Theoretische Grundlagen des Software Engineering

8: Aussagenlogik II

Stephan Schulz
schulz@eprover.org

Software Systems Engineering

Stiftung Universität Hildesheim 2003

Aufrischung

Aussagenlogische Formeln

$\mathbf{1}, \mathbf{0}, \neg, \wedge, \vee, \rightarrow, \leftrightarrow, (\ )$

Atome: Σ, Formeln über Σ: $For0_\Sigma$

Interpretation $I : \Sigma \rightarrow \{true, false\}$

Evalierungsfunktion $val_I : For0_\Sigma \rightarrow \{true, false\}$

A	B	$\neg A$	$A \wedge B$	$A \vee B$	$A \rightarrow B$	$A \leftrightarrow B$
false	*false*	*true*	*false*	*false*	*true*	*true*
false	*true*	*true*	*false*	*true*	*true*	*false*
true	*false*	*false*	*false*	*true*	*false*	*false*
true	*true*	*false*	*true*	*true*	*true*	*true*

Modell, Folgerung, Erfüllbarkeit

- Eine Interpretation I ist Modell einer Formel $A \in For0_\Sigma$, falls $val_I(A) = true$
- Eine Interpretation I ist Modell einer Formelmenge $M \subseteq For0_\Sigma$, falls $val_I(A) = true \qquad$ für alle $A \in M$
- Folgerung: $KB \models A$ if $M(A) \subseteq M(KB)$
- Tautologie: $\models A$, falls A in allen Interpretationen gültig ist.
- Eine Formel A ist unerfülbar ("widersprüchlich"), wenn sie in allen Interpretationen falsch ist.

Logische Umformungen

Logische Äquivalenz

Definition: Logische Äquivalenz

Zwei Formeln sind logisch äquivalent,
wenn sie in den gleichen Modellen wahr sind, d.h.

$$\alpha \models \beta \quad \text{und} \quad \beta \models \alpha$$

Notation

$$\alpha \equiv \beta$$

Unterformel/Teilformel

Definition

Seien $A, B \in For0_\Sigma$. B heißt Unterformel odr Teilformel von A, falls:

1. $A = B$ oder
2. $A = \neg C$ und B ist Teilformel von C oder
3. $A = (C \otimes D), \otimes \in \{\vee, \wedge, \rightarrow, \leftrightarrow\}$, und B ist Teilformel von C oder B ist Teilformel von D

Schreibweise: Menge der Teilformeln von A: $TF(A)$

Beispiel

$$TF((a \vee (\neg b \leftrightarrow c))) = \{(a \vee (\neg b \leftrightarrow c)), a, (\neg b \leftrightarrow c), \neg b, b, c\}$$
$$TF(\neg\neg\neg a) = \{\neg\neg\neg a, \neg\neg a, \neg a, a\}$$

Logische Äquivalenz

Substitutionstheorem

Sei $A \equiv B$ und C' das Ergebnis der Ersetzung einer Unterformel A in C durch B. Dann gilt:

$$C \equiv C'$$

Beispiel

$A \vee B \quad \equiv \quad B \vee A$

impliziert

$(C \wedge (A \vee B)) \rightarrow D \quad \equiv \quad (C \wedge (B \vee A)) \rightarrow D$

Substitutionstheorem

Beweis (I)

Behauptung: Sei $A \equiv B$ und C' das Ergebnis der Ersetzung einer Unterformel A in C durch B. Dann gilt $C \equiv C'$.

Zu zeigen: $I(C) = I(C')$ für alle Interpretationen I.

Beweis: Per struktureller Induktion über C

IA: C ist elementare Formel, also $C \equiv \mathbf{1}$ oder $C \equiv \mathbf{0}$ oder $C \in \Sigma$. Dann gilt notwendigerweise A=C (da C atomar ist). Also gilt: $C = A \equiv B = C'$, also $I(C) = I(C')$ für alle I.

Substitutionstheorem

Beweis (II)

IV: Behauptung gelte für alle echten Unterformeln von C
IS: Sei C eine zusammengesetzte Formel. Dann gilt: C ist von einer der folgenden Formen: $C = \neg D$ oder $C = (D \otimes E), \otimes \in \{\vee, \wedge, \rightarrow, \leftrightarrow\}$ und A ist eine Unterformel von D oder eine Unterformel von E. Sei $C \neq A$ (sonst: Wie IA).

