Nachklausur Logik, Semantik und Verifikation SS 2001

Prof. Dr. Gert Smolka, Dr. Christian Schulte

18. Oktober 2001

Name und Vorname

Matrikelnummer

Hinweise:

- Bitte alle Lösungen direkt auf den Aufgabenblättern notieren.
- Hilfsmittel sind nicht zugelassen.
- Für die Bearbeitung der Klausur stehen 150 Minuten zur Verfügung. Insgesamt sind 150 Punkte erreichbar. Die Punkteverteilung gibt Ihnen also einen Anhaltspunkt, wieviel Zeit Sie auf eine Aufgabe verwenden sollten.
- Zum Bestehen der Klausur genügt die Hälfte (75) der maximal erreichbaren Punkte.

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	$\sum$
5	12	14	14	8	5	7	4	11	15	12	9	5	8	14	8	151

Note	

Aufgabe 1: Aussagenlogik ($1+1+1+1+1=5$**)** Sei *Cla* die Menge der aussagenlogischen Klauseln und f die folgende Funktion:

$$\begin{aligned} f &\in \mathcal{P}_{fin}(Cla) \to Den \\ f(S) &= \mathcal{K}[\![S]\!] \end{aligned}$$

(a) Ist f injektiv?

(b) Ist f surjektiv?

(c) Gilt $\forall S_1, S_2 \in \mathcal{P}_{fin}(Cla) : \ (S_1 \subseteq S_2 \Rightarrow f(S_1) \subseteq f(S_2))$

(d) Gilt $\exists C \in Cla : \ \mathcal{D}[\![\{C\}]\!] = f(\{C\})$?

(e) Gilt $\forall S \in \mathcal{P}_{fin}(Cla)\ \forall S' \subsetneq S : \ \mathcal{K}[\![S]\!] \neq \mathcal{K}[\![S']\!]$?

Aufgabe 2: Aussagenlogik ($2+5+5=12$**)** Seien X, Y, $Z \in \mathit{Var}$ paarweise verschiedene Variablen. Zusätzlich sei die Variablenordnung $X < Y < Z$.

(a) Geben Sie eine aussagenlogische Formel A an mit:

$$\mathcal{M}[\![A]\!] = \{\sigma \in \Sigma \mid \sigma(X) + \sigma(Y) + \sigma(Z) = 1\}$$

(b) Geben Sie einen binären Entscheidungsbaum für A an.

(c) Geben Sie ein reduziertes OBDD für A an. Sie dürfen dabei die Knoten für 0 und 1 mehr als einmal verwenden.

Aufgabe 3: Aussagenlogik ($4+2+4+2+2=14$**)** Seien $X, Y, Z \in \mathit{Var}$ verschiedene aussagenlogische Variablen. Gegeben sei die folgende aussagenlogische Formel:

$$(\neg X \wedge \neg Y \wedge Z) \vee (X \wedge Z) \vee (X \wedge Y \wedge \neg Z)$$

(a) Geben Sie die disjunktive Primform an. Benutzen Sie dazu Resolution und geben Sie den Resolutionsgraphen an.

(b) Geben Sie eine disjunktive Minimalform an.

(c) Geben Sie eine konjunktive Normalform an. Benutzen Sie dazu ein Tableau mit Subsumtion.

(d) Geben Sie die konjunktive Primform an. Sie brauchen keinen Resolutionsgraphen anzugeben.

(e) Geben Sie eine konjunktive Minimalform an.

Aufgabe 4: Transformation von Formeln ($2 + 2 + 10 = 14$) Nehmen Sie an, dass die Syntax für aussagenlogische Formeln alternativ wie folgt definiert ist:

$$A, B, C \in \mathit{For} = 0 \quad | \quad 1 \quad | \quad X \quad | \quad A \to B; C$$

Dabei soll $A \to B; C$ dieselbe Semantik wie die Formel $(\neg A \vee B) \wedge (A \vee C)$ haben.

