Aussagenlogik: Syntax

Aussagenlogische Formeln über einer Menge X von Variablen sind induktiv definiert:

- jede Variable $x \in X$ ist eine Formel
- ist F eine Formel, dann auch $\neg F$
- sind F und G Formeln, dann auch $(F \wedge G)$
- sind F und G Formeln, dann auch $(F \vee G)$

Aussagenlogik ist die einfachste Form der Logik, die sich nur mit der logischen Verknüpfung von Elementaraussagen, die wahr oder falsch sein können, befasst.

Wir betrachten hier nur die Verknüpfungen Negation $\neg$, Konjunktion $\wedge$ und Diskunktion $\vee$. Man kann aber zeigen, dass sich alle möglichen logischen Verknüpfungen aus diesen zusammensetzen lassen. So ist z.B. die Implikation $F \rightarrow G$ definierbar als $\neg F \vee G$.

Aussagenlogik dient auch der Beschreibung von digitalen Schaltkreisen.

Aussagenlogik: Semantik

Für eine Bewertung $\alpha : X \to \{0, 1\}$ der Variablen X wird induktiv der Wert $\alpha(F)$ einer Formel F definiert:

- $\alpha(x)$ ist durch α gegeben
- $\alpha(\neg F) = 1 - \alpha(F)$
- $\alpha(F \wedge G) = \min(\alpha(F), \alpha(G))$
- $\alpha(F \vee G) = \max(\alpha(F), \alpha(G))$

Definition: α erfüllt F, wenn $\alpha(F) = 1$ ist.

Man schreibt dafür auch $\alpha \models F$

F ist Tautologie, wenn $\alpha \models F$ für alle α gilt.

F ist erfüllbar, wenn es eine Bewertung α gibt mit $\alpha \models F$.

Für eine Bewerung der Variablen mit Wahrheitswerten, wobei 1 als "wahr" und 0 als "falsch" interpretiert wird, lässt sich der Wahrheitswert einer zusammengesetzten Formel gemäß der angegebenen Regeln ausrechnen, die dem intuitiven Verständnis der Bedeutung der Verknüpfungen entsprechen.

Eine Bewertung erfüllt eine Formel, wenn diese mir den gegebene Werten für die Variablen wahr wird. Ist eine Formel unabhängig von der Bewertung der Variablen immer wahr, wie z.B. $F \vee \neg F$, dann heißt sie *Tautologie*.

Eine Formel F ist genau dann erfüllbar, wenn ihre Negation $\neg F$ keine Tautologie ist.

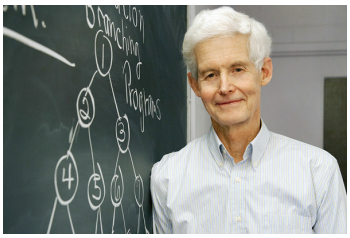
Das Erfüllbarkeitsproblem

Problem SAT

Instanz:	aussagenlogische Formel F
Frage:	Ist F erfüllbar ?

Theorem

SAT ist NP-vollständig.



Stephen A. Cook hat den Begriff der NP-Vollständigkeit entdeckt, und SAT als erstes NP-vollständiges Problem nachgewiesen.

Photo ©University of Toronto

Das Problem SAT war das erste, das als NP-Vollständig erkannt wurde. Ausgehend davon wurden in der Folge zahlreiche Probleme durch Reduktion als NP-vollständig nachgewiesen. Heute sind Tausende von NP-vollständigen Problemen aus allen Bereichen der Informatik bekannt.

Für seine Arbeiten zur NP-Vollständigkeit erhielt Stephen Cook 1982 den Turing-Award.

NP-Vollständigkeit von SAT

SAT ist in NP: F erfüllbar gdw $\exists \alpha : \alpha \models F$
$\alpha \models F$ kann in Zeit $O(|F|)$ geprüft werden.

SAT ist NP-schwer: Sei A in NP, wir werden zeigen $A \leq_P$ SAT.

