Klausur Formale Systeme

Fakultät für Informatik

WS 2011/2012

Prof. Dr. Peter H. Schmitt

12. April 2012

Name: ______________________

Vorname: ______________________

Matrikel-Nr.: ______________________

Nummer dieser Klausur:

Bitte notieren Sie sich diese Nummer! Unter dieser Nummer wird das Ergebnis Ihrer Klausur veröffentlicht.

Die Bearbeitungszeit beträgt 60 Minuten.

A1 (12)	A2 (4)	A3 (8)	A4 (9)	A5 (9)	A6 (9)	A7 (9)	Σ (60)

Bewertungstabelle bitte frei lassen!

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

Bonus: ______ **Gesamtpunkte:**

1 Zur Einstimmung (5+3+4 Punkte)

a. Bitte kreuzen Sie in der folgenden Tabelle die für die prädikatenlogischen Formeln zutreffende Eigenschaft an. Für korrekte Antworten erhalten Sie einen Punkt, **für falsche Antworten wird *ein halber* Punkt abgezogen**. Dabei werden jedoch nie weniger als 0 Punkte für die Tabelle vergeben. r ist ein einstelliges Prädikatensymbol, p, q sind zweistellige Prädikatensymbole, f ist ein einstelliges Funktionssymbol, c ist ein Konstantensymbol, die übrigen Bezeichner sind Variablen.

	keine Formel der PL1	erfüllbar (aber nicht allgemeing.)	allgemeingültig (und erfüllbar)	unerfüllbar
$\big(\forall x \exists y\ p(x,y)\big) \to \big(\forall x\ p(x, f(x))\big)$		**X**		
$\forall x \forall y\ \big(\neg x \doteq y \vee q(x,y)\big) \wedge \forall z\ \neg q(z,z)$				**X**
$\mathbf{1} \to \mathbf{0}$				**X**
$\big(\forall x\ r(r(x))\big) \to r(r(r(c)))$	**X**			
$\big(\exists x \forall y\ p(x,y)\big) \to \big(\exists x\ p(x, f(x))\big)$			**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
Zu jedem nichtdeterministischen Büchi-Automat $\mathcal{A}$ gibt es einen deterministischen Büchi-Automaten $\mathcal{B}$, so dass $L^\omega(\mathcal{A}) = L^\omega(\mathcal{B})$ gilt.		**X**
Es gibt eine Formel φ über der Signatur $\{0, 1, +, *, \}$, so dass weder $PA \models \varphi$ noch $PA \models \neg\varphi$ gilt. (PA ist das Axiomensystem der Peano-Arithmetik.)	**X**	
Die LTL-Formel $\big((A \wedge B)\ \mathbf{U}\ C\big) \leftrightarrow \big((A\ \mathbf{U}\ C) \wedge (B\ \mathbf{U}\ C)\big)$ ist allgemeingültig.	**X**	

c. Bitte ergänzen Sie in den folgenden Aussagen das fehlende Wort so, dass die enstehenden Aussagen korrekt sind. Für jede korrekte Antwort erhalten Sie einen Punkt (und **für falsche Antworten *keinen* Abzug**) in dieser Teilaufgabe.

i. Eine Klausel, die weniger als zwei positive Literale enthält, wird [Horn] -Klausel genannt.

ii. Eine Kripke-Struktur $\mathcal{K} = (S, R, I)$ besteht aus dem [Kripke-Rahmen] $\mathcal{R} = (S, R)$ und der Interpretation I.

iii. Die Formel $\forall x \exists y \forall z \big(r(x,y) \to \neg(r(z,y) \wedge r(y,z))\big)$ ist in [Pränexnormal] -Form.

iv. Die AL-Formel A ist eine [(Craig-)Interpolante] für die Formeln $A \wedge B$ und $A \vee C$.

2 DPLL (4 Punkte)

Gegeben sei

$$M := \big\{\{A, B, \neg C, \neg D\}, \{C, \neg D\}, \{A, D\}, \{B, \neg C, D\}, \{\neg A, D\}, \{\neg B, \neg D\}, \{\neg A, B\}\big\}$$

Zeigen Sie mit Hilfe des Davis-Putnam-Loveland-Algorithmus, dass die Menge M von aussagenlogischen Klauseln unerfüllbar ist.

Fallunterscheidung nach B.