Sei die Funktion t wie folgt definiert:

$$\begin{aligned} t &\in \mathit{For} \to \mathit{For} \\ t(0) &= 1 \\ t(1) &= 0 \\ t(X) &= X \to 0; 1 \\ t(A \to B; C) &= t(A) \to t(C); t(B) \end{aligned}$$

(a) Geben Sie eine passende Definition für $\mathcal{F} \in \mathit{For} \to \Sigma \to \{0, 1\}$ an.

$$\mathcal{F}[\![0]\!]\sigma =$$

$$\mathcal{F}[\![1]\!]\sigma =$$

$$\mathcal{F}[\![X]\!]\sigma =$$

$$\mathcal{F}[\![A \to B; C]\!]\sigma =$$

(b) Geben Sie eine passende Definition für $\mathcal{M} \in \mathit{For} \to \mathcal{P}(\Sigma)$ an.

$$\mathcal{M}[\![0]\!] =$$

$$\mathcal{M}[\![1]\!] =$$

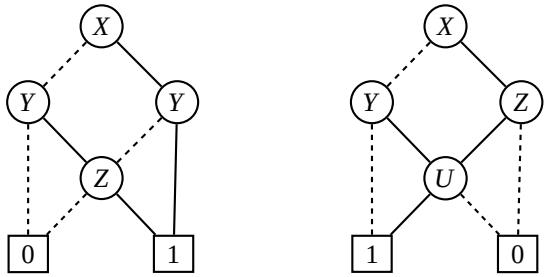
$$\mathcal{M}[\![X]\!] =$$

$$\mathcal{M}[\![A \to B; C]\!] =$$

(c) Sei $A \in \mathit{For}$ und $\sigma \in \Sigma$. Beweisen Sie durch strukturelle Induktion über A:

$$\mathcal{F}[\![t(A)]\!]\sigma = 1 - \mathcal{F}[\![A]\!]\sigma$$

Aufgabe 5: OBDDs ($3 + 3 + 2 = 8$**)** Gegeben seien die folgenden OBDDs.



O_1 O_2

(a) Geben Sie eine äquivalente disjunktive Normalform für O_1 an.

(b) Geben Sie eine äquivalente disjunktive Normalform für O_2 an.

(c) Sei A eine zu O_1 äquivalente aussagenlogische Formel. Geben Sie ein reduziertes OBDD mit Variablenordnung $X < Y < Z$ für $\neg A$ an.

Aufgabe 6: Aussagenlogische Unerfüllbarkeit ($1 + 4 = 5$**)** Zeigen Sie durch ein geschlossenes Tableau, dass die folgende aussagenlogische Formel unerfüllbar ist:

$$(X \vee \neg U) \wedge (U \vee \neg Z) \wedge (Z \vee \neg Y \vee X) \wedge \neg X \wedge Y$$

Dabei sind $X, Y, Z, U \in \mathit{Var}$ vier verschiedene Variablen.

(a) Welches Tableau verwenden Sie (konjunktiv, disjunktiv)?

(b) Geben Sie das Tableau an:

Aufgabe 7: Grundregeln und Fixpunkte ($2+2+1+1+1=7$) Sei die Menge $M \subseteq \mathbb{Z}$ durch die folgenden Inferenzregeln definiert:

$$\frac{}{4 \in M} \qquad \frac{x \in M \qquad y = 2x+1 \mod 6}{y \in M} \qquad \frac{x \in M \qquad y = 3x+2 \mod 6}{y \in M}$$

(a) Geben Sie die durch die Inferenzregeln definierte Grundregelmenge R an.

$R =$

(b) Geben Sie die Mengen $\hat{R}^0(\emptyset)$, $\hat{R}^1(\emptyset)$, $\hat{R}^2(\emptyset)$, $\hat{R}^3(\emptyset)$ und $\hat{R}^4(\emptyset)$ an.

$\hat{R}^0(\emptyset) =$

$\hat{R}^1(\emptyset) =$

$\hat{R}^2(\emptyset) =$

$\hat{R}^3(\emptyset) =$

$\hat{R}^4(\emptyset) =$

(c) Geben Sie die Menge $\bigcup_{i \in \mathbb{N}} \hat{R}^i(\emptyset)$ an.

(d) Geben Sie den kleinsten Fixpunkt von $\hat{R}$ an.

(e) Geben Sie das kleinste $P \subseteq \mathbb{Z}$ an mit $\hat{R}(P) \subseteq P$.

Aufgabe 8: Approximation von Funktionen ($2 + 2 = 4$**)** Gegeben sei die folgende rekursive Prozedurdeklaration:

```
fun gcd(n,m) = if n=0 then m
               else gcd(m mod n, n)
val gcd : int * int -> int
```

(a) Geben Sie das der Deklaration entsprechende Funktional `gcdFun` an.

(b) Geben Sie die ersten vier Approximationen für `gcd` an.

Aufgabe 9: Fallunterscheidung für IMP ($1+1+3+3+3=11$**)** Wir betrachten eine Variante IMP' von IMP, in der es zusätzlich zum Konditional auch eine Fallunterscheidung gibt. Die Ausführung einer Fallunterscheidung

`case` b_1 `then` c_1 `|` b_2 `then` c_2

ist folgendermassen:

- Wenn b_1 gilt, wird c_1 ausgeführt.
- Wenn b_2 gilt und b_1 nicht gilt, wird c_2 ausgeführt.
- Gelten weder b_1 noch b_2, wird keines der beiden Kommandos ausgeführt.

