

verlassen).

Sei $x = x_1, \dots, x_n \in \Sigma^*$ die Eingabe von M .

Konstruktion einer Formel F mit

$$x \in L \Leftrightarrow F \text{ ist erfüllbar.}$$

Sei $\Gamma = \{a_1, \dots, a_l\}$ das Anfangsalphabet

$Z = \{z_1, \dots, z_k\}$ die Zustandsmenge von M

F enthält folgende Variable:

Variable	Indizes	intendierte Bedeutung
$zust_{t,z}$	$t = 0, \dots, p(n)$ $z \in Z$	$zust_{t,z} = 1 \Leftrightarrow$ nach t Schritten befindet sich M im Zustand z
$pos_{t,i}$	$t = 0, \dots, p(n)$ $i = -p(n), \dots, p(n)$	$pos_{t,i} = 1 \Leftrightarrow$ M 's Schreib-Lesekopf befindet sich nach t Schritten auf Position i
$band_{t,i,a}$	$t = 0, \dots, p(n)$ $i = -p(n), \dots, p(n)$ $a \in \Gamma$	$band_{t,i,a} = 1 \Leftrightarrow$ nach t Schritten befindet sich auf Bandposition i das Zeichen a

F besteht aus mehreren Bauteilen:

$$G(x_1, \dots, x_m) = 1 \Leftrightarrow \text{für genau ein } i \text{ ist } x_i = 1.$$

Behauptung

G existiert und es gilt $size(G) = O(m^2)$.

Beweis.

$$G = \left(\bigvee_{i=1}^k x_i \right) \wedge \left(\bigwedge_{j=1}^{m-1} \bigwedge_{l=j+1}^m (\neg(x_j \wedge x_l)) \right)$$

Die erste Teilformel wird genau dann wahr, wenn mindestens eine Variable wahr ist.

Die zweite Teilformel wird genau dann wahr, wenn höchstens eine Variable wahr wird.

$$F = R \wedge A \wedge \ddot{U}_1 \wedge \ddot{U}_2 \wedge E, \text{ wobei}$$

R für Randbedingung

A für Anfangsbedingung

$\ddot{U}_1, \ddot{U}_2$ für Übergangsbedingung und

E für Endbedingung steht.

R drückt aus:

- Zu jedem Zeitpunkt t ergibt sich für genau ein z $zust_{t,z} = 1$.
- Zu jedem Zeitpunkt t gibt es genau eine Bandposition i mit $pos_{t,i} = 1$.
- Zu jedem Zeitpunkt t und jeder Bandposition i gibt es genau ein a mit $band_{t,i,a} = 1$

$$R = \bigwedge_t [G(zust_{t,z_1}, \dots, zust_{t,z_k}) \wedge G(pos_{t,-p(n)}, \dots, pos_{t,p(n)}) \wedge \bigwedge_i G(band_{t,i,a_1}, \dots, band_{t,i,a_l})]$$

A beschreibt den Status der Variablen für den Fall $t = 0$:

$$A = zust_{0,z_0} \wedge pos_{0,1} \wedge \bigwedge_{j=1}^n band_{0,j,x_j} \wedge \bigwedge_{j=-p(n)}^0 band_{0,j,\square} \wedge \bigwedge_{j=n+1}^{p(n)} band_{0,j,\square}$$

$\ddot{U}_1$ beschreibt den Übergang von Zeitpunkt t nach $t + 1$ an der Kopfposition ($y \in \{-1, 0, +1\}$):

$$\ddot{U}_1 = \bigwedge_{t,z,i,a} [(zust_{t,z} \wedge pos_{t,i} \wedge band_{t,i,a}) \rightarrow \bigvee_{z',a',y} \text{mit } \delta(z,a) \ni (z',a',y) (zust_{t+1,z'} \wedge pos_{t+1,i+y} \wedge band_{t+1,i,a'})]$$

$\ddot{U}_2$ besagt, daß auf den übrigen Bandfeldern nichts passiert:

$$\ddot{U}_2 = \bigwedge_{t,i,a} ((\neg pos_{t,i} \wedge band_{t,i,a}) \rightarrow band_{t+1,i,a})$$

E überprüft, ob der Endzustand erreicht ist (wird auf jeden Fall im Zeitpunkt $p(n)$ erreicht):

$$E = \bigvee_{z \in E} zust_{p(n),z}$$

($\rightarrow$): Sei $x \in L$

$\Rightarrow \exists$ nichtdeterministische Rechnung der Länge $p(n)$, die in einen Endzustand führt.

