Script generated by TTT

Title: Mayr: 2012 ds (25.10.2012)

Date: Thu Oct 25 10:14:33 CEST 2012

Duration: 91:43 min

Pages: 36

WS 2012/13

Diskrete Strukturen

Ernst W. Mayr

Fakultät für Informatik
TU München

http://www14.in.tum.de/lehre/2012WS/ds/

Wintersemester 2012

Formalismen der Aussagenlogik

- Die Aussagenlogik (wie jede Logik) bildet eine formale Sprache.
- Eine formale Sprache wird durch ihre Syntax und ihre Semantik definiert.
- Die Syntax der Sprache legt durch Regeln fest, welche Zeichenketten wohlgeformte Ausdrücke sind.
  Die wohlgeformten Ausdrücke einer Logik heißen Formeln.
- Die Semantik legt die Bedeutung der Ausdrücke fest.
  Eine formale Semantik ordnet jedem (wohlgeformten) Ausdruck ein mathematisches Objekt zu, welches die Bedeutung des Ausdrucks darstellt.

Formalismen der Aussagenlogik

- Die Aussagenlogik (wie jede Logik) bildet eine formale Sprache.
- Eine formale Sprache wird durch ihre Syntax und ihre Semantik definiert.
- Die Syntax der Sprache legt durch Regeln fest, welche Zeichenketten wohlgeformte Ausdrücke sind.
  Die wohlgeformten Ausdrücke einer Logik heißen Formeln.
- Die Semantik legt die Bedeutung der Ausdrücke fest.
  Eine formale Semantik ordnet jedem (wohlgeformten) Ausdruck ein mathematisches Objekt zu, welches die Bedeutung des Ausdrucks darstellt.

Syntax

- Eine formale Syntax besteht aus einem Vokabular und einer Menge von Formationsregeln/Bildungsgesetzen.
- Das Vokabular legt fest, welche Zeichen in Ausdrücken vorkommen dürfen
- Die Bildungsgesetze legen fest, welche Zeichenketten über dem Vokabular zulässig oder wohlgeformt sind (und welche nicht).

Syntax für die Aussagenlogik (ohne Quantoren)

1. true und false sind Formeln (alternativ: 1/0, wahr/falsch, ...);
2. eine Aussagenvariable (wie x oder p) ist eine Formel;
3. sind F und G Formeln, dann ist auch

Beispiele für aussagenlogische Formeln

- Beispiele für aussagenlogische Formeln sind:
  1. $(p \wedge q) \Rightarrow r$
  2. $(p \Rightarrow q) \Rightarrow (\neg q \Rightarrow \neg p)$
  3. $(p \Rightarrow q) \equiv (\neg q \Rightarrow \neg p)$
  4. $(p \vee q) \Rightarrow (p \wedge q)$
- Keine Formeln sind dagegen:

Semantik der Aussagenlogik

- Eine Belegung („eine Welt“) ist eine Funktion von einer Menge von Aussagenvariablen in die Menge $\{0, 1\}$ der Wahrheitswerte.
- Die Belegung $p \mapsto 0$, $q \mapsto 1$ ist eine Belegung für die Formel $p \Rightarrow q$.
- Unter der Belegung $p \mapsto 1$, $q \mapsto 0$ ist der Wert der Formel $p \Rightarrow q$ gleich 0 (oder **false**).
- Unter der Belegung $p \mapsto 0$, $q \mapsto 1$ ist der Wert der Formel $p \Rightarrow q$ gleich 1 (oder **true**).
- Die Semantik einer booleschen Formel ist ihr Wert unter allen möglichen Belegungen (der darin vorkommenden Variablen).

Wahrheitstabellen

Damit ergibt sich

- Die Formel $\neg p$ ergibt genau dann **wahr** wenn p mit 0/**false** belegt wird.
- Die Formel $p \Rightarrow q$ ist genau dann **false**, wenn p gleich 1/**true** und q gleich 0/**false** ist.
- Wir sagen, dass eine Belegung eine Formel erfüllt, falls unter der Belegung der resultierende Wahrheitswert der Formel gleich 1/**true** ist.

Wahrheitstabellen

Damit ergibt sich

- Die Formel $\neg p$ ergibt genau dann **wahr** wenn p mit 0/**false** belegt wird.
- Die Formel $p \Rightarrow q$ ist genau dann **false**, wenn p gleich 1/**true** und q gleich 0/**false** ist.
- Wir sagen, dass eine Belegung eine Formel erfüllt, falls unter der Belegung der resultierende Wahrheitswert der Formel gleich 1/**true** ist.