1. $B = 0$

	$\{A, B, \neg C, \neg D\}$,	$\{C, \neg D\}$,	$\{A, D\}$,	$\{B, \neg C, D\}$,	$\{\neg A, D\}$,	$\{\neg B, \neg D\}$,	$\{\neg A, B\}$
$B = 0$	$\{A, \neg C, \neg D\}$,	$\{C, \neg D\}$,	$\{A, D\}$,	$\{\neg C, D\}$,	$\{\neg A, D\}$,	$-$,	$\{\neg A\}$
$\Rightarrow A = 0$	$\{\neg C, \neg D\}$,	$\{C, \neg D\}$,	$\{D\}$,	$\{\neg C, D\}$,	$-$,	$-$,	$-$
$\Rightarrow D = 1$	$\{\neg C\}$,	$\{C\}$,	$-$,	$-$,	$-$,	$-$,	$-$
$\Rightarrow C = 0$	$-$,	$\square$,	$-$,	$-$,	$-$,	$-$,	$-$

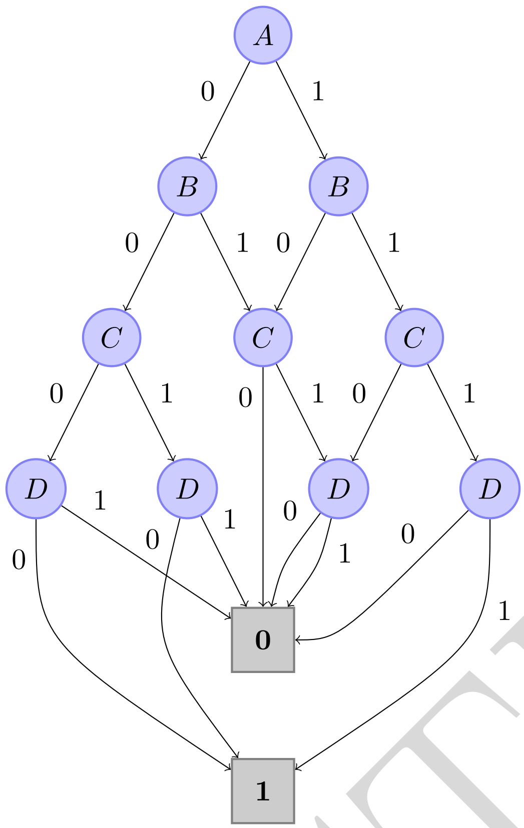
2. $B = 1$

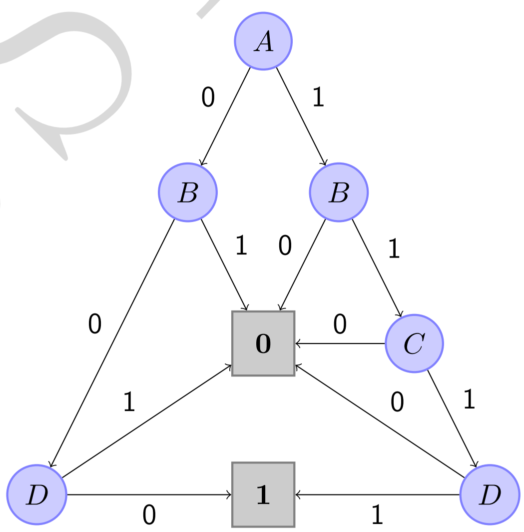
	$\{A, B, \neg C, \neg D\}$,	$\{C, \neg D\}$,	$\{A, D\}$,	$\{B, \neg C, D\}$,	$\{\neg A, D\}$,	$\{\neg B, \neg D\}$,	$\{\neg A, B\}$
$B = 1$	$-$,	$\{C, \neg D\}$,	$\{A, D\}$,	$-$,	$\{\neg A, D\}$,	$\{\neg D\}$,	$-$
$\Rightarrow D = 0$	$-$,	$-$,	$\{A\}$,	$-$,	$\{\neg A\}$,	$-$,	$-$
$\Rightarrow A = 1$	$-$,	$-$,	$-$,	$-$,	$\square$,	$-$,	$-$

Nur eine Fallunterscheidung (ein „choose“) ist notwendig, ab dann benötigt der Algorithmus wegen der Unit-Elimination keine Entscheidungen mehr.

3 Shannon-Graphen (6+2 Punkte)

a. Konstruieren Sie zu dem folgenden Shannnon-Graphen den reduzierten Shannon-Graphen zu der Variablen-Ordnung $A < B < C < D$.





b. Lesen Sie eine disjunktive Normalform (DNF) aus dem in Aufgabenteil a. gegebenen Shannon-Graphen ab und geben Sie diese an.

$(A \wedge B \wedge C \wedge D) \vee (\neg A \wedge \neg B \wedge C \wedge \neg D) \vee (\neg A \wedge \neg B \wedge \neg C \wedge \neg D)$

4 Formalisieren in Prädikatenlogik (1+2+4+2 Punkte)

Diese Aufgabe thematisiert das Lügner-Paradoxon

Epimenides der Kreter sagte: Alle Kreter sind Lügner.

