Script generated by TTT

Title: Seidl: Info2 (24.11.2017)

Date: Fri Nov 24 16:16:08 CET 2017

Duration: 116:30 min

Pages: 182

Zentralübung: Schleifeninvarianten

zur VL. Funktionale Programmierung und Verifikation (EIDI2)

M.Sc. Nico Hartmann

24. November 2017

Inhalt

Inhalt

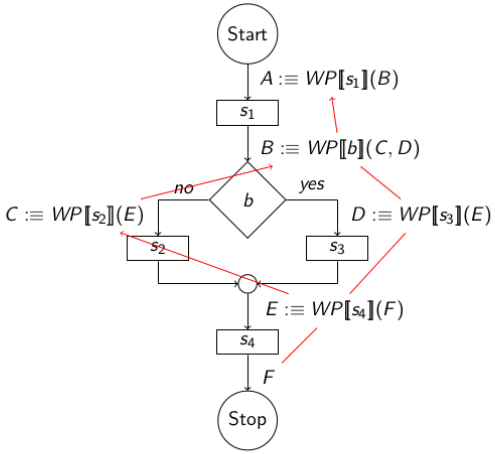
Vorausgesetzt (und nicht im Detail besprochen) werden folgende Kenntnisse:

- MiniJava Anweisungen und deren konkrete Semantik
- Bedeutung der schwächsten Vorbedingungen (WPs)
- Verifikationsverfahren mittels WP-Kalkül
- Terminierungsbeweise mittels WP-Kalkül
- Definitionen der WP-Operatoren ($WP[\![.]\!]$)
- Aussagenlogik (insb. Umformungsregeln, Implikation)

Warum Schleifeninvarianten?

Warum Schleifeninvarianten?

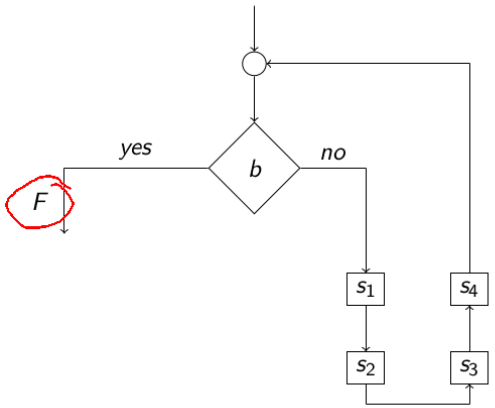
Wie können wir die schwächsten Vorbedingungen für F finden?



- Direkt rückwärts durch den Kontrollfluss berechnen

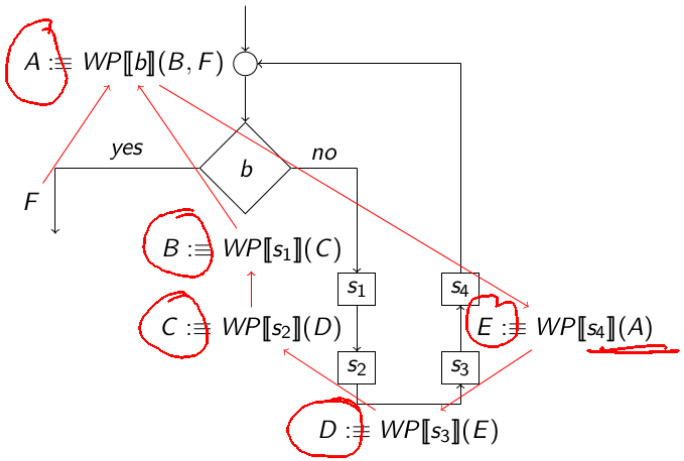
Warum Schleifeninvarianten?

Wie können wir die schwächsten Vorbedingungen für F finden?



Warum Schleifeninvarianten?

Wie können wir die schwächsten Vorbedingungen für F finden?



- WPs hängen zyklisch voneinander ab

Warum Schleifeninvarianten?

In der Schleife hängen alle WPs voneinander ab

- Keine lässt sich ohne die andere berechnen

Warum Schleifeninvarianten?

An welcher Stelle geben wir eine Zusicherung vor?

- Jeder Programmpunkt in der Schleife ist möglich

Warum Schleifeninvarianten?

An welcher Stelle geben wir eine Zusicherung vor?

- Jeder Programmpunkt in der Schleife ist möglich

Wir entscheiden uns für den "Join"-Punkt der Schleife

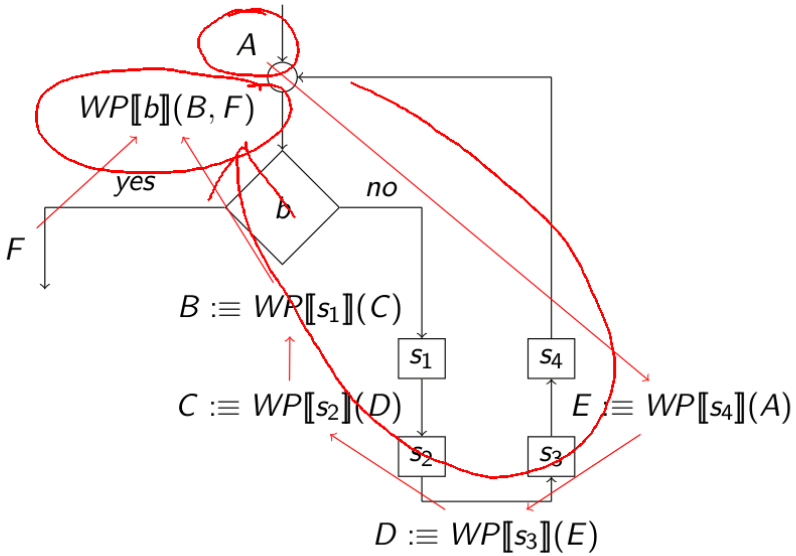
- Ist ein markanter Punkt jeder Schleife
- Wird vor und nach jedem Schleifendurchlauf erreicht
- Zusicherungen sind etwas einfacher zu bestimmen
- Wir können unsere Lösungen besser vergleichen

Warum Schleifeninvarianten?

Wie können wir zeigen, dass unsere Vorgabe richtig war?

- Was bedeutet "richtig" hier überhaupt?

Warum Schleifeninvarianten?

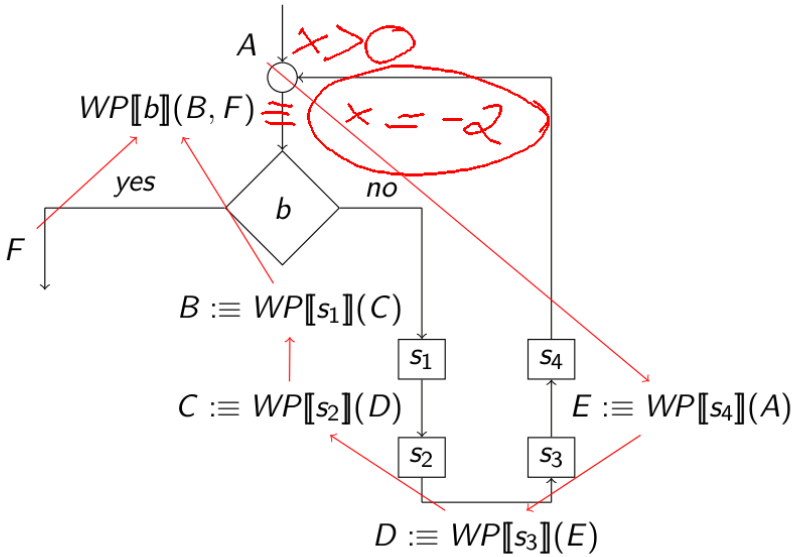


Warum Schleifeninvarianten?

$WP⟦b⟧(B, F)$ ist die schwächste Vorbedingung von A, also genau das was mindestens gelten muss, damit A gilt

- Die Frage ist also: Erfüllt A seine eigene Mindestvoraussetzung?
- A muss also so stark sein wie $WP⟦b⟧(B, F)$ oder stärker

Warum Schleifeninvarianten?



Warum Schleifeninvarianten?

$WP⟦b⟧(B, F)$ ist die schwächste Vorbedingung von A, also genau das was mindestens gelten muss, damit A gilt

- Die Frage ist also: Erfüllt A seine eigene Mindestvoraussetzung?
- A muss also so stark sein wie $WP⟦b⟧(B, F)$ oder stärker

Warum Schleifeninvarianten?

$WP[\![b]\!](B, F)$ ist die schwächste Vorbedingung von A, also genau das was mindestens gelten muss, damit A gilt

- Die Frage ist also: Erfüllt A seine eigene Mindestvoraussetzung?
- A muss also so stark sein wie $WP[\![b]\!](B, F)$ oder stärker

Es muss $A \implies WP[\![b]\!](B, F)$ gelten

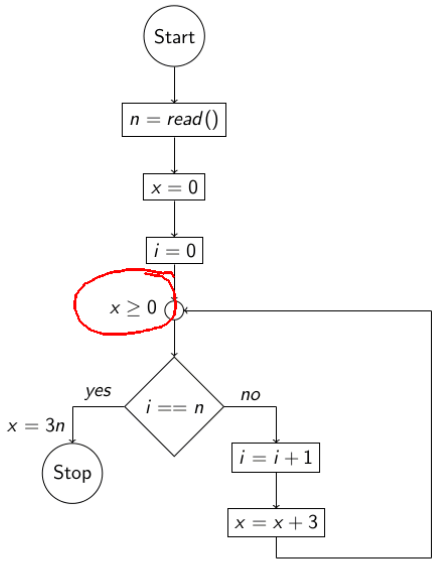
- Das nennen wir dann lokal konsistent

Invarianten wählen

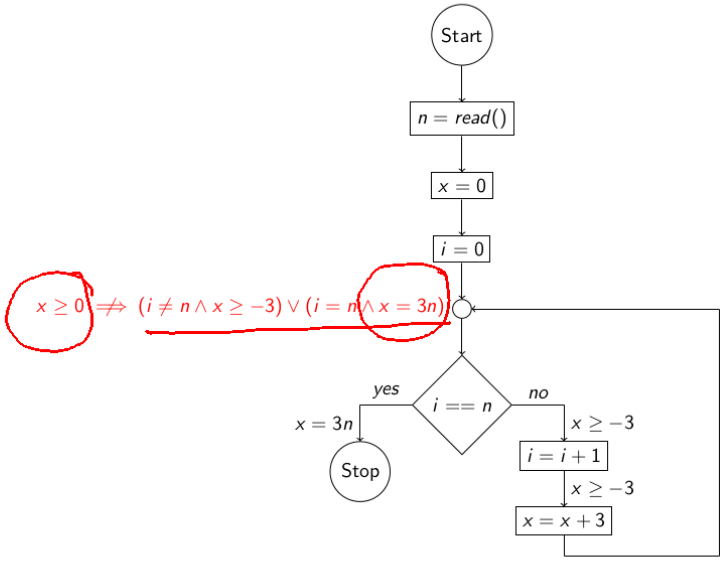
Invarianten wählen

Was ist, wenn wir die Schleifeninvariante zu schwach wählen?

Invarianten wählen



Invarianten wählen



Invarianten wählen

Was ist, wenn wir die Schleifeninvariante zu schwach wählen?

- Es lässt sich keine lokale Konsistenz zeigen
- Aussage lässt sich nicht beweisen

Invarianten wählen

Was ist, wenn wir die Schleifeninvariante zu schwach wählen?

- Es lässt sich keine lokale Konsistenz zeigen
- Aussage lässt sich nicht beweisen

Invarianten wählen

Was ist, wenn wir die Schleifeninvariante zu schwach wählen?

- es lässt sich keine lokale Konsistenz zeigen
- Aussage lässt sich nicht beweisen

Was ist, wenn wir die Schleifeninvariante zu stark wählen?

- Aussage lässt sich nur noch für einen Teil der Programmausführungen/Eingaben beweisen
- Formeln werden größer, Rechnungen u.U. aufwändiger

Invarianten wählen

Was ist, wenn wir die Schleifeninvariante zu schwach wählen?

- es lässt sich keine lokale Konsistenz zeigen
- Aussage lässt sich nicht beweisen

Was ist, wenn wir die Schleifeninvariante zu stark wählen?

- Aussage lässt sich nur noch für einen Teil der Programmausführungen/Eingaben beweisen
- Formeln werden größer, Rechnungen u.U. aufwändiger

Invarianten wählen

Was ist, wenn wir die Schleifeninvariante zu schwach wählen?

- es lässt sich keine lokale Konsistenz zeigen
- Aussage lässt sich nicht beweisen

Was ist, wenn wir die Schleifeninvariante zu stark wählen?

- Aussage lässt sich nur noch für einen Teil der Programmausführungen/Eingaben beweisen
- Formeln werden größer, Rechnungen u.U. aufwändiger

Invarianten wählen

Wie findet man nun eine geeignete Invariante?

- **NICHT** durch Raten!
- Indem man die Schleife/das Programm versteht

Invarianten wählen

Wie findet man nun eine geeignete Invariante?

