Klausur Formale Systeme

Universität Karlsruhe
Fakultät für Informatik

SS 2009

Prof. Dr. Bernhard Beckert

8. April 2009

Name: ______________________

Vorname: ______________________

Matrikel-Nr.: ______________________

Bitte kleben Sie hier Ihren Platzaufkleber auf!

Bitte geben Sie auf jedem benutzten Blatt rechts oben
Ihren Namen und Ihre Matrikel-Nummer an!

A1 (15)	A2 (10)	A3 (5)	A4 (7)	A5 (9)	A6 (8)	A7 (6)	Σ (60)

Bewertungstabelle bitte frei lassen!

Zum Bestehen der Klausur sind 20 der erreichbaren 60 Punkte hinreichend.

Bonus: ______ **Gesamtpunkte:** ☐

1 Zur Einstimmung (4 + 4 + 3 + 4 = 15 Punkte)

Kreuzen Sie in den folgenden Tabellen alles Zutreffende an.

Für jede falsche Antwort wird ein halber Punkt abgezogen!
(Dabei werden jedoch keinesfalls weniger als 0 Punkte für jede der vier Teilaufgaben vergeben.)

Hinweise:

- „PL1“ steht für „Prädikatenlogik erster Stufe (mit Gleichheit $\doteq$)“, wie sie in der Vorlesung vorgestellt wurde. Auf diese beziehen sich in Teilaufgabe a. auch die Begriffe „erfüllbar“, „allgemeingültig“ und „unerfüllbar“.
- In Teilaufgabe a. kann eine Formel mehr als eine der genannten Eigenschaften haben. In Teilaufgabe b., c. und d. *genau* eine.
- p und q sind Prädikatssymbole, f ist ein Funktionssymbol, a und b sind Konstanten, x und y sind Variablen.
- Es gelten die üblichen Klammereinsparungsregeln.

a.

	<u>keine</u> Formel der PL1	erfüllbar	allgemein-gültig	uner-füllbar
$p(a) \leftrightarrow (p(b) \leftrightarrow (p(a) \leftrightarrow p(b)))$		X	X	
$(\forall x(p(x) \leftrightarrow q(x))) \rightarrow p \doteq q$	X			
$((\exists x\, p(x)) \rightarrow (\exists x\, q(x))) \rightarrow \exists x(p(x) \rightarrow q(x))$		X	X	
$\neg\exists x\exists y(f(x) \doteq f(y))$				X

b.

	Richtig	Falsch
Zu jeder aussagenlogischen Formel der Länge n gibt es eine äquivalente (nicht nur erfüllbarkeitsäquivalente) Formel der Länge $O(n^2)$ in konjunktiver Normalform.		X
Zu jeder LTL-Formel F, die als einzigen temporallogischen Operator $\mathbf{U}_w$ (weak until) enthält, gibt es eine LTL-Formel F', die als einzigen temporallogischen Operator $\mathbf{U}$ (das „normale“ until) enthält.	X	
Nimmt man zu einem logischen Kalkül weitere Ableitungsregeln hinzu, so bleibt die Korrektheit des Kalküls davon in jedem Fall unberührt.		X
Für alle aussagenlogischen Formeln F, G gilt: $F \wedge G$ ist genau dann erfüllbar, wenn F und G beide erfüllbar sind.		X

1 Zur Einstimmung *(Fortsetzung)*

c.

	Ja	Nein
Ist eine prädikatenlogische Formel F geschlossen, dann ist jede Substitution für F kollisionsfrei.	**X**	
Es gibt einen Term t, der mit jedem Term t' unifizierbar ist.		**X**
Zu jedem Term t gibt es einen Term t', so dass t und t' unifizierbar sind.	**X**	

d. Sind folgenden LTL-Formeln allgemeingültig, d.h., gelten sie in allen ω-Strukturen?

