel, die nicht erfüllbar sind.

Aufgabe: Beschreibe co-CLIQUE.

Aufgabe: Gelten folgende Behauptungen?

- $\mathcal{P} =$ co-$\mathcal{P}$?
- $\mathcal{NP} =$ co-$\mathcal{NP}$?

Komplementsprachen

Definition

Zu einer Sprache $L \subseteq \Sigma^*$ definieren wir co-L als das Komplement der Sprache, also co-$L := \Sigma^* \setminus L$.

Für eine Klasse von Sprachen wie $\mathcal{P}$ definieren wir die „co"-Klasse (wie z.B. co-$\mathcal{P}$) als Menge der Komplemente (und nicht etwa als Komplement der Klasse – warum?).

Beispiel: co-3SAT: Die aussagenlogischen Formeln mit 3 Variablen pro Klausel, die nicht erfüllbar sind.

Aufgabe: Beschreibe co-CLIQUE.

Aufgabe: Gelten folgende Behauptungen?

- $\mathcal{P} =$ co-$\mathcal{P}$?
- $\mathcal{NP} =$ co-$\mathcal{NP}$?

Komplementsprachen

Definition

Zu einer Sprache $L \subseteq \Sigma^*$ definieren wir co-L als das Komplement der Sprache, also co-$L := \Sigma^* \setminus L$.

Für eine Klasse von Sprachen wie $\mathcal{P}$ definieren wir die „co"-Klasse (wie z.B. co-$\mathcal{P}$) als Menge der Komplemente (und nicht etwa als Komplement der Klasse – warum?).

Beispiel: co-3SAT: Die aussagenlogischen Formeln mit 3 Variablen pro Klausel, die nicht erfüllbar sind.

Aufgabe: Beschreibe co-CLIQUE.

Aufgabe: Gelten folgende Behauptungen?

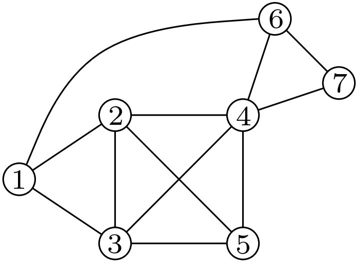
- $\mathcal{P} =$ co-$\mathcal{P}$?
- $\mathcal{NP} =$ co-$\mathcal{NP}$?
- $\mathcal{NP} \neq$ co-$\mathcal{NP} \Rightarrow \mathcal{P} \neq \mathcal{NP}$?

Aufgabe

Betrachte das Problem INDEPENDENT SET (IS):

- **Gegeben:** Graph $G = (V, E)$, Parameter $K \leq |V|$
- **Frage:** Gibt es eine unabhängige Menge der Größe K in G, d. h. eine Menge $V' \subseteq V$ mit $|V'| \geq K$, sodass $\{v, w\} \notin E$ für alle $v, w \in V'$?

Finde in folgendem Graphen $G_1 = (V_1, E_1)$ eine unabhängige Menge maximaler Größe:



Aufgabe

Betrachte das Problem INDEPENDENT SET (IS):

- **Gegeben:** Graph $G = (V, E)$, Parameter $K \leq |V|$
- **Frage:** Gibt es eine unabhängige Menge der Größe K in G, d. h. eine Menge $V' \subseteq V$ mit $|V'| \geq K$, sodass $\{v, w\} \notin E$ für alle $v, w \in V'$?

Formuliere das komplementäre Problem co-INDEPENDENT SET.

Aufgabe

Betrachte das Problem INDEPENDENT SET (IS):

- **Gegeben:** Graph $G = (V, E)$, Parameter $K \leq |V|$
- **Frage:** Gibt es eine unabhängige Menge der Größe K in G, d. h. eine Menge $V' \subseteq V$ mit $|V'| \geq K$, sodass $\{v, w\} \notin E$ für alle $v, w \in V'$?

Zeichne $\overline{G_1} = (V_1, \overline{E_1})$, wobei $\overline{E_1} = \{\{v, w\} \mid v, w \in V_1, \{v, w\} \notin E_1\}$.
Bestimme eine Clique maximaler Größe in $\overline{G_1}$.
Was fällt dabei auf?

