Aufgabe 2:

(*Methode „f()“*)

Stichwörter: wp-Kalkül

Gegeben sei folgendes Programm: wp-Kalkül

```
int f(int x, int y) {
  /* P */
  x = 2 * x + 1 + x * x;
  y += 7;
  if (x > 196) {
    y = 2 * y;
  } else {
    y -= 8;
    x *= 2;
  } /* Q */
  return x + y;
}
```

Bestimmen Sie die schwächste Vorbedingung (weakest precondition), für die die Nachbedingung $Q := (x \geq 8) \wedge (y\%2 = 1)$ noch zutrifft.

Lösungsvorschlag

Mit dem Distributivgesetz der Konjugation gilt:

$$\begin{aligned}&\text{wp}(\texttt{"A; if(b) B; else C;"}, Q) \equiv\\ &\text{wp}(\texttt{"A;"}, b) \wedge \text{wp}(\texttt{"A;B;"}, Q)\\ &\vee\\ &\text{wp}(\texttt{"A;"}, \neg b) \wedge \text{wp}(\texttt{"A;C;"}, Q)\end{aligned}$$

Der tatsächliche Programmcode wird eingesetzt:

$$\begin{aligned}&\text{wp}(\texttt{"x=2*x+1+x*x;y+=7;if(x>196){y=2*y;}else{y-=8;x*=2;}"}, (x \geq 8) \wedge (y\%2 = 1)) \equiv\\ &\text{wp}(\texttt{"x=2*x+1+x*x;y+=7;"}, x > 196) \wedge\\ &\text{wp}(\texttt{"x=2*x+1+x*x;y+=7;y=2*y;"}, (x \geq 8) \wedge (y\%2 = 1))\\ &\vee\\ &\text{wp}(\texttt{"x=2*x+1+x*x;y+=7;"}, x \leq 196) \wedge\\ &\text{wp}(\texttt{"x=2*x+1+x*x;y+=7;y-=8;x*=2;"}, (x \geq 8) \wedge (y\%2 = 1))\\ &=: \text{P}\end{aligned}$$

Nebenrechnung: wp$(\texttt{"A;"}, b)$

bWpPseudoMatheUmgebung $\text{wp}(\texttt{"x=2*x+1+x*x;y+=7;"}, x > 196)$

Wir lassen $y+ = 7$ weg, weil in der Nachbedingung kein y vorkommt und setzen in den Term $x > 196$ für das x die erste Code-Zeile $2 \cdot x + 1 + x \cdot x$ ein.

$$\equiv \quad \text{wp}(\texttt{""}, 2 \cdot x + 1 + x \cdot x > 196)$$

Nach der Transmformationsregel *Nichts passiert, die Vorbedingung bleibt gleich* kann das auch so geschrieben werden:

$$\equiv \quad 2 \cdot x + 1 + x \cdot x > 196$$

Die erste binomische Formel (Plus-Formel) lautet $(a+b)^2 = a^2 + 2ab + b^2$. Man kann die Formel auch umgedreht verwenden: $a^2 + 2ab + b^2 = (a+b)^2$. Die erste Code-Zeile $2 \cdot x + 1 + x \cdot x$ kann umformuliert werden in $1 + 2 \cdot 1 \cdot x + x \cdot x = 1^2 + 2 \cdot 1 \cdot x + x^2 = (1+x)^2 = (x+1)^2$. Wir haben für a die Zahl 1 und für b den Buchstaben x eingesetzt.

$$\equiv \quad (x+1)^2 > 196$$

Nebenrechnung: wp(`"A;B;"`, Q)

bWpPseudoMatheUmgebung wp(`"x=2*x+1+x*x;y+=7;y=2*y;"`, $(x \geq 8) \land (y\%2 = 1)$)

Für das x in der Nachbedingung setzen wir die erste Code-Zeile $2 \cdot x + 1 + x \cdot x$ ein. Für das y in der Nachbedingung setzen wir dritte Code-Zeile `y=2*y;` ein und dann die zweite Code-Zeile `y+=7;`. Das wp-Kalkül arbeitet den Code rückswärts ab. in $y\%2$ die dritte Anweisung $y = 2 \cdot y$ einfügen: $2 \cdot y\%2$ dann in $2 \cdot y\%2$ die zweite Anweisung $y = y + 7$ einfügen: $2 \cdot (y+7)\%2$

$$\equiv \quad (x+1)^2 \geq 8 \land 2(y+7)\%2 = 1$$

Diese Aussage ist falsch, da $2(y+7)$ immer eine gerade Zahl ergibt und der Rest von einer Division durch zwei einer geraden Zahl immer 0 ist und nicht 1.

$$\equiv \quad (x+1)^2 \geq 8 \land \text{falsch}$$

$$\equiv \quad \text{falsch}$$

Nebenrechnung: wp(`"A;"`, $\neg b$)

bWpPseudoMatheUmgebung wp(`"x=2*x+1+x*x;y+=7;"`, $x \leq 196$)