- **NICHT** durch Raten!
- Indem man die Schleife/das Programm versteht

Solange wir nur gültige Aussagen verwenden, können wir wenig falsch machen

- Mit einer stärkeren Invariante wird der Beweis immer funktionieren
- Mit einer schwächeren Invariante wird der Beweis zwar scheitern, uns aber einen guten Hinweis darauf geben, was uns in der Invariante fehlt

Invarianten wählen

Das eröffnet zwei Herangehensweisen

1. Alle gültigen Zusicherungen verwenden
   - Beweis klappt garantiert (wenn sich die Aussage beweisen lässt)
   - Beweis wird länger und komplizierter
   - Es kann mitunter sehr schwierig sein alle geltenden Zusammenhänge zu finden

Invarianten wählen

Das eröffnet zwei Herangehensweisen

1. Alle gültigen Zusicherungen verwenden
   - Beweis klappt garantiert (wenn sich die Aussage beweisen lässt)
   - Beweis wird länger und komplizierter
   - Es kann mitunter sehr schwierig sein alle geltenden Zusammenhänge zu finden
2. Mit einer schwächeren Zusicherung starten und bei Bedarf verstärken
   - Beweis ist kürzer und einfacher
   - Rechnungen müssen u.U (mehrfach) wiederholt werden

Invarianten wählen

Die beste Herangehensweise ist ein Mittelweg:

- Mit Aussagen starten, bei denen man bereits vorher vermutet, dass man diese benötigen wird (natürlich nur gültige)
- Wenn der Beweis scheitert, um die nötigen Aussagen verstärken und wiederholen bis er gelingt

Invarianten wählen

Die beste Herangehensweise ist ein Mittelweg:

- Mit Aussagen starten, bei denen man bereits vorher vermutet, dass man diese benötigen wird (natürlich nur gültige)
- Wenn der Beweis scheitert, um die nötigen Aussagen verstärken und wiederholen bis er gelingt

Was hilft um eine (möglichst) ideale Startaussage zu finden?

- Gutes Verständnis von (imperativen) Programmen
- Übung und Erfahrung
- Die folgenden Tipps

Die Besten Invarianten Finden - 10 Tipps

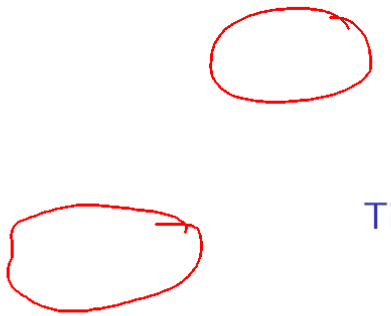
Die Besten Invarianten Finden - Definitionen

Im Folgenden verwenden wir diese Variablen:

- x - Ergebnisvariable, über die wir etwas Beweisen wollen
- y - Für zusätzliche Berechnungen
- i - Schleifenzähler
- n, m - Programmeingaben, die mit $read()$ eingelesen werden
- k - Zusäztliche Hilfsvariable
- I - Schleifeninvariante

Wir gehen außerdem davon aus, dass alle Variablen entsprechend des Beispiels initialisiert sind, ohne dass wir dies explizit angeben. In der Regel sind x, y, i dabei 0.

Tipp 0



Tipp 1

Die Besten Invarianten finden - Tipp 1

$$WP[\![x = x + 2]\!](i \geq 0) \equiv i \geq 0$$

$$WP[\![i = i + 1]\!](i \geq 0) \equiv i + 1 \geq 0$$
$$\equiv i \geq -1$$

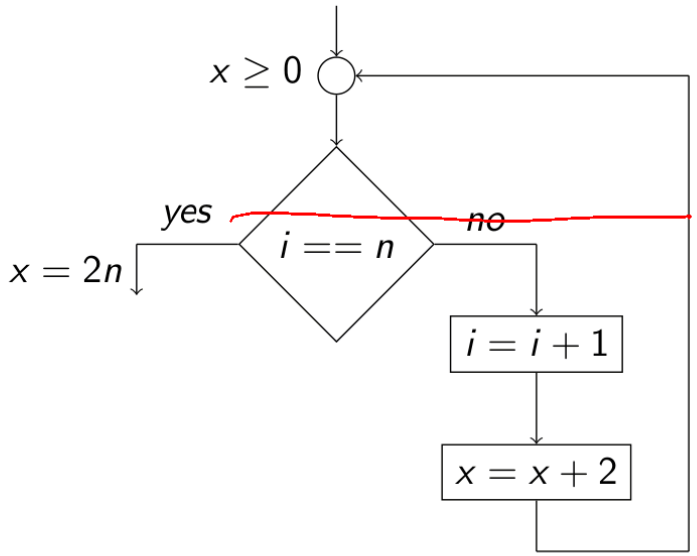
Die Besten Invarianten finden - Tipp 1

$$i \geq 0 \Rightarrow (i \neq n \wedge i \geq -1) \vee (i = n \wedge x = 2n)$$

Warum können wir das nicht zeigen?

- Wir wissen nichts über x
- Also muss eine Aussage über x in die Invariante

Die Besten Invarianten finden - Tipp 1



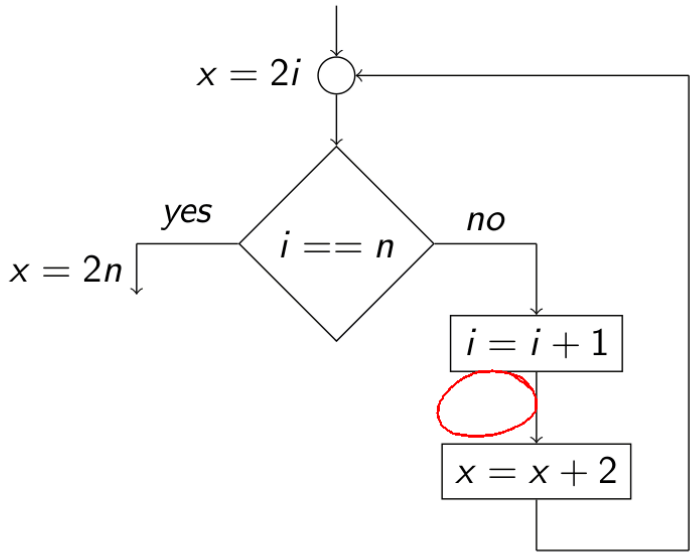
Die Besten Invarianten finden - Tipp 1

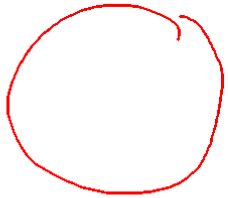
$$x \geq 0 \Rightarrow (i \neq n \wedge x \geq -2) \vee (i = n \wedge x = 2n)$$

Warum können wir das nicht zeigen?

- Weil unsere Informationen über x in der Schleife zu unpräzise sind
- Wir benötigen eine genauere Aussage über den Wert von x innerhalb der Schleife

Die Besten Invarianten finden - Tipp 1





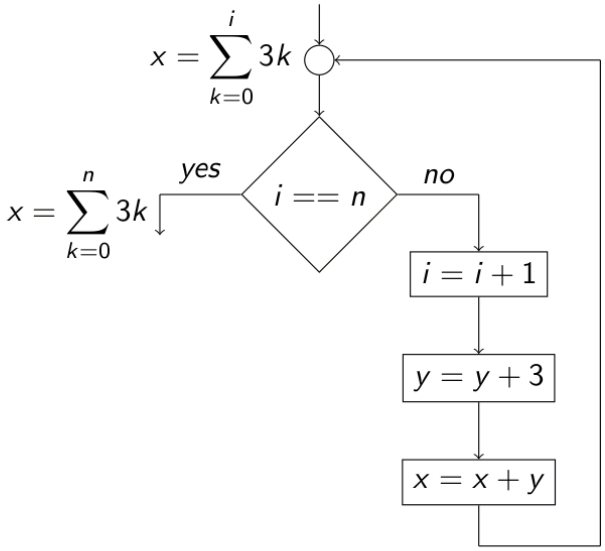
Tipp 2

Die Besten Invarianten finden - Tipp 1

Tipp 1

Wir benötigen eine Aussage über den Wert der Variablen, über die wir etwas beweisen wollen (x) in der Schleifeninvariante. Die Aussage muss dabei mindestens so präzise ($\neq, \geq, \leq, =$) sein, wie die Aussage, die wir beweisen wollen.

Die Besten Invarianten finden - Tipp 2



Die Besten Invarianten finden - Tipp 2

$$WP[\![x = x + y]\!](x = \sum_{k=0}^{i} 3k) \equiv x + y = \sum_{k=0}^{i} 3k$$

$$\equiv x = \sum_{k=0}^{i} 3k - y$$

Die Besten Invarianten finden - Tipp 2

$$WP[\![x = x + y]\!](x = \sum_{k=0}^{i} 3k) \equiv x + y = \sum_{k=0}^{i} 3k$$

$$\equiv x = \sum_{k=0}^{i} 3k - y$$

$$WP[\![y = y + 3]\!](x = \sum_{k=0}^{i} 3k - y) \equiv x = \sum_{k=0}^{i} 3k - y - 3$$

Die Besten Invarianten finden - Tipp 2

$$WP[\![x = x + y]\!](x = \sum_{k=0}^{i} 3k) \equiv x + y = \sum_{k=0}^{i} 3k$$

$$\equiv x = \sum_{k=0}^{i} 3k - y$$

$$WP[\![y = y + 3]\!](x = \sum_{k=0}^{i} 3k - y) \equiv x = \sum_{k=0}^{i} 3k - y - 3$$

$$WP[\![i = i + 1]\!](x = \sum_{k=0}^{i} 3k - y - 3) \equiv x = \sum_{k=0}^{i+1} 3k - y - 3$$

Die Besten Invarianten finden - Tipp 2

$$x = \sum_{k=0}^{i} 3k \stackrel{?}{\Longrightarrow} x = \sum_{k=0}^{i+1} 3k - y - 3$$

Die Besten Invarianten finden - Tipp 2

$$x = \sum_{k=0}^{i} 3k \not\Longrightarrow x = \sum_{k=0}^{i+1} 3k - y - 3$$

Warum können wir das nicht zeigen?

- Wir wissen nichts über y
- Also muss eine Aussage über y in die Invariante

Die Besten Invarianten finden - Tipp 2

$$\begin{aligned} WP[\![x = x + y]\!](x = \sum_{k=0}^{i} 3k \wedge y = 3i) &\equiv x + y = \sum_{k=0}^{i} 3k \\ &\equiv x = \sum_{k=0}^{i} 3k - y \wedge y = 3i \\ &\equiv x = \sum_{k=0}^{i} 3k - 3i \wedge y = 3i \\ &\equiv x = \sum_{k=0}^{i-1} 3k \wedge y = 3i \end{aligned}$$

Die Besten Invarianten finden - Tipp 2

$$\begin{aligned} WP[\![y = y + 3]\!](x = \sum_{k=0}^{i-1} 3k \wedge y = 3i) &\equiv x = \sum_{k=0}^{i-1} 3k \wedge y + 3 = 3i \\ &\equiv x = \sum_{k=0}^{i-1} 3k \wedge y = 3i - 3 \\ &\equiv x = \sum_{k=0}^{i-1} 3k \wedge y = 3(i-1) \end{aligned}$$