Gegeben sei die prädikatenlogische Signatur, welche genau

die nullstelligen Funktionssymbole (für Epimenides und Thales):	e, t
das einstellige Funktionssymbol:	$\mathit{besterFreund}(\cdot)$
und die einstelligen Prädikatensymbole:	$\mathit{Kreter}(\cdot)$, $\mathit{Lügner}(\cdot)$

enthält. Formalisieren Sie die angegebenen Eigenschaften in Prädikatenlogik erster Stufe mit Gleichheit. Benutzen Sie dabei jeweils nur die angegebenen Prädikaten- und Funktionssymbole.

a. Epimenides und Thales sind Kreter.
benötigte Prädikate und Funktionen: t, e, $\mathit{Kreter}(\cdot)$

(a) $\boxed{kreter(t) \land kreter(e)}$

b. Genau dann, wenn Epimenides kein Lügner ist, gilt: Alle Kreter sind Lügner.
benötigte Prädikate und Funktionen: e, $\mathit{Kreter}(\cdot)$, $\mathit{Lügner}(\cdot)$

(b) $\boxed{\neg \mathit{Lügner}(e) \leftrightarrow \forall x(\mathit{Kreter}(x) \to \mathit{Lügner}(x))}$

c. Ergänzen Sie folgende Interpretation (D, I), so dass sie ein Modell der obigen Formeln (a) und (b) ist:

D	= { Epimenides, Thales }		
I(e)	= $\boxed{\text{Epimenides}}$	; I(t) =	$\boxed{\text{Thales}}$
I(Kreter)	= { $\boxed{\text{Epimenides, Thales}}$ }		
I($\mathit{Lügner}$)	= { $\boxed{\text{Epimenides}}$ }		

d. Der beste Freund eines jeden Kreter ist Epimenides.
benötigte Prädikate und Funktionen: e, $\mathit{besterFreund}(\cdot)$, $\mathit{Kreter}(\cdot)$

(d) $\boxed{\forall x(Kreter(x) \to besterFreund(x) \doteq e)}$

5 Resolutionskalkül (9 Punkte)

Gegegeben sei die (unten stehende) Menge R von prädikatenlogischen Klauseln. Darin sind $p(\cdot,\cdot), r(\cdot)$ Prädikatensymbole, $f(\cdot), c, d$ Funktionssymbole und x eine Variable.

Zeigen Sie mithilfe des Resolutionskalküls, dass R unerfüllbar ist. Machen Sie bei jedem Resolutionsschritt erkenntlich, aus **welchen Ausgangsklauseln** die Resolvente entsteht und **welche Substitution** Sie dazu verwendet haben.

$$R = \{ \underset{(1)}{\{p(d,x), r(x)\}}, \underset{(2)}{\{\neg p(x,c), \neg p(x,d)\}}, \underset{(3)}{\{\neg r(f(x))\}}, \underset{(4)}{\{p(x,d), \neg p(x,c)\}}, \underset{(5)}{\{\neg r(x), r(f(x))\}} \}$$

(6)	$\{\neg p(x,c)\}$	(2), (4)	$\sigma = \{\}$
(7)	$\{p(d,x), r(f(x))\}$	(1), (5)	$\sigma = \{\}$
(5′)	$\{\neg r(z), r(f(z))\}$		Variante von (5)
(8)	$\{p(d,x), r(f(f(x)))\}$	(7), (5′)	$\sigma = \{z/f(x)\}$
(9)	$\{p(d,x)\}$	(3), (8)	$\sigma = \{\}$
(9′)	$\{p(d,x')\}$		Variante von (9)
(10)	$\square$	(6), (9′)	$\sigma = \{x/d, x'/c\}$

Der letzte Schritt wäre nicht möglich gewesen, hätte man auf die Variantenbildung ((9) $\rightsquigarrow$ (9′)) verzichtet, denn $p(c,x)$ und $p(x,d)$ sind nicht unifizierbar.

6 Java Modeling Language (JML) (3+4+2 Punkte)

Gegeben seien die folgenden drei Java-Klassendeklarationen:

```
class Bank  {
    Kunde[] kunden;
}
```

```
class Kunde {
    Konto[] konten;
    int summe() { ... }
}
```

```
class Konto {
    Bank zugehoerigeBank;
    int kontostand;
    boolean m(int x) { ... }
}
```

a. Die Methode `Konto.m(int x)` besitzt folgenden JML-Vertrag. Geben Sie die Bedeutung des Vertrages in natürlicher Sprache wieder:

```
/*@ public normal_behaviour
  @   requires x >= 0;
  @   ensures \result == (\old(kontostand) >= x);
  @   ensures \result  ==> kontostand == \old(kontostand) - x;
  @   ensures !\result ==> kontostand == \old(kontostand);
  @   assignable this.kontostand;
  @*/
```

Wird die Methode `m` mit einem nicht-negativen Parameter aufgerufen, so gilt:

- Die Methode terminiert ohne Ausnahme.
- Es wird höchstens das Feld `kontostand` dieses Objektes verändert.
- Wenn der Stand des Kontos wenigstens `x` ist, so wird der Stand um diesen Wert verringert und `true` zurückgeliefert.
- Wenn der Stand weniger als `x` ist, so bleibt der Kontostand der alte und es wird `false` zurückgeliefert.

