A Denotational Engineering of Programming Languages

…

Part 8: Total correctness of programs
(Section 7.7 of the book)

Andrzej Jacek Blikle

April 5th, 2020

The repetition of weak total correctness

GENERAL (NONDETERMINISTIC) CASE

$A \subseteq PB$ – weak total correctness wrt precondition A and postcondition B

For every a:A, **there is** a-execution of P that terminates in B (but there may be another one, that does not terminate in B or does not terminate at all)

DETERMINISTIC CASE

$A \subseteq FB$ – For every a : A, F.a = ! and F.a : B

$A \subseteq FB$ iff $AF \subseteq B$ and $F : A \longmapsto S$

A proof of total correctness may be split into two steps.

Weak total correctness

No recursion (nondeterministic)

Sequential composition

$$\begin{array}{l} A \subseteq PB \\ C \subseteq QD \text{ there is } C \\ B \subseteq C \\ \hline A \subseteq (P;Q)\ D \end{array}$$

Strengthening precondition

$$\begin{array}{l} A \subseteq PB \\ C \subseteq A \\ \hline C \subseteq PB \end{array}$$

Conditional composition; $C \cap \neg C = \emptyset$

$$\begin{array}{ll} (A \cap C) & \subseteq PB \\ (A \cap \neg C) & \subseteq QB \\ A & \subseteq C \mid \neg C \\ \hline A \subseteq \textbf{if } (C,\neg C) \textbf{ then } P \textbf{ else } Q \textbf{ fi } B & \end{array}$$

Weakening postcondition

$$\begin{array}{l} A \subseteq PB \\ B \subseteq C \\ \hline A \subseteq PC \end{array}$$

Not in Hoare's logic!

Total correctness
Nondeterministic multirecursion

A componentwise CPO of vectors of relations

$\mathbf{R} = (R_1,\ldots,R_n)$ $\quad \mathbf{A} = (A_1,\ldots,A_n)$ $\quad \mathbf{B} = (B_1,\ldots,B_n)$ $\quad n \geq 1$

Let **R** be the least solution of $\mathbf{X} = \Psi.\mathbf{X}$,

Rule 7.7.2-1

there exists a family of preconditions $\{\mathbf{C}_i \mid i \geq 0\}$
and a family of postconditions $\{\mathbf{D}_i \mid i \geq 0\}$ such that

(1) $(\forall i \geq 0)\ \mathbf{C_i} \subseteq (\Psi^i.\emptyset)\mathbf{D}_i$
(2) $\mathbf{A} \subseteq \mathbf{U}\{\mathbf{C}_i \mid i \geq 0\}$
(3) $(\forall i \geq 0)\ \mathbf{D_i} \subseteq \mathbf{B}$

---

(4) $\mathbf{A} \subseteq \mathbf{RB}$

Total correctness

Nondeterministic single recursion

$R \subseteq S \times S, \quad A, \quad B \subseteq S$

R is the least solution of $X = \Psi.X$,

Rule 7.7.2-2

there exists a family of preconditions $\{A_i \mid i \geq 0\}$
and a family of postconditions $\{B_i \mid i \geq 0\}$ such that

(1) $(\forall i \geq 0)\ A_i \subseteq (\Psi^i.\varnothing)A_i$
(2) $A \subseteq U\{A_i \mid i \geq 0\}$
(3) $(\forall i \geq 0)\ B_i \subseteq B$

---

(4) $A \subseteq RB$

Where is the proof of halting property of R?

By (1), states from A_i initiate executions with exectly i recursive calls.

Total correctness

Simple recursion (nondetermnistic)

If T is the least solution of $X = HXT \mid E$ then for any $A, B \subseteq S$

Rule 7.6.2-3

there exists a family of preconditions $\{A_i \mid i \geq 0\}$
and a family of postconditions $\{B_i \mid i \geq 0\}$ such that

$(\forall i \geq 0)\ A_i \subseteq (H^i E T^i) B_i$

$A \subseteq U\{A_i \mid i \geq 0\}$

$(\forall i \geq 0)\ B_i \subseteq B$

$A \subseteq RB$

Total correctness

While instruction in a nondeterministic case

R = **while** (C, ¬C) **do** P **od**

R = [C]P R | [¬C]

R = ([C]P)*[¬C]

Rule 7.6.2-3

there exists a family of preconditions $\{A_i \mid i \geq 0\}$
and a family of postconditions $\{B_i \mid i \geq 0\}$ such that

$(\forall i \geq 0)\ A_i \subseteq ([C]P)^i[\neg C]\ B_i$

$A \subseteq U\{A_i \mid i \geq 0\}$

$(\forall i \geq 0)\ B_i \subseteq B$

$A \subseteq$ **while** (C, ¬C) **do** P **od** B

Clean total correctness of while
Auxiliary concepts

ograniczona powtarzalność

F : S → S has a limited replicability in a set N ⊆ S if there is no infinite sequence

s, F.s, F.(F.s),… in N.

dobrze ufundowany

A partially ordered set (U, >) is said to be a well-founded set, if there is no infinite decreasing sequence in it, i.e., a sequence $u_1 > u_2 > \ldots$

Lemma 7.7.2-1

If there exists a well founded set (U, <) and a function K : N ⟼ U such that for any a : N, F.a = !, F.a : N and

K.a > K.(F.b)

then F has limited replicability in N.

Clean total correctness of while
Deterministic case

For any $F : S \to S$, any $A,B,N \subseteq S$, and any disjoint $C,\neg C \subseteq S$

(1) $A \subseteq N$

(2) $N \subseteq C \mid \neg C$

(3) $N \cap \neg C \subseteq B$

(4) $(N \cap C) \subseteq FN$ (clean total correctness of F)

(5) [C]F has limited replicability in N

$A \subseteq$ **while** $(C,\neg C)$ **do** F **od** B

No abortion or looping


Thank you for
your attention