Vorbemerkungen

if $(x > 7)$ $y = 0$; *else* $y = 1$;

Wenn der Mond ein grüner Käse ist, dann fressen alle Bananen graue Elefanten.

$q(1) = 1$,
$q(i) = q(i-1) + 2i - 1$ für $i \geq 2$
Welchen Wert hat $q(6)$?

24 ist durch 2 teilbar.	Wenn 24 durch 2 teilbar ist
24 ist durch 3 teilbar.	und 24 durch 3 teilbar ist,
24 ist durch 6 teilbar.	so ist 24 durch 6 teilbar.

Literatur

U. Schöning: Logik für Informatiker. Reihe Informatik, Bd. 56, BI-Wissenschaftsverlag, Mannheim, 1989.

J. Kelly: Logik (im Klartext). Pearson Studium, München, 2003.

B. Heinemann / K. Weihrauch: Logik für Informatiker. Teubner-Verlag, Stuttgart, 1992.

E. Börger: Berechenbarkeit, Komplexität, Logik. Vieweg-Verlag, Braunschweig, 1985.

D. Gabbay: Elementary Logics: A Procedural Perspective. Prentice Hall Europe, 1998.

Aussagen

Eine Aussage ist ein sprachliches oder gedankliches Gebilde, dem genau einer der beiden Wahrheitswerte *wahr* oder *falsch* zukommt.

Prinzip der Zweiwertigkeit: Jede Aussage ist wahr oder falsch.

Prinzip vom ausgeschlossenen Widerspruch: Es gibt keine Aussage, die sowohl wahr als auch falsch ist.

Die Sonne kreist um die Erde.

Heute ist schönes Wetter.

x ist eine Primzahl.

Es gibt unendlich viele Primzahlzwillinge.

Wörter

Alphabet — nichtleere Menge
Buchstabe — Element eines Alphabets

Wort (über V) — Folge von Buchstaben (aus V)

V^* (bzw. V^+) — Menge aller (nichtleeren) Wörter über V

Produkt (Katenation) von Wörter — Hintereinanderschreiben von Wörtern

v Teilwort von w — $w = x_1 v x_2$ für gewisse $x_1, x_2 \in V^*$
v Anfangsstück von w — $w = vx$ für ein gewisses $x \in V^*$

$\#_a(w)$ — Anzahl der Vorkommen des Buchstaben a im Wort w

$|w| = \sum_{a \in V} \#_a(w)$ — Länge des Wortes $w \in V^*$

Aussagenlogischer Ausdruck - Definition

Alphabet $V = \{(,),\neg,\wedge,\vee,\rightarrow,\leftrightarrow\} \cup \underbrace{\{p_1,p_2,p_3,\ldots,p_n,\ldots\}}_{var}$

Definition: i) Jede Variable p_i, $i \in \mathbf{N}$, ist ein aussagenlogischer Ausdruck über V.

ii) Sind A und B aussagenlogische Ausdrücke über V, so sind auch

$$\neg A,\ (A \wedge B),\ (A \vee B),\ (A \rightarrow B),\ (A \leftrightarrow B)$$

aussagenlogische Ausdrücke über V.

iii) Ein Wort über V ist nur dann ein aussagenlogischer Ausdruck über V, falls dies aufgrund endlich oftmaliger Anwendung von i) und ii) der Fall ist.

Aussagenlogischer Ausdruck - Beispiele

a) $((p_3 \vee \neg p_1) \rightarrow (p_2 \leftrightarrow p_3))$ — ja

b) $\neg\neg\neg p_1$ — ja

c) $\neg p_1 \vee p_2$ — nein

d) $(\rightarrow p_1)$ — nein

Definition: Ein aussagenlogischer Ausdruck heißt <u>Literal</u>, falls er die Form p_i oder $\neg p_i$ für ein $i \in \mathbf{N}$ hat.

