Klausur Formale Systeme

Fakultät für Informatik

WS 2019/20

Prof. Dr. Bernhard Beckert

28. Februar 2020

Name: ______________________

Vorname: ______________________

Matrikel-Nr.: ______________________

Die Bearbeitungszeit beträgt 60 Minuten.

A1 (12)	A2 (9)	A3 (7)	A4 (8)	A5 (9)	A6 (7)	A7 (8)	Σ (60)

Bewertungstabelle bitte frei lassen!

Gesamtpunkte:

1 Zur Einstimmung (4+5+3 = 12 Punkte)

a. Seien p ein einstelliges Prädikatensymbol und f ein einstelliges Funktionssymbol.

Geben Sie für folgende prädikatenlogische Formeln – **falls möglich** – Interpretationen I über dem Universum $D = \{a, b\}$ an, und zwar jeweils

- eine Interpretation, in der die Formel **wahr** ist, und
- eine Interpretation, in der die Formel **falsch** ist.

In den Fällen, in denen eine Interpretation mit der gesuchten Eigenschaft **nicht existiert**, geben Sie dies an.

Hinweis: Es muss explizit angegeben werden, wenn eine passende Interpretation nicht existiert (schreiben Sie „existiert nicht" neben den Kasten). Es genügt nicht, die Beschreibung der Interpretation leer zu lassen.

i. $\exists x\, \forall y\, (f(x) \doteq y)$

Interpretation, in der die Formel wahr ist:

$I(f)(a) =$	$I(f)(b) =$

Interpretation, in der die Formel falsch ist:

$I(f)(a) =$	$I(f)(b) =$

ii. $(\exists x\, p(x)) \to (\exists y\, p(f(y)))$

Interpretation, in der die Formel wahr ist:

$I(p)(a) =$	$I(p)(b) =$	$I(f)(a) =$	$I(f)(b) =$

Interpretation, in der die Formel falsch ist:

$I(p)(a) =$	$I(p)(b) =$	$I(f)(a) =$	$I(f)(b) =$

Fortsetzung 1 Zur Einstimmung

b. Geben Sie kurze Antworten zu folgenden Fragen bzw. Aufgaben:

i. Zeichnen Sie den reduzierten Shannongraphen, der eine aussagenlogische Tautologie repräsentiert.

ii. Geben Sie eine Substitution σ an, für die es **keine** Substitution ϕ mit $\phi \circ \sigma = id$ gibt

iii. Wir wollen aussagenlogische Formel in disjunktiver Normalform (DNF) auf Erfüllbarkeit untersuchen. Welche syntaktische Eigenschaft der einzelnen Klauseln muss man dafür überprüfen?

iv. Seien `m` und `n` zwei Java-Methoden, wobei `m` von `n` aufgerufen wird. Ein JML-Methodenvertrag für `m` enthalte die Vorbedingung „`requires false;`“. Beim Beweis, dass `n` seinen Vertrag erfüllt, wird der Vertrag von `m` als schon bewiesen angenommen und verwendet. Auf welches Problem stößt man dabei?

v. Wie überprüft man, ob ein Büchi-Automat eine nicht-leere Sprache akzeptiert?

c. Zeigen Sie mit Hilfe des **Tableaukalküls** der Aussagenlogik, dass folgende Formel allgemeingültig ist. Notieren Sie dabei:

- den Regeltyp (α, β) und die Formel, auf die eine Regel angewendet wird,
- bei Abschlüssen die beiden Partner.

$$0\ (A \wedge (A \to B)) \to B \qquad (1)$$

2 Theorien ((2+3) + (2+2) = 9 Punkte)

a. Wir betrachten die Arithmetik über den natürlichen Zahlen (mit + und $*$).