Sei M eine DTM, die R_A entscheidet, und $p()$ und $q()$ Polynome, so dass für w mit $|w| = n$:

- jede Berechnung von M hält nach $p(n)$ Schritten.
- es gibt ein Zertifikat z mit $|z| \leq q(n)$ gdw. $x \in A$

Konstruiere Formel $F_{M,w}$ so dass $F_{M,w}$ erfüllbar ist gdw.
es ein Zertifikat z gibt, für das die Berechnung von M bei Eingabe w und z im Endzustand hält.

$F_{M,w}$ wird in Zeit $O(p(|w|)^2)$ aus w berechnet.

Um zu zeigen, dass SAT NP-vollständig ist, muss ein beliebiges Problem A in NP auf SAT polynomiell reduziert werden. Die einzige Information, die über A zur Verfügung steht, ist die Charakterisierung mittels Existenz von Zertifikaten, und dass R_A von einer DTM in polynomieller Zeit erkannt wird. Daher muss die Reduktion ausgehend von dieser Maschine konstruiert werden.

Konstruktion der Formel $F_{M,w}$

Sei $w = a_1 \dots a_n$ und $\ell := q(n)$, $t := p(n)$.

Berechnung von M hat $t+1$ Konfigurationen

$$K_0 , K_1 , \dots , K_t .$$

Jede Konfiguration K_i hat $t+1$ Symbole

$$a_{i,0} , a_{i,1} , \dots , a_{i,t} .$$

Variablen sind $z_1, \dots, z_\ell$ für das Zertifikat,

sowie für $i, j \leq t$, $q \in Q$ und $b \in \Gamma$

- $x_{i,j,b}$ mit der Bedeutung $a_{i,j} = b$
- $x_{i,j,q}$ mit der Bedeutung $a_{i,j} = q$

Für jede Eingabe w mit $|w| = n$ hält die Berechnung von M nach höchstens $t = p(n)$ Schritten, also hat jede Berechnung höchstens $t+1$ Konfigurationen. Falls die Berechnung nach weniger als t Schritten hält wird die letzte Konfiguration einfach wiederholt, dass genau sie genau $t+1$ Konfigurationen hat

Jede Konfiguration kann auch höchstens $t+1$ Symbole (Bandsymbole oder Zustand) enthalten. In der Beschreibung wird jede Konfiguration mit Leerzeichen aufgefüllt, so dass sie genau die Länge $t+1$ hat.

Die Variablen, aus denen die Formel aufgebaut wird, dienen der Beschreibung der Konfigurationen in der Berechnung: für jede Konfiguration i und Stelle j in der Konfiguration gibt es $|\Gamma| + 1$ viele Variablen, von denen genau eine wahr ist, je nachdem was an dieser Stelle der Konfiguration steht.

Konstruktion der Formel $F_{M,w}$

Die Formel $F_{M,w}$ ist $\quad S \wedge \bigwedge_{i=1}^{t} N_i \wedge E$, wobei

- S drückt aus, dass K_0 richtige Startkonfiguration ist,
- E drückt aus, dass K_t im Endzustand ist
- N_i drückt aus, dass $K_{i-1} \vdash_M K_i$,
  oder K_{i-1} ist Haltekonfiguration und $K_{i-1} = K_i$.

$$
\begin{aligned}
S \;:= {} & x_{0,0,q_0} \wedge x_{0,1,a_1} \wedge \ldots \wedge x_{0,n,a_n} \wedge x_{0,n+1,\#} \\
& \wedge \bigwedge_{1 \le i \le \ell} \big((x_{0,n+i+1,0} \wedge \neg z_i) \vee (x_{0,n+i+1,1} \wedge z_i) \big) \\
& \wedge x_{0,n+\ell+2,\square} \wedge \ldots \wedge x_{0,t,\square}
\end{aligned}
$$

E ist $\quad \bigvee_{q \in F} E_q \quad$ wobei $\quad E_q = x_{t,0,q} \vee \ldots \vee x_{t,t,q}$

Die Formel S sagt dass K_0 die Anfangskonfiguration $q_0 w \# z$ ist. Die Formel E drückt aus, dass in der letzten Konfiguration K_t ein Endzustand vorkommt.