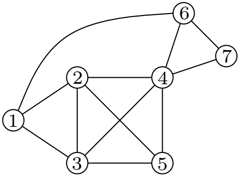
Aufgabe

Betrachte das Problem INDEPENDENT SET (IS):

- **Gegeben:** Graph $G = (V, E)$, Parameter $K \leq |V|$
- **Frage:** Gibt es eine unabhängige Menge der Größe K in G, d. h. eine Menge $V' \subseteq V$ mit $|V'| \geq K$, sodass $\{v, w\} \notin E$ für alle $v, w \in V'$?

Beweise die $\mathcal{NP}$-Vollständigkeit von IS. Gehe dabei wie folgt vor:

1. Zeige: IS $\in \mathcal{NP}$.
2. Zeige: V' Clique in $G \iff V'$ unabhängige Menge in $\overline{G} = (V, \overline{E})$, wobei $\overline{E} = \{\{v, w\} \mid v, w \in V, \{v, w\} \notin E\}$
3. Zeige, dass IS $\mathcal{NP}$-schwer ist.



COLOR

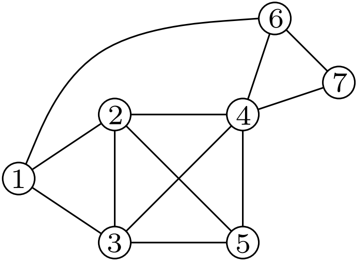
Problem

Gegeben: Graph $G = (V, E)$ und ein Parameter $K \in \mathbb{N}$
Frage: Gibt es eine Knotenfärbung von G mit höchstens K Farben, sodass zwei adjazente Knoten verschiedene Farben besitzen?

- Bei festem K nur $\mathcal{NP}$-vollständig für $K \geq 3$ (sonst in $\mathcal{P}$).

Aufgabe

Für welche K ist der folgende Graph eine Ja-Instanz für das Problem COLOR?



EXACT COVER

Problem

Gegeben: Eine Menge $\mathcal{S}$ von Teilmengen einer Menge X
Frage: Gibt es eine Teilmenge $\mathcal{S}^*$ von $\mathcal{S}$, sodass jedes Element aus X in genau einem der $s \in \mathcal{S}^*$ enthalten ist?

Beispiel

$$X = \{a, b, c, d, e, f, g, h\}$$

$$\mathcal{S} = \{\{a, c, e\}, \{a, f, g\}, \{b, d\}, \{b, f, h\}, \{e, h, i\}, \{f, h, i\}, \{d, g, i\}\}$$

EXACT COVER

Karlsruher Institut für Technologie

Problem

Gegeben: Eine Menge $\mathcal{S}$ von Teilmengen einer Menge X
Frage: Gibt es eine Teilmenge $\mathcal{S}^*$ von $\mathcal{S}$, sodass jedes Element aus X in genau einem der $s \in \mathcal{S}^*$ enthalten ist?

Beispiel

$$X = \{a, b, c, d, e, f, g, h\}$$

$$\mathcal{S} = \{\{a, c, e\}, \{a, f, g\}, \{b, d\}, \{b, f, h\}, \{e, h, i\}, \{f, h, i\}, \{d, g, i\}\}$$

EXACT COVER

Problem

Gegeben: Eine Menge $\mathcal{S}$ von Teilmengen einer Menge X
Frage: Gibt es eine Teilmenge $\mathcal{S}^*$ von $\mathcal{S}$, sodass jedes Element aus X in genau einem der $s \in \mathcal{S}^*$ enthalten ist?

Beispiel

$$X = \{a, b, c, d, e, f, g, h\}$$

$$\mathcal{S} = \{\{a, c, e\}, \{a, f, g\}, \{b, d\}, \{b, f, h\}, \{e, h, i\}, \{f, h, i\}, \{d, g, i\}\}$$

$$\mathcal{S}^* = \{\{a, c, e\}, \{b, f, h\}, \{d, g, i\}\}$$

SUBSET-SUM

Karlsruher Institut für Technologie

Problem

Gegeben:

- Eine Menge S von Ganzzahlen
- Eine Ganzzahl n.

