Klausur Logik, Semantik und Verifikation
SS 2001

Prof. Dr. Gert Smolka, Dr. Christian Schulte

11. Juli 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	17	$\sum$
5	12	14	14	4	5	7	4	11	15	12	9	5	8	14	8	3	150

Note	

Aufgabe 1: Aussagenlogik ($1+1+1+1+1=5$**)** Sei *For* die Menge der aussagenlogischen Formeln, *PF* die Menge der Primformen, und f die folgende Funktion:

$$\begin{aligned} f &\in For \to PF \\ f(A) &= S, \text{ mit } S \text{ ist die konjunktive Primform von } A \end{aligned}$$

(a) Ist f injektiv?

(b) Ist f surjektiv?

(c) Gilt $\forall A \in For: \; FV(\{\{A\}\}) = FV(f(A))$? Dabei bezeichnet FV die Funktion, die einer Klauselmenge die in ihr auftretenden Variablen zuordnet.

(d) Gilt $\exists A \in For: \; \mathcal{D}[\![\{\{A\}\}]\!] = \mathcal{K}[\![f(A)]\!]$?

(e) Gilt $\forall S \in PF \; \forall S' \subsetneq S: \; \mathcal{K}[\![S]\!] \neq \mathcal{K}[\![S']\!]$?

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:

$$\mathcal{M}[\![A]\!] = \{\sigma \in \Sigma \mid \sigma(X) + \sigma(Y) + \sigma(Z) = 2\}$$

(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:

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

(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:

$$A, B \in \mathit{For} = X \quad | \quad \neg A \quad | \quad A \Rightarrow B$$

Sei die Funktion t wie folgt definiert:

$$\begin{array}{rcl} t & \in & \mathit{For} \to \mathit{For} \\ t(X) & = & \neg X \\ t(\neg A) & = & \neg t(A) \\ t(A \Rightarrow B) & = & \neg(t(B) \Rightarrow t(A)) \end{array}$$

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

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

$$\mathcal{F}[\![\neg A]\!]\sigma \quad =$$

$$\mathcal{F}[\![A \Rightarrow B]\!]\sigma \quad =$$

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

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

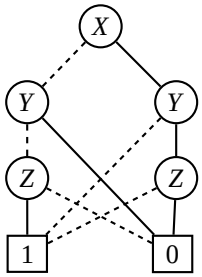
$$\mathcal{M}[\![\neg A]\!] \quad =$$

$$\mathcal{M}[\![A \Rightarrow B]\!] \quad =$$

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

$$\mathcal{F}[\![t(A)]\!]\sigma = 1 \quad \Longleftrightarrow \quad \mathcal{F}[\![A]\!]\sigma = 0$$

Aufgabe 5: OBDDs ($3 + 1 = 4$**)** Gegeben sei das folgende OBDD.



(a) Geben Sie eine äquivalente disjunktive Normalform an.

(b) Sei ein reduziertes OBDD für eine beliebige Formel A gegeben. Wieviele Knoten hat ein reduziertes OBDD mit gleicher Variablenordnung für $\neg A$ (gleich viele, verschieden viele)?

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

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

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:

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

(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 min(n,m) = if n=0 then 0
               else if m=0 then 0
                    else 1 + min(n-1,m-1)
val min : int * int -> int
```

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

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

Aufgabe 9: Do-while-Schleifen ($1 + 1 + 3 + 3 + 3 = 11$**)** Wir betrachten eine Variante IMP' von IMP, in der es zusätzlich do-while-Schleifen (`do c while b`) gibt. Die Ausführung eines do-while-Kommandos

```
do c while b
```

führt `c` mindestens einmal aus, und die Ausführung von `c` wird wiederholt solange `b` gilt. Tipp: Die do-while-Schleife entspricht `do c while (b)` in C.

(a) Geben Sie ein zu `do c while b` äquivalentes IMP'-Kommando ohne do-while-Schleifen an.

(b) Geben Sie ein zu `while b do c` äquivalentes IMP'-Kommando ohne while-do-Schleifen an.

(c) Geben Sie für die operationale Semantik von IMP' die Inferenzregeln für do-while-Schleifen an.

$$\frac{\mathcal{B}[\![b]\!]\sigma' = 1}{\sigma \vdash \texttt{do } c \texttt{ while } b \Rightarrow}$$

$$\frac{\mathcal{B}[\![b]\!]\sigma' = 0}{\sigma \vdash \texttt{do } c \texttt{ while } b \Rightarrow}$$

(d) Geben Sie für die denotationale Semantik von IMP' die Gleichung für do-while-Schleifen zusammen mit einer passenden Hilfsfunktion Γ' an.

$\mathcal{C}[\![\texttt{do } c \texttt{ while } b]\!] =$

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

$$\frac{}{\vdash \{A\}\ \texttt{do}\ c\ \texttt{while}\ b\ \{B \wedge \neg b\}}$$

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:

$$(X \geq 1, \quad 2^Y \leq X \wedge X < 2^{Y+1})$$

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

$\{ X \geq 0 \}$
```
Y:=0; Z:=0;
```
$\{ I \}$
```
while Y+Z+Z+1≤X do
    Y:=Y+Z+Z+1; Z:=Z+1;
```
$\{ Z^2 \leq X \wedge X < (Z+1)^2 \wedge Y = Z^2 \}$

(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+1
```

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 Zuweisung an.

(c) Definieren Sie mithilfe der denotationalen Semantik von IMP: Ein Kommando c *erfüllt* eine Spezifikation $\langle A, B\rangle$ genau dann, wenn

(d) Ist es testbar, ob ein Kommando c eine Spezifikation $\langle A, B\rangle$ erfüllt?

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 und g sind verschiedene einstellige Funktionssymbole, a ist ein Konstantensymbol):

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

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

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

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

(c) Geben Sie eine Teilmenge von #*Com* 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 überabzählbares Universum hat?

(e) Ist prädikatenlogische Unerfüllbarkeit testbar?

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

$$M \text{ unerfüllbar} \quad \Longleftrightarrow \quad \forall M' \subseteq M : \ M' \text{ unerfüllbar}$$

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

(h) Ist Unerfüllbarkeit 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:

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

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

$A \wedge B \ \mapsto$

$\exists x\ A \ \mapsto$

(b) Geben Sie die rechten Seiten für konjunktive prädikatenlogische Vereinfachung an. Geben Sie auch die Bedingungen für die Regeln (4) und (5) an.

(1) $S, (C, \neg\neg A) \ \overset{s}{\rightarrow}$

(2) $S, (C, A_1 \vee A_2) \ \overset{s}{\rightarrow}$

(3) $S, (C, \neg(A_1 \vee A_2) \ \overset{s}{\rightarrow}$

(4) $S, (C, \forall x\ A) \ \overset{s}{\rightarrow}$

falls

(5) $S, (C, \neg\forall x\ A) \ \overset{s}{\rightarrow}$

falls

(c) Geben Sie eine Ableitung

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

an, so dass S literal ist.

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

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.

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

(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.

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

Aufgabe 17: Fragen zu Unifikation ($1 + 2 = 3$**)**

(a) Seien t_1 und t_2 zwei unifizierbare Grundterme. Geben Sie einen prinizipalen Unifikator von $\{t_1 \doteq t_2\}$ an.

(b) Definieren Sie: Eine Gleichungsmenge E ist *gelöst*, genau dann wenn