Karlsruher Institut für Technologie

Klausur Formale Systeme

Fakultät für Informatik

SS 2015

Prof. Dr. Bernhard Beckert

31. Juli 2015

Name: ______________________

Vorname: ______________________

Matrikel-Nr.: ______________________

Die Bearbeitungszeit beträgt 60 Minuten.

A1 (10)	A2 (8)	A3 (6)	A4 (7)	A5 (9)	A6 (11)	A7 (9)	Σ (60)

Bewertungstabelle bitte frei lassen!

Gesamtpunkte: ☐

1 Zur Einstimmung (5+5 = 10 Punkte)

a. Kreuzen Sie in der folgenden Tabelle alles Zutreffende an.

Für jede korrekte Antwort gibt es einen Punkt, **für jede falsche Antwort wird ein *halber Punkt* abgezogen!** (Dabei werden jedoch keinesfalls weniger als 0 Punkte für jede der zwei 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“.
- P_1, P_2, und p sind Prädikatensymbole, f ist ein Funktionssymbol, c ist ein Konstantensymbol, und x, y sind Variablen.
- Es gelten die üblichen Klammereinsparungsregeln.

	keine Formel der PL1	allgemeingültig	erfüllbar, aber nicht allgemeingültig	unerfüllbar
$\big(\forall x(p(f(x)) \to \neg p(f(x)))\big) \land p(c)$			X	
$\big(\forall x(p(f(x)) \to \neg p(f(x)))\big) \land p(f(c))$				X
$(P_1 \to P_2) \land (P_2 \to \neg P_1)$			X	
$\exists f \, \forall x \, (f(x) \doteq x)$	X			
$\big(\forall x \, f(x) \doteq x\big) \to \big(\forall x \forall y \, (f(x) \doteq f(y) \to x \doteq y)\big)$		X		

b. Bitte kreuzen Sie in der folgenden Tabelle das Zutreffende an. Für korrekte Antworten erhalten Sie einen Punkt, **für falsche Antworten wird *ein Punkt* abgezogen**. Dabei werden jedoch nie weniger als 0 Punkte für diese Teilaufgabe vergeben.

	Richtig	Falsch
Jede erfüllbare Formel der Prädikatenlogik mit Gleichheit hat auch ein Modell mit einer unendlichen Domäne.		X
Sei Σ eine endliche aussagenlogische Signatur. Wenn für zwei aussagenlogische Formeln F und G über Σ die Formel $F \to G$ allgemeingültig ist, so hat G mindestens so viele erfüllende Belegungen wie F.	X	
Die beiden prädikatenlogischen Terme $h(f(x), g(y))$ und $h(f(y), g(f(x)))$ sind unifizierbar.		X
Wenn in einer Kripkestruktur $\mathcal{K} = (S, R, I)$ die Formel A in allen Zuständen $s \in S$ wahr ist, dann ist auch $\Box A$ in allen Zuständen wahr.	X	
Wenn eine aussagenlogische Formel allgemeingültig ist, dann hat der reduzierte Shannongraph zu dieser Formel genau einen Knoten.	X	

Zur Begründung:

a.

