Abstrakte Interpretation

12./14. Jan. 2005

J.Burghardt, FIRST

Übersicht

- Motivation
- Collecting Semantics
- Vom Programm zum Mengengleichungssystem
- Der Fixpunktsatz
- Mit dem Fixpunktsatz zur Lösung

Übersicht

- Abstrakte Interpretation
- Korrektheit
- Überführbarkeit
- Terminierung
- Aussagekraft

Übersicht

- Statische Analyse mit PolySpace
- Ergänzungen
- Literatur

Motivation

Model-Checking-Techniken sind nur anwendbar,
wenn das zu verifizierende Programm nur endlich viele Zustände hat.

Sobald z.B. mehrere `int`-Variablen auftreten,
wird der Zustandsraum unendlich bzw. jedenfalls zu groß für Model-Checking.

Wir wollen im Folgenden einen Ansatz entwickeln,
der für diese Art von Programmen besser geeignet ist.

“Collecting Semantics”

Zu einem gegebenen imperativen Programm suchen wir für jeden Punkt im Programmablauf die Menge der dort möglichen Variablenwerte.

Beim Testen würde man das Programm nacheinander mit verschiedenen einzelnen Eingabewerten ablaufen lassen und die auftretenden Variablenwerte beobachten.

Wir wollen stattdessen versuchen, durch Analyse der Programmstruktur die Mengen der auftretenden Werte “auf einen Schlag” zu berechnen.

Wir rechnen also nicht mit einzelnen Werten, sondern gleich mit (möglicherweise auch unendlichen) Mengen von Werten.

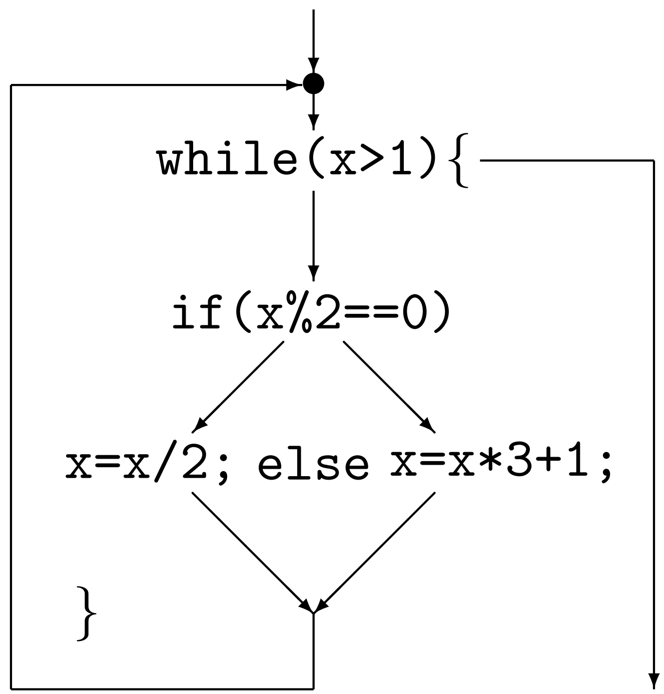
“Collecting Semantics”: Anwendungen

Wenn wir für jede Stelle eines Programms die Menge der dort möglichen Variablenwerte berechnen könnten, wüßten wir alles über die lokalen Eigenschaften des Programms.

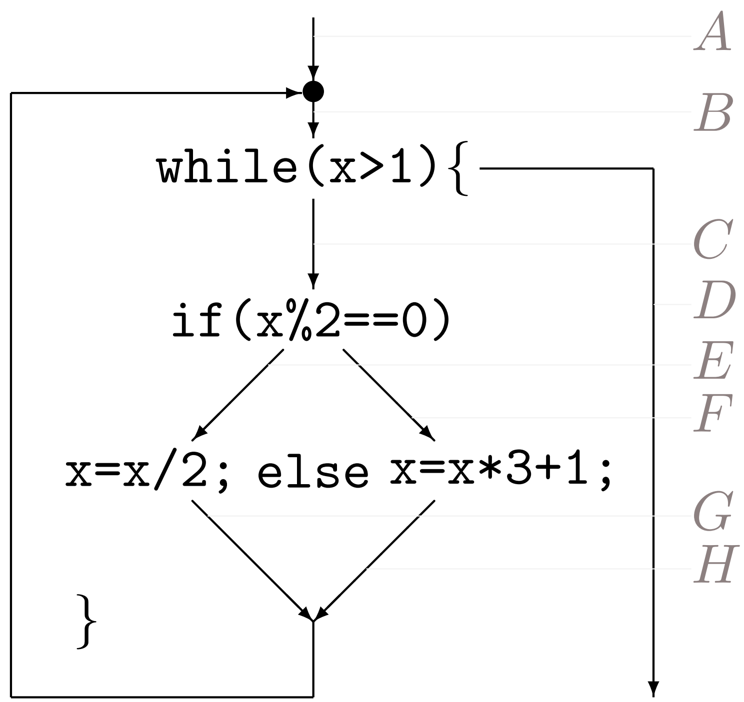
Wir könnten Fragen beantworten wie z.B. kann ein hier ein Überlauf, eine Division durch Null, ein `NULL`-Pointer auftreten, ist hier der Feldindex in gültigen Grenzen, wird diese Stelle überhaupt erreicht.

Wir könnten aber nichts über Terminierung und nichts über den Zusammenhang zwischen Ein- und Ausgabe sagen.

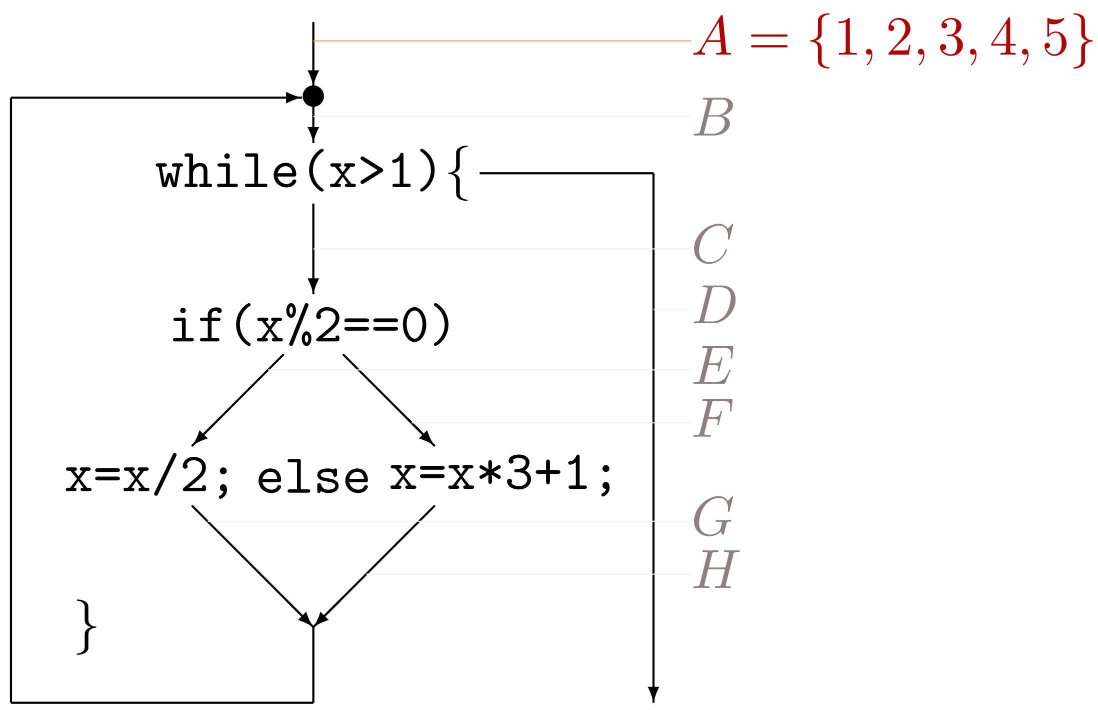
Vom Programm zum Mengen-Gleichungssystem



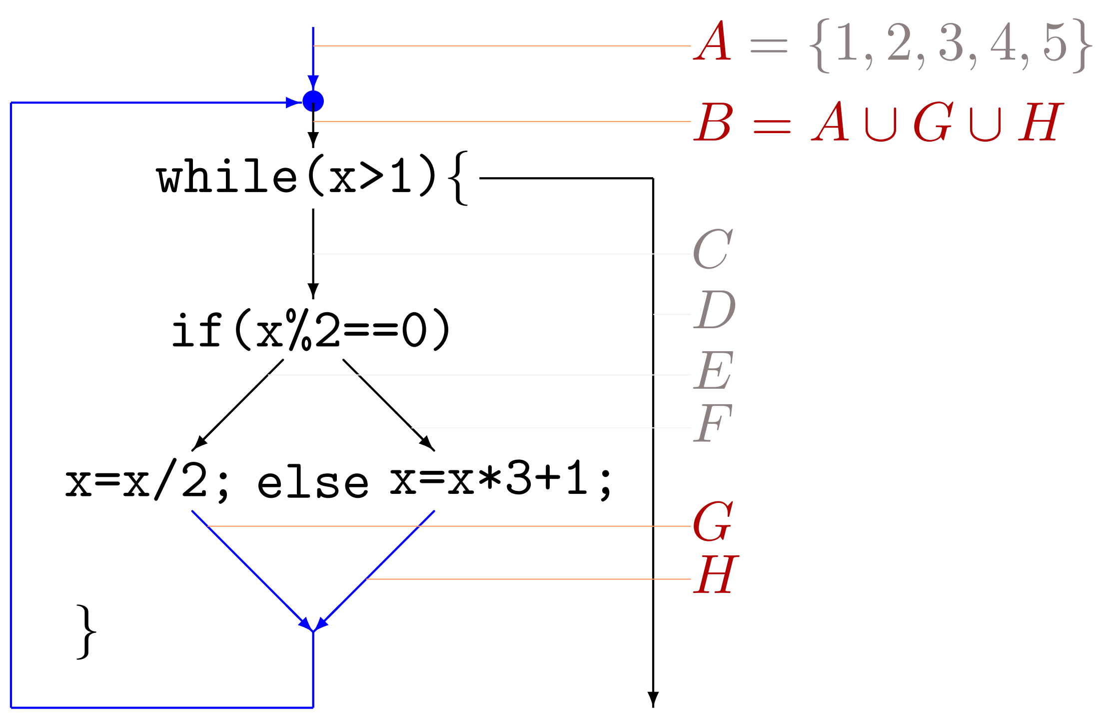
Vom Programm zum Mengen-Gleichungssystem



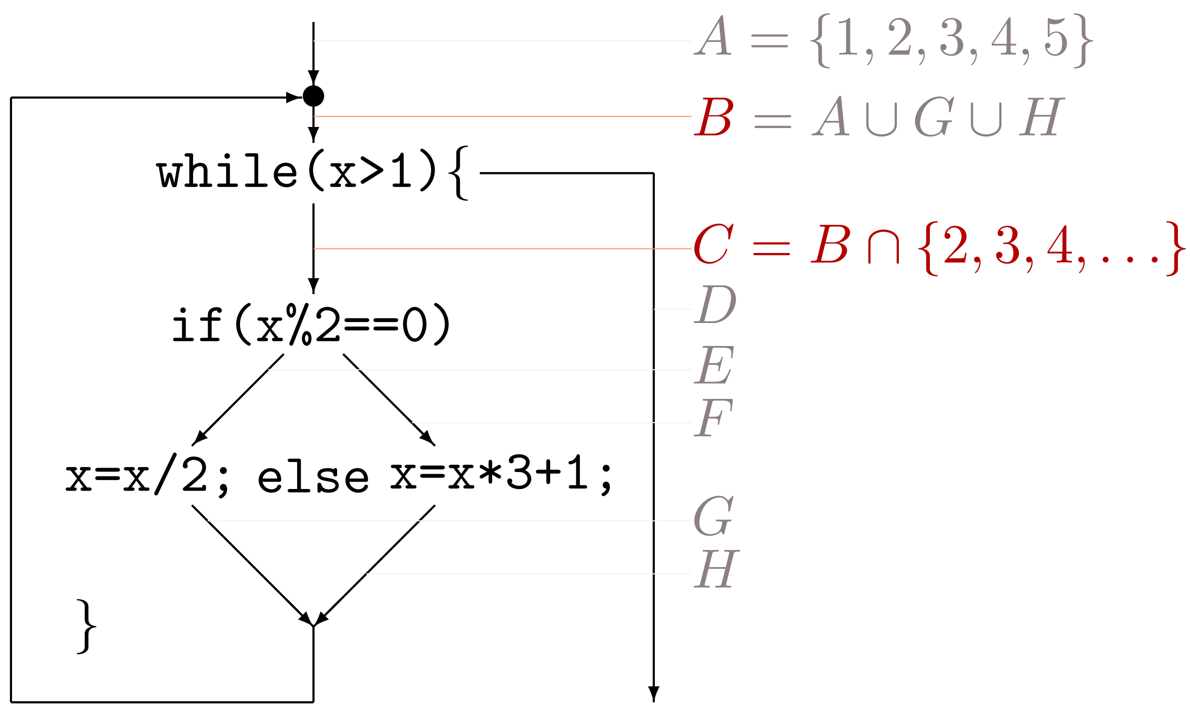
Vom Programm zum Mengen-Gleichungssystem



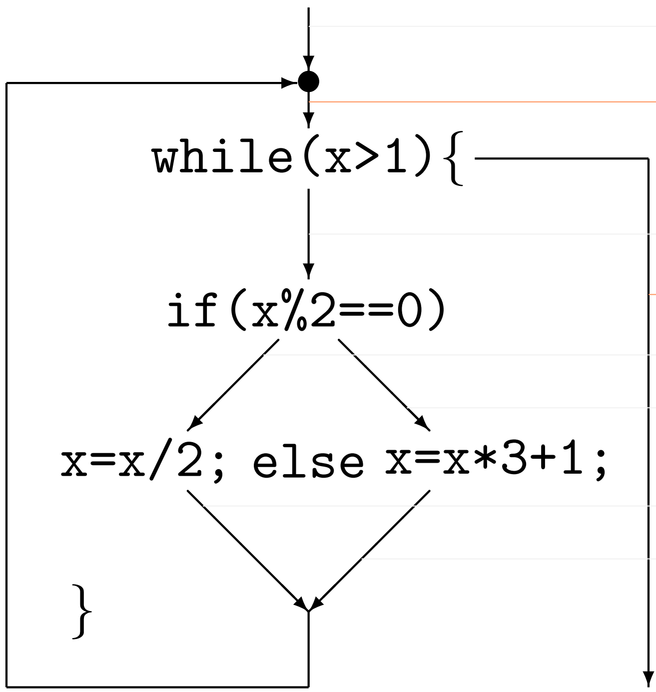
Vom Programm zum Mengen-Gleichungssystem



Vom Programm zum Mengen-Gleichungssystem



Vom Programm zum Mengen-Gleichungssystem



$A = \{1, 2, 3, 4, 5\}$

$B = A \cup G \cup H$

$C = B \cap \{2, 3, 4, \ldots\}$

$D = B \cap \{\ldots, -2, -1, 0, 1\}$

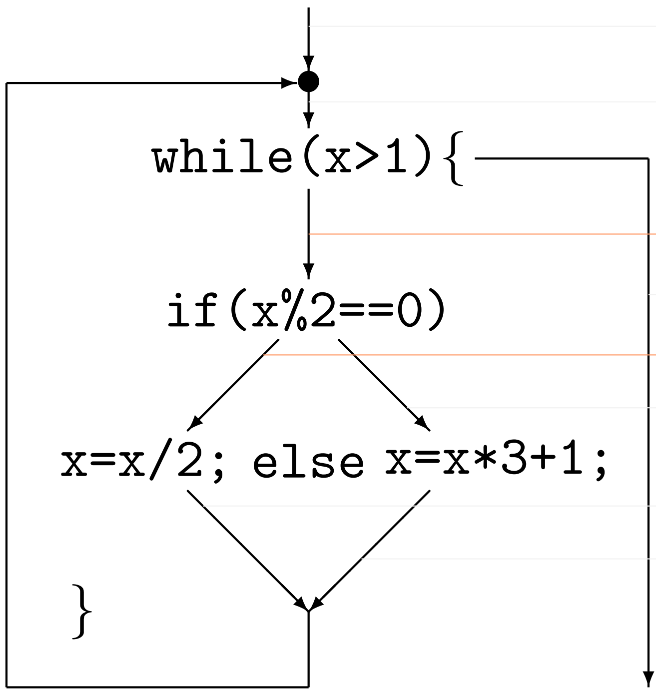
E

F

G

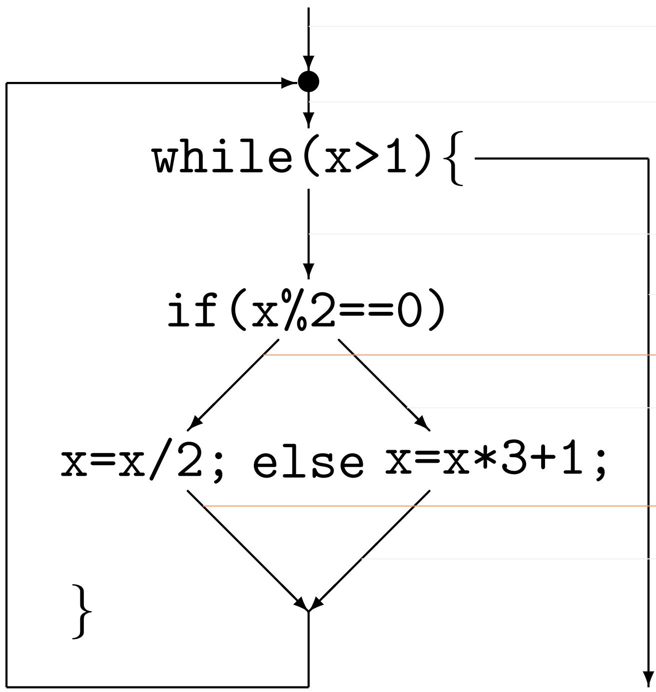
H

Vom Programm zum Mengen-Gleichungssystem



$$A = \{1, 2, 3, 4, 5\}$$
$$B = A \cup G \cup H$$
$$C = B \cap \{2, 3, 4, \ldots\}$$
$$D = B \cap \{\ldots, -2, -1, 0, 1\}$$
$$E = C \cap \{\ldots, -4, -2, 0, 2, 4, \ldots\}$$
$$F$$
$$G$$
$$H$$

Vom Programm zum Mengen-Gleichungssystem



$A = \{1, 2, 3, 4, 5\}$

$B = A \cup G \cup H$

$C = B \cap \{2, 3, 4, \ldots\}$

$D = B \cap \{\ldots, -2, -1, 0, 1\}$

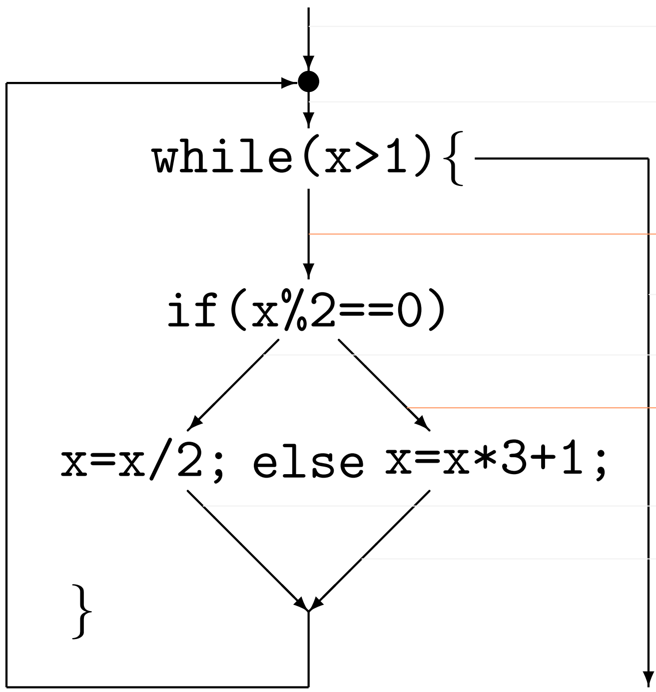
$E = C \cap \{\ldots, -4, -2, 0, 2, 4, \ldots\}$

F

$G = \{n/2 \mid n \in E\}$

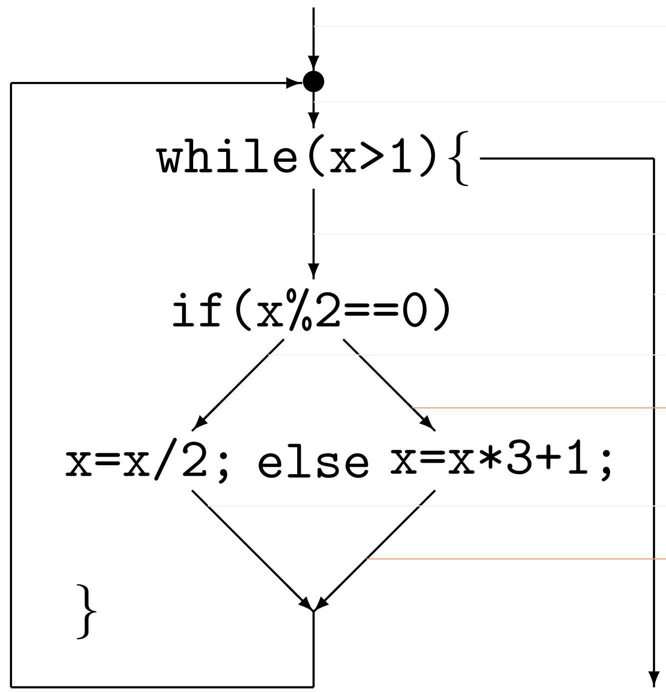
H

Vom Programm zum Mengen-Gleichungssystem



$$A = \{1, 2, 3, 4, 5\}$$
$$B = A \cup G \cup H$$
$$C = B \cap \{2, 3, 4, \ldots\}$$
$$D = B \cap \{\ldots, -2, -1, 0, 1\}$$
$$E = C \cap \{\ldots, -4, -2, 0, 2, 4, \ldots\}$$
$$F = C \cap \{\ldots, -3, -1, 1, 3, \ldots\}$$
$$G = \{n/2 \mid n \in E\}$$
$$H$$

Vom Programm zum Mengen-Gleichungssystem



$A = \{1, 2, 3, 4, 5\}$

$B = A \cup G \cup H$

$C = B \cap \{2, 3, 4, \ldots\}$

$D = B \cap \{\ldots, -2, -1, 0, 1\}$

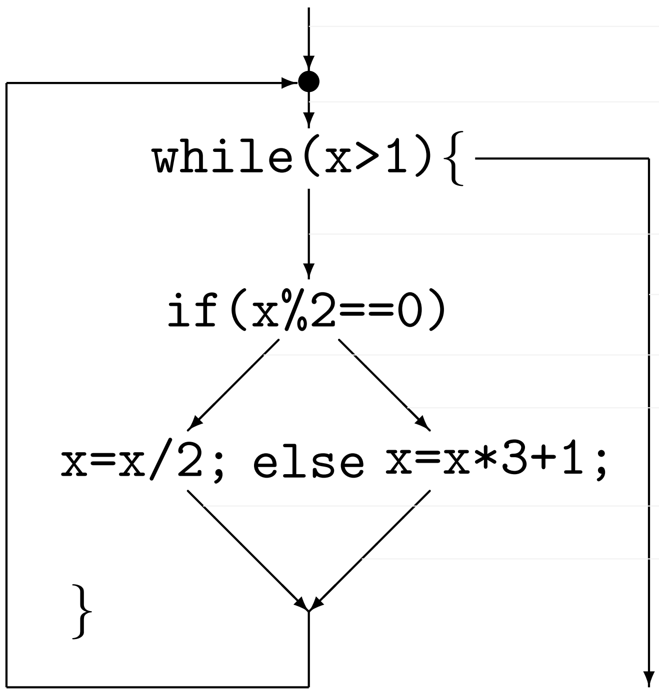
$E = C \cap \{\ldots, -4, -2, 0, 2, 4, \ldots\}$

$F = C \cap \{\ldots, -3, -1, 1, 3, \ldots\}$

$G = \{n/2 \mid n \in E\}$

$H = \{3 \cdot n + 1 \mid n \in F\}$

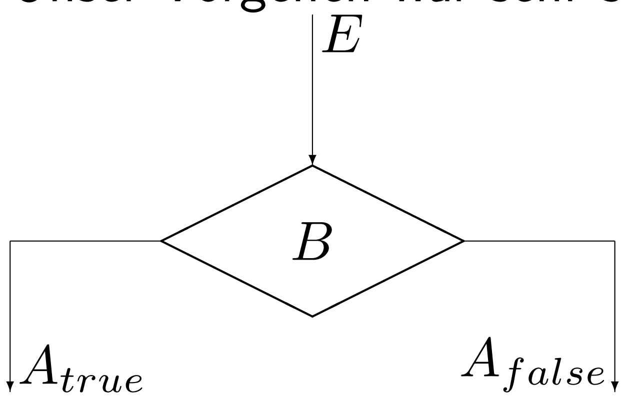
Vom Programm zum Mengen-Gleichungssystem

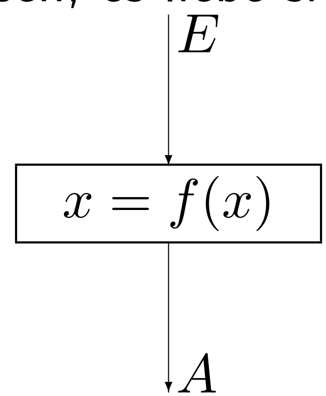


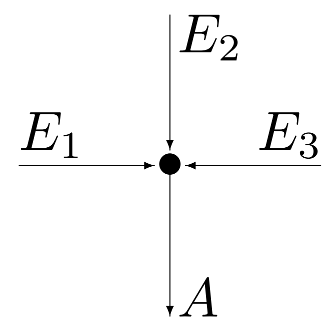
$$A = \{1, 2, 3, 4, 5\}$$
$$B = A \cup G \cup H$$
$$C = B \cap \{2, 3, 4, \ldots\}$$
$$D = B \cap \{\ldots, -2, -1, 0, 1\}$$
$$E = C \cap \{\ldots, -4, -2, 0, 2, 4, \ldots\}$$
$$F = C \cap \{\ldots, -3, -1, 1, 3, \ldots\}$$
$$G = \{n/2 \mid n \in E\}$$
$$H = \{3 \cdot n + 1 \mid n \in F\}$$

Vom Programm zum Mengen-Gleichungssystem

Wir haben aus einem (Spielbeispiel-)Programm ein Mengen-Gleichungssystem abgeleitet.
Unser Vorgehen war sehr systematisch, es ließe sich leicht automatisieren:







$$A_{true} = E \cap \{x \mid B(x)\}$$
$$A_{false} = E \cap \{x \mid \neg B(x)\}$$

$$A = \{f(x) \mid x \in E\}$$

$$A = E_1 \cup E_2 \cup E_3$$

Programme mit mehreren Variablen

In unserem Beispielprogramm tritt nur eine Variable (`int x;`) auf.

Programme mit mehreren Variablen (z.B. `int x, y z;`) lasssen sich durch Verwendung von Record-Typen auf eine Variable zurückführen (z.B. `struct { int x,y,z } vars;`).

Wir werden sie daher hier nicht gesondert behandeln.

Vom Gleichungssystem zur Lösung

Hat ein solches Gleichungssystem zwischen Mengen eine Lösung?

Wie können wir sie finden?

Hat es eine eindeutige Lösung?

Vom Gleichungssystem zur Lösung

Hat ein solches Gleichungssystem zwischen Mengen eine Lösung?

Wie können wir sie finden?

Hat es eine eindeutige Lösung?

Vom Gleichungssystem zur Lösung

Hat ein solches Gleichungssystem zwischen Mengen eine Lösung?
Das ist zu erwarten: wenn wir das Programm nacheinander mit jedem einzelnen Eingabewert ablaufen lassen und an jedem Programmpunkt A,. . . ,H die beobachteten Werte sammeln (daher "collecting semantics"), sollten wir sie finden.

Wie können wir sie finden?

Hat es eine eindeutige Lösung?

Vom Gleichungssystem zur Lösung

Hat ein solches Gleichungssystem zwischen Mengen eine Lösung?
Das ist zu erwarten: wenn wir das Programm nacheinander mit jedem einzelnen Eingabewert ablaufen lassen und an jedem Programmpunkt A,. . . ,H die beobachteten Werte sammeln (daher "collecting semantics"), sollten wir sie finden.
Das geht aber nur, wenn die Eingabemenge endlich ist.

Wie können wir sie finden?

Hat es eine eindeutige Lösung?

Vom Gleichungssystem zur Lösung

Hat ein solches Gleichungssystem zwischen Mengen eine Lösung?
Das ist zu erwarten: wenn wir das Programm nacheinander mit jedem einzelnen Eingabewert ablaufen lassen und an jedem Programmpunkt A,. . . ,H die beobachteten Werte sammeln (daher “collecting semantics”), sollten wir sie finden.
Das geht aber nur, wenn die Eingabemenge endlich ist.

Wie können wir sie finden?

Hat es eine eindeutige Lösung?

Vom Gleichungssystem zur Lösung

Hat ein solches Gleichungssystem zwischen Mengen eine Lösung?
Das ist zu erwarten: wenn wir das Programm nacheinander mit jedem einzelnen Eingabewert ablaufen lassen und an jedem Programmpunkt A,. . . ,H die beobachteten Werte sammeln (daher "collecting semantics"), sollten wir sie finden.
Das geht aber nur, wenn die Eingabemenge endlich ist.

Wie können wir sie finden?

Hat es eine eindeutige Lösung?
Nein.
Auf der nächsten Folie werden mehrere Lösungen gezeigt.
Wir müssen uns klar werden, welche die "richtige" ist.

Vom Gleichungssystem zur Lösung

Hat ein solches Gleichungssystem zwischen Mengen eine Lösung?
Das ist zu erwarten: wenn wir das Programm nacheinander mit jedem einzelnen Eingabewert ablaufen lassen und an jedem Programmpunkt A,. . . ,H die beobachteten Werte sammeln (daher "collecting semantics"), sollten wir sie finden.
Das geht aber nur, wenn die Eingabemenge endlich ist.

Wie können wir sie finden?

Hat es eine eindeutige Lösung?
Nein.
Auf der nächsten Folie werden mehrere Lösungen gezeigt.
Wir müssen uns klar werden, welche die "richtige" ist.

