Script generated by TTT

Title: Esparza: Diskrete Strukturen (05.11.2013)

Date: Tue Nov 05 13:47:35 CET 2013

Duration: 83:54 min

Pages: 33

Kapitel II – Grundlagen; Logik

- Logischen Inferenzen: Formalisierung.
  - Eine logische Inferenz ist eine Formel der Gestalt $F \rightarrow G$. Dabei ist F die Annahme und G die Konklusion. Eine logische Inferenz ist korrekt wenn sie gültig ist.
  - Notation: $F \models G$ (in Worten: G folgt aus F) bezeichnet, dass $F \rightarrow G$ gültig ist.

  Achtung! "G folgt aus F" ist nicht dasselbe wie "F impliziert G"

$F \rightarrow G$

1 1 1

$F \models G$

$F \rightarrow G$

β

Kapitel II – Grundlagen; Logik

- Äquivalenzregeln
  - Um Äquivalenzketten zu konstruieren können wir Äquivalenzregeln verwenden: Äquivalenzschemen, die instanziert werden können, um äquivalente Formeln zu gewinnen.
  - Äquivalenzregeln enthalten Formelvariablen (Platzhalter für Formeln).
  - Beispiel: Die Regel $(F \vee G) \wedge H \equiv (F \wedge H) \vee (G \wedge H)$ sagt: "Für alle Formeln F, G, H gilt: $(F \vee G) \wedge H$ und $(F \wedge H) \vee (G \wedge H)$ sind äquivalent"

Kapitel II – Grundlagen; Logik

- Äquivalenzregeln für $\wedge$, $\vee$, $\neg$
  - Identität: $F \wedge \textbf{true} \equiv F$
    $F \vee \textbf{false} \equiv F$
  - Dominanz: $F \vee \textbf{true} \equiv \textbf{true}$
    $F \wedge \textbf{false} \equiv \textbf{false}$
  - Idempotenz: $F \vee F \equiv F$
    $F \wedge F \equiv F$
  - Doppelte Negation: $\neg\neg F \equiv F$
  - Triviale Tautologie/Kontradiktion:
    $F \vee \neg F \equiv \textbf{true}$
    $F \wedge \neg F \equiv \textbf{false}$

Kapitel II – Grundlagen; Logik

- Äquivalenzregeln für $\wedge, \vee, \neg$
  - Kommutativität: $F \vee G \equiv G \vee F$
    $F \wedge G \equiv G \wedge F$
  - Assoziativität: $(F \vee G) \vee H \equiv F \vee (G \vee H)$
    $(F \wedge G) \wedge H \equiv F \wedge (G \wedge H)$
  - Distributivität: $F \vee (G \wedge H) \equiv (F \vee G) \wedge (F \vee H)$
    $F \wedge (G \vee H) \equiv (F \wedge G) \vee (F \wedge H)$
  - De Morgan's: $\neg(F \wedge G) \equiv \neg F \vee \neg G$
    $\neg(F \vee G) \equiv \neg F \wedge \neg G$

Augustus
De Morgan
(1806-1871)

Kapitel II – Grundlagen; Logik

- Äquivalenzregeln für andere Operatoren
  - Mit Hilfe von Äquivalenzregeln lassen sich logische Operatoren durch andere Operatoren ausdrücken.
  - Exklusives-Oder: $F \otimes G \equiv (F \vee G) \wedge \neg (F \wedge G)$
    $F \otimes G \equiv (F \wedge \neg G) \vee (G \wedge \neg F)$
  - Implikation: $F \rightarrow G \equiv \neg F \vee G$
    $F \vee G \equiv \neg F \rightarrow G$
  - Bikonditional: $F \leftrightarrow G \equiv (F \rightarrow G) \wedge (G \rightarrow F)$
    $F \leftrightarrow G \equiv \neg(F \otimes G)$