- **i.** Der linke Faktor der Konjunktion ist äquivalent zu $\forall x \; \neg p(f(x))$.
  Die Formel ist erfüllt für: $D = \{0, 1\}, I(c) = 0, I(f) = x \mapsto 1, I(p) = \{0\}$.
  Die Formel ist nicht erfüllt für: $D = \{0, 1\}, I(c) = 0, I(f) = x \mapsto 1, I(p) = \{1\}$.
- **ii.** Der linke Faktor der Konjunktion ist äquivalent zu $\forall x \; \neg p(f(x))$. Sei dieser erfüllbar mit Modell D, I, also $I \models \forall x \; \neg p(f(x))$. Dann ist auch die Instanz mit c für x erfüllt: $I \models \neg p(f(c))$. Das ist im Widerspruch zum zweiten Faktor der Konjunktion – ein solches Modell kann also nicht existieren.
- **iii.** Ist erfüllt für $I = \emptyset$ und nicht erfüllt für $I = \{P_1, P_2\}$.
- **iv.** Dies ist eine Formel der Prädikatenlogik zweiter Stufe, der der Quantor $\exists f$ rangiert über eine Variable, die für eine Funktion steht. (Als Formel der PL2 ist diese übrigens allgemeingültig, weil die Identität id_D auf dem Universum genau diese Eigenschaft hat.)
- **v.** Die Aussage dieser Formel lautet: Die identische Funktion f ist injektiv; und das ist allgemeingültig. Die Prämisse $\big(\forall x \, f(x) \doteq x\big)$ besagt, dass f die identische Funktion ist und die Konklusion $\big(\forall x \, \forall y \, (f(x) \doteq f(y) \to x \doteq y)\big)$ formalisiert, dass f injektiv ist.

b.

- **i.** Die Formel $\exists x \forall y \; x \doteq y$ hat nur Modelle mit genau einem Element im Universum.
- **ii.** Beh: Jedes Modell I von F ist Modell von G. Wegen $I \models F$ und $I \models F \to G$ ist (nach Modus Ponens) auch $I \models G$.
- **iii.** Die Anwendung von Robinson's Unifizierungsalgorithmus liefert nach einem Schritt, dass x und y unifiziert werden müssen: $h(f(x), g(x))$ bzw. $h(f(x), g(f(x)))$. Der nächste Schritt würde die Unifikation von x und $f(x)$ erfordern. Das geht nicht (*occur check*).
- **iv.** Sei $\mathcal{K}$ eine Kripkestruktur, in der A in jedem Zustand gilt, aber $\Box A$ in einem Zustand s nicht gilt. Dann gilt also $s \models \neg \Box A$, und äquivalent $s \models \Diamond \neg A$. Es muss also einen Zustand s' mit sRs' geben, so dass $s' \not\models A$. Widerspruch.
- **v.** Der reduzierte Shannon-Graph einer allgemeingültigen Formel besteht genau aus dem Knoten mit der Markierung $\boxed{1}$.

2 Beweis für eine Eigenschaft aussagenlogischer Klauseln (8 Punkte)

Beweisen Sie den folgenden Satz:

> **Satz.** Eine Menge M aussagenlogischer Klauseln über der Signatur Σ ist *genau dann* allgemeingültig, wenn für jede Klausel $K \in M$ gilt:
>
> $$\text{es gibt eine aussagenlogische Variable } P_K \in \Sigma \text{ mit: } \quad P_K \in K \text{ und } \neg P_K \in K \qquad (*)$$

Der Beweis hat zwei Teile:

a. Annahme: Jede Klausel K in M habe die Eigenschaft $(*)$.

Zu zeigen: M ist allgemeingültig, also unter jeder Belegung V wahr.

Sei V eine beliebige Belegung.
Sei $K \in M$ beliebig.
Es gilt $V(P_K) = W$ oder $V(\neg P_K) = W$. Da die Literale in Klauseln diskunktiv verknüpft sind und $P_K, \neg P_K \in K$, folgt $V(K) = W$.
Da K beliebig gewählt war, gilt $V(K) = W$ für alle $K \in M$. Also gilt $V(M) = W$.
Da V beliebig gewählt war, gilt $V(M) = W$ für alle Belegungen V. Also ist M allgemeingültig.

b. Annahme: M sei allgemeingültig.

Zu zeigen: Jede Klausel $K \in M$ habe die Eigenschaft $(*)$.

Angenommen, es gebe eine Klausel $K \in M$, die die Eigenschaft *nicht* hat.
Definiere die Belegung V_K wie folgt:

$$V(P) = \begin{cases} W & \text{falls } \neg P \in K \\ F & \text{sonst} \end{cases}$$

Da K die Eigenschaft $(*)$ laut Annahme nicht hat, gilt nun für alle $P \in \Sigma$:

- Falls $P \in K$, dann $\neg P \notin K$, also $V(P) = F$.
- Falls $\neg P \in K$, dann $V(P) = W$, also $V(\neg P) = F$.