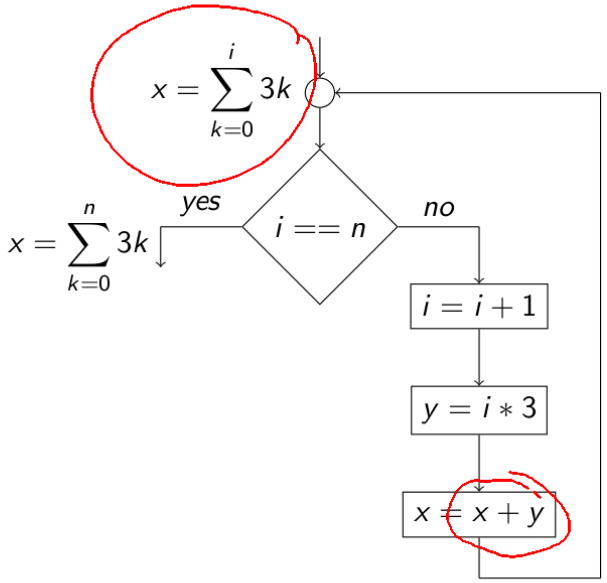
Die Besten Invarianten finden - Tipp 2

$$\begin{aligned} WP[\![y = y + 3]\!](x = \sum_{k=0}^{i-1} 3k \wedge y = 3i) &\equiv x = \sum_{k=0}^{i-1} 3k \wedge y + 3 = 3i \\ &\equiv x = \sum_{k=0}^{i-1} 3k \wedge y = 3i - 3 \\ &\equiv x = \sum_{k=0}^{i-1} 3k \wedge y = 3(i-1) \end{aligned}$$

$$WP[\![i = i + 1]\!](x = \sum_{k=0}^{i-1} 3k \wedge y = 3(i-1)) \equiv x = \sum_{k=0}^{i} 3k \wedge y = 3i$$

$$\equiv I$$

Die Besten Invarianten finden - Tipp 2



Die Besten Invarianten finden - Tipp 2

$$WP[\![x = x + y]\!](x = \sum_{k=0}^{i} 3k) \equiv x + y = \sum_{k=0}^{i} 3k$$

$$\equiv x = \sum_{k=0}^{i} 3k - y$$

Die Besten Invarianten finden - Tipp 2

$$WP[\![x = x + y]\!](x = \sum_{k=0}^{i} 3k) \equiv x + y = \sum_{k=0}^{i} 3k$$

$$\equiv x = \sum_{k=0}^{i} 3k - y$$

$$WP[\![y = i * 3]\!](x = \sum_{k=0}^{i} 3k - y) \equiv x = \sum_{k=0}^{i} 3k - 3i$$

$$\equiv x = \sum_{k=0}^{i-1} 3k$$

$$WP[\![i = i + 1]\!](x = \sum_{k=0}^{i-1} 3k) \equiv x = \sum_{k=0}^{i} 3k$$

$$\equiv I$$

Die Besten Invarianten finden - Tipp 2

$$WP[\![x = x + y]\!](x = \sum_{k=0}^{i} 3k) \equiv x + y = \sum_{k=0}^{i} 3k$$

$$\equiv x = \sum_{k=0}^{i} 3k - y$$

Die Besten Invarianten finden - Tipp 2

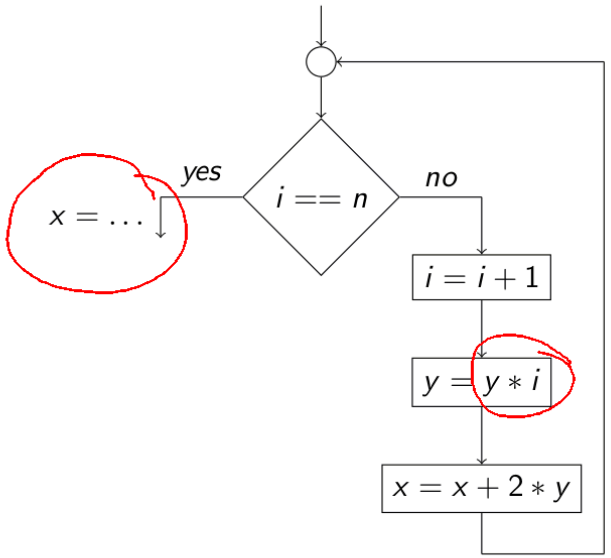
$$
\begin{aligned}
WP[\![y = y + 3]\!](x = \sum_{k=0}^{i-1} 3k \wedge y = 3i) &\equiv x = \sum_{k=0}^{i-1} 3k \wedge y + 3 = 3i \\
&\equiv x = \sum_{k=0}^{i-1} 3k \wedge y = 3i - 3 \\
&\equiv x = \sum_{k=0}^{i-1} 3k \wedge y = 3(i-1)
\end{aligned}
$$

Die Besten Invarianten finden - Tipp 2

$$
\begin{aligned}
WP[\![y = y + 3]\!](x = \sum_{k=0}^{i-1} 3k \wedge y = 3i) &\equiv x = \sum_{k=0}^{i-1} 3k \wedge y + 3 = 3i \\
&\equiv x = \sum_{k=0}^{i-1} 3k \wedge y = 3i - 3 \\
&\equiv x = \sum_{k=0}^{i-1} 3k \wedge y = 3(i-1)
\end{aligned}
$$

Tipp 3

Die Besten Invarianten finden - Tipp 3



Die Besten Invarianten finden - Tipp 3

Wir machen eine Tabelle:

#	0	1	2	3	4
i	0	1	2	3	4
x	2	4	8	20	68
y	1	1	2	6	24

$= i!$

Welche Formeln gelten nun für x und y?

Die Besten Invarianten finden - Tipp 3

Wir machen eine Tabelle:

#	0	1	2	3	4	5	6	7	8
i	0	1	2	3	4	5	6	7	8
x	2	4	8	20	68	308	1748	11828	92468
y	1	1	2	6	24	120	720	5040	40320

Welche Formeln gelten nun für x und y?

Die Besten Invarianten finden - Tipp 3

Wir machen eine nützlichere Tabelle:

#	0	1	2	3		
i	0	1	2	3		
x	2					
y	1					

Die Besten Invarianten finden - Tipp 3

$x = x + 2 \cdot i$

Wir machen eine nützlichere Tabelle:

#	0	1	2	3		
i	0	1	2	3		
x	2	2 $+2 * 1$				
y	1					

Die Besten Invarianten finden - Tipp 3

Wir machen eine nützlichere Tabelle:

#	0	1	2	3		
i	0	1	2	3		
x	2	2 $+2*1$				
y	1	1				

Die Besten Invarianten finden - Tipp 3

Wir machen eine nützlichere Tabelle:

#	0	1	2	3		
i	0	1	2	3		
x	2	2 $+2*1$				
y	1					

Die Besten Invarianten finden - Tipp 3

Wir machen eine nützlichere Tabelle:

#	0	1	2	3		
i	0	1	2	3		
x	2	2 $+2*1$	2 $+2*1$ $+2*1*2$	2 $+2*1$ $+2*1*2$ $+2*1*2*3$		
y	1	1	$1*2$			

Die Besten Invarianten finden - Tipp 3

Wir machen eine nützlichere Tabelle:

#	0	1	2	3	$\cdots$	i
i	0	1	2	3	$\cdots$	i
x	2	2 $+2*1$	2 $+2*1$ $+2*1*2$	2 $+2*1$ $+2*1*2$ $+2*1*2*3$	$\cdots$ $\cdots$ $\cdots$ $\cdots$	
y	1	1	$1*2$	$1*2*3$	$\cdots$	

Die Besten Invarianten finden - Tipp 3

Wir machen eine nützlichere Tabelle:

#	0	1	2	3	$\cdots$	i
i	0	1	2	3	$\cdots$	i
x	2	2 $+2*1$	2 $+2*1$ $+2*1*2$	2 $+2*1$ $+2*1*2$ $+2*1*2*3$	$\cdots$ $\cdots$ $\cdots$ $\cdots$	2 $+2*1$ $+2*1*2$ $+2*1*2*3$ $\vdots$ $+2*1*\cdots*i$
y	1	1	$1*2$	$1*2*3$	$\cdots$	

Die Besten Invarianten finden - Tipp 3

Wir machen eine nützlichere Tabelle:

#	0	1	2	3	$\cdots$	i
i	0	1	2	3	$\cdots$	i
x	2	2 $+2*1$	2 $+2*1$ $+2*1*2$	2 $+2*1$ $+2*1*2$ $+2*1*2*3$	$\cdots$ $\cdots$ $\cdots$ $\cdots$	2 $+2*1$ $+2*1*2$ $+2*1*2*3$ $\vdots$ $+2*1*\cdots*i$
y	1	1	$1*2$	$1*2*3$	$\cdots$	$1*2*3*\cdots*i$

54/134

Die Besten Invarianten finden - Tipp 3

Jetzt noch eine $\cdots$-freie Darstellung finden

$$1*2*3*\cdots*i$$

Die Besten Invarianten finden - Tipp 3

Jetzt noch eine $\cdots$-freie Darstellung finden

$$1*2*3*\cdots*i = i! = y$$

$$2 + (2*1) + (2*1*2) + (2*1*2*3) + \cdots + (2*1*2*3*\cdots*i)$$

55/134

Die Besten Invarianten finden - Tipp 3

Jetzt noch eine $\cdots$-freie Darstellung finden

$$1 * 2 * 3 * \cdots * i = i! = y$$

$$\begin{aligned} & 2 + (2 * 1) + (2 * 1 * 2) + (2 * 1 * 2 * 3) + \cdots + (2 * 1 * 2 * 3 * \cdots * i) \\ = \; & 2 * (1 + 1 + (1 * 2) + (1 * 2 * 3) + \cdots + (1 * 2 * 3 * \cdots * i)) \end{aligned}$$

2.! 3.! + ... + i!

Die Besten Invarianten finden - Tipp 3

Jetzt noch eine $\cdots$-freie Darstellung finden

$$1 * 2 * 3 * \cdots * i = i! = y$$

$$\begin{aligned} & 2 + (2 * 1) + (2 * 1 * 2) + (2 * 1 * 2 * 3) + \cdots + (2 * 1 * 2 * 3 * \cdots * i) \\ = \; & 2 * (1 + 1 + (1 * 2) + (1 * 2 * 3) + \cdots + (1 * 2 * 3 * \cdots * i)) \\ = \; & 2 * (0! + 1! + 2! + 3! + \cdots + i!) \end{aligned}$$

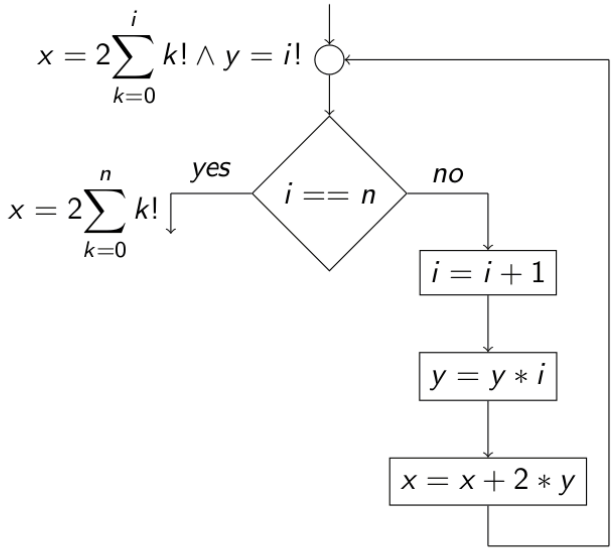
Die Besten Invarianten finden - Tipp 3

Jetzt noch eine $\cdots$-freie Darstellung finden

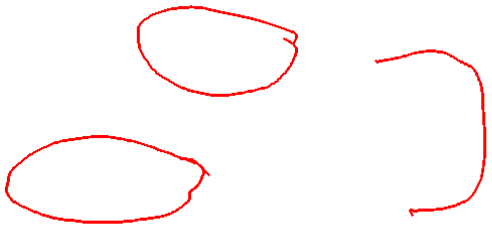
$$1 * 2 * 3 * \cdots * i = i! = y$$

$$\begin{aligned} & 2 + (2 * 1) + (2 * 1 * 2) + (2 * 1 * 2 * 3) + \cdots + (2 * 1 * 2 * 3 * \cdots * i) \\ = \; & 2 * (1 + 1 + (1 * 2) + (1 * 2 * 3) + \cdots + (1 * 2 * 3 * \cdots * i)) \\ = \; & 2 * (0! + 1! + 2! + 3! + \cdots + i!) \\ = \; & 2 * \sum_{k=0}^{i} k! = x \end{aligned}$$

Die Besten Invarianten finden - Tipp 3



Tipp 4

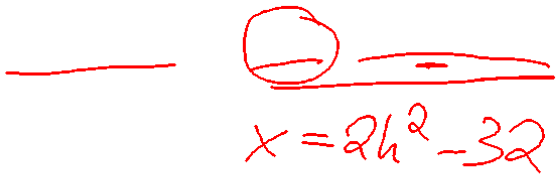


Die Besten Invarianten finden - Tipp 4

Warum kann die Invariante $x = 2i^2 - 32$ niemals ausreichen um $x = 2n^2 + 16|n|$ zu beweisen?

Die Besten Invarianten finden - Tipp 4

Warum kann die Invariante $x = 2i^2 - 32$ niemals ausreichen um $x = 2n^2 + 16|n|$ zu beweisen?



Die Besten Invarianten finden - Tipp 4

Warum kann die Invariante $x = 2i^2 - 32$ niemals ausreichen um $x = 2n^2 + 16|n|$ zu beweisen?

Betrachten wir die WP-Berechnung an der Verzweigung:

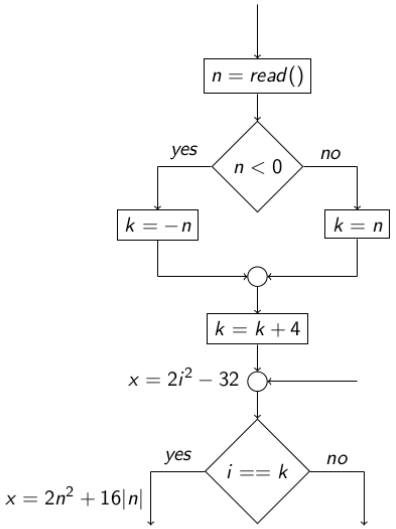
$$x = 2i^2 - 32 \implies (i = k \wedge x = 2n^2 + 16|n|) \vee (\dots)$$

Aus $x = 2i^2 - 32$ und $i = k$ können wir $x = 2k^2 - 32$ folgern, aber wir wissen nicht, wie wir $x = 2n^2 + 16|n|$ dahin umformen können.

