

# LVA 185.276 Analyse und Verifikation (SS 2020)

## Selbsteinschätzungstest 10

Mi, 27.05.2020

*Stoff: Vorlesungsteil V, Kapitel 15, 16 und 17*

*Abstrakte Interpretation, Modellprüfung, Datenflussanalyse*

(Ohne Abgabe, ohne Beurteilung)

### Teil V, Kapitel 15 ‘Abstrakte Interpretation und Datenflussanalyse’

1. Was ist eine Galois-Verbindung? Welche Bestandteile gibt es? Wie sind sie miteinander verbunden? Wie hängen sie zusammen?
  - Was bedeuten Informationsgewinn und Informationsverlust in einer Galoisverbindung?
    2. Was bedeuten sie formal?
    3. Was informell?
  - Geben Sie ein
    4. triviales
    5. nicht triviales

Beispiel für eine Galois-Verbindung an.
6. In welcher Weise ist die Konkretisierungsfunktion einer Galois-Verbindung durch deren Abstraktionsfunktion eindeutig bestimmt?
7. Wenn eine Galois-Verbindung mit Abstraktionsfunktion  $\alpha$  und Konkretisierungsfunktion  $\gamma$  vorliegt, was weiß man dann über Eigenschaften von  $\alpha$  und  $\gamma$ ?
8. Was ist eine Adjunktion?
9. In welcher Weise liefern Adjunktionen eine Charakterisierung von Galois-Verbindungen?
10. Wo spielt im Verhältnis von Datenflussanalyse und reverser Datenflussanalyse der Adjunktionsbegriff eine Rolle?
11. Wann spricht man von einer Galois-Passung?
12. Was kann man in jedem Fall über die Eigenschaften von Abstraktions- und Konkretisierungsfunktionen von Galois-Verbindungen aussagen?
13. Was bedeutet der Begriff der Ordnungsähnlichkeit im Zusammenhang mit Galois-Passungen?
14. In einer Galois-Passung enthält der Verband der abstrakten Ebene keine überflüssigen Elemente. Was ist damit gemeint?
  - Was lässt sich über die Injektivität und Surjektivität von Konkretisierungs- und Abstraktionsfunktionen in
    15. Galois-Verbindungen
    16. Galois-Passungensagen?
17. Sind Ihre Beispiele als Antwort zu Frage 4 und 5 auch Beispiele für Galois-Passungen?
18. Was sind Prinzipien bzw. Wege zur systematischen Konstruktion von Galois-Verbindungen?

- Was ist ein
  19. Galois-System?
  20. System abstrakter Interpretationen?
  21. Turm von Galois-Systemen oder Systemen abstrakter Interpretationen?
- Was bedeuten
  22. Korrektheit
  23. Vollständigkeit
 in einem Galois-System?
- 24. In welcher Weise können wir Optimalität einer abstrakten Interpretation verstehen?
- 25. Was bedeutet der Begriff der Beobachtungsäquivalenz zweier abstrakter Semantiken?

### Teil V, Kapitel 16 ‘Modellprüfung und Datenflussanalyse’

1. Wie sieht das Grundproblem der Modellprüfung aus?
2. Wofür steht die Abkürzung CEGAR?
3. Welche Ergebnisse können am Ende eines Modellprüfungslaufs stehen?
4. In welcher Weise unterstützt ein CEGAR-fähiger Modellprüfer einen Anwender?
5. Was unterscheidet Transitionssysteme und Kripke-Strukturen?
6. Welche syntaktischen Konstrukte umfasst der modale  $\mu$ -Kalkül?
7. Beschreiben Sie informell die Semantik der syntaktischen Konstrukte des modalen  $\mu$ -Kalküls.
8. Was versteht man unter Modalitäten, was unter Rückwärtsmodalitäten des modalen  $\mu$ -Kalküls?
9. Was bedeuten die abgeleiteten Operatoren **AG** und **U** des modalen  $\mu$ -Kalküls informell?
10. Welche Analogie lässt sich zwischen Modellprüfung und Datenflussanalyse aufzeigen?

### Teil V, Kapitel 17 ‘Modellprüfung und Abstrakte Interpretation’

1. Was ist verfahrenstechnisch das Hauptproblem, die Hauptschwierigkeit von Modellprüfungsverfahren?
2. Warum haben Modellprüfungsverfahren für Hardware früher reüssiert als für Software?
3. Modellprüfung, Datenflussanalyse, abstrakte Interpretation. Gegensatz, Ergänzung, Symbiose? Begründen Sie Ihre Antwort.