Also belegt V alle Literale in K mit F, und damit gilt $V(K) = F$. Daraus folgt $V(M) = F$.
Das steht im Widerspruch zur Allgemeingültigkeit von M.
Also ist die Annahme falsch, und alle Klauseln $K \in M$ haben die Eigenschaft $(*)$.

3 Aussagenlogik, kurze KNF (1+5 = 6 Punkte)

Gegeben sei eine aussagenlogische Signatur Σ mit $2n$ Variablen $A_1, \ldots, A_n, B_1, \ldots, B_n$.

Die schematische aussagenlogische Formel

$$\phi = \neg(A_1 \leftrightarrow B_1) \lor \ldots \lor \neg(A_n \leftrightarrow B_n)$$

über Σ hat die folgende Eigenschaft: ϕ ist genau dann in einer Variablenbelegung wahr, wenn es (mindestens) einen Index $1 \leqslant i \leqslant n$ gibt, so dass A_i und B_i unterschiedlich belegt sind.

a. Geben Sie eine schematische aussagenlogische Formel χ über Σ an, die äquivalent zu ϕ ist und nur Konjunktion $\land$, Disjunktion $\lor$ und Negation $\neg$ als logische Operationen enthält.

$\chi = (A_1 \land \neg B_1) \lor (\neg A_1 \land B_1) \lor \ldots \lor (A_n \land \neg B_n) \lor (\neg A_n \land B_n)$

b. Geben Sie eine aussagenlogische Formel ψ über einer geeigneten Signatur an, die in konjunktiver Normalform und erfüllbarkeitsäquivalent zu ϕ und χ ist. Machen Sie dabei Ihre Vorgehensweise deutlich.

Hinweis: Nutzen Sie zur Konstruktion die in der Vorlesung vorgestellte Idee der kurzen KNF.

Idee: Führe eine Abkürzung für jedes der Disjunkte in χ. Die Disjunktion dieser Abkürzungen stellt den Grundstein für ψ dar. Er muß nur noch mit den in KNF umgeformten Definitionen für die Abkürzungen konjunktiv verknüpft werden.
Sei $\Sigma' = \Sigma \cup \{T_1, \ldots, T_n, T'_1, \ldots, T'_n\}$.
$\psi = (T_1 \lor \ldots \lor T_n \lor T'_1 \lor \ldots \lor T'_n) \land (\neg A_i \lor B_i \lor T_i) \land (A_i \lor \neg T_i) \land (\neg B_i \lor \neg T_i) \land (A_i \lor \neg B_i \lor T'_i) \land (\neg A_i \lor \neg T'_i) \land (B_i \lor \neg T'_i)$ für $1 \leqslant i \leqslant n$.

Alternativ ist es auch möglich, Abkürzungen für komplette Nicht-Äquivalenzen einzuführen:

Sei $\Sigma' = \Sigma \cup \{T_1, \ldots, T_n\}$.
$\psi = (T_1 \lor \ldots \lor T_n) \land (\neg A_i \lor \neg B_i \lor \neg T_i) \land (\neg A_i \lor B_i \lor T_i) \land (A_i \lor \neg B_i \lor T_i) \land (A_i \lor B_i \lor \neg T_i)$ für $1 \leqslant i \leqslant n$.

Alternativ ist es auch möglich, das normale KKNF-Verfahren anzuwenden.

4 Formalisieren in PL1 (1+2+1+3 = 7 Punkte)

Formalisieren Sie die vier folgenden Aussagen mittels Prädikatenlogik erster Stufe mit Gleichheit. Benutzen Sie dafür jeweils die angegebenen interpretierten Symbole.

a. Kein Mensch ist eine Insel.
Prädikate: $mensch(\cdot), insel(\cdot)$.