Aussagenlogischer Ausdruck - Charakterisierung

Satz: Ein Wort A ist genau dann ein aussagenlogischer Ausdruck über V, wenn es die folgenden fünf Bedingungen (gleichzeitig) erfüllt:

1. Das Wort A beginnt mit einer Variablen oder mit $\neg$ oder mit $($.
2. Auf eine Variable oder $)$ folgt in A das Symbol $)$ oder ein Element aus $\{\wedge, \vee, \rightarrow, \leftrightarrow\}$, oder die Variable bzw. $)$ ist das letzte Symbol des Wortes.
3. Auf ein Element aus $\{(, \neg, \wedge, \vee, \rightarrow, \leftrightarrow\}$ folgt in A eine Variable oder $\neg$ oder $($.
4. $\#_((A) = \#_)(A) = \#_{\{\wedge,\vee,\rightarrow,\leftrightarrow\}}(A)$.
5. Für jede Stelle in A, an der $($ steht, d.h. $A = W(W'$, gibt es ein Wort B mit folgenden Eigenschaften:
   – $A = W(BW''$,
   – für jedes echte Anfangsstück U von $(B$ gilt $\#_((U) \neq \#_)(U)$,
   – $\#_(((B) = \#_)((B) = \#_{\{\wedge,\vee,\rightarrow,\leftrightarrow\}}((B)$.

Aussagenlogischer Ausdruck - Wertberechnung

Definition. Eine Belegung ist eine Funktion $\alpha : var \rightarrow \{0,1\}$

Definition: Der Wert $w_\alpha(C)$ eines aussalogischen Ausdruck C unter der Belegung α ist induktiv wie folgt definiert:

– Ist $C = p_i$ für eine Variable p_i, $i \in \mathbf{N}_0$, so gilt $w_\alpha(p_i) = \alpha(p_i)$.
– Ist $C = \neg A$, so gilt $w_\alpha(\neg A) = 0$ genau dann, wenn $w_\alpha(A) = 1$ gilt.
– Ist $C = (A \wedge B)$, so gilt $w_\alpha((A \wedge B)) = 1$ genau dann, wenn $w_\alpha(A) = w_\alpha(B) = 1$ gilt.
– Ist $C = (A \vee B)$, so gilt $w_\alpha((A \vee B)) = 0$ genau dann, wenn $w_\alpha(A) = w_\alpha(B) = 0$ gilt.
– Ist $C = (A \rightarrow B)$, so gilt $w_\alpha((A \rightarrow B)) = 0$ genau dann, wenn $w_\alpha(A) = 1$ und $w_\alpha(B) = 0$ gelten.
– Ist $C = (A \leftrightarrow B)$, so gilt $w_\alpha((A \leftrightarrow B)) = 1$ genau dann, wenn $w_\alpha(A) = w_\alpha(B)$ gilt.

Boolesche Funktion

Definition: Sei $n \in \mathbf{N}$. Unter einer n-stelligen Booleschen Funktion f verstehen wir eine Funktion von $\{0,1\}^n$ in $\{0,1\}$.

Beispiel:

x_1	x_2	x_3	b
0	0	0	1
0	0	1	0
0	1	0	1
0	1	1	1
1	0	0	0
1	0	1	1
1	1	0	0
1	1	1	1

Satz: Für $n \in \mathbf{N}$ gibt es 2^{2^n} Boolesche Funktionen.

Ausdruck versus Funktion I

Definition: Sei A ein aussagenlogischer Ausdruck A mit $var(A) \subseteq \{p_1, p_2, \ldots, p_n\}$. Die von A induzierte n-stellige Boolesche Funktion $f_{A,n}$ ist durch

$$f_{A,n}(x_1, x_2, \ldots, x_n) = w_\alpha(A) \text{ mit } \alpha(p_i) = x_i \text{ für } 1 \leq i \leq n$$

definiert.

x_1	x_2	$f_{(p_1 \wedge p_2)}(\underline{x})$	$f_{(p_1 \vee p_2)}(\underline{x})$	$f_{(p_1 \rightarrow p_2)}(\underline{x})$	$f_{(p_1 \leftrightarrow p_2)}(\underline{x})$
0	0	0	0	1	1
0	1	0	1	1	0
1	0	0	1	0	0
1	1	1	1	1	1

Ausdruck versus Funktion II

$A = ((p_3 \vee \neg p_1) \rightarrow (p_2 \leftrightarrow p_3))$

$B = \neg p_1,\ C(p_3 \vee B),\ D = (p_2 \leftrightarrow p_3)$ und $A = (C \rightarrow D)$

