Definition:

Sei X eine endliche Menge Boolescher Variablen. Eine **Wahrheitsbelegung** für X ist eine Funktion $T : X \to \{\text{true}, \text{false}\}$. Wir erweitern T auf die Menge $L := X \dot{\cup} \{\bar{x} : x \in X\}$ der **Literale** über X, indem wir $T(\bar{x}) := \text{true}$ genau dann setzen, wenn $T(x) = \text{false}$. Eine **Klausel** über X ist eine Menge von Literalen über X. Sie wird von T genau dann **erfüllt**, wenn mindestens eines ihrer Literale durch T auf true gesetzt wird. Eine Familie $\mathcal{Z}$ von Klauseln über X ist genau dann **erfüllbar**, wenn es eine Wahrheitsbelegung gibt, die alle Klauseln in $\mathcal{Z}$ gleichzeitig erfüllt.

Notation: Statt z.B. $\{\{x_1, \bar{x_2}\}, \quad \{\bar{x_1}, x_3\}, \quad \{x_1, x_2, x_3\}\}$ für eine Familie von Klauseln schreibt man $(x_1 \vee \bar{x_2}) \wedge (\bar{x_1} \vee x_3) \wedge (x_1 \vee x_2 \vee x_3)$.

SATISFIBILITY (SAT)

Instanz: Eine Menge X von Variablen und eine Familie $\mathcal{Z}$ von Klauseln über X.
Frage: Ist $\mathcal{Z}$ erfüllbar?

Definition

Ein Entscheidungsproblem $\mathcal{P} = (X, Y)$ ist in NP, wenn es ein Polynom p und ein Entscheidungsproblem $\mathcal{P}' = (X', Y')$ in P gibt, wobei

$$X' := \{x\#c \mid x \in X, c \in \{0,1\}^{\lfloor p(\text{size}(x))\rfloor}\}, \quad \text{so dass}$$

$$Y = \{y \in X \mid \text{ es gibt } c \in \{0,1\}^{\lfloor p(\text{size}(x))\rfloor} \text{ mit } y\#c \in Y'\}.$$

c: Zertifikat für y.

Beispiele für Probleme in NP:

- HAMILTON-KREIS:
  Instanz: Ein ungerichteter Graph G
  Frage: Besitzt G einen Hamilton-Kreis?
- STABILE MENGE:
  Instanz: Ein ungerichteter Graph G und eine ganze Zahl k
  Frage: Besitzt G eine stabile Menge mit k Knoten?
- SATISFIABILITY
  Instanz: Menge X von Variablen und Familie $\mathcal{Z}$ von Klauseln über X.
  Frage: Ist $\mathcal{Z}$ erfüllbar?

Definition

Sei A ein Alphabet und $R \subseteq A^* \times A^*$ ein Berechnungsproblem. Eine R **benutzende Orakel-Turingmaschine** ist (für $N \in \mathbb{Z}_+$) eine Funktion

$$\Phi : \{0, \ldots, N\} \times \bar{A} \times \bar{A} \quad \to \quad \{-2, \ldots, N\} \times \bar{A} \times \bar{A} \times \{-1, 0, 1\} \times \{-1, 0, 1\}$$

Berechnung: wie bei einer 2-Band-T.M., bis auf diese Unterschiede: Anfangs sei $\text{time}^{(0)} := 0$. Wenn $\Phi\left(n^{(i)}, s^{(i)}_{\pi(i)}, t^{(i)}_{\rho(i)}\right) = (-2, \sigma, \tau, \delta, \epsilon)$ in Schritt i, dann sei $x \in A^k$ mit $k := \min\left\{j \in \mathbb{N} \mid t^{(i)}_j = \sqcup\right\} - 1$ und $x_j := t^{(i)}_j$ für $j = 1, \ldots, k$ der String auf Band 2. Falls $x \in X_R$, dann

- überschreibe Band 2 mit $t^{(i+1)}_j = y_j$ für $j = 1, \ldots, \text{size}(y)$ und $t^{(i+1)}_{\text{size}(y)+1} = \sqcup$ für ein $(x, y) \in R$,
- setze $\text{time}^{(i+1)} := \text{time}^{(i)} + 1 + \text{size}(y)$ und $n^{(i+1)} := n^{(i)} + 1$.

Sonst sei $\text{time}^{(i+1)} := \text{time}^{(i)} + 1$. Die Berechnung läuft, bis $n^{(i)} = -1$. Dann sei $\text{time}(\Phi, x) := \text{time}^{(i)}$. Output: wie bei der 2-Band-T.M.

