LVA 185.276 Analyse und Verifikation (SS 2020)

Selbsteinschätzungstest 3

Mo, 16.03.2020

Stoff: Vorlesungsteil I, Kapitel 3, 4 und 5

Denotationelle und axiomatische Semantik, Axiomatische Ausführungszeitanalyse

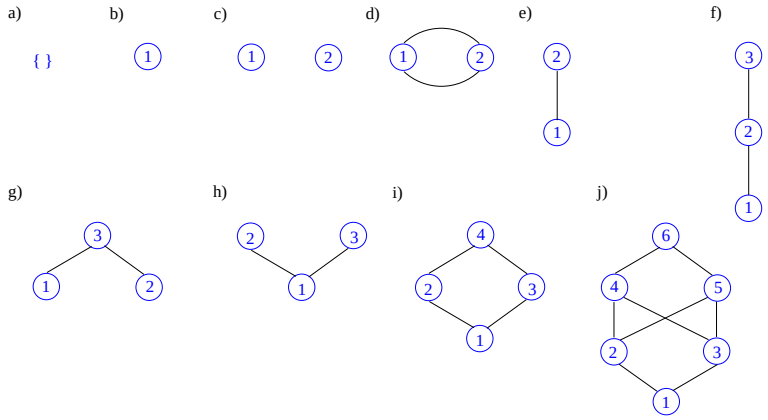
(Ohne Abgabe, ohne Beurteilung)

Teil I, Kapitel 3 'Denotationelle Semantik von WHILE'

Die Festlegung der denotationellen Semantik von WHILE stützt sich auf vollständige partielle Ordnungen, spezielle partielle Ordnungen. Überprüfen Sie, welche der folgenden in Form von Hasse-Diagrammen (bzw. Hasse-Diagramm-ähnlichen Diagrammen) gegebenen (Halb-) Ordnungen (engl. pre-order)

1. partielle Ordnungen (engl. partial order)
2. vollständige partielle Ordnungen (engl. chain-complete partial order (CCPO))
3. Verbände (engl. lattice)
4. vollständige Verbände (engl. complete lattice)

sind. Begründen Sie Ihre Antwort, wenn eine Eigenschaft nicht erfüllt ist (s. Anhang A.2.1 und A.2.8 für partielle Ordnungen und Hasse-Diagramme, Anhang A.4 für Verbände und vollständige Verbände). Verbände, speziell vollständige Verbände, sind in Kapitel 7, 8 und 9 von zentraler Bedeutung.



Teil I, Kapitel 4 'Axiomatische Semantik von WHILE'

1. Was sollen die unterschiedlichen Sprechweisen *Hoare-Tripel*, *Hoaresche Zusicherung* zum Ausdruck bringen?
2. Was bedeutet Korrektheit, was Vollständigkeit eines Beweiskalküls? Illustrieren Sie Ihre Antwort am Beispiel des Hoare-Kalküls für partielle Korrektheit.
3. Gibt es ein WHILE-Programm π, für das die Hoaresche Zusicherung

   $$\{true\} \;\; \pi \; \{false\}$$

   total korrekt ist?
4. Sei π ein Übersetzer, ein Programm, das Programme einer Quellsprache Q in Programme einer Zielsprache Z überführt. Was erwartet man (mindestens) von π, um π einen korrekten Übersetzer von Q nach Z zu nennen? Sind partielle und totale Korrektheit im Sinn der entsprechenden Hoare-Kalküle geeignet, um diese Erwartung(en) an π formal zu fassen? Wie begründen Sie Ihre Antwort?

5. Warum sind in Vor- und Nachbedingung Hoarescher Zusicherungen neben Variablen, die im Programm vorkommen, i.a. auch Variablen nötig, die nicht im Programm vorkommen, sog. *logische Variablen*?

6. Welcher Zusammenhang, welche Beziehung besteht zwischen partieller und totaler Korrektheit?

7. In der Zuweisungsregel des Kalküls für totale Korrektheit (beide Varianten V1 und V2) werden die eckigen Klammern mit überladener Bedeutung verwendet:

   $$[\text{ass}] \quad \frac{}{[p[t/x]]\ x{:=}t\ [p]} \qquad \begin{array}{l}(\text{Rückwärtssubstitution,}\\ \text{Rückwärtsregel})\end{array}$$

   Welche sind das?

8. Was unterscheidet *schwächste* von *schwächsten liberalen Vorbedingungen* Hoarescher Zusicherungen?

9. Warum lassen sich Beweise partieller und totaler Korrektheit auch bei allergrößtem Bemühen nicht vollständig automatisieren?

10. Für die Zuweisung sehen die Hoare-Kalküle für partielle und totale Korrektheit eine sog. Rückwärtszuweisungsregel vor. Wie kommt es zu dieser Namensgebung? Illustrieren Sie Ihre Antwort anhand der entsprechenden Regel.

11. Warum hat man sich in den Kalkülen für die Behandlung von Zuweisungen für eine Rückwärts-, nicht für eine Vorwärtsregel entschieden?

12. Welches ist die kanonische Beweisform partieller und totaler Korrektheitsbeweise von Hoare-Tripeln? Welche ist eine schreibökonomischere Variante? Warum kann man diese ökonomischere Variante als ausreichend betrachten?

Teil I, Kapitel 5 'Axiomatische Ausführungszeitanalyse'

Ein Echtzeitsystem heißt

- *hart*, wenn das Überschreiten einer Zeitvorgabe das System ab diesem Moment unbrauchbar und nutzlos macht.
- *weich*, wenn bei Überschreiten von Zeitvorgaben das System nicht schlagartig unbrauchbar wird, sondern sein Nutzen nach Ausmaß der Überschreitung mehr und mehr abnimmt (bis ebenfalls hin zur Nutzlosigkeit).
- *sicherheitskritisch*, wenn das Überschreiten von Zeitvorgaben schwere Auswirkungen auf Leib und Leben oder hohe Sachwerte hat.

1. Nennen Sie einige Beispiele für harte, weiche und sicherheitskritische Echtzeichtsysteme.

2. Welche Art von Aussagen zum Laufzeitverhalten eines Programms sind mithilfe des Kalküls aus Kapitel 5 möglich? Sind Beweise mithilfe dieses Kalküls für den Nützlichkeitsnachweis harter, weicher oder sicherheitskritischer Echtzeitsysteme geeignet? Begründen Sie Ihre Antwort.

3. Wie kann man die Bedeutung der Regeln für die Fallunterscheidung und die sequentielle Komposition des Laufzeitabschätzungskalküls informell erklären:

   $$[\text{ite}_e] \quad \frac{[p \wedge b]\ \ \pi_1\ \ [e \Downarrow q],\ \ [p \wedge \neg b]\ \ \pi_2\ \ [e \Downarrow q]}{[p]\ \text{if}\ b\ \text{then}\ \pi_1\ \text{else}\ \pi_2\ \text{fi}\ \ [e \Downarrow q]}$$

   $$[\text{comp}_e] \quad \frac{[p \wedge e_2^{'}{=}u]\ \ \pi_1\ \ [e_1 \Downarrow r \wedge e_2 \leq u],\ \ [r]\ \ \pi_2\ \ [e_2 \Downarrow q]}{[p]\ \ \pi_1;\pi_2\ \ [e_1{+}e_2^{'} \Downarrow q]}$$

   wobei u frische logische Variable.

   Warum kommt die Regel für die die Fallunterscheidung mit einem Abschätzungsterm e aus? Warum braucht die Regel für die sequentielle Komposition neben zwei Termen e_1 und e_2 noch einen dritten Term $e_2^{'}$?