Die Formeln N_i, die die Übergänge von M von einer Konfiguration in die nächste beschreiben, werden auf den nächsten zwei Folien beschrieben.

Konstruktion der Formel N_i

Die Formel N_i ist $\bigwedge_{j \leq t} (A_{i,j} \vee B_{i,j})$, wobei

- $A_{i,j}$ drückt aus, wie $a_{i,j}$ von $a_{i-1,j-1}a_{i-1,j}a_{i-1,j+1}$ abhängt, wobei eines davon der Zustand in K_{i-1} ist.
- $B_{i,j}$ sagt: der Zustand in K_{i-1} ist so weit von $a_{i-1,j}$ entfernt, dass $a_{i,j} = a_{i-1,j}$.

$B_{i,j}$ ist:

$$\bigvee_{a \in \Gamma} x_{i-1,j-1,a} \wedge \bigvee_{a \in \Gamma} x_{i-1,j+1,a} \wedge \bigvee_{a \in \Gamma} (x_{i-1,j,a} \wedge x_{i,j,a})$$

Konstruktion der Formel N_i

Theorie für MI

Die Klassen P und NP
NP-Vollständige Probleme
Aussagenlogik
NP-Vollständigkeit von SAT
Spezialfälle von SAT
Weitere NP-vollständige Probleme

$A_{i,j}$ ist eine Disjunktion von Teilformeln, die jeweils $a_{i,j}$ für eine Kopfposition $j-1$, j oder $j+1$ in K_{i-1} und einen Übergang von M beschreiben.

Ist z.B. $\delta(q, a) = (p, b, R)$, dann enthält $A_{i,j}$ die Teilformeln

$$x_{i-1,j-1,q} \wedge x_{i-1,j,a} \wedge x_{i,j-1,b} \wedge x_{i,j,p} \wedge \bigvee_{a \in \Gamma} (x_{i-1,j+1,a} \wedge x_{i,j+1,a})$$

$$\bigvee_{a \in \Gamma} (x_{i-1,j-1,a} \wedge x_{i,j-1,a}) \wedge x_{i-1,j,q} \wedge x_{i-1,j+1,a} \wedge x_{i,j,b} \wedge x_{i,j+1,p}$$

Ist $\delta(q, a) = (p', b, L)$, dann enthält $A(i, j)$ auch die Teilformel

$$\bigvee_{a \in \Gamma} (x_{i-1,j,a} \wedge x_{i,j+1,a}) \wedge x_{i-1,j+1,q} \wedge x_{i-1,j+2,a} \wedge x_{i,j,p'} \wedge x_{i,j+2,b}$$

Konjunktive Normalform

- Ein Literal a ist eine Variable x oder negierte Variable $\neg x$. Abkürzung: $\bar{x}$ statt $\neg x$.
- Eine Klausel ist eine Disjunktion $C = a_1 \vee \ldots \vee a_k$ von Literalen.
- Eine Formel in KNF ist eine Konjunktion $F = C_1 \wedge \ldots C_m$ von Klauseln.
- Eine Formel in KNF ist in k-KNF, wenn jede Klausel höchstens k Literale enthät.

KNF-SAT ist das Problem SAT für Formeln in KNF

k-SAT ist das Problem SAT für Formeln in k-KNF

Die Erfülltheit von Formeln in KNF ist besonders einfach zu definieren: α erfüllt F, genau dann wenn α jede Klausel in F erfüllt, und eine Klausel ist genau dann erfüllt, wenn α mindestens eines der Literale darin zu 1 macht. Diese einfache Struktur erlaubt es, KNF-SAT oder 3-SAT auf viele Probleme zu reduzieren.

NP-Vollständigkeit

Für eine Formel F konstruiere Formel $E(F)$ mit:

- $E(F)$ ist in 3-KNF
- $|E(F)| \leq O(|F|)$
- $E(F)$ ist erfüllbar gdw. F erfüllbar ist.