LTL-Formel	Allgemeingültig	Nicht allgemeingültig
$(A\,\mathbf{U}\,B) \rightarrow \mathbf{X}(A\,\mathbf{U}\,B)$		**X**
$\Box A \rightarrow (A \vee B)$	**X**	
$\Diamond(A \wedge B) \rightarrow \Diamond(A\,\mathbf{U}\,B)$	**X**	
$(B\,\mathbf{U}\,\Box A) \leftrightarrow \Box(A \vee B)$		**X**

2 Formalisieren in Aussagenlogik / Markierungsalogrithmus (2,5 + 2,5 + 5 = 10 Punkte)

Eine Familie möchte eine Party feiern. Dazu lädt sie die Familien Kunze (K), Müller (M), Schulze (S) und Wolf (W) ein. Die befreundeten Familien finden sich jedoch nur unter gewissen Bedingungen auf der Feier ein. Die Bedingungen lauten:

1. Familie Müller kommt, wenn sowohl Familie Kunze als auch Familie Schulze kommen.

Aussage: $K \wedge S \rightarrow M$ Klausel(n): (1) $\{\neg K, \neg S, M\}$ bzw. $K \wedge S \rightarrow M$

2. Wenn Familie Schulze nicht zur Party kommt, dann kommt Familie Wolf ebenfalls nicht.

Aussage: $\neg S \rightarrow \neg W$ Klausel(n): (2) $\{S, \neg W\}$ bzw. $W \rightarrow S$

3. Wenn Familie Kunze absagt, dann werden Familie Schulze oder Familie Wolf (oder gar beide) absagen.

Aussage: $\neg K \rightarrow (\neg S \vee \neg W)$ Klausel(n): (3) $\{K, \neg S, \neg W\}$ bzw. $S \wedge W \rightarrow K$

4. Wenn Familie Wolf erscheint, dann auch Familie Müller

Aussage: $W \rightarrow M$

Negat: $\neg(W \rightarrow M)$ Klausel(n): (4) $\{W\}$ bzw. W und (5) $\{\neg M\}$ bzw. $M \rightarrow \mathbf{0}$

a. Formalisieren Sie die Aussagen 1–4 sowie das Negat der Aussage 4 in Aussagenlogik (tragen Sie Ihr Ergebnis in die obige Tabelle ein). Benutzen Sie dabei die Variablen K für *Kunzes kommen*, M für *Müllers kommen*, S für *Schulzes kommen* und W für *Wolfs kommen*.

b. Wandeln Sie die Aussagen 1–3 und das Negat der Aussage 4 in Klauselnormalform um (tragen Sie Ihr Ergebnis in die obige Tabelle ein); dabei können Sie die normale Schreibweise für Klauseln oder die alternative Schreibweise für Hornklauseln (Implikationen) verwenden.

c. Zeigen Sie mit Hilfe des **Markierungsalgorithmus** für Hornformeln, dass die 4. Aussage aus den Aussagen 1–3 folgt, indem Sie zeigen, dass die Menge von Klauseln unerfüllbar ist, die den Aussagen 1–3 und dem Negat der Aussage 4 entsprechen.

Dokumentieren Sie, in welcher Reihenfolge und warum Atome markiert werden.

1. Schritt Wegen Klausel 4 wird W in den Klauseln 2,3,4 markiert.

2. Schritt Wegen Klausel 2 wird S in den Klauseln 1,2,3 markiert.

3. Schritt Wegen Klausel 3 wird K in den Klauseln 1,2,3 markiert.

4. Schritt Wegen Klausel 1 wird M in den Klauseln 1,5 markiert.

5. Schritt Wegen Klausel 5 wird $\mathbf{0}$ markiert, woraus die Unerfüllbarkeit der Klauselmenge folgt.

3 Formalisieren in Prädikatenlogik (1 + 2 + 2 = 5 Punkte)

Gegeben sei eine prädikatenlogische Signatur, die

- das zweistellige Prädikatensymbol klg (für kleiner oder gleich),
- das einstellige Prädikatensymbol m

enthält.

Zudem sei eine beliebige Interpretation (D, I) über dieser Signatur gegeben.

a. Geben Sie eine Formel der Prädikatenlogik **erster Stufe** an, die genau dann in (D, I) wahr ist, wenn gilt:

Die Menge $I(m)$ ist nicht leer.

$$\exists x\, m(x)$$

b. Geben Sie eine Formel der Prädikatenlogik **erster Stufe** an, die genau dann in (D, I) wahr ist, wenn gilt:

$I(m)$ besitzt ein Minimum bezüglich $I(klg)$.