Beweis des Satzes von Cook (I)

Die **Variablenmenge** $V(x)$ enthalte:

- eine Variable $v_{ij\sigma}$ für $i \in \{0, \ldots, Q\}$, $j \in \{-Q, \ldots, Q\}$ und $\sigma \in \bar{A}$:
  Soll genau dann true sein, wenn zur Zeit i an Stelle j des Bandes das Symbol σ steht.
- eine Variable w_{ijn} für $i \in \{0, \ldots, Q\}$, $j \in \{-Q, \ldots, Q\}$ und $n \in \{-1, \ldots, N\}$:
  Soll genau dann true sein, wenn zur Zeit i die Bandposition gleich j ist und $n^{(i)} = n$.

Ziel:

Die Klauselfamilie $\mathcal{Z}(x)$ soll genau dann erfüllbar sein, wenn es einen String c mit $\text{output}(\Phi, x\#c) = 1$ gibt.

Beweis des Satzes von Cook (II)

Klauseln (in Mengenschreibweise):

Die folgenden Mengen sind Klauseln der Familie $\mathcal{Z}(x)$

- Zur Zeit i soll an Bandposition j genau ein Zeichen stehen:
  - $\{v_{ij\sigma} \mid \sigma \in \bar{A}\}$
    für $i \in \{0, \ldots, Q\}$ und $j \in \{-Q, \ldots, Q\}$.
  - $\{\overline{v_{ij\sigma}}, \overline{v_{ij\tau}}\}$
    für $i \in \{0, \ldots, Q\}$, $j \in \{-Q, \ldots, Q\}$ und $\sigma, \tau \in \bar{A}$ mit $\sigma \neq \tau$.

- Zur Zeit i soll genau eine Bandposition j betrachtet werden und genau ein Zustand n angenommen werden:
  - $\{w_{ijn} \mid j \in \{-Q, \ldots, Q\}, n \in \{-1, \ldots, N\}\}$ für $i \in \{0, \ldots, Q\}$.
  - $\{\overline{w_{ijn}}, \overline{w_{ij'n'}}\}$ für $i \in \{0, \ldots, Q\}$, $\{j, j'\} \subseteq \{-Q, \ldots, Q\}$ und $\{n, n'\} \subseteq \{-1, \ldots, N\}$ mit $(j, n) \neq (j', n')$.

Beweis des Satzes von Cook (III)

Weitere Klauseln:

- Die Berechnung beginnt korrekt mit Eingabe $x\#c$ für ein $c \in \{0,1\}^{\lfloor p(\text{size}(x))\rfloor}$
  - $\{v_{0,j,x_j}\}$ für $j \in \{1,\ldots,\text{size}(x)\}$.
  - $\{v_{0,\text{size}(x)+1,\#}\}$.
  - $\{v_{0,\text{size}(x)+1+j,0}, v_{0,\text{size}(x)+1+j,1}\}$ für $j \in \{1,\ldots,\lfloor p(\text{size}(x))\rfloor\}$.
  - $\{v_{0,j,\sqcup}\}$
    für $j \in \{-Q,\ldots,0\}$ und $j \in \{\text{size}(x)+2+\lfloor p(\text{size}(x))\rfloor,\ldots,Q\}$
  - $\{w_{010}\}$

- Die Übergangsfunktion wir korrekt dargestellt:
  - $\{\overline{v_{ij\sigma}}, \overline{w_{ijn}}, v_{i+1,j,\tau}\}$, $\{\overline{v_{ij\sigma}}, \overline{w_{ijn}}, w_{i+1,j+\delta,m}\}$ für $i \in \{0,\ldots,Q\}$, $j \in \{-Q,\ldots,Q\}$, $\sigma \in \bar{A}$, $n \in \{0,\ldots,N\}$, wobei $\Phi(n,\sigma) = (m,\tau,\delta)$

Beweis des Satzes von Cook (IV)

Weitere Klauseln:

- Bei $n^{(i)} = -1$ endet die Berechnung:
  - $\{\overline{w_{i,j,-1}}, w_{i+1,j,-1}\}$, $\{\overline{w_{i,j,-1}}, \overline{v_{i,j,\sigma}}, v_{i+1,j,\sigma}\}$
    für $i \in \{0, \ldots, Q-1\}$, $j \in \{-Q, \ldots, Q\}$ and $\sigma \in \bar{A}$.
- Ungescannte Bandpositionen bleiben unverändert:
  - $\{\overline{v_{ij\sigma}}, \overline{w_{ij'n}}, v_{i+1,j,\sigma}\}$
    für $i \in \{0, \ldots, Q-1\}$, $\sigma \in \bar{A}$, $n \in \{-1, \ldots, N\}$ und
    $\{j, j'\} \subseteq \{-Q, \ldots, Q\}$ mit $j \neq j'$.
- Die Ausgabe ist 1:
  - $\{v_{Q,1,1}\}$, $\{v_{Q,2,\sqcup}\}$