Karlsruher Institut für Technologie

Name: _____

Vorname: _____

Matrikel-Nr.: _____

Klausurnummer:

_____

Klausur Formale Systeme

Fakultät für Informatik

WS 2025/26

Prof. Dr. Bernhard Beckert

05. März 2026

Die Bearbeitungszeit beträgt 60 Minuten.

A1 (9)	A2 (11)	A3 (5)	A4 (7)	A5 (10)	A6 (10)	A7 (8)	Σ (60)

Bewertungstabelle bitte frei lassen!

Gesamtpunkte:

Matr.-Nr.:

1 Zur Einstimmung (1,5 + (2 + 2,5) + 3 = 9 Punkte)

a. Überprüfen Sie die folgende Hornformel auf Erfüllbarkeit. Benutzen Sie den Markierungsalgorithmus (auch „Erfüllbarkeitstest für Hornformeln“) aus der Vorlesung. Geben Sie unter „Schritt n“ an, welches Literal im n-ten Schritt markiert wurde. Geben Sie zudem an, ob der Algorithmus mit „Erfüllbar“ oder „Unerfüllbar“ terminiert.

$$(\neg P_1 \vee P_3) \ \wedge \ (\neg P_3 \vee P_2) \ \wedge \ (\neg P_1 \vee \neg P_2) \ \wedge \ P_1$$

Schritt 1:	Schritt 2:	Schritt 3:	Schritt 4:

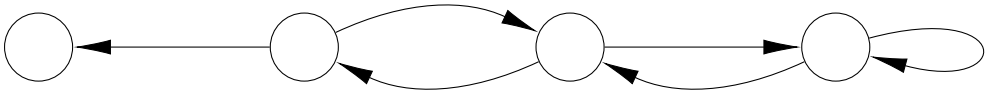
Ergebnis: _____

_____

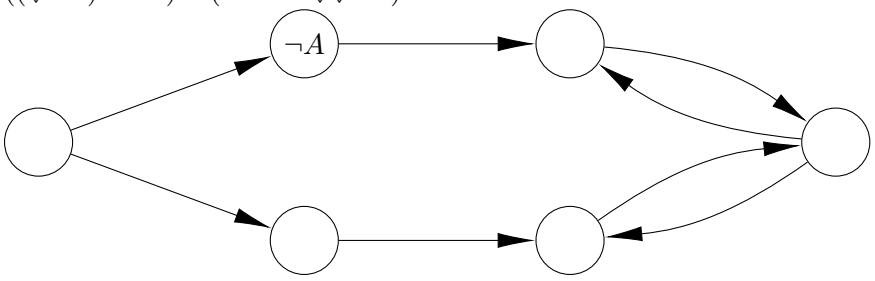
b. Geben Sie je eine Belegung der aussagenlogischen Variable A (A oder $\neg A$) in den Welten der folgenden Kripkestrukturen an, so dass die jeweils gegebene Formel in der Welt wahr ist.

Hinweis: Die Formel **0** entspricht der Formel *Falsch*, die in keiner Welt wahr ist.

i. $(\Diamond A \wedge \Diamond \neg A) \ \vee \ (\Box \mathbf{0} \leftrightarrow \neg A)$



ii. $((\Diamond \neg A) \rightarrow A) \wedge (A \rightarrow \Box \Diamond \Diamond \neg A)$



Fortsetzung 1 Zur Einstimmung

c. Transformieren Sie die aussagenlogische Formel

$$\neg\Big((P \vee Q) \to R\Big)$$

in die **kurze konjunktive Normalform**. Verwenden Sie das Verfahren aus der Vorlesung. Geben Sie als Zwischenschritte die Definition der Hilfsvariablen an.

2 Konservative Erweiterungen von Theorien

(2 + 5 + 4 = 11 Punkte)

Diese Aufgabe behandelt das Konzept der *konservativen Erweiterung* einer Theorie. Gegeben eine Theorie $\mathcal{T}(T)$ mit Signatur Σ, nennen wir eine Theorie $\mathcal{T}(T')$ über Signatur $\Sigma' \supseteq \Sigma$ eine konservative Erweiterung von $\mathcal{T}(T)$, wenn alle Formeln über der kleineren Signatur Σ, die aus der größeren Theorie $\mathcal{T}(T')$ folgen, schon aus der kleineren Theorie $\mathcal{T}(T)$ folgen. Formal definieren wir dies wie folgt:

Definition.

