

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 $F.a : B$

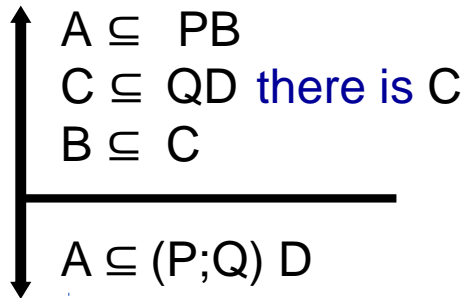
$A \subseteq FB$ iff $AF \subseteq B$ and $F : A \mapsto S$

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

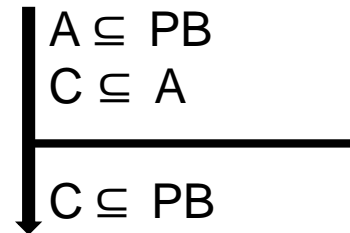
Weak total correctness

No recursion (nondeterministic)

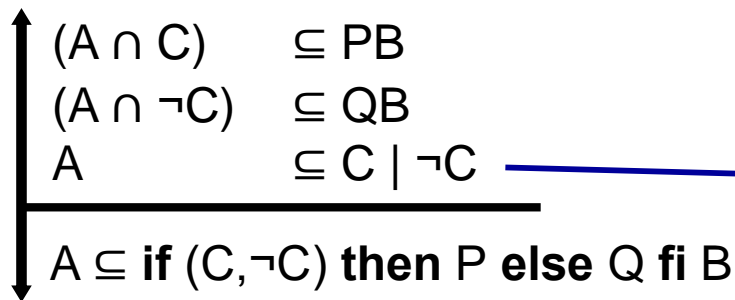
Sequential composition



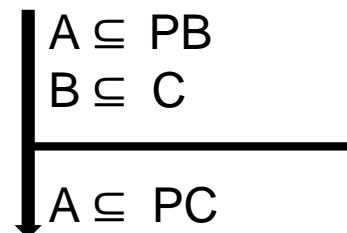
Strengthening precondition



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



Weakening postcondition



Not in Hoare's logic!

Total correctness

Nondeterministic multirecursion

A componentwise CPO of vectors of relations

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

Let \mathbf{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

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

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) $(\forall i \geq 0) A_i \subseteq (\Psi^i.\emptyset)A_i$

(2) $A \subseteq \bigcup\{A_i \mid i \geq 0\}$

(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 exactly i recursive calls.

Total correctness

Simple recursion (nondeterministic)

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

$$\begin{array}{l} (\forall i \geq 0) A_i \subseteq (H^i E T^i) B_i \\ A \subseteq U\{A_i \mid i \geq 0\} \\ (\forall i \geq 0) B_i \subseteq B \end{array}$$

$A \subseteq RB$

Total correctness

While instruction in a nondeterministic case

$R = \mathbf{while} (C, \neg C) \mathbf{do} P \mathbf{od}$

$R = [C]P R \mid [\neg C]$

$R = ([C]P)^*[\neg C]$

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
 $(\forall i \geq 0) A_i \subseteq ([C]P)^i[\neg C] B_i$
 $A \subseteq U\{A_i \mid i \geq 0\}$
 $(\forall i \geq 0) B_i \subseteq B$

↓ $A \subseteq \mathbf{while} (C, \neg C) \mathbf{do} P \mathbf{od} B$

Clean total correctness of while

Auxiliary concepts

ograniczona powtarzalność

$F : S \rightarrow S$ has a limited replicability in a set $N \subseteq S$ if there is no infinite sequence

$s, F.s, F.(F.s), \dots$ 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 $u_1 > u_2 > \dots$

Lemma 7.7.2-1

If there exists a well founded set $(U, <)$ and a function $K : N \mapsto U$ 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 $F : S \rightarrow S$, 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

$A \subseteq \mathbf{while} (C, \neg C) \mathbf{do} F \mathbf{od} B$

No abortion or looping



Thank you for
your attention