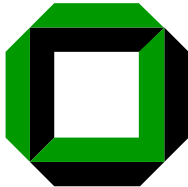


Formale Systeme

Prof. P.H. Schmitt

Fakultät für Informatik
Universität Karlsruhe (TH)

Winter 2007/2008



Sudoku

5	3			7				
6			1	9	5			
	9	8					6	
8				6				3
4			8		3			1
7				2				6
	6					2	8	
			4	1	9			5
				8			7	9



Sudoku

Vervollständigen Sie das Sudoku so, daß

5	3			7				
6			1	9	5			
	9	8					6	
8				6				3
4			8		3			1
7				2				6
	6					2	8	
			4	1	9			5
				8			7	9

- in jeder der neun Spalten
- in jeder der neun Reihen
- und in jeder der neun Regionen

alle Zahlen von 1 bis 9 vorkommen.



Sudoku

Lösung

5	3	4	6	7	8	9	1	2
6	7	2	1	9	5	3	4	8
1	9	8	3	4	2	5	6	7
8	5	9	7	6	1	4	2	3
4	2	6	8	5	3	7	9	1
7	1	3	9	2	4	8	5	6
9	6	1	5	3	7	2	8	4
2	8	7	4	1	9	6	3	5
3	4	5	2	8	6	1	7	9



Lösungsweg via Aussagenlogik

Wir führen für jede Zellenposition (i, j) des Sudoku und jede Zahl k zwischen 1 und 9 eine Boolesche Variable

$$D_{i,j}^k$$

ein, mit der Vorstellung, daß $D_{i,j}^k$ den Wert *wahr* hat, wenn auf dem Feld (i, j) die Zahl k steht.

Wir benutzen kartesische Koordinaten zur Notation von Positionen.

So ist z.B. $D_{9,1}^9$ wahr, wenn in der rechten unteren Ecke die Zahl 9 steht.



Sudoku Regeln als AL-Formeln

$$D_{1,9}^1 \vee D_{2,9}^1 \vee D_{3,9}^1 \vee D_{4,9}^1 \vee D_{5,9}^1 \vee D_{6,9}^1 \vee D_{7,9}^1 \vee D_{8,9}^1 \vee D_{9,9}^1$$

sagt, daß die Ziffer 1 mindestens einmal in der ersten Zeile vorkommen muß.

$$D_{1,1}^1 \vee D_{1,2}^1 \vee D_{1,3}^1 \vee D_{1,4}^1 \vee D_{1,5}^1 \vee D_{1,6}^1 \vee D_{1,7}^1 \vee D_{1,8}^1 \vee D_{1,9}^1$$

sagt, daß die Ziffer 1 mindestens einmal in der ersten Spalte vorkommen muß.

$$D_{1,1}^1 \vee D_{1,2}^1 \vee D_{1,3}^1 \vee D_{2,1}^1 \vee D_{2,2}^1 \vee D_{2,3}^1 \vee D_{3,1}^1 \vee D_{3,2}^1 \vee D_{3,3}^1$$

sagt, daß die Ziffer 1 mindestens einmal in der Region links unten vorkommen muß.



Zusätzliche AL-Formeln

Die bisherigen Formeln beschreiben Sudoku noch nicht genau.

Man muß noch sagen, daß auf jeder Zelle höchstens **eine** Zahl stehen kann.

$\neg(D_{1,1}^1 \wedge D_{1,1}^2), \neg(D_{1,1}^1 \wedge D_{1,1}^3), \neg(D_{1,1}^1 \wedge D_{1,1}^4), \neg(D_{1,1}^1 \wedge D_{1,1}^5),$
 $\neg(D_{1,1}^1 \wedge D_{1,1}^6), \neg(D_{1,1}^1 \wedge D_{1,1}^7), \neg(D_{1,1}^1 \wedge D_{1,1}^8), \neg(D_{1,1}^1 \wedge D_{1,1}^9),$
 $\neg(D_{1,1}^2 \wedge D_{1,1}^3), \neg(D_{1,1}^2 \wedge D_{1,1}^4), \neg(D_{1,1}^2 \wedge D_{1,1}^5), \neg(D_{1,1}^2 \wedge D_{1,1}^6),$
 $\neg(D_{1,1}^2 \wedge D_{1,1}^7), \neg(D_{1,1}^2 \wedge D_{1,1}^8), \neg(D_{1,1}^2 \wedge D_{1,1}^9), \neg(D_{1,1}^3 \wedge D_{1,1}^4),$
usw. . .



Zusätzliche AL-Formeln

Allgemein:

$$\neg(D_{i,j}^s \wedge D_{i,j}^t)$$

für alle $1 \leq i, j, s, t \leq 9$ mit $s < t$.

Ergibt $81 * 36 = 2916$ Formeln.