1. Eine Theorie $\mathcal{T}(T')$ über einer Signatur Σ' heißt *Erweiterung* einer Theorie $\mathcal{T}(T)$ über Σ, wenn

   $$\Sigma \subseteq \Sigma' \qquad \text{und} \qquad T \subseteq T' \ .$$

2. Gilt darüber hinaus für alle Formeln ϕ über Σ:

   $$T' \models \phi \qquad \text{genau dann, wenn} \qquad T \models \phi$$

   dann ist $\mathcal{T}(T')$ eine *konservative* Erweiterung von $\mathcal{T}(T)$.

Hinweis: In einer konservativen Erweiterung $\mathcal{T}(T')$ ist jede Formel ϕ über Σ, die in $\mathcal{T}(T')$ allgemeingültig ist, auch in $\mathcal{T}(T)$ allgemeingültig.

a. Wir definieren die folgenden Signaturen:

$$\Sigma = \{P\} \qquad\qquad \Sigma' = \{P, Q\}.$$

In welchen der beiden folgenden Fälle ist $\mathcal{T}(T')$ (über Σ') eine konservative Erweiterung von $\mathcal{T}(T)$ (über Σ)? Begründen Sie Ihre Antwort.

i. $T_1 = \emptyset$ und $T_1' = \{Q\}$

ii. $T_2 = \emptyset$ und $T_2' = \{Q,\ P \leftrightarrow Q\}$

Fortsetzung 2 Konservative Erweiterungen von Theorien

b. Für prädikatenlogische Formeln ist das Konzept der konservativen Erweiterung analog definiert.

Sei nun O die Theorie partieller Ordnungen über der Signatur, die nur $<$ enthält, also

$$O = \mathcal{T}\big(\{\forall x\, \neg(x < x),\ \forall x\, \forall y\, \forall z\, ((x < y \wedge y < z) \rightarrow x < z\}\big)$$

Sei O' eine Erweiterung von O über einer Signatur mit einer zusätzlichen Konstante max, in der axiomatisiert ist, dass max ein maximales Element bzgl. $<$ ist.

Begründen Sie, warum O' keine konservative Erweiterung von O ist.

c. Zeigen Sie:

Ist T eine vollständige Theorie, dann ist jede Erweiterung T' von T konservativ.

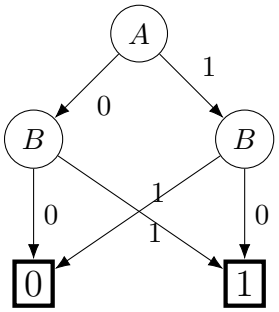
Hinweise:

- Eine Theorie heißt vollständig, wenn für alle Formeln ϕ über Σ gilt:
  $T \models \phi$ oder $T \models \neg\phi$
- Per Definition dürfen Theorien nicht inkonsistent sein ($T \not\models \mathbf{0}$).

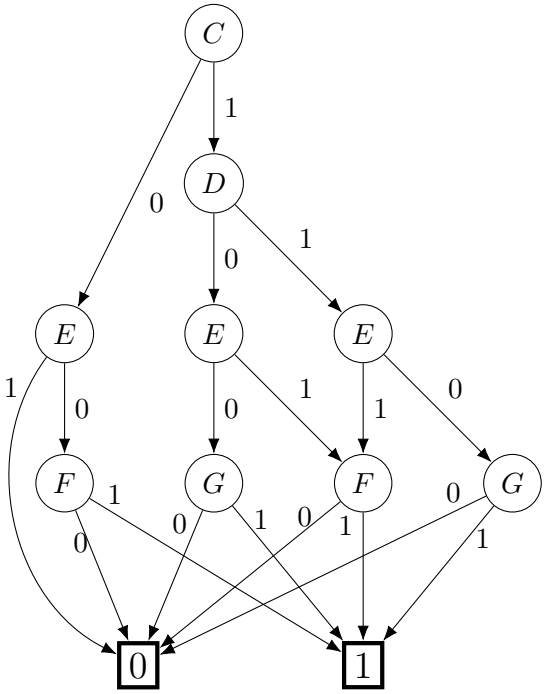
3 Shannongraph (1 + 4 = 5 Punkte)

Diese Aufgabe beschäftigt sich mit Shannongraphen (auch Binary Decision Diagrams genannt).

a. Geben Sie an welche Formel der folgende Shannongraph darstellt.



b. Unten sehen Sie einen Shannongraphen. Geben Sie den zugehörigen reduzierten Shannongraphen an.



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

Im Folgenden formalisieren und analysieren wir ein vereinfachtes, modulares, service-orientiertes Komponentensystem mithilfe der sortierten Prädikatenlogik erster Stufe.

Wir verwenden eine mehrsortige Signatur Σ mit Prädikatensymbolen $\{p, r, q\}$ mit den zwei Sorten C (*Komponente*) und S (*Dienst*).

