Einführung in die Theoretische Informatik

Woche 2

Harald Zankl

Institut für Informatik @ UIBK
Wintersemester 2014/2015

Zusammenfassung der letzten LVA

Beispiel

Wenn das Kind schreit, dann hat es Hunger.
Das Kind schreit.
Also, hat das Kind Hunger.

Fakt

Die Korrektheit dieser Schlussfigur ist unabhängig von den konkreten Aussagen.

Definition (*Modus Ponens*)

Wenn A, dann B.
A gilt.
Also, gilt B.

Inhalte der Lehrveranstaltung

Einführung in die Logik

Syntax & Semantik der Aussagenlogik, Formales Beweisen, Konjunktive und Disjunktive Normalformen

Einführung in die Algebra

Boolesche Algebra, Universelle Algebra, Logische Schaltkreise

Einführung in die Theorie der Formalen Sprachen

Grammatiken und Formale Sprachen, Reguläre Sprachen, Kontextfreie Sprachen

Einführung in die Berechenbarkeitstheorie

Algorithmisch unlösbare Probleme, Turing Maschinen, Registermaschinen

Einführung in die Programmverifikation

Prinzipien der Analyse von Programmen, Verifikation nach Hoare

Syntax der Aussagenlogik

Definition

Sei AT eine Menge von atomaren Formeln (oder Atomen), deren Elemente mit p, q, r, ... bezeichnet werden

Definition

Wahrheitswertsymbole:

$$\mathsf{True} \qquad \mathsf{False}$$

Junktoren:

$$\neg \qquad \wedge \qquad \vee \qquad \rightarrow$$

Syntax der Aussagenlogik (2)

Definition

Die Formeln der Aussagenlogik sind induktiv definiert:

1. Eine atomare Formel p ist eine Formel,
2. ein Wahrheitswertsymbol (True, False) ist eine Formel, und
3. wenn A und B Formeln sind, dann sind
   $$\neg A \qquad (A \wedge B) \qquad (A \vee B) \qquad (A \rightarrow B)$$
   auch Formeln

Beispiel

Der Ausdruck $((\mathsf{p} \rightarrow \neg \mathsf{q}) \rightarrow (\neg \mathsf{q} \rightarrow \neg \mathsf{p}))$ ist eine Formel

Konvention

Wir verwenden die folgende Präzedenz:

$$\neg > \vee, \wedge > \rightarrow \qquad \rightarrow \text{ ist rechts-assoziativ: } A \rightarrow (B \rightarrow C)$$

Semantik der Aussagenlogik

Definition

1. T und F bezeichnen die beiden betrachteten Wahrheitswerte
2. Belegung $\mathsf{v} \colon \mathsf{AT} \rightarrow \{\mathsf{T}, \mathsf{F}\}$ assoziiert Atome mit Wahrheitswerten

Beispiel

Betrachte die Atome p, q und r, sowie die folgende Belegung:

$$\mathsf{v}(a) := \begin{cases} \mathsf{T} & a = \mathsf{p} \\ \mathsf{F} & a = \mathsf{q} \\ \mathsf{F} & a = \mathsf{r} \end{cases}$$

Wir schreiben auch $\mathsf{v}(\mathsf{p}) = \mathsf{T}$, $\mathsf{v}(\mathsf{q}) = \mathsf{F}$, $\mathsf{v}(\mathsf{r}) = \mathsf{F}$.

Semantik der Aussagenlogik (2)

Definition

1. Atome sind Platzhalter für konkrete atomare Aussagen (Formeln)
2. Junktoren sind formale Zeichen, die Aussagen verbinden
   $$\underbrace{\neg}_{\text{Negation}} \quad \underbrace{\wedge}_{\text{Konjunktion}} \quad \underbrace{\vee}_{\text{Disjunktion}} \quad \underbrace{\rightarrow}_{\text{Implikation}}$$
3. Die Bedeutung wird durch Wahrheitstafeln definiert

¬	
T	F
F	T

∧	T	F
T	T	F
F	F	F

∨	T	F
T	T	T
F	T	F

→	T	F
T	T	F
F	T	T

Beispiel

Die allgemeine Aussage „Wenn p, dann q“ schreiben wir:

$$p \rightarrow q$$

Semantik der Aussagenlogik (3)