E ist polynomielle Reduktion von SAT auf 3-SAT:

Theorem

$SAT \leq_P$ 3-SAT

Also sind KNF-SAT und k-SAT für $k \geq 3$ NP-vollständig.

Dagegen ist 2-SAT in P.

Da jede Formel in 3-KNF auch in k-KNF für jedes $k \geq 3$, und insbesondere in KNF ist, ist E auch eine Reduktion von SAT auf k-SAT und auf KNF-SAT. Daher sind auch diese allgemeineren Spezialfälle von SAT NP-vollständig.

Konstruktion der Formel $E(F)$

Für jede Teilformel G von F neue Variable y_G, und definierende Formeln D_G:

- $G = a$ Literal:

$$\begin{aligned} D_a &= (y_a \leftrightarrow a) = (y_a \rightarrow a) \wedge (a \rightarrow y_a) \\ &= (\bar{y}_a \vee a) \wedge (\bar{a} \vee y_a) \end{aligned}$$

- $G = \neg H$ Negation:

$$\begin{aligned} D_{\neg H} &= (y_{\neg H} \leftrightarrow \bar{y}_H) = (y_{\neg H} \rightarrow \bar{y}_H) \wedge (\bar{y}_H \rightarrow y_{\neg H}) \\ &= (\bar{y}_{\neg H} \vee \bar{y}_H) \wedge (y_H \vee y_{\neg H}) \end{aligned}$$

Die definierenden Formeln D_G stellen sicher, dass in jeder erfüllenden Bewertung die Variable y_G denselben Wert bekommen muss, den die Formel G unter dieser Bewertung hat.

Die Äquivalenzen verwenden die Tatsache, dass eine Implikation $F \rightarrow G$ äquivalent ist zu $\neg F \vee G$.

Konstruktion der Formel $E(F)$

- $G = H_1 \vee H_2$ Disjunktion:

$$\begin{aligned} D_G &= (y_G \leftrightarrow (y_{H_1} \vee y_{H_2})) \\ &= (\bar{y}_G \vee y_{H_1} \vee y_{H_2}) \wedge (\bar{y}_{H_1} \vee y_G) \wedge (\bar{y}_{H_2} \vee y_G) \end{aligned}$$

- $G = H_1 \wedge H_2$ Konjunktion:

$$\begin{aligned} D_G &= (y_G \leftrightarrow (y_{H_1} \wedge y_{H_2})) \\ &= (\bar{y}_G \vee y_{H_1}) \wedge (\bar{y}_G \vee y_{H_2}) \wedge (\bar{y}_{H_1} \vee \bar{y}_{H_2} \vee y_G) \end{aligned}$$

$$E(F) = y_F \wedge \bigwedge_{G \text{ Teilformel von } F} D_G$$

Hier wird für die Äquivalenzen neben der oben genannten Tatsache noch die Regel von DeMorgan $\neg(F \wedge G) = (\neg F \vee \neg G)$ und das Distributivgesetz verwendet.

$E(F)$ ist offensichtlich in 3-KNF und von der Größenordnung $O(|F|)$. Bleibt zu zeigen, dass $E(F)$ genau dann erfüllbar ist, wenn F erfüllbar ist.

Sei also $\alpha \models F$, dann setzen wir α zu einer Belegung α^* der Variablen von $E(F)$ fort mittels $\alpha^*(y_G) := \alpha(G)$. Dann ist leicht zu sehen, dass die Formeln D_G alle erfüllt sind, und da $\alpha(F) = 1$ ist, ist auch $\alpha^*(y_F) = 1$, somit ist jede Klausel in $E(F)$ erfüllt.

Ist andererseits $\beta \models E(F)$, dann definiere β' als die Einschränkung von β auf die Variablen von F. Durch Induktion über den Formelaufbau zeigt man leicht, dass wegen der Erfülltheit der Formeln D_G für jede Teilformal G von F gilt: $\beta(y_G) = \beta'(G)$. Also muss auch $\beta'(F) = 1$ sein, somit $\beta' \models F$.