- Fall 1: $C = \neg D$. Dann ist A Unterformel von D. Sei D' die Formel, die entsteht, wenn man A durch B ersetzt. Laut IV gilt: $val_I(D) = val_I(D')$ für alle I. Wir zeigen: Dann gilt auch $val_I(C) = val_I(C')$.
  - Fall 1a): $val_I(C) = false \Longrightarrow val_I(D) = true = val_I(D')$ $\Longrightarrow val_I(C') = false$ per Definition val_I
  - Fall 1b): $val_I(C) = true \Longrightarrow val_I(D) = false = val_I(D')$ $\Longrightarrow val_I(C') = true$ per Definition val_I

Substitutionstheorem

Beweis (III)

IS: (Fortgesetzt)

- Fall 2: $C = D \vee E$. Sei oBdA A Unterformel von D
  - Fall 2a(i): $val_I(D) = true \Longrightarrow val_I(D') = true$ per IV $\Longrightarrow val_I(D' \vee E) = true \Longrightarrow val_I(C') = true$
  - Fall 2a(ii): $val_I(E) = true \Longrightarrow val_I(D' \vee E) = true \Longrightarrow val_I(C') = true$
  - Fall 2b): $val_I(C) = false \Longrightarrow val_I(D) = false$ und $val_I(E) = false \Longrightarrow val_I(D') = false$ (per IV) $\Longrightarrow val_I(D' \vee E) = false \Longrightarrow val_I(C') = false$
- Fall 3- n: $C = (D \otimes E), \otimes \in \{\wedge, \rightarrow, \leftrightarrow\}$: Analog (aber mühsam).

q.e.d.

Wichtige Äquivalenzen (1)

$(A \wedge B) \equiv (B \wedge A)$	Kommutativität von $\wedge$
$(A \vee B) \equiv (B \vee A)$	Kommutativität von $\vee$
$((A \wedge B) \wedge C) \equiv (A \wedge (B \wedge C))$	Assoziativität von $\wedge$
$((A \vee B) \vee C) \equiv (A \vee (B \vee C))$	Assoziativität von $\vee$
$(A \wedge A) \equiv A$	Idempotenz für $\wedge$
$(A \vee A) \equiv A$	Idempotenz für $\vee$
$\neg\neg A \equiv A$	Doppelnegation
$(A \rightarrow B) \equiv (\neg B \rightarrow \neg A)$	Kontraposition

Wichtige Äquivalenzen (2)

$(A \rightarrow B) \equiv (\neg A \vee B)$	Elimination Implikation
$(A \leftrightarrow B) \equiv ((A \rightarrow B) \wedge (B \rightarrow A)$	Elimination Äquivalenz
$\neg(A \wedge B) \equiv (\neg A \vee \neg B)$	de Morgans Regeln
$\neg(A \vee B) \equiv (\neg A \wedge \neg B)$	de Morgans Regeln
$(A \wedge (B \vee C)) \equiv ((A \wedge B) \vee (A \wedge C))$	Distributivität von $\wedge$ über $\vee$
$(A \vee (B \wedge C)) \equiv ((A \vee B) \wedge (A \vee C))$	Distributivität von $\vee$ über $\wedge$

Wichtige Äquivalenzen (zusammengefasst)

$(A \wedge B)$	$\equiv (B \wedge A)$	Kommutativität von $\wedge$
$(A \vee B)$	$\equiv (B \vee A)$	Kommutativität von $\vee$
$((A \wedge B) \wedge C)$	$\equiv (A \wedge (B \wedge C))$	Assoziativität von $\wedge$
$((A \vee B) \vee C)$	$\equiv (A \vee (B \vee C))$	Assoziativität von $\vee$
$(A \wedge A)$	$\equiv A$	Idempotenz für $\wedge$
$(A \vee A)$	$\equiv A$	Idempotenz für $\vee$
$\neg\neg A$	$\equiv A$	Doppelnegation
$(A \rightarrow B)$	$\equiv (\neg B \rightarrow \neg A)$	Kontraposition
$(A \rightarrow B)$	$\equiv (\neg A \vee B)$	Elimination Implikation
$(A \leftrightarrow B)$	$\equiv ((A \rightarrow B) \wedge (B \rightarrow A))$	Elimination Äquivalenz
$\neg(A \wedge B)$	$\equiv (\neg A \vee \neg B)$	de Morgans Regeln
$\neg(A \vee B)$	$\equiv (\neg A \wedge \neg B)$	de Morgans Regeln
$(A \wedge (B \vee C))$	$\equiv ((A \wedge B) \vee (A \wedge C))$	Distributivität von $\wedge$ über $\vee$
$(A \vee (B \wedge C))$	$\equiv ((A \vee B) \wedge (A \vee C))$	Distributivität von $\vee$ über $\wedge$