Allgemeingültige Aussagen

Definition 19

- Eine (aussagenlogische) Formel p heißt allgemeingültig (oder auch eine Tautologie), falls p unter jeder Belegung **wahr** ist.
- Eine (aussagenlogische) Formel p heißt erfüllbar, falls es (mindestens) eine Belegung gibt, unter der p **wahr** ist.

Damit folgt:

Allgemeingültige Aussagen

Definition 19

- Eine (aussagenlogische) Formel p heißt allgemeingültig (oder auch eine Tautologie), falls p unter jeder Belegung **wahr** ist.
- Eine (aussagenlogische) Formel p heißt erfüllbar, falls es (mindestens) eine Belegung gibt, unter der p **wahr** ist.

Damit folgt:

- Die Formel $(p \Rightarrow q) \equiv (\neg q \Rightarrow \neg p)$ ist allgemeingültig (eine Tautologie).
- Die Formel **false** $\Rightarrow p$ ist allgemeingültig.
- Die Formel $(p \vee \neg q) \wedge \neg p$ ist erfüllbar.
- Die Formel $p \wedge q \wedge (p \Rightarrow \neg q)$ ist nicht erfüllbar.

Starting Recognition...

Definition 20

- Unter dem Erfüllbarkeitsproblem (SAT) verstehen wir die Aufgabe, festzustellen, ob eine gegebene (aussagenlogische) Formel erfüllbar ist.
- Unter dem Tautologieproblem (TAUT) verstehen wir die Aufgabe, festzustellen, ob eine gegebene (aussagenlogische) Formel eine Tautologie ist.

Boolesche Funktionen

Sei $\mathbb{B}$ die Menge $\{0, 1\}$ der booleschen Werte.
Jede n-stellige boolesche Funktion bildet jede Kombinationen der Werte der n Eingangsgrößen jeweils auf einen Funktionswert aus $\{0, 1\}$ ab.

$$f : \mathbb{B}^n \ni (x_1, \ldots, x_n) \mapsto f(x_1, x_2, \ldots, x_n) \in \mathbb{B}$$

Beobachtung: Da $|\mathbb{B}| = 2$, gibt es genau 2^n verschiedene Tupel in $\mathbb{B}^n$.
Da wir für jedes dieser Tupel den Funktionswert beliebig $\in \mathbb{B}$ wählen können, gibt es genau 2^{2^n} verschiedene (totale) Boolesche Funktionen mit n Argumenten.

Boolesche Funktionen mit einem Argument

Nach der obigen Formel gibt es $2^{2^1} = 4$ boolesche Funktionen mit einem Argument:

x	f_1	f_2	f_3	f_4
0	0	1	0	1
1	0	1	1	0

f_1: „falsch“-Funktion
f_2: „wahr“-Funktion
f_3: Identität
f_4: Negation

Wir betrachten nun die Menge aller zweistelligen booleschen Funktionen.

(Unäre und) binäre Verknüpfungen boolescher Werte:

			$\vee$	$\Leftarrow$		$\Rightarrow$		$\equiv$ $=$	$\wedge$	nand	$\not\equiv$ $\neq$					nor	
t	t	t	t	t	t	t	t	t	t	f	f	f	f	f	f	f	f
t	f	t	t	t	t	f	f	f	f	t	t	t	t	f	f	f	f
f	t	t	t	f	f	t	t	f	f	t	t	f	f	t	t	f	f
f	f	t	f	t	f	t	f	t	f	t	f	t	f	t	f	t	f

Normalformen boolescher Funktionen

Jeder boolesche Ausdruck kann durch (äquivalente) Umformungen in gewisse Normalformen gebracht werden!

Disjunktive Normalform (DNF) und Vollkonjunktion:
Eine Vollkonjunktion ist ein boolescher Ausdruck,

- in dem **alle** Variablen **einmal** vorkommen (jeweils als negiertes oder nicht negiertes Literal),
- alle Literale durch Konjunktionen $\wedge$ („und“) verbunden sind.

Die disjunktive („oder“, $\vee$) Verbindung von Vollkonjunktionen nennt man disjunktive Normalform (DNF). Statt $\neg a$ schreiben wir hier (auch, der Kürze halber) $\overline{a}$.

$$f(a,b,c) = \underbrace{\underbrace{(a \wedge b \wedge \overline{c})}_{\text{Vollkonjunktion}} \vee \underbrace{(\overline{a} \wedge b \wedge \overline{c})}_{\text{Vollkonjunktion}} \vee \ldots \vee \underbrace{(\overline{a} \wedge \overline{b} \wedge c)}_{\text{Vollkonjunktion}}}_{\text{disjunktive Verknüpfung der Vollkonjunktionen}}$$

Normalformen boolescher Funktionen

Jeder boolesche Ausdruck kann durch (äquivalente) Umformungen in gewisse Normalformen gebracht werden!