$x_1 = \alpha(p_1)$	$x_2 = \alpha(p_2)$	$x_3 = \alpha(p_3)$	$w_\alpha(B)$	$w_\alpha(C)$	$w_\alpha(D)$	$w_\alpha(A)$
0	0	0	1	1	1	1
0	0	1	1	1	0	0
0	1	0	1	1	0	0
0	1	1	1	1	1	1
1	0	0	0	0	1	1
1	0	1	0	1	0	0
1	1	0	0	0	0	1
1	1	1	0	1	1	1

Semantische Äquivalenz

Definition: Ein aussagenlogischer Ausdruck A heißt semantisch äquivalent zum aussagenlogischen Ausdruck B, wenn für jede Belegung α die Beziehung $w_\alpha(A) = w_\alpha(B)$ gilt.

Bezeichnung: $A \equiv B$

Satz: Die semantische Äquivalenz ist eine Äquivalenzrelation auf der Menge der aussagenlogischen Ausdrücke.

Lemma: Seien A und B zwei aussagenlogische Ausdrücke und $n \in \mathbf{N}$ eine natürliche Zahl, so dass $var(A) \cup var(B) \subseteq \{p_1, p_2, \ldots, p_n\}$ gilt. Dann sind A und B genau dann semantisch äquivalent, wenn $f_{A,n} = f_{B,n}$ gilt.

Tautologie, Kontradiktion, Erfüllbarkeit

Definition: i) Ein aussagenlogischer Ausdruck A heißt Tautologie, falls $w_\alpha(A) = 1$ für jede Belegung α gilt.

ii) Ein aussagenlogischer Ausdruck A heißt Kontradiktion oder unerfüllbar, falls $w_\alpha(A) = 0$ für jede Belegung α gilt.

iii) Ein aussagenlogischer Ausdruck A heißt erfüllbar, falls A keine Kontradiktion ist.

Lemma: Zwei aussagenlogische Ausdrücke A und B sind genau dann semantisch äquivalent, wenn der Ausdruck $(A \leftrightarrow B)$ eine Tautologie ist.

Tautologien I

Satz: Die folgenden aussagenlogische Ausdrücke sind Tautologien:

i)	$(\neg\neg p_1 \leftrightarrow p_1)$	(doppelte Verneinung)
ii)	$[(p_1 \wedge p_1) \leftrightarrow p_1]$	
iii)	$[(p_1 \vee p_1) \leftrightarrow p_1]$	
iv)	$[(p_1 \wedge p_2) \leftrightarrow (p_2 \wedge p_1)]$	(Kommutativität der Konjunktion)
v)	$[(p_1 \vee p_2) \leftrightarrow (p_2 \vee p_1)]$	(Kommutativität der Disjunktion)
vi)	$[(p_1 \leftrightarrow p_2) \leftrightarrow (p_2 \leftrightarrow p_1)]$	
vii)	$[((p_1 \wedge p_2) \wedge p_3) \leftrightarrow (p_1 \wedge (p_2 \wedge p_3))]$	(Assoziativität der Konjunktion)
viii)	$[((p_1 \vee p_2) \vee p_3) \leftrightarrow (p_1 \vee (p_2 \vee p_3))]$	(Assoziativität der Disjunktion)

Tautologien II

Satz: (Fortsetzung)

ix)	$[((p_1 \wedge p_2) \vee p_3) \leftrightarrow ((p_1 \vee p_3) \wedge (p_2 \vee p_3))]$	(Distributivgesetz)
x)	$[((p_1 \vee p_2) \wedge p_3) \leftrightarrow ((p_1 \wedge p_3) \vee (p_2 \wedge p_3))]$	(Distributivgesetz)
xi)	$[(p_1 \wedge p_2) \leftrightarrow \neg(\neg p_1 \vee \neg p_2)]$	(de Morgan-Regel)
xii)	$[(p_1 \vee p_2) \leftrightarrow \neg(\neg p_1 \wedge \neg p_2)]$	(de Morgan-Regel)
xiii)	$[(p_1 \rightarrow p_2) \leftrightarrow (\neg p_2 \rightarrow \neg p_1)]$	(Kontraposition)
xiv)	$[(p_1 \rightarrow p_2) \leftrightarrow (\neg p_1 \vee p_2)]$	
xv)	$[(p_1 \leftrightarrow p_2) \leftrightarrow ((p_1 \rightarrow p_2) \wedge (p_2 \rightarrow p_1))]$	
xvi)	$[(p_1 \wedge (p_1 \rightarrow p_2)) \rightarrow p_2]$	
xvii)	$[((p_1 \rightarrow p_2) \wedge (p_2 \rightarrow p_3)) \rightarrow (p_1 \rightarrow p_3)]$	