Wichtige Äquivalenzen mit **1** und **0**

$$
\begin{aligned}
(A \wedge \neg A) &\equiv \mathbf{0} \\
(A \vee \neg A) &\equiv \mathbf{1} \qquad \text{Tertium non datur} \\
(A \wedge \mathbf{1}) &\equiv A \\
(A \wedge \mathbf{0}) &\equiv \mathbf{0} \\
(A \vee \mathbf{1}) &\equiv \mathbf{1} \\
(A \vee \mathbf{0}) &\equiv A
\end{aligned}
$$

Ein zweiter Kalkül: Logische Umformung

Definition: Äquivalenzumformung

- (Wiederholte) Ersetzung einer (Unter-)Formel durch äquivalente Formel
- Anwendung des Substitutionstheorems

Definition: $\vdash_{LU}$

- Wir schreiben $A \vdash_{LU} B$wenn A mit Äquivalenzumformungen in B umgeformt werden kann.
- Wir schreiben $\vdash_{LU} B$ falls $\mathbf{1} \vdash_{LU} B$

Ein zweiter Kalkül: Logische Umformung

Theorem:

Der Kalkül der logischen Umformungen ist korrekt:
$\vdash_{LU} B$ impliziert $\models B$
Der Kalkül der logischen Umformungen ist vollständig:
$\models B$ impliziert $\vdash_{LU} B$

Anmerkung

Der Kalkül der logischen Umformungen ist nicht vollständig für Folgerungen: $A \models B$ impliziert nicht $A \vdash_{UL} B$
Beispiel: $a \wedge b \models a$, aber $a \wedge b \not\vdash_{UL} a$

Deduktionstheorem

Deduktionstheorem

$$KB \models A \qquad \text{gdw.} \qquad KB \rightarrow A \quad \text{ist allgemeingültig}$$

(verbindet logische Folgerbarkeit und Allgemeingültigkeit)

Folgerungen

- $M \cup \{A\} \models B$ gdw. $M \models A \rightarrow B$
- A, B sind logisch äquivalent gdw. $A \leftrightarrow B$ ist allgemeingültig

Allgemeingültigkeit / Ableitbarkeit / Unerfüllbarkeit

Theorem

A ist allgemeingültig gdw. $\neg A$ ist unerfüllbar

(verbindet Allgemeingültigkeit und Unerfüllbarkeit)

Theorem

$KB \models A$ gdw. $(KB \wedge \neg A)$ ist unerfüllbar

(verbindet logische Ableitbarkeit und Unerfüllbarkeit)

Zusammenhang der Eigenschaften

Aus den Theoremen folgt

- Logische Folgerbarkeit
- Allgemeingültigkeit
- Unerfüllbarkeit

…können jeweils aufeinander zurückgeführt werden!

Kalkül für eine dieser Eigenschaften genügt

Das Craigsche Interpolationstheorem

Theorem

Seien A,B aussagenlogische Formeln mit

$$\models A \rightarrow B$$

dann gibt es eine Formel C mit

$$\models A \rightarrow C \quad \text{und} \quad \models C \rightarrow B,$$

so daß in C nur solche aussagenlogischen Atome $P \in \Sigma$ vorkommen, die sowohl in A als auch in B vorkommen.

Normalformen

Idee: Normalformen

Aussagenlogische Formeln: Kompliziert, verschachtelt

- Optimiert für Ausdruckskraft
- Erlaubt kompakte Spezifikationen

Algorithmen und Kalküle: Einfacher für einfachere Sprachen

- Weniger Fälle zu betrachten
- Regulärerer Code

Konvertierung in einfachere Teilsprache

Normalformen

Normalformen

Definition: Literal

Ein Literal ist ein Atom (aussagenlogische Variable) oder die Negation eines Atoms.