Kapitel II – Grundlagen; Logik

- Beweis von Äquivalenzen mit Äquivalenzregeln
  - Zeige $\neg(p \vee (\neg p \wedge q)) \equiv \neg p \wedge \neg q$

$$
\begin{aligned}
\neg(p \vee (\neg p \wedge q)) &\equiv \neg p \wedge \neg(\neg p \wedge q) \\
&\equiv \neg p \wedge (\neg\neg p \vee \neg q) \\
&\equiv \neg p \wedge (p \vee \neg q) \\
&\equiv (\neg p \wedge p) \vee (\neg p \wedge \neg q) \\
&\equiv \mathbf{false} \vee (\neg p \wedge \neg q) \\
&\equiv (\neg p \wedge \neg q) \vee \mathbf{false} \\
&\equiv \neg p \wedge \neg q
\end{aligned}
$$

Kapitel II – Grundlagen; Logik

- Beweis von Äquivalenzen mit Äquivalenzregeln
  - Zeige, dass $p \rightarrow q \equiv \neg q \rightarrow \neg p$.

$$
\begin{aligned}
p \rightarrow q &\equiv \neg p \vee q \\
&\equiv q \vee \neg p \\
&\equiv \neg\neg q \vee \neg p \\
&\equiv \neg q \rightarrow \neg p
\end{aligned}
$$

Kapitel II – Grundlagen; Logik

- Beweis von Äquivalenzen mit Äquivalenzregeln
  - Eine Formel F ist eine Tautologie gdw. $F \equiv \mathbf{true}$
  - Zeige, dass $((p \vee q) \wedge (\neg p \vee r) \wedge (s \vee \neg s)) \rightarrow (q \vee r)$ eine Tautologie ist.

$$((p \vee q) \wedge (\neg p \vee r) \wedge (s \vee \neg s)) \rightarrow (q \vee r)$$
$$\equiv ((p \vee q) \wedge (\neg p \vee r) \wedge \mathbf{true}) \rightarrow (q \vee r)$$
$$\equiv ((p \vee q) \wedge (\neg p \vee r)) \rightarrow (q \vee r)$$
$$\equiv \neg((p \vee q) \wedge (\neg p \vee r)) \vee (q \vee r)$$
$$\equiv (\neg(p \vee q) \vee \neg(\neg p \vee r)) \vee (q \vee r)$$

Kapitel II – Grundlagen; Logik

- Beweis von Äquivalenzen mit Äquivalenzregeln

$$\equiv (\neg(p \vee q) \vee \neg(\neg p \vee r)) \vee (q \vee r)$$
$$\equiv (\neg p \wedge \neg q) \vee (p \wedge \neg r) \vee q \vee r$$
$$\equiv (\neg p \wedge \neg q) \vee q \vee (p \wedge \neg r) \vee r$$
$$\equiv ((\neg p \vee q) \wedge (\neg q \vee q)) \vee ((p \vee r) \wedge (\neg r \vee r))$$
$$\equiv ((\neg p \vee q) \wedge \mathbf{true}) \vee ((p \vee r) \wedge \mathbf{true})$$
$$\equiv \neg p \vee q \vee p \vee r \qquad \text{(Beachte: Klammern weggelassen)}$$
$$\equiv \neg p \vee p \vee q \vee r$$
$$\equiv \mathbf{true} \vee q \vee r$$
$$\equiv \mathbf{true}$$

Kapitel II – Grundlagen; Logik

- Beweis von nicht-Äquivalenzen
  - Um zu zeigen, dass F und G nicht äquivalent sind reicht es, eine Belegung anzugeben, die zu F und G passt, und F wahr macht und G falsch (oder umgekehrt).
  - Eine solche Belegung kann systematisch mit einer Wahrheitstabelle gesucht werden, aber nicht mit Äquivalenzregeln.
  - In der Praxis oft besser:
    - Finde mit Hilfe von Regeln "einfachere" Formeln F' und G' mit $F \equiv F'$ und $G \equiv G'$.
    - Finde eine Belegung, die zeigt, dass F' und G' nicht äquivalent sind.