Frage: Gibt es eine Teilmenge S^*, sodass die Summe der Elemente von S^* gleich n ist?

PARTITION

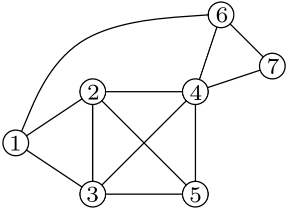
Problem

Gegeben: Eine Menge von natürlichen Zahlen
Frage: Kann man diese Zahlen in zwei Mengen aufteilen, sodass die Summe der Zahlen in den beiden Mengen gleich ist?

Aufgabe

Ein Vertex Cover eines Graphen $G = (V, E)$ ist eine Teilmenge $V' \subseteq V$, so dass jede Kante aus E zu mindestens einem Knoten aus V' inzident ist.
Das Problem VERTEX COVER besteht nun darin, zu entscheiden, ob es für einen Graphen $G = (V, E)$ und einen Parameter $k \leq |V|$ ein Vertex Cover der Größe höchstens k gibt.

1. Finde in folgendem Graphen ein Vertex Cover minimaler Größe:



2. Zeige, dass VERTEX COVER $\mathcal{NP}$-vollständig ist.

Lösungsskizze

Karlsruher Institut für Technologie

VERTEX COVER $\in \mathcal{NP}$**:** Für eine gegebene Menge V' kann in Polyzeit überprüft werden, ob sie eine Teilmenge von V ist und alle Kanten von G zu mindestens einem Knoten aus V' inzident sind.

VERTEX COVER $\mathcal{NP}$**-schwer:** Reduktion von INDEPENDENT SET:

- Gegeben eine Instanz $(G = (V, E), K)$ von INDEPENDENT SET.
- Konstruiere daraus eine Instanz $(G' = G, K' = |V| - K)$ von VERTEX COVER (geht offensichtlich in Polyzeit).
- Behauptung: Es gibt ein Independent Set mit Größe K in G
  $\Leftrightarrow$ Es gibt ein Vertex Cover der Größe $|V| - K$ von G.
- Beweis: $V' \subseteq V$ ist Independent Set der Größe K
  $\Leftrightarrow$ Keine zwei Knoten aus V' sind durch eine Kante verbunden
  $\Leftrightarrow$ Jede Kante ist zu höchstens einem Knoten aus V' inzident
  $\Leftrightarrow$ Jede Kante ist zu mindestens einem Knoten aus $V \setminus V'$ inzident
  $\Leftrightarrow$ $V \setminus V'$ ist ein Vertex Cover von G

Lösungsskizze

Karlsruher Institut für Technologie

VERTEX COVER $\in \mathcal{NP}$: Für eine gegebene Menge V' kann in Polyzeit überprüft werden, ob sie eine Teilmenge von V ist und alle Kanten von G zu mindestens einem Knoten aus V' inzident sind.

VERTEX COVER $\mathcal{NP}$-schwer: Reduktion von INDEPENDENT SET:

- Gegeben eine Instanz $(G = (V, E), K)$ von INDEPENDENT SET.
- Konstruiere daraus eine Instanz $(G' = G, K' = |V| - K)$ von VERTEX COVER (geht offensichtlich in Polyzeit).
- Behauptung: Es gibt ein Independent Set mit Größe K in G
  $\Leftrightarrow$ Es gibt ein Vertex Cover der Größe $|V| - K$ von G.
- Beweis: $V' \subseteq V$ ist Independent Set der Größe K
  $\Leftrightarrow$ Keine zwei Knoten aus V' sind durch eine Kante verbunden
  $\Leftrightarrow$ Jede Kante ist zu höchstens einem Knoten aus V' inzident
  $\Leftrightarrow$ Jede Kante ist zu mindestens einem Knoten aus $V \setminus V'$ inzident
  $\Leftrightarrow$ $V \setminus V'$ ist ein Vertex Cover von G

Lösungsskizze

VERTEX COVER $\in \mathcal{NP}$: Für eine gegebene Menge V' kann in Polyzeit überprüft werden, ob sie eine Teilmenge von V ist und alle Kanten von G zu mindestens einem Knoten aus V' inzident sind.