Definition: Klausel

Eine Klausel ist eine Disjunktion von Literalen.

- Mehrstellige Disjunktionen: $(A \vee \neg B \vee C)$
- Einstellige Disjunktionen: A
- Die nullstellige Disjunktion (leere Klausel): **0** oder $\Box$

Konjunktive Normalform

Definition: Konjunktive Normalform (KNF)

Eine Formel in konjunktiver Normalform oder Klauselnormalform ist eine Konjunktion von Klauseln.
Die Konjunktion kann mehrstellig, einstellig oder nullstellig sein.

Beispiele

- $(A \vee \neg B) \;\wedge\; (B \vee \neg C \vee \neg D)$
- $A \vee B$
- $A \wedge (B \vee C)$
- $A \wedge B$
- $\mathbf{1}$

Disjunktive Normalform

Definition: Disjunktive Normalform (DNF)

Eine Formel in disjunktiver Normalform ist eine Disjunktion von Konjunktionen von Literalen.

Disjunktionen und Konjunktionen können mehrstellig, einstellig oder nullstellig sein.

Beispiele

- $(A \wedge \neg B) \ \vee \ (B \wedge \neg C \wedge \neg D)$
- $A \wedge B$
- $A \vee (B \wedge C)$
- $A \vee B$
- $\mathbf{0}$

Konjunktive und Disjunktive Normalform

Eigenschaften

Zu jeder aussagenlogischen Formel gibt es
– eine äquivalente Formel in KNF
– eine äquivalente Formel in DNF

DNF und KNF einer Formel sind nicht eindeutig

DNF und KNF können aus einer Wahrheitstafel abgelesen werden
– Disjunktionen in der KNF entsprechen den Zeilen mit *true*
– Konjunktionen in der DNF entsprechen den Zeilen mit *false*

DNF und KNF können durch Umformungen hergestellt werden

Umformung in KNF

Vier Schritte

1. Elimination von $\leftrightarrow$
   Verwende $A \leftrightarrow B \equiv (A \rightarrow B) \wedge (B \rightarrow A)$
2. Elimination von $\rightarrow$
   Verwende $A \rightarrow B \equiv \neg A \vee B$
3. „Nach innen schieben" von $\neg$
   Verwende de Morgans Regeln und $\neg\neg A \equiv A$
4. „Nach innen schieben" von $\vee$
   Verwende Distributivität von $\vee$ über $\wedge$

Umformung in KNF: Beispiel

0. Gegeben

$$B_{1,1} \leftrightarrow (P_{1,2} \vee P_{2,1})$$

1. Elimination von $\leftrightarrow$

$$(B_{1,1} \rightarrow (P_{1,2} \vee P_{2,1})) \;\wedge\; ((P_{1,2} \vee P_{2,1}) \rightarrow B_{1,1})$$

2. Elimination von $\rightarrow$

$$(\neg B_{1,1} \vee P_{1,2} \vee P_{2,1}) \;\wedge\; (\neg(P_{1,2} \vee P_{2,1}) \vee B_{1,1})$$

Umformung in KNF: Beispiel

2. Elimination von $\rightarrow$

$$(\neg B_{1,1} \lor P_{1,2} \lor P_{2,1}) \;\land\; (\neg(P_{1,2} \lor P_{2,1}) \lor B_{1,1})$$

3. Nach innen schieben von $\neg$

$$(\neg B_{1,1} \lor P_{1,2} \lor P_{2,1}) \;\land\; ((\neg P_{1,2} \land \neg P_{2,1}) \lor B_{1,1})$$

4. Nach innen schieben von $\lor$

$$(\neg B_{1,1} \lor P_{1,2} \lor P_{2,1}) \;\land\; (\neg P_{1,2} \lor B_{1,1}) \;\land\; (\neg P_{2,1} \lor B_{1,1})$$

Beispiel zur exponentiellen Länge der KNF

Gegeben

$$A_n \quad = \quad (P_{1,1} \wedge P_{1,2}) \vee \ldots \vee (P_{n,1} \wedge P_{n,2})$$

Zu A_n äquivalente KNF

$$\bigwedge \{P_{1,f(1)} \vee \ldots \vee P_{n,f(n)} \mid f : \{1, \ldots, n\} \to \{1, 2\}\}$$