- Es fehlt eine Beziehung von n zu i oder k.

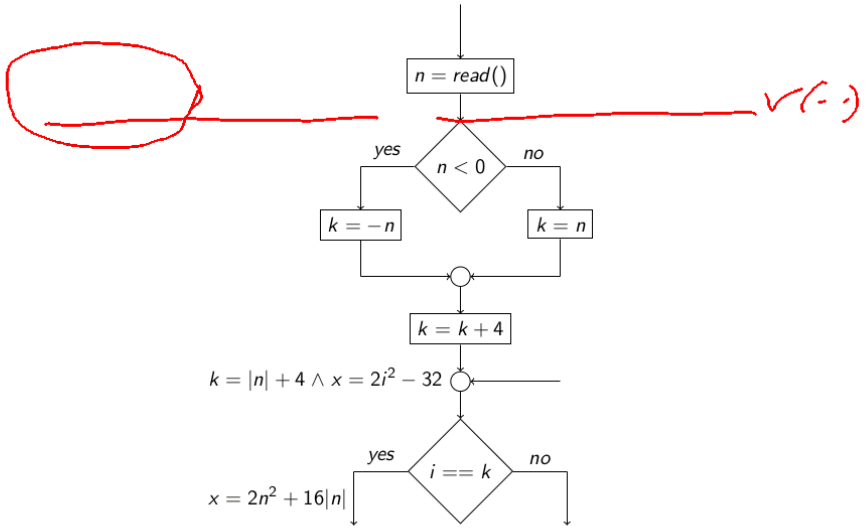
Die Besten Invarianten finden - Tipp 4

Gibt es eine Beziehung von n zu i oder k?



Die Besten Invarianten finden - Tipp 4

Gibt es eine Beziehung von n zu i oder k?



Die Besten Invarianten finden - Tipp 4

$$k = |n| + 4 \wedge x = 2i^2 - 32 \implies i = k \wedge x = 2n^2 + 16|n|$$
$$\equiv |n| = k - 4 \wedge x = 2i^2 - 32 \implies i = k \wedge x = 2(k-4)^2 + 16k - 64$$

Die Besten Invarianten finden - Tipp 4

$$k = |n| + 4 \wedge x = 2i^2 - 32 \implies i = k \wedge x = 2n^2 + 16|n|$$
$$\equiv |n| = k - 4 \wedge x = 2i^2 - 32 \implies i = k \wedge x = 2(k-4)^2 + 16k - 64$$
$$\equiv |n| = k - 4 \wedge x = 2i^2 - 32 \implies i = k \wedge x = 2k^2 - 32$$

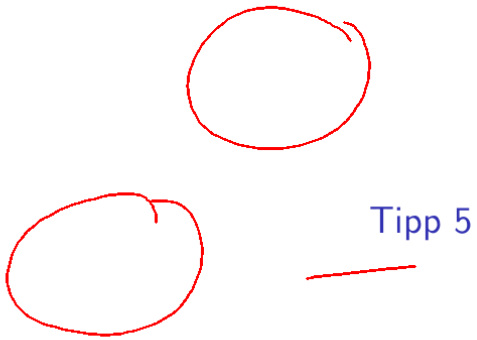
Die Besten Invarianten finden - Tipp 4

Tipp 4

Die Variablen, die zur Berechnung von x im Beweisziel verwendet werden und diejenigen, die dazu in der Invariante verwendet werden, müssen in Beziehung stehen. Wenn diese Beziehung nicht aus der Verzweigungsbedingung folgt, müssen weitere Aussagen zur Invariante hinzugefügt werden.

Die Besten Invarianten finden - Tipp 4

$$
\begin{aligned}
k = |n| + 4 \wedge x = 2i^2 - 32 &\implies i = k \wedge x = 2n^2 + 16|n| \\
\equiv |n| = k - 4 \wedge x = 2i^2 - 32 &\implies i = k \\
&\quad \wedge x = 2(k-4)^2 + 16k - 64 \\
\equiv |n| = k - 4 \wedge x = 2i^2 - 32 &\implies i = k \wedge x = 2k^2 - 32
\end{aligned}
$$



Tipp 5

Die Besten Invarianten finden - Tipp 5

$$
\begin{aligned}
WP[\![x = x + 2]\!](x = 2i) &\equiv x + 2 = 2i \\
&\equiv x = 2(i-1)
\end{aligned}
$$

$$
\begin{aligned}
WP[\![i = i + 1]\!](x = 2(i-1)) &\equiv x = 2i \\
&\equiv I
\end{aligned}
$$

Die Besten Invarianten finden - Tipp 5

$$x = 2i \stackrel{?}{\Longrightarrow} (i < n \wedge x = 2i) \vee (i \geq n \wedge x = 2n)$$

Die Besten Invarianten finden - Tipp 5

$$x = 2i \not\Longrightarrow (i < n \wedge x = 2i) \vee (i \geq n \wedge x = 2n)$$

Warum können wir das nicht zeigen?

- wir wissen am Schleifenausgang nur, dass $i \geq n$ und können deshalb nicht $x = 2n$ zu $x = 2i$ umschreiben
- wir benötigen die Aussage, dass dort genau $i = n$ gilt

Die Besten Invarianten finden - Tipp 5

$$x = 2i \not\Longrightarrow (i < n \wedge x = 2i) \vee (i \geq n \wedge x = 2n)$$

Warum können wir das nicht zeigen?

- wir wissen am Schleifenausgang nur, dass $i \geq n$ und können deshalb nicht $x = 2n$ zu $x = 2i$ umschreiben
- wir benötigen die Aussage, dass dort genau $i = n$ gilt

Wir verstärken die Aussage (WP):

$$(i < n \wedge x = 2i) \vee (i \geq n \wedge x = 2n)$$

Die Besten Invarianten finden - Tipp 5

$$x = 2i \stackrel{?}{\Longrightarrow} x = 2i \wedge i \leq n$$

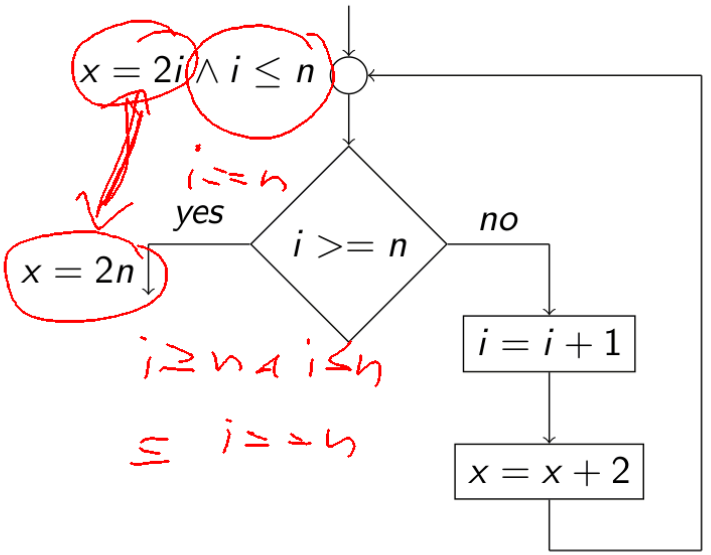
Die Besten Invarianten finden - Tipp 5

$$x = 2i \not\Rightarrow x = 2i \wedge i \leq n$$

Warum können wir das dennoch immer noch nicht zeigen?

- weil uns jetzt ein $i \leq n$ in der Invariante fehlt

Die Besten Invarianten finden - Tipp 5



Die Besten Invarianten finden - Tipp 5

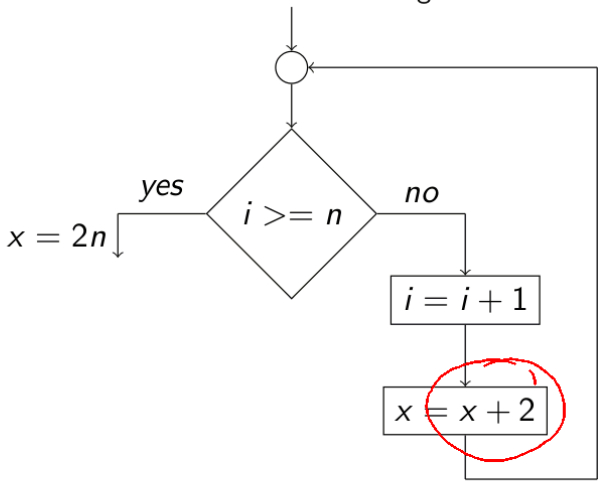
$$WP[\![x = x + 2]\!](x = 2i \wedge i \leq n) \equiv x + 2 = 2i \wedge i \leq n$$
$$\equiv x = 2(i-1) \wedge i \leq n$$

$$WP[\![i = i + 1]\!](x = 2(i-1) \wedge i \leq n) \equiv x = 2i \wedge i < n$$

Tipp 6

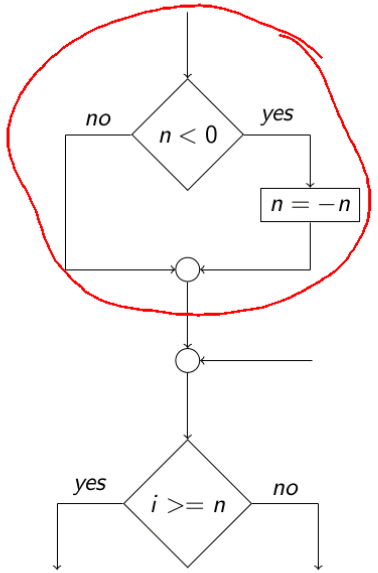
Die Besten Invarianten finden - Tipp 6

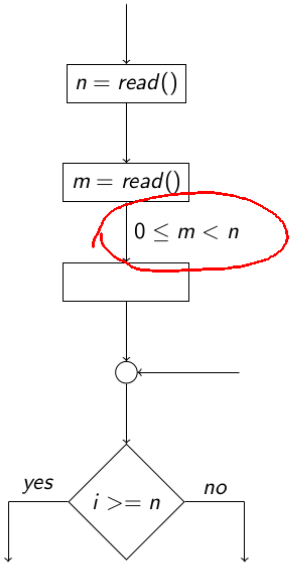
Betrachten wir noch einmal das Programm:



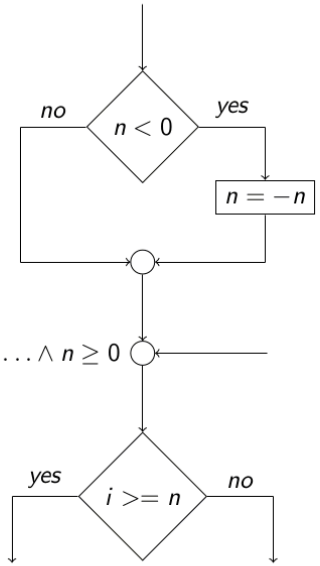
- Berechnet dieses Programm überhaupt $x = 2n$ für negative n?

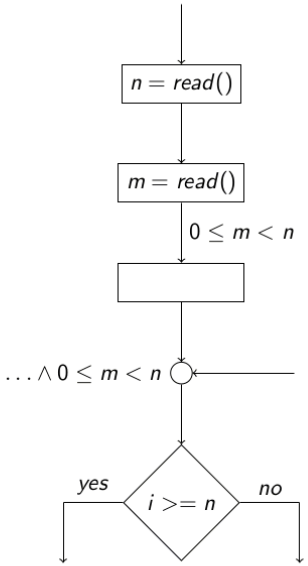
Die Besten Invarianten finden - Tipp 6



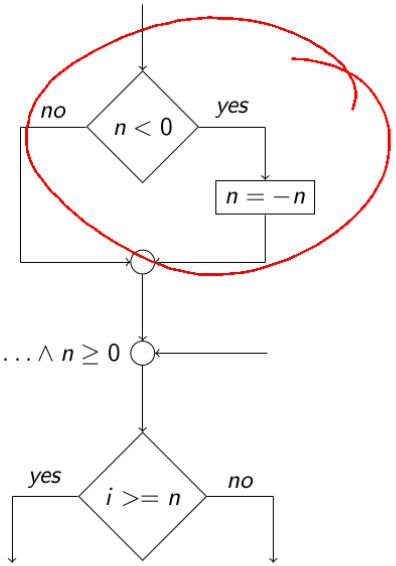


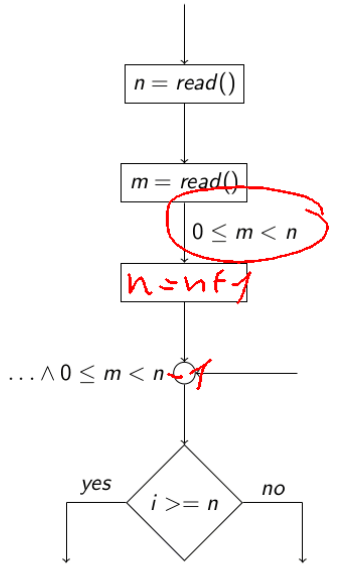
Die Besten Invarianten finden - Tipp 6





Die Besten Invarianten finden - Tipp 6





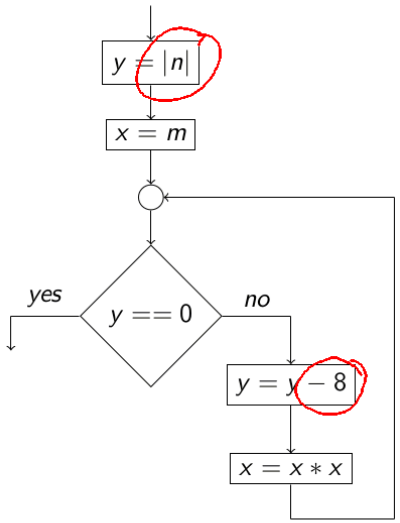
Die Besten Invarianten finden - Tipp 6

Tipp 6

Werden Programmeingaben begrenzt, z.B. durch Ziehen von Beträgen, vorzeitigen Programmabbruch bei unerwünschten Eingaben oder durch gegebene Zusicherungen, so kann die Information über die Werte der Eingabevariablen $(n, m, \dots)$, die innerhalb der Schleife zulässig sind, in der Invariante sinnvoll sein.