Disjunktive Normalform (DNF) und Vollkonjunktion:
Eine Vollkonjunktion ist ein boolescher Ausdruck,

- in dem **alle** Variablen **einmal** vorkommen (jeweils als negiertes oder nicht negiertes Literal),
- alle Literale durch Konjunktionen $\wedge$ („und“) verbunden sind.

Die disjunktive („oder“, $\vee$) Verbindung von Vollkonjunktionen nennt man disjunktive Normalform (DNF). Statt $\neg a$ schreiben wir hier (auch, der Kürze halber) $\overline{a}$.

$$f(a,b,c) = \underbrace{\underbrace{(a \wedge b \wedge \overline{c})}_{\text{Vollkonjunktion}} \vee \underbrace{(\overline{a} \wedge b \wedge \overline{c})}_{\text{Vollkonjunktion}} \vee \ldots \vee \underbrace{(\overline{a} \wedge \overline{b} \wedge c)}_{\text{Vollkonjunktion}}}_{\text{disjunktive Verknüpfung der Vollkonjunktionen}}$$

Ableitung der disjunktiven Normalform aus einer Wertetabelle

- jede Zeile der Wertetabelle entspricht einer Vollkonjunktion
- Terme mit Funktionswert „0“ tragen nicht zum Funktionsergebnis bei („oder“ von 0)

a	b	f(a,b)
0	0	0
0	1	1
1	0	1
1	1	0

Ableitung der disjunktiven Normalform aus einer Wertetabelle

- jede Zeile der Wertetabelle entspricht einer Vollkonjunktion
- Terme mit Funktionswert „0“ tragen nicht zum Funktionsergebnis bei („oder“ von 0)

a	b	f(a,b)
0	0	0
0	1	1
1	0	1
1	1	0

- bilde Vollkonjunktionen für Zeilen mit Funktionswert „1“
$\rightarrow$ Zeilen 2 und 3 („0“ in Tabelle $\equiv$ Negation der Variablen)
- keine solche Zeile: $f(a,b) = 0$
- Zeile 2: $\overline{a} \wedge b$
- Zeile 3: $a \wedge \overline{b}$
- disjunktive Verknüpfung der Vollkonjunktionen:
$f(a,b) = (\overline{a} \wedge b) \vee (a \wedge \overline{b})$

Konjunktive Normalform (KNF/CNF) und Volldisjunktion

Eine Volldisjunktion ist ein boolescher Ausdruck,

- in dem **alle** Variablen **einmal** vorkommen (in Form eines negierten oder nicht negierten Literals),
- alle Literale durch Disjunktionen $\vee$ („oder") verbunden sind.

Die konjunktive („und") Verbindung von Volldisjunktionen nennt man konjunktive Normalform, kurz KNF (engl.: CNF).

$$f(a,b,c) = \underbrace{\underbrace{(a \vee b \vee \overline{c})}_{\text{Volldisjunktion}} \wedge \underbrace{(\overline{a} \vee b \vee \overline{c})}_{\text{Volldisjunktion}} \wedge \ldots \wedge \underbrace{(\overline{a} \vee \overline{b} \vee c)}_{\text{Volldisjunktion}}}_{\text{konjunktive Verknüpfung der Volldisjunktionen}}$$

Konjunktive Normalform (KNF/CNF) und Volldisjunktion

Eine Volldisjunktion ist ein boolescher Ausdruck,

- in dem **alle** Variablen **einmal** vorkommen (in Form eines negierten oder nicht negierten Literals),
- alle Literale durch Disjunktionen $\vee$ („oder") verbunden sind.