Hinweis: Ein Element ist Minimum einer Menge, wenn es selbst in der Menge enthalten ist und kleiner oder gleich jedem Element der Menge ist.

$$\exists x(m(x) \land \forall y(m(y) \rightarrow klg(x, y)))$$

c. Geben Sie eine Formel der Prädikatenlogik **zweiter Stufe** an, die genau dann in (D, I) wahr ist, wenn gilt:

Jede nicht-leere Teilmenge $M \subseteq D$ von D besitzt ein Minimum bezüglich $I(klg)$.

Hinweis: Verwenden Sie M als Variable zweiter Stufe.

$$\forall M\Big((\exists x\, M(x)) \rightarrow \big(\exists x(M(x) \land \forall y(M(y) \rightarrow klg(x, y)))\big)\Big)$$

4 Komplexität von Erfüllbarkeitsproblemen (7 Punkte)

Eine aussagenlogische Klausel ist genau dann eine Doppel-Horn-Klausel, wenn sie **höchstens zwei positive Literale** besitzt.

Um zu zeigen, dass das Erfüllbarkeitsproblem für Doppel-Horn-Klauselmengen NP-hart ist, genügt es zu beweisen, dass 3SAT polynomiell auf Doppel-Horn reduziert werden kann, das heißt:

> Zu einer beliebigen Menge M von Klauseln, diese jeweils höchsten drei Literalen enthalten (3SAT), kann mit polynomiellem Aufwand eine Menge N von Doppel-Horn-Klauseln konstruiert werden, die genau dann erfüllbar ist, wenn M erfüllbar ist.

Geben Sie eine solche Konstruktion einer Doppel-Horn-Klauselmenge N aus einer 3SAT-Klauselmengen M an (für beliebige 3SAT Mengen M).

Hinweis: Es genügt, dass Ihre Konstruktionsvorschrift die gewünschten Eigenschaften hat. Sie müssen *nicht* beweisen, dass sie sie hat.

Sei $\{P_1, \dots, P_s\}$ die Menge der in M auftretenden aussagenlogischen Variablen, und sei $\{Q_1, \dots, Q_s\}$ eine Menge von (neuen) Variablen, die nicht in M auftreten.

Die Idee der Konstruktion ist, dass $\neg Q_i$ an Stelle von $\neg P_i$ verwendet werden kann. Es soll also $Q_i \leftrightarrow \neg P_i$ gelten. Das lässt sich durch die Klauselmenge

$$L := \big\{\{Q_i, P_i\}, \{\neg Q_i, \neg P_i\} \mid i = 1 \dots, s\big\}$$

ausgedrücken. L ist offensichtlich eine Doppel-Horn-Klauselmenge.

M' entstehe dadurch aus M, indem jedes positive Literal P_i in M durch $\neg Q_i$ ersetzt wird. M' enthält damit keine positiven Literale mehr, ist also eine Doppel-Horn-Klauselmenge.

Schließlich sei

$$N := M' \cup L \ .$$

Die Menge N ist

- eine Doppel-Horn-Klauselmenge,
- erfüllbarkeitsäquivalent zu M,
- in $O(|M|)$ vielen Schritten aus M konstruierbar,

was jedoch nach der Aufgabenstellung nicht im einzelnen bewiesen werden muss.