### Teil I – V, Verschiedene Kapitel

1. Erweitere den Hoare-Kalkül für totale Korrektheit um eine Regel zur Behandlung der repeat-Schleife:

$$\text{repeat } \pi \text{ until } b \text{ end}$$

ohne sich dabei auf die Existenz der while-Schleife und deren entsprechende Hoare-Kalkülregel abzustützen.

2. Beweise mit der Regel aus der vorigen Aufgabe die Korrektheit des Hoare-Tripels:

$$[x > 0] \quad z := 0; \quad u := x; \quad \text{repeat } z := z + y; \quad u := u - 1 \quad \text{until } u = 0 \quad \text{end} \quad [z = x * y]$$

3. Wie lässt sich die Richtigkeit der Regel aus Aufgabenteil 1 zeigen? Was ist zu beweisen?

4. Was hat es mit der Dualität Fixpunkte von Funktionen und Lösungen von Gleichungssystemen auf sich? Illustriere diese Dualität am Beispiel von Datenflussanalyse.
5. Erläutere die Idee sog. *chaotischer Iteration*.
6. Inflationäre Funktionen werden synonym oft auch wie bezeichnet?
7. Was ist die Besonderheit des chaotischen Fixpunkttheorems im Vergleich zu anderen Fixpunkttheoremen?
8. Anweisungen können partiell oder total tot sein. Was bedeutet das?
9. Eine Anweisung an einer Programmstelle ist entweder tot oder nicht. Eine Anweisung an einer Programmstelle ist entweder geisterhaft oder nicht. Tot und geisterhaft sind für eine Anweisung Boolesche Eigenschaften (Eigenschaft gilt bzw. gilt nicht). Tot und geisterhaft sind deshalb in gleicher Weise Beispiele sog. Bitvektorprobleme. Richtig oder falsch? Begründen Sie Ihre Antwort.
10. Was sind sog. *kritische Kanten* in einem Programm? Welche Bedeutung haben sie für Programmtransformationen, die Anweisungen an andere Programmstellen verschieben (sollen)?
11. Welche Bedeutung hat das Chaotische Fixpunkttheorem aus Kapitel 11 für die Beseitigung partiell toter Anweisungen in einem Programm?
12. Erklären Sie die Intuition, die dem Gleichungssystem zur Berechnung geisterhafter Variablen zugrundeliegt:

$$\begin{aligned}
 \text{N-FAINT}_n^v &= \overline{\text{LifeEnforcingUse}_n^v} * \\
 &\quad (\text{X-FAINT}_n^v + \text{Mod}_n^v) * \\
 &\quad (\text{X-FAINT}_n^{\text{LhsVar}_n} + \overline{\text{AssUse}_n^v}) \\
 \text{X-FAINT}_n^v &= \prod_{m \in \text{succ}(n)} \text{N-FAINT}_m^v
 \end{aligned}$$

13. Für die Charakterisierungen zweier Formel  $p$  und  $q$  gilt:  $Ch(p) \subseteq Ch(q)$ . Was gilt für die Implikationsbeziehung zwischen  $p$  und  $q$ ?
14. Ordnen Sie die Begriffe Relation, Quasiordnung, partielle Ordnung, Äquivalenzrelation, kettenvollständige partielle Ordnung, Verband, vollständiger Verband im Stil eines Hasse-Diagramms an. Was bedeutet es, wenn in Ihrem Diagramm zwei Begriffe unmittelbar miteinander verbunden sind?
15. Zur näheren Beschreibung oder Bestimmung von was dienen die Begriffe
  - (a) ordnungserhaltend?
  - (b) größte untere Schranken erhaltend?
  - (c) kleinste obere Schranken erhaltend?
 Wie sind diese Begriffe formal definiert?
16. Was verstehen wir unter einem *SUP*-konservativen DFA-Algorithmus, was unter einem *SUP*-straffen?
17. Die einfache-Konstanten-Analyse ist *SUP*-konservativ, für schleifenfreie Programme sogar *SUP*-straff. Richtig oder falsch? Begründen Sie Ihre Antwort.
18. In Kapitel 7 haben wir die Semantik von Ausdrücken über den Zwischenschritt einer Interpretation von Konstanten- und Operatorsymbolen eingeführt; in Kapitel 1 haben wir die Semantik von Ausdrücken ohne explizite Interpretationsfunktion eingeführt. Ist das Vorgehen in Kapitel 7 zu aufwändig? Oder das in Kapitel 1 womöglich zu einfach? Begründen Sie Ihre Antwort.
19. Wann sprechen wir von Operatoren, wann von Operationen? Wann von Relatoren, wann von Relationen?
20. Induktive Beweise über die Länge von Berechnungsfolgen oder den Aufbau von Ableitungsbäumen lassen sich als Spezialisierungen anderer induktiver Beweisprinzipien auffassen. Welcher?