Die konjunktive („und") Verbindung von Volldisjunktionen nennt man konjunktive Normalform, kurz KNF (engl.: CNF).

$$f(a,b,c) = \underbrace{\underbrace{(a \vee b \vee \overline{c})}_{\text{Volldisjunktion}} \wedge \underbrace{(\overline{a} \vee b \vee \overline{c})}_{\text{Volldisjunktion}} \wedge \ldots \wedge \underbrace{(\overline{a} \vee \overline{b} \vee c)}_{\text{Volldisjunktion}}}_{\text{konjunktive Verknüpfung der Volldisjunktionen}}$$

Ableitung der konjunktiven Normalform

- jede Zeile der Wertetabelle entspricht einer Volldisjunktion
- Terme mit Funktionswert „1" tragen nicht zum Funktionsergebnis bei („und" mit 1)

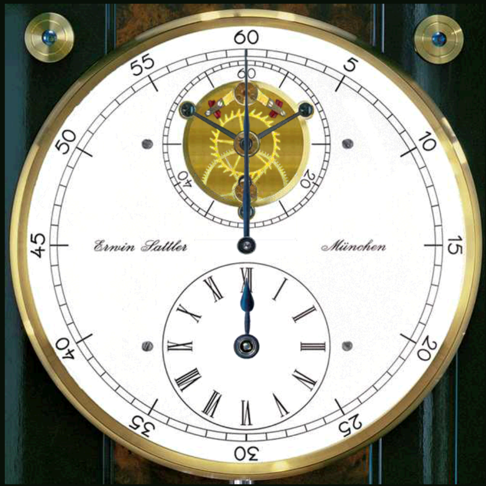
a	b	$f(a,b)$
0	0	0
0	1	1
1	0	0
1	1	1

Ableitung der konjunktiven Normalform

- jede Zeile der Wertetabelle entspricht einer Volldisjunktion
- Terme mit Funktionswert „1" tragen nicht zum Funktionsergebnis bei („und" mit 1)

a	b	$f(a,b)$
0	0	0
0	1	1
1	0	0
1	1	1

- bilde Volldisjunktionen für Zeilen mit Funktionswert „0" $\rightarrow$ Zeilen 1 und 3 („1" in Tabelle $\equiv$ Negation der Variablen)
- keine solche Zeile: $f(a,b) = 1$
- Zeile 1: $a \vee b$
- Zeile 3: $\overline{a} \vee b$
- konjunktive Verknüpfung der Volldisjunktionen: $f(a,b) = (a \vee b) \wedge (\overline{a} \vee b)$



Ableitung der konjunktiven Normalform

- jede Zeile der Wertetabelle entspricht einer Volldisjunktion
- Terme mit Funktionswert „1“ tragen nicht zum Funktionsergebnis bei („und“ mit 1)

a	b	$f(a,b)$
0	0	0
0	1	1
1	0	0
1	1	1

- bilde Volldisjunktionen für Zeilen mit Funktionswert „0“ $\rightarrow$ Zeilen 1 und 3 („1“ in Tabelle $\equiv$ Negation der Variablen)
- keine solche Zeile: $f(a,b) = 1$
- Zeile 1: $a \vee b$
- Zeile 3: $\overline{a} \vee b$
- konjunktive Verknüpfung der Volldisjunktionen: $f(a,b) = (a \vee b) \wedge (\overline{a} \vee b)$

Vergleich von DNF und KNF:

	DNF	KNF
wähle Zeilen mit Funktionswert	1	0
Bildung der Teil-Terme	Negation der „0“ Einträge Verknüpfung der Literale mit „und“	Negation der „1“ Einträge Verknüpfung der Literale mit „oder“
Verknüpfung der Teil-Terme	mit „oder“	mit „und“

De Morgan’sche Regeln

Durch Auswerten der Wahrheitswertetabelle stellen wir fest, dass

$$(p \vee q) \equiv \overline{\overline{p} \wedge \overline{q}}$$

allgemeingültig ist; ebenso

$$(p \wedge q) \equiv \overline{\overline{p} \vee \overline{q}}\,.$$

Diese beiden Tautologien werden als die De Morgan'schen Regeln bezeichnet, benannt nach Augustus de Morgan (1806–1871).

Starting Recognition...

Modus Ponens

Durch Auswerten der Wahrheitstabelle stellen wir ebenfalls fest, dass

$$((p \Rightarrow q) \wedge p) \Rightarrow q$$

allgemeingültig ist.
Intuitiv bedeutet dies, dass wir, falls wir wissen, dass $p \Rightarrow q$ wahr ist (d.h., aus p (aussagenlogisch) stets q folgt) und dass auch p gilt, die Gültigkeit von q folgern können.

Dieses Prinzip des Modus Ponens wird in Beweisen sehr häufig verwendet.

Wichtige Bemerkung:

Ist eine boolesche Formel $F(x_1, \ldots, x_n)$ mit den Variablen $x_1, \ldots, x_n$ allgemeingültig, und sind $F_1, \ldots, F_n$ boolesche Formeln (mit den Variablen $x_1, \ldots, x_r$), dann ist auch

$$F(F_1, \ldots, F_n)$$

allgemeingültig (mit den Variablen $x_1, \ldots, x_r$).

