2. Klausur Logik, Semantik und Verifikation (SS 2003)

Prof. Dr. Gert Smolka   Marco Kuhlmann, MSc

2. August 2003

Name	Sitzplatz
Matrikelnummer	Code

Bitte öffnen Sie das Klausurheft erst dann, wenn Sie dazu aufgefordert werden.

Sie können die Klausur nur auf dem für Sie vorgesehen Platz mitschreiben. Sie müssen das mit Ihrem Namen und Ihrer Matrikelnummer versehene Klausurheft verwenden.

Hilfsmittel sind nicht zugelassen. Am Arbeitsplatz dürfen nur Schreibgeräte, Getränke, Speisen und Ausweise mitgeführt werden. Taschen und Jacken müssen an den Wänden des Klausursaals zurückgelassen werden.

Verlassen des Saals ohne Abgabe des Klausurhefts gilt als Täuschungsversuch.

Wenn Sie während der Bearbeitung zur Toilette müssen, geben Sie bitte Ihr Klausurheft bei der Aufsicht ab. Es kann immer nur eine Person zur Toilette.

Alle Lösungen müssen auf den bedruckten rechten Seiten des Klausurhefts notiert werden. Die leeren linken Seiten dienen als Platz für Skizzen und werden **nicht korrigiert.** Notizpapier ist nicht zugelassen. Sie können mit Bleistift schreiben.

Für die Bearbeitung der Klausur stehen 150 Minuten zur Verfügung. Insgesamt können 150 Punkte erreicht werden. Die für jede Aufgabe angebene Punktzahl gibt Ihnen also einen Anhaltspunkt, wieviel Zeit Sie auf die Bearbeitung der Aufgabe verwenden sollten. Zum Bestehen der Klausur genügen 75 Punkte.

Bitte legen Sie zur Identifikation Ihren Personalausweis bzw. Reisepass sowie Ihren Studierendenausweis neben sich.

Viel Erfolg!

1	2	3	4	5	6	7	8	9	Summe
18	12	15	18	15	24	21	12	15	150

Note

Aufgabe 1: Analyse von Lambda-Termen (18 = 12 + 3 + 3**)**

Sei der folgende Lambda-Term gegeben:

$$\lambda g f x . g(f x)(g(\lambda y . x) x) \qquad \text{mit} \qquad \tau g = (\mathbb{N} \to \mathbb{N}) \to \mathbb{N} \to \mathbb{N}.$$

(a) Geben Sie die de Bruijnsche Darstellung des Terms an.

(b) Geben Sie die Stufe des Terms an.

(c) Geben Sie die Variablen g, f, x und y als Paare (n, t) an. Nehmen Sie dabei an, dass der Term α-normal ist.

Aufgabe 2: Lambda-Elimination ($12 = 3 * 4$**)**

Sei eine Struktur $\mathcal{A}$ gegeben, die die Konstanten I, K, S wie üblich interpretiert:

$$\begin{aligned} Ix &\models\!\mid_{\mathcal{A}} x \\ Kyx &\models\!\mid_{\mathcal{A}} y \\ Sfgx &\models\!\mid_{\mathcal{A}} fx(gx) \end{aligned}$$

Geben Sie für die folgenden Terme $\mathcal{A}$-äquivalente kombinatorische Terme an:

$\lambda yx\,.\,fx \models\!\mid_{\mathcal{A}}$

$\lambda xy\,.\,y(xy) \models\!\mid_{\mathcal{A}}$

$\lambda x\,.\,xa \models\!\mid_{\mathcal{A}}$

Aufgabe 3: Pränexform (15 = 3 + 5 + 7)

Ein Term ist in ∃∀-Pränexform, wenn er die Form

$$\exists x_1 \dots \exists x_m \forall y_1 \dots \forall y_n M$$

hat, wobei $m, n \geq 0$ gelten soll und M ein Term ist, der keine Quantorenkonstanten enthält. Wir betrachten eine Struktur $\mathcal{A}$, die die logischen Konstanten $\forall, \exists, \wedge, \Rightarrow$ wie üblich interpretiert und in der daher die folgenden Äquivalenzen gelten:

$$\begin{array}{rlrl}
\neg(\exists x\colon M) & \models\!\mid_{\mathcal{A}} \forall x\colon \neg M & \neg(\forall x\colon M) & \models\!\mid_{\mathcal{A}} \exists x\colon \neg M \\
\forall x \exists y\colon M & \models\!\mid_{\mathcal{A}} \exists z \forall x\colon M[y := zx] & \exists x \forall y\colon M & \models\!\mid_{\mathcal{A}} \forall z \exists x\colon M[y := zx] \\
\exists x\colon M \wedge N & \models\!\mid_{\mathcal{A}} (\exists x\colon M) \wedge N & \forall x\colon M \vee N & \models\!\mid_{\mathcal{A}} (\forall x\colon M) \vee N \\
\exists x\colon M \vee N & \models\!\mid_{\mathcal{A}} (\exists x\colon M) \vee N & \forall x\colon M \wedge N & \models\!\mid_{\mathcal{A}} (\forall x\colon M) \wedge N
\end{array}$$

Die untersten 4 Äquivalenzen gelten nur für den Fall, dass x in N nicht frei vorkommt.

Bestimmen Sie zu den folgenden Termen $\mathcal{A}$-äquivalente Terme in ∃∀-Pränexform:

$\forall x\, \exists y\colon f x y \models\!\mid_{\mathcal{A}}$

$\forall x\colon (\forall y\colon f y) \Rightarrow f x \models\!\mid_{\mathcal{A}}$

$\forall x\colon (\forall y\colon f x y) \Leftrightarrow g x \models\!\mid_{\mathcal{A}}$

Aufgabe 4: Ordnungseigenschaften ($18 = 6 * 3$)

Sei eine Menge X und eine partielle Ordnung $\leq$ für X gegeben.

(a) Geben Sie ein Prädikat $os \in X \to (X \to \mathbb{B}) \to \mathbb{B}$ an, das testet, ob ein $x \in X$ eine *obere Schranke* einer durch ihre charakteristische Funktion $f \in X \to \mathbb{B}$ gegebenen Menge ist.

$os = \lambda\, x \in X\,.\, \lambda\, f \in X \to \mathbb{B}\,.$

(b) Geben Sie ein Prädikat $sup \in X \to (X \to \mathbb{B}) \to \mathbb{B}$ an, das testet, ob ein $x \in X$ das *Supremum* einer durch ihre charakteristische Funktion $f \in X \to \mathbb{B}$ gegebenen Menge ist.

$sup = \lambda\, x \in X\,.\, \lambda\, f \in X \to \mathbb{B}\,.$

(c) Geben Sie ein Prädikat $ge \in X \to (X \to \mathbb{B}) \to \mathbb{B}$ an, das testet, ob ein $x \in X$ das *größte Element* einer durch ihre charakteristische Funktion $f \in X \to \mathbb{B}$ gegebenen Menge ist.

$ge = \lambda\, x \in X\,.\, \lambda\, f \in X \to \mathbb{B}\,.$

(d) Geben Sie ein Prädikat $me \in X \to (X \to \mathbb{B}) \to \mathbb{B}$ an, das testet, ob ein $x \in X$ ein *maximales Element* einer durch ihre charakteristische Funktion $f \in X \to \mathbb{B}$ gegebenen Menge ist.

$me = \lambda\, x \in X\,.\, \lambda\, f \in X \to \mathbb{B}\,.$

(e) Geben Sie ein Prädikat $ak \in (\mathbb{N} \to X) \to \mathbb{B}$ an, das testet, ob eine Folge $f \in \mathbb{N} \to X$ eine *aufsteigende Kette* gemäß $\leq$ ist.

$ak = \lambda\, f \in \mathbb{N} \to X\,.$

(f) Geben Sie ein Prädikat $sup' \in X \to (\mathbb{N} \to X) \to \mathbb{B}$ an, das testet, ob ein $x \in X$ das *Supremum* einer Folge $f \in \mathbb{N} \to X$ ist.

$sup' = \lambda\, x \in X\,.\, \lambda\, f \in \mathbb{N} \to X\,.$

Aufgabe 5: Endliche Mengen (15)

Sei eine Menge X gegeben. Sie sollen ein Prädikat $\mathit{fin} \in (X \to \mathbb{B}) \to \mathbb{B}$ angeben, das testet, ob eine durch ihre charakteristische Funktion $f \in X \to \mathbb{B}$ gegebene Menge endlich ist. Zur Beschreibung des Prädikats stehen Ihnen die Booleschen Operationen, Quantifizierung, Gleichheit und die Menge $\mathbb{N}$ der natürlichen Zahlen zur Verfügung.