Zur Erklärung: Diese Method implementiert die Operation „Abheben, wenn das Konto die nötige Deckung besitzt“ und liefert als Ergebnis dieser Operation, ob die Abbuchung stattgefunden hat oder nicht.

b. Geben Sie eine Klasseninvariante für die Klasse `Bank` an, die folgendes besagt:

Jeder Kunde einer Bank hat wenigstens ein Konto, das zu dieser Bank gehört.

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

```
invariant (\forall int i; 0<=i && i < this.kunden.length;
(\exists int j; 0<=j && j < this.kunden[i].konten.length;
this.kunden[i].konten[j].zugehoerigeBank == this));
```

Name:
Matr.-Nr.:

Fortsetzung von Aufgabe 6

c. Vervollständigen Sie im folgenden JML-Methodenvertrag die **Nachbedingung**. Die angegebene Methodenimplementierung summiert die Kontostände aller Konten eines Kunden auf.

```
class Kunde {
    Konto[] konten;

    /*@ public normal_behaviour
      @ requires true;
      @
      @ ensures
      @
      @ assignable \nothing;
      @*/
    int summe() {
       int s = 0;
       for(int i = 0; i < konten.length; i++) {
           s += konten[i].kontostand;
       }
       return s;
    }
}
```

```
ensures \result == (\sum int i; 0<=i && i < konten.length; konten[i].kontostand);
```

7 Modallogik, Büchi und LTL (1+1+2+1+4 Punkte)

Modallogik

a. Setzen Sie einen modallogischen Operator in die graue Leerstelle, so dass die Formel in allen Kripke-Rahmen allgemeingültig wird.

$$(\Box p \to p) \leftrightarrow (\neg p \to \boxed{\Diamond} p)$$

b. Welche Klasse von Kripke-Rahmen wird durch die modallogische Formel

$$p \to \Diamond p$$

charakterisiert?

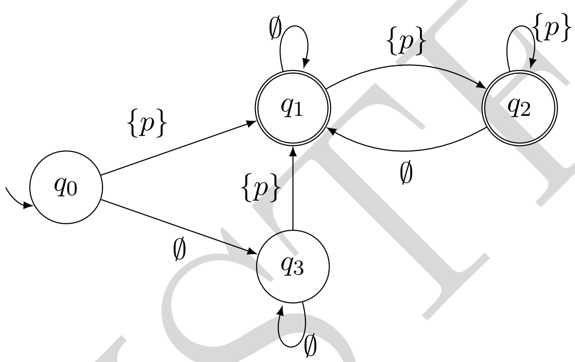
die reflexiven Kripke-Rahmen

Büchi und LTL

Die folgenden LTL-Formeln haben die Signatur $\{p\}$, die Büchi-Automaten das Alphabet $V = \{\emptyset, \{p\}\}$.

c. Geben Sie eine LTL-Formel A_0 an, welche genau in den *omega-Strukturen* wahr ist, die der folgende Büchi-Automat $\mathcal{A}_0$ akzeptiert (d.h., so dass $L^\omega(\mathcal{A}_0) = \{\xi \in V^\omega : \xi \models A_0\}$ gilt).

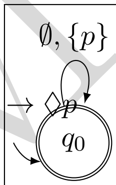
$(\mathcal{A}_0)$



$A_0 = \boxed{\Diamond p}$

d. Geben Sie einen Büchi-Automaten $\mathcal{A}_1$ an, der genau A_1 akzeptiert (d.h., so dass $L^\omega(\mathcal{A}_1) = \{\xi \in V^\omega : \xi \models A_1\}$ gilt).

$(\mathcal{A}_1)$



$A_1 = p \to \Diamond p$

e. Geben Sie einen Büchi-Automaten $\mathcal{A}_2$ an, der genau A_2 akzeptiert (d.h., so dass $L^\omega(\mathcal{A}_2) = \{\xi \in V^\omega : \xi \models A_2\}$ gilt).

$(\mathcal{A}_2)$

$A_2 = p \rightarrow \Diamond\Box p$