5 Tableaukalkül (9 Punkte)

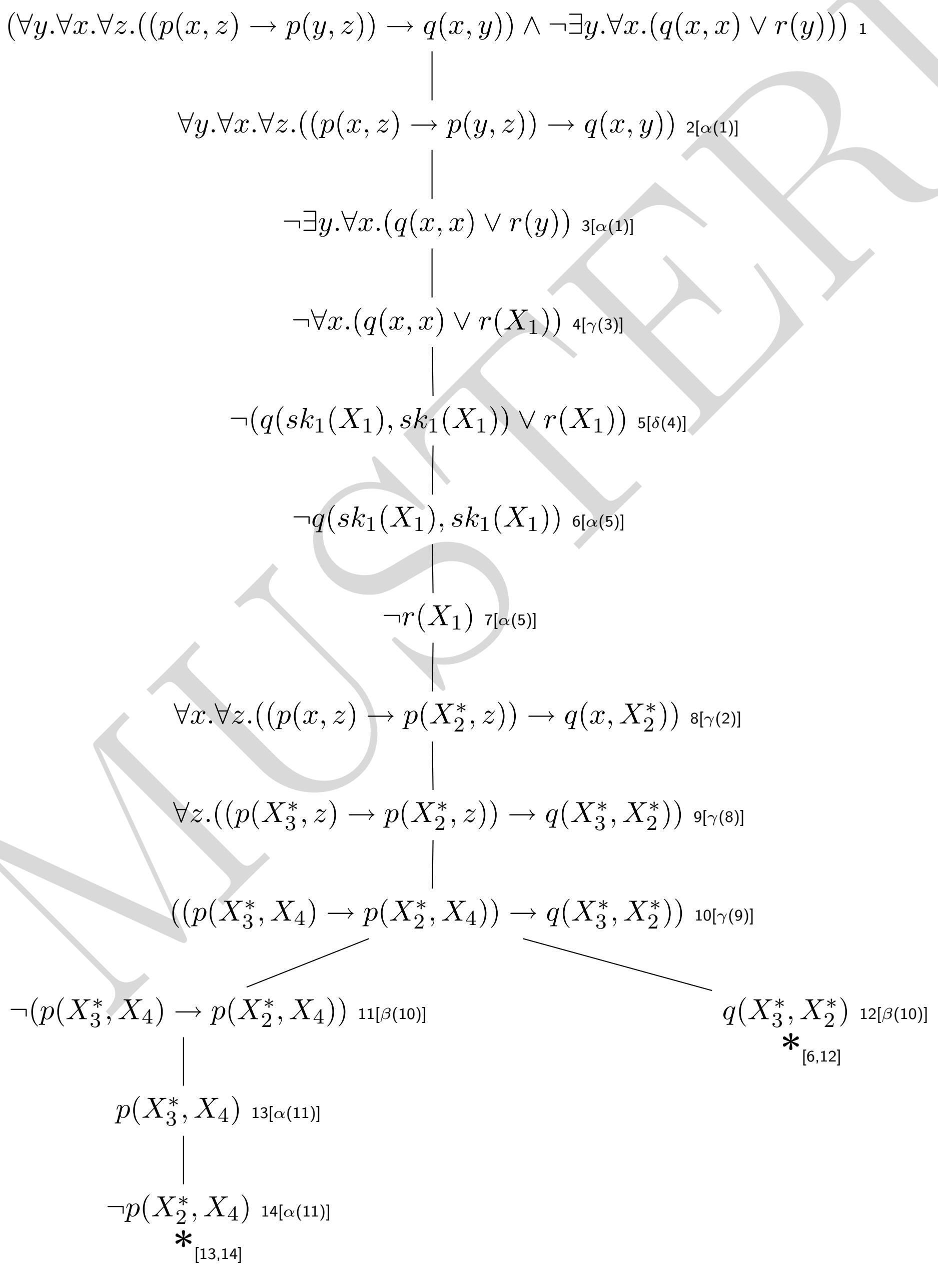
Zeigen Sie mit Hilfe des prädikatenlogischen Tableaukalküls aus der Vorlesung, dass die Formel

$$\forall y \forall x \forall z \big((p(x,z) \to p(y,z)) \to q(x,y) \big) \land \neg \exists y \forall x (q(x,x) \lor r(y))$$

unerfüllbar ist.