Quantoren

Sei $F(p, q, \ldots)$ eine boolesche Formel mit den Variablen p, q, ... Manchmal (oder auch öfters) wollen wir (aus F abgeleitete) Eigenschaften G ausdrücken, die aussagen, dass

1. es eine Belegung für p gibt, so dass dann die resultierende Formel gilt, also
$$G(q, \ldots) = F(0, q, \ldots) \vee F(1, q, \ldots)\,;$$
2. für jede Belegung von p dann die resultierende Formel gilt, also
$$H(q, \ldots) = F(0, q, \ldots) \wedge F(1, q, \ldots)\,;$$

Hierfür verwenden wir die folgende Notation:

Quantoren

Sei $F(p, q, \ldots)$ eine boolesche Formel mit den Variablen p, q, ... Manchmal (oder auch öfters) wollen wir (aus F abgeleitete) Eigenschaften G ausdrücken, die aussagen, dass

1. es eine Belegung für p gibt, so dass dann die resultierende Formel gilt, also
$$G(q, \ldots) = F(0, q, \ldots) \vee F(1, q, \ldots)\,;$$
2. für jede Belegung von p dann die resultierende Formel gilt, also
$$H(q, \ldots) = F(0, q, \ldots) \wedge F(1, q, \ldots)\,;$$

Hierfür verwenden wir die folgende Notation:

Prädikatenlogik

Oft wollen wir Eigenschaften betrachten, die Elemente über einem anderen Universum als dem der booleschen Werte $\mathbb{B}$ betreffen.

Sei $\mathcal{U}$ ein solches Universum.

Definition 21

Prädikatenlogik

Oft wollen wir Eigenschaften betrachten, die Elemente über einem anderen Universum als dem der booleschen Werte $\mathbb{B}$ betreffen.

Sei $\mathcal{U}$ ein solches Universum.

Definition 21

- Ein Prädikat P über $\mathcal{U}$ ist eine Teilmenge von $\mathcal{U}^n$, für ein geeignetes $n \in \mathbb{N}_0$.
- Die Formel $P(x_1, \ldots, x_n) \in \mathbb{B}$ ist **true** gdw $(x_1, \ldots, x_n)$ Element der entsprechenden Teilmenge ist.

Beispiel 22

Sei das Universum die Menge $\mathbb{N} \setminus \{1\}$, sei $P(n)$ das Prädikat „$n \in \mathbb{N} \setminus \{1\}$ ist prim“, und sei „$<$“das Prädikat „kleiner als“ (geschrieben in Infix-Notation), dann bedeutet

- $(\forall n \in \mathbb{N} \setminus \{1\}\ \exists p \in \mathbb{N} \setminus \{1\})[P(p) \wedge (p > n)]$
  „Es gibt unendlich viele Primzahlen!“

Bemerkungen:

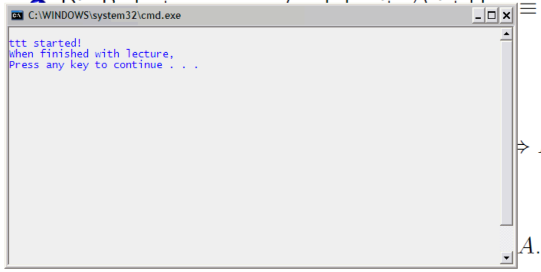
1. Die Bedeutung von $\equiv$ (und damit $\not\equiv$) ist klar. $\equiv$ wird oft, vor allem in Beweisen, auch als

   $$\Leftrightarrow$$

   geschrieben (im Englischen: iff, if and only if).
2. Für zwei boolesche Aussagen A und B ist $A \Rightarrow B$ falsch genau dann wenn $A = t$ und $B = f$.
3. $A \Rightarrow B$ ist damit äquivalent zu $\neg A \vee B$.
4. $A \Rightarrow B$ ist damit auch äquivalent zu $\neg B \Rightarrow \neg A$.

Wichtige Beobachtung:
Gilt also (oder beweisen wir korrekt) $A \Rightarrow f$ (also: „aus der Bedingung/Annahme A folgt ein Widerspruch“), so ist A falsch!

Bemerkungen:



$\equiv$ wird oft, vor allem in Beweisen,

$\Rightarrow B$ falsch genau dann wenn $A = t$

A.

Wichtige Beobachtung:

Gilt also (oder beweisen wir korrekt) $A \Rightarrow f$ (also: „aus der Bedingung/Annahme A folgt ein Widerspruch“), so ist A falsch!