Parallele Substitution I

Bezeichnung: $psub(A, p, B)$ ist das Wort, das aus A entsteht, indem man *jedes* Vorkommen von p in A durch B ersetzt

Lemma: Seien A und B aussagenlogische Ausdrücke, p eine Variable und α eine Belegung. Ferner sei die Belegung β durch

$$\beta(q) = \begin{cases} \alpha(q) & q \neq p \\ w_\alpha(B) & q = p \end{cases}$$

definiert. Dann gilt

$$w_\alpha(psub(A, p, B)) = w_\beta(A)\,.$$

Parallele Substitution II

Satz: Sind A eine Tautologie und p eine Variable, so ist für jeden aussagenlogischen Ausdruck B auch $psub(A, p, B)$ eine Tautologie.

Satz: Sind A und A' zwei semantische äquivalente Ausdrücke und p eine Variable, so sind für jeden aussagenlogischen Ausdruck B auch die Ausdrücke $psub(A, p, B)$ und $psub(A', p, B)$ semantisch äquivalent.

Sequentielle Substitution und ein Lemma

Bezeichnung: Für aussagenlogische Ausdrücke A und B und einen Teilausdruck C von A ist $ssub(A, C, B)$ die Menge der Wörter, die aus A entsteht, indem wir *ein* Vorkommen von C in A durch B ersetzen.

Satz: Seien B und C zwei semantisch äquivalente Ausdrücke, A ein Ausdruck und C ein Teilausdruck von A. Dann ist A zu jedem Ausdruck aus $ssub(A, C, B)$ semantisch äquivalent.

Satz: Seien B und C zwei semantisch äquivalente Ausdrücke, A eine Tautologie und C ein Teilausdruck von A. Dann ist jeder Ausdruck aus $ssub(A, C, B)$ eine Tautologie.

Lemma: Für einen Ausdruck A, eine Tautologie B und eine Kontradiktion C gelten

$$A \wedge B \equiv A \quad \text{und} \quad A \vee C \equiv A \,.$$

Normalformen I

Definition: Ein aussagenlogischer Ausdruck A ist in konjunktiver Normalform, falls A die Form

$$A = (A_1 \wedge A_2 \wedge \ldots \wedge A_m)$$

für ein $m \geq 1$ hat, wobei jeder der Ausdrücke A_i, $1 \leq i \leq m$, die Form

$$A_i = (A_{i,1} \vee A_{i,2} \vee \ldots \vee A_{i,n_i})$$

mit $n_i \geq 1$ hat, in der jeder Ausdruck $A_{i,j}$, $1 \leq i \leq m$, $1 \leq j \leq n_i$, ein Literal ist.

Normalformen II

Definition: Ein aussagenlogischer Ausdruck A ist in disjunktiver Normalform, falls A die Form

$$A = (A_1 \vee A_2 \vee \ldots \vee A_m)$$

für ein $m \geq 1$ hat, wobei jeder der Ausdrücke A_i, $1 \leq i \leq m$, die Form

$$A_i = (A_{i,1} \wedge A_{i,2} \wedge \ldots \wedge A_{i,n_i})$$

mit $n_i \geq 1$ hat, in der jeder Ausdruck $A_{i,j}$, $1 \leq i \leq m$, $1 \leq j \leq n_i$, ein Literal ist.

Normalformen III

Satz: Zu jedem aussagenlogischen Ausdruck gibt es einen semantisch äquivalenten Ausdruck, bei dessen Konstruktion nur Negation, Konjunktion und Disjunktion (Alternative) benutzt werden.

Satz: Zu jedem aussagenlogischen Ausdruck A gibt es aussagenlogische Ausdrücke B in konjunktiver Normalform und C in disjunktiver Normalform, für die $A \equiv B$ und $A \equiv C$ gelten.

Folgerung: Zu jeder n-stelligen Booleschen Funktion f gibt es einen aussagenlogischen Ausdruck A mit $var(A) = \{p_1, p_2, \ldots, p_n\}$ und $f = f_A$.