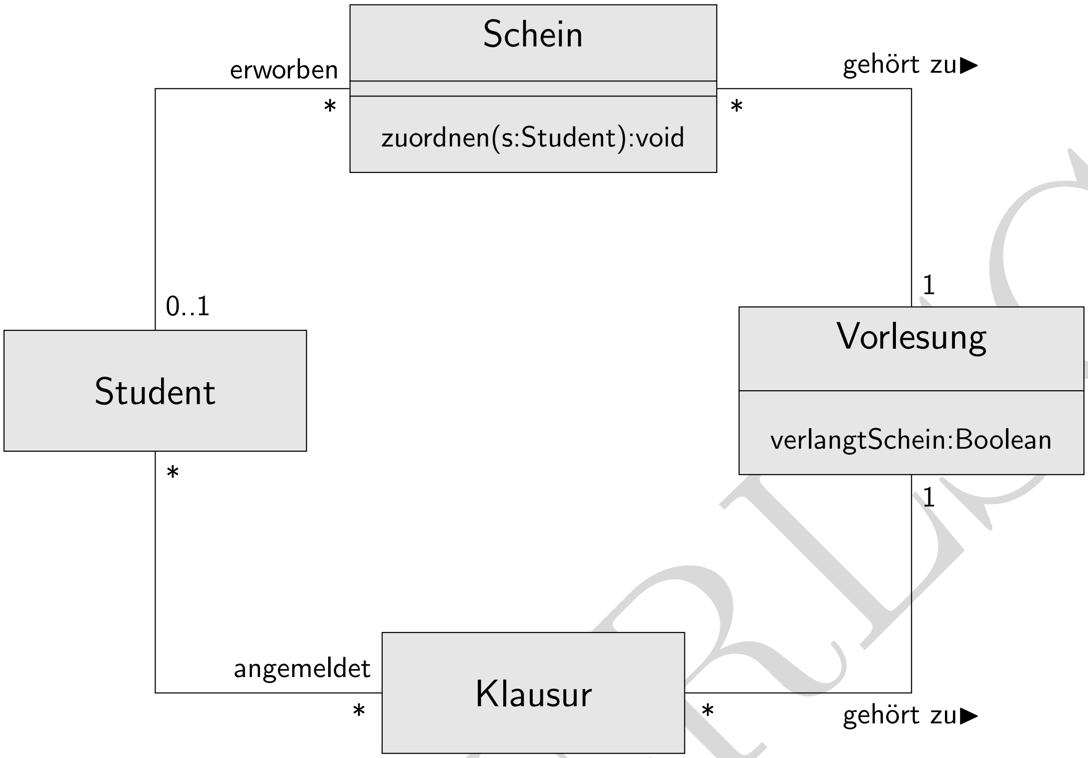
Notieren Sie dabei:

- bei jeder Erweiterung, durch welche Regelanwendung eine Formel auf dem Tableau entstanden ist,
- bei Abschlüssen die beiden Partner,
- die schließende Substitution



Unification by $\{X2 = sk1(X1), X3 = sk1(X1)\}$

UML-Diagramm zu Aufgabe 6



Übersicht über wichtige OCL-Operationen

Folgende Operationen sind auf alle Gesamtheiten (Mengen, Multimengen und Listen) anwendbar.

Operation	**Ergebnis** (bei Anwendung auf M)
`size()`	die Anzahl der Elemente in M.
`including(o)`	die Gesamtheit, die M erweitert um o entspricht.
`collect(v|exp)`	die Gesamtheit, die entsteht, wenn der Audruck *exp* für jedes Element in M ausgewertet wird.
`intersection(N)`	der Durchschnitt von M und N.
`union(N)`	die Vereinigung von M und N.
`includes(o)`	wahr genau dann, wenn o ein Element in M ist.
`includesAll(N)`	wahr genau dann, wenn jedes Element n der Gesamtheit N auch ein Element in M ist.
`isEmpty()`	wahr genau dann, wenn M kein Element enthält.
`exists(v|b)`	wahr genau dann, wenn es ein Element v in M gibt, so dass dafür der boolesche Ausdruck b zu wahr auswertet.
`forAll(v|b)`	wahr genau dann, wenn für jedes Element v in M der boolesche Ausdruck b zu wahr auswertet.
`select(v|b)`	die Gesamtheit der Elemente v von M, die b erfüllen.