Die Besten Invarianten finden - Tipp 7

Was fällt in diesem Programm auf?



Die Besten Invarianten finden - Tipp 7

Die Schleife enthält keinen klassischen Schleifenzähler (i).

Wie lässt dennoch eine Beziehung zwischen den Variablen herstellen und eine Invariante definieren?

- Wir denken uns einen Schleifenzähler δ
- Anschließend setzen wir die relevanten Variablen mit diesem in Beziehung
- Dann lösen wir nach δ auf und setzen ein

Die Besten Invarianten finden - Tipp 7

Die Schleife enthält keinen klassischen Schleifenzähler (i).

Wie lässt dennoch eine Beziehung zwischen den Variablen herstellen und eine Invariante definieren?

- Wir denken uns einen Schleifenzähler δ
- Anschließend setzen wir die relevanten Variablen mit diesem in Beziehung
- Dann lösen wir nach δ auf und setzen ein

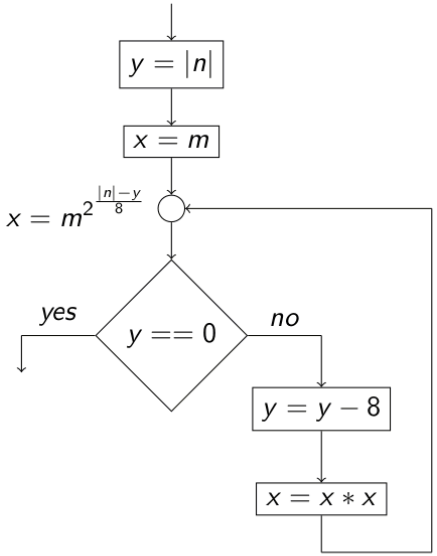
$$y = |n| - 8\delta$$

$$\delta = \frac{|n| - y}{8}$$

$$x = m^{2\delta}$$

$$x = m^{2^{\frac{|n|-y}{8}}}$$

Die Besten Invarianten finden - Tipp 7



Tipp 8

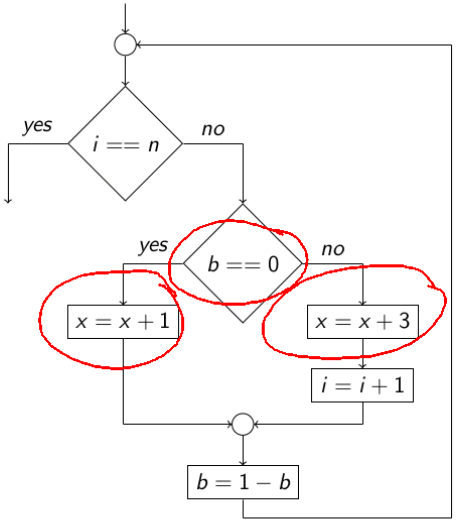
Die Besten Invarianten finden - Tipp 8

Wie könnte hier eine Invariante aussehen?

#	0	1	2	3	4	5	6	7	8	9
i	0	0	1	1	2	2	3	3	4	4
x	0	1	4	5	8	9	12	13	16	17

Die Besten Invarianten finden - Tipp 8

Wie könnte hier eine Invariante aussehen?



Die Besten Invarianten finden - Tipp 8

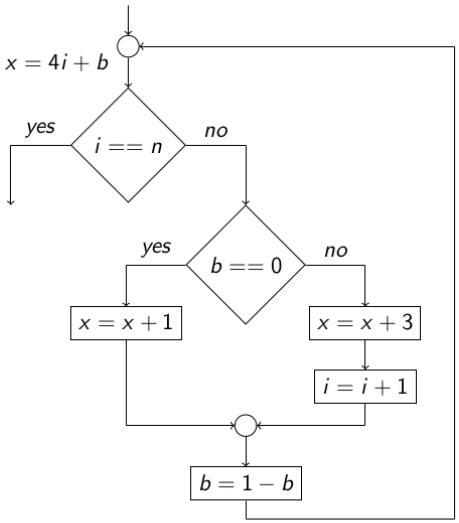
Wie könnte hier eine Invariante aussehen?

#	0	1	2	3	4	5	6	7	8	9
i	0	0	1	1	2	2	3	3	4	4
x	0	1	4	5	8	9	12	13	16	17

$x = 4i + b$

Die Besten Invarianten finden - Tipp 8

Wie könnte hier eine Invariante aussehen?



Die Besten Invarianten finden - Tipp 8

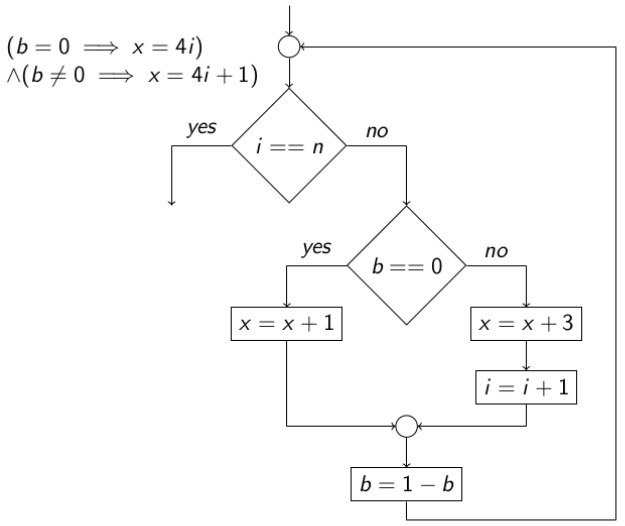
Wie könnte hier eine Invariante aussehen?

#	0	1	2	3	4	5	6	7	8	9
i	0	0	1	1	2	2	3	3	4	4
b	0	1	0	1	0	1	0	1	0	1
x	0	1	4	5	8	9	12	13	16	17

$(b = 0 \implies x = 4i) \wedge (b = 1 \implies x = 4i + 1)$

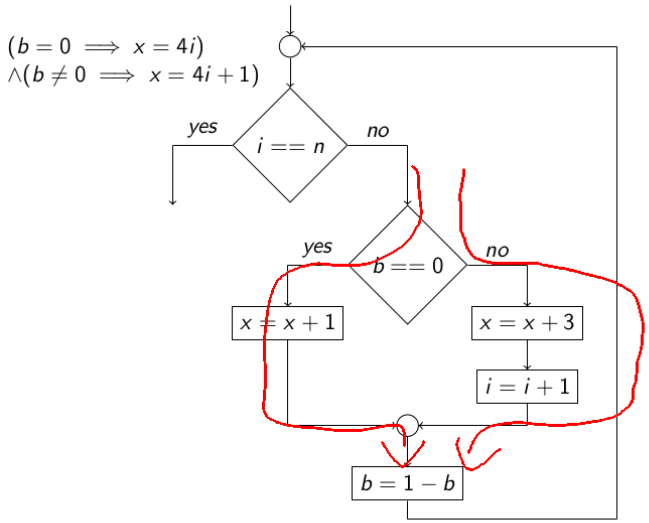
Die Besten Invarianten finden - Tipp 8

Wie könnte hier eine Invariante aussehen?

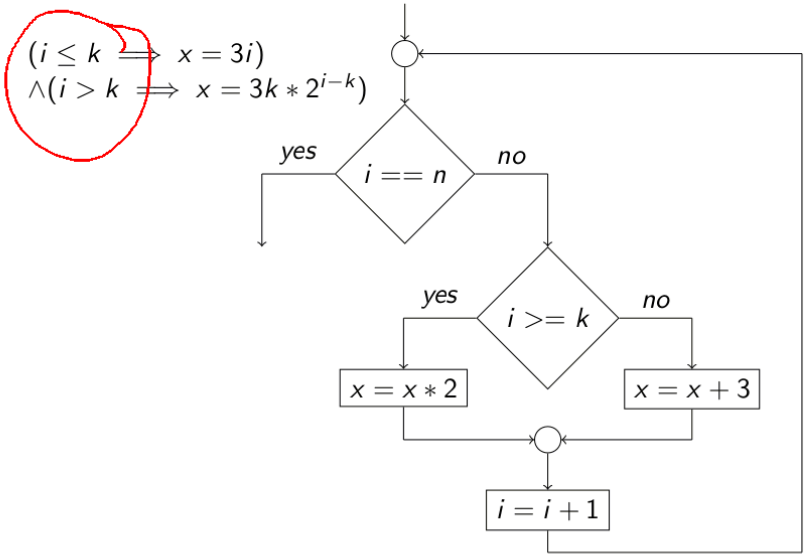


Die Besten Invarianten finden - Tipp 8

Wie könnte hier eine Invariante aussehen?

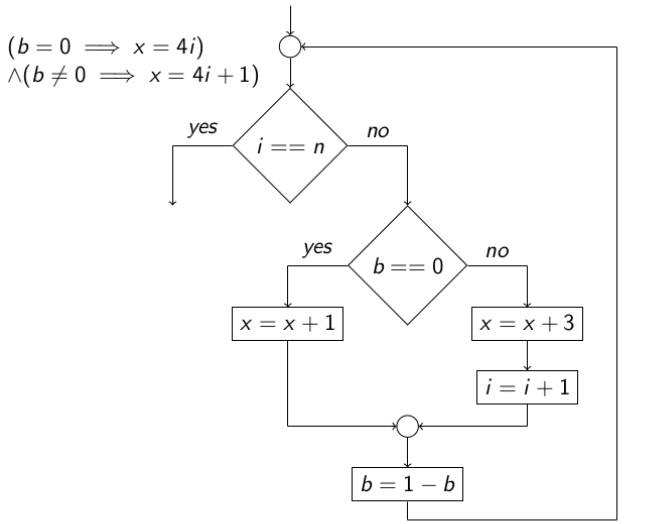


Die Besten Invarianten finden - Tipp 8



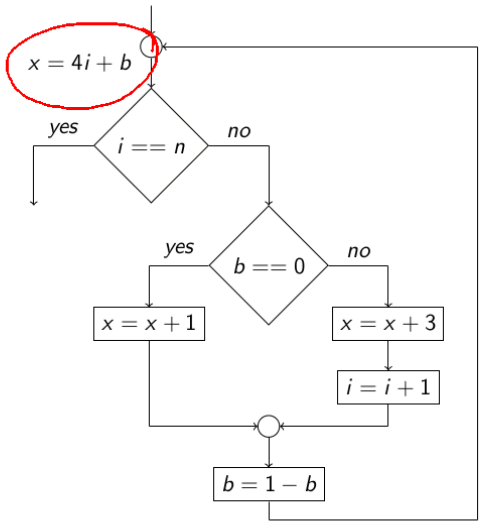
Die Besten Invarianten finden - Tipp 8

Wie könnte hier eine Invariante aussehen?



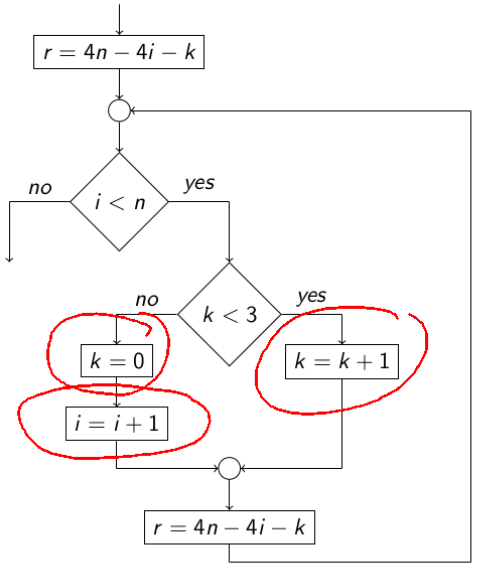
Die Besten Invarianten finden - Tipp 8

Wie könnte hier eine Invariante aussehen?