Normalformen IV

$A = ((p_3 \vee \neg p_1) \rightarrow (p_2 \leftrightarrow p_3))$

disjunktive Normalform	konjunktive Normalform
$M = \{(0,0,0),(0,1,1),(1,0,0),$ $(1,1,0),(1,1,1)\}$	$M' = \{(0,0,1),(0,1,0),(1,0,1)\}$
$m_{(0,0,0)} = (\neg p_1 \wedge \neg p_2 \wedge \neg p_3)$ $m_{(0,1,1)} = (\neg p_1 \wedge p_2 \wedge p_3)$ $m_{(1,0,0)} = (p_1 \wedge \neg p_2 \wedge \neg p_3)$ $m_{(1,1,0)} = (p_1 \wedge p_2 \wedge \neg p_3)$ $m_{(1,1,1)} = (p_1 \wedge p_2 \wedge p_3)$	$s_{(0,0,1)} = (p_1 \vee p_2 \vee \neg p_3)$ $s_{(0,1,0)} = (p_1 \vee \neg p_2 \vee p_3)$ $s_{(1,0,1)} = (\neg p_1 \vee p_2 \vee \neg p_3)$
$((\neg p_1 \wedge \neg p_2 \wedge \neg p_3) \vee (\neg p_1 \wedge p_2 \wedge p_3)$ $\vee (p_1 \wedge \neg p_2 \wedge \neg p_3) \vee (p_1 \wedge p_2 \wedge \neg p_3)$ $\vee (p_1 \wedge p_2 \wedge p_3))$	$((p_1 \vee p_2 \vee \neg p_3) \wedge (p_1 \vee \neg p_2 \vee p_3)$ $\wedge (\neg p_1 \vee p_2 \vee \neg p_3))$

Entscheidungsprobleme

Probleme:

Ist ein gegebener aussagenlogischer Ausdruck erfüllbar?

Ist ein gegebener aussagenlogischer Ausdruck eine Tautologie?

Ist ein gegebener aussagenlogischer Ausdruck eine Kontradiktion?

Reduktionen:
Ein Ausdruck A ist genau dann eine Kontradiktion, wenn A nicht erfüllbar ist.
Ein Ausdruck A ist genau dann eine Tautologie, wenn $\neg A$ nicht erfüllbar ist.

Definitionsbasierter Algorithmus

Eingabe: Aussagenlogischer Ausdruck A mit n Variablen

$m = 0$; $i = 0$;

`while` $(m == 0$ && $i < 2^n)$ $\{m = w_{\alpha_i}(A);\ i = i + 1;\}$

`if` $(m == 0)$ Gib „A ist nicht erfüllbar" aus;
`else` Gib „A ist erfüllbar" aus;

(dabei ist α_i die Belegung für die $\alpha_i(p_1)\alpha_i(p_2)\ldots\alpha_i(p_n)$ die Binärdarstellung von i ist)

Komplexität: exponentiell

Klausel und Resolvente

Definition: Eine Klausel über $\{p_1, p_2, \ldots, p_n\}$ ist eine Menge

$$K = \{p_{i_1}, p_{i_2}, \ldots, p_{i_r}, \neg p_{j_1}, \neg p_{j_2}, \ldots, \neg p_{i_s}\}$$

mit

$$\{p_{i_1}, p_{i_2}, \ldots, p_{i_r}\} \subseteq \{p_1, \ldots, p_n\} \text{ und } \{p_{j_1}, p_{j_2}, \ldots, p_{j_s}\} \subseteq \{p_1, \ldots, p_n\}\,.$$

Definition: K_1, K_2 und R seien Klauseln. R heißt Resolvente von K_1 und K_2, falls es eine Variable p derart gibt, dass

– $p \in K_1$ und $\neg p \in K_2$ und

– $R = (K_1 \setminus \{p\}) \cup (K_2 \setminus \{\neg p\})$

gelten.

