

Aufgabe 3: wp-Kalkül und Schleifeninvariante

Gegeben Sei folgendes Programm:

```
1 long doubleFac (long n) {
2     /* P */ long df = 1;
3     for (long x = n; x > 1; x -= 2) {
4         df *= x;
5     } /* Q */
6     return df;
7 }
```

sowie die Vorbedingung $P \equiv n \geq 0$ und Nachbedingung $Q \equiv (df = n!!)$ wobei gilt

$$n!! := \begin{cases} 2^k \cdot k! & n \text{ gerade, } k := \frac{n}{2} \\ \frac{(2k)!}{2^k \cdot k!} & n \text{ ungerade, } k := \frac{n+1}{2} \end{cases}$$

Exkurs: Fakultät

Die Fakultät ist eine Funktion, die einer natürlichen Zahl das Produkt aller natürlichen Zahlen (ohne Null) kleiner und gleich dieser Zahl zuordnet. Für alle natürlichen Zahlen n ist

$$n! = 1 \cdot 2 \cdot 3 \cdot \dots \cdot n = \prod_{k=1}^n k$$

Exkurs: Doppelfakultät

Die seltener verwendete „Doppelfakultät“ oder „doppelte Fakultät“ ist für gerade n das Produkt aller geraden Zahlen kleiner gleich n . Für ungerade n ist es das Produkt aller ungeraden Zahlen kleiner gleich n . Sie ist definiert als:

$$n!! = \begin{cases} n \cdot (n-2) \cdot (n-4) \cdot \dots \cdot 2 & \text{für } n \text{ gerade und } n > 0, \\ n \cdot (n-2) \cdot (n-4) \cdot \dots \cdot 1 & \text{für } n \text{ ungerade und } n > 0, \\ 1 & \text{für } n \in \{-1, 0\} \end{cases}$$

Häufig werden anstelle der Doppelfakultät Ausdrücke mit der gewöhnlichen Fakultät verwendet. Es gilt $(2k)!! = 2^k k!$ und $(2k-1)!! = \frac{(2k)!}{2^k k!}$

Zur Vereinfachung nehmen Sie im Folgenden an, dass die verwendeten Datentypen unbeschränkt sind und daher keine Überläufe auftreten können.

- (a) Welche der folgenden Bedingungen ist eine zum Beweisen der Korrektheit der Methode mittels wp-Kalkül (Floyd-Hoare-Kalkül) sinnvolle Schleifeninvariante?

- (i) $df = n!! - x!! \wedge x \geq 1$
- (ii) $df = (n - x)!! \wedge x \geq 1$
- (iii) $df \cdot x!! = n!! \wedge x \geq 0$
- (iv) $(df + x)!! = n!! \wedge x \geq 0$

Zunächst wird der Code in einen äquivalenten Code mit while-Schleife umgewandelt:

```

1 long doubleFac (long n) {
2     /* P */ long df = 1;
3     long x = n ;
4     while (x > 1) {
5         df = df * x;
6         x = x - 2;
7     } /* Q */
8     return df;
9 }

```

$$(i) \text{ df} = n!! - x!! \wedge x \geq 1$$

$$(ii) \text{ df} = (n - x)!! \wedge x \geq 1$$

Die ersten beiden Bedingungen sind unmöglich, da z. B. für $n = 2$ nach der Schleife $x = 0$ gilt und daher $x \geq 1$ verletzt wäre.

$$(iii) \text{ df} \cdot x!! = n!! \wedge x \geq 0$$

Nach dem Ausschlussprinzip ist es daher die dritte Bedingung:
 $I \equiv (\text{df} + x)!! = n!! \wedge x \geq 0$.

$$(iv) (\text{df} + x)!! = n!! \wedge x \geq 0$$

Die letzte kann es auch nicht sein, da vor der Schleife $\text{df} = 1$ und $x = n$ gilt, d.h. $(\text{df} + x)!! = (1 + n)!!$. Jedoch ist offenbar $(1 + n)!! \neq n!!$.

\Rightarrow Die Schleifeninvariante lautet: $\text{df} \cdot x!! = n!! \wedge x \geq 0$

- (b) Zeigen Sie formal mittels wp-Kalkül, dass die von Ihnen gewählte Bedingung unmittelbar vor Beginn der Schleife gilt, wenn zu Beginn der Methode die Anfangsbedingung P gilt.