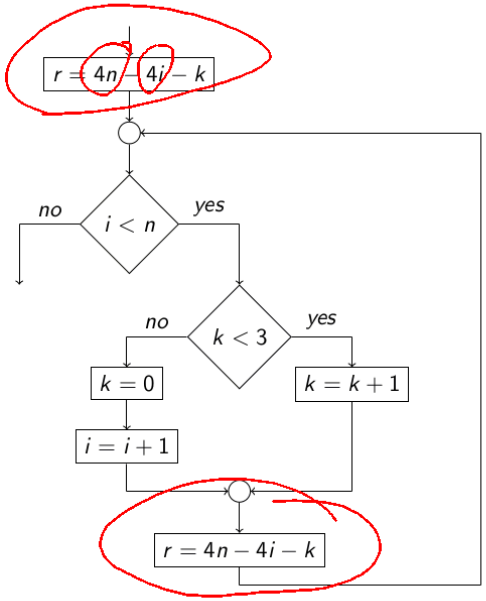


Tipp 9

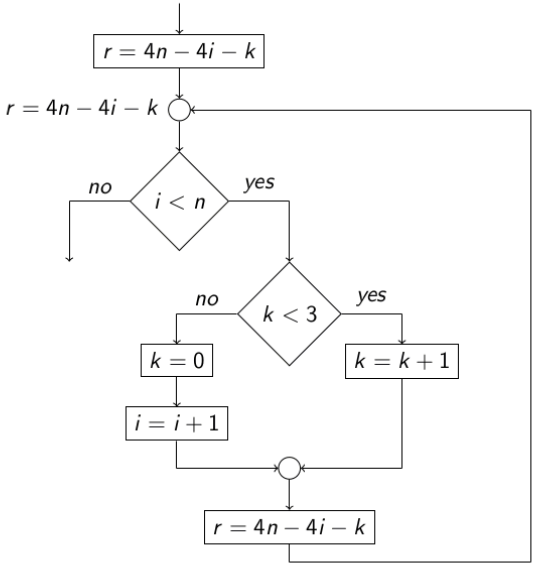
Die Besten Invarianten finden - Tipp 9



Die Besten Invarianten finden - Tipp 9



Die Besten Invarianten finden - Tipp 9



Die Besten Invarianten finden - Tipp 9

Tipp 9

In einem Terminierungsbeweis wird eine Aussage über r in der Invariante benötigt. Es gilt dabei immer die für r ermittelte Berechnungsvorschrift.

$\Longrightarrow r > 4n - 4i - k$

Die Besten Invarianten finden - Tipp 10

Wir betrachten das Programm erneut.

Was muss für A und B gezeigt werden um Terminierung zu beweisen?

- $A \implies r > 0$
- $B \implies r > 4n - 4i - k$

Die Besten Invarianten finden - Tipp 10

Wir betrachten das Programm erneut.

Was muss für A und B gezeigt werden um Terminierung zu beweisen?

- $A \implies r > 0$
- $B \implies r > 4n - 4i - k$

Die Besten Invarianten finden - Tipp 10

Wir betrachten das Programm erneut.

Was muss für A und B gezeigt werden um Terminierung zu beweisen?

- $A \implies r > 0$
- $B \implies r > 4n - 4i - k$

Die Besten Invarianten finden - Tipp 10

$$WP[\![k < 3]\!](r > 4n - 4i - 4, r > 4n - 4i - k - 1)$$
$$\equiv (k \geq 3 \wedge r > 4n - 4i - 4) \vee (k < 3 \wedge r > 4n - 4i - k - 1)$$

Welche Möglichkeiten haben wir hier, um die beiden Seiten in die gleiche Form zu bekommen?

Die Besten Invarianten finden - Tipp 10

$$WP[\![k < 3]\!](r > 4n - 4i - 4, r > 4n - 4i - k - 1)$$
$$\equiv (k \geq 3 \wedge r > 4n - 4i - 4) \vee (k < 3 \wedge r > 4n - 4i - k - 1)$$

Welche Möglichkeiten haben wir hier, um die beiden Seiten in die gleiche Form zu bekommen?

Können wir die -4 in der linken Klammer irgendwie in $-k-1$ umschreiben?

- Ja, wenn wir wüssten, dass dort $k = 3$ gilt.
- Betrachtet man das Programm, wird klar, dass dort tatsächlich immer $k = 3$.
- Also Verstärken wir ...

Die Besten Invarianten finden - Tipp 10

$$WP[\![r = 4n - 4i - k]\!](r = 4n - 4i - k) \equiv true$$
$$\Longleftarrow \quad r > 4n - 4i - k \equiv: B$$

$$WP[\![k = k + 1]\!](r > 4n - 4i - k) \equiv r > 4n - 4i - k - 1$$

$$WP[\![i = i + 1]\!](r > 4n - 4i - k) \equiv r > 4n - 4i - k - 4$$

$$WP[\![k = 0]\!](r > 4n - 4i - k - 4) \equiv r > 4n - 4i - 4$$

Die Besten Invarianten finden - Tipp 10

$$WP[\![r = 4n - 4i - k]\!](r = 4n - 4i - k) \equiv true$$
$$\Longleftarrow \quad r > 4n - 4i - k \equiv: B$$

$$WP[\![k = k + 1]\!](r > 4n - 4i - k) \equiv r > 4n - 4i - k - 1$$

$$WP[\![i = i + 1]\!](r > 4n - 4i - k) \equiv r > 4n - 4i - k - 4$$

$$WP[\![k = 0]\!](r > 4n - 4i - k - 4) \equiv r > 4n - 4i - 4$$

Die Besten Invarianten finden - Tipp 10

$$
\begin{aligned}
& WP[\![k < 3]\!](r > 4n - 4i - 4, r > 4n - 4i - k - 1) \\
\equiv\ & (k \geq 3 \wedge r > 4n - 4i - 4) \vee (k < 3 \wedge r > 4n - 4i - k - 1)
\end{aligned}
$$

Die Besten Invarianten finden - Tipp 10

$$
\begin{aligned}
& WP[\![i < n]\!](true, r > 4n - 4i - k - 1 \wedge k \leq 3 \wedge i < n) \\
\equiv\ & (i \geq n) \vee (i < n \wedge r > 4n - 4i - k - 1 \wedge k \leq 3)
\end{aligned}
$$

Die Besten Invarianten finden - Tipp 10

$$
\begin{aligned}
& WP[\![i < n]\!](true, r > 4n - 4i - k - 1 \wedge k \leq 3 \wedge i < n) \\
\equiv\ & (i \geq n) \vee (i < n \wedge r > 4n - 4i - k - 1 \wedge k \leq 3) \\
\Longleftarrow\ & (i \geq n \wedge r > 4n - 4i - k - 1 \wedge k \leq 3) \\
& \quad \vee (i < n \wedge r > 4n - 4i - k - 1 \wedge k \leq 3)
\end{aligned}
$$

Die Besten Invarianten finden - Tipp 10

$$
\begin{aligned}
& WP[\![i < n]\!](true, r > 4n - 4i - k - 1 \wedge k \leq 3 \wedge i < n) \\
\equiv\ & (i \geq n) \vee (i < n \wedge r > 4n - 4i - k - 1 \wedge k \leq 3) \\
\Longleftarrow\ & (i \geq n \wedge r > 4n - 4i - k - 1 \wedge k \leq 3) \\
& \quad \vee (i < n \wedge r > 4n - 4i - k - 1 \wedge k \leq 3) \\
\equiv\ & r > 4n - 4i - k - 1 \wedge k \leq 3
\end{aligned}
$$

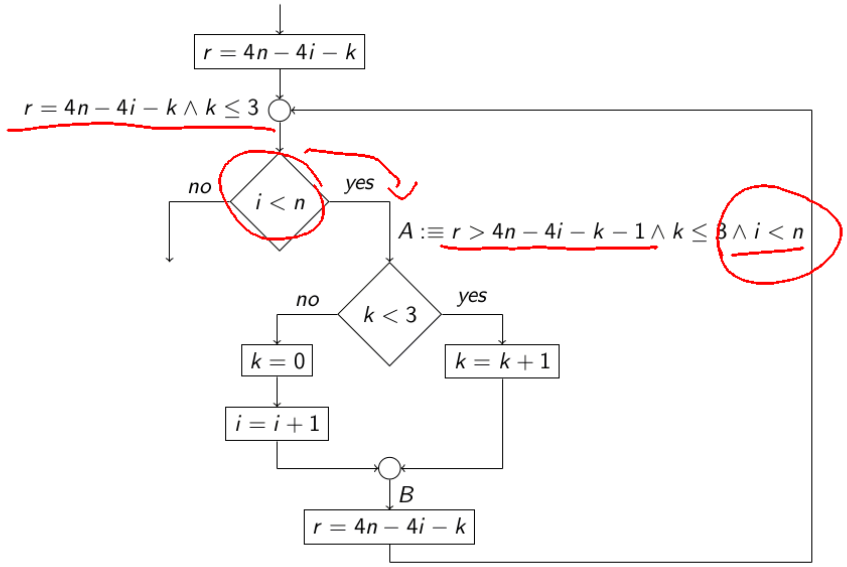
Die Besten Invarianten finden - Tipp 10

$$r = 4n - 4i - k \not\Rightarrow r > 4n - 4i - k - 1 \wedge k \leq 3$$

Warum können wir das nicht zeigen?

- Weil uns ein $k \leq 3$ in der Invariante fehlt.
- Hätten wir das erahnen können?
- Warum benötigen wir nichts über i und n in der Invariante?

Die Besten Invarianten finden - Tipp 10

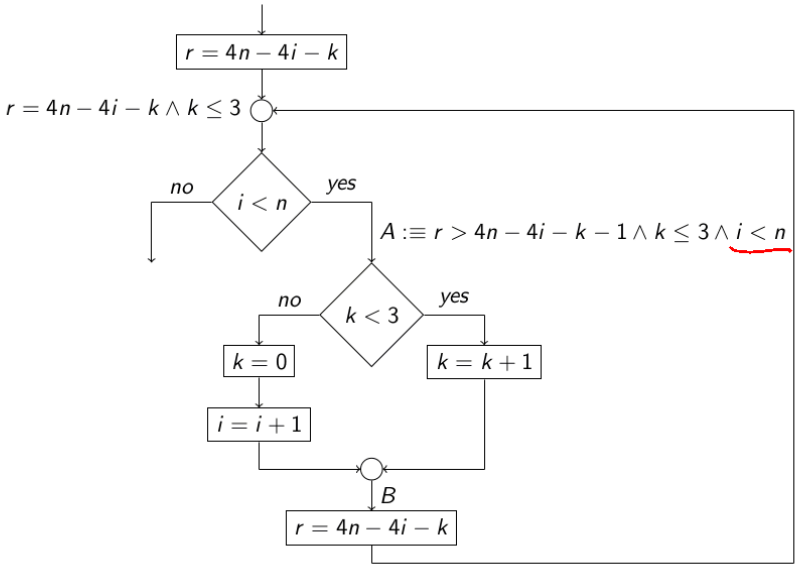


Die Besten Invarianten finden - Tipp 10

Tipp 10

Für die Terminierung benötigen wir Aussagen über alle Variablen in der Invarianten, die für die Berechnung von r benötigt werden und über die sich keine starken Beziehungen aus der Schleifenbedingung folgern lassen (wobei "stark" hier mindestens $\leq, \geq$ meint).

Die Besten Invarianten finden - Tipp 10



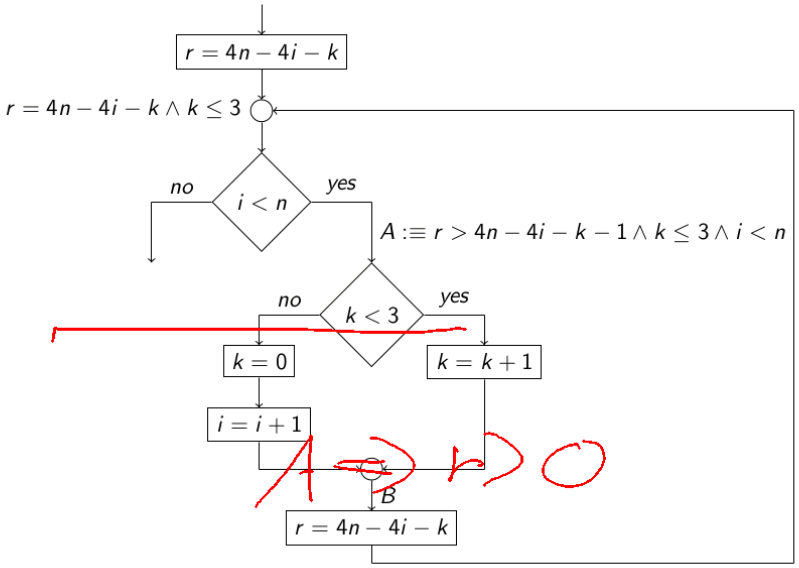
Beispiel 1

Die Besten Invarianten finden - Tipp 10

Tipp 10

Für die Terminierung benötigen wir Aussagen über alle Variablen in der Invarianten, die für die Berechnung von r benötigt werden und über die sich keine starken Beziehungen aus der Schleifenbedingung folgern lassen (wobei "stark" hier mindestens $\leq, \geq$ meint).