Zur Auswertung der Formeln werden nur solche Interpretationen über Σ verwendet, in denen

- das Universum $U = U^C \uplus U^S$ ausschließlich eine Menge U^C von Komponenten und eine disjunkte Menge U^S von Diensten umfasst;
- $p(x^C, y^S) : C \times S$ genau dann wahr ist, wenn die Komponente x^C den Dienst y^S bereitstellt (*provides*);
- $r(x^C, y^S) : C \times S$ genau dann wahr ist, wenn die Komponente x^C den Dienst y^S benötigt (*requires*);
- $q(x^S) : S$ genau dann wahr ist, wenn der Dienst s aktiv ist (*quality* of service).

Hinweis: Nutzen Sie v, w, x, y, z als Variablen und annotieren Sie, wie in der Vorlesung die Sorte der jeweiligen Variable (bspw. x^S für eine Variable x von Sorte S).

Formalisieren Sie die folgenden Sachverhalte in sortierter Prädikatenlogik mit Gleichheit über Σ.

a. Wenn ein von einer Komponente bereitgestellter Dienst aktiv ist, dann müssen alle von dieser Komponente benötigten Dienste ebenfalls aktiv sein.

b. Jeder von einer Komponente benötigte Dienst muss von mindestens einer *anderen* Komponente bereitgestellt werden.

c. Gegenseitige Dienstabhängigkeiten zwischen zwei unterschiedlichen Komponenten sind nicht erlaubt.

5 Resolutionskalkül (4 + 6 = 10 Punkte)

a. Betrachten Sie die Folgerung

$$(\forall x \forall y\ r(x,y) \rightarrow \neg r(y,x))\ ,\ (\exists z \forall x\ r(z,x)) \quad \models \quad (\exists z\ \forall x\ \neg r(x,z))$$

Beachten Sie, dass x, y, z Variablen sind.

Formulieren Sie für die obige Folgerung eine Klauselmenge in konjunktiver Normalform, sodass Sie mit dem Resolutionskalkül einen Widerspruchsbeweis führen können, der die Folgerung beweist. Falls Sie neue Funktionssymbole oder Konstanten einführen, geben Sie dies explizit an.

b. Beweisen Sie die Unerfüllbarkeit der folgenden Klauselmenge mit dem Resolutionskalkül. Geben Sie alle notwendigen Substitutionen an. Beachten Sie, dass u, v, w, x, y, z Variablen sind und c, d Konstante sind.

$$\{\neg r(x,y), \neg r(y,z), r(x,z)\}, \quad \{\neg r(v,w), r(w,v)\}, \quad \{r(c,d)\}, \quad \{r(d,c)\}, \quad \{\neg r(u,u)\}$$

6 Spezifikation mit der Java Modeling Language (JML)

(5 + (3 + 2) = 10 Punkte)

a. Geben Sie in natürlicher Sprache wieder, was der folgende JML-Methodenvertrag für die Methode `m` aussagt.

```
public final class A {
    /*@ normal_behavior
      @  requires (\forall int i; 0 <= i < a.length; a[i] == 0 || a[i] == 1);
      @  requires 0 <= start < a.length;
      @  ensures 0 <= \result;
      @  ensures 0 <= start + \result <= a.length;
      @  ensures (\forall int i; start <= i < start + \result; a[i] == a[start]);
      @  ensures start + \result < a.length ==> a[start + \result] != a[start];
      @  assignable \nothing;
      @*/
    static int m(int[] a, int start) { ... }
}
```

Fortsetzung 6 Spezifikation mit der Java Modeling Language

b. Gegeben sei der folgende Auszug aus der Implementierung eines gerichteten Graphen. Ein Graph (Klasse `Graph`) speichert dabei seine Knoten (Klasse `Knoten`) als Array ohne Duplikate.

Außerdem soll jeder Graph ein Array seiner starken Zusammenhangskomponenten (SCCs) speichern. Sie können dabei davon ausgehen, dass diese bereits korrekt berechnet wurden. Eine SCC enthält dabei eine Referenz auf den zugehörigen Graphen sowie ein Array der Knoten der SCC.

Für die Modellierung stehen ihnen zwei Methoden zur Verfügung, die `pure` sind und deshalb auch in der Spezifikation verwendet werden dürfen:

- Die Methode `in(Knoten n)` gibt genau dann `true` zurück, wenn der gegebene Knoten sich im aktuellen SCC (`this`) befindet.
- Die **statische** Methode `erreichbar(Knoten ziel, Knoten start)` gibt genau dann `true` zurück, wenn der übergebene Knoten `ziel` von `start` aus in beliebig vielen Schritten erreichbar ist. Jeder Knoten gilt dabei als von sich selbst aus erreichbar.