Wiederholung

Syntax und Semantik der Aussagenlogik



Vokabular der Aussagenlogik

Logische Zeichen

- 1** Symbol für den Wahrheitswert „wahr“
- 0** Symbol für den Wahrheitswert „falsch“
- $\neg$ Negationssymbol („nicht“)
- $\wedge$ Konjunktionssymbol („und“)
- $\vee$ Disjunktionssymbol („oder“)
- $\rightarrow$ Implikationssymbol („wenn . . . dann“)
- $\leftrightarrow$ Symbol für beiderseitige Implikation („genau dann, wenn“)
- (,) die beiden Klammern



Vokabular der Aussagenlogik

Signatur

Eine (aussagenlogische) *Signatur* ist eine abzählbare Menge Σ von Symbolen, etwa

$$\Sigma = \{P_0, \dots, P_n\}$$

oder

$$\Sigma = \{P_0, P_1, \dots\}.$$

Die Elemente von Σ heißen auch *atomare Aussagen*, *Atome* oder *Aussagevariablen*.



Formeln der Aussagenlogik

Zur Signatur Σ ist $For0_\Sigma$, die Menge der

Formeln über Σ

induktiv definiert durch

- ① $1 \in For0_\Sigma$
 $0 \in For0_\Sigma$
 $\Sigma \subseteq For0_\Sigma$
- ② wenn $A, B \in For0_\Sigma$ dann sind auch

$\neg A$

$(A \wedge B)$

$(A \vee B)$

$(A \rightarrow B)$

$(A \leftrightarrow B)$

Elemente von $For0_\Sigma$



Übungsaufgaben

Beweisen Sie durch **strukturelle Induktion**:

- ① Ist $A \in For_0_\Sigma$ und sind B, C Teilformeln von A , dann gilt
 - entweder C ist Teilformel von B
 - oder B ist echte Teilformel von C
 - oder B, C liegen disjunkt.
- ② Ist B Teilformel von $A \in For_0_\Sigma$ und zugleich Präfix von A , dann sind A, B identisch.
Volle Klammerung vorausgesetzt.



Semantik der Aussagenlogik

Es sei Σ eine aussagenlogische Signatur. Eine **Interpretation** über Σ ist eine beliebige Abbildung

$$I : \Sigma \rightarrow \{W, F\}.$$

Zu jedem I über Σ wird eine zugehörige **Auswertung** der Formeln über Σ definiert

$$val_I : For_0\Sigma \rightarrow \{W, F\}$$

mit:

$$val_I(\mathbf{1}) = W$$

$$val_I(\mathbf{0}) = F$$

$$val_I(P) = I(P) \quad \text{für jedes } P \in \Sigma$$

$$val_I(\neg A) = \begin{cases} F & \text{falls } val_I(A) = W \\ W & \text{falls } val_I(A) = F \end{cases}$$



Semantik der Aussagenlogik (Forts.)

val_I auf $(A \wedge B)$, $(A \vee B)$, $(A \rightarrow B)$, $(A \leftrightarrow B)$ wird gemäß der folgenden Tabelle berechnet

$val_I(A)$	$val_I(B)$	$val_I(A \wedge B)$	$val_I(A \vee B)$	$val_I(A \rightarrow B)$	$val_I(A \leftrightarrow B)$
W	W	W	W	W	W
W	F	F	W	F	F
F	W	F	W	W	F
F	F	F	F	W	W



Quiz

Welche der folgenden Formeln sind Tautologien?

- 1 $(A \rightarrow B) \rightarrow (\neg B \rightarrow \neg A)$ *ja*
- 2 $\neg(A \rightarrow B) \leftrightarrow (A \wedge \neg B)$ *ja*
- 3 $\neg(A \vee B) \rightarrow (A \vee B)$ *nein*
- 4 $(A \rightarrow B) \rightarrow (\neg A \rightarrow \neg B)$ *nein*
- 5 $(\neg A \vee B) \vee (A \wedge \neg B)$ *ja*



Logische Grundbegriffe

- ① Ein **Modell** einer Formel $A \in For0_\Sigma$ ist eine Interpretation I über Σ mit $val_I(A) = W$.
- ② Zu einer Formelm**enge** $M \subseteq For0_\Sigma$ ist ein Modell von M eine Interpretation I , welche Modell von jedem $A \in M$ ist.
- ③ $A \in For0_\Sigma$ heißt **allgemeingültig**
gdw
 $val_I(A) = W$ für jede Interpretation I über Σ .
- ④ $A \in For0_\Sigma$ heißt **erfüllbar**
gdw
es gibt eine Interpretation I über Σ mit $val_I(A) = W$.



Logische Grundbegriffe (Forts.)

Σ sei eine Signatur, $M \subseteq For0_\Sigma$, $A, B \in For0_\Sigma$.

- ① $M \models A$ lies: **aus M folgt A**

gdw

Jedes Modell von M ist auch Modell von A .