- Sei $\mathcal{N} = \{\phi \mid (\mathbb{N}, I_{\mathcal{N}}) \models \phi\}$ die Theorie, die durch das Standardmodell $(\mathbb{N}, I_{\mathcal{N}})$ der natürlichen Zahlen definiert ist.
- Sei $\mathcal{PA} = \{\phi \mid PA \models \phi\}$ die Theorie, die durch die Peano-Axiome PA definiert ist.

Diskutieren Sie (kurz) den Unterschied dieser beiden Theorien bzgl. folgender Aspekte:

i. Welche der Theorien enthält mehr Formeln, welche hat mehr Modelle?

ii. Sind die beiden Theorien axiomatisierbar? … entscheidbar? … rekursiv aufzählbar?

b. Sie arbeiten für eine Firma, die Motoren mit der dafür notwendigen Steuerungssoftware herstellt. Sie sollen Lizenzen für SMT-Solver erwerben, die die Entwicklungsingenieure der Firma nutzbringend verwenden können. Auf dem Markt gibt es vier SMT-Solver, die jeweils eine Theorie besonders gut unterstützen: (1) Arithmetik ganzer Zahlen, (2) Arithmetik reeller Zahlen, (3) Fließkomma-Arithmetik und (4) Arithmetik über Bitvektoren. Leider kann sich die Firma nur zwei dieser SMT-Solver leisten. Welche zwei wählen Sie und warum?

Hinweis: Es gibt für jeden der vier SMT-Solver gute Argumente.

i. SMT-Solver 1:

ii. SMT-Solver 2:

3 Shannongraphen (3+4 = 7 Punkte)

Zeichnen Sie zu jeder der folgenden aussagenlogischen Formeln den reduzierten Shannongraphen. Die Variablenordnung ist dabei $A < B < C$.

a. $(A \rightarrow B) \vee C$

b. $(A \leftrightarrow B) \wedge C$

4 Formalisieren in PL1 (2+2+2+2 = 8 Punkte)

Gegeben sei die prädikatenlogische Signatur $\Sigma = (\{sat\}, \{\emptyset, union, calc\}, \alpha)$. Sie enthält das Prädikatensymbol $sat(\cdot)$, sowie die Funktionssymbole $\emptyset$, $union(\cdot, \cdot)$ und $calc(\cdot)$.

Zur Auswertung der Formeln werden nur solche Interpretationen (D, I) über Σ verwendet, in denen

- das Universum D eine Menge aussagenlogischer Formelmengen ist,
- das Prädikat $sat(x)$ genau dann wahr ist, wenn die Formelmenge x erfüllbar ist,
- die Konstante $\emptyset$ die leere Formelmenge repräsentiert,
- die Funktion $calc(x)$ eine durch die Anwendung des Kalküls K aus x erhaltene Formelmenge zurückliefert,
- die Funktion $union(x_1, x_2)$ die Vereinigung der Formelmengen x_1 und x_2 zurückliefert.

Geben Sie jeweils eine Formel der Prädikatenlogik mit Gleichheit über Σ an, die folgende Sachverhalte darstellt:

a. Die leere Formelmenge ist erfüllbar.

b. Beim Anwenden des Kalküls K auf eine beliebige Formelmenge erhält man eine erfüllbarkeitsäquivalente Formelmenge.

c. Die Vereinigung zweier erfüllbarer Formelmengen kann unerfüllbar sein.

d. Beim Anwenden des Kalküls K auf eine erfüllbare Formelmenge erhält man die leere Formelmenge.

5 Resolutionskalkül (9 Punkte)

Zeigen Sie mit Hilfe des Resolutionskalküls für die Prädikatenlogik, dass folgende Klauselmenge unerfüllbar ist. Notieren Sie bei jedem Schritt die Klauseln, auf die die Resolutionsregel angewandt wurde, sowie **die verwendete Substitution**.

Signatur: p, q sind Prädikate; c ist eine Konstante; f ist eine Funktion; x_1, x_2, x_3, x_4, x_5 sind Variablen.