Formulieren Sie folgende Objektinvarianten der Klassen `Graph` und `SCC`:

i. „Der Graph ist partitioniert in seine starken Zusammenhangskomponenten, jeder Knoten ist also in genau einer SCC enthalten.“

ii. „Jede SCC ist stark zusammenhängend, d.h. innerhalb der SCC ist jeder Knoten von jedem anderen aus erreichbar.“

Hinweise: Alle Felder und Methoden sind `public`, zur besseren Lesbarkeit sind die Sichtbarkeits-Modifikatoren weggelassen.

Der Code befindet sich auf der nächsten Klausurseite

```
class Knoten {
  // ...
}
```

Invariante der Klasse `Graph`:

```
class Graph {
  Knoten[] knoten;
  SCC[] sccs;

  // i. Der Graph ist partitioniert in seine starken Zusammenhangskomponenten,
  //    jeder Knoten ist also in genau einer SCC enthalten.
  /*@ invariant _____________________________________________________________
    @ _____________________________________________________________________
    @ _____________________________________________________________________
    @ _____________________________________________________________________
    @ _____________________________________________________________________
    @ _____________________________________________________________________
    @ _____________________________________________________________________
    @ _____________________________________________________________________ @*/
  // ...
}
```

Invariante der Klasse `SCC`:

```
class SCC {
  Graph g;
  Knoten[] sccKnoten;

  // ii. Jede SCC ist stark zusammenhängend,
  //     d.h. innerhalb der SCC ist jeder Knoten von jedem anderen aus erreichbar.
  /*@ invariant _____________________________________________________________
    @ _____________________________________________________________________
    @ _____________________________________________________________________
    @ _____________________________________________________________________
    @ _____________________________________________________________________
    @ _____________________________________________________________________
    @ _____________________________________________________________________ @*/



  /*@ pure @*/ boolean in(Knoten n) { /* ... */ }

  /*@ pure @*/ static boolean erreichbar(Knoten ziel, Knoten start) { /* ... */ }
  // ...
}
```

7 Lineare Temporale Logik (LTL)

((3 + 0,5 + 0,5) + 4 = 8 Punkte)

Ein geheimnisvoller Zauberer bewacht eine uralte Schatztruhe mit zwei Knöpfen und zwei Lichtern.

Nutzen Sie für die Bearbeitung der folgenden Teilaufgaben die Signatur $\Sigma = \{B, P, S, O\}$. Zur Auswertung der Formeln werden nur solche Strukturen über Σ verwendet in denen die Variablen die folgende Bedeutung haben:

B: Der blaue Knopf wird gedrückt

P: Der pinke Knopf wird gedrückt

S: Das Sternlicht leuchtet

O: Das Kreislicht leuchtet

a. i. Entschlüsseln Sie den Zauber

Der Zauberer verkündet:

> „Um die Truhe zu öffnen, musst du die Knöpfe genau in der folgenden Sequenz betätigen, andernfalls bleibt sie für immer verschlossen!“

$$B \wedge \mathbf{X}\Big(P \wedge \Diamond\big(S \wedge \mathbf{X}(B \,\mathbf{U}\, O)\big)\Big)$$

Beschreiben Sie in natürlicher Sprache mit welcher Abfolge von Aktionen die Truhe geöffnet werden kann.

ii. Formulieren Sie die folgenden Anforderungen in LTL

- Das Sternlicht wird irgendwann eingeschaltet und bleibt danach für immer eingeschaltet.
- Es dürfen zu keinem Zeitpunkt beide Knöpfe gleichzeitig gedrückt werden.

Fortsetzung 7 Lineare Temporale Logik (LTL)

b. Geben Sie einen nicht-deterministischen Büchi-Automaten an, dessen akzeptierte Sprache genau der Menge der erfüllenden Strukturen der Formel $B \wedge \mathbf{X}\Big(P \wedge \Diamond\big(S \wedge \mathbf{X}(B \,\mathbf{U}\, O)\big)\Big)$ entspricht.

Für das Vokabular $V = \mathcal{P}(\Sigma)$ (die Potenzmenge von Σ) werden die folgenden Abkürzungen definiert:

$$V_B = \{X \in V | B \in X\} \qquad V_P = \{X \in V | P \in X\}$$
$$V_S = \{X \in V | S \in X\} \qquad V_O = \{X \in V | O \in X\}$$

Sie dürfen an den Kanten des Automaten auch Mengen-Ausdrücke wie $V \setminus V_P$ verwenden.