Programmeren & Correctheid

Docent: Prof. dr. F.S. de Boer, email: frb@cwi.nl
Assistent: Hans-Dieter Hiep, email: hdh@cwi.nl

Literatuur
Verification of Sequential and Concurrent Programs.
Krzysztof R. Apt, Frank S. de Boer, Ernst-Rüdiger Olderog.
Series: Texts in Computer Science. Springer.
3rd ed. 2nd Printing. ISBN: 978-1-84882-744-8.

Te behandelen stof
Course Towards Object-Oriented Program Verification (zie *Preface*: *Outlines of One-Semester Courses* en slides). Uit bovenstaand boek behandelen we de hoofdstukken 2, 3, 4, en 5 onderverdeeld in de volgende blokken B1-3:

	Onderwerp	Secties uit het boek
B1	Partiële Correctheid While Programma's	2.1, 2.2, 2.4, 2.5, 2.7, 3.1, 3.3, 3.4 3.10, 3.11.
B2	Totale Correctheid While Programma's	3.3, 3.4 en 3.8..
B3	Partiële Correctheid Recursieve Programma's	4.1, 4.3, 5.1, 5.2, 5.3.

Evaluatie

- De behandelde stof (zie de paragraaf "Te behandelen stof" hierboven) wordt schriftelijk geëxamineerd .
- Daarnaast wordt er voor elke blok een *deeltentamen* gegeven. In totaal zijn er dus drie deeltentamens (t.z.t. worden de data bekend gemaakt).

    1. **Het eerste deeltentamen vindt plaats op vrijdag 13 Maart, tijdens het werkcollege**. De stof betreft blok B1.

Voor het eindcijfer telt het schriftelijk tentamen voor 75%. Het gemiddelde van de deeltentamens telt voor 25%.

Agenda We maken in de opgaven (en de uitwerkingen) gebruik van de volgende afkortingen:

$$\begin{array}{rll}
\bigwedge_{i=1}^{n} p_i & \text{staat voor} & p_1 \wedge ... \wedge p_n \\
s \leq t & \text{staat voor} & s < t \vee s = t \\
s \leq t < u & \text{staat voor} & s \leq t \wedge t < u \\
s \neq t & \text{staat voor} & \neg(s = t) \\
\exists x, y : p & \text{staat voor} & \exists x : \exists y : p \\
\forall x, y : p & \text{staat voor} & \forall x : \exists y : p \\
\exists x \leq t : p & \text{staat voor} & \exists x : (x \leq t \wedge p) \\
\forall x \leq t : p & \text{staat voor} & \forall x : (x \leq t \rightarrow p) \\
\forall x \in [s : t] : p & \text{staat voor} & \forall x : (s \leq x \leq t \rightarrow p)
\end{array}$$

In de slides maken we ook gebruik van andere voor zich sprekende afkortingen (als $\forall n : s \leq n \leq t : p$ voor $\forall n : (s \leq n \wedge n \leq t) \rightarrow p)$). Zie verder werkcollege opgaven voor meer informatie over wat er tijdens het werkcollege is behandeld.

7-2 Introduktie (zie slides 1 t/m 21).
Opgaven: Zie slide 18.

14-2 Hoofdstuk 2, secties 2.1, 2.2, , 2.4, 2.5 en 2.7, en sectie 3.1 van hoofdstuk 3. Zie ook slides 22–30.
Opgaven:

1. Bereken de volgende substituties:
   (a) $(x = Y \wedge y = X)[y := z][x := y][z := x]$
   (merk op dat $z := x; x := y; y := z$ de waarden van de integer variabelen x en y verwisselt ("swapt").

   (b) $(a[i] = Y \wedge a[j] = X)[a[j] := z][a[i] := a[j]][z := a[i]]$
2. Stel dat we geen *gebonden* variabelen in p herbenoemen als we een substitutie $[u := t]$ toepassen (zie Sectie 2.7 van het boek). Laat zien dat er dan *ongeldige* instanties zijn van het assignment axioma, d.w.z., vind een postconditie p en een assignment $u := t$ zodat $\{p[u := t]\}\ u := t\ \{p\}$ *niet* waar is.
3. Opgave 3.4 (Boek) en voor welke statements gelden de volgende correctheidsbeweringen.
4. Onderzoek of de assertie

$$a[a[n]] \leq \textbf{if } a[a[n]] = a[n] \textbf{ then } a[a[n]] \textbf{ else } a[a[a[n]]] \textbf{ fi}$$

waar is voor alle arrays a (van type **integer** $\rightarrow$ **integer**). Zo niet, geef een tegenvoorbeeld.

5. Welke programma's S waarin de variabele z niet voorkomt voldoen aan

$$\{x = z * z\}S\{x = z\}$$

voor partiële correctheid?

6. Specificeer een programma dat de sectie $a[1 : n]$ van array a van type **integer** $\rightarrow$ **integer** sorteert (let op: hier is ook voor nodig dat het resultaat een permutatie is van de de initiele array a).

7. Opgave 2.2(i) uit het boek en bereken
   (a) $(\exists z : z = x - 1)[x := z]$
   (b) $(\exists y : y = x - 1)[x := z]$

21-2 Hoofdstuk 3, sectie 3.3 (Partial Correctness). Zie ook slides 31 – 35.
Opgaven:

1. (a) Bewijs de correctheidbewering

$$\{\textbf{true}\}\ \textbf{while true do}\ \text{skip}\ \textbf{od}\ \{\textbf{false}\}$$

   (b) Bewijs vervolgens dat

$$\{p\}\ \textbf{while true do}\ \text{skip}\ \textbf{od}\ \{q\}$$

   voor willekeurige preconditie p en postconditie q.

2. Bewijs de correctheidsbewering (array copy)

$$\{i = 0\}\ \textbf{while}\ i < k\ \textbf{do}\ a[i] := b[i]; i := i + 1\ \textbf{od}\ \{\forall 0 \leq n < k : a[n] = b[n]\}$$

28-2 Hoofdstuk 3, sectie 3.4 (Proof Outlines en Partial Correctness). Zie ook slides 36 – 41.
Opgaven 3.9(ii) (in PW, partial correctness) en 3.10(i) uit het boek, en opgave

1. Bewijs de correctheidsbewering (array copy)

$$\{i = 1\}\ \textbf{while}\ i < k\ \textbf{do}\ a[i] := b[i]; i := i + 1\ \textbf{od}\ \{\forall n : 1 \leq n < k : a[n] = b[n]\}$$