Hinweis: Mit der allgemeinen Resolutionsregel können die Klauseln (2) und (3) so resolviert werden, dass eine Einerklausel entsteht.

(1) $\{q(x_1),\ q(f(x_1))\}$ (2) $\{\neg q(x_2),\ \neg q(f(x_2))\}$ (3) $\{q(x_3),\ q(c))\}$

(4) $\{\neg q(f(f(c))),\ \neg p(x_4)\}$ (5) $\{p(x_5), \neg q(f(x_5))\}$

6 Spezifikation mit der Java Modeling Language

(3+4 = 7 Punkte)

a. Geben Sie die Bedeutung der Nachbedingung (**ensures-Klauseln**) in dem folgenden JML-Methodenvertrag in natürlicher Sprache wieder.

```
public class A {
    public int[] s;
    public int[] t;

    /*@ normal_behaviour
      @  requires t != null;
      @  assignable t;
      @  ensures t != null && t.length == \old(t.length);
      @  ensures (\forall int i; 0 <= i && i < t.length;
      @              i < s.length ==> t[i] == s[i]);
      @  ensures (\forall int i; 0 <= i && i < t.length;
      @              s.length <= i ==> t[i] == p);
      @*/
    public void m(int p) { ... }
}
```

Fortsetzung 6 Spezifikation mit der Java Modeling Language

b. Sei weiterhin eine Methode `f` in der obigen Klasse `A`. Vervollständigen Sie den nachstehenden JML-Methodenvertrag für `f`, so dass er Folgendes besagt:

Die Methode terminiert, wirft keine Exception und erfüllt folgende Nachbedingungen:

- Die Methode gibt ein von `null` verschiedenes `int`-Array zurück, das entweder genau so viele Elemente wie das Array `s` oder genau so viele Elemente wie das Array `t` enthält. Das zurückgegebene Array enthält aber nicht mehr Elemente als `s` und nicht mehr Elemente als `t`.
- Dabei enthält das zurückgegebene Array an jeder Stelle den Absolutwert der Differenz zwischen den Werten aus `s` und `t` an der jeweils gleichen Indexposition.

```
public class A {
    public int[] s;
    public int[] t;
    /*@
      @
      @
      @
      @
      @
      @
      @
      @
      @
      @
      @
      @
      @
      @*/
    public int[] f() { ... }
}
```

7 Lineare Temporale Logik (LTL) und Büchi-Automaten ((2+1)+5 = 8 Punkte)

a. Release-Operator

i. Formen Sie die LTL-Formel $\Box a$ so um, dass Sie eine äquivalente LTL-Formel erhalten, die nur den Release-Operator ($a\mathbf{V}b$) verwendet. Verwenden Sie dazu die Tautologien aus der Vorlesung.
Hinweis: $a\ \mathbf{V}\ b \quad \equiv \quad \neg(\neg a\ \mathbf{U}\ \neg b)$

$\Box a \quad \equiv$ ______________________________

ii. Bildet der Release-Operator eine Basis für die LTL-Operatoren $(\Box, \Diamond, \mathbf{U}, \mathbf{X})$? Begründen Sie!

____

____

b. Geben Sie einen nicht-deterministischen Büchi-Automaten an, dessen akzeptierte Sprache den Modellen (ω-Wörtern) der LTL-Formel

$$(\Diamond a) \rightarrow ((\neg b)\ \mathbf{U}\ a)$$

über der Signatur $\Sigma = \{a, b\}$ entspricht.

Für das Vokabular $V = \mathbb{P}(\Sigma)$ (Potenzmenge von Σ) werden die folgenden, aus der Vorlesung bekannten Abkürzungen definiert:

$$A = \{M \in V \mid a \in M\} \subset V \qquad B = \{M \in V \mid b \in M\} \subset V$$
$$\bar{A} = \{M \in V \mid a \notin M\} \subset V \qquad \bar{B} = \{M \in V \mid b \notin M\} \subset V$$