Die Besten Invarianten finden - Tipp 10



Die Besten Invarianten finden - Tipp 10

$$
\begin{aligned}
& WP[\![k < 3]\!](r > 4n - 4i - 4, r > 4n - 4i - k - 1) \\
\equiv\ & (k \geq 3 \wedge r > 4n - 4i - 4) \vee (k < 3 \wedge r > 4n - 4i - k - 1) \\
\Longleftarrow\ & (k = 3 \wedge r > 4n - 4i - 4) \vee (k < 3 \wedge r > 4n - 4i - k - 1) \\
\equiv\ & (k = 3 \wedge r > 4n - 4i - k - 1) \vee (k < 3 \wedge r > 4n - 4i - k - 1) \\
\equiv\ & r > 4n - 4i - k - 1 \wedge k \leq 3 \\
\Longleftarrow\ & r > 4n - 4i - k - 1 \wedge k \leq 3 \wedge i < n \equiv: A
\end{aligned}
$$

Die Besten Invarianten finden - Tipp 10

$$
\begin{aligned}
& WP[\![i < n]\!](true, r > 4n - 4i - k - 1 \wedge k \leq 3 \wedge i < n) \\
\equiv\ & (i \geq n) \vee (i < n \wedge r > 4n - 4i - k - 1 \wedge k \leq 3) \\
\Longleftarrow\ & (i \geq n \wedge r > 4n - 4i - k - 1 \wedge k \leq 3) \\
& \vee (i < n \wedge r > 4n - 4i - k - 1 \wedge k \leq 3)
\end{aligned}
$$

Praktische Beispiele - Beispiel 1

Was lässt sich sofort über die Invariante sagen?

Praktische Beispiele - Beispiel 1

Was lässt sich sofort über die Invariante sagen?

Praktische Beispiele - Beispiel 1

#	0	1	2	3	4	$\cdots$	i
i	0	1	2	3	4	$\cdots$	i
y	0	0					
		$y+2\cdot i+1=+1$					
	$=0$	$=1$					
x	0						
		$y+1$					

Praktische Beispiele - Beispiel 1

#	0	1	2	3	4	$\cdots$	i
i	0	1	2	3	4	$\cdots$	i
y	0	0 $+1$ $+2i+1$	0 $+1$ $+3$				
	$=0$	$=1$	$=4$				
x	0	0 $+1+1$					

Praktische Beispiele - Beispiel 1

#	0	1	2	3	4	$\cdots$	i
i	0	1	2	3	4	$\cdots$	i
y	0	0 $+1$ $+2i+1$	0 $+1$ $+3$				
	$=0$	$=1$	$=4$				
x	0	0 $+1+1$	0 $+1+1$ $+4+1$				

Praktische Beispiele - Beispiel 1

#	0	1	2	3	4	$\cdots$	i
i	0	1	2	3	4	$\cdots$	i
y	0	0 $+1$	0 $+1$ $+3$	0 $+1$ $+3$ $+5$			
	$=0$	$=1$	$=4$	$=9$			
x	0	0 $+1+1$	0 $+1+1$ $+4+1$				

Praktische Beispiele - Beispiel 1

#	0	1	2	3	4	$\cdots$	i
i	0	1	2	3	4	$\cdots$	i
y	0	0 $+1$	0 $+1$ $+3$	0 $+1$ $+3$ $+5$	0 $+1$ $+3$ $+5$ $+7$		
	$=0$	$=1$	$=4$	$=9$	$=16$		
x	0	0 $+1+1$	0 $+1+1$ $+4+1$	0 $+1+1$ $+4+1$ $+9+1$			

Praktische Beispiele - Beispiel 1

#	0	1	2	3	4	$\cdots$	i
i	0	1	2	3	4	$\cdots$	i
y	0	0	0	0	0		0
		$+1$	$+1$	$+1$	$+1$		$+1$
			$+3$	$+3$	$+3$		$+3$
				$+5$	$+5$	$\cdots$	$+5$
					$+7$		$+7$
							$\vdots$
	$=0$	$=1$	$=4$	$=9$	$=16$	$\cdots$	$=i^2$
x	0	0	0	0	0		
		$+1+1$	$+1+1$	$+1+1$	$+1+1$		
			$+4+1$	$+4+1$	$+4+1$		
				$+9+1$	$+9+1$		
					$+16+1$		

Praktische Beispiele - Beispiel 1

#	0	1	2	3	4	$\cdots$	i
i	0	1	2	3	4	$\cdots$	i
y	0	0	0	0	0		0
		$+1$	$+1$	$+1$	$+1$		$+1$
			$+3$	$+3$	$+3$		$+3$
				$+5$	$+5$	$\cdots$	$+5$
					$+7$		$+7$
							$\vdots$
	$=0$	$=1$	$=4$	$=9$	$=16$	$\cdots$	$=i^2$
x	0	0	0	0	0		0
		$+1+1$	$+1+1$	$+1+1$	$+1+1$		$+1+1$
			$+4+1$	$+4+1$	$+4+1$		$+4+1$
				$+9+1$	$+9+1$	$\cdots$	$+9+1$
					$+16+1$		$+16+1$
							$\vdots$
							$+i^2+1$

Praktische Beispiele - Beispiel 1

Was lässt sich sofort über die Invariante sagen?

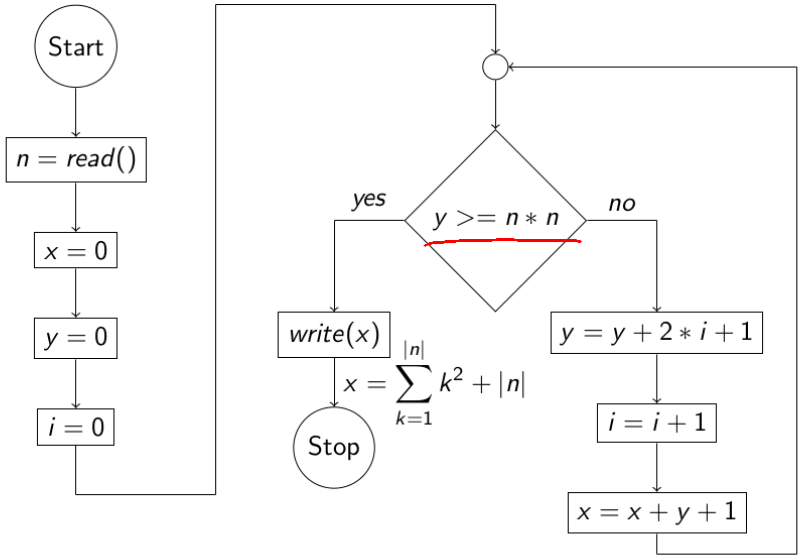
- Wir brauchen eine präzise Aussage ($=$) über x (Tipp 1)
- Wir brauchen eine präzise Aussage ($=$) über y (Tipp 2)
- Wir erkennen die Zusammenhänge mit einer Tabelle (Tipp 3)

Wir haben also:

$$x = \sum_{k=0}^{i} k^2 + i \wedge y = i^2$$

Können wir noch mehr erkennen?

Praktische Beispiele - Beispiel 1



Praktische Beispiele - Beispiel 1

Los geht's mit: $I :\equiv x = \sum_{k=0}^{i} k^2 + i \wedge y = i^2 \wedge y \leq n^2$

$$WP[\![x = x + y + 1]\!](x = \sum_{k=0}^{i} k^2 + i \wedge y = i^2 \wedge y \leq n^2)$$

Praktische Beispiele - Beispiel 1

Los geht's mit: $I :\equiv x = \sum_{k=0}^{i} k^2 + i \wedge y = i^2 \wedge y \leq n^2$

$$WP[\![x = x + y + 1]\!](x = \sum_{k=0}^{i} k^2 + i \wedge y = i^2 \wedge y \leq n^2)$$

$$\equiv x + y + 1 = \sum_{k=0}^{i} k^2 + i \wedge y = i^2 \wedge y \leq n^2$$

$$\equiv x = \sum_{k=0}^{i} k^2 + i - y - 1 \wedge y = i^2 \wedge y \leq n^2$$

Praktische Beispiele - Beispiel 1

Los geht's mit: $I :\equiv x = \sum_{k=0}^{i} k^2 + i \wedge y = i^2 \wedge y \leq n^2$

$$WP[\![x = x + y + 1]\!](x = \sum_{k=0}^{i} k^2 + i \wedge y = i^2 \wedge y \leq n^2)$$

$$\equiv x + y + 1 = \sum_{k=0}^{i} k^2 + i \wedge y = i^2 \wedge y \leq n^2$$

$$\equiv x = \sum_{k=0}^{i} k^2 + i - y - 1 \wedge y = i^2 \wedge y \leq n^2$$

$$\equiv x = \sum_{k=0}^{i} k^2 - i^2 + (i-1) \wedge y = i^2 \wedge y \leq n^2$$

$$\equiv x = \sum_{k=0}^{i-1} k^2 + (i-1) \wedge y = i^2 \wedge y \leq n^2$$

Praktische Beispiele - Beispiel 1

$$WP[\![i = i + 1]\!](x = \sum_{k=0}^{i-1} k^2 + (i-1) \wedge y = i^2 \wedge y \leq n^2)$$

$$\equiv x = \sum_{k=0}^{i} k^2 + i \wedge y = (i+1)^2 \wedge y \leq n^2$$

Praktische Beispiele - Beispiel 1

$$WP[\![i = i + 1]\!](x = \sum_{k=0}^{i-1} k^2 + (i-1) \wedge y = i^2 \wedge y \leq n^2)$$

$$\equiv x = \sum_{k=0}^{i} k^2 + i \wedge y = (i+1)^2 \wedge y \leq n^2$$

$$WP[\![y = y + 2i + 1]\!](x = \sum_{k=0}^{i} k^2 + i \wedge y = (i+1)^2 \wedge y \leq n^2)$$

$$\equiv x = \sum_{k=0}^{i} k^2 + i \wedge y + 2i + 1 = i^2 + 2i + 1 \wedge y \leq n^2$$

Praktische Beispiele - Beispiel 1

$$WP[\![i = i + 1]\!](x = \sum_{k=0}^{i-1} k^2 + (i-1) \wedge y = i^2 \wedge y \leq n^2)$$

$$\equiv x = \sum_{k=0}^{i} k^2 + i \wedge y = (i+1)^2 \wedge y \leq n^2$$

$$WP[\![y = y + 2i + 1]\!](x = \sum_{k=0}^{i} k^2 + i \wedge y = (i+1)^2 \wedge y \leq n^2)$$

$$\equiv x = \sum_{k=0}^{i} k^2 + i \wedge y + 2i + 1 = i^2 + 2i + 1 \wedge y \leq n^2$$

$$\equiv x = \sum_{k=0}^{i} k^2 + i \wedge y = i^2 \wedge y \leq n^2$$

Praktische Beispiele - Beispiel 1

$$WP[\![y >= n * n]\!](x = \sum_{k=0}^{i} k^2 + i \wedge y = i^2 \wedge y \leq n^2, x = \sum_{k=1}^{|n|} k^2 + |n|)$$

$$\equiv (y < n^2 \wedge x = \sum_{k=0}^{i} k^2 + i \wedge y = i^2 \wedge y \leq n^2)$$

$$\vee (y \geq n^2 \wedge x = \sum_{k=1}^{|n|} k^2 + |n|)$$

$$\Longleftarrow (y < n^2 \wedge x = \sum_{k=0}^{i} k^2 + i \wedge y = i^2)$$

$$\vee (y = n^2 \wedge x = \sum_{k=1}^{|n|} k^2 + |n| \wedge y = i^2)$$

Praktische Beispiele - Beispiel 1

$$(y < n^2 \wedge x = \sum_{k=0}^{i} k^2 + i \wedge y = i^2)$$

$$\vee (y = n^2 \wedge x = \sum_{k=1}^{|n|} k^2 + |n| \wedge y = i^2)$$

Praktische Beispiele - Beispiel 1

$$(y < n^2 \wedge x = \sum_{k=1}^{i} k^2 + i \wedge y = i^2)$$
$$\vee (y = n^2 \wedge x = \sum_{k=1}^{|i|} k^2 + |i| \wedge y = i^2)$$

Praktische Beispiele - Beispiel 1

$$(y < n^2 \wedge x = \sum_{k=1}^{i} k^2 + i \wedge y = i^2)$$
$$\vee (y = n^2 \wedge x = \sum_{k=1}^{|i|} k^2 + |i| \wedge y = i^2)$$

Warum können wir jetzt nicht weitermachen?