Mehrere Lösungen

Gleichungssystem

$$
\begin{aligned}
A &= \{1, 2, 3, 4, 5\}\\
B &= A \cup G \cup H\\
C &= B \cap \{2, 3, 4, ...\}\\
D &= B \cap \{..., \text{-}2, \text{-}1, 0, 1\}\\
E &= C \cap \{..., \text{-}2, 0, 2, ...\}\\
F &= C \cap \{..., \text{-}1, 1, 3, ...\}\\
G &= \{n/2 \mid n \in E\}\\
H &= \{3 \cdot n + 1 \mid n \in F\}
\end{aligned}
$$

Mehrere Lösungen

Gleichungssystem

$$
\begin{aligned}
A &= \{1, 2, 3, 4, 5\} \\
B &= A \cup G \cup H \\
C &= B \cap \{2, 3, 4, ...\} \\
D &= B \cap \{..., \text{-}2, \text{-}1, 0, 1\} \\
E &= C \cap \{..., \text{-}2, 0, 2, ...\} \\
F &= C \cap \{..., \text{-}1, 1, 3, ...\} \\
G &= \{n/2 \mid n \in E\} \\
H &= \{3 \cdot n + 1 \mid n \in F\}
\end{aligned}
$$

Lösung 1

$$
\begin{aligned}
A &= \{1, 2, 3, 4, 5\} \\
B &= \{1, 2, 3, 4, 5, 8, 10, 16\} \\
C &= \{2, 3, 4, 5, 8, 10, 16\} \\
D &= \{1\} \\
E &= \{2, 4, 8, 10, 16\} \\
F &= \{3, 5\} \\
G &= \{1, 2, 4, 5, 8\} \\
H &= \{10, 16\}
\end{aligned}
$$

Mehrere Lösungen

Gleichungssystem

$$
\begin{aligned}
A &= \{1,2,3,4,5\} \\
B &= A \cup G \cup H \\
C &= B \cap \{2,3,4,...\} \\
D &= B \cap \{...,\text{-}2,\text{-}1,0,1\} \\
E &= C \cap \{...,\text{-}2,0,2,...\} \\
F &= C \cap \{...,\text{-}1,1,3,...\} \\
G &= \{n/2 \mid n \in E\} \\
H &= \{3 \cdot n + 1 \mid n \in F\}
\end{aligned}
$$

Lösung 2

$$
\begin{aligned}
A &= \{1,2,3,4,5\} \\
B &= \{1,2,3,4,5,8,10,16,32,64,128,256,...\} \\
C &= \{2,3,4,5,8,10,16,32,64,128,256,...\} \\
D &= \{1\} \\
E &= \{2,4,8,10,16,32,64,128,256,...\} \\
F &= \{3,5\} \\
G &= \{1,2,4,5,8,16,32,64,128,256,...\} \\
H &= \{10,16\}
\end{aligned}
$$

Mehrere Lösungen

Gleichungssystem

$A = \{1, 2, 3, 4, 5\}$
$B = A \cup G \cup H$
$C = B \cap \{2, 3, 4, ...\}$
$D = B \cap \{..., -2, -1, 0, 1\}$
$E = C \cap \{..., -2, 0, 2, ...\}$
$F = C \cap \{..., -1, 1, 3, ...\}$
$G = \{n/2 \mid n \in E\}$
$H = \{3 \cdot n + 1 \mid n \in F\}$

Lösung 2

$A = \{1, 2, 3, 4, 5\}$
$B = \{1, 2, 3, 4, 5, 8, 10, 16, 32, 64, 128, 256, ...\}$
$C = \{2, 3, 4, 5, 8, 10, 16, 32, 64, 128, 256, ...\}$
$D = \{1\}$
$E = \{2, 4, 8, 10, 16, 32, 64, 128, 256, ...\}$
$F = \{3, 5\}$
$G = \{1, 2, 4, 5, 8, 16, 32, 64, 128, 256, ...\}$
$H = \{10, 16\}$

Mehrere Lösungen

Gleichungssystem

$A = \{1, 2, 3, 4, 5\}$
$B = A \cup G \cup H$
$C = B \cap \{2, 3, 4, ...\}$
$D = B \cap \{..., -2, -1, 0, 1\}$
$E = C \cap \{..., -2, 0, 2, ...\}$
$F = C \cap \{..., -1, 1, 3, ...\}$
$G = \{n/2 \mid n \in E\}$
$H = \{3 \cdot n + 1 \mid n \in F\}$

Lösung 2

$A = \{1, 2, 3, 4, 5\}$
$B = \{1, 2, 3, 4, 5, 8, 10, 16, 32, 64, 128, 256, ...\}$
$C = \{2, 3, 4, 5, 8, 10, 16, 32, 64, 128, 256, ...\}$
$D = \{1\}$
$E = \{2, 4, 8, 10, 16, 32, 64, 128, 256, ...\}$
$F = \{3, 5\}$
$G = \{1, 2, 4, 5, 8, 16, 32, 64, 128, 256, ...\}$
$H = \{10, 16\}$

Mehrere Lösungen

Gleichungssystem

$$
\begin{aligned}
A &= \{1, 2, 3, 4, 5\} \\
B &= A \cup G \cup H \\
C &= B \cap \{2, 3, 4, \ldots\} \\
D &= B \cap \{\ldots, \text{-}2, \text{-}1, 0, 1\} \\
E &= C \cap \{\ldots, \text{-}2, 0, 2, \ldots\} \\
F &= C \cap \{\ldots, \text{-}1, 1, 3, \ldots\} \\
G &= \{n/2 \mid n \in E\} \\
H &= \{3 \cdot n + 1 \mid n \in F\}
\end{aligned}
$$

Lösung 2

$$
\begin{aligned}
A &= \{1, 2, 3, 4, 5\} \\
B &= \{1, 2, 3, 4, 5, 8, 10, 16, 32, 64, 128, 256, \ldots\} \\
C &= \{2, 3, 4, 5, 8, 10, 16, 32, 64, 128, 256, \ldots\} \\
D &= \{1\} \\
E &= \{2, 4, 8, 10, 16, 32, 64, 128, 256, \ldots\} \\
F &= \{3, 5\} \\
G &= \{1, 2, 4, 5, 8, 16, 32, 64, 128, 256, \ldots\} \\
H &= \{10, 16\}
\end{aligned}
$$

Mehrere Lösungen

Gleichungssystem

$A = \{1, 2, 3, 4, 5\}$
$B = A \cup G \cup H$
$C = B \cap \{2, 3, 4, ...\}$
$D = B \cap \{..., -2, -1, 0, 1\}$
$E = C \cap \{..., -2, 0, 2, ...\}$
$F = C \cap \{..., -1, 1, 3, ...\}$
$G = \{n/2 \mid n \in E\}$
$H = \{3 \cdot n + 1 \mid n \in F\}$

Lösung 2

$A = \{1, 2, 3, 4, 5\}$
$B = \{1, 2, 3, 4, 5, 8, 10, 16, 32, 64, 128, 256, ...\}$
$C = \{2, 3, 4, 5, 8, 10, 16, 32, 64, 128, 256, ...\}$
$D = \{1\}$
$E = \{2, 4, 8, 10, 16, 32, 64, 128, 256, ...\}$
$F = \{3, 5\}$
$G = \{1, 2, 4, 5, 8, 16, 32, 64, 128, 256, ...\}$
$H = \{10, 16\}$

Mehrere Lösungen

Gleichungssystem

$$
\begin{aligned}
A &= \{1,2,3,4,5\}\\
B &= A \cup G \cup H\\
C &= B \cap \{2,3,4,...\}\\
D &= B \cap \{...,\text{-}2,\text{-}1,0,1\}\\
E &= C \cap \{...,\text{-}2,0,2,...\}\\
F &= C \cap \{...,\text{-}1,1,3,...\}\\
G &= \{n/2 \mid n \in E\}\\
H &= \{3 \cdot n + 1 \mid n \in F\}
\end{aligned}
$$

Lösung 2

$$
\begin{aligned}
A &= \{1,2,3,4,5\}\\
B &= \{1,2,3,4,5,8,10,16,32,64,128,256,...\}\\
C &= \{2,3,4,5,8,10,16,32,64,128,256,...\}\\
D &= \{1\}\\
E &= \{2,4,8,10,16,32,64,128,256,...\}\\
F &= \{3,5\}\\
G &= \{1,2,4,5,8,16,32,64,128,256,...\}\\
H &= \{10,16\}
\end{aligned}
$$

Mehrere Lösungen

Gleichungssystem

$A = \{1, 2, 3, 4, 5\}$
$B = A \cup G \cup H$
$C = B \cap \{2, 3, 4, ...\}$
$D = B \cap \{..., \text{-}2, \text{-}1, 0, 1\}$
$E = C \cap \{..., \text{-}2, 0, 2, ...\}$
$F = C \cap \{..., \text{-}1, 1, 3, ...\}$
$G = \{n/2 \mid n \in E\}$
$H = \{3 \cdot n + 1 \mid n \in F\}$

Lösung 2

$A = \{1, 2, 3, 4, 5\}$
$B = \{1, 2, 3, 4, 5, 8, 10, 16, 32, 64, 128, 256, ...\}$
$C = \{2, 3, 4, 5, 8, 10, 16, 32, 64, 128, 256, ...\}$
$D = \{1\}$
$E = \{2, 4, 8, 10, 16, 32, 64, 128, 256, ...\}$
$F = \{3, 5\}$
$G = \{1, 2, 4, 5, 8, 16, 32, 64, 128, 256, ...\}$
$H = \{10, 16\}$

Mehrere Lösungen

Gleichungssystem

$A = \{1, 2, 3, 4, 5\}$
$B = A \cup G \cup H$
$C = B \cap \{2, 3, 4, ...\}$
$D = B \cap \{..., \text{-}2, \text{-}1, 0, 1\}$
$E = C \cap \{..., \text{-}2, 0, 2, ...\}$
$F = C \cap \{..., \text{-}1, 1, 3, ...\}$
$G = \{n/2 \mid n \in E\}$
$H = \{3 \cdot n + 1 \mid n \in F\}$

Lösung 2

$A = \{1, 2, 3, 4, 5\}$
$B = \{1, 2, 3, 4, 5, 8, 10, 16, 32, 64, 128, 256, ...\}$
$C = \{2, 3, 4, 5, 8, 10, 16, 32, 64, 128, 256, ...\}$
$D = \{1\}$
$E = \{2, 4, 8, 10, 16, 32, 64, 128, 256, ...\}$
$F = \{3, 5\}$
$G = \{1, 2, 4, 5, 8, 16, 32, 64, 128, 256, ...\}$
$H = \{10, 16\}$

Mehrere Lösungen

Gleichungssystem

$$
\begin{aligned}
A &= \{1,2,3,4,5\}\\
B &= A \cup G \cup H\\
C &= B \cap \{2,3,4,...\}\\
D &= B \cap \{...,\text{-}2,\text{-}1,0,1\}\\
E &= C \cap \{...,\text{-}2,0,2,...\}\\
F &= C \cap \{...,\text{-}1,1,3,...\}\\
G &= \{n/2 \mid n \in E\}\\
H &= \{3 \cdot n + 1 \mid n \in F\}
\end{aligned}
$$

Lösung 2

$$
\begin{aligned}
A &= \{1,2,3,4,5\}\\
B &= \{1,2,3,4,5,8,10,16,32,64,128,256,...\}\\
C &= \{2,3,4,5,8,10,16,32,64,128,256,...\}\\
D &= \{1\}\\
E &= \{2,4,8,10,16,32,64,128,256,...\}\\
F &= \{3,5\}\\
G &= \{1,2,4,5,8,16,32,64,128,256,...\}\\
H &= \{10,16\}
\end{aligned}
$$

Mehrere Lösungen

Gleichungssystem

$$
\begin{aligned}
A &= \{1,2,3,4,5\}\\
B &= A \cup G \cup H\\
C &= B \cap \{2,3,4,...\}\\
D &= B \cap \{...,\text{-}2,\text{-}1,0,1\}\\
E &= C \cap \{...,\text{-}2,0,2,...\}\\
F &= C \cap \{...,\text{-}1,1,3,...\}\\
G &= \{n/2 \mid n \in E\}\\
H &= \{3 \cdot n + 1 \mid n \in F\}
\end{aligned}
$$

Lösung 2

$$
\begin{aligned}
A &= \{1,2,3,4,5\}\\
B &= \{1,2,3,4,5,8,10,16,32,64,128,256,...\}\\
C &= \{2,3,4,5,8,10,16,32,64,128,256,...\}\\
D &= \{1\}\\
E &= \{2,4,8,10,16,32,64,128,256,...\}\\
F &= \{3,5\}\\
G &= \{1,2,4,5,8,16,32,64,128,256,...\}\\
H &= \{10,16\}
\end{aligned}
$$

Lösung 1 ist durch Programmausführung ermittelt worden.
Jede Lösung muß mindestens diese Werte enthalten, Lösung 1 ist die kleinste.
Bei Lösung 2 und 3 "zirkulieren" Werte in der Schleife, die nicht aus Eingabewerten entstanden sind.

Mehrere Lösungen

Gleichungssystem	Lösung 3
$A = \{1, 2, 3, 4, 5\}$	$A = \{1, 2, 3, 4, 5\}$
$B = A \cup G \cup H$	$B = \{1, 2, 3, ...\}$
$C = B \cap \{2, 3, 4, ...\}$	$C = \{2, 3, 4, ...\}$
$D = B \cap \{..., \text{-}2, \text{-}1, 0, 1\}$	$D = \{1\}$
$E = C \cap \{..., \text{-}2, 0, 2, ...\}$	$E = \{2, 4, 6, ...\}$
$F = C \cap \{..., \text{-}1, 1, 3, ...\}$	$F = \{3, 5, 7, ...\}$
$G = \{n/2 \mid n \in E\}$	$G = \{1, 2, 3, ...\}$
$H = \{3 \cdot n + 1 \mid n \in F\}$	$H = \{10, 16, 22, ...\}$

Lösung 1 ist durch Programmausführung ermittelt worden.
Jede Lösung muß mindestens diese Werte enthalten, Lösung 1 ist die kleinste.
Bei Lösung 2 und 3 “zirkulieren” Werte in der Schleife, die nicht aus Eingabewerten entstanden sind.

Mehrere Lösungen

Gleichungssystem	Lösung 3
$A = \{1, 2, 3, 4, 5\}$	$A = \{1, 2, 3, 4, 5\}$
$B = A \cup G \cup H$	$B = \{1, 2, 3, ...\}$
$C = B \cap \{2, 3, 4, ...\}$	$C = \{2, 3, 4, ...\}$
$D = B \cap \{..., \text{-}2, \text{-}1, 0, 1\}$	$D = \{1\}$
$E = C \cap \{..., \text{-}2, 0, 2, ...\}$	$E = \{2, 4, 6, ...\}$
$F = C \cap \{..., \text{-}1, 1, 3, ...\}$	$F = \{3, 5, 7, ...\}$
$G = \{n/2 \mid n \in E\}$	$G = \{1, 2, 3, ...\}$
$H = \{3 \cdot n + 1 \mid n \in F\}$	$H = \{10, 16, 22, ...\}$

Lösung 1 ist durch Programmausführung ermittelt worden.
Jede Lösung muß mindestens diese Werte enthalten, Lösung 1 ist die kleinste.
Bei Lösung 2 und 3 “zirkulieren” Werte in der Schleife, die nicht aus Eingabewerten entstanden sind.

Mehrere Lösungen

Gleichungssystem	Lösung 3
$A = \{1,2,3,4,5\}$	$A = \{1,2,3,4,5\}$
$B = A \cup G \cup H$	$B = \{1,2,3,...\}$
$C = B \cap \{2,3,4,...\}$	$C = \{2,3,4,...\}$
$D = B \cap \{...,\text{-}2,\text{-}1,0,1\}$	$D = \{1\}$
$E = C \cap \{...,\text{-}2,0,2,...\}$	$E = \{2,4,6,...\}$
$F = C \cap \{...,\text{-}1,1,3,...\}$	$F = \{3,5,7,...\}$
$G = \{n/2 \mid n \in E\}$	$G = \{1,2,3,...\}$
$H = \{3 \cdot n + 1 \mid n \in F\}$	$H = \{10,16,22,...\}$

Lösung 1 ist durch Programmausführung ermittelt worden.
Jede Lösung muß mindestens diese Werte enthalten, Lösung 1 ist die kleinste.
Bei Lösung 2 und 3 “zirkulieren” Werte in der Schleife, die nicht aus Eingabewerten entstanden sind.

Mehrere Lösungen

Gleichungssystem	Lösung 3
$A = \{1, 2, 3, 4, 5\}$	$A = \{1, 2, 3, 4, 5\}$
$B = A \cup G \cup H$	$B = \{1, 2, 3, ...\}$
$C = B \cap \{2, 3, 4, ...\}$	$C = \{2, 3, 4, ...\}$
$D = B \cap \{..., -2, -1, 0, 1\}$	$D = \{1\}$
$E = C \cap \{..., -2, 0, 2, ...\}$	$E = \{2, 4, 6, ...\}$
$F = C \cap \{..., -1, 1, 3, ...\}$	$F = \{3, 5, 7, ...\}$
$G = \{n/2 \mid n \in E\}$	$G = \{1, 2, 3, ...\}$
$H = \{3 \cdot n + 1 \mid n \in F\}$	$H = \{10, 16, 22, ...\}$

Lösung 1 ist durch Programmausführung ermittelt worden.
Jede Lösung muß mindestens diese Werte enthalten, Lösung 1 ist die kleinste.
Bei Lösung 2 und 3 “zirkulieren” Werte in der Schleife, die nicht aus Eingabewerten entstanden sind.

Mehrere Lösungen

Gleichungssystem	Lösung 3
$A = \{1,2,3,4,5\}$	$A = \{1,2,3,4,5\}$
$B = A \cup G \cup H$	$B = \{1,2,3,...\}$
$C = B \cap \{2,3,4,...\}$	$C = \{2,3,4,...\}$
$D = B \cap \{...,\text{-}2,\text{-}1,0,1\}$	$D = \{1\}$
$E = C \cap \{...,\text{-}2,0,2,...\}$	$E = \{2,4,6,...\}$
$F = C \cap \{...,\text{-}1,1,3,...\}$	$F = \{3,5,7,...\}$
$G = \{n/2 \mid n \in E\}$	$G = \{1,2,3,...\}$
$H = \{3 \cdot n + 1 \mid n \in F\}$	$H = \{10,16,22,...\}$

Lösung 1 ist durch Programmausführung ermittelt worden.
Jede Lösung muß mindestens diese Werte enthalten, Lösung 1 ist die kleinste.
Bei Lösung 2 und 3 “zirkulieren” Werte in der Schleife, die nicht aus Eingabewerten entstanden sind.

Mehrere Lösungen

Gleichungssystem	Lösung 3
$A = \{1, 2, 3, 4, 5\}$	$A = \{1, 2, 3, 4, 5\}$
$B = A \cup G \cup H$	$B = \{1, 2, 3, ...\}$
$C = B \cap \{2, 3, 4, ...\}$	$C = \{2, 3, 4, ...\}$
$D = B \cap \{..., \text{-}2, \text{-}1, 0, 1\}$	$D = \{1\}$
$E = C \cap \{..., \text{-}2, 0, 2, ...\}$	$E = \{2, 4, 6, ...\}$
$F = C \cap \{..., \text{-}1, 1, 3, ...\}$	$F = \{3, 5, 7, ...\}$
$G = \{n/2 \mid n \in E\}$	$G = \{1, 2, 3, ...\}$
$H = \{3 \cdot n + 1 \mid n \in F\}$	$H = \{10, 16, 22, ...\}$

Lösung 1 ist durch Programmausführung ermittelt worden.
Jede Lösung muß mindestens diese Werte enthalten, Lösung 1 ist die kleinste.
Bei Lösung 2 und 3 “zirkulieren” Werte in der Schleife, die nicht aus Eingabewerten entstanden sind.

Mehrere Lösungen

Gleichungssystem	Lösung 3
$A = \{1, 2, 3, 4, 5\}$	$A = \{1, 2, 3, 4, 5\}$
$B = A \cup G \cup H$	$B = \{1, 2, 3, ...\}$
$C = B \cap \{2, 3, 4, ...\}$	$C = \{2, 3, 4, ...\}$
$D = B \cap \{..., \text{-}2, \text{-}1, 0, 1\}$	$D = \{1\}$
$E = C \cap \{..., \text{-}2, 0, 2, ...\}$	$E = \{2, 4, 6, ...\}$
$F = C \cap \{..., \text{-}1, 1, 3, ...\}$	$F = \{3, 5, 7, ...\}$
$G = \{n/2 \mid n \in E\}$	$G = \{1, 2, 3, ...\}$
$H = \{3 \cdot n + 1 \mid n \in F\}$	$H = \{10, 16, 22, ...\}$

Lösung 1 ist durch Programmausführung ermittelt worden.
Jede Lösung muß mindestens diese Werte enthalten, Lösung 1 ist die kleinste.
Bei Lösung 2 und 3 “zirkulieren” Werte in der Schleife, die nicht aus Eingabewerten entstanden sind.

Mehrere Lösungen

Gleichungssystem	Lösung 3
$A = \{1,2,3,4,5\}$	$A = \{1,2,3,4,5\}$
$B = A \cup G \cup H$	$B = \{1,2,3,...\}$
$C = B \cap \{2,3,4,...\}$	$C = \{2,3,4,...\}$
$D = B \cap \{..., \text{-}2, \text{-}1, 0, 1\}$	$D = \{1\}$
$E = C \cap \{..., \text{-}2, 0, 2, ...\}$	$E = \{2,4,6,...\}$
$F = C \cap \{..., \text{-}1, 1, 3, ...\}$	$F = \{3,5,7,...\}$
$G = \{n/2 \mid n \in E\}$	$G = \{1,2,3,...\}$
$H = \{3 \cdot n + 1 \mid n \in F\}$	$H = \{10,16,22,...\}$

Lösung 1 ist durch Programmausführung ermittelt worden.
Jede Lösung muß mindestens diese Werte enthalten, Lösung 1 ist die kleinste.
Bei Lösung 2 und 3 “zirkulieren” Werte in der Schleife, die nicht aus Eingabewerten entstanden sind.

Mehrere Lösungen

Gleichungssystem	Lösung 3
$A = \{1, 2, 3, 4, 5\}$	$A = \{1, 2, 3, 4, 5\}$
$B = A \cup G \cup H$	$B = \{1, 2, 3, ...\}$
$C = B \cap \{2, 3, 4, ...\}$	$C = \{2, 3, 4, ...\}$
$D = B \cap \{..., \text{-}2, \text{-}1, 0, 1\}$	$D = \{1\}$
$E = C \cap \{..., \text{-}2, 0, 2, ...\}$	$E = \{2, 4, 6, ...\}$
$F = C \cap \{..., \text{-}1, 1, 3, ...\}$	$F = \{3, 5, 7, ...\}$
$G = \{n/2 \mid n \in E\}$	$G = \{1, 2, 3, ...\}$
$H = \{3 \cdot n + 1 \mid n \in F\}$	$H = \{10, 16, 22, ...\}$

Lösung 1 ist durch Programmausführung ermittelt worden.
Jede Lösung muß mindestens diese Werte enthalten, Lösung 1 ist die kleinste.
Bei Lösung 2 und 3 "zirkulieren" Werte in der Schleife, die nicht aus Eingabewerten entstanden sind.

Mehrere Lösungen

Gleichungssystem

$$
\begin{aligned}
A &= \{1,2,3,4,5\}\\
B &= A \cup G \cup H\\
C &= B \cap \{2,3,4,...\}\\
D &= B \cap \{...,\text{-}2,\text{-}1,0,1\}\\
E &= C \cap \{...,\text{-}2,0,2,...\}\\
F &= C \cap \{...,\text{-}1,1,3,...\}\\
G &= \{n/2 \mid n \in E\}\\
H &= \{3 \cdot n + 1 \mid n \in F\}
\end{aligned}
$$

Lösung 1 ist durch Programmausführung ermittelt worden.
Jede Lösung muß mindestens diese Werte enthalten, Lösung 1 ist die kleinste.
Bei Lösung 2 und 3 “zirkulieren” Werte in der Schleife, die nicht aus Eingabewerten entstanden sind.

Mehrere Lösungen

Gleichungssystem

$$
\begin{aligned}
A &= \{1, 2, 3, 4, 5\} \\
B &= A \cup G \cup H \\
C &= B \cap \{2, 3, 4, ...\} \\
D &= B \cap \{..., \text{-}2, \text{-}1, 0, 1\} \\
E &= C \cap \{..., \text{-}2, 0, 2, ...\} \\
F &= C \cap \{..., \text{-}1, 1, 3, ...\} \\
G &= \{n/2 \mid n \in E\} \\
H &= \{3 \cdot n + 1 \mid n \in F\}
\end{aligned}
$$

Lösung 3

$$
\begin{aligned}
A &= \{1, 2, 3, 4, 5\} \\
B &= \{1, 2, 3, 4, 5, 8, 10, 16, 32, 64, 128, 256, ...\} \\
C &= \{2, 3, 4, 5, 8, 10, 16, 32, 64, 128, 256, ...\} \\
D &= \{1\} \\
E &= \{2, 4, 8, 10, 16, 32, 64, 128, 256, ...\} \\
F &= \{3, 5, 7, ...\} \\
G &= \{1, 2, 4, 5, 8, 16, 32, 64, 128, 256, ...\} \\
H &= \{10, 16, 22, ...\}
\end{aligned}
$$

Lösung 1 ist durch Programmausführung ermittelt worden.
Jede Lösung muß mindestens diese Werte enthalten, Lösung 1 ist die kleinste.
Bei Lösung 2 und 3 "zirkulieren" Werte in der Schleife, die nicht aus Eingabewerten entstanden sind.

Vom Gleichungssystem zur kleinsten Lösung

Wie können wir nun die kleinste Lösung finden?

Vom Gleichungssystem zur kleinsten Lösung

Wie können wir nun die kleinste Lösung finden?

Wir können einen Fixpunktsatz aus der Verbandstheorie verwenden.

Vom Gleichungssystem zur kleinsten Lösung

Wie können wir nun die kleinste Lösung finden?

Wir können einen Fixpunktsatz aus der Verbandstheorie verwenden.

Dazu formen wir das Gleichungssystem in einen Operator Φ um, so daß jeder Fixpunkt von Φ, d.h. jedes $\langle A, \ldots, H \rangle$ mit $\Phi(\langle A, \ldots, H \rangle) = \langle A, \ldots, H \rangle$ eine Lösung des Gleichungssystems ist.

Vom Gleichungssystem zur kleinsten Lösung

Wie können wir nun die kleinste Lösung finden?

Wir können einen Fixpunktsatz aus der Verbandstheorie verwenden.

Dazu formen wir das Gleichungssystem in einen Operator Φ um, so daß jeder Fixpunkt von Φ, d.h. jedes $\langle A, \ldots, H \rangle$ mit $\Phi(\langle A, \ldots, H \rangle) = \langle A, \ldots, H \rangle$ eine Lösung des Gleichungssystems ist.

Zunächst: vom Gleichungssystem zum Operator

Gleichungssystem

$$
\begin{array}{lcl}
A & = & \{1, 2, 3, 4, 5\} \\
B & = & A \cup G \cup H \\
C & = & B \cap \{2, 3, 4, \ldots\} \\
D & = & B \cap \{\ldots, -2, -1, 0, 1\} \\
E & = & C \cap \{\ldots, -4, -2, 0, 2, 4, \ldots\} \\
F & = & C \cap \{\ldots, -3, -1, 1, 3, \ldots\} \\
G & = & \{n/2 \mid n \in E\} \\
H & = & \{3 \cdot n + 1 \mid n \in F\}
\end{array}
$$

Operator

$\Phi : \wp(\boldsymbol{Z})^8 \longrightarrow \wp(\boldsymbol{Z})^8$,

$\Phi(\langle A, B, C, D, E, F, G, H \rangle) =$

$$
\begin{array}{lll}
\langle & \{1,2,3,4,5\} & , \\
& A \cup G \cup H & , \\
& B \cap \{2,3,4,\ldots\} & , \\
& B \cap \{\ldots,-2,-1,0,1\} & , \\
& C \cap \{\ldots,-4,-2,0,2,4,\ldots\} & , \\
& C \cap \{\ldots,-3,-1,1,3,\ldots\} & , \\
& \{n/2 \mid n \in E\} & , \\
& \{3 \cdot n + 1 \mid n \in F\} & \rangle
\end{array}
$$

Fixpunkt ist Lösung

$$\Phi(\langle A, B, C, D, E, F, G, H \rangle) = \langle A, B, C, D, E, F, G, H \rangle \Leftrightarrow$$

$$\begin{array}{lcll}
A & = & \{1, 2, 3, 4, 5\} & \wedge \\
B & = & A \cup G \cup H & \wedge \\
C & = & B \cap \{2, 3, 4, \ldots\} & \wedge \\
D & = & B \cap \{\ldots, -2, -1, 0, 1\} & \wedge \\
E & = & C \cap \{\ldots, -4, -2, 0, 2, 4, \ldots\} & \wedge \\
F & = & C \cap \{\ldots, -3, -1, 1, 3, \ldots\} & \wedge \\
G & = & \{n/2 \mid n \in E\} & \wedge \\
H & = & \{3 \cdot n + 1 \mid n \in F\} &
\end{array}$$

$$
\begin{aligned}
\Phi(\langle A, B, C, D, E, F, G, H\rangle) = \langle A, B, C, D, E, F, G, H\rangle \Leftrightarrow \\
& \{1, 2, 3, 4, 5\} && \wedge \\
& A \cup G \cup H && \wedge \\
& B \cap \{2, 3, 4, \ldots\} && \wedge \\
& B \cap \{\ldots, -2, -1, 0, 1\} && \wedge \\
& C \cap \{\ldots, -4, -2, 0, 2, 4, \ldots\} && \wedge \\
& C \cap \{\ldots, -3, -1, 1, 3, \ldots\} && \wedge \\
& \{n/2 \mid n \in E\} && \wedge \\
& \{3 \cdot n + 1 \mid n \in F\}
\end{aligned}
$$

Zunächst: vom Gleichungssystem zum Operator

Gleichungssystem
Operator
Fixpunkt ist Lösung

$\Phi : \wp(\boldsymbol{Z})^8 \longrightarrow \wp(\boldsymbol{Z})^8,$

$\Phi(\langle A, B, C, D, E, F, G, H\rangle) = \langle A, B, C, D, E, F, G, H\rangle \Leftrightarrow$

$$
\begin{array}{lcll}
\langle A & = & \{1, 2, 3, 4, 5\} & , \wedge \\
B & = & A \cup G \cup H & , \wedge \\
C & = & B \cap \{2, 3, 4, \ldots\} & , \wedge \\
D & = & B \cap \{\ldots, -2, -1, 0, 1\} & , \wedge \\
E & = & C \cap \{\ldots, -4, -2, 0, 2, 4, \ldots\} & , \wedge \\
F & = & C \cap \{\ldots, -3, -1, 1, 3, \ldots\} & , \wedge \\
G & = & \{n/2 \mid n \in E\} & , \wedge \\
H & = & \{3 \cdot n + 1 \mid n \in F\} & \rangle
\end{array}
$$

Programme mit mehreren Variablen

Treten mehrere Variablen im Programm auf, wird Φ entsprechend komplizierter, z.B. $\Phi : \wp(\boldsymbol{Z}^3)^8 \longrightarrow \wp(\boldsymbol{Z}^3)^8$ für 3 Variablen und 8 Programmstellen.

Z.B. `y=x*y-2;` führt zu
$\Phi(\langle A, \ldots, H \rangle) = \langle \ldots, \{\langle x, x \cdot y - 2 \rangle \mid \langle x, y \rangle \in E\}, \ldots \rangle$.

Z.B. `if(x<y+1)` führt zu
$\Phi(\langle A, \ldots, H \rangle) = \langle \ldots, B \cap \{\langle x, y \rangle \mid x, y \in \boldsymbol{Z} \wedge x < y + 1\}, \ldots \rangle$.

Der Fixpunktsatz

Sei M mit $(\sqsubseteq)$ ein vollständiger Verband und $\Phi : M \longrightarrow M$ eine monotone und stetige Abbildung.
Dann hat Φ einen kleinsten Fixpunkt $X \in M$, nämlich
$X = \bigsqcup \{\perp,\ \Phi(\perp),\ \Phi(\Phi(\perp)),\ \Phi(\Phi(\Phi(\perp))), \ldots\}$.

Der Fixpunktsatz

Sei M mit $(\sqsubseteq)$ ein vollständiger Verband und $\Phi : M \longrightarrow M$ eine monotone und stetige Abbildung.
Dann hat Φ einen kleinsten Fixpunkt $X \in M$, nämlich
$X = \bigsqcup \{\perp,\ \Phi(\perp),\ \Phi(\Phi(\perp)),\ \Phi(\Phi(\Phi(\perp))), \ldots\}$.

Um diesen Satz verstehen und anwenden zu können, benötigen wir einige formale Definitionen.

Der Fixpunktsatz

Sei M mit $(\sqsubseteq)$ ein vollständiger Verband und $\Phi : M \longrightarrow M$ eine monotone und stetige Abbildung.
Dann hat Φ einen kleinsten Fixpunkt $X \in M$, nämlich
$X = \bigsqcup \{\perp,\ \Phi(\perp),\ \Phi(\Phi(\perp)),\ \Phi(\Phi(\Phi(\perp))), \ldots\}$.

Um diesen Satz verstehen und anwenden zu können, benötigen wir einige formale Definitionen.

Ordnung

Sei M eine Menge.

Eine Relation $(\sqsubseteq) \subseteq M \times M$ heißt *Ordnungsrelation* auf M,
wenn für alle $x, y, z \in M$ gilt:

$x \sqsubseteq x$	(Reflexivität)
$x \sqsubseteq y \wedge y \sqsubseteq x \Rightarrow x = y$	(Antisymmetrie)
$x \sqsubseteq y \wedge y \sqsubseteq z \Rightarrow x \sqsubseteq z$	(Transitivität).

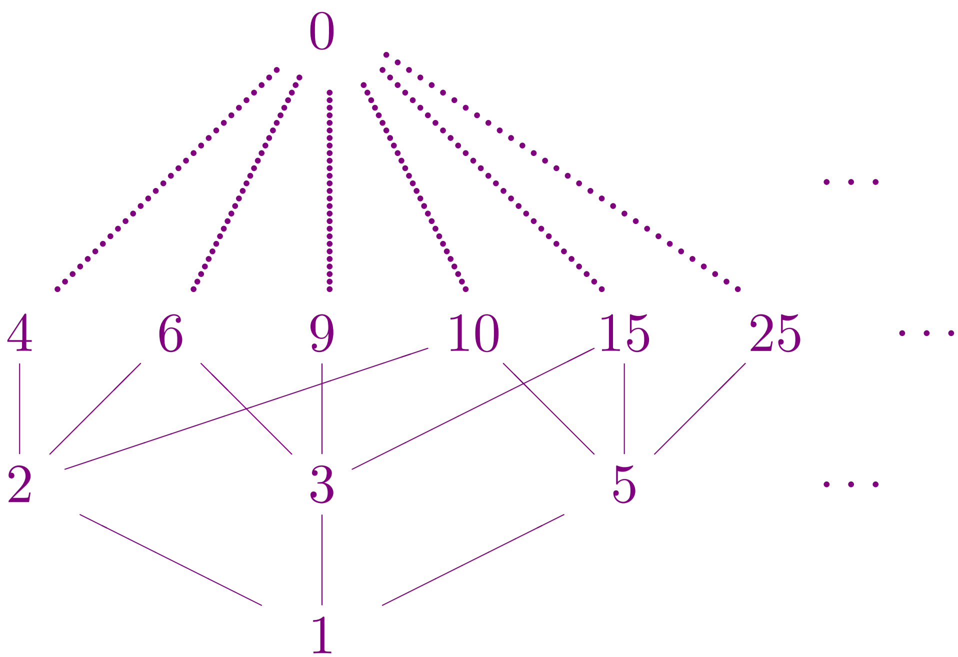
Beispiele . . .

. . . aus der Analysis:

$\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, jeweils mit dem üblichen $(\leq)$

Beispiele . . .

. . . aus der Zahlentheorie:



$\mathbb{N}$ mit “x ist Teiler von y” $(x \mid y)$

Das Beispiel zeigt: nicht alle Elemente müssen miteinander vergleichbar sein.

Beispiele . . .

. . . aus der Mengenlehre:

$\wp(I\!N)$ mit $A_1 \sqsubseteq A_2 \Leftrightarrow A_1 \subseteq A_2$

. . . im Hinblick auf unsere Anwendung:

$\wp(\boldsymbol{Z})^8$ mit $\langle A_1, \ldots, H_1 \rangle \sqsubseteq \langle A_2, \ldots, H_2 \rangle \Leftrightarrow A_1 \subseteq A_2 \wedge \ldots \wedge H_1 \subseteq H_2$

Z.B. $\langle \{\}, \{1\}, \{\}, \{\}, \{\}, \{\}, \{3,5\}, \{\} \rangle \sqsubseteq \langle \{\}, \boldsymbol{Z}, \{\}, \{\}, \{\}, \{\}, \{3,4,5\}, \{\} \rangle$

Schranke

Ein Element $x \in M$ heißt *obere Schranke* einer Teilmenge $S \subseteq M$, wenn $s \sqsubseteq x$ für alle $s \in S$.

x heißt *kleinste obere Schranke* von S, wenn $x \sqsubseteq x'$ für jede obere Schranke x' von S.

Analog wird "*untere Schranke*" und "*größte untere Schranke*" definiert.

Beispiele

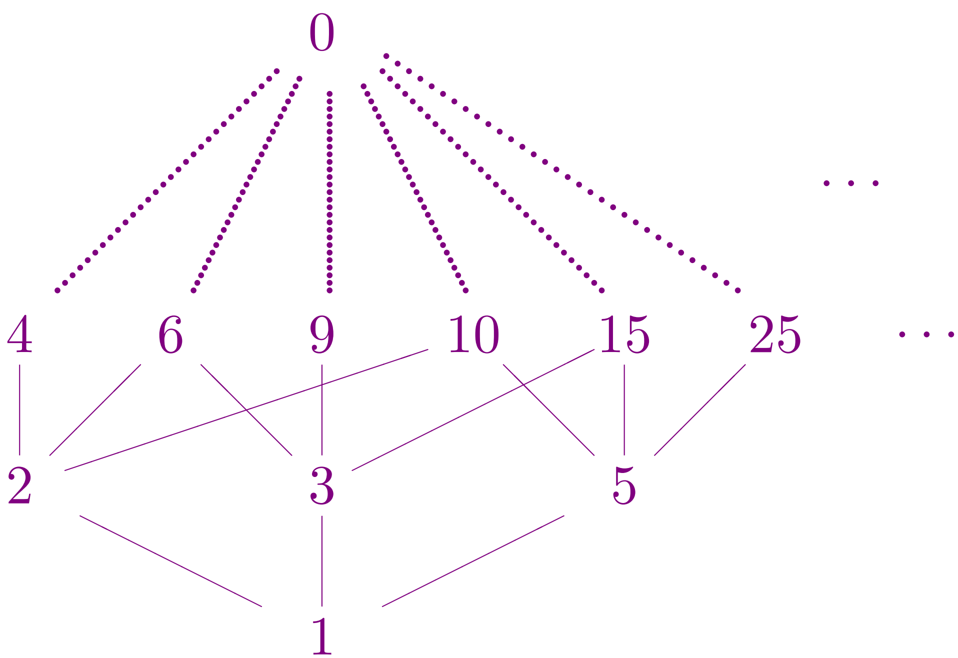
$1.42 \in \mathbb{Q}$ ist eine obere Schranke der Menge $\{x \in \mathbb{Q} \mid x \cdot x \leq 2\}$.

$1.415 \in \mathbb{Q}$ ist eine kleinere.

Es gibt in $\mathbb{Q}$ keine kleinste.