6 Object Constraint Language (3 + 2 + 3 = 8 Punkte)

Auf der linken Seite ist ein UML-Klassendiagramm abgebildet. Es modelliert den Zusammenhang zwischen Vorlesungen, Studenten, Klausuren und Übungsscheinen (kurz: Schein): Jede Klausur und jeder Schein gehört zu genau einer Vorlesung. Zu einer Klausur können Studenten angemeldet sein. Ein Student hat eine Menge von Scheinen erworben, wobei jeder Schein genau einem Studenten zugeordnet ist.

a. Geben Sie eine OCL-Invariante für die Klasse Student an, die folgenden Sachverhalt formalisiert:

> Ein Student kann nur zu einer Klausur angemeldet sein, wenn die zugehörige Vorlesung keinen Schein verlangt oder er einen Schein für die Vorlesung erworben hat.

```
context Student:
inv: angemeldet->forAll(k | (not k.vorlesung.verlangtSchein) or
                            erworben.vorlesung.includes(k.vorlesung))
```

b. Geben Sie die Bedeutung der folgenden OCL-Invarianten in natürlicher Sprache wieder:

```
context Student
inv: Vorlesung.allInstances->
          forAll(v | self.erworben.select(vorlesung=v)->size() <= 1)
```

Jeder Student erwirbt pro Vorlesung höchstens einen Schein.

c. Die Klasse Schein enthält die Methode „zuordnen“. Geben Sie einen Methodenvertrag an, der besagt:

> Vorbedingung dafür, dass ein Schein einem Studenten zugeordnet wird, ist, dass der Student noch keinen Schein für dieselbe Vorlesung erworben hat.
> Nach der Zuordnung enthält die Menge der erworbenen Scheine dieses Studenten genau alle zuvor erworbenen Scheine und diesen (neuen) Schein.

```
context Schein::zuordnen(s:Student)
pre:   not s.erworben.vorlesung->includes(self.vorlesung)
post:  s.erworben = s.erworben@pre->including(self)
```

7 Modallogik (3 + 3 = 6 Punkte)

Ein Kripkerahmen (S, R) heißt *schwach funktional*, wenn es für jedes $s \in S$ **höchstens ein** $t \in S$ gibt mit $(s, t) \in R$.

a. Zeigen Sie, dass die modallogische Formel

$$\Box p \to \Diamond p$$

nicht allgemeingültige Formel in der Klasse der schwach funktionalen Rahmen ist. Geben Sie dazu eine Kripke-Struktur mit schwach funktionalem Rahmen an, in der die Formel nicht gilt. Begründen Sie, warum es sich um ein Gegenbeispiel handelt.

Die Kripke-Struktur

$$\mathcal{K} = (\{s\}, \emptyset, I)$$

mit nur einer möglichen Welt s, leerer Zugänglichkeitsrelation $R = \emptyset$ und beliebiger Interpretation I ist ein Gegenbeispiel.

Begründung:

- $\mathcal{K}$ ist schwach funktional, denn für die eine Welt s gilt, dass es kein (und damit höchstens ein) t gibt mit $(s, t) \in R$.
- da von s keine Welt erreichbar ist, gilt trivialer Weise

  $$val_s(\Diamond p) = F \quad \text{und} \quad val_s(\Box p) = W$$

  und also

  $$val_s(\Box p \to \Diamond p) = F$$

b. Zeigen Sie, dass die modallogische Formel

$$\Diamond p \to \Box p$$

in der Klasse der schwach funktionalen Rahmen allgemeingültig ist.

Vervollständigen Sie dazu folgenden Beweis:

Sei $\mathcal{K} = (S, R, I)$ eine beliebige schwach funktionale Kripkestruktur. Sei $s \in S$ beliebig.
1. Fall: Es gelte $val_s(\Diamond p) = F$. Dann gilt trivialer Weise auch $val_s(\Diamond p \to \Box p)$.
2. Fall: Es gelte $val_s(\Diamond p) = W$. Dann ...

... gibt es nach der Definition der Semantik von $\Diamond$ eine Welt $t \in S$ mit $(s, t) \in R$ und $val_t(p) = W$.

Da $\mathcal{K}$ schwach funktional ist, gibt es höchstens eine und also keine andere von t verschiedene Welt $t' \in S$ mit $(s, t') \in R$.

Also gilt für alle Welten $t \in S$ mit $(s, t) \in R$, dass $val_t(p) = W$.

Nach der Definition der Semantik von $\Box$ folgt, dass $val_s(\Box p) = W$ und damit $val_s(\Diamond p \to \Box p) = W$.