$\Rightarrow$ Alle Teilformeln von F erhalten den Wert 1.

$\Rightarrow F(x)$ erhält den Wert 1.

$\Rightarrow F(x)$ ist erfüllbar.

($\leftarrow$): Sei $F(x)$ erfüllbar.

$\Rightarrow \exists$ Belegung, die F und alle Teilformeln den Wert 1 annehmen läßt.

Insbesondere ist R erfüllt:

$\Rightarrow zust_{t,z}, pos_{t,i}, band_{t,i,a}$ können $\forall t$ als Konfiguration von M interpretiert werden.

Insbesondere ist A erfüllt:

für $t = 0$ kann aus den Variablenwerten die Startkonfiguration von M abgelesen werden.

Insbesondere sind $\ddot{U}_1, \ddot{U}_2$ erfüllt:

$\Rightarrow$ zwischen t und $t + 1$ ist die Nachfolgekonditionsbedingung erfüllt.

$\Rightarrow \forall t = 0, 1, 2, \dots$ ist eine mögliche nichtdeterministische Rechnung beschrieben.

Insbesondere ist E erfüllt:

$\Rightarrow$ Rechnung erreicht Endzustand.

Insgesamt gilt also :

$$x \in L(M)$$

Noch zu zeigen: F ist in polynomieller Zeit berechenbar:

Offenbar ist der Aufwand zur Erzeugung von F linear in der Länge von F .

$$\text{Wegen } |R| = O(n^2)$$

$$|A| = O(n)$$

$$|\ddot{U}_1| = O(n^2)$$

$$|\ddot{U}_2| = O(n^2)$$

$$|E| = O(1)$$

$$\text{gilt } |F| = O(n^2)$$

■

NP-Berechnungen: "guess and check"

Alle deterministischen Algorithmen zur Berechnung von SAT haben Komplexität $2^{O(n)}$.

(Z.B. systematisches Durchprobieren aller Eingabeformeln).

Da SAT NP-hart ist folgt:

$$NP \subseteq \bigcup_{p \text{ Polynom}} TIME(2^{p(n)})$$

2.4 Weitere NP-vollständige Probleme

2.4.1 3SAT

Definition. (3SAT)

Gegeben: Boolesche Formel F in KNF mit höchstens 3 Literalen pro Klausel.

Gefragt: Ist F erfüllbar?

Satz.

3SAT ist NP-vollständig.

Beweis. 1.) $3SAT \in NP$, klar mit “guess and check”-Argument.

2.) 3SAT NP-hart.

Es reicht zu zeigen : $SAT \leq_p 3SAT$.

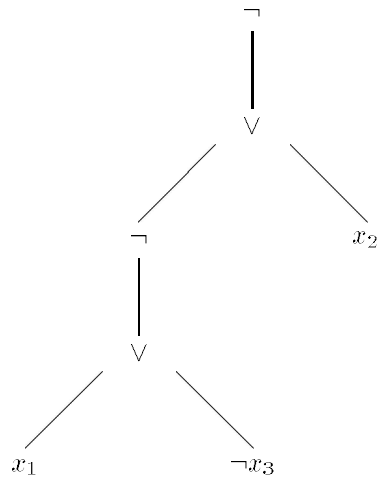
Angabe eines polynomiellen Verfahrens, das eine beliebige Formel F in eine Formel F' in KNF mit höchstens 3 Literalen pro Klausel umformt mit:

$$F \text{ erfüllbar} \Leftrightarrow F' \text{ erfüllbar.}$$

(Dabei genügt “Erfüllbarkeitsäquivalenz”. “Äquivalenz ist nicht notwendig.)

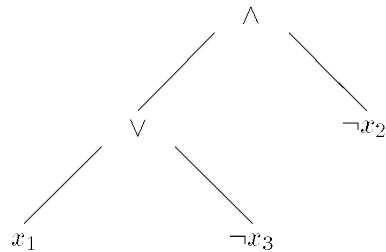
Allgemeine Verfahren zur Überführung von F in äquivalente KNF benötigt i.a. exponentielle Zeit und garantiert nicht, daß alle Klauseln höchstens 3 Literale enthalten.