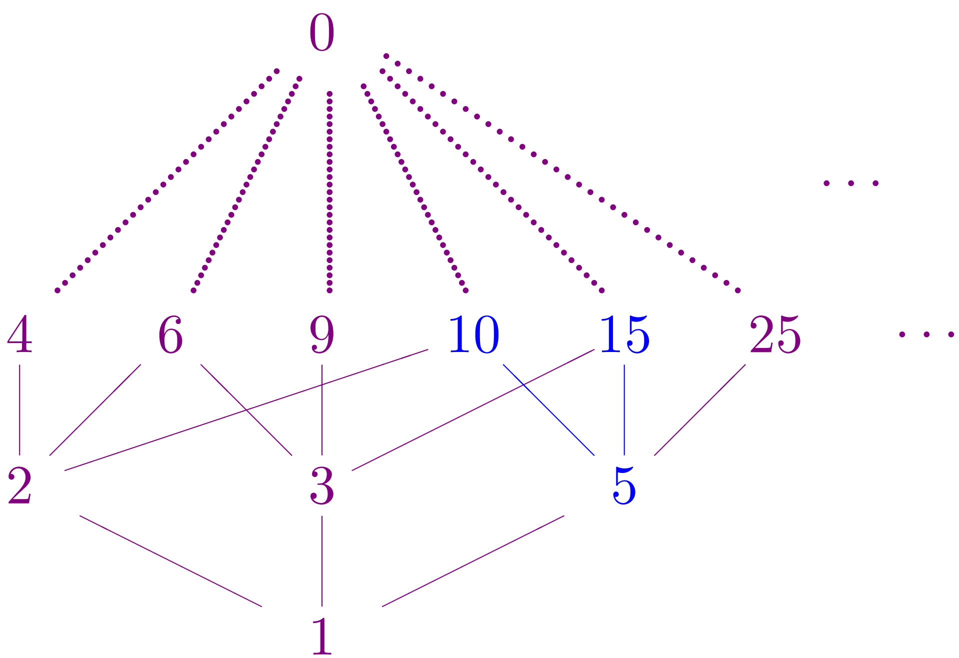
In $\mathbb{R}$ gibt es eine kleinste obere Schranke
nämlich $\sqrt{2} \in \mathbb{R}$.

Beispiele



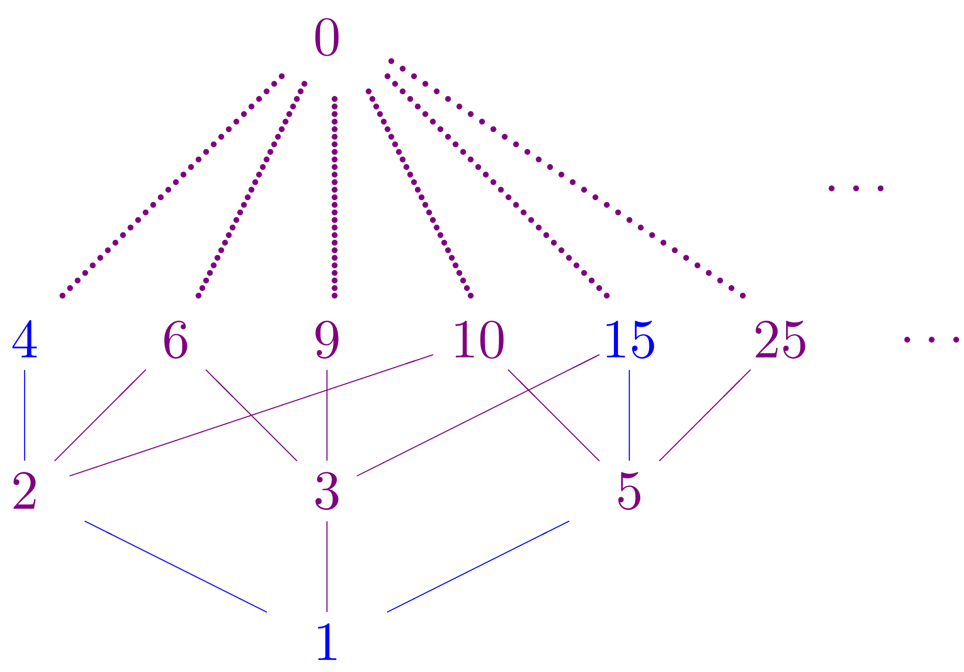
$ggT(x,y)$ bzw. $kgV(x,y)$ ist die größte untere bzw. kleinste obere Schranke von $\{x,y\}$ bzgl. $I\!N$ mit $(|)$.

Beispiele



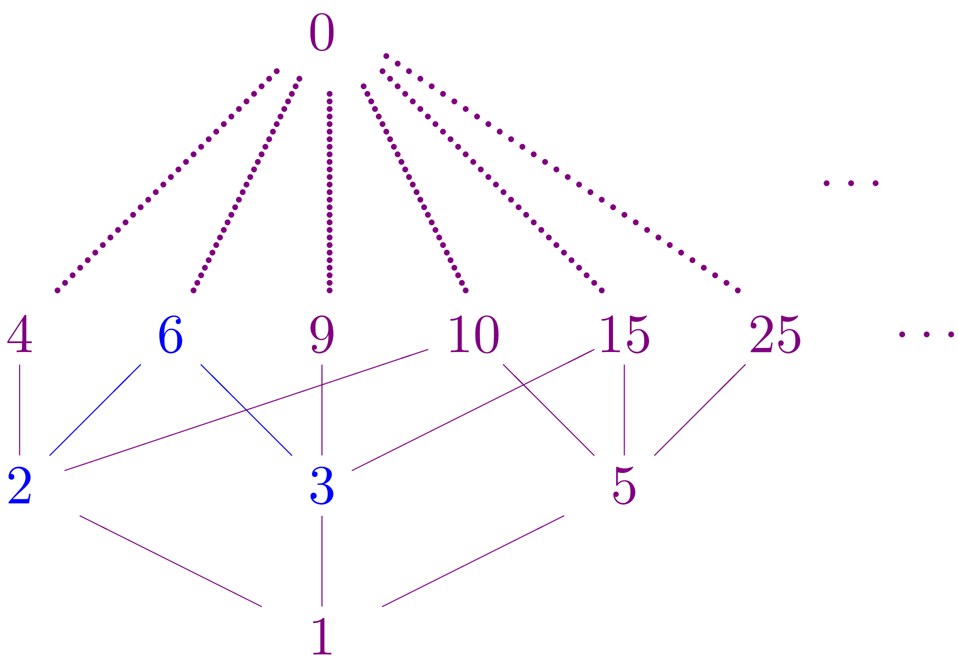
$ggT(x,y)$ bzw. $kgV(x,y)$ ist die größte untere bzw. kleinste obere Schranke von $\{x,y\}$ bzgl. $I\!N$ mit $(|)$.

Beispiele



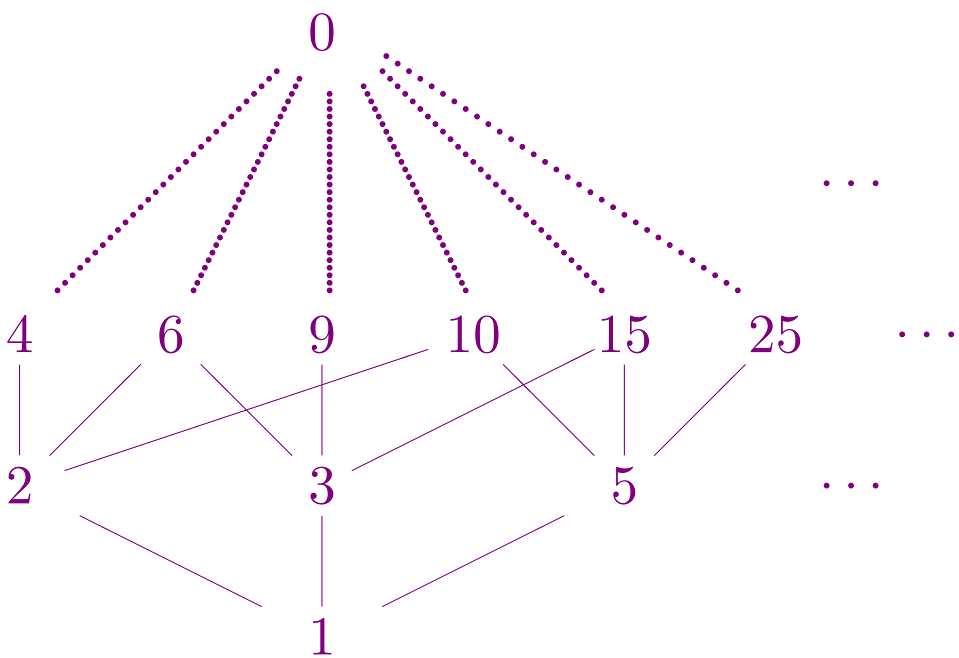
$ggT(x, y)$ bzw. $kgV(x, y)$ ist die größte untere bzw. kleinste obere Schranke von $\{x, y\}$ bzgl. $\mathbb{N}$ mit $(|)$.

Beispiele



$ggT(x, y)$ bzw. $kgV(x, y)$ ist die größte untere bzw. kleinste obere Schranke von $\{x, y\}$ bzgl. $I\!N$ mit $(|)$.

Beispiele



$ggT(x, y)$ bzw. $kgV(x, y)$ ist die größte untere bzw. kleinste obere Schranke von $\{x, y\}$ bzgl. $I\!N$ mit $(|)$.

Beispiele

$A_1 \cup \ldots \cup A_n$ bzw. $A_1 \cap \ldots \cap A_n$ ist kleinste obere bzw. größte untere Schranke von $\{A_1, \ldots, A_n\}$.

$\langle A_1 \cup A_2, \ldots, H_1 \cup H_2 \rangle$ bzw. $\langle A_1 \cap A_2, \ldots, H_1 \cap H_2 \rangle$ ist kleinste obere bzw. größte untere Schranke von $\{\langle A_1, \ldots, H_1 \rangle, \langle A_2, \ldots, H_2 \rangle\}$.

Verband

Die Menge M mit der Ordnungsrelation $(\sqsubseteq)$ heißt *vollständiger Verband*, wenn für alle $S \subseteq M$ stets die kleinste obere und die größte untere Schranke von S existiert.

Wir schreiben $\bigsqcup S$ bzw. $\bigsqcap S$ für die kleinste obere bzw. größte untere Schranke von S.

Wir schreiben $\perp$ bzw. $\top$ für $\bigsqcup M$ bzw. $\bigsqcap M$,
also für das kleinste bzw. größte Element in M überhaupt.

Beispiele für vollständige Verbände

$\mathbb{Z} \cup \{-\infty, +\infty\}$ und $\mathbb{R} \cup \{-\infty, +\infty\}$, jeweils mit dem üblichen $(\leq)$
$\top$ entspricht $+\infty$, $\bot$ entspricht $-\infty$

$\mathbb{N}$ mit "ist Teiler von" (z.B. $\bigsqcup\{1, 3, 5, 7, 9, 11, \ldots\} = 0$)

$\wp(\mathbb{Z})$
$\top$ entspricht $\mathbb{Z}$,
$\bot$ entspricht $\{\}$,
$\bigsqcup S$ entspricht $\bigcup S$,
$\bigsqcap S$ entspricht $\bigcap S$

$\wp(\mathbb{Z})^8$
$\top$ entspricht $\langle \mathbb{Z}, \ldots, \mathbb{Z} \rangle$,
$\bot$ entspricht $\langle \{\}, \ldots, \{\} \rangle$

Keine vollständigen Verbände sind:

$\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$
(haben kein größtes Element)

$\mathbb{Q} \cup \{-\infty, +\infty\}$
($\{x \in \mathbb{Q} \mid x \cdot x \leq 2\}$ hat keine kleinste obere Schranke)

Monotone Abbildung

Seien M mit $(\sqsubseteq)$ sowie M' mit $(\sqsubseteq')$ vollständige Verbände.

Eine Abbildung $\Phi : M \longrightarrow M'$ heißt *monoton*,
wenn $x \sqsubseteq y \Rightarrow \Phi(x) \sqsubseteq' \Phi(y)$ für alle $x, y \in M$.

Beispiele

$f : \mathbb{R} \cup \{-\infty, +\infty\} \longrightarrow \mathbb{R} \cup \{-\infty, +\infty\}$
ist monoton (in unserem Sinne)
genau dann, wenn f monoton wachsend im Sinne der Analysis ist.

$f : \mathbb{N} \longrightarrow \mathbb{N}$ mit $f(x) = x \cdot x$ ist monoton (bzgl. "ist Teiler von").

$f(x) = x + 1$ ist nicht monoton,
denn $6 \sqsubseteq 24$, aber $f(6) = 7 \not\sqsubseteq 25 = f(24)$.

Beispiele

$f : \wp(\boldsymbol{Z}) \longrightarrow \wp(\boldsymbol{Z})$ mit $f(A) = A \cup \{1, 2, 3\}$ ist monoton (bzgl. $(\subseteq)$).

$f(A) = A \cap \{1, 2, 3\}$ ist monoton.

$f(A) = \{10 - a \mid a \in A\}$ ist monoton,
z.B. ist $\{-1, 10\} \sqsubseteq \{-1, 10, 100\}$ und
$f(\{-1, 10\}) = \{11, 0\} \sqsubseteq \{11, 0, -90\} = f(\{-1, 10, 100\})$.

$f(A) = \boldsymbol{Z} \setminus A$ ist nicht monoton, denn $\{\} \sqsubseteq \boldsymbol{Z}$, aber $f(\{\}) = \boldsymbol{Z} \not\sqsubseteq \{\} = f(\boldsymbol{Z})$.

$\Phi : \wp(\boldsymbol{Z})^8 \longrightarrow \wp(\boldsymbol{Z})^8$ aus dem "collecting semantics"–Beispiel ist monoton.

Stetige Abbildung

Eine Abbildung $\Phi : M \longrightarrow M'$ heißt *stetig*,
wenn $\Phi(\bigsqcup S) = \bigsqcup' \{\Phi(s) \mid s \in S\}$ für jede Teilmenge $S \subseteq M$.

Beispiele

$f : \boldsymbol{R} \cup \{-\infty, +\infty\} \longrightarrow \boldsymbol{R} \cup \{-\infty, +\infty\}$ ist stetig (in unserem Sinn), wenn $f(sup(S)) = sup(\{f(x) \mid x \in S\})$

Unser $\Phi : \wp(\boldsymbol{Z})^8 \longrightarrow \wp(\boldsymbol{Z})^8$ aus dem "collecting semantics"–Beispiel ist stetig.

Allgemeiner: jedes Φ, das nur mit Hilfe von $(\cup)$, $(\cap)$ und $\{f(x) \mid x \in \ldots\}$ definiert wurde, ist stetig.
Insbesondere ist daher jedes Φ, das einem Mengengleichungssystem für ein imperatives Programm entspricht, stetig.

Nochmal: Fixpunktsatz

Sei M mit $(\sqsubseteq)$ ein vollständiger Verband
und $\Phi : M \longrightarrow M$ eine monotone und stetige Abbildung.
Dann hat Φ einen kleinsten Fixpunkt $X \in M$, nämlich
$X = \bigsqcup \; \{\perp,\ \Phi(\perp),\ \Phi(\Phi(\perp)),\ \Phi(\Phi(\Phi(\perp))), \ldots\}$.

Nochmal: Fixpunktsatz

Sei M mit $(\sqsubseteq)$ ein vollständiger Verband
und $\Phi : M \longrightarrow M$ eine monotone und stetige Abbildung.
Dann hat Φ einen kleinsten Fixpunkt $X \in M$, nämlich
$X = \bigsqcup \{\bot,\ \Phi(\bot),\ \Phi(\Phi(\bot)),\ \Phi(\Phi(\Phi(\bot))), \ldots\}$.

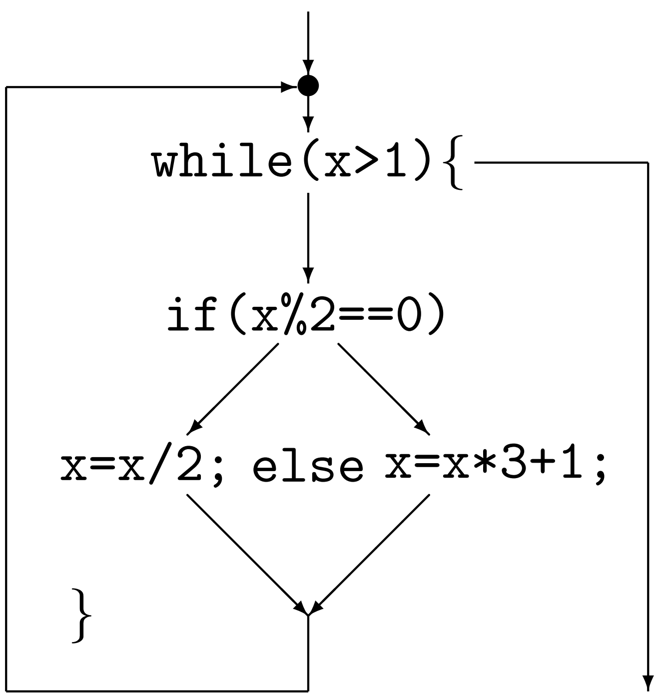
Da unser $M = \wp(\boldsymbol{Z})^8$ vollständiger Verband
und unser $\Phi : \wp(\boldsymbol{Z})^8 \longrightarrow \wp(\boldsymbol{Z})^8$ monotone und stetige Abbildung ist,
können wir den Satz anwenden.
Der Fixpunkt X hat die Form $\langle A, \ldots, H \rangle$;
er ist eine Lösung des ursprünglichen Mengen–Gleichungssystems.

Nochmal: Fixpunktsatz

Sei M mit $(\sqsubseteq)$ ein vollständiger Verband
und $\Phi : M \longrightarrow M$ eine monotone und stetige Abbildung.
Dann hat Φ einen kleinsten Fixpunkt $X \in M$, nämlich
$X = \bigsqcup \{\bot,\ \Phi(\bot),\ \Phi(\Phi(\bot)),\ \Phi(\Phi(\Phi(\bot))), \ldots\}$.

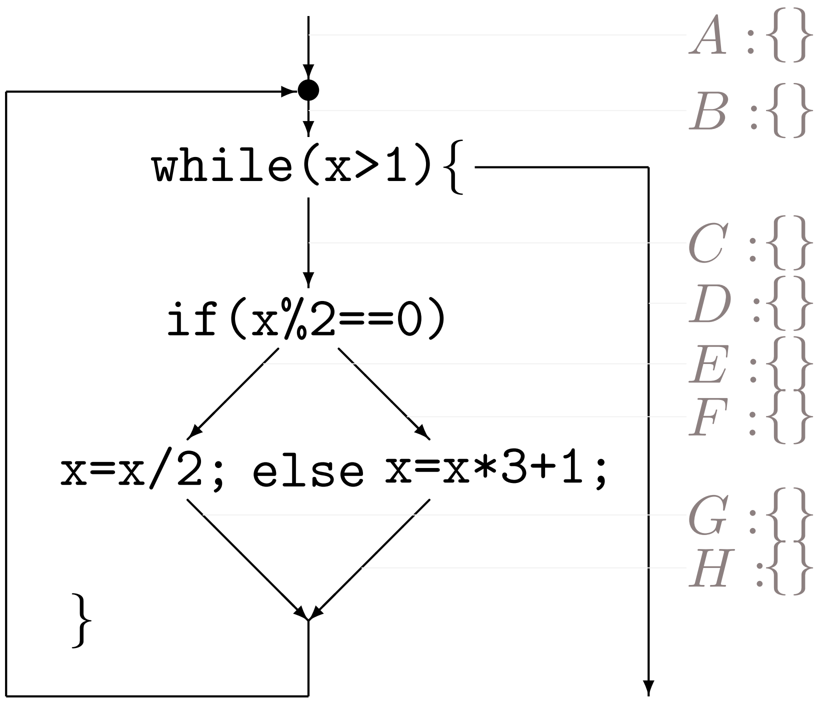
Da unser $M = \wp(\boldsymbol{Z})^8$ vollständiger Verband
und unser $\Phi : \wp(\boldsymbol{Z})^8 \longrightarrow \wp(\boldsymbol{Z})^8$ monotone und stetige Abbildung ist,
können wir den Satz anwenden.
Der Fixpunkt X hat die Form $\langle A, \ldots, H \rangle$;
er ist eine Lösung des ursprünglichen Mengen–Gleichungssystems.

Mit dem Fixpunktsatz zur Lösung

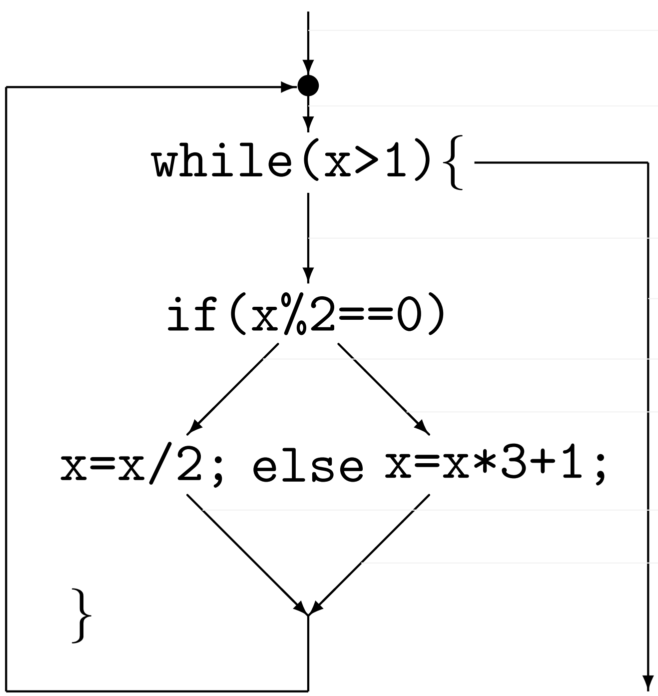


Mit dem Fixpunktsatz zur Lösung

neu: $\perp$

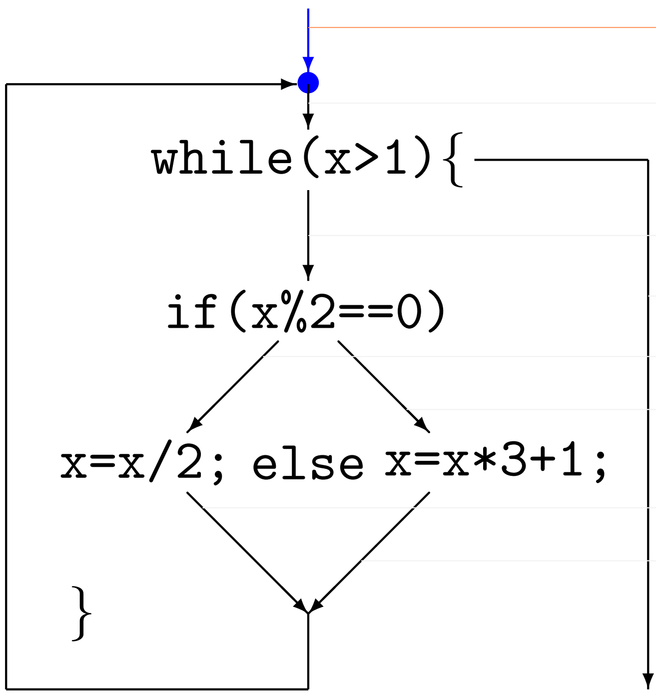


Mit dem Fixpunktsatz zur Lösung



	neu: $\Phi(\perp)$	alt: $\perp$
A :		$\{\}$
B :		$\{\}$
C :		$\{\}$
D :		$\{\}$
E :		$\{\}$
F :		$\{\}$
G :		$\{\}$
H :		$\{\}$

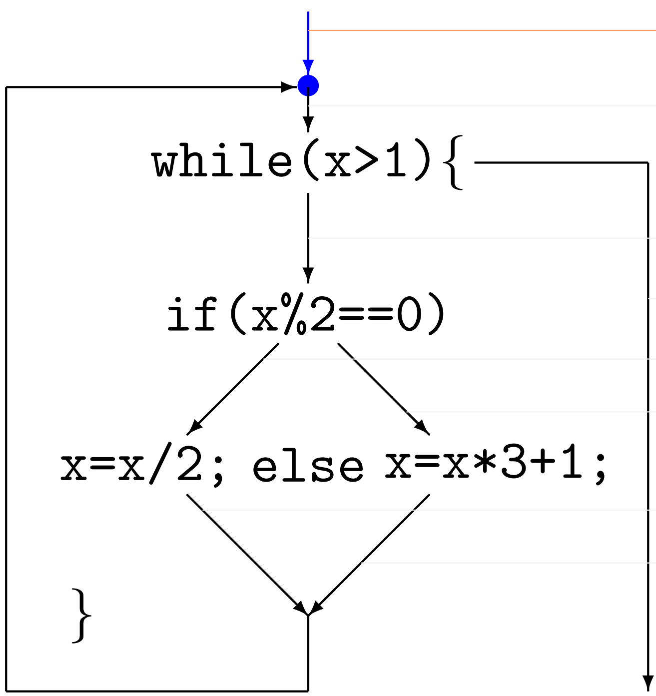
Mit dem Fixpunktsatz zur Lösung



	neu: $\Phi(\perp)$	alt: $\perp$
A	$\{1,2,3,4,5\}$	$\{\}$
B	$\{\}$	$\{\}$
C	$\{\}$	$\{\}$
D	$\{\}$	$\{\}$
E	$\{\}$	$\{\}$
F	$\{\}$	$\{\}$
G	$\{\}$	$\{\}$
H	$\{\}$	$\{\}$

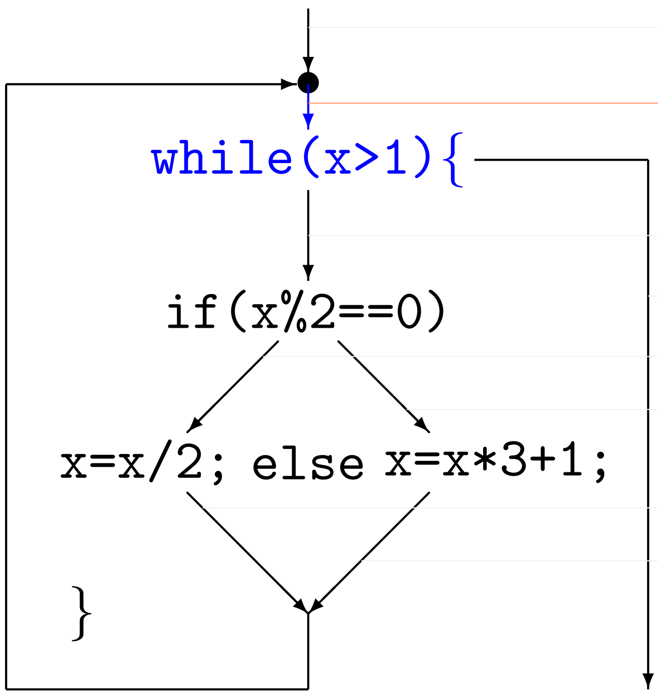
$$A = \{1,2,3,4,5\}$$

Mit dem Fixpunktsatz zur Lösung



	neu: $\Phi(\Phi(\perp))$	alt: $\Phi(\perp)$
A :		$\{1, 2, 3, 4, 5\}$
B :		$\{\}$
C :		$\{\}$
D :		$\{\}$
E :		$\{\}$
F :		$\{\}$
G :		$\{\}$
H :		$\{\}$

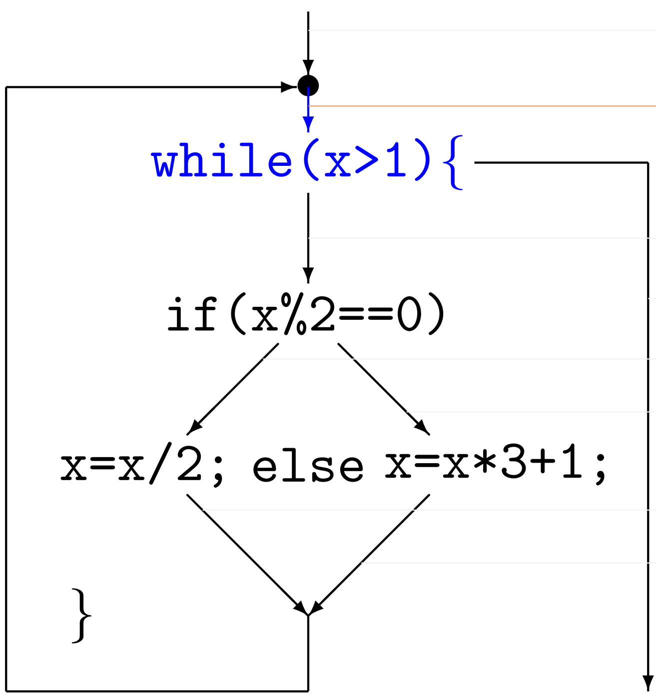
Mit dem Fixpunktsatz zur Lösung



	neu: $\Phi(\Phi(\perp))$	alt: $\Phi(\perp)$
A	$\{1,2,3,4,5\}$	$\{1,2,3,4,5\}$
B	$\{1,2,3,4,5\}$	$\{\}$
C	$\{\}$	$\{\}$
D	$\{\}$	$\{\}$
E	$\{\}$	$\{\}$
F	$\{\}$	$\{\}$
G	$\{\}$	$\{\}$
H	$\{\}$	$\{\}$

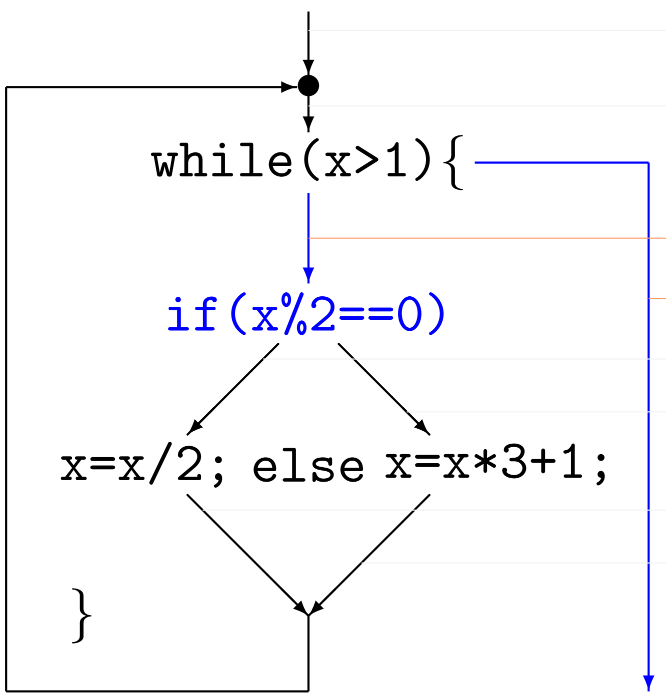
$$B = A \cup G \cup H$$

Mit dem Fixpunktsatz zur Lösung



	neu: $\Phi^3(\perp)$	alt: $\Phi(\Phi(\perp))$
A :		$\{1, 2, 3, 4, 5\}$
B :		$\{1, 2, 3, 4, 5\}$
C :		$\{\}$
D :		$\{\}$
E :		$\{\}$
F :		$\{\}$
G :		$\{\}$
H :		$\{\}$

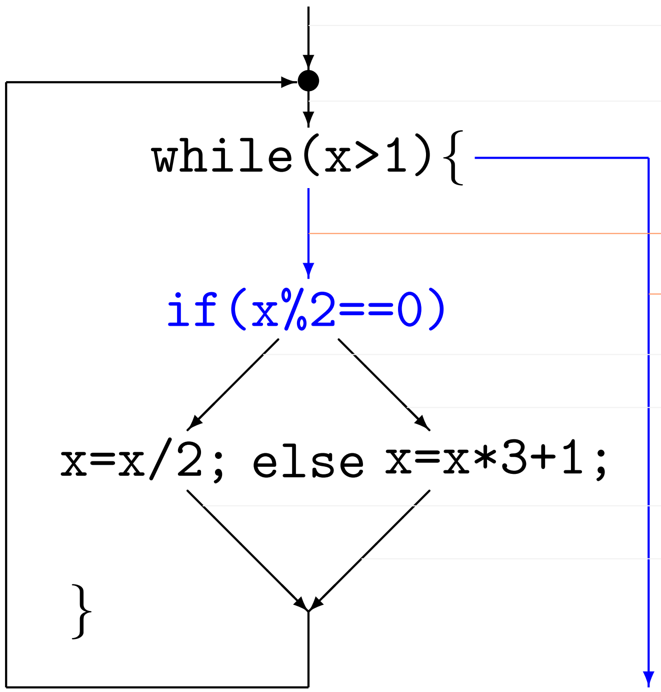
Mit dem Fixpunktsatz zur Lösung



	neu: $\Phi^3(\perp)$	alt: $\Phi(\Phi(\perp))$
A	$\{1,2,3,4,5\}$	$\{1,2,3,4,5\}$
B	$\{1,2,3,4,5\}$	$\{1,2,3,4,5\}$
C	$\{2,3,4,5\}$	$\{\}$
D	$\{1\}$	$\{\}$
E	$\{\}$	$\{\}$
F	$\{\}$	$\{\}$
G	$\{\}$	$\{\}$
H	$\{\}$	$\{\}$

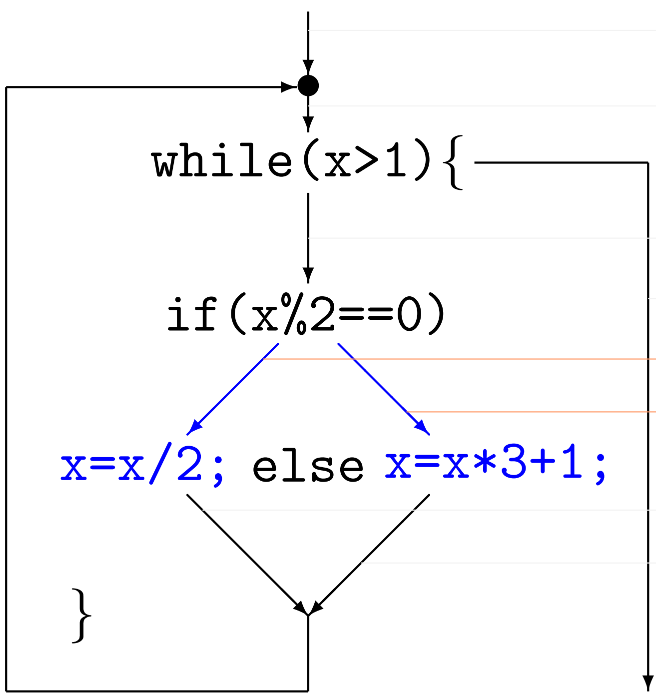
$$C = B \cap \{2,3,4,\ldots\}$$
$$D = B \cap \{\ldots,-2,-1,0,1\}$$

Mit dem Fixpunktsatz zur Lösung



	neu: $\Phi^4(\perp)$	alt: $\Phi^3(\perp)$
A :		$\{1,2,3,4,5\}$
B :		$\{1,2,3,4,5\}$
C :		$\{2,3,4,5\}$
D :		$\{1\}$
E :		$\{\}$
F :		$\{\}$
G :		$\{\}$
H :		$\{\}$