Größe der KNF

- Literale in A_n: $2 * n$
- Literale in KNF von A_n: $n * 2^n$

Beispiel zur exponentiellen Länge der KNF

Zu A_n äquivalente KNF

$$\bigwedge\{P_{1,f(1)} \vee \ldots \vee P_{n,f(n)} \mid f : \{1, \ldots, n\} \to \{1, 2\}\}$$

Für $n = 3$

$$\begin{array}{lclc}
(P_{1,1} \vee P_{2,1} \vee P_{3,1}) & \wedge & (P_{1,1} \vee P_{2,1} \vee P_{3,2}) & \wedge \\
(P_{1,1} \vee P_{2,2} \vee P_{3,1}) & \wedge & (P_{1,1} \vee P_{2,2} \vee P_{3,2}) & \wedge \\
(P_{1,2} \vee P_{2,1} \vee P_{3,1}) & \wedge & (P_{1,2} \vee P_{2,1} \vee P_{3,2}) & \wedge \\
(P_{1,2} \vee P_{2,2} \vee P_{3,1}) & \wedge & (P_{1,2} \vee P_{2,1} \vee P_{3,2}) &
\end{array}$$

KNF: Mengenschreibweise

Notation

- Klausel als Menge von Literalen
- Formel in KNF als Menge von Klauseln

Beispiel

$$(\neg B_{1,1} \vee P_{1,2} \vee P_{2,1}) \ \wedge \ (\neg P_{1,2} \vee B_{1,1} \ \wedge \ (\neg P_{2,1} \vee B_{1,1})$$

als

$$\{\ \{\neg B_{1,1}, P_{1,2}, P_{2,1}\},\ \{\neg P_{1,2}, B_{1,1}\},\ \{\neg P_{2,1}, B_{1,1}\}\ \}$$

KNF: Mengenschreibweise

Mengeneigenschaften:

$$\{\neg B_{1,1}, P_{1,2}, P_{2,1}, P_{1,2}\} = \{\neg B_{1,1}, P_{1,2}, P_{2,1}\} = \{P_{2,1}, \neg B_{1,1}, P_{1,2}\}$$

Bedeutung der leeren Menge

- Leere Klausel
  - = leere Menge von Literalen
  - = leere Disjunktion
  - = **0**
- Leere Menge von Klauseln
  - = leere Konkunktion
  - = **1**

Vereinfachung der KNF: Subsumption

Theorem

Enthält eine (aussagenlogische) KNF-Formel (= Klauselmenge) Klauseln K, K' mit

$$K \subsetneq K'$$

dann entsteht eine äquivalente Formel, wenn K' weggelassen wird

Sprechweise

K subsumiert K'

Das SAT- Problem (Erfüllbarkeitsproblem)

Definition: SAT- Problem

Gegeben: Eine aussagenlogische Formel F

Frage: Ist F erfüllbar?

Theorem (ohne Beweis)

SAT ist ein NP- vollständiges Problem

NP- Vollständigkeit

Zur Erinnerung

NP- vollständig heißt:

SAT ist nichtdeterministisch in polynomieller Zeit entscheidbar

Jedes nichtdeterministisch in polynomieller Zeit entscheidbare Problem kann in polynomieller Zeit auf SAT reduziert werden

Wenn es stimmt, dass $NP \neq P$,
dann ist SAT nicht in polynomieller Zeit entscheidbar

Teilklassen des Erfüllbarkeitsproblems

Definition: k- KNF

Eine Formel in k- KNF- Form ist eine KNF- Formel, deren Klauseln höchstens k Literale haben

Theorem

- KNF ist NP- vollständig (ohne Beweis)
- 3- KNF ist NP- vollständig (Idee: Kodiere KNF in 3-KNF)
- 2- KNF ist polynomiell entscheidbar (Baue Implikationsketten)
- DNF ist polynomiell entscheidbar (Beweis trivial)

Resolution

Der aussagenlogische Resolutionkalkül

Wesentliche Eigenschaften

- Widerlegungskalkül: Testet auf Unerfüllbarkeit
- Voraussetzung: Alle Formeln in konjunktiver Normalform
- Eine einzige Regel
- Operiert auf Klauseln (in Mengenschreibweise)

Bermerkungen

Notation

Leere Klausel: $\Box$

Effekt der leeren Klausel

Ist M eine Formel in Klauselnormalform und gilt $\Box \in M$, so ist M unerfüllbar.