Kapitel II – Grundlagen; Logik

- Beweis von nicht-Äquivalenzen

  Zeige: $((p \rightarrow q) \rightarrow r)$ und $(p \rightarrow (q \rightarrow r))$ sind nicht-äquivalent.

1. $((p \rightarrow q) \rightarrow r) \equiv (\neg(\neg p \vee q) \vee r) \equiv ((p \wedge \neg q) \rightarrow r)$
2. $(p \rightarrow (q \rightarrow r)) \equiv (\neg p \vee \neg q \vee r)$
3. $((p \wedge \neg q) \vee r)$ und $(\neg p \vee \neg q \vee r)$ sind nicht äquivalent:

$((p \wedge \neg q) \vee r)$	falsch für	$p \mapsto 0, q \mapsto 1, r \mapsto 0$
$(\neg p \vee \neg q \vee r)$	wahr für	$p \mapsto 0, q \mapsto 1, r \mapsto 0$

Kapitel II – Grundlagen; Logik

- Vergleich: Wahrheitstabelle vs. Äquivalenzregeln
  - Vorteile der Wahrheitstabellen:
    - Automatische und einfache Methode.
    - Terminiert garantiert mit der richtigen Antwort
  - Nachteile der Wahrheitstabellen:
    - Die Wahrheitstabelle einer Formel mit n Variablen enthält 2^n Zeilen. Die Methode ist daher völlig ungeeignet für großes n.
    - Die Wahrheitstabelle jeder Formel mit n Variablen enthält 2^n Zeilen, egal wie „dumm" die Formel ist

$$p_1 \wedge \neg p_1 \wedge F$$

Kapitel II – Grundlagen; Logik

- Vergleich: Wahrheitstabelle vs. Äquivalenzregeln
  - Vorteile der Äquivalenzregeln:
    - Ab vier/fünf Variablen die bessere Methode für Menschen.
    - Richtige Sequenz von Regelanwendungen kann schnell zum Ziel führen.
  - Nachteile der Äquivalenzregeln:
    - Die „richtige" Regel muss erraten werden.
    - Terminierung ist nicht garantiert
    - Kann nur zeigen , das $F \equiv G$ gilt, aber nicht, dass es nicht gilt.

Kapitel II – Grundlagen; Logik

- Vergleich: Wahrheitstabelle vs. Äquivalenzregeln
  - Vorteile der Äquivalenzregeln:
    - Ab vier/fünf Variablen die bessere Methode für Menschen.
    - Richtige Sequenz von Regelanwendungen kann schnell zum Ziel führen.
  - Nachteile der Äquivalenzregeln:
    - Die „richtige" Regel muss erraten werden.
    - Terminierung ist nicht garantiert
    - Kann nur zeigen , das $F \equiv G$ gilt, aber nicht, dass es nicht gilt.

Kapitel II – Grundlagen; Logik

- Wieviele verschiedene Operatoren gibt es?
  - Die Semantik von Operatoren (Konnektoren, Junktoren) kann durch Wahrheitstabellen dargestellt werden.
  - Da die Wahrheitstabelle einer Formel mit n Variablen 2^n Einträge (1/0) hat, gibt es genau ??? verschiedene Wahrheitstabellen für Formeln mit n Variablen.

Kapitel II – Grundlagen; Logik

- Vollständige Mengen von Operatoren.
  - Einige Operatoren können durch andere „ausgedrückt werden“. Z.B. aus $p \rightarrow q \equiv \neg p \vee q$ folgt $F \rightarrow G \equiv F \vee G$ für beliebige Formeln F und G.
  - Formal: Ein Operator OP der Stelligkeit $k \geq 0$ kann durch die Operatoren $OP_1, \dots, OP_n$ ausgedrückt werden wenn es eine Formel F über $OP_1, \dots, OP_n$ (ohne die Konstanten **true** und **false**) gibt mit $OP(p_1, \cdots, p_k) \equiv F$
  - Eine Menge M von Operatoren ist vollständig wenn jeder Operator (egal welcher Arität) durch die Operatoren von M ausgedrückt werden kann.