Mit dem Fixpunktsatz zur Lösung

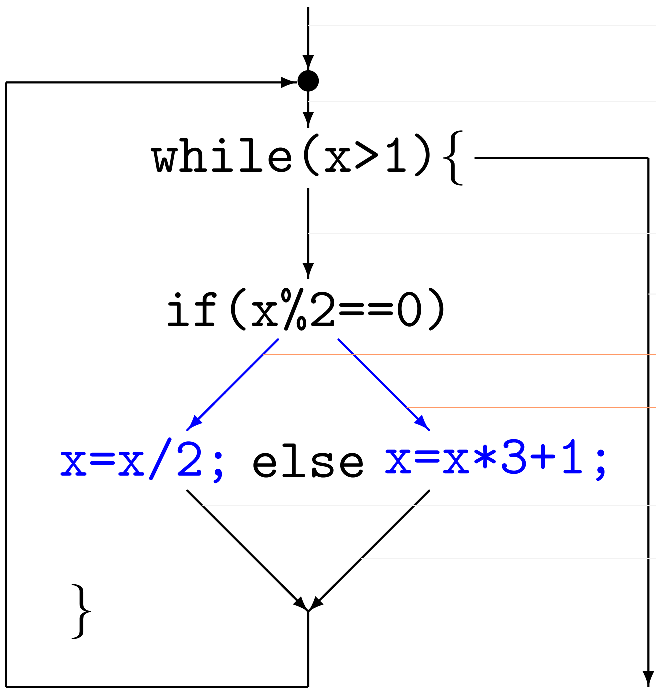


	neu: $\Phi^4(\bot)$	alt: $\Phi^3(\bot)$
A	$\{1,2,3,4,5\}$	$\{1,2,3,4,5\}$
B	$\{1,2,3,4,5\}$	$\{1,2,3,4,5\}$
C	$\{2,3,4,5\}$	$\{2,3,4,5\}$
D	$\{1\}$	$\{1\}$
E	$\{2,4\}$	$\{\}$
F	$\{3,5\}$	$\{\}$
G	$\{\}$	$\{\}$
H	$\{\}$	$\{\}$

$$E = C \cap \{\ldots,-4,-2,0,2,4,\ldots\}$$

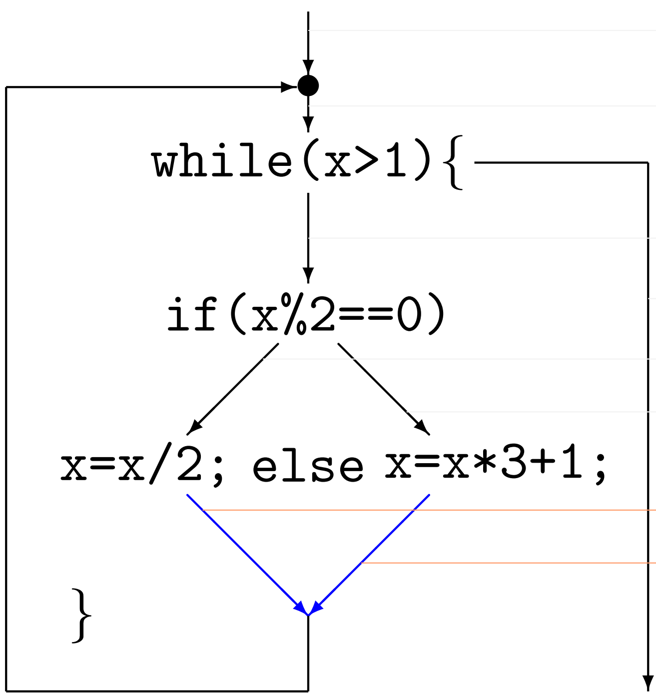
$$F = C \cap \{\ldots,-3,-1,1,3,\ldots\}$$

Mit dem Fixpunktsatz zur Lösung



	neu: $\Phi^5(\perp)$	alt: $\Phi^4(\perp)$
$A:$		$\{1,2,3,4,5\}$
$B:$		$\{1,2,3,4,5\}$
$C:$		$\{2,3,4,5\}$
$D:$		$\{1\}$
$E:$		$\{2,4\}$
$F:$		$\{3,5\}$
$G:$		$\{\}$
$H:$		$\{\}$

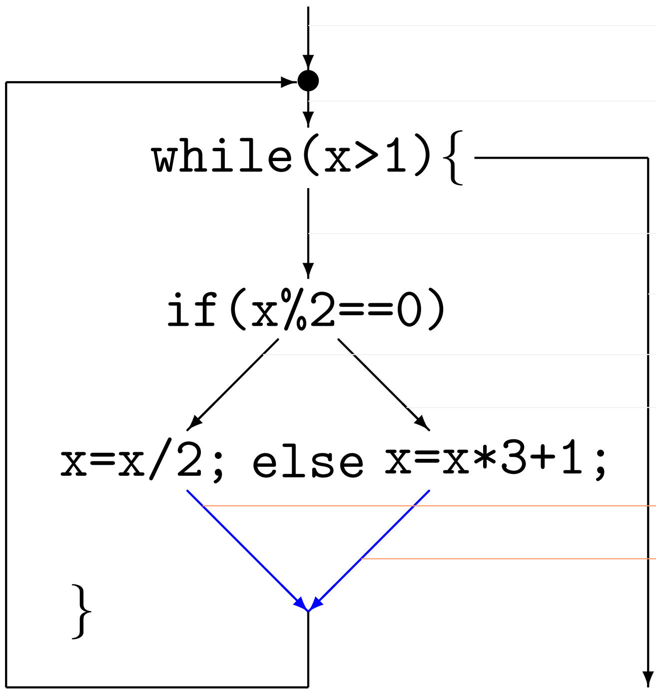
Mit dem Fixpunktsatz zur Lösung



	neu: $\Phi^5(\bot)$	alt: $\Phi^4(\bot)$
A	$\{1,2,3,4,5\}$	$\{1,2,3,4,5\}$
B	$\{1,2,3,4,5\}$	$\{1,2,3,4,5\}$
C	$\{2,3,4,5\}$	$\{2,3,4,5\}$
D	$\{1\}$	$\{1\}$
E	$\{2,4\}$	$\{2,4\}$
F	$\{3,5\}$	$\{3,5\}$
G	$\{1,2\}$	$\{\}$
H	$\{10,16\}$	$\{\}$

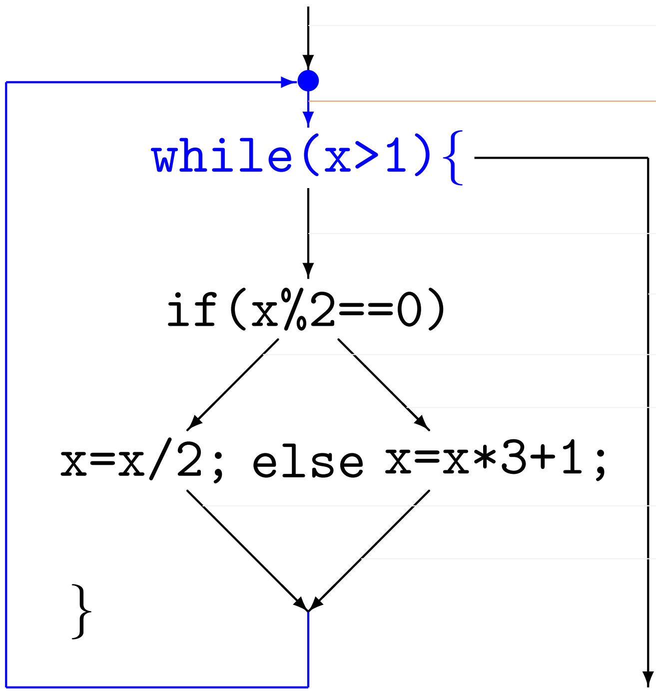
$$G = \{n/2 \mid n \in E\}$$
$$H = \{3 \cdot n + 1 \mid n \in F\}$$

Mit dem Fixpunktsatz zur Lösung



	neu: $\Phi^6(\perp)$	alt: $\Phi^5(\perp)$
$A:$		$\{1,2,3,4,5\}$
$B:$		$\{1,2,3,4,5\}$
$C:$		$\{2,3,4,5\}$
$D:$		$\{1\}$
$E:$		$\{2,4\}$
$F:$		$\{3,5\}$
$G:$		$\{1,2\}$
$H:$		$\{10,16\}$

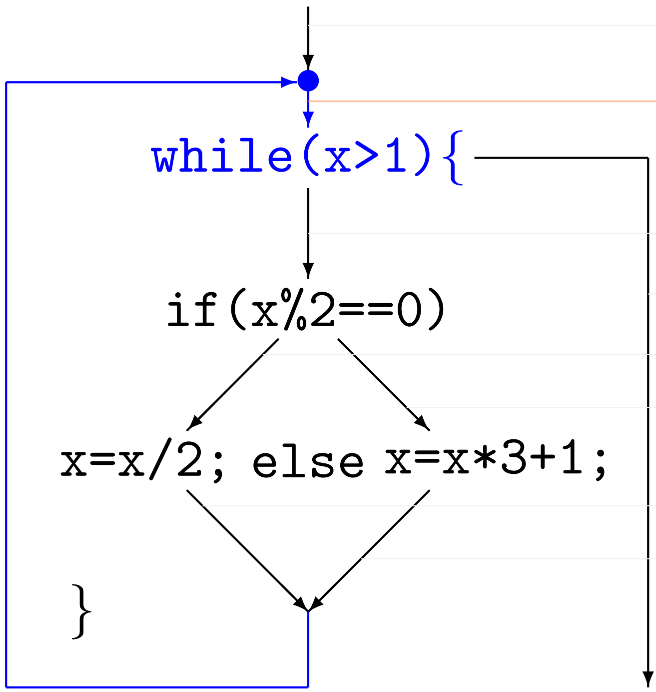
Mit dem Fixpunktsatz zur Lösung



	neu: $\Phi^6(\bot)$	alt: $\Phi^5(\bot)$
A :	$\{1,2,3,4,5\}$	$\{1,2,3,4,5\}$
B :	$\{1,2,3,4,5,10,16\}$	$\{1,2,3,4,5\}$
C :	$\{2,3,4,5\}$	$\{2,3,4,5\}$
D :	$\{1\}$	$\{1\}$
E :	$\{2,4\}$	$\{2,4\}$
F :	$\{3,5\}$	$\{3,5\}$
G :	$\{1,2\}$	$\{1,2\}$
H :	$\{10,16\}$	$\{10,16\}$

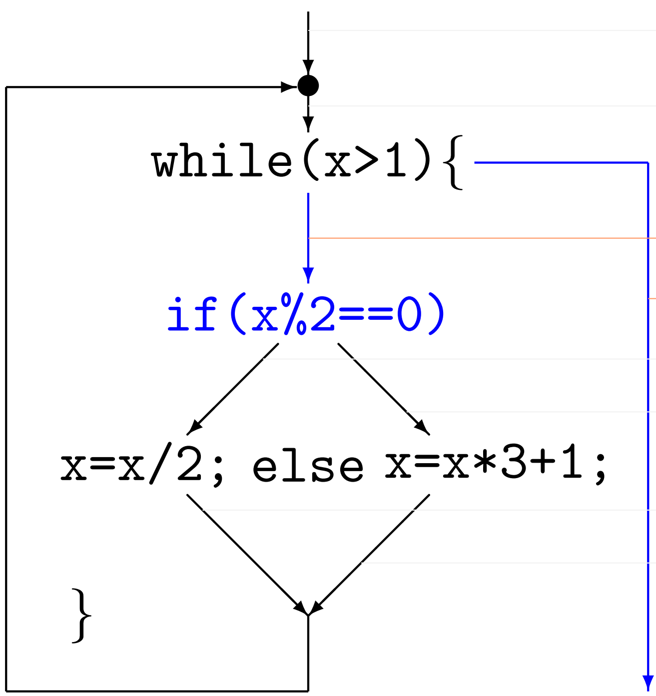
$$B = A \cup G \cup H$$

Mit dem Fixpunktsatz zur Lösung



	neu: $\Phi^7(\perp)$	alt: $\Phi^6(\perp)$
$A:$		$\{1,2,3,4,5\}$
$B:$		$\{1,2,3,4,5,10,16\}$
$C:$		$\{2,3,4,5\}$
$D:$		$\{1\}$
$E:$		$\{2,4\}$
$F:$		$\{3,5\}$
$G:$		$\{1,2\}$
$H:$		$\{10,16\}$

Mit dem Fixpunktsatz zur Lösung

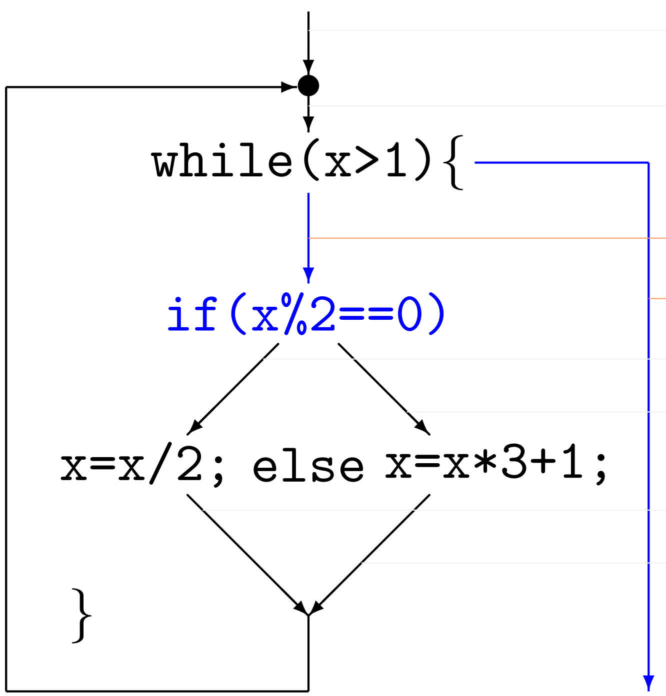


	neu: $\Phi^7(\perp)$	alt: $\Phi^6(\perp)$
A :	$\{1,2,3,4,5\}$	$\{1,2,3,4,5\}$
B :	$\{1,2,3,4,5,10,16\}$	$\{1,2,3,4,5,10,16\}$
C :	$\{2,3,4,5,10,16\}$	$\{2,3,4,5\}$
D :	$\{1\}$	$\{1\}$
E :	$\{2,4\}$	$\{2,4\}$
F :	$\{3,5\}$	$\{3,5\}$
G :	$\{1,2\}$	$\{1,2\}$
H :	$\{10,16\}$	$\{10,16\}$

$$C = B \cap \{2,3,4,\ldots\}$$

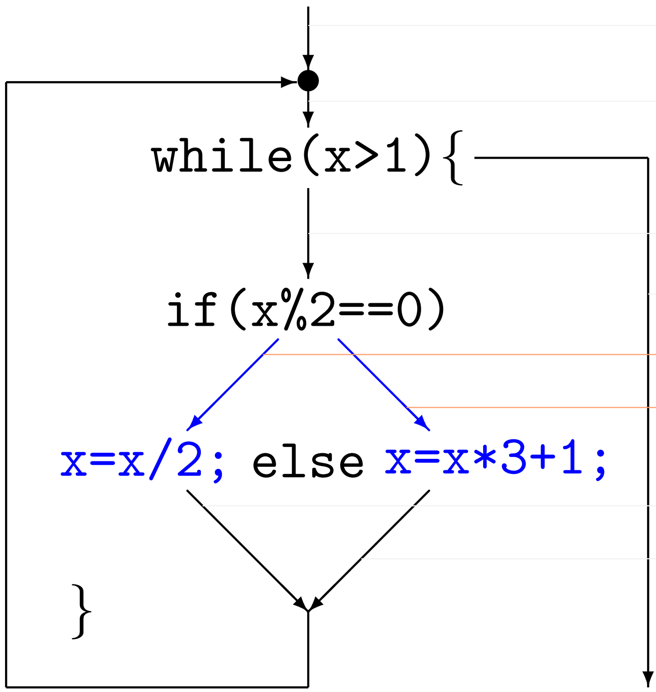
$$D = B \cap \{\ldots,-2,-1,0,1\}$$

Mit dem Fixpunktsatz zur Lösung



	neu: $\Phi^8(\perp)$	alt: $\Phi^7(\perp)$
A :		$\{1, 2, 3, 4, 5\}$
B :		$\{1, 2, 3, 4, 5, 10, 16\}$
C :		$\{2, 3, 4, 5, 10, 16\}$
D :		$\{1\}$
E :		$\{2, 4\}$
F :		$\{3, 5\}$
G :		$\{1, 2\}$
H :		$\{10, 16\}$

Mit dem Fixpunktsatz zur Lösung

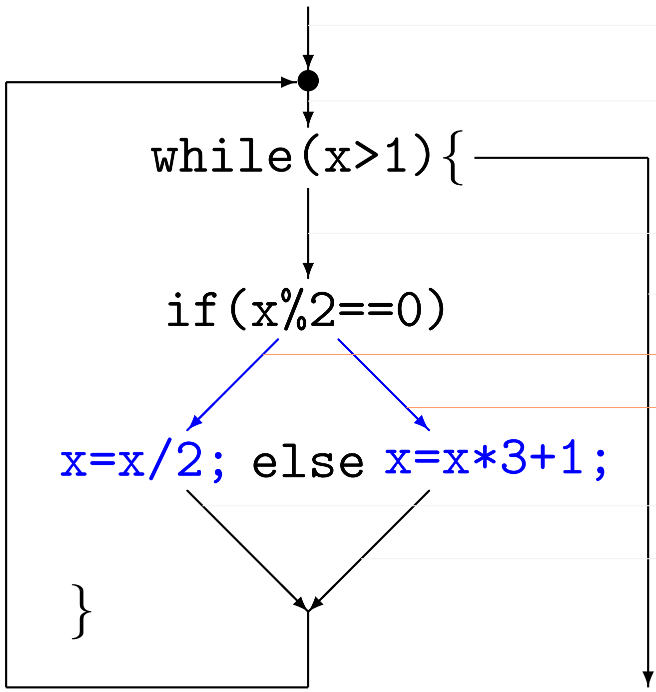


	neu: $\Phi^8(\perp)$	alt: $\Phi^7(\perp)$
A	$\{1,2,3,4,5\}$	$\{1,2,3,4,5\}$
B	$\{1,2,3,4,5,10,16\}$	$\{1,2,3,4,5,10,16\}$
C	$\{2,3,4,5,10,16\}$	$\{2,3,4,5,10,16\}$
D	$\{1\}$	$\{1\}$
E	$\{2,4,10,16\}$	$\{2,4\}$
F	$\{3,5\}$	$\{3,5\}$
G	$\{1,2\}$	$\{1,2\}$
H	$\{10,16\}$	$\{10,16\}$

$$E = C \cap \{\ldots, -4, -2, 0, 2, 4, \ldots\}$$

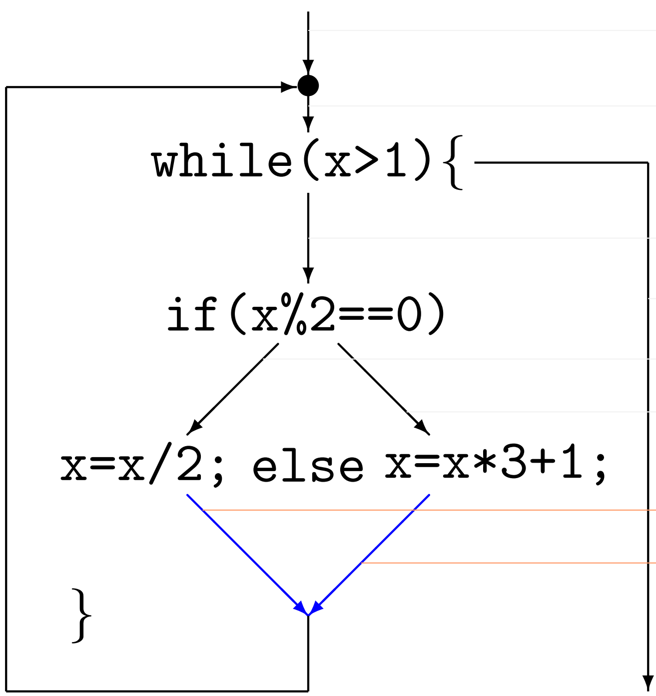
$$F = C \cap \{\ldots, -3, -1, 1, 3, \ldots\}$$

Mit dem Fixpunktsatz zur Lösung



	neu: $\Phi^9(\bot)$	alt: $\Phi^8(\bot)$
A :		$\{1,2,3,4,5\}$
B :		$\{1,2,3,4,5,10,16\}$
C :		$\{2,3,4,5,10,16\}$
D :		$\{1\}$
E :		$\{2,4,10,16\}$
F :		$\{3,5\}$
G :		$\{1,2\}$
H :		$\{10,16\}$

Mit dem Fixpunktsatz zur Lösung

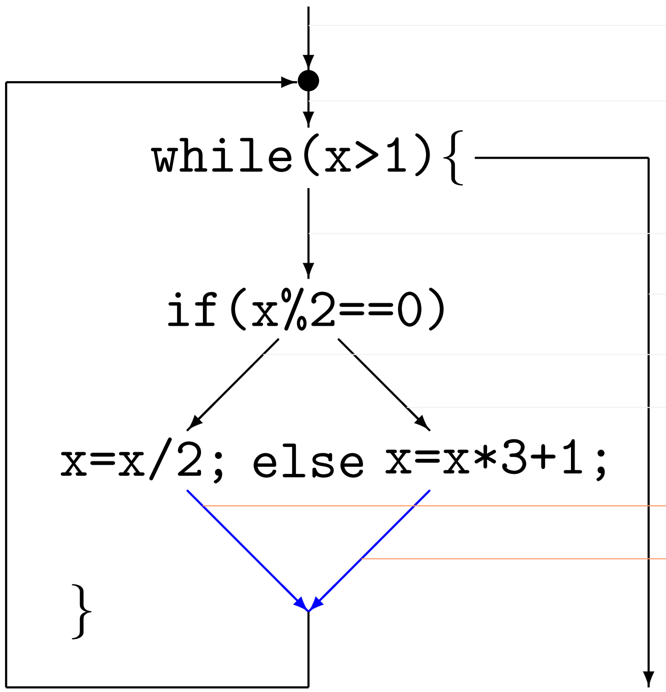


	neu: $\Phi^9(\perp)$	alt: $\Phi^8(\perp)$
A	$\{1,2,3,4,5\}$	$\{1,2,3,4,5\}$
B	$\{1,2,3,4,5,10,16\}$	$\{1,2,3,4,5,10,16\}$
C	$\{2,3,4,5,10,16\}$	$\{2,3,4,5,10,16\}$
D	$\{1\}$	$\{1\}$
E	$\{2,4,10,16\}$	$\{2,4,10,16\}$
F	$\{3,5\}$	$\{3,5\}$
G	$\{1,2,5,8\}$	$\{1,2\}$
H	$\{10,16\}$	$\{10,16\}$

$$G = \{n/2 \mid n \in E\}$$

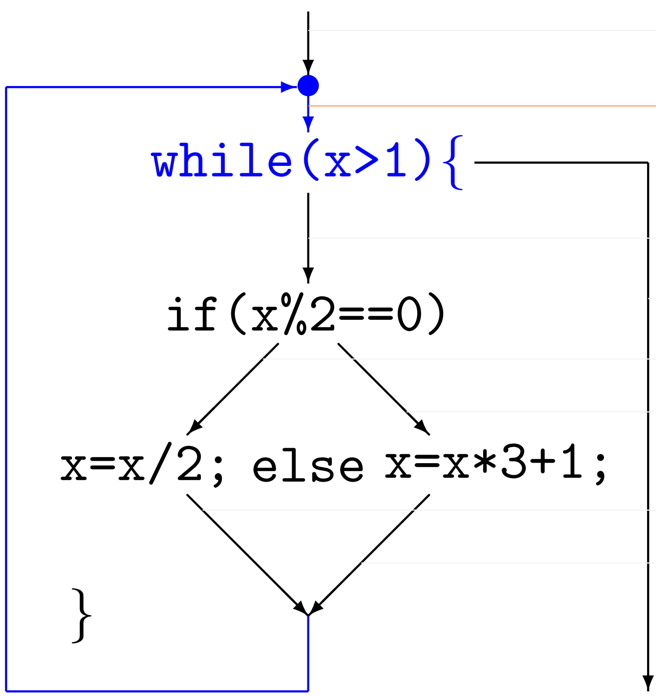
$$H = \{3 \cdot n + 1 \mid n \in F\}$$

Mit dem Fixpunktsatz zur Lösung



	neu: $\Phi^{10}(\perp)$	alt: $\Phi^{9}(\perp)$
A :		$\{1,2,3,4,5\}$
B :		$\{1,2,3,4,5,10,16\}$
C :		$\{2,3,4,5,10,16\}$
D :		$\{1\}$
E :		$\{2,4,10,16\}$
F :		$\{3,5\}$
G :		$\{1,2,5,8\}$
H :		$\{10,16\}$

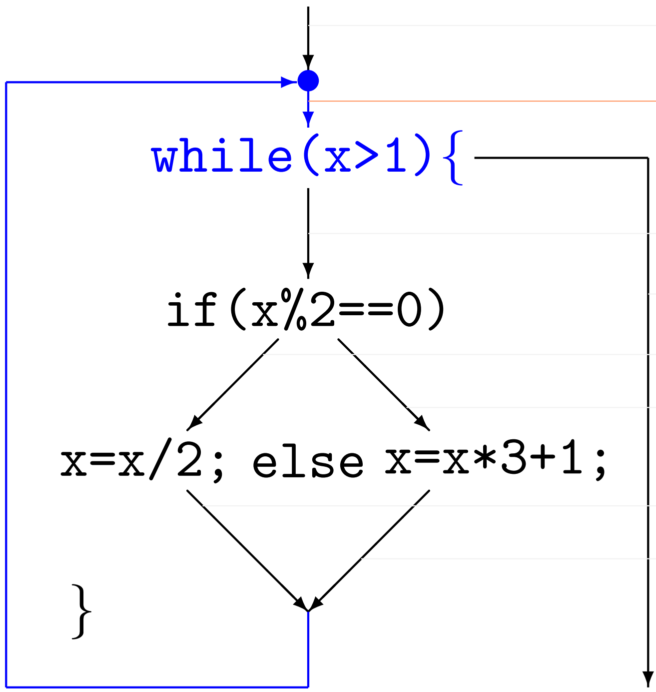
Mit dem Fixpunktsatz zur Lösung



	neu: $\Phi^{10}(\perp)$	alt: $\Phi^{9}(\perp)$
A	$:\{1,2,3,4,5\}$	$\{1,2,3,4,5\}$
B	$:\{1,2,3,4,5,8,10,16\}$	$\{1,2,3,4,5,10,16\}$
C	$:\{2,3,4,5,10,16\}$	$\{2,3,4,5,10,16\}$
D	$:\{1\}$	$\{1\}$
E	$:\{2,4,10,16\}$	$\{2,4,10,16\}$
F	$:\{3,5\}$	$\{3,5\}$
G	$:\{1,2,5,8\}$	$\{1,2,5,8\}$
H	$:\{10,16\}$	$\{10,16\}$

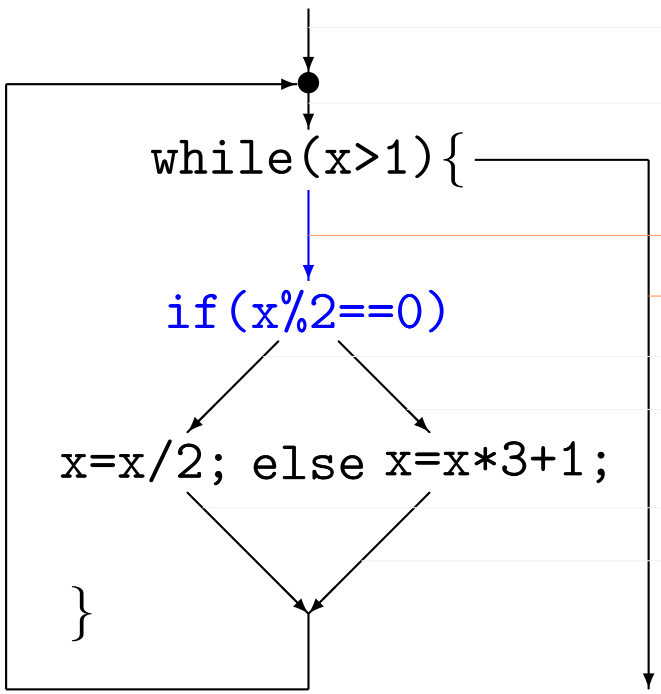
$$B = A \cup G \cup H$$

Mit dem Fixpunktsatz zur Lösung



	neu: $\Phi^{11}(\perp)$	alt: $\Phi^{10}(\perp)$
$A:$		$\{1,2,3,4,5\}$
$B:$		$\{1,2,3,4,5,8,10,16\}$
$C:$		$\{2,3,4,5,10,16\}$
$D:$		$\{1\}$
$E:$		$\{2,4,10,16\}$
$F:$		$\{3,5\}$
$G:$		$\{1,2,5,8\}$
$H:$		$\{10,16\}$

Mit dem Fixpunktsatz zur Lösung

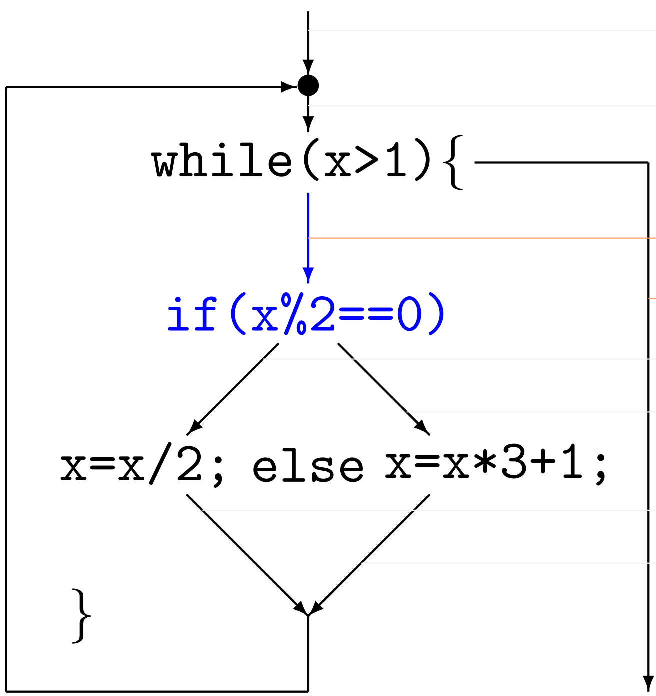


	neu: $\Phi^{11}(\perp)$	alt: $\Phi^{10}(\perp)$
A :	$\{1,2,3,4,5\}$	$\{1,2,3,4,5\}$
B :	$\{1,2,3,4,5,8,10,16\}$	$\{1,2,3,4,5,8,10,16\}$
C :	$\{2,3,4,5,8,10,16\}$	$\{2,3,4,5,10,16\}$
D :	$\{1\}$	$\{1\}$
E :	$\{2,4,10,16\}$	$\{2,4,10,16\}$
F :	$\{3,5\}$	$\{3,5\}$
G :	$\{1,2,5,8\}$	$\{1,2,5,8\}$
H :	$\{10,16\}$	$\{10,16\}$

$$C = B \cap \{2,3,4,\ldots\}$$

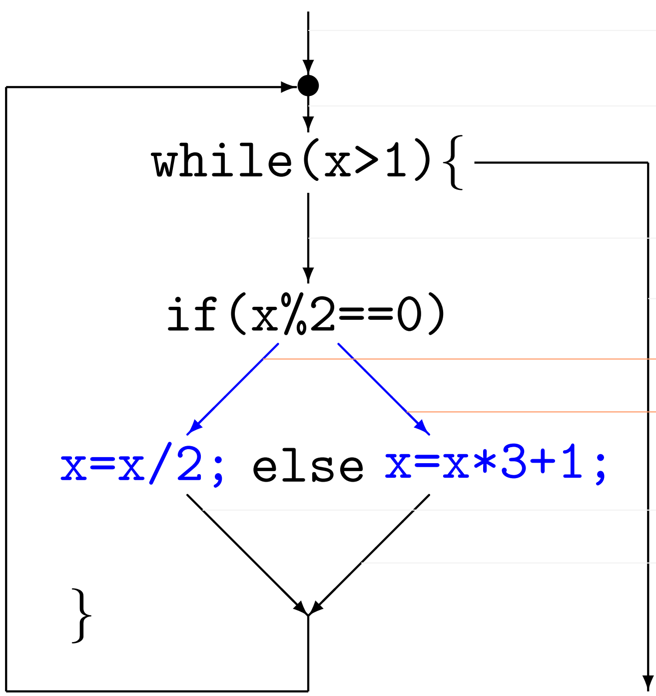
$$D = B \cap \{\ldots,-2,-1,0,1\}$$

Mit dem Fixpunktsatz zur Lösung



	neu: $\Phi^{12}(\perp)$	alt: $\Phi^{11}(\perp)$
$A:$		$\{1,2,3,4,5\}$
$B:$		$\{1,2,3,4,5,8,10,16\}$
$C:$		$\{2,3,4,5,8,10,16\}$
$D:$		$\{1\}$
$E:$		$\{2,4,10,16\}$
$F:$		$\{3,5\}$
$G:$		$\{1,2,5,8\}$
$H:$		$\{10,16\}$

Mit dem Fixpunktsatz zur Lösung

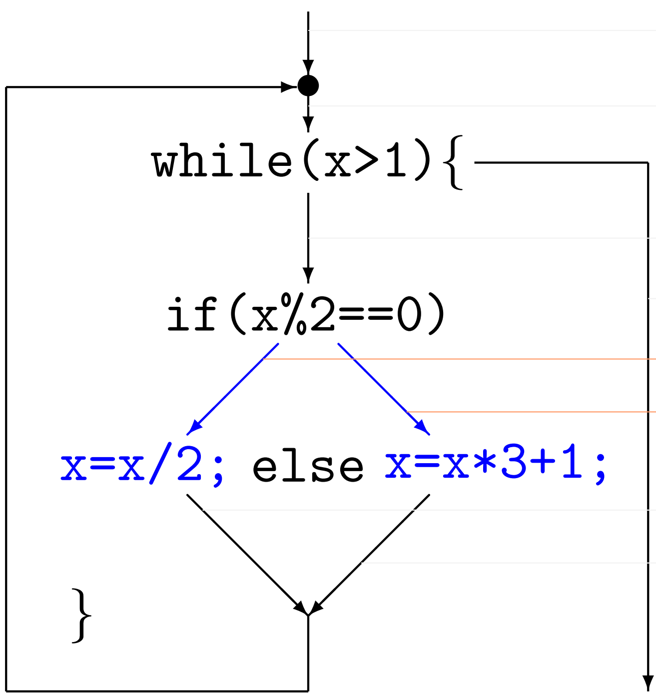


	neu: $\Phi^{12}(\bot)$	alt: $\Phi^{11}(\bot)$
A :	$\{1,2,3,4,5\}$	$\{1,2,3,4,5\}$
B :	$\{1,2,3,4,5,8,10,16\}$	$\{1,2,3,4,5,8,10,16\}$
C :	$\{2,3,4,5,8,10,16\}$	$\{2,3,4,5,8,10,16\}$
D :	$\{1\}$	$\{1\}$
E :	$\{2,4,8,10,16\}$	$\{2,4,10,16\}$
F :	$\{3,5\}$	$\{3,5\}$
G :	$\{1,2,5,8\}$	$\{1,2,5,8\}$
H :	$\{10,16\}$	$\{10,16\}$

$$E = C \cap \{\ldots,-4,-2,0,2,4,\ldots\}$$

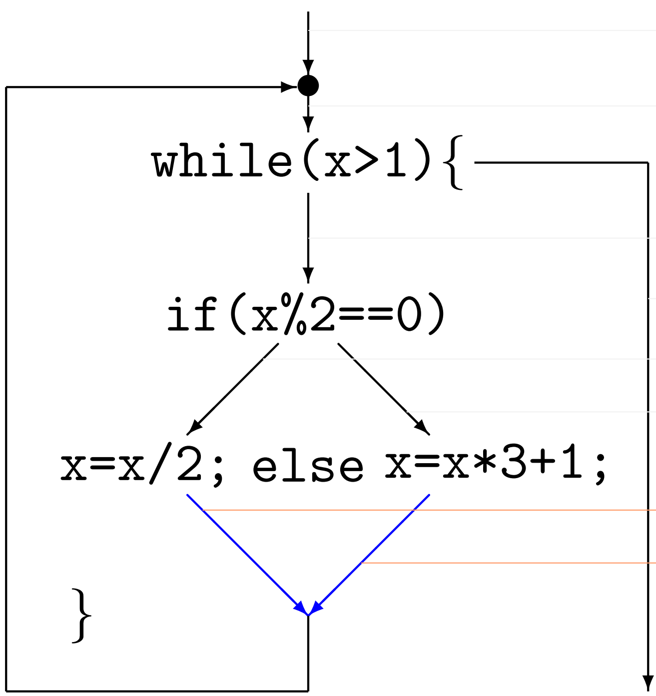
$$F = C \cap \{\ldots,-3,-1,1,3,\ldots\}$$