(a) Geben Sie ein zu

`case` b_1 `then` c_1 `|` b_2 `then` c_2

äquivalentes IMP'-Kommando ohne Fallunterscheidung an.

(b) Geben Sie ein zu

`if` b `then` c_1 `else` c_2

äquivalentes IMP'-Kommando ohne Konditional an.

(c) Geben Sie für die denotationale Semantik von IMP' die Gleichung für die Fallunterscheidung an.

(d) Geben Sie für die operationale Semantik von IMP' die Inferenzregeln für die Fallunterscheidung an.

$$\frac{}{\sigma \vdash \texttt{case}\ b_1\ \texttt{then}\ c_1\ \texttt{|}\ b_2\ \texttt{then}\ c2 \Rightarrow}$$

$$\frac{}{\sigma \vdash \texttt{case}\ b_1\ \texttt{then}\ c_1\ \texttt{|}\ b_2\ \texttt{then}\ c2 \Rightarrow}$$

$$\frac{}{\sigma \vdash \texttt{case}\ b_1\ \texttt{then}\ c_1\ \texttt{|}\ b_2\ \texttt{then}\ c2 \Rightarrow}$$

(e) Geben Sie die Hoare-Regel für die Fallunterscheidung an.

$$\frac{}{\vdash \{A\}\ \texttt{case}\ b_1\ \texttt{then}\ c_1\ \texttt{|}\ b_2\ \texttt{then}\ c2\ \{B\}}$$

Aufgabe 10: Programmkonstruktion (15**)** Zur Erinnerung: Ein mit Schleifeninvarianten annotiertes Kommando *c erfüllt* eine Spezifikation (A, B) genau dann, wenn gilt:

(1) Alle Verifikationsbedingungen für $\{A\}\ c\ \{B\}$ sind erfüllt.

(2) c weist nur Variablen zu, die in A nicht vorkommen.

(3) c terminiert für jeden Zustand, der A erfüllt.

Geben Sie ein annotiertes Kommando an, das die folgende Spezifikation erfüllt:

$$(X \geq 1, \quad 3^Y \leq X \wedge X < 3^{Y+1})$$

Aufgabe 11: Verifikation ($6 + 6 = 12$**)** Sei $I \in \mathit{Assn}$. Betrachten Sie die folgende Korrektheitsaussage:

$\{ X \geq 0 \}$
`Y:=0; Z:=X;`
$\{ I \}$
`while 2≤Z do`
`    Y:=Y+1; Z:=Z-2;`
$\{ X = 2 * Y + Z \wedge Z \geq 0 \wedge Z \leq 1 \}$

(a) Geben Sie eine Invariante I an, für die alle Verifikationsbedingungen gelten.

(b) Geben Sie die Verifikationsbedingungen an (in möglichst expliziter Form, wenden Sie insbesondere alle Substitutionen an).

Aufgabe 12: Fragen zu Programmverifikation ($4 + 2 + 2 + 1 = 9$**)**

(a) Sei c das Kommando:

```
Y:=0; while Y≠X do Y:=Y+2
```

Geben Sie $A \in \mathit{Assn}$ an, so dass die beiden folgenden Aussagen gelten:

(i) $\models \{A\}\ c\ \{X = Y\}$
(ii) $\models \{\neg A\}\ c\ \{\mathit{false}\}$

(b) Geben Sie die Hoare-Regel für die while-Schleife an.

(c) Definieren Sie mithilfe der denotationalen Semantik von IMP: Ein $W \in \mathit{Assn}$ ist *schwächste Vorbedingung* für ein Kommando c und $B \in \mathit{Assn}$ genau dann, wenn

(d) Gilt: Wenn $\models \{A\}\ c\ \{B\}$, dann ist c total korrekt für $\langle A, B\rangle$?

Aufgabe 13: Prädikatenlogische Resolution (5) Zeigen Sie mit einem Resolutionsgraphen, dass die Menge der folgenden Klauseln unerfüllbar ist (p und q sind verschiedene einstellige Prädikatensymbole, f, g und h sind verschiedene einstellige Funktionssymbole, a ist ein Konstantensymbol):

$$\{\neg p(x)\} \qquad \{p(f(y)),\ p(g(y)),\ q(h(f(y)))\} \qquad \{\neg q(h(f(z))),\ q(f(z))\} \qquad \{\neg q(f(a))\}$$

Aufgabe 14: Berechenbarkeit und Expressivität ($1+1+1+1+1+1+1+1=8$**)**

(a) Geben Sie eine Teilmenge von #*Assn* an, die entscheidbar ist.

