Semantyka i Weryfikacja Programów
Praca domowa # 3

MIMUW 2018/19

Michał Szafraniuk
219673

12 stycznia 2019

Rozwiązanie - dowód częściowej poprawności

Program, którego częściową poprawność mamy wykazać, liczy - dla zadanych a, d - przedstawienie a jako

$$a = dq + r$$

gdzie

$$q = \lfloor \frac{a}{d} \rfloor,\ r = a \bmod d$$

W programie są dwie pętle `while` więc potrzebujemy dwóch niezmienników (ψ_0, ψ_1 dla odpowiednio pętli zewnętrznej oraz wewnętrznej).

Przepiszmy kod programu z asercjami wedle wprowadzonych oznaczeń stosując podstawowe reguły logiki Hoare'a:

```
{ $a \geqslant 0 \land d > 0$ }
{ $\downarrow^{(1)}$ }
{ $\psi_0[q \mapsto 0][r \mapsto a]$ }
r := a;
q := 0;
while { $\psi_0$ } (r >= d) do (
    { $\psi_0 \land r \geqslant d$ }
    { $\downarrow^{(2)}$ }
    { $\psi_1[qq \mapsto 1][dd \mapsto d]$ }
    dd := d;
    qq := 1;
    while { $\psi_1$ } (r >= dd) do (
        { $\psi_1 \land r \geqslant dd$ }
        { $\downarrow^{(3)}$ }
        { $\psi_1[qq \mapsto qq + qq][q \mapsto q + qq][dd \mapsto dd + dd][r \mapsto r - dd]$ }
        r := r - dd;
        dd := dd + dd;
        q := q + qq;
        qq := qq + qq;
        { $\psi_1$ }
    )
```

{ $\psi_1 \wedge r < dd$ }
{ $\downarrow^{(4)}$ }
{ ψ_0 }
)
{ $\psi_0 \wedge r < d$ }
{ $\downarrow^{(5)}$ }
{ $dq + r = a \wedge 0 \leqslant r < d$ }

Aby dowieść częściowej poprawności potrzeba i wystracza:

1. podać niezmienniki ψ_0 oraz ψ_1
2. wykazać oznaczone strzałkami implikacje

„Zgadujemy” następujące niezmienniki pętli:

$$\begin{aligned}\psi_0 &\equiv (a = qd + r \wedge r \geqslant 0 \wedge d \geqslant 0 \wedge q \geqslant 0)\\ \psi_1 &\equiv (a = qd + r \wedge r \geqslant 0 \wedge dd = d \cdot qq \wedge dd \geqslant d \geqslant 0 \wedge q \geqslant 0)\end{aligned}$$

A następnie dowodzimy implikacje:

$\downarrow^{(1)}$ Następnik tej implikacji jest następujący:

$$\psi_0[q \mapsto 0][r \mapsto a] \equiv (a = 0 \cdot d + a \wedge a \geqslant 0 \wedge d \geqslant 0 \wedge 0 \geqslant 0)$$

Widać, że implikacja ewidentnie jest prawdziwa.

$\downarrow^{(2)}$ Poprzednik tej implikacji jest następujący

$$\psi_0 \wedge r \geqslant d \equiv (a = qd + r \wedge r \geqslant d \geqslant 0 \wedge q \geqslant 0)$$

Następnik tej implikacji jest następujący:

$$\psi_1[qq \mapsto 1][dd \mapsto d] \equiv (a = qd + r \wedge r \geqslant 0 \wedge d = d \cdot 1 \wedge d \geqslant d \geqslant 0 \wedge q \geqslant 0)$$

Widać, że implikacja jest ewidentnie prawdziwa.

$\downarrow^{(3)}$ Poprzednik tej implikacji jest następujący:

$$\psi_1 \wedge r \geqslant dd \equiv (a = qd + r \wedge dd = d \cdot qq \wedge r \geqslant dd \geqslant d \geqslant 0 \wedge q \geqslant 0)$$

Następnik tej implikacji jest następujący:

$$\psi_1[qq \mapsto qq + qq][q \mapsto q + qq][dd \mapsto dd + dd][r \mapsto r - dd] \equiv \\ (a = (q + qq)d + r - dd \wedge r \geqslant 0 \wedge dd = d \cdot qq \wedge dd + dd \geqslant d \geqslant 0 \wedge q + qq \geqslant 0)$$

Ponieważ $a = (q+qq)d + r - dd = qd + r + qq \cdot d - dd$ więc $(a = qd + r \wedge dd = d \cdot qq)$ implikuje $a = (q + qq)d + r - dd$. Pozostałe składniki następnika implikacji zachodzą w sposób oczywisty.

$\downarrow^{(4)}$ Poprzednik tej implikacji jest następujący:

$$\psi_1 \wedge r < dd \equiv (a = qd + r \wedge r \geqslant 0 \wedge dd = d \cdot qq \wedge dd \geqslant d \geqslant 0 \wedge q \geqslant 0 \wedge r < dd)$$

W sposób oczywisty implikuje on ψ_0

$\downarrow^{(5)}$ Implikacja jest ewidentnie prawdziwa.