Kapitel II – Grundlagen; Logik

- Vollständige Mengen von Operatoren.
  - Fakt: Die Menge $\{\neg, \vee, \wedge\}$ ist vollständig.

    Beispiel. Wir betrachten den 3-stelligen Operator ITE mit folgender Wahrheitstabelle:

p	q	r	$ITE(p,q,r)$
0	0	0	0
0	0	1	1
0	1	0	0
0	1	1	1
1	0	0	0
1	0	1	0
1	1	0	1
1	1	1	1

Es gilt:

$$\begin{aligned} ITE(p,q,r) \equiv\ & (\neg p \wedge \neg q \wedge r) \\ & \vee (\neg p \wedge q \wedge r) \\ & \vee (p \wedge q \wedge \neg r) \\ & \vee (p \wedge q \wedge r) \end{aligned}$$

Kapitel II – Grundlagen; Logik

- Vollständige Mengen von Operatoren.
  - Fakt: Die Mengen $\{\neg, \vee\}$ und $\{\neg, \wedge\}$ sind vollständig.

    Beobachtung: Sei V eine vollständige Menge und sei M eine Menge von Operatoren. Wenn jeder Operator aus V durch die Operatoren von M ausgedrückt werden kann, dann ist M auch vollständig.

    Fall $\{\neg, \vee\}$. Es reicht zu zeigen, dass $\wedge$ durch $\neg$ und $\vee$ ausgedrückt werden kann. Das wird mit der De Morgan´sche Regel erreicht:

$$p \wedge q \equiv \neg(\neg p \vee \neg q).$$

Fall $\{\neg, \wedge\}$. Symmetrisch.

Kapitel II – Grundlagen; Logik

- Vollständige Mengen von Operatoren.
  - Fakt: Die Mengen $\{\neg, \vee\}$ und $\{\neg, \wedge\}$ sind vollständig. $\{\wedge, \vee\}$

    Beobachtung: Sei V eine vollständige Menge und sei M eine Menge von Operatoren. Wenn jeder Operator aus V durch die Operatoren von M ausgedrückt werden kann, dann ist M auch vollständig.

    Fall $\{\neg, \vee\}$. Es reicht zu zeigen, dass $\wedge$ durch $\neg$ und $\vee$ ausgedrückt werden kann. Das wird mit der De Morgan´sche Regel erreicht:

$$p \wedge q \equiv \boxed{\neg(\neg p \vee \neg q).}$$

p_1	p_2	$\dots$	p_n	0 1
1	1		1	1

Fall $\{\neg, \wedge\}$. Symmetrisch.

Kapitel II – Grundlagen; Logik

- Vollständige Mengen von Operatoren. $F \to G \equiv \boxed{\neg F \vee G}$
  - Einige Operatoren können durch andere „ausgedrückt werden". Z.B. aus $p \to q \equiv \neg p \vee q$ folgt $F \to G \equiv F \vee G$ für beliebige Formeln F und G.
  - Formal: Ein Operator OP der Stelligkeit $k \geq 0$ kann durch die Operatoren $OP_1, \ldots, OP_n$ ausgedrückt werden wenn es eine Formel F über $OP_1, \ldots, OP_n$ (ohne die Konstanten **true** und **false**) gibt mit $OP(p_1, \cdots, p_k) \equiv F$
  - Eine Menge M von Operatoren ist vollständig wenn jeder Operator (egal welcher Arität) durch die Operatoren von M ausgedrückt werden kann.

F

¬F

F G
∧

F∧G

102

Kapitel II – Grundlagen; Logik

- Vollständig $F \to G \equiv \boxed{\neg F \vee G}$
  - Einige Op sgedrückt werden". $\to G \equiv$ $F \vee G$ fü
  - Formal: E 0 kann durch die ckt werden wenn es hne die Konstant $\cdot, p_k) \equiv F$
  - Eine Men g wenn jeder Op ie Operator n.