Mit dem Fixpunktsatz zur Lösung



	neu: $\Phi^{13}(\bot)$	alt: $\Phi^{12}(\bot)$
A :		$\{1, 2, 3, 4, 5\}$
B :		$\{1, 2, 3, 4, 5, 8, 10, 16\}$
C :		$\{2, 3, 4, 5, 8, 10, 16\}$
D :		$\{1\}$
E :		$\{2, 4, 8, 10, 16\}$
F :		$\{3, 5\}$
G :		$\{1, 2, 5, 8\}$
H :		$\{10, 16\}$

Mit dem Fixpunktsatz zur Lösung

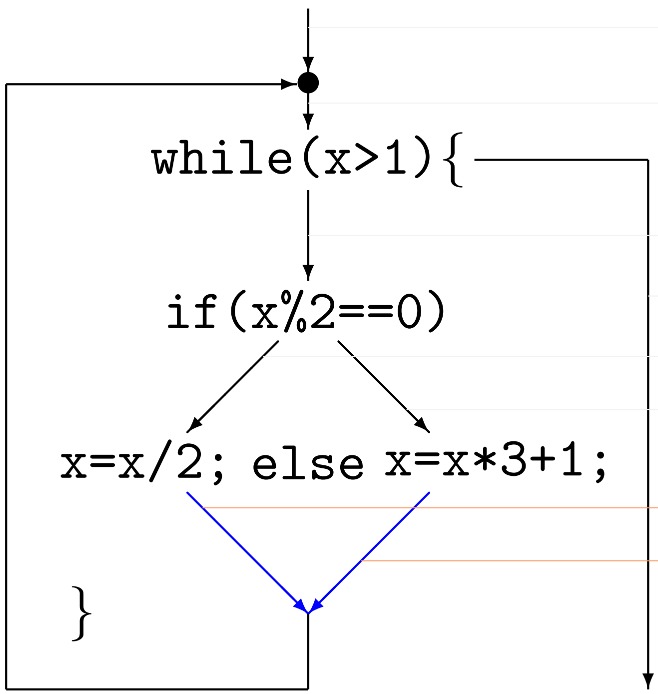


	neu: $\Phi^{13}(\perp)$	alt: $\Phi^{12}(\perp)$
A :	$\{1,2,3,4,5\}$	$\{1,2,3,4,5\}$
B :	$\{1,2,3,4,5,8,10,16\}$	$\{1,2,3,4,5,8,10,16\}$
C :	$\{2,3,4,5,8,10,16\}$	$\{2,3,4,5,8,10,16\}$
D :	$\{1\}$	$\{1\}$
E :	$\{2,4,8,10,16\}$	$\{2,4,8,10,16\}$
F :	$\{3,5\}$	$\{3,5\}$
G :	$\{1,2,4,5,8\}$	$\{1,2,5,8\}$
H :	$\{10,16\}$	$\{10,16\}$

$$G = \{n/2 \mid n \in E\}$$

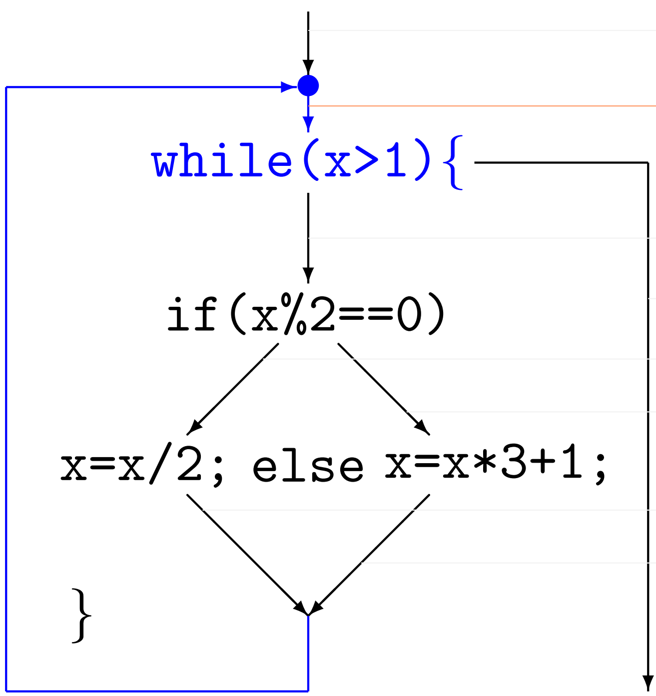
$$H = \{3 \cdot n + 1 \mid n \in F\}$$

Mit dem Fixpunktsatz zur Lösung



	neu: $\Phi^{14}(\perp)$	alt: $\Phi^{13}(\perp)$
A :		$\{1,2,3,4,5\}$
B :		$\{1,2,3,4,5,8,10,16\}$
C :		$\{2,3,4,5,8,10,16\}$
D :		$\{1\}$
E :		$\{2,4,8,10,16\}$
F :		$\{3,5\}$
G :		$\{1,2,4,5,8\}$
H :		$\{10,16\}$

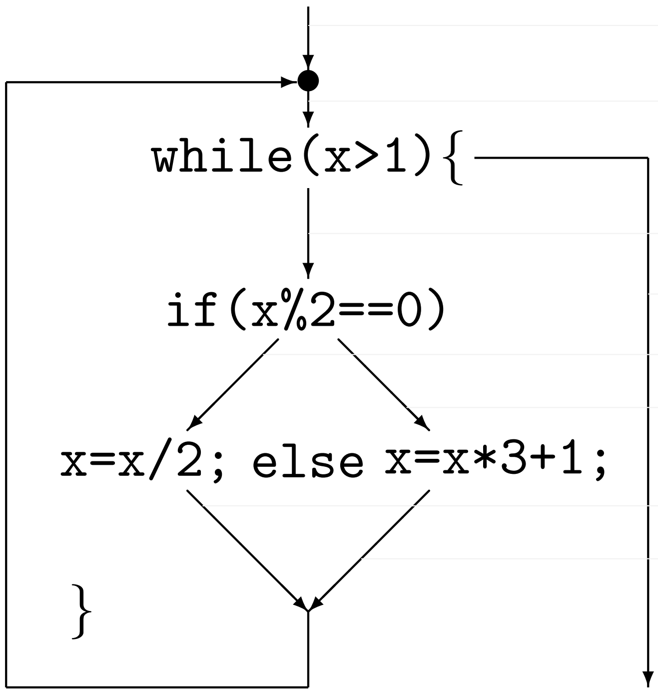
Mit dem Fixpunktsatz zur Lösung



	neu: $\Phi^{14}(\perp)$	alt: $\Phi^{13}(\perp)$
A :	$\{1,2,3,4,5\}$	$\{1,2,3,4,5\}$
B :	$\{1,2,3,4,5,8,10,16\}$	$\{1,2,3,4,5,8,10,16\}$
C :	$\{2,3,4,5,8,10,16\}$	$\{2,3,4,5,8,10,16\}$
D :	$\{1\}$	$\{1\}$
E :	$\{2,4,8,10,16\}$	$\{2,4,8,10,16\}$
F :	$\{3,5\}$	$\{3,5\}$
G :	$\{1,2,4,5,8\}$	$\{1,2,4,5,8\}$
H :	$\{10,16\}$	$\{10,16\}$

$$B = A \cup G \cup H$$

Mit dem Fixpunktsatz zur Lösung

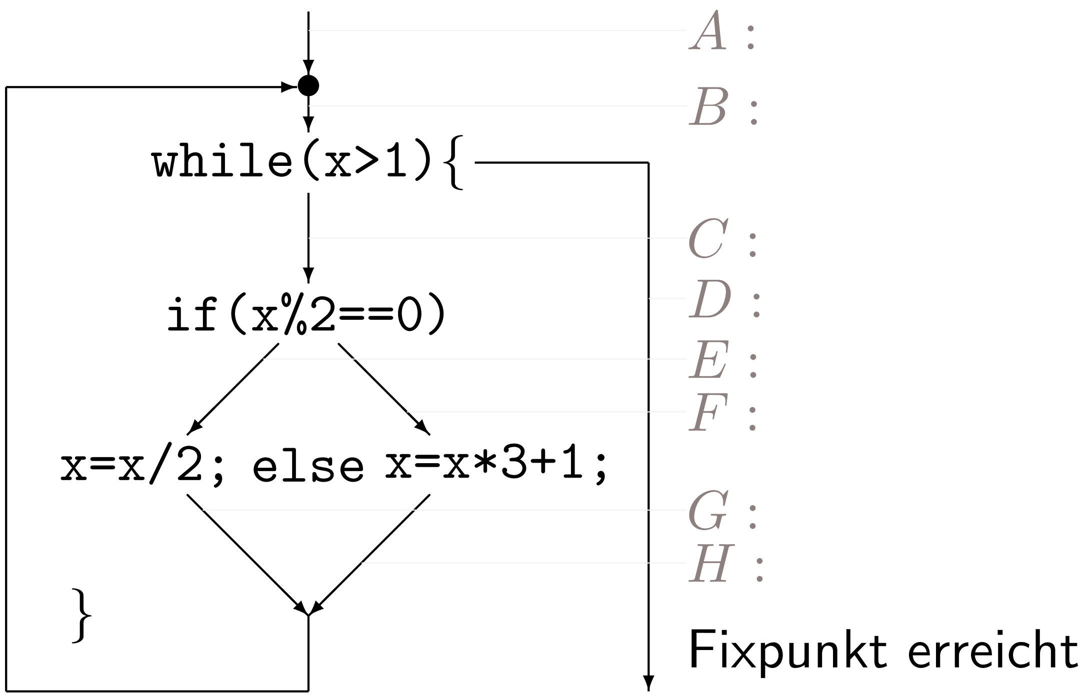


	neu: $\Phi^{14}(\perp)$	alt: $\Phi^{13}(\perp)$
A :	$\{1,2,3,4,5\}$	$\{1,2,3,4,5\}$
B :	$\{1,2,3,4,5,8,10,16\}$	$\{1,2,3,4,5,8,10,16\}$
C :	$\{2,3,4,5,8,10,16\}$	$\{2,3,4,5,8,10,16\}$
D :	$\{1\}$	$\{1\}$
E :	$\{2,4,8,10,16\}$	$\{2,4,8,10,16\}$
F :	$\{3,5\}$	$\{3,5\}$
G :	$\{1,2,4,5,8\}$	$\{1,2,4,5,8\}$
H :	$\{10,16\}$	$\{10,16\}$

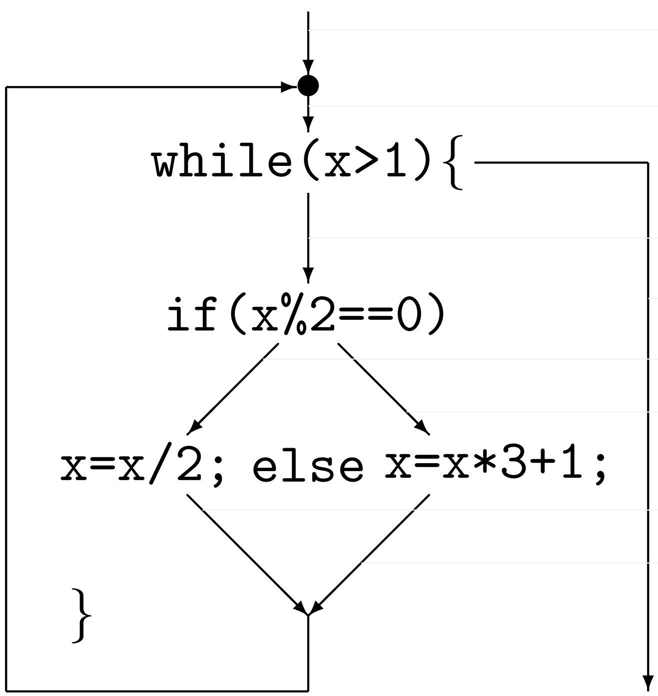
Fixpunkt erreicht

Mit dem Fixpunktsatz zur Lösung

neu: alt:



Mit dem Fixpunktsatz zur Lösung



	neu: $\Phi^{n}(\perp)$	alt: $\Phi^{n-1}(\perp)$
$A:$	$\{1,2,3,4,5\}$	$\{1,2,3,4,5\}$
$B:$	$\{1,2,3,4,5,8,10,16\}$	$\{1,2,3,4,5,8,10,16\}$
$C:$	$\{2,3,4,5,8,10,16\}$	$\{2,3,4,5,8,10,16\}$
$D:$	$\{1\}$	$\{1\}$
$E:$	$\{2,4,8,10,16\}$	$\{2,4,8,10,16\}$
$F:$	$\{3,5\}$	$\{3,5\}$
$G:$	$\{1,2,4,5,8\}$	$\{1,2,4,5,8\}$
$H:$	$\{10,16\}$	$\{10,16\}$

Fixpunkt erreicht

Fixpunkt erreicht: wieso eigentlich?

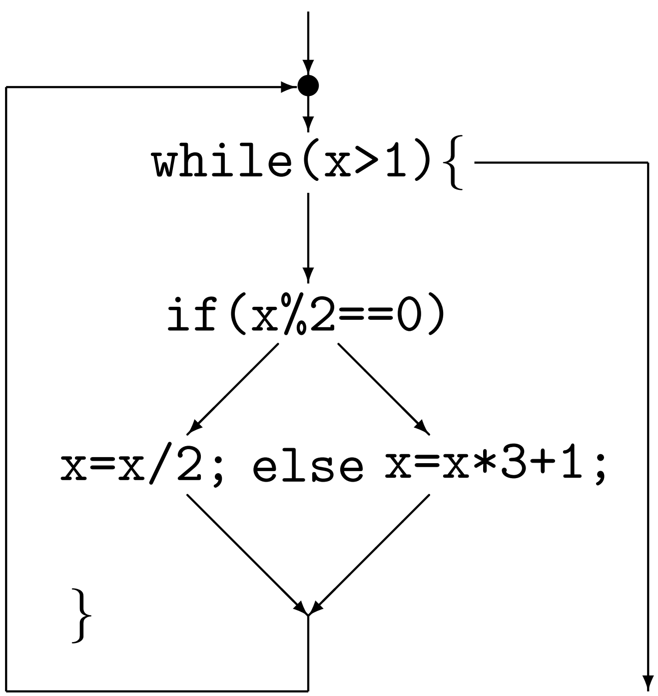
Der kleinste Fixpunkt von Φ ist nach dem Fixpunktsatz
$X = \bigsqcup \{\Phi^n(\perp) \mid n \in I\!N\}$.

Wir haben gesehen, daß $\perp \sqsubseteq \Phi(\perp) \sqsubseteq \Phi(\Phi(\perp)) \sqsubseteq \ldots \sqsubseteq \Phi^{13}(\perp) = \Phi^{14}(\perp)$.
Weitere Anwendung von Φ bringt keine Änderung mehr, d.h.
$\Phi^{13}(\perp) = \Phi^{14}(\perp) = \ldots = \Phi^n$ für alle $n > 14$.
Daher ist $\Phi^{13}(\perp)$ die kleinste obere Schranke von $\{\Phi^n(\perp) \mid n \in I\!N\}$,
d.h. $X = \Phi^{13}(\perp)$.

Collecting Semantics für $I\!\!N$

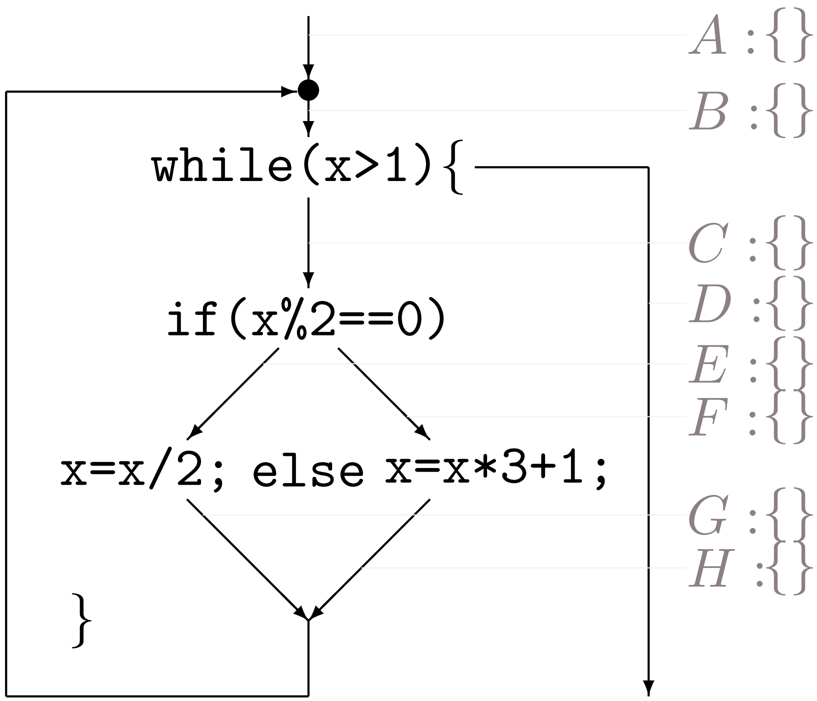
Wenn anstatt $\{1, 2, 3, 4, 5\}$ z.B. ganz $I\!\!N$ als Menge der Eingabewerte zugelassen ist, können wir die möglichen Variablenwerte durch entsprechende Änderung von Φ ebenfalls leicht ausrechnen.

Collecting Semantics für $\mathbb{N}$

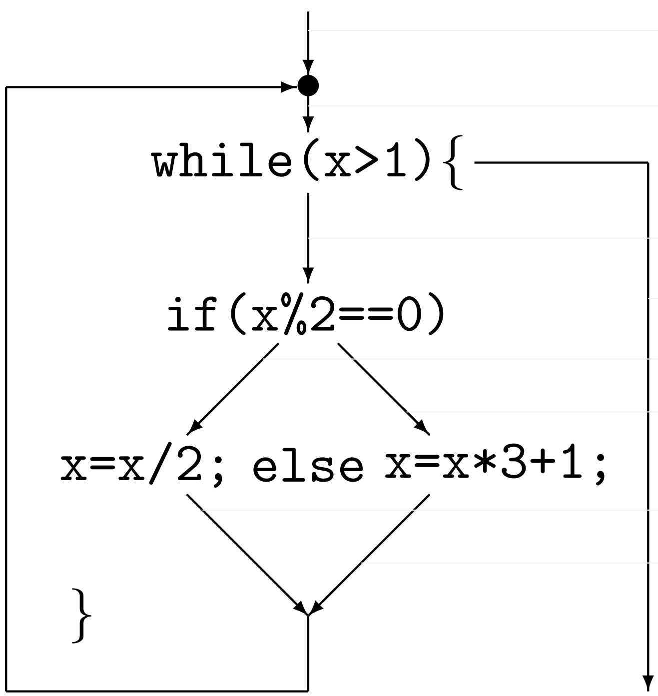


Collecting Semantics für $I\!N$

neu: $\perp$

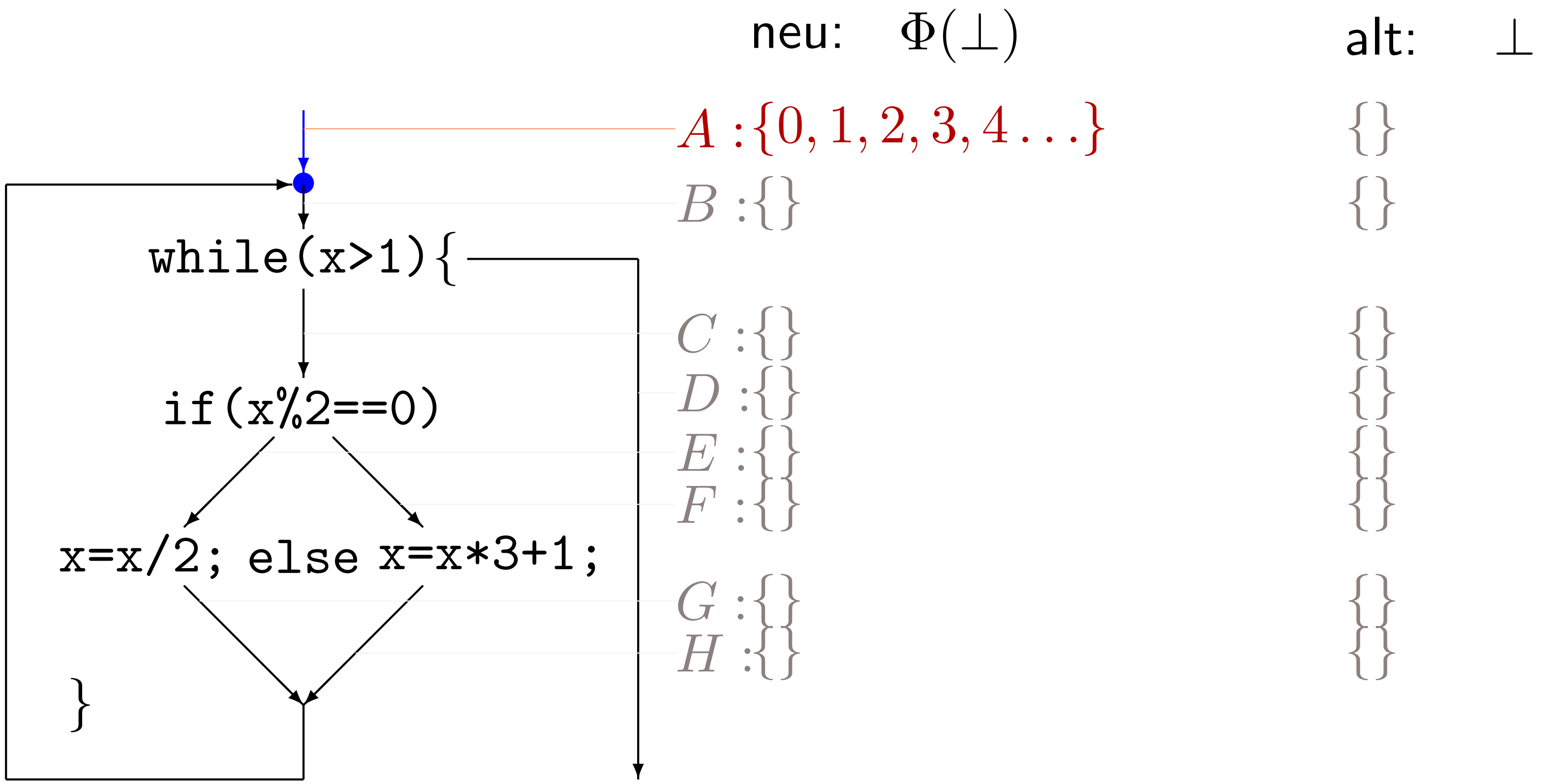


Collecting Semantics für $I\!N$



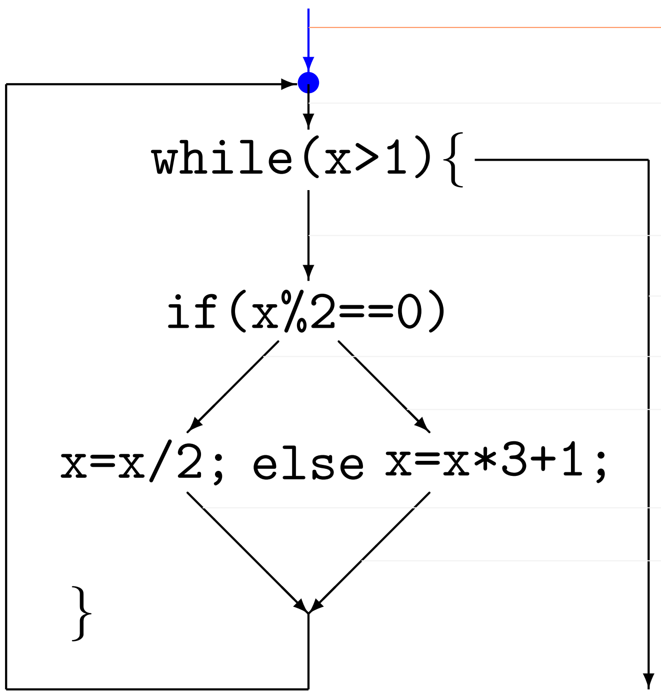
	neu: $\Phi(\bot)$	alt: $\bot$
A :		$\{\}$
B :		$\{\}$
C :		$\{\}$
D :		$\{\}$
E :		$\{\}$
F :		$\{\}$
G :		$\{\}$
H :		$\{\}$

Collecting Semantics für $I\!N$



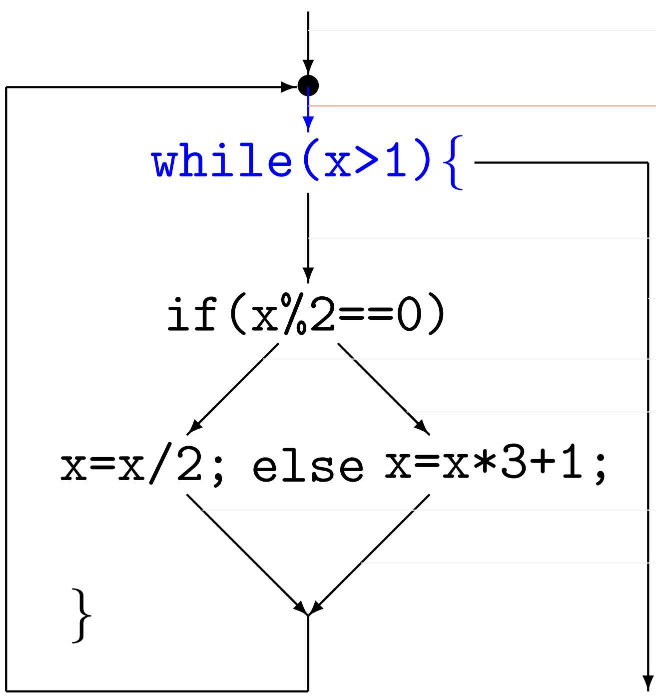
$$A = \{0, 1, 2, 3, 4, 5, \ldots\}$$

Collecting Semantics für $\mathbb{N}$



	neu: $\Phi(\Phi(\bot))$	alt: $\Phi(\bot)$
A :		$\{0, 1, 2, 3, 4 \ldots\}$
B :		$\{\}$
C :		$\{\}$
D :		$\{\}$
E :		$\{\}$
F :		$\{\}$
G :		$\{\}$
H :		$\{\}$

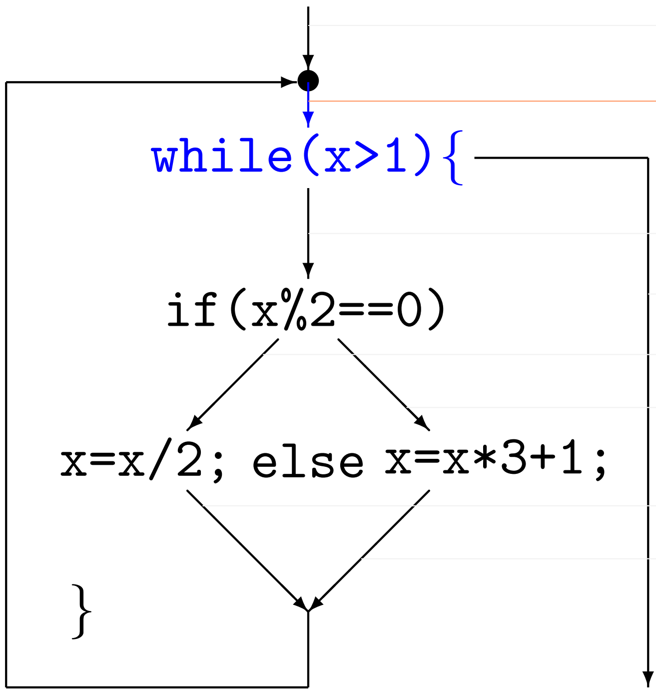
Collecting Semantics für $I\!N$



	neu: $\Phi(\Phi(\perp))$	alt: $\Phi(\perp)$
A	$\{0,1,2,3,4\ldots\}$	$\{0,1,2,3,4\ldots\}$
B	$\{0,1,2,3,4\ldots\}$	$\{\}$
C	$\{\}$	$\{\}$
D	$\{\}$	$\{\}$
E	$\{\}$	$\{\}$
F	$\{\}$	$\{\}$
G	$\{\}$	$\{\}$
H	$\{\}$	$\{\}$

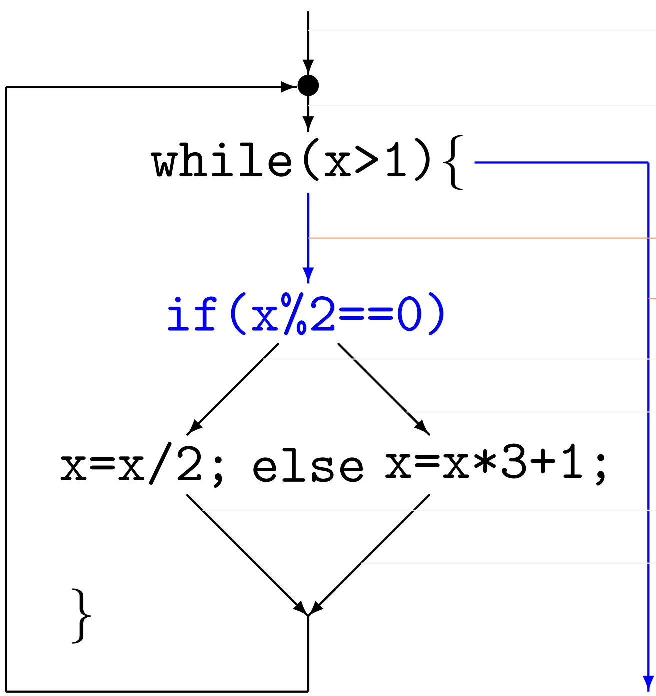
$$B = A \cup G \cup H$$

Collecting Semantics für $\mathbb{N}$



	neu: $\Phi^3(\perp)$	alt: $\Phi(\Phi(\perp))$
A :		$\{0, 1, 2, 3, 4 \ldots\}$
B :		$\{0, 1, 2, 3, 4 \ldots\}$
C :		$\{\}$
D :		$\{\}$
E :		$\{\}$
F :		$\{\}$
G :		$\{\}$
H :		$\{\}$

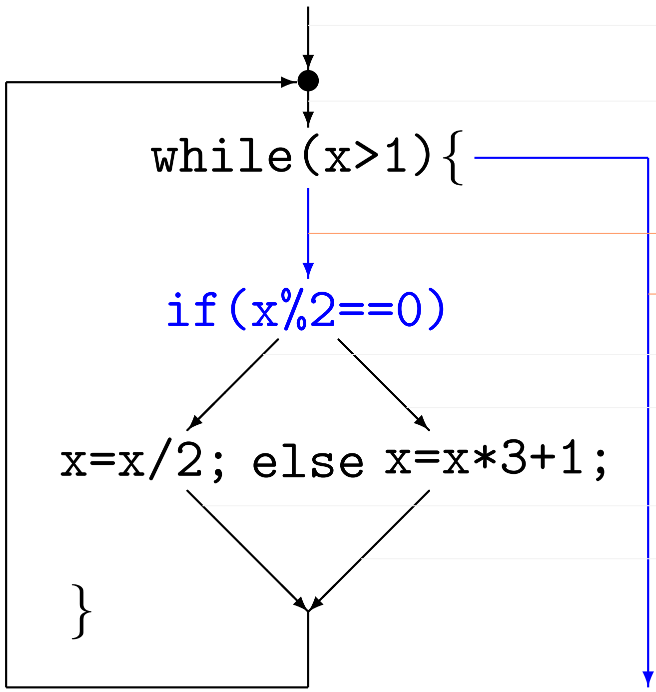
Collecting Semantics für $I\!N$



	neu: $\Phi^3(\bot)$	alt: $\Phi(\Phi(\bot))$
A	$\{0,1,2,3,4\ldots\}$	$\{0,1,2,3,4\ldots\}$
B	$\{0,1,2,3,4\ldots\}$	$\{0,1,2,3,4\ldots\}$
C	$\{2,3,4,5,6\ldots\}$	$\{\}$
D	$\{0,1\}$	$\{\}$
E	$\{\}$	$\{\}$
F	$\{\}$	$\{\}$
G	$\{\}$	$\{\}$
H	$\{\}$	$\{\}$

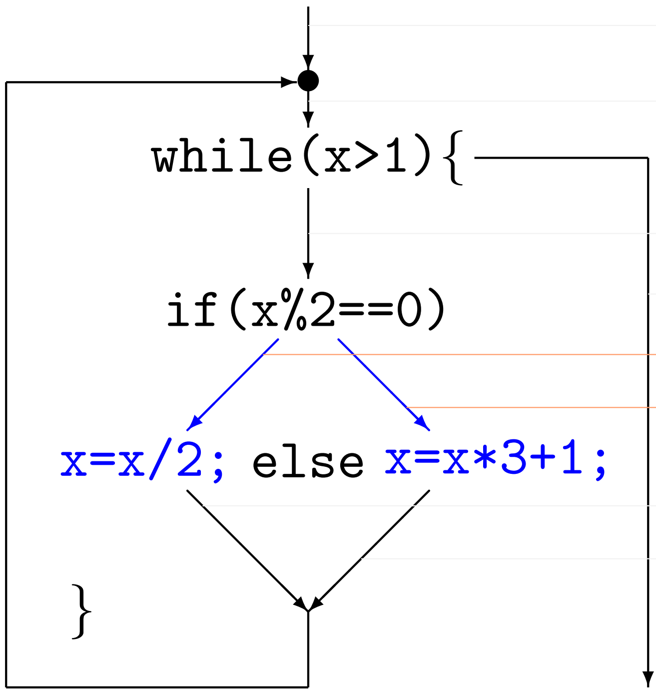
$$C = B \cap \{2,3,4,\ldots\}$$
$$D = B \cap \{\ldots,-2,-1,0,1\}$$

Collecting Semantics für $I\!N$



	neu: $\Phi^4(\bot)$	alt: $\Phi^3(\bot)$
A :		$\{0,1,2,3,4\ldots\}$
B :		$\{0,1,2,3,4\ldots\}$
C :		$\{2,3,4,5,6\ldots\}$
D :		$\{0,1\}$
E :		$\{\}$
F :		$\{\}$
G :		$\{\}$
H :		$\{\}$