Klauseln und Normalformen

Alternative $A = (p_{i_1} \vee p_{i_2} \vee \ldots \vee p_{i_r} \vee \neg p_{j_1} \vee \neg p_{j_2} \vee \ldots \vee \neg p_{i_s})$

entspricht ,,eineindeutig"

Klausel $K_A = \{p_{i_1}, p_{i_2}, \ldots, p_{i_r}, \neg p_{j_1}, \neg p_{j_2}, \ldots, \neg p_{i_s}\}$

konjunktive Normalform $A = (A_1 \wedge A_2 \wedge \ldots \wedge A_r)$

entspricht ,,eineindeutig"

Menge von Klauseln $K = \{K_{A_1}, K_{A_2}, \ldots, K_{A_r}\}$

Resolutionshülle

Definition: Für eine Menge K von Klauseln setzen wir

$$\begin{aligned} res(K) &= K \cup \{R \mid R \text{ ist Resolvente zweier Klauseln aus } K\}\,, \\ res^0(K) &= K\,, \\ res^{n+1}(K) &= res(res^n(K)) \text{ für } n \geq 0\,, \\ res^*(K) &= \bigcup_{i \geq 0} res^i(K)\,. \end{aligned}$$

Satz: Sei K eine endliche Menge von Klauseln. Dann gibt es eine natürliche Zahl $k \geq 0$ derart, dass

$$res^{k+n}(K) = res^k(K) \text{ für } n \geq 0 \quad \text{und} \quad res^*(K) = res^k(K)$$

gelten.

Aussagen zur Resolution

Lemma: Es sei R die Resolvente von $K' \in K$ und $K'' \in K$. Dann ist der zur Klauselmenge $K = \{K', K''\}$ gehörende aussagenlogische Ausdruck $A = A_K = (D_{K'} \wedge D_{K''})$ semantisch äquivalent zu dem zur Klauselmenge $L = \{K', K'', R\}$ gehörenden Ausdruck $B = A_L = (D_{K'} \wedge D_{K''} \wedge D_R)$.

Lemma: Für eine endliche Menge K von nichtleeren Klauseln sind die zu K, $res^t(K)$ für $t \geq 0$ und $res^*(K)$ gehörenden Ausdrücke semantisch äquivalent zueinander.

Satz: Der zu einer endlichen Klauselmenge K von nichtleeren Klauseln gehörende Ausdruck ist genau dann unerfüllbar, wenn $\emptyset \in res^*(K)$ gilt.

Resolutionsalgorithmus

Eingabe: Klauselmenge K eines aussagenlogischen Ausdrucks A (oder konjunktive Normalform zu A, aus der dann K gewonnen wird)

$n = 1$; $R[0] = K$; $R[1] = res(K)$;

`while` $(\emptyset \notin R[n]$ && $R[n] \neq R[n-1])$ $\{n = n+1;\ R[n] = res(R[n-1]);\}$

`if` $(\emptyset \in R[n])$ Gib "A ist unerfüllbar" aus;
`else` Gib „A ist erfüllbar" aus;

Komplexität: exponentiell

Hornausdruck

Definition:
Ein Hornausdruck ist ein aussagenlogischer Ausdruck in konjunktiver Normalform $(A_1 \wedge A_2 \wedge \ldots \wedge A_m)$, bei dem jede Alternative A_i, $1 \leq i \leq m$, höchstens eine nichtnegierte Variable enthält.

Satz:
Der Algorithmus von Horn für das Erfüllbarkeitsproblem für Hornausdrücke ist korrekt.

Algorithmus von Horn

Eingabe: Hornausdruck $A = (A_1 \wedge A_2 \wedge \ldots \wedge A_m)$

$M = \emptyset$; $b = 1$;

```
for (i = 1; i ≤ m; i++)
     if (A_i = p) {M = M ∪ {p}; b = 0;}

while (b == 0)
{ b = 1;
  for (i = 1; i ≤ m; i++)
       if (A == (p ∨ ¬q_1 ∨ ¬q_2 ∨ ... ∨ ¬q_k)
                && p ∉ M && q_j ∈ M für 1 ≤ j ≤ k)
            { M = M ∪ {p}; b = 0;}  }

a = 1;

for (i = 1; i < m; i++)
     { if (A_i == (¬q_1 ∨ ¬q_2 ∨ ... ∨ ¬q_k)
              && q_j ∈ M für 1 ≤ j ≤ k)
           a = 0;}

if (a == 0) Gib „A ist unerfüllbar" aus;
            else Gib „A ist erfüllbar" aus;
```

Komplexität: polynomiell (Polynom vom Grad 3)