A Denotational Engineering of Programming Languages

...

Part 8: Total correctness of programs

(Section 7.7 of the book)

Andrzej Jacek Blikle

May 21st, 2021

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 $F.a : B$

$$\boxed{A \subseteq FB \quad \text{iff} \quad AF \subseteq B \text{ and } F : A \longmapsto S}$$

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

Proof rules for weak total correctness

No recursion (nondeterministic)

Sequential composition

$$\frac{\begin{array}{l} A \subseteq PB \\ C \subseteq QD \\ B \subseteq C \end{array}}{A \subseteq (P;Q)\, D}$$

Strengthening precondition

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

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

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

Weakening postcondition

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

Not in Hoare's logic!

Proof rules for weak total correctness

Nondeterministic multirecursion

A componentwise CPO of vectors of relations

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

Let **R** be the least solution of **X = Ψ.X**,

Rule 7.7.2-1

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

(1) $\mathbf{A} \subseteq \mathbf{U}\{\mathbf{A}_i \mid i \geq 0\}$

(2) $(\forall i \geq 0)\ \mathbf{A}_i \subseteq (\mathbf{\Psi}^i.\boldsymbol{\varnothing})\mathbf{B}_i$

(2) (3) $(\forall i \geq 0)\ \mathbf{B}_i \subseteq \mathbf{B}$

---

(4) $\mathbf{A} \subseteq \mathbf{R}\mathbf{B}$

Proof rules for weak 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) $(\forall i \geq 0)\ A_i \subseteq (\Psi^i.\varnothing)A_i$

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

(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.

Proof rules for weak total correctness

Simple recursion (nondetermnistic)

If R is the least solution of X = HXT | 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

$$(\forall i \geq 0)\ A_i \subseteq (H^i E T^i) B_i$$
$$A \subseteq \cup\{A_i \mid i \geq 0\}$$
$$(\forall i \geq 0)\ B_i \subseteq B$$

$$A \subseteq RB$$

Proof rules for weak 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

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

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

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

A ⊆ **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.

E.g. x := x-1 has limited replicability in the set of states N = {sta | sta.x > 0}

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 ⟼ 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.

Proof rule for (strong) 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 ⊆ **while** (C,¬C) **do** F **od** B

No abortion or looping

Clean total correctness of while

Simple example

```
pre n, m > 0
 x := 1; y := m;
 while x < n do;
 x := x+1;  y := y*m
post y = m^n
```

A = {x=1 & y=m, n,m>0}

B = {y =m^n}

N = {n,m > 0 & 0 < x < n & y = m^x}

`[x<n][x:=x+1;y:=y*m]` has limitet replicability in N

(1) A ⊆ N

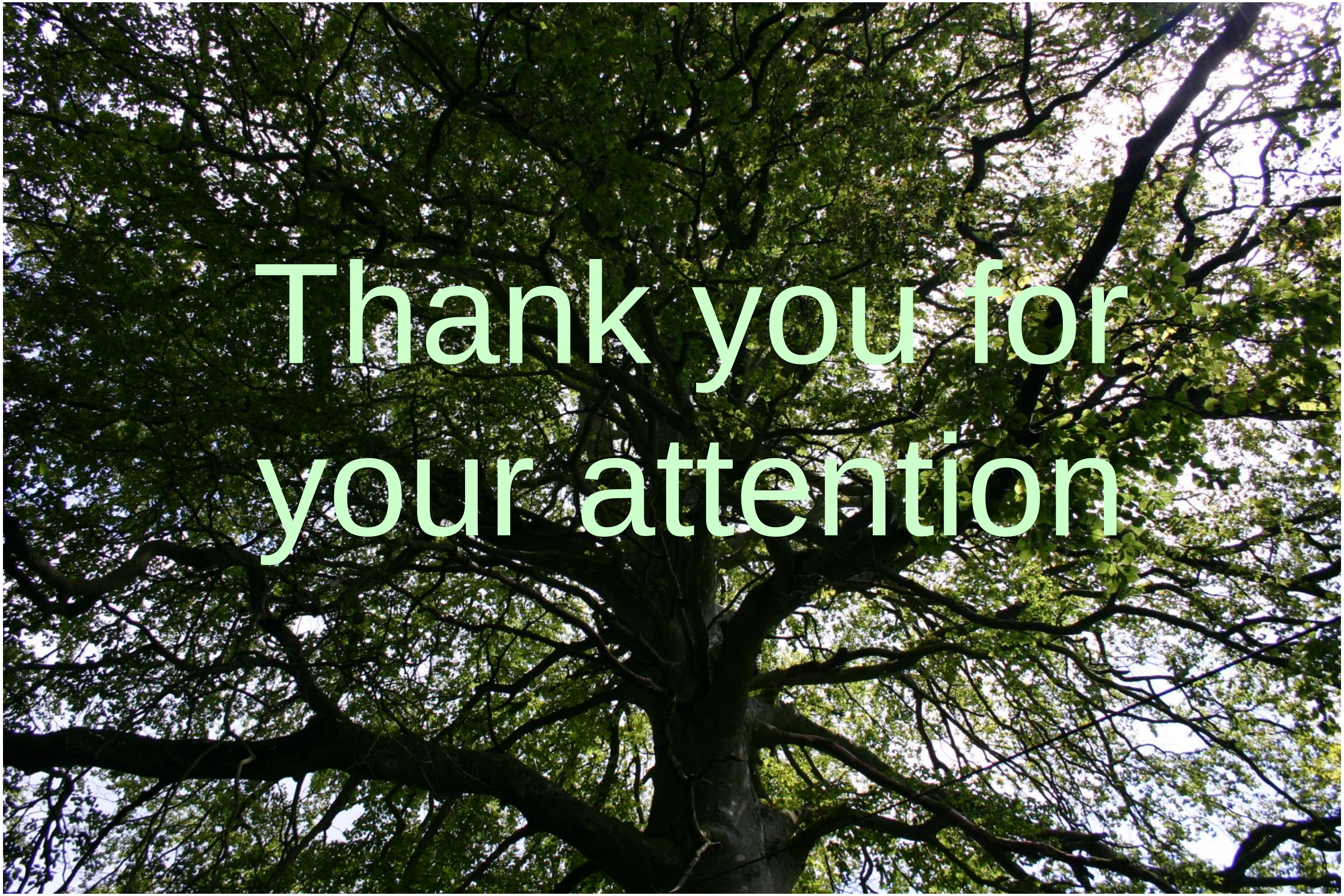
(2) N ⊆ C | ¬C

(3) N ∩ ¬C ⊆ B

(4) (N∩C) ⊆ FN (clean total correctness of F)

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

A ⊆ **while** (C,¬C) **do** F **od** B


Thank you for your attention