$\boxed{\forall x.\, mensch(x) \to \neg insel(x)}$

b. Es gibt nur ein Rudi Völler.
Prädikat: $rudivöller(\cdot)$.

$\exists x.\,(rudiv\ddot{o}ller(x) \land \forall y.\,(rudiv\ddot{o}ller(y) \to x \doteq y))$ oder $\forall x.\forall y.\,((rudiv\ddot{o}ller(x) \land rudiv\ddot{o}ller(y)) \to x \doteq y)$

c. Nur die Liebe zählt.
Prädikate: $liebe(\cdot), z\ddot{a}hlt(\cdot)$.

$\forall x.\, z\ddot{a}hlt(x) \to liebe(x)$ oder auch $\forall x.\, z\ddot{a}hlt(x) \leftrightarrow liebe(x)$

d. Wenn zwei sich streiten, freut sich der dritte.
Prädikate: $streiten(\cdot,\cdot), freuen(\cdot)$.

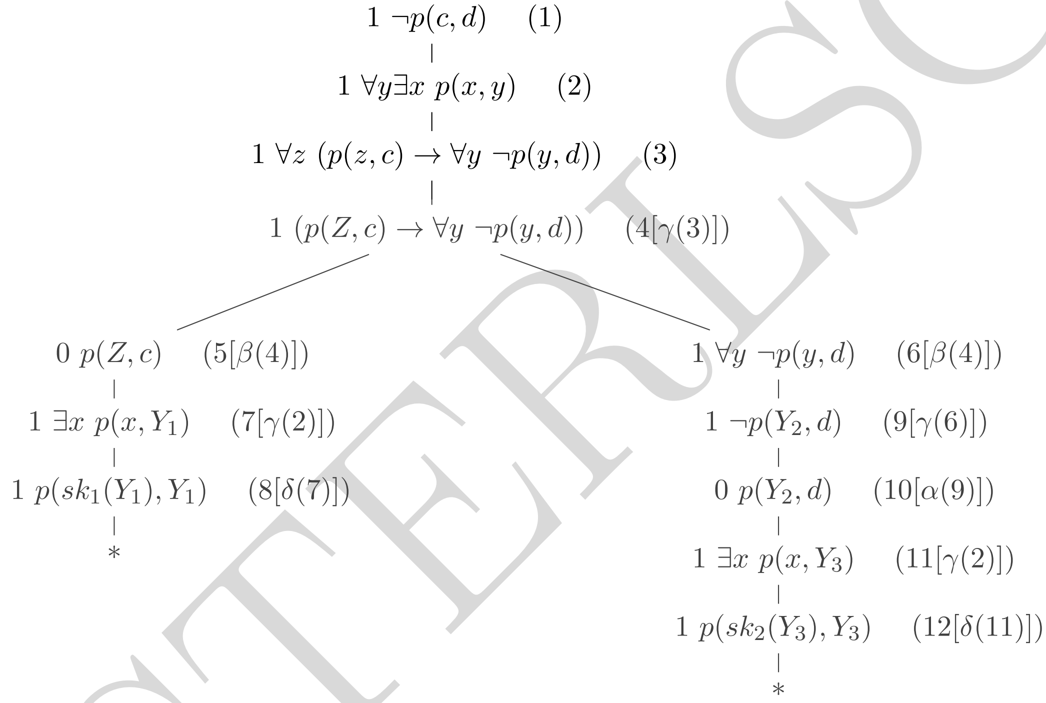
$\boxed{\forall x \forall y \forall z.\ \neg x \doteq y \land \neg x \doteq z \land \neg y \doteq z \to streiten(x,y) \to freuen(z)}$

5 Tableau (5+4 = 9 Punkte)

Die folgenden beiden Teilaufgaben erfordern die Erstellung eines Tableaus. Notieren Sie in jedem Tableau:

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

a. Vervollständigen Sie den folgenden Tableau-Beweis:



Schließende Substitution: $\sigma = \{Z/sk_1(c),\ Y_1/c,\ Y_2/sk_2(d),\ Y_3/d\}$

Fortsetzung: Tableau

b. Zeigen Sie, dass folgende Formel F **allgemeingültig** ist. Ergänzen Sie zunächst vor der Wurzel in folgendem Tableaubeweis das dazu benötigte Vorzeichen. Schließen Sie dann das Tableau.