VERTEX COVER $\mathcal{NP}$-schwer: Reduktion von INDEPENDENT SET:

- Gegeben eine Instanz $(G = (V, E), K)$ von INDEPENDENT SET.
- Konstruiere daraus eine Instanz $(G' = G, K' = |V| - K)$ von VERTEX COVER (geht offensichtlich in Polyzeit).
- Behauptung: Es gibt ein Independent Set mit Größe K in G
  $\Leftrightarrow$ Es gibt ein Vertex Cover der Größe $|V| - K$ von G.
- Beweis: $V' \subseteq V$ ist Independent Set der Größe K
  $\Leftrightarrow$ Keine zwei Knoten aus V' sind durch eine Kante verbunden
  $\Leftrightarrow$ Jede Kante ist zu höchstens einem Knoten aus V' inzident
  $\Leftrightarrow$ Jede Kante ist zu mindestens einem Knoten aus $V \setminus V'$ inzident
  $\Leftrightarrow$ $V \setminus V'$ ist ein Vertex Cover von G

Lösungsskizze

VERTEX COVER $\in \mathcal{NP}$: Für eine gegebene Menge V' kann in Polyzeit überprüft werden, ob sie eine Teilmenge von V ist und alle Kanten von G zu mindestens einem Knoten aus V' inzident sind.

VERTEX COVER $\mathcal{NP}$-schwer: Reduktion von INDEPENDENT SET:

- Gegeben eine Instanz $(G = (V, E), K)$ von INDEPENDENT SET.
- Konstruiere daraus eine Instanz $(G' = G, K' = |V| - K)$ von VERTEX COVER (geht offensichtlich in Polyzeit).
- Behauptung: Es gibt ein Independent Set mit Größe K in G $\Leftrightarrow$ Es gibt ein Vertex Cover der Größe $|V| - K$ von G.
- Beweis: $V' \subseteq V$ ist Independent Set der Größe K
  $\Leftrightarrow$ Keine zwei Knoten aus V' sind durch eine Kante verbunden
  $\Leftrightarrow$ Jede Kante ist zu höchstens einem Knoten aus V' inzident
  $\Leftrightarrow$ Jede Kante ist zu mindestens einem Knoten aus $V \setminus V'$ inzident
  $\Leftrightarrow$ $V \setminus V'$ ist ein Vertex Cover von G

KNAPSACK

Karlsruher Institut für Technologie

Problem

Gegeben: (M, w, c, W, C)

- endliche Menge von Objekten M
- Gewichtsfunktion $w : M \to \mathbb{N}_0$
- Wertfunktion $c : M \to \mathbb{N}_0$
- Maximalgewicht W und Minimalwert $C \in \mathbb{N}_0$

Frage: Existiert eine Teilmenge $M' \subseteq M$ mit

$$\sum_{a \in M'} w(a) \leq W \text{ und } \sum_{a \in M'} c(a) \geq C \text{ ?}$$

Was wären das zugehörige Optimalwertproblem und Optimierungsproblem?

KNAPSACK

Problem

Gegeben: (M, w, c, W, C)

- endliche Menge von Objekten M
- Gewichtsfunktion $w : M \to \mathbb{N}_0$
- Wertfunktion $c : M \to \mathbb{N}_0$
- Maximalgewicht W und Minimalwert $C \in \mathbb{N}_0$

Frage: Existiert eine Teilmenge $M' \subseteq M$ mit

$$\sum_{a \in M'} w(a) \leq W \text{ und } \sum_{a \in M'} c(a) \geq C\ ?$$

Was wären das zugehörige Optimalwertproblem und Optimierungsproblem?

KNAPSACK – Beispiel

Karlsruher Institut für Technologie

Gegeben: Instanz I von KNAPSACK mit $M = i_1, i_2, i_3, i_4$

	i_1	i_2	i_3	i_4
w	10	5	5	8
c	7	10	5	8

- $W = 15$
- $C = 18$

Ist I eine Ja-Instanz?