Definition

Erweiterung der Belegung v zu einem Wahrheitswert für Formeln:

$$\bar{\mathsf{v}}(p) = \mathsf{v}(p) \qquad \bar{\mathsf{v}}(\neg A) = \begin{cases} \mathsf{T} & \bar{\mathsf{v}}(A) = \mathsf{F} \\ \mathsf{F} & \bar{\mathsf{v}}(A) = \mathsf{T} \end{cases}$$

$$\bar{\mathsf{v}}(\mathsf{True}) = \mathsf{T} \qquad \bar{\mathsf{v}}(A \wedge B) = \begin{cases} \mathsf{T} & \bar{\mathsf{v}}(A) = \bar{\mathsf{v}}(B) = \mathsf{T} \\ \mathsf{F} & \text{sonst} \end{cases}$$

$$\bar{\mathsf{v}}(\mathsf{False}) = \mathsf{F} \qquad \bar{\mathsf{v}}(A \vee B) = \begin{cases} \mathsf{F} & \bar{\mathsf{v}}(A) = \bar{\mathsf{v}}(B) = \mathsf{F} \\ \mathsf{T} & \text{sonst} \end{cases}$$

$$\bar{\mathsf{v}}(A \rightarrow B) = \begin{cases} \mathsf{T} & \bar{\mathsf{v}}(A) = \mathsf{F} \text{ oder } \bar{\mathsf{v}}(B) = \mathsf{T} \\ \mathsf{F} & \text{sonst} \end{cases}$$

Beispiel

Sei $\mathsf{v}(\mathsf{p}) = \mathsf{T}$, $\mathsf{v}(\mathsf{q}) = \mathsf{F}$, dann ist $\bar{\mathsf{v}}((\mathsf{p} \rightarrow \neg \mathsf{q}) \rightarrow (\neg \mathsf{q} \rightarrow \neg \mathsf{p})) = \mathsf{F}$.

Wahrheitstabelle

Definition

Sei A eine Formel; die Wahrheitstabelle von A listet alle relevanten Belegungen v zusammen mit dem Wahrheitswert $\bar{\mathrm{v}}(A)$ auf.

Beispiel

Betrachte die Formel: $(p \to \neg q) \to (\neg q \to \neg p)$
Wir stellen die folgende Wahrheitstabelle auf:

p	q	$(p \to \neg q)$	$(\neg q \to \neg p)$	$(p \to \neg q) \to (\neg q \to \neg p)$
T	T	F	T	T
T	F	T	F	F
F	T	T	T	T
F	F	T	T	T

Eigenschaften

Definition

Eine Formel A heißt

1. erfüllbar, wenn Belegung v existiert, sodass $\bar{\mathrm{v}}(A) = \mathrm{T}$,
2. unerfüllbar, wenn keine solche Belegung existiert, und
3. gültig bzw. Tautologie, wenn für alle Belegungen v, $\bar{\mathrm{v}}(A) = \mathrm{T}$.

Beispiel

- erfüllbar: p, q, $p \wedge q$
- unerfüllbar: $p \wedge \neg p$
- Tautologie: $p \vee \neg p$, $\neg(p \wedge \neg p)$

Satz

Wenn eine Formel A gültig ist, dann ist A auch erfüllbar.

Satz

Eine Formel A ist eine Tautologie gdw. $\neg A$ unerfüllbar.

Beweis.

1. Wir zeigen die Richtung von links nach rechts:
   - angenommen $\bar{\mathrm{v}}(A) = \mathrm{T}$, für alle Belegungen v
   - also $\bar{\mathrm{v}}(\neg A) = \mathrm{F}$, für alle Belegungen v
   - somit ist $\neg A$ unerfüllbar
2. Wir zeigen die Richtung von rechts nach links:
   - angenommen $\neg A$ ist unerfüllbar
   - $\bar{\mathrm{v}}(\neg A) = \mathrm{F}$, für alle Belegungen v
   - also $\bar{\mathrm{v}}(A) = \mathrm{T}$, für alle Belegungen v und somit gültig

■

Konsequenz und Äquivalenz von Formeln

Definition (Konsequenz)