F

¬F

F G
∧

F∧G

New
Size
Current page size
Style
5mm
7mm
Orientation
Pages
1
OK
Cancel

102

Vorlesung Diskrete Strukturen WS 13/14
Prof. Dr. J. Esparza – Institut für Informatik, TU München

Kapitel II – Grundlagen; Logik

- Vollständige Mengen von Operatoren.
  - Wir betrachten die Operatoren

nand: $(F \text{ nand } G) \equiv (\neg (F \wedge G))$

F	G	F nand G
0	0	1
0	1	1
1	0	1
1	1	0

nor: $(F \text{ nor } G) \equiv (\neg (F \vee G))$

F	G	F nor G
0	0	1
0	1	0
1	0	0
1	1	0

105

Kapitel II – Grundlagen; Logik

- Vollständige Mengen von Operatoren.
  - Fakt: Die Mengen {nand} und {nor} sind vollständig.
    Für die Menge {nand}:

$$\begin{aligned}(\neg F) &\equiv (F \text{ nand } F)\\(F \wedge G) &\equiv (F \text{ nand } G) \text{ nand } (F \text{ nand } G)\\(F \vee G) &\equiv (F \text{ nand } F) \text{ nand } (G \text{ nand } G)\end{aligned}$$

106

Kapitel II – Grundlagen; Logik

- Vollständige Mengen von Operatoren.
  - Wir betrachten die Operatoren

nand: $(F \text{ nand } G) \equiv (\neg(F \wedge G))$

F	G	F nand G
0	0	1
0	1	1
1	0	1
1	1	0

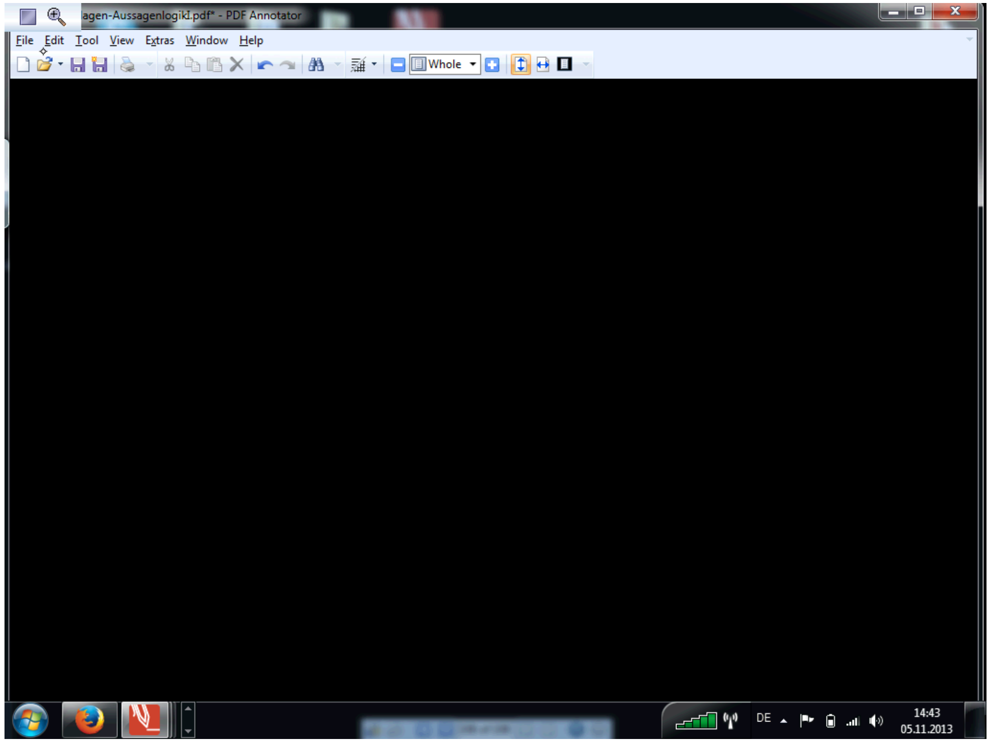
nor: $(F \text{ nor } G) \equiv (\neg(F \vee G))$