(b) Geben Sie eine Teilmenge von #*Assn* an, die testbar, aber nicht entscheidbar ist.

(c) Geben Sie eine Teilmenge von #*Assn* an, die nicht testbar ist.

(d) Gibt es eine prädikatenlogische Signatur Σ und eine Formelmenge $R \subseteq For_\Sigma$, so dass jedes Modell von R ein abzählbares Universum hat?

(e) Ist prädikatenlogische Erfüllbarkeit testbar?

(f) Sei M eine Menge aussagenlogischer Formeln. Gilt:

$$M \text{ unerfüllbar} \quad \Longleftrightarrow \quad \forall M' \in \mathcal{P}_{fin}(M) : \ M' \text{ unerfüllbar}$$

(g) Wieviel berechenbare Funktionen $f \in \mathbb{Z} \to \mathbb{Z}$ gibt es (endlich viele, abzählbar unendlich viele, überabzählbar viele)?

(h) Ist Gültigkeit in *Assn* testbar?

Aufgabe 15: Prädikatenlogische Vereinfachung ($2 + 7 + 5 = 14$**)** Nehmen Sie an, dass die Syntax für prädikatenlogische Formeln alternativ wie folgt definiert ist:

$$A, B \in \mathit{For} = p(t_1, \ldots, t_{|p|}) \quad | \quad \neg A \quad | \quad A \wedge B \quad | \quad \forall x\ A$$

(a) Geben Sie passende Definitionen für die folgenden Abkürzungen an.

$A \vee B \quad \mapsto$

$\exists x\ A \quad \mapsto$

(b) Geben Sie die rechten Seiten für disjunktive prädikatenlogische Vereinfachung an. Zur Erinnerung:

- Eine Struktur $\mathcal{A}$ heißt Modell einer Klausel C genau dann, wenn $\mathcal{A}$ zu jeder Formel in C passt, und
$$\exists \sigma \in Val_{\mathcal{A}}\ \forall A \in C\ :\ \mathcal{A}[\![A]\!]\sigma = 1$$
- Eine Struktur $\mathcal{A}$ heißt Modell einer Klauselmenge S genau dann, wenn $\mathcal{A}$ Modell einer Klausel in S ist.
- Eine Klauselmenge S heißt allgemeingültig genau dann, wenn jede Struktur, die zu jeder Formel in S passt, ein Modell von S ist.

Geben Sie auch die Bedingungen für die Regeln (4) und (5) an.

(1) $S, (C, \neg\neg A) \xrightarrow{d}$

(2) $S, (C, A_1 \wedge A_2) \xrightarrow{d}$

(3) $S, (C, \neg(A_1 \wedge A_2) \xrightarrow{d}$

(4) $S, (C, \forall x\ A) \xrightarrow{d}$

falls

(5) $S, (C, \neg\forall x\ A) \xrightarrow{d}$

falls

(c) Geben Sie eine Ableitung

$$\{\{\forall x\ (\neg\forall y\ p(x,y) \wedge \neg\forall z\ q(z))\}\} \xrightarrow{d} \cdots \xrightarrow{d} S$$

an, so dass S literal ist.

$\{\{\forall x\ (\neg\forall y\ p(x,y) \wedge \neg\forall z\ q(z))\}\}$

Aufgabe 16: Unifikation ($4+4=8$**)** Im folgenden bezeichnen $a,\ f, g, h, i$ verschiedene Funktionssymbole.

(a) Wenden Sie die Unifikationsregeln auf die folgende Gleichungsmenge an, bis Sie eine widerlegte oder gelöste Gleichungsmenge erhalten. Geben Sie einen prinzipalen Unifikator der Gleichungsmenge an, wenn einer existiert. Unterstreichen Sie widerlegte Gleichungen.

$$\{i(x, g(h(a,a)), g(h(z,z))) \doteq i(f(y,y), g(y), g(z))\} \quad \overset{u}{\rightarrow}$$

(b) Wenden Sie die Unifikationsregeln auf die folgende Gleichungsmenge an, bis Sie eine widerlegte oder gelöste Gleichungsmenge erhalten. Geben Sie einen prinzipalen Unifikator der Gleichungsmenge an, wenn einer existiert. Unterstreichen Sie widerlegte Gleichungen.

$$\{ f(h(x), g(x), i(h(x))) \doteq f(h(g(z)), g(g(y)), y)\} \quad \overset{u}{\rightarrow}$$