Analog zu Nebenrechnung 1

$$\equiv \quad (x+1)^2 \leq 196$$

Nebenrechnung: wp(`"A;C;"`, Q)

bWpPseudoMatheUmgebung wp(`"x=2*x+1+x*x;y+=7;y-=8;x*=2;"`, $(x \geq 8) \land (y\%2 = 1)$)

„`x*=2;`“: $x \cdot 2$ für x einsetzen:

$$\equiv \quad \text{wp}(\texttt{"x=2*x+1+x*x;y+=7;y-=8;"}, (2 \cdot x \geq 8) \land (y\%2 = 1))$$

„`y-=8;`“: $y - 8$ für y einsetzen:

$$\equiv \quad \text{wp}(\texttt{"x=2*x+1+x*x;y+=7;"}, (2 \cdot x \geq 8) \land ((y-8)\%2 = 1))$$

„`y+=7`“: $y + 7$ für y einsetzen:

$$\equiv \quad \text{wp}(\texttt{"x=2*x+1+x*x;"}, (2 \cdot x \geq 8) \land (((y+7)-8)\%2 = 1))$$

„`x=2*x+1+x*x;`“: $(x+1)^2$ für x einsetzen:

$$\equiv \quad \text{wp}(\texttt{""}, (2 \cdot (x+1)^2 \geq 8) \land (((y+7)-8)\%2 = 1))$$

Nur noch die Nachbedingung stehen lassen:

$$\equiv \quad (2 \cdot (x+1)^2 \geq 8) \land (((y+7)-8)\%2 = 1)$$

Subtraktion:

$$\equiv \quad (2 \cdot (x+1)^2 \geq 8) \wedge ((y-1)\%2 = 1)$$

Vereinfachen (links beide Seiten durch 2 teilen und rechts von beiden Seiten 1 abziehen)

$$\equiv \quad (\tfrac{2\cdot(x+1)^2}{2} \geq \tfrac{8}{2}) \wedge (((y-1)\%2) - 1 = 1 - 1)$$

Zwischenergebnis:

$$\equiv \quad ((x+1)^2 \geq 4) \wedge y\%2 = 0$$

Zusammenführung

Die Zwischenergebnisse aus den Nebenrechnungen zusammenfügen:

$$\equiv \quad [(x+1)^2 > 196 \wedge \text{falsch}] \vee [(x+1)^2 \leq 196 \wedge (x+1)^2 \geq 4 \wedge y\%2 = 0]$$

„falsch“ und eine Aussage verbunden mit logischem Und „$\wedge$“ ist insgesamt falsch:

$$\equiv \quad \text{falsch} \vee [(x+1)^2 \leq 196 \wedge (x+1)^2 \geq 4 \wedge y\%2 = 0]$$

falsch verbunden mit oder weglassen:

$$\equiv \quad (x+1)^2 \leq 196 \wedge (x+1)^2 \geq 4 \wedge y\%2 = 0$$

Umgruppieren, sodass nur noch ein $(x+1)^2$ geschrieben werden muss:

$$\equiv \quad 4 \leq (x+1)^2 \leq 196 \wedge y\%2 = 0$$

$4 = 2^2$ und $196 = 14^2$

$$\equiv \quad 2^2 \leq (x+1)^2 \leq 14^2 \wedge y\%2 = 0$$

Hoch zwei weg lassen: Betragsklammer $|x|$ oder auch Betragsfunktion hinzufügen (Die Betragsfunktion ist festgelegt als „Abstand einer Zahl von der Zahl Null“.

$$\equiv \quad 2 \leq |x+1| \leq 14 \wedge y\%2 = 0$$

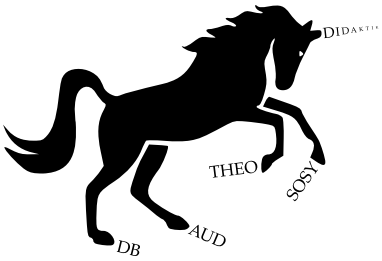
Auf die Gleichung der linken Aussage -1 anwenden:

$$\equiv \quad 1 \leq |x| \leq 13 \wedge y\%2 = 0$$

Die Betragsklammer weg lassen:

$$\equiv \quad (1 \leq x \leq 13 \vee -13 \leq x \leq -1) \wedge y\%2 = 0$$

bWpPseudoMatheUmgebung=: P



Die Bschlangaul-Sammlung
Hermine Bschlangaul and Friends

Eine freie Aufgabensammlung mit Lösungen von Studierenden für Studierende zur Vorbereitung auf die 1. Staatsexamensprüfungen des Lehramts Informatik in Bayern.

Hilf mit! Die Hermine schafft das nicht allein! Das ist ein Community-Projekt! Verbesserungsvorschläge, Fehlerkorrekturen, weitere Lösungen sind herzlich willkommen - egal wie - per Pull-Request oder per E-Mail an hermine.bschlangaul@gmx.net.Der TEX-Quelltext dieses Dokuments kann unter folgender URL aufgerufen werden: `https://github.com/bschlangaul-sammlung/examens-aufgaben/blob/main/Module/40_SOSY/05_Testen/10_Formale-Verifikation/Aufgabe_Methode-f.tex`