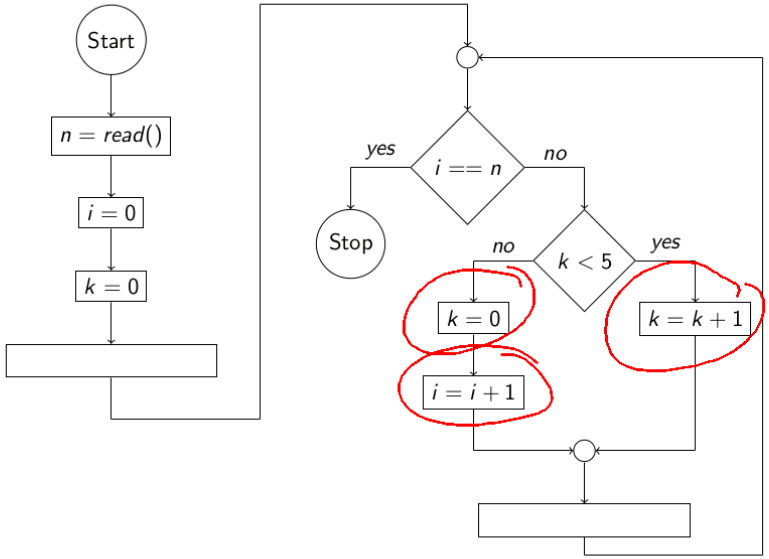
- Wir müssen die Beträge loswerden
- Das geht nur dann, wenn wir wissen, dass $i \geq 0$
- Wir verstärken die Invariante um $i \geq 0$

Praktische Beispiele - Beispiel 1

$$(y < n^2 \wedge x = \sum_{k=1}^{i} k^2 + i \wedge y = i^2)$$
$$\vee (y = n^2 \wedge x = \sum_{k=1}^{|i|} k^2 + |i| \wedge y = i^2)$$

Beispiel 2

Praktische Beispiele - Beispiel 2



Praktische Beispiele - Beispiel 2

Wie können wir die Berechnungsvorschrift für r bestimmen?

Mit einer Tabelle:

#	0	1	2	3	4	5	6	7	8	9	10	11	12	13
i	0	0	0	0	0	0	1	1	1	1	1	1	2	2
k	0	1	2	3	4	5	0	1	2	3	4	5	0	1

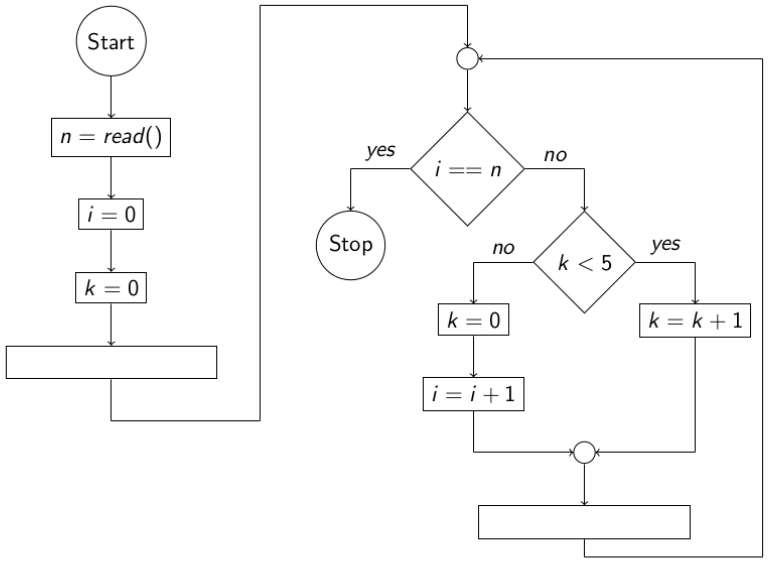
m + 60·h

h + 6i

1:30 = 90

2:15 = 135

Praktische Beispiele - Beispiel 2



Praktische Beispiele - Beispiel 2

Wie können wir die Berechnungsvorschrift für r bestimmen?

Mit einer Tabelle:

#	0	1	2	3	4	5	6	7	8	9	10	11	12	13
i	0	0	0	0	0	0	1	1	1	1	1	1	2	2
k	0	1	2	3	4	5	0	1	2	3	4	5	0	1

$r = 6n - 6i - h$

Praktische Beispiele - Beispiel 2

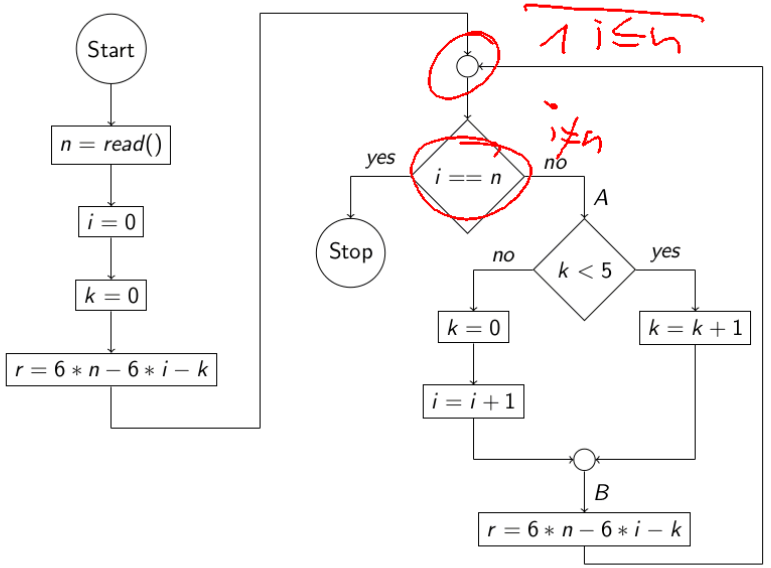
Wie können wir die Berechnungsvorschrift für r bestimmen?

Mit einer Tabelle:

#	0	1	2	3	4	5	6	7	8	9	10	11	12	13
i	0	0	0	0	0	0	1	1	1	1	1	1	2	2
k	0	1	2	3	4	5	0	1	2	3	4	5	0	1

Einen streng monotonen Zähler können wir mit $6i + k$ bauen.

Praktische Beispiele - Beispiel 2



Praktische Beispiele - Beispiel 2

Was lässt sich sofort über die Invariante sagen?

Praktische Beispiele - Beispiel 2

$$
\begin{aligned}
& WP[\![r = 6n - 6i - k]\!](r = 6n - 6i - k \wedge i \leq n \wedge k \leq 5) \\
\equiv\ & i \leq n \wedge k \leq 5 \\
\Longleftarrow\ & r > 6n - 6i - k \wedge i \leq n \wedge k \leq 5 \quad \equiv: B
\end{aligned}
$$

Praktische Beispiele - Beispiel 2

$$
\begin{aligned}
& WP[\![r = 6n - 6i - k]\!](r = 6n - 6i - k \wedge i \leq n \wedge k \leq 5) \\
\equiv\ & i \leq n \wedge k \leq 5 \\
\Longleftarrow\ & r > 6n - 6i - k \wedge i \leq n \wedge k \leq 5 \quad \equiv: B
\end{aligned}
$$

$$
\begin{aligned}
& WP[\![i = i + 1]\!](B) \\
\equiv\ & r > 6n - 6i - k - 6 \wedge i + 1 \leq n \wedge k \leq 5
\end{aligned}
$$

$$
\begin{aligned}
& WP[\![k = 0]\!](r > 6n - 6i - k - 6 \wedge i + 1 \leq n \wedge k \leq 5) \\
\equiv\ & r > 6n - 6i - 6 \wedge i < n \quad \equiv: C
\end{aligned}
$$

$$
\begin{aligned}
& WP[\![k = k + 1]\!](B) \\
\equiv\ & r > 6n - 6i - k - 1 \wedge i \leq n \wedge k + 1 \leq 5 \\
\equiv\ & r > 6n - 6i - k - 1 \wedge i \leq n \wedge k < 5 \quad \equiv: D
\end{aligned}
$$

Praktische Beispiele - Beispiel 2

$I \equiv r = 6n - 6i - k$

$$
\begin{aligned}
& WP[\![k < 5]\!](C, D) \\
\equiv\ & (k \geq 5 \wedge r > 6n - 6i - 6 \wedge i < n) \\
& \vee (k < 5 \wedge r > 6n - 6i - k - 1 \wedge i \leq n \wedge k < 5)
\end{aligned}
$$

Praktische Beispiele - Beispiel 2

$$
\begin{aligned}
& WP[\![k < 5]\!](C, D) \\
\equiv\ & (k \geq 5 \wedge r > 6n - 6i - 6 \wedge i < n) \\
& \vee (k < 5 \wedge r > 6n - 6i - k - 1 \wedge i \leq n \wedge k < 5) \\
\Longleftarrow\ & (k = 5 \wedge r > 6n - 6i - 6 \wedge i < n) \\
& \vee (k < 5 \wedge r > 6n - 6i - k - 1 \wedge i < n)
\end{aligned}
$$

Praktische Beispiele - Beispiel 2

$$
\begin{aligned}
& WP[\![k < 5]\!](C, D) \\
\equiv\ & (k \geq 5 \wedge r > 6n - 6i - 6 \wedge i < n) \\
& \vee (k < 5 \wedge r > 6n - 6i - k - 1 \wedge i \leq n \wedge k < 5) \\
\Longleftarrow\ & (k = 5 \wedge r > 6n - 6i - 6 \wedge i < n) \\
& \vee (k < 5 \wedge r > 6n - 6i - k - 1 \wedge i < n) \\
\equiv\ & (k = 5 \wedge r > 6n - 6i - k - 1 \wedge i < n) \\
& \vee (k < 5 \wedge r > 6n - 6i - k - 1 \wedge i < n)
\end{aligned}
$$

Praktische Beispiele - Beispiel 2

$$
\begin{aligned}
& WP[\![k < 5]\!](C, D) \\
\equiv\ & (k \geq 5 \wedge r > 6n - 6i - 6 \wedge i < n) \\
& \quad \vee (k < 5 \wedge r > 6n - 6i - k - 1 \wedge i \leq n \wedge k < 5) \\
\Longleftarrow\ & (k = 5 \wedge r > 6n - 6i - 6 \wedge i < n) \\
& \quad \vee (k < 5 \wedge r > 6n - 6i - k - 1 \wedge i < n) \\
\equiv\ & (k = 5 \wedge r > 6n - 6i - k - 1 \wedge i < n) \\
& \quad \vee (k < 5 \wedge r > 6n - 6i - k - 1 \wedge i < n) \\
\equiv\ & r > 6n - 6i - k - 1 \wedge i < n \wedge k \leq 5 \quad \equiv: A
\end{aligned}
$$

Praktische Beispiele - Beispiel 2

$$
\begin{aligned}
& WP[\![i == n]\!](A, true) \\
\equiv\ & (i \neq n \wedge r > 6n - 6i - k - 1 \wedge i < n \wedge k \leq 5) \vee i = n
\end{aligned}
$$

Praktische Beispiele - Beispiel 2

$$
\begin{aligned}
& WP[\![i == n]\!](A, true) \\
\equiv\ & (i \neq n \wedge r > 6n - 6i - k - 1 \wedge i < n \wedge k \leq 5) \vee i = n \\
\Longleftarrow\ & (i < n \wedge r > 6n - 6i - k - 1 \wedge k \leq 5) \\
& \quad \vee (i = n \wedge r > 6n - 6i - k - 1 \wedge k \leq 5)
\end{aligned}
$$

Praktische Beispiele - Beispiel 2

Damit haben wir:

- Unsere Invariante ist korrekt
- Zusicherungen in der Schleife sind lokal konsistent
- Beide Terminierungsbedingungen sind erfüllt

Praktische Beispiele - Beispiel 2

$$
\begin{aligned}
& WP[\![i == n]\!](A, true) \\
\equiv\ & (i \neq n \wedge r > 6n - 6i - k - 1 \wedge i < n \wedge k \leq 5) \vee i = n \\
\Longleftarrow\ & (i < n \wedge r > 6n - 6i - k - 1 \wedge k \leq 5) \\
& \quad \vee (i = n \wedge r > 6n - 6i - k - 1 \wedge k \leq 5) \\
\equiv\ & r > 6n - 6i - k - 1 \wedge i \leq n \wedge k \leq 5 \\
\Longleftarrow\ & r = 6n - 6i - k \wedge i \leq n \wedge k \leq 5 \quad \Longleftarrow I
\end{aligned}
$$

Praktische Beispiele - Beispiel 2

Damit haben wir:

- Unsere Invariante ist korrekt
- Zusicherungen in der Schleife sind lokal konsistent
- Beide Terminierungsbedingungen sind erfüllt

Jetzt müssen wir noch zum Programmstart rechnen

- Das ersparen wir uns hier
- Wir erhalten vor $n = read()$ die Zusicherung $n \geq 0$
- Wir erhalten daher *false* am Startknoten
- Das Programm terminiert auch nur für positive Eingaben

Beispiel 3