Resolutionskalkül

Definition: Resolutionsregel (einzige Regel des Kalküls)

$$\frac{C_1 \cup \{P\}, C_2 \cup \{\neg P\}}{C_1 \cup C_2}$$

wobei

- P ist eine aussagenlogische Variable
- C_1, C_2 sind Klauseln (können leer sein)

Definition: Resolvente

$C_1 \cup C_2$ heißt Resolvente von $C_1 \cup \{P\}$, $C_2 \cup \{\neg P\}$.

Resolutionskalkül

Definition: $\vdash_{Res}$

Wir schreiben $M \vdash_{Res} M'$, falls M' durch (widerholte) Anwendung der Resolutionsregel aus M entsteht, also:

Resolution: Beispiel

Gegeben die Klauselmenge

$$M = \{ \{P_1, P_2\}, \{P_1, \neg P_2\}, \{\neg P_1, P_2\}, \{\neg P_1, \neg P_2\} \}$$

Resolution

$$\frac{\{P_1, P_2\} \qquad \{P_1, \neg P_2\}}{\{P_1\}}$$

$$\frac{\{\neg P_1, P_2\} \qquad \{\neg P_1, \neg P_2\}}{\{\neg P_1\}}$$

$$\frac{\{P_1\}, \{\neg P_1\}}{\Box}$$

Insgesamt

$M \vdash_{Res} \Box$

Also: M unerfüllbar

Resolution: Bemerkungen

Vorsicht bei Klauseln mit mehreren Resolutionsmöglichkeiten

Zwei Klauseln können mehr als eine Resolvente haben
z.B.: $\{A, B\}$ und $\{\neg A, \neg B\}$

$\{A, B, C\}$ und $\{\neg A, \neg B, D\}$ haben nicht $\{C, D\}$ als Resolvente

Heuristik

Immer möglichst kleine Klauseln ableiten

Notwendigkeit der Mengenschreibweise

Die Menge

$$E = \{P_1 \vee \neg P_2,\ \neg P_1 \vee P_2,\ \neg P_1 \vee \neg P_2,\ P_1 \vee P_2\}$$

ist unerfüllbar

Es gibt folgende Resolutionsmöglichkeiten (ohne Mengenschreibweise)

$$\frac{\neg P_1 \vee \neg P_2, P_1 \vee \neg P_2}{\neg P_2 \vee \neg P_2} \qquad \frac{\neg P_1 \vee \neg P_2, \neg P_1 \vee P_2}{\neg P_1 \vee \neg P_1}$$

$$\frac{\neg P_1 \vee \neg P_1, P_1 \vee \neg P_2}{\neg P_1 \vee \neg P_2} \qquad \frac{\neg P_2 \vee \neg P_2, \neg P_1 \vee P_2}{\neg P_1 \vee \neg P_2}$$

Auf diese Weise ist $\square$ nicht herleitbar

Resolution: Korrektheit und Vollständigkeit

Theorem

Für eine Menge M von Klauseln gilt

$$M \text{ unerfüllbar} \quad \text{gdw.} \quad M \vdash_{Res} \Box$$

Zusammenfassung

Logische Umformungen

- Äquivalenzbegriff
- Wichtige Äuquivalenzen

Normalformen

- Literale, Klauseln
- Konjunktive und Disjunktive Normalform
- Umformen in KNF
- Mengenschreibweise
- Subsumtion
- SAT-Problem (SAT, 3-SAT, 2-SAT, DNF-SAT)

Resolution

- Die Resolutionsregel
- Korrektheit und Vollständigkeit

Aufgaben

Set $A = (\neg(a \vee b) \equiv (b \wedge (a \rightarrow \neg c)))$

- Bestimmmen Sie $TW(A)$
- Bestimmen Sie eine KNF von A
- Bestimmen Sie eine DNF von A

Beweisen Sie das Deduktionstheorem.

Zeigen Sie per Resolution, dass $(A \rightarrow B) \rightarrow ((B \rightarrow C) \rightarrow (A \rightarrow C))$ allgemeingültig ist.