Collecting Semantics für $I\!N$

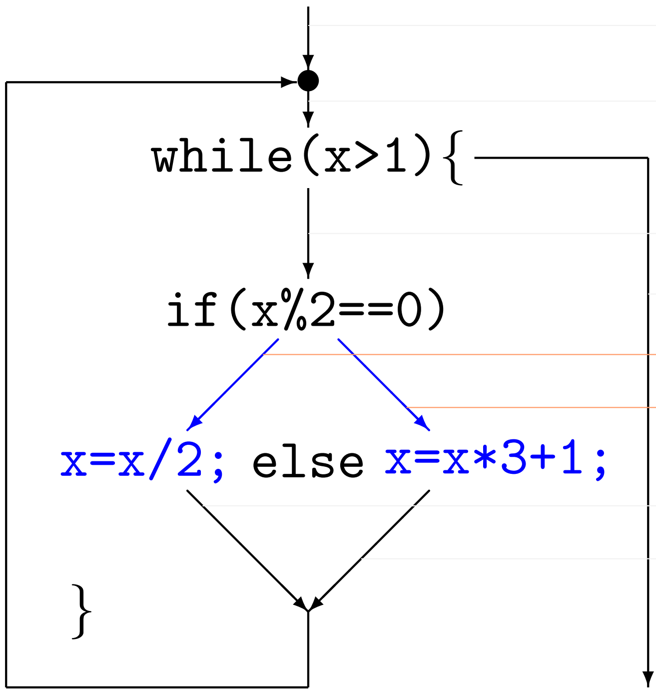


	neu: $\Phi^4(\perp)$	alt: $\Phi^3(\perp)$
A	$\{0,1,2,3,4\ldots\}$	$\{0,1,2,3,4\ldots\}$
B	$\{0,1,2,3,4\ldots\}$	$\{0,1,2,3,4\ldots\}$
C	$\{2,3,4,5,6\ldots\}$	$\{2,3,4,5,6\ldots\}$
D	$\{0,1\}$	$\{0,1\}$
E	$\{2,4,6,8,10,\ldots\}$	$\{\}$
F	$\{3,5,7,9,11,\ldots\}$	$\{\}$
G	$\{\}$	$\{\}$
H	$\{\}$	$\{\}$

$$E = C \cap \{\ldots,-4,-2,0,2,4,\ldots\}$$

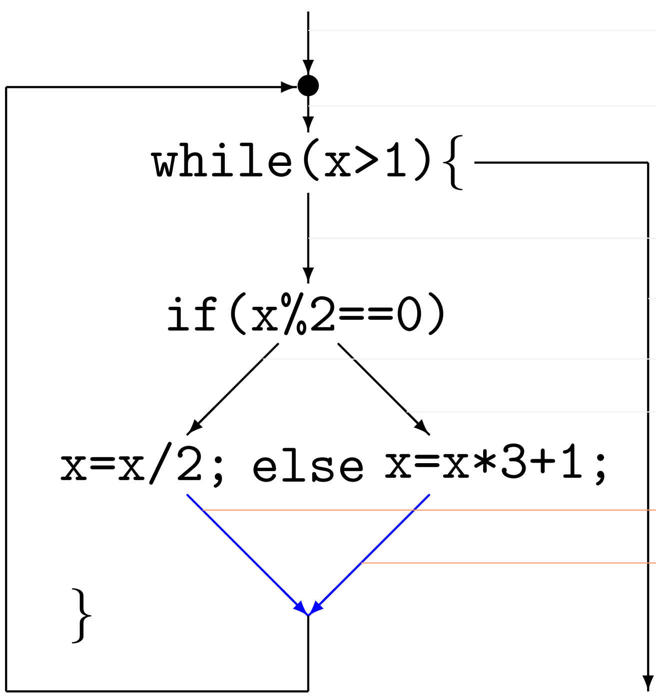
$$F = C \cap \{\ldots,-3,-1,1,3,\ldots\}$$

Collecting Semantics für $I\!N$



	neu: $\Phi^5(\perp)$	alt: $\Phi^4(\perp)$
A :		$\{0,1,2,3,4\ldots\}$
B :		$\{0,1,2,3,4\ldots\}$
C :		$\{2,3,4,5,6\ldots\}$
D :		$\{0,1\}$
E :		$\{2,4,6,8,10,\ldots\}$
F :		$\{3,5,7,9,11,\ldots\}$
G :		$\{\}$
H :		$\{\}$

Collecting Semantics für $\mathbb{N}$

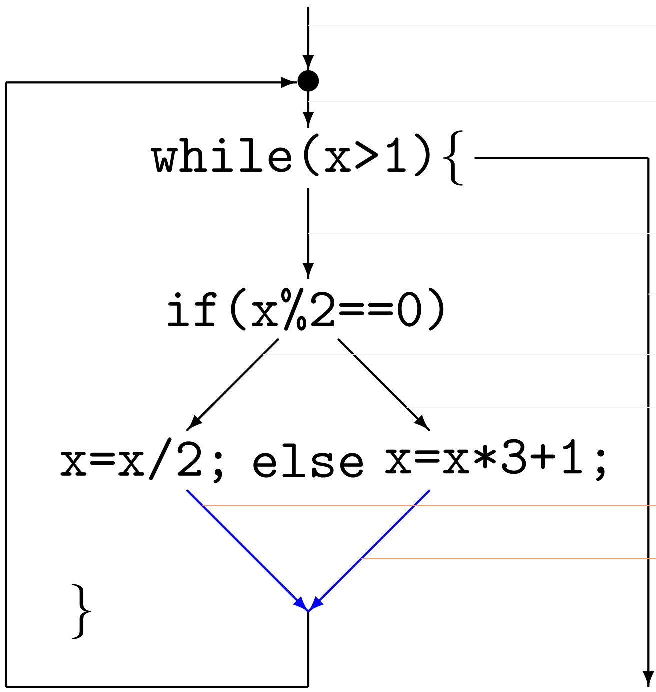


	neu: $\Phi^5(\bot)$	alt: $\Phi^4(\bot)$
A	$\{0,1,2,3,4\ldots\}$	$\{0,1,2,3,4\ldots\}$
B	$\{0,1,2,3,4\ldots\}$	$\{0,1,2,3,4\ldots\}$
C	$\{2,3,4,5,6\ldots\}$	$\{2,3,4,5,6\ldots\}$
D	$\{0,1\}$	$\{0,1\}$
E	$\{2,4,6,8,10,\ldots\}$	$\{2,4,6,8,10,\ldots\}$
F	$\{3,5,7,9,11,\ldots\}$	$\{3,5,7,9,11,\ldots\}$
G	$\{1,2,3,4,5,\ldots\}$	$\{\}$
H	$\{10,16,22,28,34,\ldots\}$	$\{\}$

$$G = \{n/2 \mid n \in E\}$$

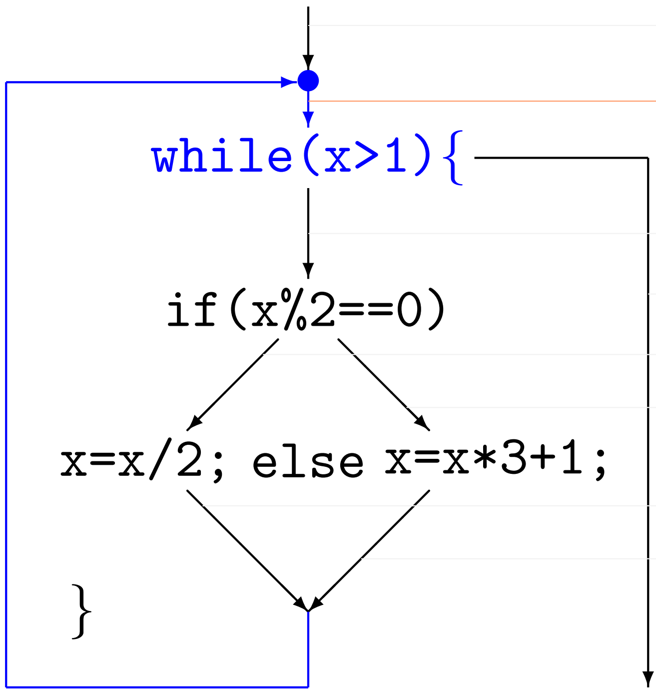
$$H = \{3 \cdot n + 1 \mid n \in F\}$$

Collecting Semantics für $I\!N$



	neu: $\Phi^6(\perp)$	alt: $\Phi^5(\perp)$
$A:$		$\{0,1,2,3,4\ldots\}$
$B:$		$\{0,1,2,3,4\ldots\}$
$C:$		$\{2,3,4,5,6\ldots\}$
$D:$		$\{0,1\}$
$E:$		$\{2,4,6,8,10,\ldots\}$
$F:$		$\{3,5,7,9,11,\ldots\}$
$G:$		$\{1,2,3,4,5,\ldots\}$
$H:$		$\{10,16,22,28,34,\ldots\}$

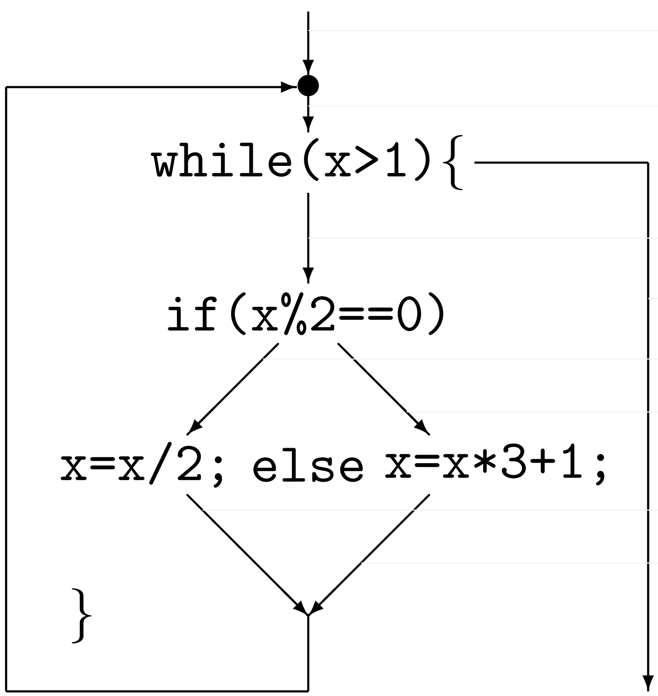
Collecting Semantics für $I\!N$



	neu: $\Phi^6(\bot)$	alt: $\Phi^5(\bot)$
A	$\{0,1,2,3,4\ldots\}$	$\{0,1,2,3,4\ldots\}$
B	$\{0,1,2,3,4\ldots\}$	$\{0,1,2,3,4\ldots\}$
C	$\{2,3,4,5,6\ldots\}$	$\{2,3,4,5,6\ldots\}$
D	$\{0,1\}$	$\{0,1\}$
E	$\{2,4,6,8,10,\ldots\}$	$\{2,4,6,8,10,\ldots\}$
F	$\{3,5,7,9,11,\ldots\}$	$\{3,5,7,9,11,\ldots\}$
G	$\{1,2,3,4,5,\ldots\}$	$\{1,2,3,4,5,\ldots\}$
H	$\{10,16,22,28,34,\ldots\}$	$\{10,16,22,28,34,\ldots\}$

$$B = A \cup G \cup H$$

Collecting Semantics für $I\!N$

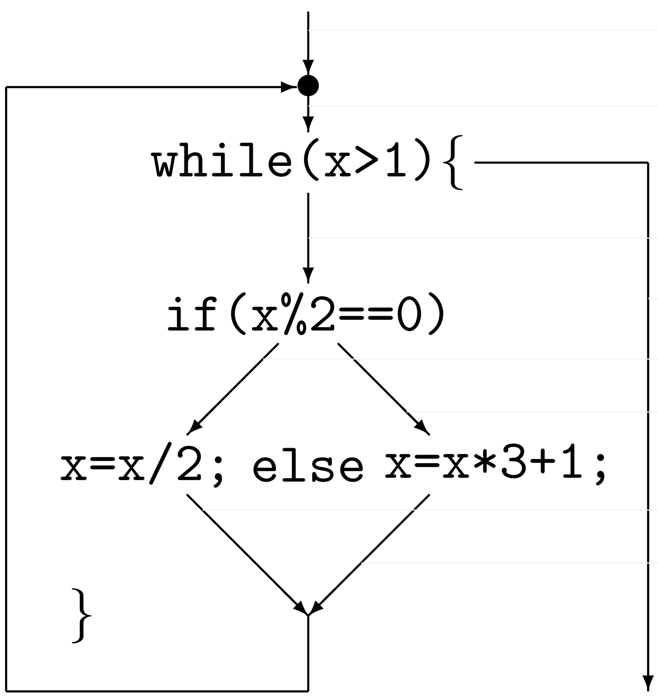


	neu: $\Phi^6(\perp)$	alt: $\Phi^5(\perp)$
A	$\{0,1,2,3,4\ldots\}$	$\{0,1,2,3,4\ldots\}$
B	$\{0,1,2,3,4\ldots\}$	$\{0,1,2,3,4\ldots\}$
C	$\{2,3,4,5,6\ldots\}$	$\{2,3,4,5,6\ldots\}$
D	$\{0,1\}$	$\{0,1\}$
E	$\{2,4,6,8,10,\ldots\}$	$\{2,4,6,8,10,\ldots\}$
F	$\{3,5,7,9,11,\ldots\}$	$\{3,5,7,9,11,\ldots\}$
G	$\{1,2,3,4,5,\ldots\}$	$\{1,2,3,4,5,\ldots\}$
H	$\{10,16,22,28,34,\ldots\}$	$\{10,16,22,28,34,\ldots\}$

Fixpunkt erreicht

Collecting Semantics für $\mathbb{N}$

neu: alt:



A :

B :

C :

D :

E :

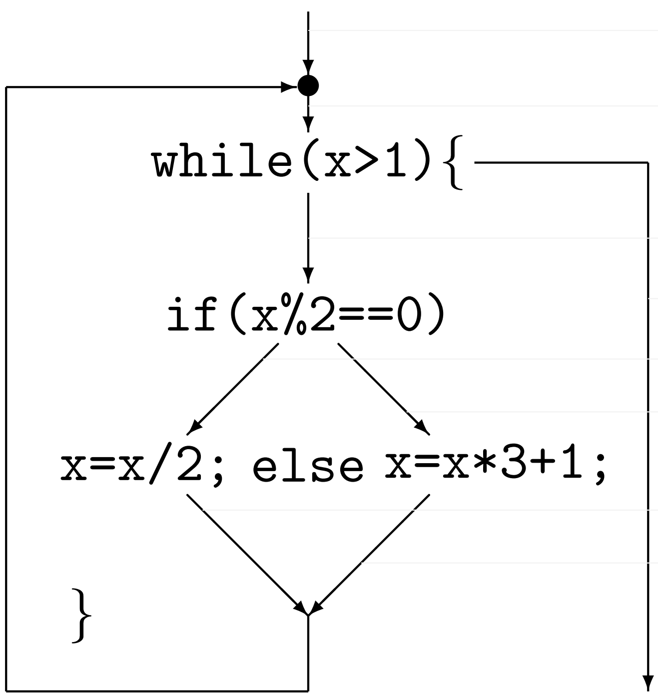
F :

G :

H :

Fixpunkt erreicht

Collecting Semantics für $I\!N$



	neu: $\Phi^{5}(\bot)$	alt: $\Phi^{5}(\bot)$
$A:$	$\{0,1,2,3,4\ldots\}$	$\{0,1,2,3,4\ldots\}$
$B:$	$\{0,1,2,3,4\ldots\}$	$\{0,1,2,3,4\ldots\}$
$C:$	$\{2,3,4,5,6\ldots\}$	$\{2,3,4,5,6\ldots\}$
$D:$	$\{0,1\}$	$\{0,1\}$
$E:$	$\{2,4,6,8,10,\ldots\}$	$\{2,4,6,8,10,\ldots\}$
$F:$	$\{3,5,7,9,11,\ldots\}$	$\{3,5,7,9,11,\ldots\}$
$G:$	$\{1,2,3,4,5,\ldots\}$	$\{1,2,3,4,5,\ldots\}$
$H:$	$\{10,16,22,28,34,\ldots\}$	$\{10,16,22,28,34,\ldots\}$

Fixpunkt erreicht

$E = C \cap \{0,2,4,\ldots\}$

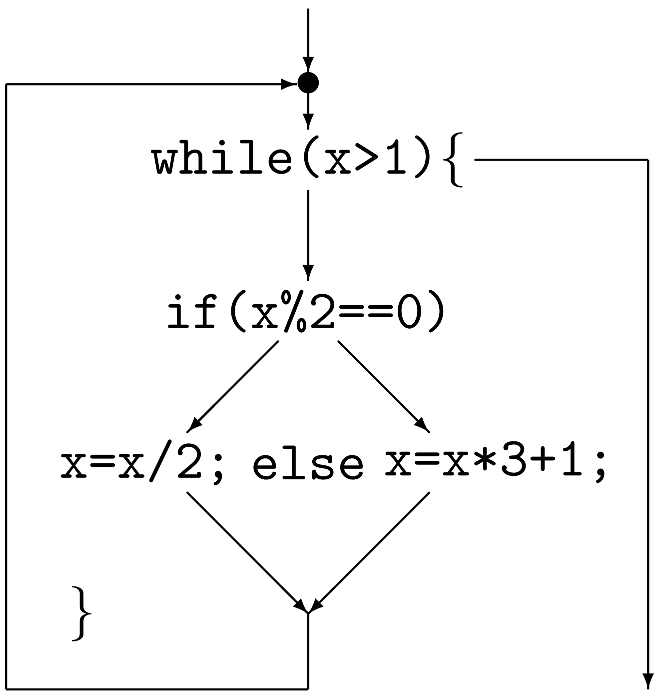
$H = \{3 \cdot x + 1 \mid x \in F\}$

Problem: Rechnen mit Mengen

Wenn z.B. die Menge aller Quadratzahlen als Eingabe zugelassen ist $^{(*)}$, bekommen wir Probleme mit den während der Berechnung auftretenden Mengen.

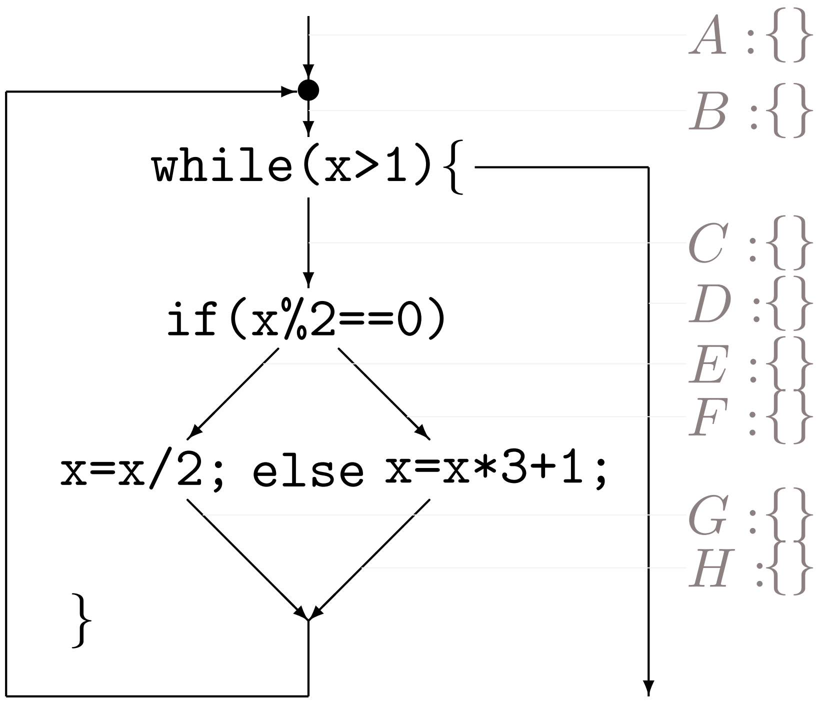
$^{(*)}$ oder vor das Programm z.B. eine Anweisung `x=x*x;` gesetzt wird und davor alle ganzen Zahlen zugelassen werden

Problem: Rechnen mit Mengen

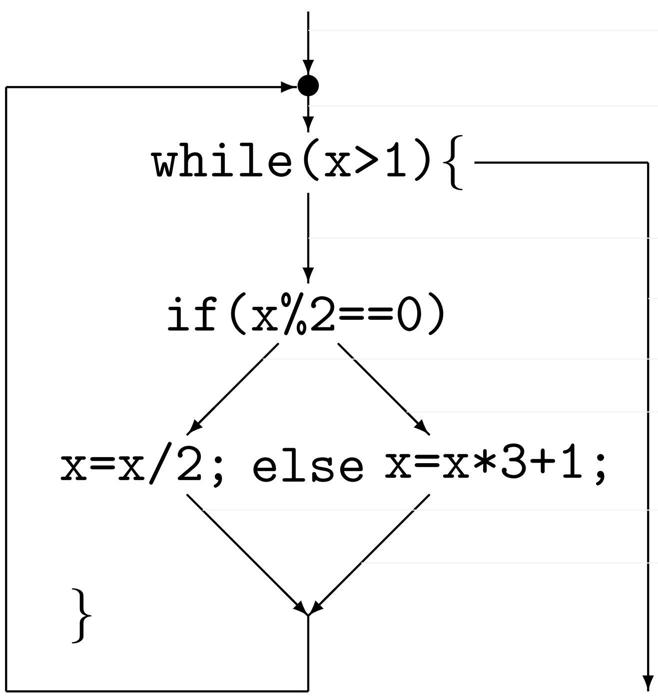


Problem: Rechnen mit Mengen

neu: $\perp$

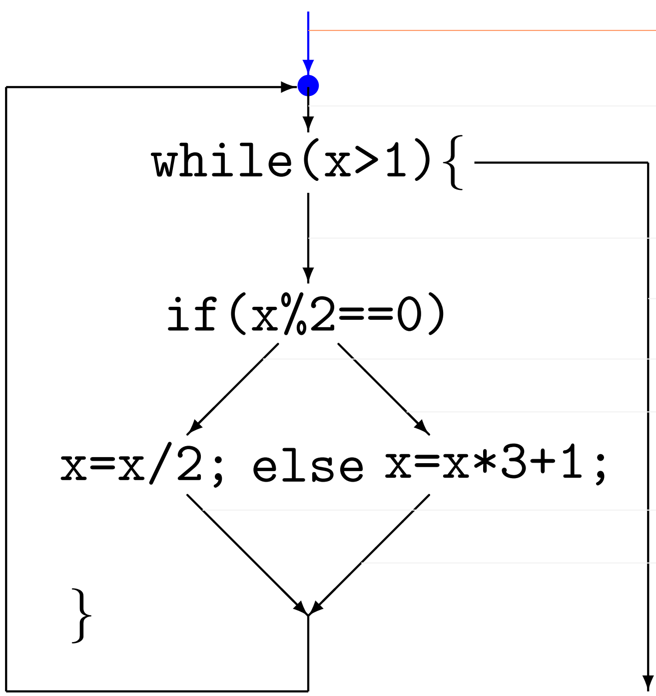


Problem: Rechnen mit Mengen



	neu: $\Phi(\bot)$	alt: $\bot$
A :		$\{\}$
B :		$\{\}$
C :		$\{\}$
D :		$\{\}$
E :		$\{\}$
F :		$\{\}$
G :		$\{\}$
H :		$\{\}$

Problem: Rechnen mit Mengen

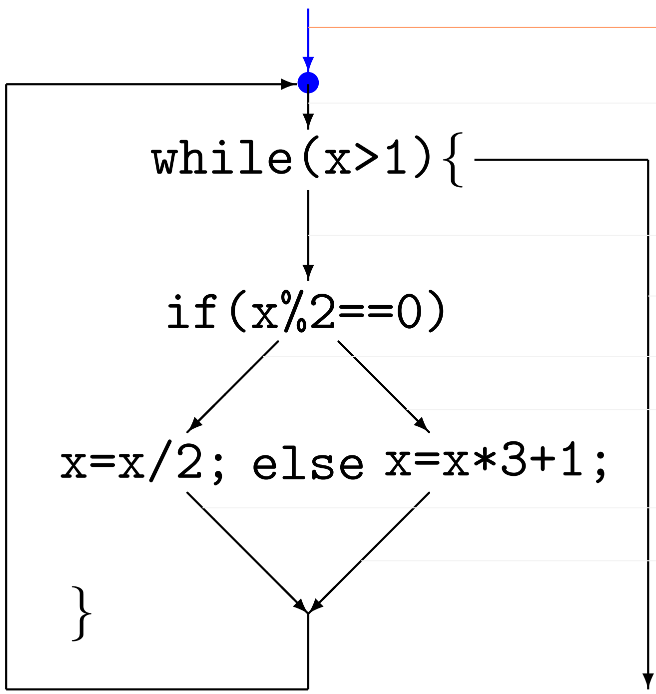


	neu: $\Phi(\perp)$	alt: $\perp$
A	$\{0,1,4,9,16,25,\ldots\}$	$\{\}$
B	$\{\}$	$\{\}$
C	$\{\}$	$\{\}$
D	$\{\}$	$\{\}$
E	$\{\}$	$\{\}$
F	$\{\}$	$\{\}$
G	$\{\}$	$\{\}$
H	$\{\}$	$\{\}$

$$A = \{0,1,4,9,16,25,\ldots\}$$

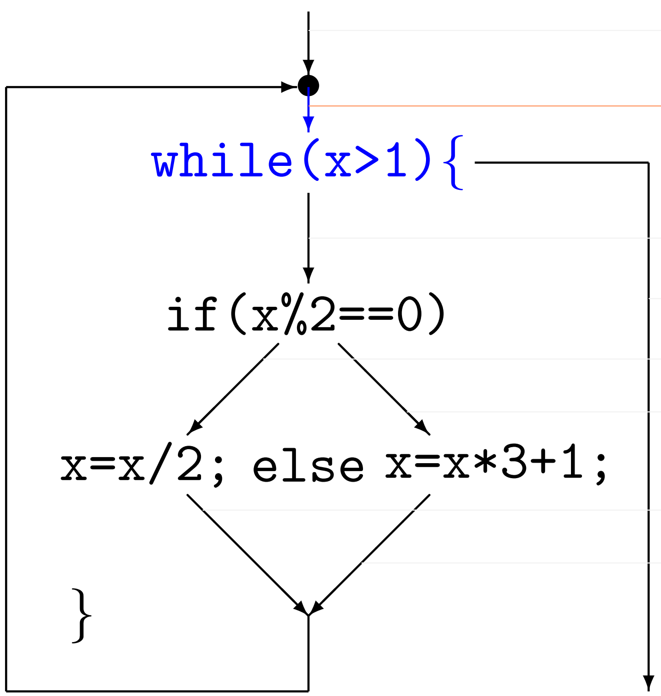
Problem: Rechnen mit Mengen

neu: $\Phi(\Phi(\perp))$ alt: $\Phi(\perp)$



	neu: $\Phi(\Phi(\perp))$	alt: $\Phi(\perp)$
A :		$\{0, 1, 4, 9, 16, 25, \ldots\}$
B :		$\{\}$
C :		$\{\}$
D :		$\{\}$
E :		$\{\}$
F :		$\{\}$
G :		$\{\}$
H :		$\{\}$

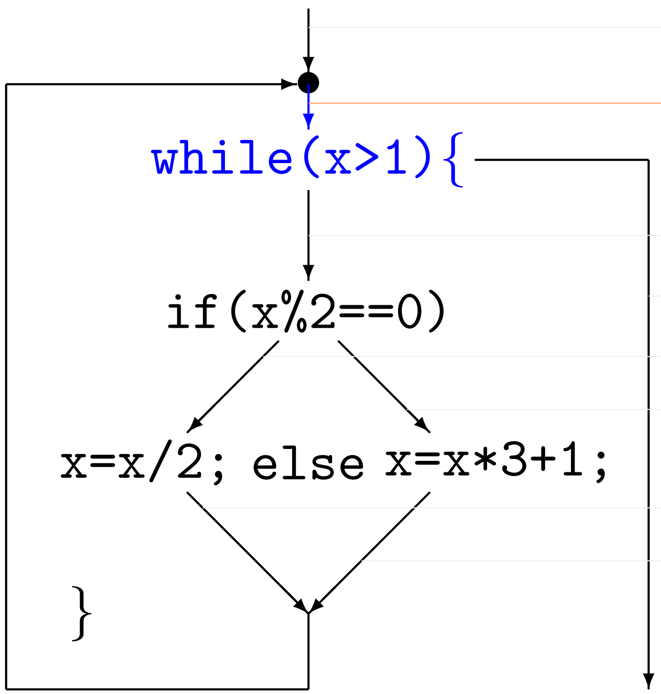
Problem: Rechnen mit Mengen



	neu: $\Phi(\Phi(\perp))$	alt: $\Phi(\perp)$
A :	$\{0,1,4,9,16,25,\ldots\}$	$\{0,1,4,9,16,25,\ldots\}$
B :	$\{0,1,4,9,16,25,\ldots\}$	$\{\}$
C :	$\{\}$	$\{\}$
D :	$\{\}$	$\{\}$
E :	$\{\}$	$\{\}$
F :	$\{\}$	$\{\}$
G :	$\{\}$	$\{\}$
H :	$\{\}$	$\{\}$

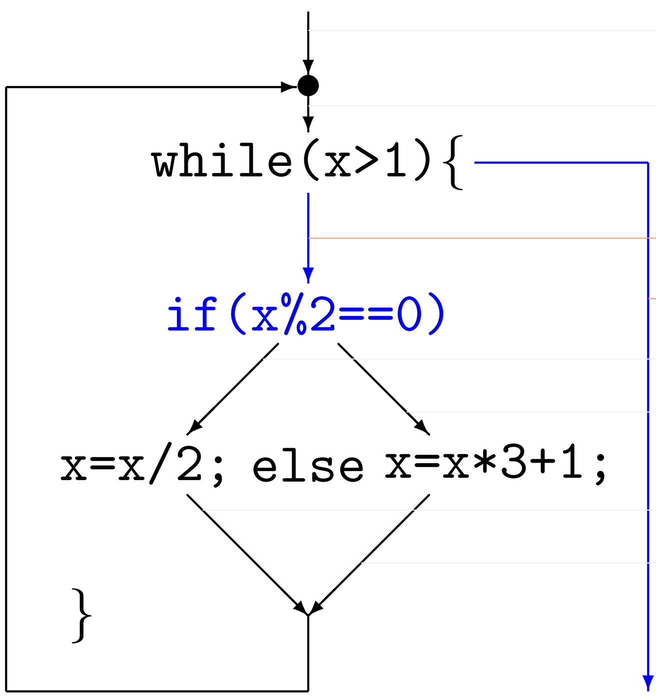
$$B = A \cup G \cup H$$

Problem: Rechnen mit Mengen



	neu: $\Phi^3(\perp)$	alt: $\Phi(\Phi(\perp))$
A :		$\{0,1,4,9,16,25,\ldots\}$
B :		$\{0,1,4,9,16,25,\ldots\}$
C :		$\{\}$
D :		$\{\}$
E :		$\{\}$
F :		$\{\}$
G :		$\{\}$
H :		$\{\}$

Problem: Rechnen mit Mengen



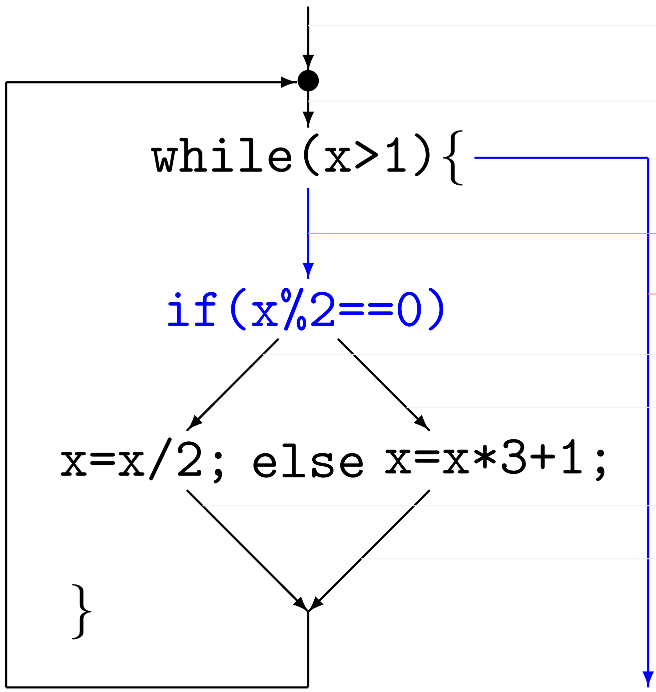
neu: $\Phi^3(\bot)$ alt: $\Phi(\Phi(\bot))$

	neu: $\Phi^3(\bot)$	alt: $\Phi(\Phi(\bot))$
A	$\{0,1,4,9,16,25,\ldots\}$	$\{0,1,4,9,16,25,\ldots\}$
B	$\{0,1,4,9,16,25,\ldots\}$	$\{0,1,4,9,16,25,\ldots\}$
C	$\{4,9,16,25,36,\ldots\}$	$\{\}$
D	$\{0,1\}$	$\{\}$
E	$\{\}$	$\{\}$
F	$\{\}$	$\{\}$
G	$\{\}$	$\{\}$
H	$\{\}$	$\{\}$

$$C = B \cap \{2,3,4,\ldots\}$$

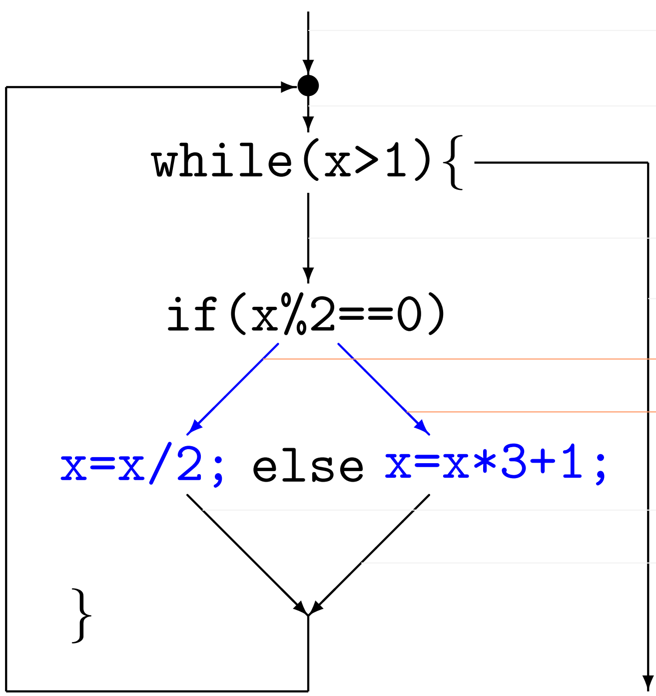
$$D = B \cap \{\ldots,-2,-1,0,1\}$$

Problem: Rechnen mit Mengen



	neu: $\Phi^4(\bot)$	alt: $\Phi^3(\bot)$
A :		$\{0, 1, 4, 9, 16, 25, \ldots\}$
B :		$\{0, 1, 4, 9, 16, 25, \ldots\}$
C :		$\{4, 9, 16, 25, 36, \ldots\}$
D :		$\{0, 1\}$
E :		$\{\}$
F :		$\{\}$
G :		$\{\}$
H :		$\{\}$

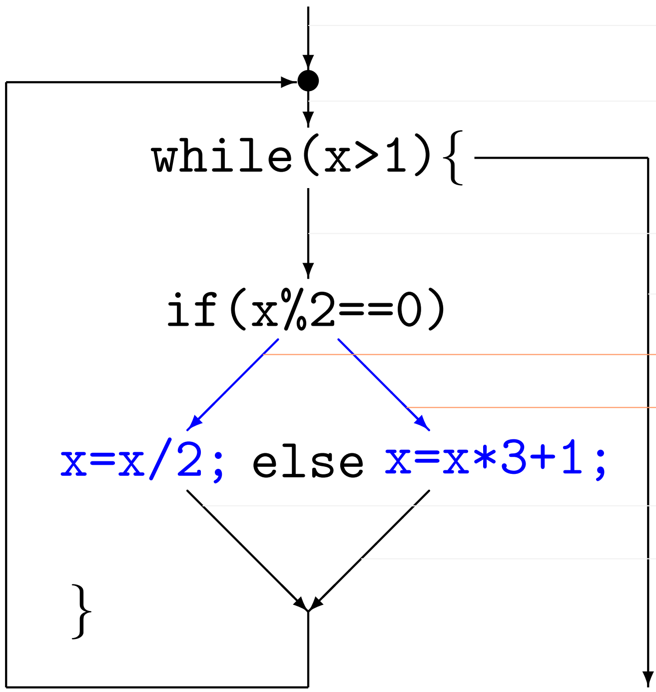
Problem: Rechnen mit Mengen



	neu: $\Phi^4(\bot)$	alt: $\Phi^3(\bot)$
A :	$\{0,1,4,9,16,25,\ldots\}$	$\{0,1,4,9,16,25,\ldots\}$
B :	$\{0,1,4,9,16,25,\ldots\}$	$\{0,1,4,9,16,25,\ldots\}$
C :	$\{4,9,16,25,36,\ldots\}$	$\{4,9,16,25,36,\ldots\}$
D :	$\{0,1\}$	$\{0,1\}$
E :	$\{4,16,36,64,100,\ldots\}$	$\{\}$
F :	$\{9,25,49,81,121,\ldots\}$	$\{\}$
G :	$\{\}$	$\{\}$
H :	$\{\}$	$\{\}$