Lösungsansätze

Orakel

$M' = \{i_2, i_4\}$ ist eine gültige Lösung. I ist somit eine Ja-Instanz.

Exponentieller Ansatz

Teste alle $2^4 = 16$ mögliche Teilmengen $M' \subseteq M$, ob sie die Bedingung erfüllen.

Greedy-Ansatz – nicht immer optimal

Sortiere die Elemente $i \in M$ nach dem Verhältnis $c(i)\,/\,w(i)$. Füge so lange Elemente mit dem besten Verhältnis aller $i \notin M'$ zu M' hinzu, solange $\sum_{i \in M'} w(i) \leq W$ mit dem hinzugefügten Element noch gilt.
Informell: Möglichst wertvolle Dinge einpacken, bis der Rucksack voll ist.

Lösungsansätze

Orakel

$M' = \{i_2, i_4\}$ ist eine gültige Lösung. I ist somit eine Ja-Instanz.

Exponentieller Ansatz

Teste alle $2^4 = 16$ mögliche Teilmengen $M' \subseteq M$, ob sie die Bedingung erfüllen.

Greedy-Ansatz – nicht immer optimal

Sortiere die Elemente $i \in M$ nach dem Verhältnis $c(i)\,/\,w(i)$. Füge so lange Elemente mit dem besten Verhältnis aller $i \notin M'$ zu M' hinzu, solange $\sum_{i \in M'} w(i) \leq W$ mit dem hinzugefügten Element noch gilt.
Informell: Möglichst wertvolle Dinge einpacken, bis der Rucksack voll ist.

Dynamische Programmierung

In $\mathcal{O}(|M|\,W)$!

Aufgabe

Gegeben sei folgende Instanz $I = (M, w, c, W, C)$ von KNAPSACK:

- $M := \{x_1, \ldots, x_7\}$
- Gewichtsfunktion w und die Kostenfunktion c sind durch folgende Tabelle gegeben:

	x_1	x_2	x_3	x_4	x_5	x_6	x_7
w	6	6	5	5	3	4	1
c	8	10	8	8	5	6	2

- Die obere Schranke für das Gewicht sei $W := 12$

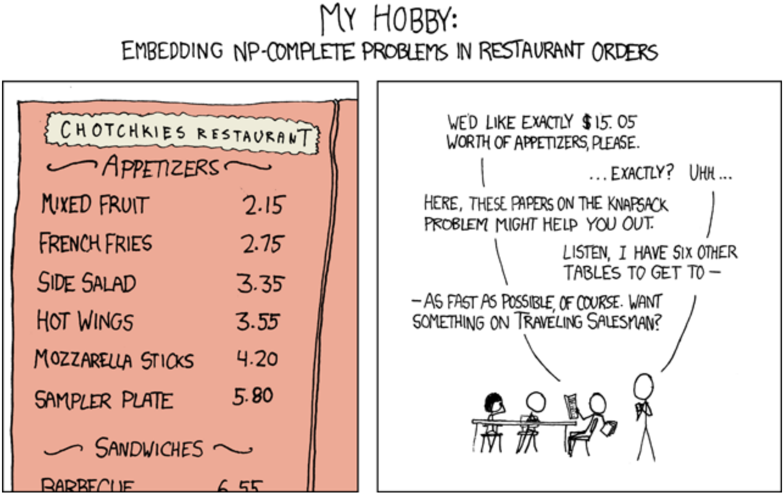
Für welche C ist I eine Ja-Instanz?

Und viele mehr!

Es gibt (sehr) viele Probleme, von denen man weiß, dass sie *NP*-vollständig sind. Es gibt ein „klassisches“ Paper von Richard Karp, in dem 21 Probleme vorgestellt werden, die großteils recht bekannt sind. Wer nicht genug bekommen kann, darf in „Introduction to the Theory of Computation“ von Michael Sipser schauen, dort gibt es sehr viele.

Es kann durchaus nützlich sein zu wissen, dass ein Problem $\mathcal{NP}$-vollständig ist; dann kann man aufhören, nach einem effizienten Algorithmus zu suchen.

Bis zum nächsten Mal!



General solutions get you a 50% tip.

Lizenzen