Die Konsequenzrelation $A_1, \dots, A_n \models B$ gilt, gdw. für alle Belegungen v:

$$\text{Wenn } \bar{\mathrm{v}}(A_1) = \mathrm{T}, \dots, \bar{\mathrm{v}}(A_n) = \mathrm{T}, \text{ dann } \quad \bar{\mathrm{v}}(B) = \mathrm{T}$$

Beispiel

$p \not\models q \quad p, q \models q \quad p \wedge q \models q \quad p \not\models p \wedge q \quad p \to q \models \neg p \vee q \quad \models p \vee \neg p$

Definition (Äquivalenz)

$A \equiv B$, wenn $A \models B$ und $B \models A$ gilt

Beispiel

$p \not\equiv q \quad p \wedge q \not\equiv q \quad p \not\equiv p \wedge q \quad p \to q \equiv \neg p \vee q$

Assoziativität und Kommutativität von Junktoren

Fakt

- *Konjunktion und Disjunktion sind assoziativ und kommutativ*
- *Wir unterscheiden nicht zwischen:*

$$(A \wedge B) \wedge C \qquad A \wedge (B \wedge C) \qquad A \wedge B \wedge C$$
$$A \wedge B \qquad B \wedge A$$

Definition

1. $\bigwedge_{i=1}^{n} A_i = A_1 \wedge \cdots \wedge A_n$
2. $\bigwedge_{i=1}^{0} A_i =$ True
3. $\bigvee_{i=1}^{n} A_i = A_1 \vee \cdots \vee A_n$
4. $\bigvee_{i=1}^{0} A_i =$ False

Äquivalenzen I

Lemma (Elementare Äquivalenzen)

$$\begin{array}{rrrr} \neg\neg A \equiv A & A \vee \text{True} \equiv \text{True} & A \wedge \text{True} \equiv A & A \rightarrow \text{True} \equiv \text{True} \\ & A \vee \text{False} \equiv A & A \wedge \text{False} \equiv \text{False} & A \rightarrow \text{False} \equiv \neg A \\ & A \vee A \equiv A & A \wedge A \equiv A & \text{True} \rightarrow A \equiv A \\ & A \vee \neg A \equiv \text{True} & A \wedge \neg A \equiv \text{False} & \text{False} \rightarrow A \equiv \text{True} \\ & & & A \rightarrow A \equiv \text{True} \end{array}$$

Lemma (Distributivgesetze und Andere)

$$A \wedge (B \vee C) \equiv (A \wedge B) \vee (A \wedge C) \qquad A \vee (B \wedge C) \equiv (A \vee B) \wedge (A \vee C)$$
$$A \rightarrow B \equiv \neg A \vee B \qquad \neg(A \rightarrow B) \equiv A \wedge \neg B$$

Äquivalenzen II

Lemma (Kommutativ- und Assoziativgesetze)

$$A \wedge B \equiv B \wedge A \qquad A \vee B \equiv B \vee A$$
$$A \wedge (B \wedge C) \equiv (A \wedge B) \wedge C \qquad A \vee (B \vee C) \equiv (A \vee B) \vee C$$

Lemma (Absorptionsgesetze)

$$A \wedge (A \vee B) \equiv A \qquad A \vee (A \wedge B) \equiv A$$
$$A \wedge (\neg A \vee B) \equiv A \wedge B \qquad A \vee (\neg A \wedge B) \equiv A \vee B$$

Lemma (Gesetze von de Morgan)

$$\neg(A \wedge B) \equiv \neg A \vee \neg B \qquad \neg(A \vee B) \equiv \neg A \wedge \neg B$$

Gleiches durch Gleiches Ersetzen

Definition

Eine *Teilformel* A einer Formel B ist ein Teilausdruck von B, der wiederum eine Formel ist.

Satz

1. *Seien A, B Formeln und E, F Teilformeln von A, B*
2. *Gelte $E \equiv F$*
3. *B ist das Resultat der Ersetzung von E durch F in A*

Dann gilt $A \equiv B$

Beispiel

Seien $A = (p \rightarrow q) \wedge r$ und $B = (\neg p \vee q) \wedge r$.
Da $p \rightarrow q \equiv \neg p \vee q$ gilt $(p \rightarrow q) \wedge r \equiv (\neg p \vee q) \wedge r$.