VU Programm- und Systemverifikation
Solution: Hoare Logic

May 21, 2016

Solution for Task 1

$\{\mathsf{true}\}$
$\{(0 < n) \vee (0 = n) \vee (0 > n)\}$ ⑧
`r = -1;`
$\left\{ \begin{array}{c} ((r = -1) \wedge (0 < n \vee 0 > n)) \\ \vee \\ ((0 = n) \wedge (r = -1 \vee r = 0)) \end{array} \right\}$ ⑦
`i = 0;`
$\left\{ \begin{array}{c} \big((r = -1) \wedge (i^2 < n \vee i^2 > n)\big) \\ \vee \\ \big((i^2 = n) \wedge (r = -1 \vee r = i)\big) \end{array} \right\}$ ⑥
`while (i ≤ n ∧ r == -1) {`
$\left\{ ((i \leq n) \wedge (r = -1)) \wedge \left(\begin{array}{c} \big((r = -1) \wedge (i^2 < n \vee i^2 > n)\big) \\ \vee \\ \big((i^2 = n) \wedge (r = -1 \vee r = i)\big) \end{array} \right) \right\}$ ⑤
$\{(r = -1)\}$ ④
`  if (i*i == n)`
$\left\{ (i^2 = n) \wedge \left(\begin{array}{c} \big((i = -1) \wedge (i^2 < n \vee i^2 > n)\big) \\ \vee \\ \Big((i^2 = n) \wedge \Big(i = -1 \vee \underbrace{i = i}_{true}\Big)\Big) \end{array} \right) \right\}$ ③
`    r = i;`
`  else`
$\left\{ (i^2 \neq n) \wedge \left(\begin{array}{c} \big((r = -1) \wedge ((i+1)^2 < n \vee (i+1)^2 > n)\big) \\ \vee \\ \big(((i+1)^2 = n) \wedge (r = -1 \vee r = (i+1))\big) \end{array} \right) \right\}$ ②
`    i = i + 1;`
$\left\{ \begin{array}{c} \big((r = -1) \wedge (i^2 < n \vee i^2 > n)\big) \\ \vee \\ \big((i^2 = n) \wedge (r = -1 \vee r = i)\big) \end{array} \right\}$ ①
}
$\{(i = \sqrt{n}) \vee (r < 0)\}$

①	loop invariant

② assignment from ①;
we rewrite this to

$$\left\{ (i^2 \neq n) \wedge \left(\begin{array}{c} \big((r = -1) \wedge ((i+1)^2 < n \vee (i+1)^2 > n)\big) \\ \vee \\ \big(((i+1)^2 = n) \wedge (r = -1) \vee ((i+1)^2 = n) \wedge (r = (i+1))\big) \end{array} \right) \right\}$$

now factor out $(r = -1)$:

$$\left\{ (i^2 \neq n) \wedge \left(\begin{array}{c} (r = -1) \wedge \underbrace{\big((i+1)^2 < n \vee (i+1)^2 > n \vee (i+1)^2 = n\big)}_{true} \\ \vee \\ ((i+1)^2 = n) \wedge (r = (i+1)) \end{array} \right) \right\}$$

so we obtain

$$\left\{ (i^2 \neq n) \wedge \left(\begin{array}{c} (r = -1) \\ \vee \\ ((i+1)^2 = n) \wedge (r = (i+1)) \end{array} \right) \right\}$$

③ assignment from ①
simplifies to $(i^2 = n)$, since $(i^2 = n) \wedge (i^2 < n \vee i^2 > n)$ is false

---

④ Using the *rule of consequence*, we strengthen the terms from ② and ③ to $(i^2 \neq n) \wedge (r = -1)$ and $(i^2 = n) \wedge (r = -1)$, respectively.
Consequently $(r = -1)$ is the pre-condition of the conditional statement.

---

④ The loop invariant conjoined with the loop entrance condition.
This conjunction trivially implies ④.

---

⑤,⑥,⑦ With the assignment rule, we prove that the loop invariant holds on entrance.

Finally, we conjoin the loop invariant with the negated loop entrance condition

$$(i > n) \vee (r \vee -1)\,.$$

We perform a case split:

- If $(i \leq n)$, then $(r \neq -1)$, and therefore by the loop invariant $r = i = \sqrt{n}$.
- If $(r = -1)$ then the post-condition is trivially satisfied.