F	G	F nor G
0	0	1
0	1	0
1	0	0
1	1	0

Kapitel II – Grundlagen; Logik

- Zusammenfassung Boolesche Operatoren

Formaler Name	Umg.spr.	Stelligkeit	Symbol
Negation	NICHT	Mon.	$\neg$
Konjunktion	UND	Dyad.	$\wedge$
Disjunktion	ODER	Dyad.	$\vee$
Exclusives-Oder	XOR	Dyad.	$\otimes$
Implikation	IMPLIZIERT	Dyad.	$\rightarrow$
Bikonditional	IFF (GDW)	Dyad.	$\leftrightarrow$
NAND	NAND	Dyad.	nand
NOR	NOR	Dyad.	nor



Kapitel II – Grundlagen; Logik

- Zusammenfassung Boolesche Operatoren

Formaler Name	Umg.spr.	Stelligkeit	Symbol
Negation	NICHT	Mon.	$\neg$
Konjunktion	UND	Dyad.	$\wedge$
Disjunktion	ODER	Dyad.	$\vee$
Exclusives-Oder	XOR	Dyad.	$\otimes$
Implikation	IMPLIZIERT	Dyad.	$\rightarrow$

Modellierung von Sudoku

- Problem:
  - Gegeben ein Sudoku S
  - Konstruiere eine aussagenlogische Formel F_S, die folgende (noch nicht formal definierte) Eigenschaft erfüllt:
    - Eine (minimale) zu F_S passende Belegung macht F_S wahr genau dann, wenn die Belegung die Lösung des Sudokus charakterisiert.

Modellierung von Sudoku

- Variablen: $\{X_{YZ} \mid X,Y,Z \in \{1,\dots,9\}\}$
- Bedeutung von X_{YZ}: auf der Zeile Y, Spalte Z, liegt die Zahl X.
- Jede Zahl komm in jeder Zeile vor :

$$\bigwedge_{X=1}^{9} \bigwedge_{Y=1}^{9} (X_{Y1} \vee X_{Y2} \vee \ldots \vee X_{Y9})$$

Modellierung von Sudoku

- Jede Zahl komm in jeder Spalte vor :

$$\bigwedge_{X=1}^{9} \bigwedge_{Z=1}^{9} (X_{1Z} \vee X_{2Z} \vee \ldots \vee X_{9Z})$$

- Jede Zahl kommt im ersten Quadrat vor (die Formel n für die andere Quadrate sind analog):

$$\bigwedge_{X=1}^{9} \left(\bigvee_{Y=1}^{3} \bigvee_{Z=1}^{3} X_{YZ} \right)$$

Modellierung von Sudoku

- Jedes Feld enthält höchstens eine Zahl:

$$\bigwedge_{Y=1}^{9} \bigwedge_{Z=1}^{9} \bigwedge_{X=1}^{9} \bigwedge_{\substack{U=1 \\ U \neq X}}^{9} (\neg X_{YZ} \vee \neg U_{YZ})$$

- Anfangskonfiguration: z.B.

  $4_{11} \wedge 9_{15} \wedge \ldots \wedge 4_{99}$

Modellierung von Sudoku

- Sei F_S die Formel, die aus der Konjunktion aller vorherigen Formel besteht.
- In F_S kommen 729 (9^3) atomare Formeln vor.
- Sei β eine Belegung aller atomaren Variablen X_{YZ}. β entspricht eine Lösung des Sudokus genau dann, wenn $[F_S](\beta)=1$.
- Wenn der Sudoku gut formuliert ist, dann hat F_S genau eine erfüllende Belegung.

Modellierung von Sudoku

- Sei F_S die Formel, die aus der Konjunktion vorherigen Formel besteht.
- In F_S kommen 729 (9^3) atomare Formeln v
- Sei β eine Belegung aller atomaren Variab X_{YZ}. β entspricht eine Lösung des Sudoku genau dann, wenn $[F_S](\beta)=1$.
- Wenn der Sudoku gut formuliert ist, dann F_S genau eine erfüllende Belegung.