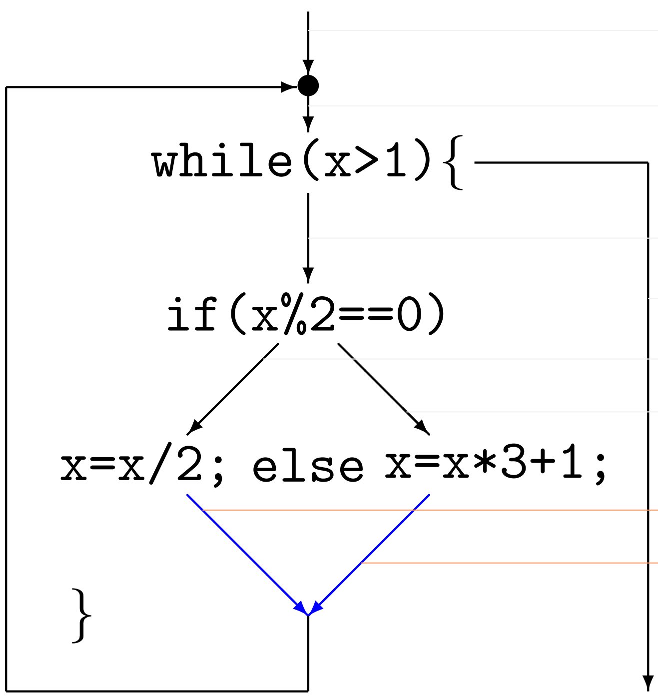
$$E = C \cap \{\ldots,-4,-2,0,2,4,\ldots\}$$
$$F = C \cap \{\ldots,-3,-1,1,3,\ldots\}$$

Problem: Rechnen mit Mengen



	neu: $\Phi^5(\bot)$	alt: $\Phi^4(\bot)$
A :		$\{0, 1, 4, 9, 16, 25, \ldots\}$
B :		$\{0, 1, 4, 9, 16, 25, \ldots\}$
C :		$\{4, 9, 16, 25, 36, \ldots\}$
D :		$\{0, 1\}$
E :		$\{4, 16, 36, 64, 100, \ldots\}$
F :		$\{9, 25, 49, 81, 121, \ldots\}$
G :		$\{\}$
H :		$\{\}$

Problem: Rechnen mit Mengen

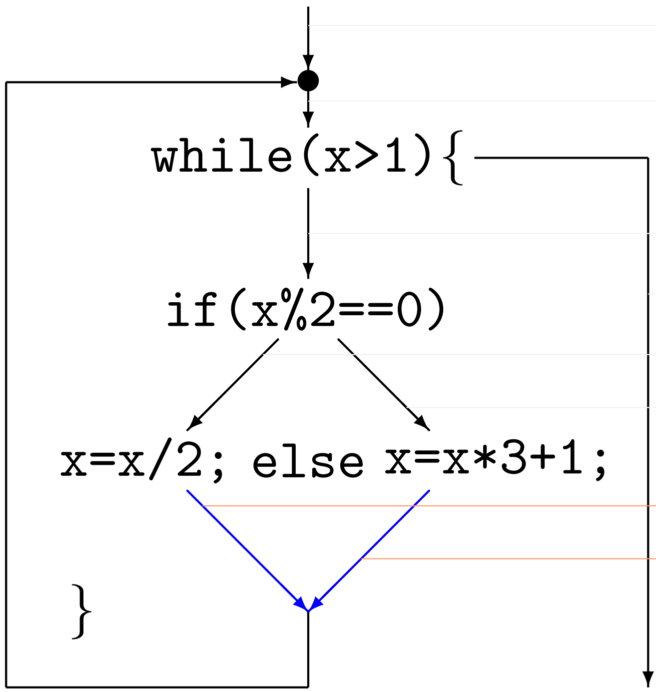


	neu: $\Phi^5(\bot)$	alt: $\Phi^4(\bot)$
A :	$\{0,1,4,9,16,25,\ldots\}$	$\{0,1,4,9,16,25,\ldots\}$
B :	$\{0,1,4,9,16,25,\ldots\}$	$\{0,1,4,9,16,25,\ldots\}$
C :	$\{4,9,16,25,36,\ldots\}$	$\{4,9,16,25,36,\ldots\}$
D :	$\{0,1\}$	$\{0,1\}$
E :	$\{4,16,36,64,100,\ldots\}$	$\{4,16,36,64,100,\ldots\}$
F :	$\{9,25,49,81,121,\ldots\}$	$\{9,25,49,81,121,\ldots\}$
G :	$\{2,8,18,32,50,\ldots\}$	$\{\}$
H :	$\{28,76,148,244,364,\ldots\}$	$\{\}$

$$G = \{n/2 \mid n \in E\}$$

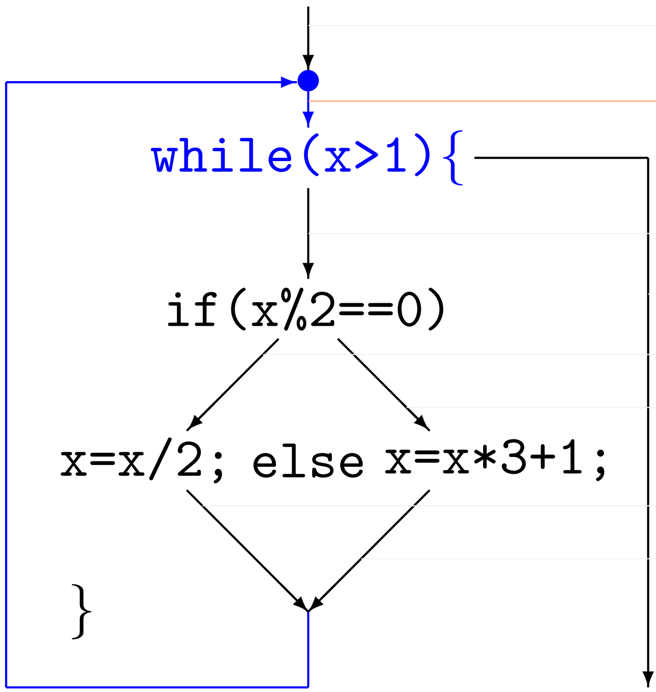
$$H = \{3 \cdot n + 1 \mid n \in F\}$$

Problem: Rechnen mit Mengen



	neu: $\Phi^6(\bot)$	alt: $\Phi^5(\bot)$
A :		$\{0, 1, 4, 9, 16, 25, \ldots\}$
B :		$\{0, 1, 4, 9, 16, 25, \ldots\}$
C :		$\{4, 9, 16, 25, 36, \ldots\}$
D :		$\{0, 1\}$
E :		$\{4, 16, 36, 64, 100, \ldots\}$
F :		$\{9, 25, 49, 81, 121, \ldots\}$
G :		$\{2, 8, 18, 32, 50, \ldots\}$
H :		$\{28, 76, 148, 244, 364, \ldots\}$

Problem: Rechnen mit Mengen

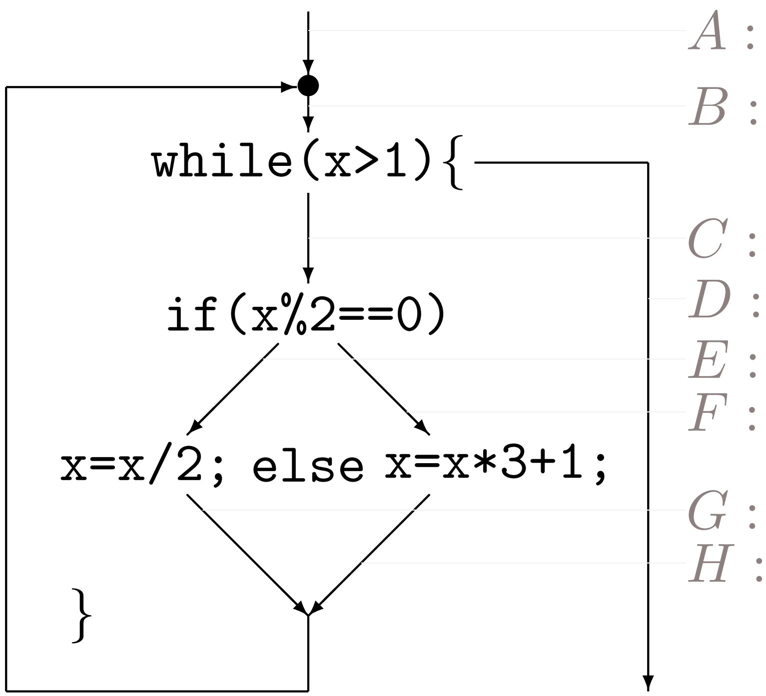


	neu: $\Phi^6(\perp)$	alt: $\Phi^5(\perp)$
A	$:\{0,1,4,9,16,25,\ldots\}$	$\{0,1,4,9,16,25,\ldots\}$
B	$:\{?,\ldots,?,\ldots\}$	$\{0,1,4,9,16,25,\ldots\}$
C	$:\{4,9,16,25,36,\ldots\}$	$\{4,9,16,25,36,\ldots\}$
D	$:\{0,1\}$	$\{0,1\}$
E	$:\{4,16,36,64,100,\ldots\}$	$\{4,16,36,64,100,\ldots\}$
F	$:\{9,25,49,81,121,\ldots\}$	$\{9,25,49,81,121,\ldots\}$
G	$:\{2,8,18,32,50,\ldots\}$	$\{2,8,18,32,50,\ldots\}$
H	$:\{28,76,148,244,364,\ldots\}$	$\{28,76,148,244,364,\ldots\}$

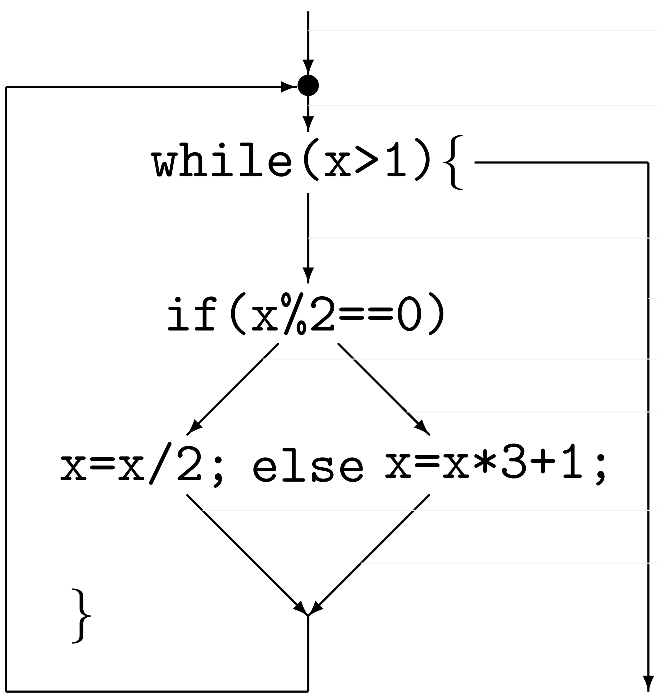
$$B = A \cup G \cup H$$

Problem: Rechnen mit Mengen

neu: alt:



Problem: Rechnen mit Mengen



	neu: $\Phi^{5}(\underline{\bot})$	alt: $\Phi^{5}(\underline{\bot})$
$A:$	$\{0,1,4,9,16,25,\ldots\}$	$\{0,1,4,9,16,25,\ldots\}$
$B:$	$\{0,1,4,9,16,25,\ldots\}$	$\{0,1,4,9,16,25,\ldots\}$
$C:$	$\{4,9,16,25,36,\ldots\}$	$\{4,9,16,25,36,\ldots\}$
$D:$	$\{0,1\}$	$\{0,1\}$
$E:$	$\{4,16,36,64,100,\ldots\}$	$\{4,16,36,64,100,\ldots\}$
$F:$	$\{9,25,49,81,121,\ldots\}$	$\{9,25,49,81,121,\ldots\}$
$G:$	$\{2,8,18,32,50,\ldots\}$	$\{2,8,18,32,50,\ldots\}$
$H:$	$\{28,76,148,244,364,\ldots\}$	$\{28,76,148,244,364,\ldots\}$

Fixpunkt erreicht

[illegible]

Problem: Rechnen mit Mengen

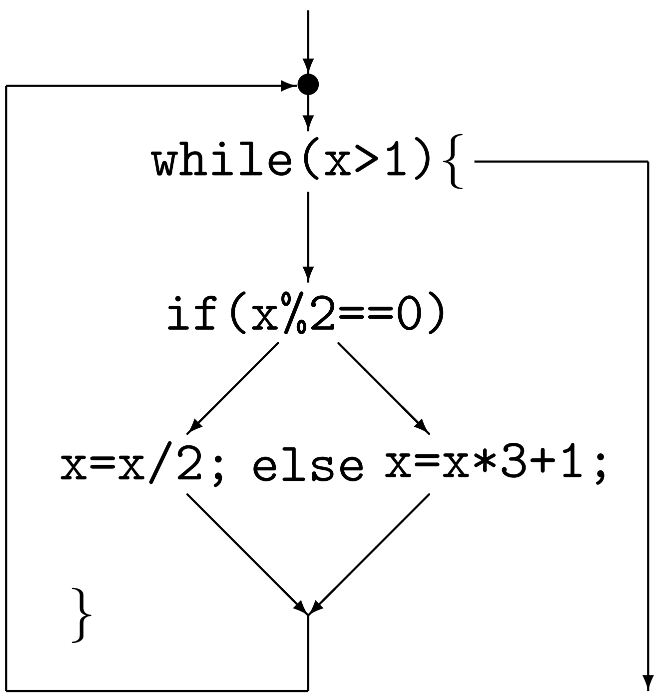
Letztendlich soll die Fixpunktberechnung per Computer durchgeführt werden.

Dafür muß eine geeignete Datenstruktur zur Darstellung der auftretenden Mengen gefunden werden.

Bitvektoren können nur endliche Mengen (z.B. $\{0, \ldots, 2^{43}\}$ mit 1024 GB Speicher) darstellen.
Treten z.B. 10 Variablen im Programm auf, kann jeweils nur ein Wertebereich $\{0, \ldots, 18\}$ mit 1024 GB dargestellt werden.

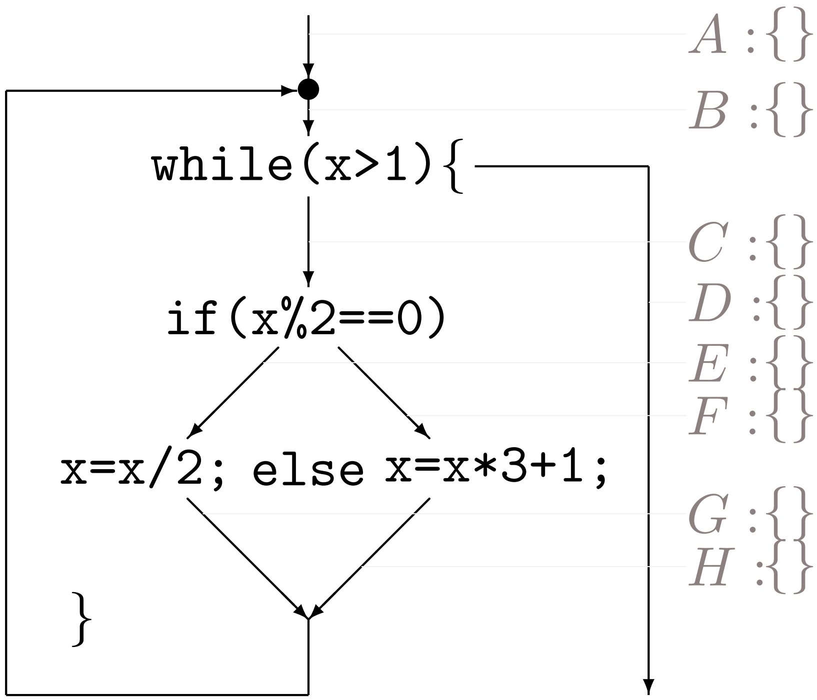
Wir versuchen daher, die Mengen in symbolischer Form darzustellen.

Rechnen mit Mengen (symbolisch)



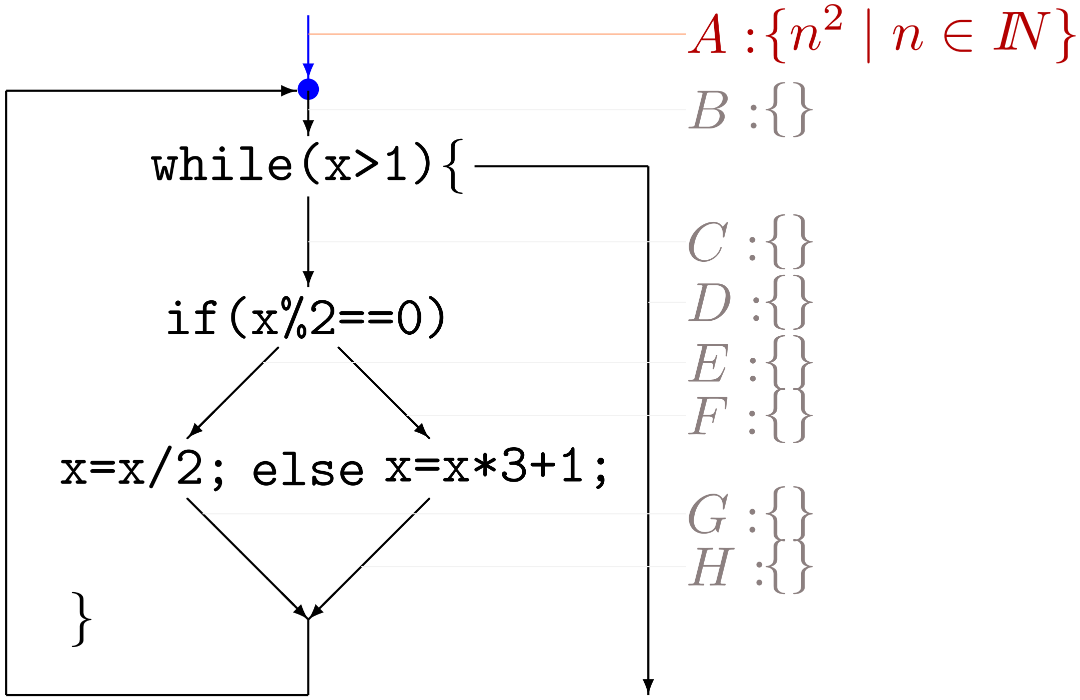
Rechnen mit Mengen (symbolisch)

neu: $\perp$



Rechnen mit Mengen (symbolisch)

neu: $\Phi(\perp)$



$$A = \{n^2 \mid n \in I\!\!N\}$$

Rechnen mit Mengen (symbolisch)

neu: $\Phi(\perp)$

```
while(x>1){
if(x%2==0)
```

$A: \{n^2 \mid n \in I\!N\}$

$B: \{\}$

$C: \{\}$

$D: \{\}$

$E: \{\}$

$F: \{\}$

$G: \{\}$

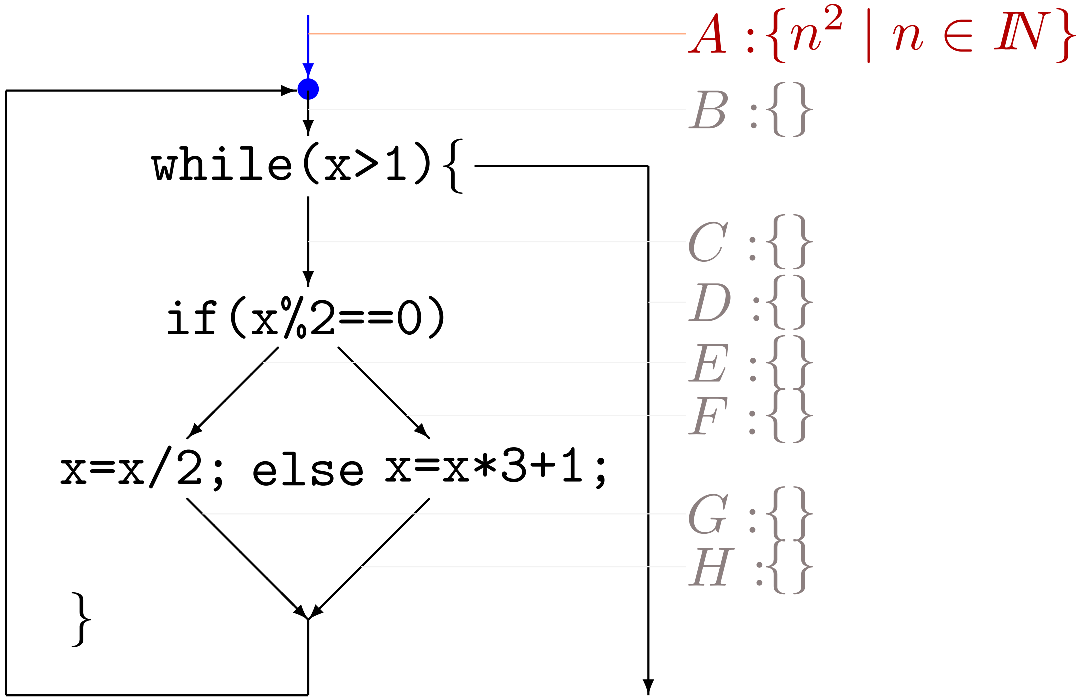
$H: \{\}$

Unendliche Mengen müssen mit Hilfe von symbolischen Prädikaten ("intensional") dargestellt werden.

$$A = \{n^2 \mid n \in I\!N\}$$

Rechnen mit Mengen (symbolisch)

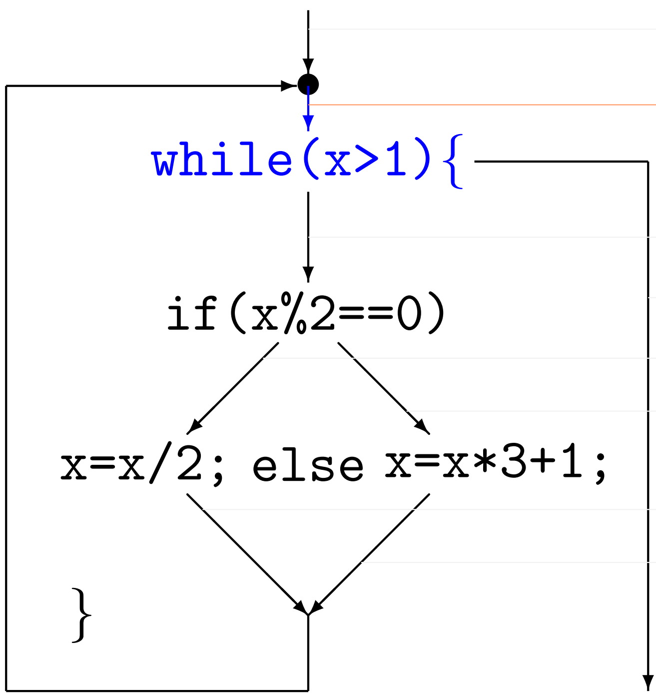
neu: $\Phi(\perp)$



$$A = \{n^2 \mid n \in I\!\!N\}$$

Rechnen mit Mengen (symbolisch)

neu: $\Phi(\Phi(\bot))$



$A : \{n^2 \mid n \in \mathbb{N}\}$

$B : \{n^2 \mid n \in \mathbb{N}\}$

$C : \{\}$

$D : \{\}$

$E : \{\}$

$F : \{\}$

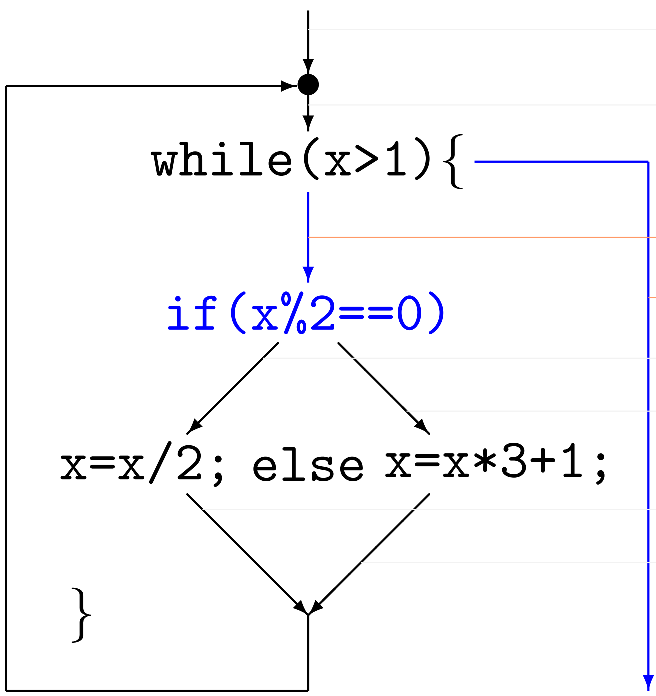
$G : \{\}$

$H : \{\}$

$$B = A \cup G \cup H$$

Rechnen mit Mengen (symbolisch)

neu: $\Phi^3(\bot)$



$A : \{n^2 \mid n \in I\!N\}$

$B : \{n^2 \mid n \in I\!N\}$

$C : \{n^2 \mid n \in I\!N \wedge n \geq 2\}$

$D : \{0, 1\}$

$E : \{\}$

$F : \{\}$

$G : \{\}$

$H : \{\}$

$$C = B \cap \{n \mid n \in \mathbb{Z} \wedge n > 1\}$$

$$D = B \cap \{n \mid n \in \mathbb{Z} \wedge n \leq 1\}$$

Rechnen mit Mengen (symbolisch)

neu: $\Phi^3(\bot)$

```
while(x>1){
```

$A : \{n^2 \mid n \in \mathbb{N}\}$

$B : \{n^2 \mid n \in \mathbb{N}\}$

$C : \{n^2 \mid n \in \mathbb{N} \wedge n \geq 2\}$

$D : \{0, 1\}$

```
if(x%2==0)
```

$E : \{\}$

$F : \{\}$

$G : \{\}$

$H : \{\}$

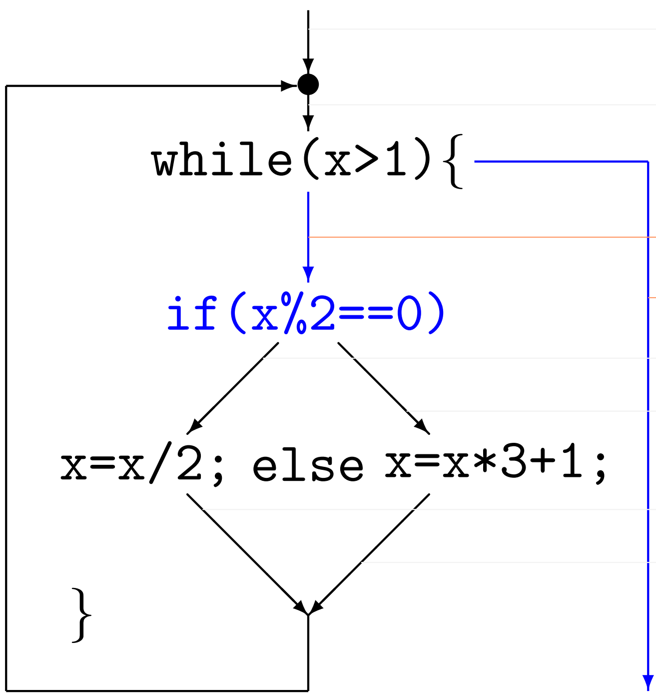
Für den Durchschnitt zweier intensionaler Mengenausdrücke muß ein Resultat-Mengenausdruck bestimmt werden können.

$$C = B \cap \{n \mid n \in \mathbf{Z} \wedge n > 1\}$$

$$D = B \cap \{n \mid n \in \mathbf{Z} \wedge n \leq 1\}$$

Rechnen mit Mengen (symbolisch)

neu: $\Phi^3(\perp)$



$A : \{n^2 \mid n \in \mathbb{N}\}$

$B : \{n^2 \mid n \in \mathbb{N}\}$

$C : \{n^2 \mid n \in \mathbb{N} \wedge n \geq 2\}$

$D : \{0, 1\}$

$E : \{\}$

$F : \{\}$

$G : \{\}$

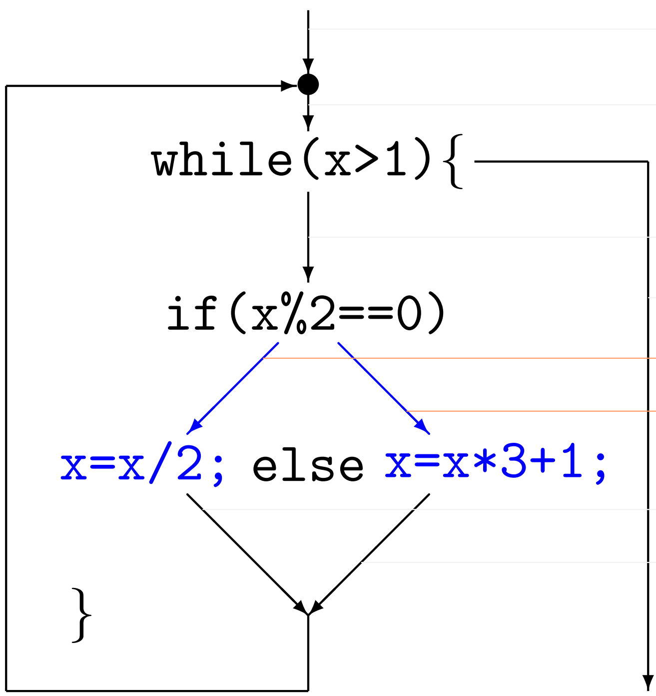
$H : \{\}$

$$C = B \cap \{n \mid n \in \mathbb{Z} \wedge n > 1\}$$

$$D = B \cap \{n \mid n \in \mathbb{Z} \wedge n \leq 1\}$$

Rechnen mit Mengen (symbolisch)

neu: $\Phi^4(\perp)$



$A: \{n^2 \mid n \in \mathbb{N}\}$

$B: \{n^2 \mid n \in \mathbb{N}\}$

$C: \{n^2 \mid n \in \mathbb{N} \wedge n \geq 2\}$

$D: \{0, 1\}$

$E: \{4n^2 \mid n \in \mathbb{N} \wedge n \geq 1\}$

$F: \{4n^2+4n+1 \mid n \in \mathbb{N} \wedge n \geq 1\}$

$G: \{\}$

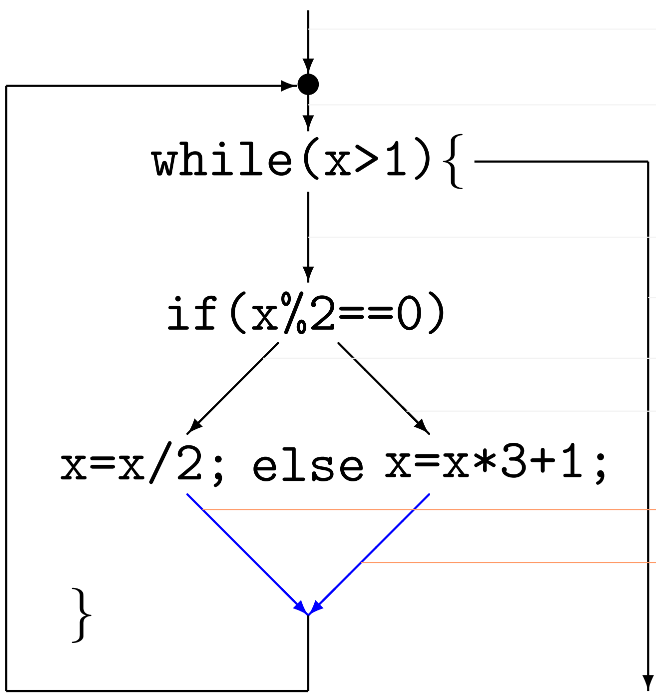
$H: \{\}$

$$E = C \cap \{n \mid n \in \mathbb{Z} \wedge n\%2 = 0\}$$

$$F = C \cap \{n \mid n \in \mathbb{Z} \wedge n\%2 \neq 0\}$$

Rechnen mit Mengen (symbolisch)

neu: $\Phi^5(\bot)$



$A : \{n^2 \mid n \in I\!N\}$

$B : \{n^2 \mid n \in I\!N\}$

$C : \{n^2 \mid n \in I\!N \land n \geq 2\}$

$D : \{0, 1\}$

$E : \{4n^2 \mid n \in I\!N \land n \geq 1\}$

$F : \{4n^2 + 4n + 1 \mid n \in I\!N \land n \geq 1\}$

$G : \{2n^2 \mid n \in I\!N \land n \geq 1\}$

$H : \{12n^2 + 12n + 4 \mid n \in I\!N \land n \geq 1\}$

$$G = \{n/2 \mid n \in E\}$$

$$H = \{3 \cdot n + 1 \mid n \in F\}$$

Rechnen mit Mengen (symbolisch)

neu: $\Phi^5(\bot)$

```
while(x>1){
if(x%2==0)
```

$A : \{n^2 \mid n \in \mathbb{N}\}$

$B : \{n^2 \mid n \in \mathbb{N}\}$

$C : \{n^2 \mid n \in \mathbb{N} \wedge n \geq 2\}$

$D : \{0, 1\}$

$E : \{4n^2 \mid n \in \mathbb{N} \wedge n \geq 1\}$

$F : \{4n^2 + 4n + 1 \mid n \in \mathbb{N} \wedge n \geq 1\}$

$G : \{2n^2 \mid n \in \mathbb{N} \wedge n \geq 1\}$

$H : \{12n^2 + 12n + 4 \mid n \in \mathbb{N} \wedge n \geq 1\}$

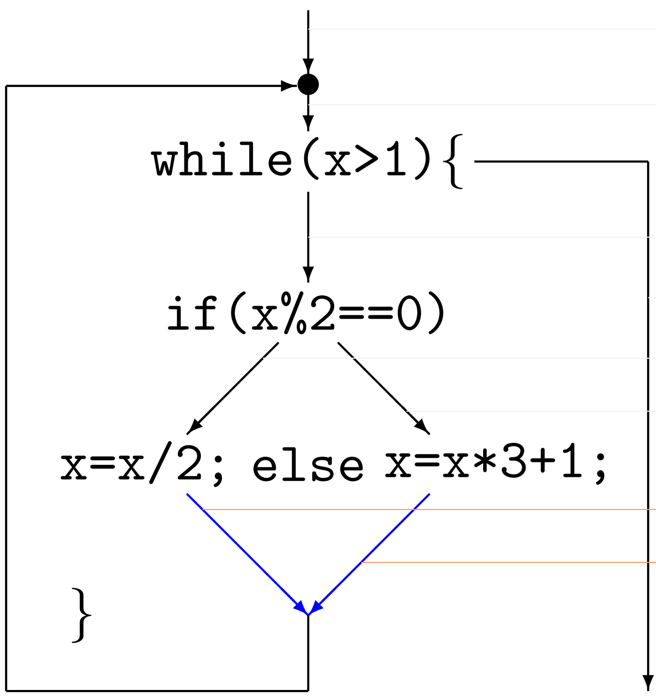
Für die Anwendung im Programm auftretender Operationen auf einen Mengenausdruck muß ein Resultat-Mengenausdruck bestimmt werden können.

$$G = \{n/2 \mid n \in E\}$$

$$H = \{3 \cdot n + 1 \mid n \in F\}$$

Rechnen mit Mengen (symbolisch)

neu: $\Phi^5(\perp)$



$A: \{n^2 \mid n \in I\!N\}$

$B: \{n^2 \mid n \in I\!N\}$

$C: \{n^2 \mid n \in I\!N \wedge n \geq 2\}$

$D: \{0, 1\}$

$E: \{4n^2 \mid n \in I\!N \wedge n \geq 1\}$

$F: \{4n^2 + 4n + 1 \mid n \in I\!N \wedge n \geq 1\}$

$G: \{2n^2 \mid n \in I\!N \wedge n \geq 1\}$

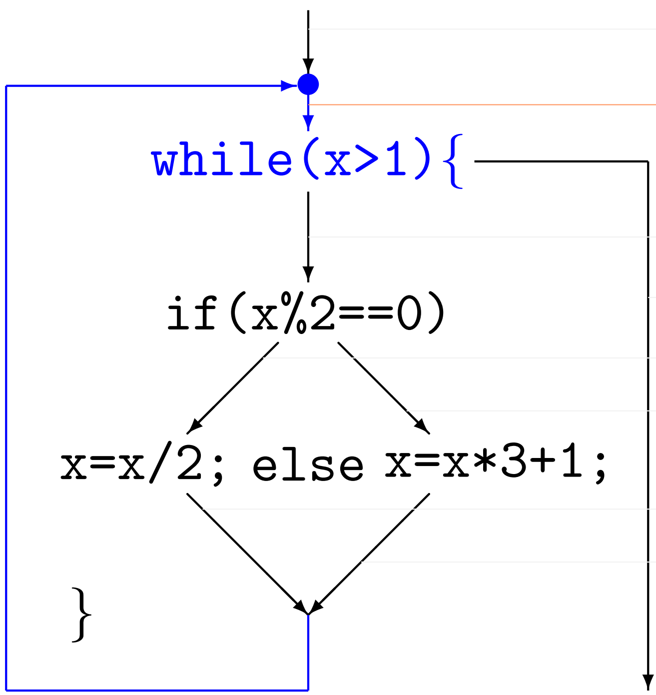
$H: \{12n^2 + 12n + 4 \mid n \in I\!N \wedge n \geq 1\}$

$$G = \{n/2 \mid n \in E\}$$

$$H = \{3 \cdot n + 1 \mid n \in F\}$$

Rechnen mit Mengen (symbolisch)

neu: $\Phi^6(\perp)$



$A : \{n^2 \mid n \in I\!N\}$

$B : \{n^2 \mid n \in I\!N\} \cup \{2n^2 \mid n \in I\!N\} \cup \{12n^2 + 12n + 4 \mid n \in I\!N\}$

$C : \{n^2 \mid n \in I\!N \wedge n \geq 2\}$

$D : \{0, 1\}$

$E : \{4n^2 \mid n \in I\!N \wedge n \geq 1\}$

$F : \{4n^2 + 4n + 1 \mid n \in I\!N \wedge n \geq 1\}$

$G : \{2n^2 \mid n \in I\!N \wedge n \geq 1\}$

$H : \{12n^2 + 12n + 4 \mid n \in I\!N \wedge n \geq 1\}$

$$B = A \cup G \cup H$$

Rechnen mit Mengen (symbolisch)

neu: $\Phi^6(\perp)$

```
while(x>1){
```

Um feststellen zu können, ob ein Fixpunkt erreicht ist, muß entschieden werden können, ob zwei intensionale Mengenausdrücke die gleiche Menge beschreiben.