Erläuterung des Verfahrens am Beispiel:

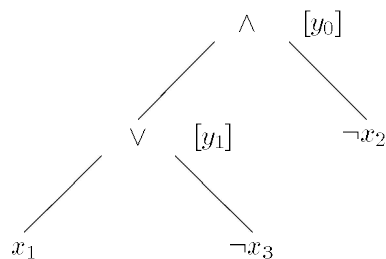


1. Schritt

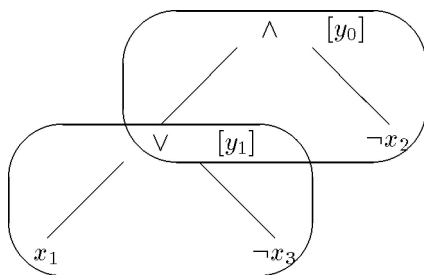
Mit den DeMorgan'schen Regeln werden alle Negationszeichen zu den Variablen gebracht.

2. Schritt

Jedem inneren Knoten wird eine Variable $\{y_0, y_1, \dots\}$ zugeordnet, wobei der Baumwurzel y_0 zugeordnet wird.

3. Schritt

Jedem inneren Knoten wird eine Teilformel der Form $(v \leftrightarrow (y \circ z))$, $\circ \in \{\wedge, \vee\}$ zugeordnet. Man erhält eine neue Formel F_1 , indem man alle Teilformeln durch $\wedge$ verknüpft und für die Wurzel y_0 die Teilformel $[y_0]$ hinzunimmt.



Es gilt:

$$F \text{ erfüllbar} \Leftrightarrow F_1 \text{ erfüllbar}$$

$(\rightarrow)$: Eine erfüllende Belegung von F liefert eine erfüllende Belegung von F_1 .
 $(\leftarrow)$: Die Belegung der x -Variablen einer erfüllenden Belegung von F_1 liefert eine erfüllende Belegung für F .

4. Schritt

Umformung jeder Teilformel in KNF.

Es entstehen Klauseln mit höchstens 3 Literalen.

Das Verfahren ist polynomial, da jede Teilformel in konstanter Länge umgeformt werden kann.

Beispiel $[a \rightarrow (b \vee c)] \mapsto (a \vee \neg b) \wedge (\neg a \vee b \vee c) \wedge (a \vee \neg c)$
 $[a \leftarrow (b \wedge c)] \mapsto (\neg a \vee b) \wedge (\neg a \vee c) \wedge (a \vee \neg b \vee \neg c)$

$\Rightarrow F_1 = y_0 \wedge (\neg y_0 \vee y_1) \wedge (\neg y_0 \vee \neg x_2) \wedge (y_0 \vee \neg y_1 \vee x_2) \wedge (y_1 \vee \neg x_1) \wedge (\neg y_1 \vee x_1 \vee \neg x_3) \wedge (y_1 \vee x_3)$

mit

F_1 ist erfüllbarkeitsäquivalent mit F .

Umformung von F in F_1 ist in polynomialer Zeit möglich. ■

Bemerkung

Für ein analoges Problem gilt:

$2SAT \in P$, da es nur polynomial viele verschiedene Klauseln mit höchstens 2 Literalen über $\{x_1, \dots, x_n\}$ gibt.

2.4.2 CLIQUE

Definition. (CLIQUE)

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

Gefragt: Besitzt G eine "Clique" der Größe k ?

Wobei Clique ein vollständiger Teilgraph $G' = (V', E')$ ist, mit

$$(u, v) \in E' \quad \forall u, v \in V', \quad u \neq v$$

Satz.

CLIQUE ist NP-vollständig.

Beweis.

1.) CLIQUE $\in NP$ mit "guess and check".

2.) CLIQUE ist NP-hart.

Sei F Formel in KNF mit (genau) 3 Literalen pro Klausel.

$F = (z_{1,1} \vee z_{1,2} \vee z_{1,3}) \wedge \dots \wedge (z_{m,1} \vee z_{m,2} \vee z_{m,3})$ mit $z_{i,j} \in \{x_1, x_2, \dots\} \wedge \{\neg x_1, \neg x_2, \dots\}$