$\mathit{fin} = \lambda\, f \in X \to \mathbb{B}\,.$

Aufgabe 6: Schleifen ($24 = 3 + 3 + 3 * 6$)

Hacker Erdulf will IMP um ein neues Schleifenkonstrukt

$$\mathsf{do}\ c\ \mathsf{while}\ b$$

erweitern. Nach gründlicher Überlegung kommt er zu dem Schluss, dass seine Schleife die folgende Äquivalenz erfüllen soll:

$$\mathsf{do}\ c\ \mathsf{while}\ b \quad \models\!\mid \quad c\ ;\ \mathsf{if}\ b\ \mathsf{then}\ \mathsf{do}\ c\ \mathsf{while}\ b\ \mathsf{else}\ \mathsf{skip}$$

(a) Beschreiben Sie Erdulfs Schleife mithilfe der üblichen While-Schleife:

$\mathsf{do}\ c\ \mathsf{while}\ b\ \models\!\mid$

(b) Beschreiben Sie Erdulfs Schleife mithilfe eines regulären Programms.

$\mathsf{do}\ c\ \mathsf{while}\ b\ \models\!\mid$

(c) Geben Sie die denotationale Semantik für Erdulfs Schleife an.

$\mathcal{C}(\mathsf{do}\ c\ \mathsf{while}\ b)\sigma = \mathit{fix}(\Gamma(\mathcal{C}(c), \mathcal{B}(b)))\sigma$

$\Gamma(\phi, \beta) = \lambda\, \psi \in \Sigma \to \Sigma_\perp\,.\, \lambda\, \sigma \in \Sigma\,.$

(d) Geben Sie die Verifikationsregel für Erdulfs Schleife an.

(e) Geben Sie mithilfe von 2 Inferenzregeln die operationale Semantik für Erdulfs Schleife an.

Aufgabe 7: Programmverifikation ($21 = 6 + 15$)

Sei das Programm

```
C:=Y; Z:=X;
(if 0≤Y then D:=-1 else D:=1);
while C≠0 do (Z:=Z+D; C:=C+D)
```

und die Spezifikation $(\Sigma, \{Z = X - Y\})$ gegegeben. Nehmen Sie dabei an, dass Programme auch Boolesche Ausdrücke der Form $a_1 \neq a_2$ verwenden dürfen.

(a) Nennen Sie die Verifikationsbedingungen für das Programm und die Spezifikation.

(b) Geben Sie eine Invariante an, sodass die Verifikationsbedingungen erfüllt sind.

Aufgabe 8: Berechenbarkeit ($12 = 6 * 2$)

Geben Sie die folgenden Definitionen an:

(a) Eine Menge $X \subseteq \mathbb{Z}$ heißt *entscheidbar*, wenn

(b) Eine Menge $X \subseteq \mathbb{Z}$ heißt *prüfbar*, wenn

Geben Sie für jede der folgenden Mengen an, ob sie prüfbar ist. Richtige Antworten zählen 2 Punkte, falsche -2 Punkte.

(a) $\{\, \#c \mid c \in \mathit{Com} \,\wedge\, \mathcal{F}(c)(\#c) = 7 \,\}$

(b) $\{\, \#c \mid c \in \mathit{Com} \,\wedge\, \mathcal{F}(c)0 \neq 7 \,\}$

(c) $\{\, \#c \mid c \in \mathit{Com} \,\wedge\, \exists x \in \mathbb{Z}\colon \mathcal{F}(c)x \neq \bot \,\}$

(d) $\{\, \#c \mid c \in \mathit{Com} \,\wedge\, \mathcal{F}(c) \neq (\lambda x \in \mathbb{Z}\,\mathbf{.}\, 1) \,\}$

Aufgabe 9: Satz von Rice (15)

Sie sollen den Satz von Rice beweisen. Dabei sollen Sie davon Gebrauch machen, dass die folgende Menge nicht prüfbar ist:

$$S_0 \stackrel{\text{def}}{=} \{\#c \mid c \in \mathit{Com} \wedge \mathcal{F}(c)0 = \perp\}$$

Satz Sei $BF \subseteq \mathbb{Z} \to \mathbb{Z}_\perp$ die Menge der berechenbaren Funktionen und sei

$$(\lambda x\,.\,\perp) \in F \subsetneq BF.$$

Dann ist $\#F =_{\text{def}} \{\#c \mid c \in \mathit{Com} \wedge \mathcal{F}(c) \in F\}$ nicht prüfbar.