Hinweis: Vergeben Sie Abkürzungen für Teilformeln von F (durch geeignetes Markieren der Teilformeln und Benennung im dafür vorgesehenen Kasten), die Sie dann im Beweis verwenden können.

Vorzeichen $\boxed{0}$ $\overbrace{\Big((\forall x\ q(x)) \to \big(\exists z \forall y\ q(y) \lor p(z,z)\big)\Big) \lor \neg\big(\exists z \forall y\ q(y) \lor p(z,z)\big)}^{F}$ (1)

Abk. für Teilformeln

$0\ \Big(\forall x\ q(x) \to \big(\exists z \forall y\ q(x) \lor p(z,z)\big)\Big)$ (2)

$0\ \neg\big(\exists z \forall y\ q(x) \lor p(z,z)\big)$ (3)

$0\ \forall x\ q(x)$ (4)

$0\ \exists z \forall y\ q(x) \lor p(z,z)$ (5)

$1\ \exists z \forall y\ q(x) \lor p(z,z)$ (6)

$*$

6 Spezifikation mit der Java Modeling Language

(4+4+3 = 11 Punkte)

Hinweis: Zur Erinnerung ist hier die Syntax einiger JML-Konstrukte wiederholt:

Allquantor	(`\forall` T x ; *Bedingung* ; *Bedingung*)
Existenzquantor	(`\exists` T x ; *Bedingung* ; *Bedingung*)
Summe	(`\sum` T x ; *Bedingung* ; *Ausdruck*)
Minimum	(`\min` T x ; *Bedingung* ; *Ausdruck*)

In dieser Aufgabe werden zweidimensionale Felder (Typ `int[][]`) verwendet. Wir nehmen an, dass der erste Index die Zeile und der zweite die Spalte in diesem Feld angibt. `coll[i][j]` ist damit der Wert in der i-ten Zeile und j-ten Spalte.

Gegeben sei die Klasse `C`, die folgendermaßen definiert ist.

```
class C {
    int[][] coll;

    /*@ public normal_behaviour
      @   ensures \result <==>
      @     (\exists int i; 0<=i && i<coll.length;
      @      (\forall int j; 0<=j && j<a.length;
      @       (\exists int k; 0<=k && k<coll[i].length;
      @        a[j] == coll[i][k])));
      @   assignable \nothing;
      @*/
    boolean m(int[] a) { ... }
}
```

Aufgaben:

a. Geben Sie in natürlicher Sprache wieder, was der Methodenvertrag für die Methode `m` besagt.

Die Methode terminiert ohne Ausnahme, und es werden keine Speicherstellen von existierenden Objekten verändert. Die Methode liefert genau dann `true` zurück, wenn es eine Zeile in `coll` gibt, so dass jedes Element aus a in dieser Spalte auftritt.

Fortsetzung: Spezifikation mit der Java Modeling Language

b. Geben Sie eine Klasseninvariante für die Klasse `C` an, die folgendes formalisiert:

> Jede Zeile in `coll` hat dieselbe Anzahl von Spalten.

```
/*@ invariant
  @
  @
  @
  @
  @*/
```

```
(\forall int i,j; 0<=i && i<j && j<coll.length; coll[i].length == coll[j].length);
oder (\forall int i; 0<=i && i<coll.length; coll[i].length == coll[0].length);
oder (\exists int k; (\forall int i; 0<=i && i<coll.length; coll[i].length == k));
```

c. Die Klasse `C` soll nun um eine neue Methode `sums` erweitert werden. Ergänzen Sie dazu den unten stehenden Methodenvertrag um eine Nachbedingung, die besagt:

> Die Methode liefert eine Referenz auf ein Feld zurück, dessen Länge gleich der Zahl der Zeilen von `coll` ist.
>
> Jeder Wert in diesem Feld ist gleich der Summe der Einträge der entsprechenden Zeile in `coll`.

```
/*@ public normal_behaviour
  @   requires true;
  @   ensures
  @
  @
  @
  @
  @
  @
  @
  @
  @
  @   assignable \nothing;
  @*/
int[] sums() { ... }
```

```
   \result.length == coll.length;
&& (\forall int i; 0<=i && i<\result.length;
      \result[i] == (\sum int k; 0<=k && k<coll[i].length; coll[i][k]))
```

7 Büchi-Automaten und LTL (2+3+3+1 = 9 Punkte)

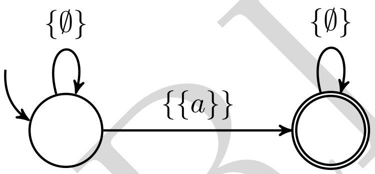
Gegeben sei die aussagenlogische Signatur $\Sigma = \{a\}$.

a. Vervollständigen Sie den vorgegebenen Büchi-Automaten $\mathcal{A}$ über dem Alphabet $V = \{\emptyset, \{a\}\}$ so, dass er die wie folgt beschriebene Sprache L akzeptiert:

$$L = \{w \in V^\omega \mid \text{es gibt genau ein } n \in \mathbb{N}, \text{ so dass } a \in w(n)\}$$

Hinweis: Es existiert eine Lösung, die mit den vorgegebenen zwei Zuständen auskommt – Lösungen mit weiteren Zuständen sind auch erlaubt.
Denken Sie daran, den Anfangszustand sowie die finalen Zustände des Automaten zu kennzeichnen.

$\mathcal{A}$:



b. Geben Sie zu der in Teilaufgabe **a.** gegebenen Sprache L eine äquivalente Formel φ in linearer temporaler Logik (LTL) unter Verwendung der atomaren Aussage a an (d.h., es muss gelten: $L = \{\xi \in V^\omega : \xi \models \varphi\}$).

Lösung: $\varphi = \boxed{\neg a \,\mathbf{U}\, (a \wedge \mathbf{X}\Box\neg a)}$

c. Nennen Sie die notwendigen Schritte, um die **Erfüllbarkeit** einer LTL-Formel F mit Hilfe von Büchi-Automaten zu überprüfen.

1. Man konstruiert den Büchi-Automaten $\mathcal{A}_F$ mit $L^\omega(\mathcal{A}_F) = \{\xi \in V^\omega \mid \xi \models F\}$

2. Es gilt: F ist genau dann erfüllbar, wenn $\boxed{L^\omega(\mathcal{A}_F) \neq \emptyset}$

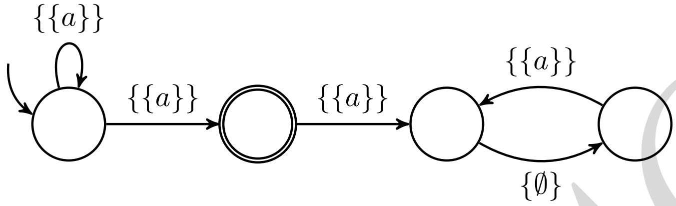
3. Dies überprüft man, indem man einen erreichbaren Endzustand sucht, der auf einer Schleife liegt.

Existiert ein solcher Zustand, so gilt $L^\omega(\mathcal{A}_F) \neq \emptyset$.

Fortsetzung: Büchi-Automaten und LTL

d. Geben Sie zu folgendem Büchi-Automaten $\mathcal{B}$ eine LTL-Formel ψ an, so dass $L^\omega(\mathcal{B}) = \{\xi \in V^\omega : \xi \models \psi\}$ gilt.

$\mathcal{B}$:



Lösung: $\psi =$ **0** ______________________