Zu zeigen $P \Rightarrow \text{wp}(\text{"Code vor der Schleife"}, I)$

$$\begin{aligned}
 \text{wp}(\text{"Code vor der Schleife"}, I) &\equiv \text{wp}(\text{"df} = 1; x = n;", (\text{df} \cdot x)!! = n!! \wedge x \geq 0) \\
 &\equiv \text{wp}(\text{"df} = 1;", (\text{df} \cdot n)!! = n!! \wedge n \geq 0) \\
 &\equiv \text{wp}("", (1 \cdot n)!! = n!! \wedge n \geq 0) \\
 &\equiv n!! = n!! \wedge n \geq 0 \\
 &\equiv n \geq 0 \\
 &\equiv P
 \end{aligned}$$

Insbesondere folgt damit die Behauptung.

- (c) Zeigen Sie formal mittels wp-Kalkül, dass die von Ihnen gewählte Bedingung tatsächlich eine Invariante der Schleife ist.

zu zeigen: $I \wedge \text{Schleifenbedingung} \Rightarrow \text{wp}(\text{"Code in der Schleife"}, I)$

Bevor wir dies beweisen, zeigen wir erst $x \cdot (x - 2)!! = x!!$.

- Fall x ist gerade ($n!! = 2^k \cdot k!$ für $k := \frac{n}{2}$):

$$x \cdot (x - 2)!! = x \cdot 2^{\frac{x-2}{2}} \cdot (\frac{x-2}{2})! = x \cdot \frac{1}{2} \cdot 2^{\frac{x}{2}} \cdot (\frac{x}{2} - 1)! = 2^{\frac{x}{2}} \cdot (\frac{x}{2})! = x!!$$

Nebenrechnung (Division mit gleicher Basis: $x^{a-b} = \frac{x^a}{x^b}$):

$$2^{\frac{x-2}{2}} = 2^{(\frac{x}{2} - \frac{2}{2})} = \frac{2^{\frac{x}{2}}}{2^{\frac{2}{2}}} = \frac{2^{\frac{x}{2}}}{2^1} = \frac{2^{\frac{x}{2}}}{2} = \frac{1}{2} \cdot 2^{\frac{x}{2}}$$

Nebenrechnung ($n! = (n - 1)! \cdot n$):

$$x \cdot \frac{1}{2} \cdot (\frac{x}{2} - 1)! = \frac{x}{2} \cdot (\frac{x}{2} - 1)! = \frac{x}{2}!$$

- Fall x ist ungerade:

Dies benutzen wir nun, um den eigentlichen Beweis zu führen:

$$\begin{aligned} \text{wp}(\text{"Code vor der Schleife"}, I) &\equiv \text{wp}(\text{"df = df * x; x = x - 2;"}, (\text{df} \cdot x)!! = n!! \wedge x \geq 0) \\ &\equiv \text{wp}(\text{"df = df * x;"}, (\text{df} \cdot (x - 2))!! = n!! \wedge x - 2 \geq 0) \\ &\equiv \text{wp}(\text{"", } (\text{df} \cdot x \cdot (x - 2))!! = n!! \wedge x - 2 \geq 0) \\ &\equiv (\text{df} \cdot x)!! = n!! \wedge x \geq 2 \\ &\equiv (\text{df} \cdot x)!! = n!! \wedge x > 1 \\ &\equiv I \wedge x > 1 \\ &\equiv I \wedge \text{Schleifenbedingung} \end{aligned}$$

- (d) Zeigen Sie formal mittels wp-Kalkül, dass am Ende der Methode die Nachbedingung Q erfüllt wird.

z.z. $I \wedge \neg \text{Schleifenbedingung} \Rightarrow \text{wp}(\text{"Code nach der Schleife"}, Q)$

Wir vereinfachen den Ausdruck $I \wedge \neg \text{Schleifenbedingung}$:

$$\begin{aligned} I \wedge \neg \text{Schleifenbedingung} &\equiv I \wedge (x \leq 1) \equiv I \wedge ((x = 0) \vee (x = 1)) \equiv \\ & (I \wedge (x = 0)) \vee (I \wedge (x = 1)) \equiv (\text{df} \cdot 1 = n!!) \vee (\text{df} \cdot 1 = n!!) \equiv \text{df} = n!! \end{aligned}$$

Damit gilt:

$$\text{wp}(\text{"Code nach der Schleife"}, Q) \equiv \text{wp}(\text{"", } \text{df} = n!!) \equiv \text{df} = n!! \equiv I \wedge \neg \text{Schleifenbedingung}$$

- (e) Beweisen Sie, dass die Methode immer terminiert. Geben Sie dazu eine Terminierungsfunktion an und begründen Sie kurz ihre Wahl.

Sei $T(x) := x$. T ist offenbar ganzzahlig. Da x in jedem Schleifendurchlauf um 2 verringert wird, ist T streng monoton fallend. Aus der Schleifeninvariante folgt $x \geq 0$ und daher ist x auch nach unten beschränkt. Damit folgt $I \Rightarrow T \geq 0$ und T ist eine gültige Terminie-

rungsfunktion.