- ② $A, B \in For0_\Sigma$ heißen **logisch äquivalent**

gdw

$A \models_\Sigma B$ und $B \models_\Sigma A$



Einige Beispiele allgemeingültiger Formeln

$$A \rightarrow A$$

Selbstimplikation

$$\neg A \vee A$$

Tertium non datur

$$A \rightarrow (B \rightarrow A)$$

Abschwächung

$$0 \rightarrow A$$

Ex falso quodlibet

$$A \wedge A \leftrightarrow A$$

Idempotenz

$$A \wedge (A \vee B) \leftrightarrow A$$

Absorption

$$A \wedge (B \vee C) \leftrightarrow (A \wedge B) \vee (A \wedge C)$$

Distributivität

$$A \vee (B \wedge C) \leftrightarrow (A \vee B) \wedge (A \vee C)$$

Distributivität



Einige Beispiele allgemeingültiger Formeln (Fortsetzung)

$(A \rightarrow B) \leftrightarrow (\neg B \rightarrow \neg A)$ Kontraposition

$(A \rightarrow (B \rightarrow C)) \leftrightarrow$

$((A \rightarrow B) \rightarrow (A \rightarrow C))$ Verteilen

$\neg(A \vee B) \leftrightarrow \neg A \wedge \neg B$ De Morgan

$\neg(A \wedge B) \leftrightarrow \neg A \vee \neg B$ De Morgan



Einfache Sätze

Theorem

- ① A erfüllbar gdw $\neg A$ nicht allgemeingültig
- ② $\models A$ gdw A ist allgemeingültig.
- ③ $\models \neg A$ gdw A ist unerfüllbar.
- ④ $A \models B$ gdw $\models A \rightarrow B$
- ⑤ $M \cup \{A\} \models B$ gdw $M \models A \rightarrow B$
- ⑥ A, B sind logisch äquivalent gdw $A \leftrightarrow B$ ist allgemeingültig.



Das Craigsche Interpolationslemma

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.

An eventuelle Vorkommen von **1** und **0** in C werden keine Einschränkungen gemacht.



Interpolationslemma: Beweis

Seien $P_1, \dots, P_n$ alle in A vorkommenden aussagenlogischen Atome, die nicht in B vorkommen.

Für Konstanten $c_i \in \{1, 0\}$ bezeichnen wir mit $A[c_1, \dots, c_n]$ die Formeln, die aus A hervorgeht, indem P_i durch c_i ersetzt wird für alle $1 \leq i \leq n$.

Wir setzen

$$C \equiv \bigvee_{(c_1, \dots, c_n) \in \{1, 0\}^n} A[c_1, \dots, c_n]$$

Offensichtlich kommen in C nur noch aussagenlogische Atome vor, die A und B gemeinsam sind.



Beweis (Forts. 1)

Sei jetzt I eine Interpretation mit $val_I(A) = W$,
dann gilt auch

$$val_I(A[c_1, \dots, c_n]) = W$$

für $c_i = I(P_i)$.

Damit gilt auch $val_I(C) = W$.

Insgesamt haben wir also schon $\models A \rightarrow C$ gezeigt.



Beweis (Forts. 2)

Sei jetzt I eine Interpretation mit $val_I(C) = W$.

Für (mindestens) eine Wahl von Konstanten $(c_1, \dots, c_n) \in \{\mathbf{1}, \mathbf{0}\}^n$ gilt also $val_I(A[c_1, \dots, c_n]) = W$.

Dieselbe Aussage können wir auch anders schreiben: Wir definieren die Belegung J durch

$$J(P) = \begin{cases} W & \text{falls } P = P_i \text{ für } 1 \leq i \leq n \text{ mit } c_i = \mathbf{1} \\ F & \text{falls } P = P_i \text{ für } 1 \leq i \leq n \text{ mit } c_i = \mathbf{0} \\ I(P) & \text{sonst} \end{cases}$$

Offensichtlich gilt $val_J(A) = W$

Nach der Voraussetzung gilt also auch $val_J(B) = W$.

Da I und J sich nur unterscheiden für die aussagenlogische Atome, die nicht in B vorkommen, gilt auch

$$val_I(B) = W.$$



Revival des Craigschen Interpolationslemmas

Anwendung des Interpolationslemmas in der Modellprüfung (model checking) durch Ken McMillan.

siehe

<http://www.cs.utah.edu/tphols2004/mcmillan.abstract.html>

Interpolation and SAT-based Model Checking

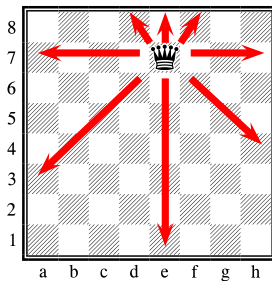
K.L. McMillan

Proceedings Computer Aided Verification (CAV03)



Das 8-Damen Problem

Man platziere acht Damen so auf einem Schachbrett, daß sie sich gegenseitig nicht bedrohen.



Eine Lösung des 8-Damen Problems