$A: \{n^2 \mid n \in I\!N\}$

$B: \{n^2 \mid n \in I\!N\} \cup \{2n^2 \mid n \in I\!N\} \cup \{12n^2 + 12n + 4 \mid n \in I\!N\}$

$C: \{n^2 \mid n \in I\!N \wedge n \geq 2\}$

$D: \{0, 1\}$

$E: \{4n^2 \mid n \in I\!N \wedge n \geq 1\}$

$F: \{4n^2 + 4n + 1 \mid n \in I\!N \wedge n \geq 1\}$

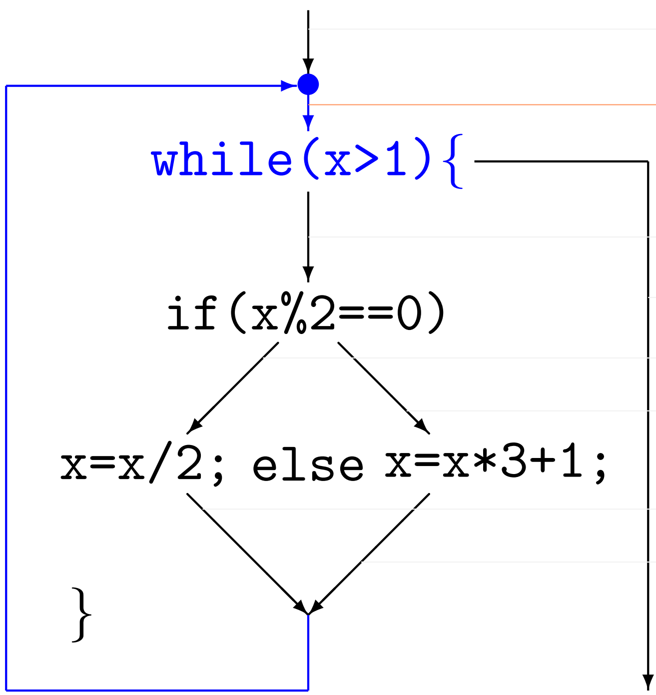
$G: \{2n^2 \mid n \in I\!N \wedge n \geq 1\}$

$H: \{12n^2 + 12n + 4 \mid n \in I\!N \wedge n \geq 1\}$

$$B = A \cup G \cup H$$

Rechnen mit Mengen (symbolisch)

neu: $\Phi^6(\perp)$



$A : \{n^2 \mid n \in \mathbb{N}\}$

$B : \{n^2 \mid n \in \mathbb{N}\} \cup \{2n^2 \mid n \in \mathbb{N}\} \cup \{12n^2+12n+4 \mid n \in \mathbb{N}\}$

$C : \{n^2 \mid n \in \mathbb{N} \wedge n \geq 2\}$

$D : \{0, 1\}$

$E : \{4n^2 \mid n \in \mathbb{N} \wedge n \geq 1\}$

$F : \{4n^2+4n+1 \mid n \in \mathbb{N} \wedge n \geq 1\}$

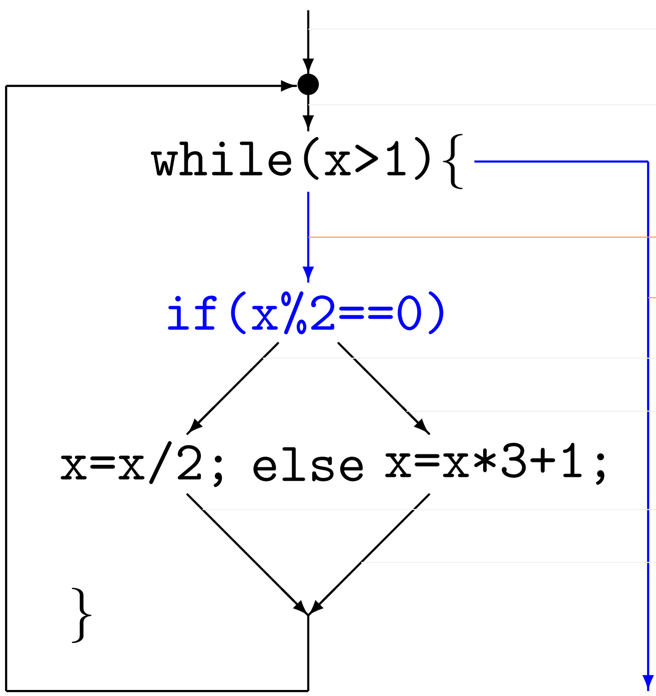
$G : \{2n^2 \mid n \in \mathbb{N} \wedge n \geq 1\}$

$H : \{12n^2+12n+4 \mid n \in \mathbb{N} \wedge n \geq 1\}$

$$B = A \cup G \cup H$$

Rechnen mit Mengen (symbolisch)

neu: $\Phi^7(\perp)$



$A: \{n^2 \mid n \in \mathbb{N}\}$

$B: \{n^2 \mid n \in \mathbb{N}\} \cup \{2n^2 \mid n \in \mathbb{N}\} \cup \{12n^2 + 12n + 4 \mid n \in \mathbb{N}\}$

$C: \{n^2 \mid n \in \mathbb{N} \wedge n \geq 2\} \cup \{2n^2 \mid n \in \mathbb{N} \wedge n \geq 1\} \cup \{12n^2 + 12n + 4 \mid n \in \mathbb{N}\}$

$D: \{0, 1\}$

$E: \{4n^2 \mid n \in \mathbb{N} \wedge n \geq 1\}$

$F: \{4n^2 + 4n + 1 \mid n \in \mathbb{N} \wedge n \geq 1\}$

$G: \{2n^2 \mid n \in \mathbb{N} \wedge n \geq 1\}$

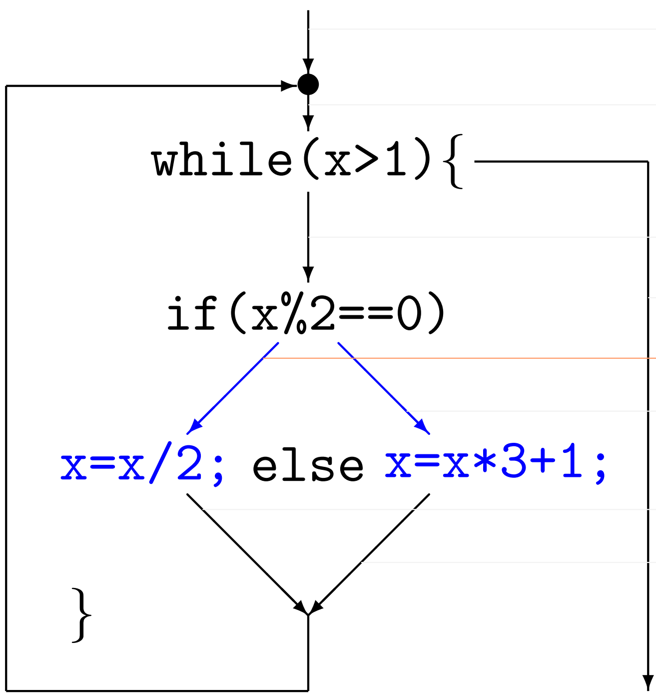
$H: \{12n^2 + 12n + 4 \mid n \in \mathbb{N} \wedge n \geq 1\}$

$$C = B \cap \{n \mid n \in \mathbb{Z} \wedge n > 1\}$$

$$D = B \cap \{n \mid n \in \mathbb{Z} \wedge n \leq 1\}$$

Rechnen mit Mengen (symbolisch)

neu: $\Phi^8(\perp)$



$A: \{n^2 \mid n \in I\!N\}$

$B: \{n^2 \mid n \in I\!N\} \cup \{2n^2 \mid n \in I\!N\} \cup \{12n^2+12n+4 \mid n \in I\!N\}$

$C: \{n^2 \mid n \in I\!N \wedge n \geq 2\} \cup \{2n^2 \mid n \in I\!N \wedge n \geq 1\}$

$D: \{0,1\} \qquad \cup \{12n^2+12n+4 \mid n \in I\!N\}$

$E: \{4n^2 \mid n \in I\!N \wedge n \geq 1\} \cup \{2n^2 \mid n \in I\!N \wedge n \geq 1\}$

$F: \qquad \cup \{12n^2+12n+4 \mid n \in I\!N$

$G: \{2n^2 \mid n \in I\!N \wedge n \geq 1\}$

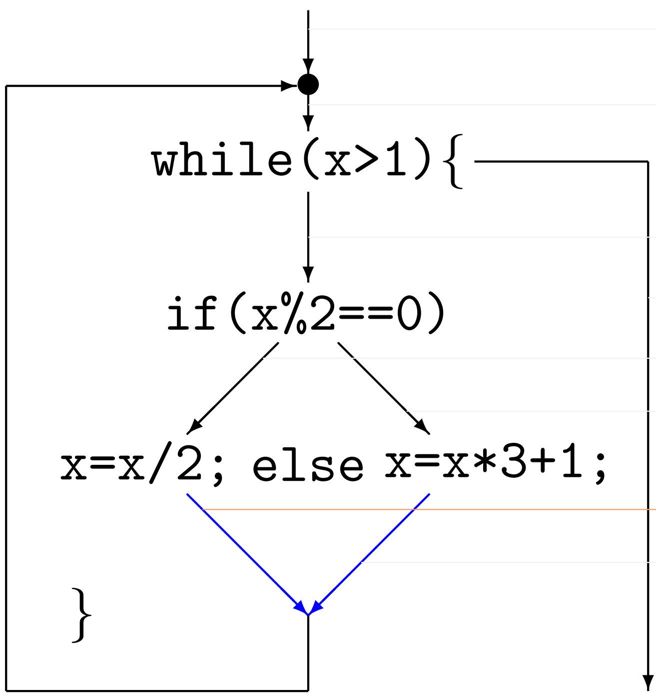
$H: \{12n^2+12n+4 \mid n \in I\!N \wedge n \geq 1\}$

$$E = C \cap \{n \mid n \in \boldsymbol{Z} \wedge n\%2 = 0\}$$

$$F = C \cap \{n \mid n \in \boldsymbol{Z} \wedge n\%2 \neq 0\}$$

Rechnen mit Mengen (symbolisch)

neu: $\Phi^9(\perp)$



$A : \{n^2 \mid n \in \mathbb{N}\}$

$B : \{n^2 \mid n \in \mathbb{N}\} \cup \{2n^2 \mid n \in \mathbb{N}\} \cup \{12n^2+12n+4 \mid n \in \mathbb{N}\}$

$C : \{n^2 \mid n \in \mathbb{N} \wedge n \geq 2\} \cup \{2n^2 \mid n \in \mathbb{N} \wedge n \geq 1\}$

$D : \{0, 1\} \qquad \cup \{12n^2+12n+4 \mid n \in \mathbb{N}\}$

$E : \{4n^2 \mid n \in \mathbb{N} \wedge n \geq 1\} \cup \{2n^2 \mid n \in \mathbb{N} \wedge n \geq 1\}$

$F : \qquad \cup \{12n^2+12n+4 \mid n \in \mathbb{N}$

$G : \{2n^2 \mid n \in \mathbb{N} \wedge n \geq 1\} \cup \{n^2 \mid n \in \mathbb{N} \wedge n \geq 1\}$

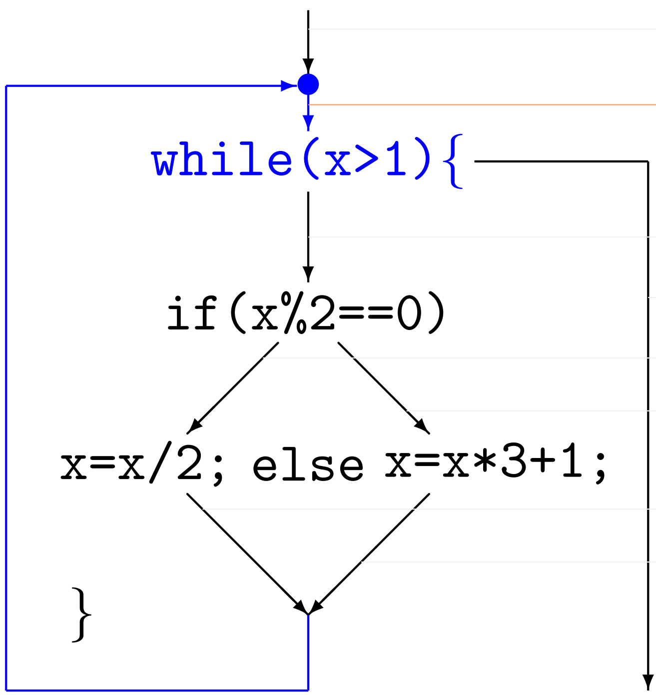
$H : \qquad \cup \{6n^2+6n+2 \mid n \in \mathbb{N}\}$

$$G = \{n/2 \mid n \in E\}$$

$$H = \{3 \cdot n + 1 \mid n \in F\}$$

Rechnen mit Mengen (symbolisch)

neu: $\Phi^{10}(\bot)$



$A : \{n^2 \mid n \in \mathbb{N}\}$

$B : \{\ldots\} \cup \ldots$

$C : \{n^2 \mid n \in \mathbb{N} \wedge n \geq 2\} \cup \{2n^2 \mid n \in \mathbb{N} \wedge n \geq 1\}$

$D : \{0, 1\} \qquad \cup \{12n^2 + 12n + 4 \mid n \in \mathbb{N}\}$

$E : \{4n^2 \mid n \in \mathbb{N} \wedge n \geq 1\} \cup \{2n^2 \mid n \in \mathbb{N} \wedge n \geq 1\}$

$F : \{4n^2 + 4n + 1 \mid n \in \mathbb{N} \wedge n \geq 1\} \cup \{12n^2 + 12n + 4 \mid n \in \mathbb{N}$

$G : \{2n^2 \mid n \in \mathbb{N} \wedge n \geq 1\} \cup \{n^2 \mid n \in \mathbb{N} \wedge n \geq 1\}$

$H : \{12n^2 + 12n + 4 \mid n \in \mathbb{N} \wedge n \geq 1\} \cup \{6n^2 + 6n + 2 \mid n \in \mathbb{N}\}$

$$B = A \cup G \cup H$$

Rechnen mit Mengen (symbolisch)

neu: $\Phi^{10}(\bot)$

```
while(x>1){
if(x%2==0)
```

$A : \{n^2 \mid n \in I\!N\}$

$B : \{\ldots\} \cup \ldots$

$C : \{n^2 \mid n \in I\!N \wedge n \geq 2\} \cup \{2n^2 \mid n \in I\!N \wedge n \geq 1\}$

$D : \{0, 1\} \cup \{12n^2 + 12n + 4 \mid n \in I\!N\}$

$E : \{4n^2 \mid n \in I\!N \wedge n \geq 1\} \cup \{2n^2 \mid n \in I\!N \wedge n \geq 1\}$

$F : \{4n^2 + 4n + 1 \mid n \in I\!N \wedge n \geq 1\} \cup \{12n^2 + 12n + 4 \mid n \in I\!N$

$G : \{2n^2 \mid n \in I\!N \wedge n \geq 1\} \cup \{n^2 \mid n \in I\!N \wedge n \geq 1\}$

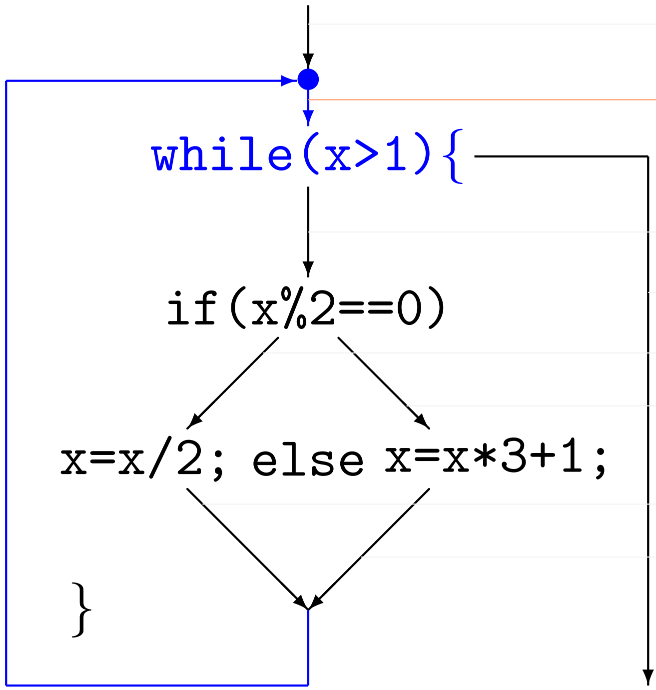
$H : \{12n^2 + 12n + 4 \mid n \in I\!N \wedge n \geq 1\} \cup \{6n^2 + 6n + 2 \mid n \in I\!N\}$

Wahrscheinlich terminiert die Fixpunktberechnung nicht.

$$B = A \cup G \cup H$$

Rechnen mit Mengen (symbolisch)

neu: $\Phi^{10}(\bot)$



$A: \{n^2 \mid n \in I\!N\}$

$B: \{\ldots\} \cup \ldots$

$C: \{n^2 \mid n \in I\!N \wedge n \geq 2\} \cup \{2n^2 \mid n \in I\!N \wedge n \geq 1\}$

$D: \{0, 1\} \qquad \cup \{12n^2 + 12n + 4 \mid n \in I\!N\}$

$E: \{4n^2 \mid n \in I\!N \wedge n \geq 1\} \cup \{2n^2 \mid n \in I\!N \wedge n \geq 1\}$

$F: \{4n^2 + 4n + 1 \mid n \in I\!N \wedge n \geq 1\} \cup \{12n^2 + 12n + 4 \mid n \in I\!N$

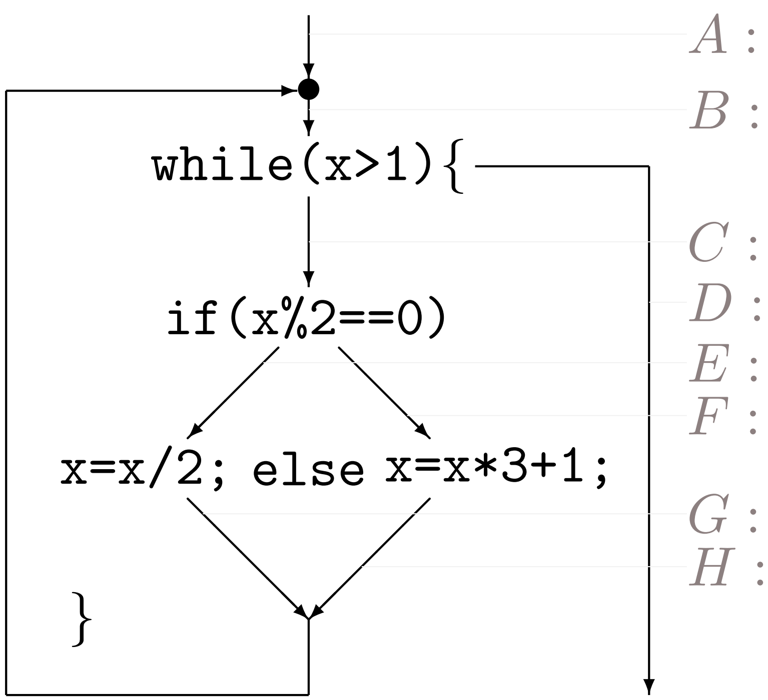
$G: \{2n^2 \mid n \in I\!N \wedge n \geq 1\} \cup \{n^2 \mid n \in I\!N \wedge n \geq 1\}$

$H: \{12n^2 + 12n + 4 \mid n \in I\!N \wedge n \geq 1\} \cup \{6n^2 + 6n + 2 \mid n \in I\!N\}$

$$B = A \cup G \cup H$$

Rechnen mit Mengen (symbolisch)

neu:



Rechnen mit Mengen (symbolisch)

neu: $\Phi(\Phi(\Phi(\bot)))$

```
while(x>1){
```

$A : \{n^2 \mid n \in I\!N\}$

$B : \{n^2 \mid n \in I\!N\} \cup \{2n^2 \mid n \in I\!N\} \cup \{12n^2+12n+4 \mid n \in I\!N\}$

$C : \{n^2 \mid n \in I\!N \wedge n \geq 2\} \cup \{2n^2 \mid n \in I\!N \wedge n \geq 1\}$

$D : \{0, 1\} \qquad \cup \{12n^2+12n+4 \mid n \in I\!N\}$

$E : \{4n^2 \mid n \in I\!N \wedge n \geq 1\} \cup \{2n^2 \mid n \in I\!N \wedge n \geq 1\}$

$F : \{4n^2+4n+1 \mid n \in I\!N \wedge n \geq 1\} \cup \{12n^2+12n+4 \mid n \in I\!N$

$G : \{2n^2 \mid n \in I\!N \wedge n \geq 1\} \cup \{n^2 \mid n \in I\!N \wedge n \geq 1\}$

$H : \{12n^2+12n+4 \mid n \in I\!N \wedge n \geq 1\} \cup \{6n^2+6n+2 \mid n \in I\!N\}$

Um feststellen zu können,

Wahrscheinlich terminiert die Fixpunktberechnung nicht.

Fixpunkt erreicht

$E = C \cap \{n \mid n \in \mathbb{Z} \wedge n\%2 = 0\}$

$F = C \cap \{n \mid n \in \mathbb{Z} \wedge n\%2 \neq 0\}$

Rechnen mit symbolischen intensionalen Mengenausdrücken

Zusammenfassung der Anforderungen:

1. Mindestens Durchschnitt, Vereinigung und Programmoperations-Anwendung muß für Mengenausdrücke berechenbar sein, das Resultat muß insbesondere ausdrückbar sein.
2. Die (extensionale) Gleichheit von Mengenausdrücken muß entscheidbar sein.

Dafür gibt es keine geeigneten Kalküle.
Wegen 2. muß die Form der in Mengenausdrücken erlaubten Prädikate stark eingeschränkt werden.
Dann können aber Mengen, die sich aus der Anwendung von Programmoperationen ergeben, nur in den seltensten Fällen noch ausgedrückt werden.
Außerdem können wir nicht garantieren, daß die Fixpunktberechnung terminiert.

A B S T R A K T E I N T E R P R E T A T I O N

Die genaue Menge der möglichen Variablenwerte an jedem Programmpunkt läßt sich also i.allg. nicht automatisch berechnen.

Wir versuchen daher im Folgenden, wenigstens grobe Informationen über die Programmpunkte zu bestimmen.

Dazu fassen wir jeweils mehrere Einzelwerte zu einem “abstrakten Wert” zusammen.

Abstrakte Interpretation

Je nach Anwendung kommen z.B. infrage:

konkrete Werte	abstrakter Wert
. . . , -3, -2, -1	neg
0	null
1, 2, 3, . . .	pos
. . . -4, -2, 0, 2, 4, . . .	even
. . . -3, -1, 1, 3, . . .	odd

Abstrakte Interpretation

Da wir ohnehin mit Wertemengen statt Einzelwerten rechnen, können wir auch Mengen abstrahieren:

konkrete Mengen	abstrakte Menge
$\{4, 8\}$, $\{4, 7, 8\}$, $\{4, 5, 6, 7, 8\}$, ...	$[4 \ldots 8]$
$\{1, 2, 3, 4, \ldots\}$, $\{1, 2, 4, 8, \ldots\}$, $\{1, 4, 9, 16, \ldots\}$, ...	$[1 \ldots \infty]$

Wenn wir zu jedem Programmpunkt die abstrakte Menge bestimmen können, können wir wenigstens Aussagen über bestimmte Eigenschaften machen, je nach Abstraktionsverfahren z.B. über Vorzeichen oder Wertebereich einer Variablen.

Anforderungen an eine Abstraktion

Korrektheit:
Die für einen Programmpunkt berechnete abstrakte Wertemenge soll die tatsächlich auftretende konkrete Wertemenge nach oben abschätzen.
Überführbarkeit:
Jedes Programmkonstrukt (Verzweigung, Zusammenführung, Zuweisung, . . .) muß sich in eine abstrakte Operation / Gleichung überführen lassen. Insbesondere die im Programm auftretenden Operationen müssen eine abstrakte Entsprechung haben.
Terminierung:
Wir suchen ein Verfahren zur Berechnung der abstrakten Mengen, von dem wir garantieren können, daß es immer terminiert.
Aussagekraft:
Die abstrakten Mengen sollen genügend präzise sein, um die (benutzergegebenen) Eigenschaften an den Programmpunkten entscheiden zu können.

Anforderungen: Korrektheit

Die für einen Programmpunkt berechnete abstrakte Wertemenge soll die tatsächlich auftretende konkrete Wertemenge nach oben abschätzen.

Anforderungen: Korrektheit

Die für einen Programmpunkt berechnete abstrakte Wertemenge soll die tatsächlich auftretende konkrete Wertemenge nach oben abschätzen.

Satz (Cousot,Cousot 1976):
Sei M mit $(\sqsubseteq)$ und M' mit $(\sqsubseteq')$ vollständiger Verband,
$M \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} M'$ eine Galois-Verbindung,
$\Phi : M \longrightarrow M$ monoton und stetig,
X der kleinste Fixpunkt von Φ und
$X' = \bigsqcup' \{\bot',\ \Phi'(\bot'),\ \Phi'(\Phi'(\bot')),\ \Phi'(\Phi'(\bot')),\ \ldots\}$.
Dann ist $X \sqsubseteq \gamma(X')$.

Anforderungen: Korrektheit

Die für einen Programmpunkt berechnete abstrakte Wertemenge soll die tatsächlich auftretende konkrete Wertemenge nach oben abschätzen.

Satz (Cousot,Cousot 1976):
Sei M mit $(\sqsubseteq)$ und M' mit $(\sqsubseteq')$ vollständiger Verband,
$M \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} M'$ eine Galois-Verbindung,
$\Phi : M \longrightarrow M$ monoton und stetig,
X der kleinste Fixpunkt von Φ und
$X' = \bigsqcup' \{\bot', \ \Phi'(\bot'), \ \Phi'(\Phi'(\bot')), \ \Phi'(\Phi'(\bot')), \ \ldots\}$.
Dann ist $X \sqsubseteq \gamma(X')$.

Wir benötigen noch eine weitere formale Definition.

Anforderungen: Korrektheit

Die für einen Programmpunkt berechnete abstrakte Wertemenge soll die tatsächlich auftretende konkrete Wertemenge nach oben abschätzen.

Satz (Cousot,Cousot 1976):
Sei M mit $(\sqsubseteq)$ und M' mit $(\sqsubseteq')$ vollständiger Verband,
$M \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} M'$ eine Galois-Verbindung,
$\Phi : M \longrightarrow M$ monoton und stetig,
X der kleinste Fixpunkt von Φ und
$X' = \bigsqcup' \{\perp', \ \Phi'(\perp'), \ \Phi'(\Phi'(\perp')), \ \Phi'(\Phi'(\perp')), \ \ldots\}$.
Dann ist $X \sqsubseteq \gamma(X')$.

Anforderungen: Korrektheit

Die für einen Programmpunkt berechnete abstrakte Wertemenge soll die tatsächlich auftretende konkrete Wertemenge nach oben abschätzen.

Satz (Cousot,Cousot 1976):
Sei M mit $(\sqsubseteq)$ und M' mit $(\sqsubseteq')$ vollständiger Verband,
$M \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} M'$ eine Galois-Verbindung,
$\Phi : M \longrightarrow M$ monoton und stetig,
X der kleinste Fixpunkt von Φ und
$X' = \bigsqcup{}' \{\bot',\ \Phi'(\bot'),\ \Phi'(\Phi'(\bot')),\ \Phi'(\Phi'(\bot')),\ \ldots\}$.
Dann ist $X \sqsubseteq \gamma(X')$.

Wir benötigen noch eine weitere formale Definition.

Galois-Verbindung

Seien M mit $(\sqsubseteq)$ und M' mit $(\sqsubseteq')$ vollständige Verbände.

Sei $\alpha : M \longrightarrow M'$ und $\gamma : M' \longrightarrow M$ monotone Abbildungen,
so daß $x \sqsubseteq \gamma(\alpha(x))$ für alle $x \in M$ und $\alpha(\gamma(x')) \sqsubseteq' x'$ für alle $x' \in M'$.

Wir nennen das Paar α, γ eine Galois-Verbindung zwischen M und M'
und schreiben $M \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} M'$.

$\alpha(x)$ ist die Abstraktion von x,
d.h. die präzisest-mögliche Darstellung von x in M'.

$\gamma(x')$ ist die Konkretisierung von x',
d.h. das unpräziseste Element in M, das noch durch x' dargestellt werden kann.

Beispiel Vorzeichen

$M = \wp(\boldsymbol{Z})$ mit $(\subseteq)$, $\quad M' = \wp(\{-, 0, +\})$ mit $(\subseteq)$.

Wir definieren die Abstraktion α zunächst auf einelementigen Mengen:

$$\alpha(\{n\}) = \begin{cases} \{-\} & \text{falls} \quad n < 0 \\ \{0\} & \text{falls} \quad n = 0 \\ \{+\} & \text{falls} \quad n > 0 \end{cases}$$

Für beliebige Mengen $S \subseteq \boldsymbol{Z}$ definieren wir:

$$\alpha(S) = \bigcup_{n \in S} \alpha(\{n\}).$$

Beispiel Vorzeichen

$M = \wp(\boldsymbol{Z})$ mit $(\subseteq)$, $\quad M' = \wp(\{-, 0, +\})$ mit $(\subseteq)$.

Wir definieren die Abstraktion α zunächst auf einelementigen Mengen:

$$\alpha(\{n\}) = \begin{cases} \{-\} & \text{falls} \quad n < 0 \\ \{0\} & \text{falls} \quad n = 0 \\ \{+\} & \text{falls} \quad n > 0 \end{cases}$$

Für beliebige Mengen $S \subseteq \boldsymbol{Z}$ definieren wir:

$$\alpha(S) = \bigcup_{n \in S} \alpha(\{n\}).$$

Z.B.

$\alpha(\{\text{-}2, \text{-}1\}) = \alpha(\{\text{-}2\}) \cup \alpha(\{\text{-}1\}) = \{-\} \cup \{-\} = \{-\}$,

$\alpha(\{0, 2, 4, 6, \ldots\}) = \alpha(\{0\}) \cup \alpha(\{2\}) \cup \alpha(\{4\}) \cup \alpha(\{6\}) \cup \ldots = \{0, +\}$.

Beispiel Vorzeichen

$M = \wp(\boldsymbol{Z})$ mit $(\subseteq)$, $\quad M' = \wp(\{-, 0, +\})$ mit $(\subseteq)$.

Wir definieren die Abstraktion α zunächst auf einelementigen Mengen:

$$\alpha(\{n\}) = \begin{cases} \{-\} & \text{falls} \quad n < 0 \\ \{0\} & \text{falls} \quad n = 0 \\ \{+\} & \text{falls} \quad n > 0 \end{cases}$$

Für beliebige Mengen $S \subseteq \boldsymbol{Z}$ definieren wir:

$$\alpha(S) = \bigcup_{n \in S} \alpha(\{n\}).$$

Entsprechend definieren wir die Konkretisierung γ durch

$$\begin{array}{lcl} \gamma(\{-\}) & = & \{\ldots, \text{-}3, \text{-}2, \text{-}1\} \\ \gamma(\{0\}) & = & \{0\} \\ \gamma(\{+\}) & = & \{1, 2, 3, \ldots\} \\ \gamma(S') & = & \bigcup_{s \in S'} \gamma(\{s\}). \end{array}$$

Beispiel Vorzeichen

$M = \wp(\boldsymbol{Z})$ mit $(\subseteq)$, $M' = \wp(\{-, 0, +\})$ mit $(\subseteq)$.

Wir definieren die Abstraktion α zunächst auf einelementigen Mengen:

$$\alpha(\{n\}) = \begin{cases} \{-\} & \text{falls} \quad n < 0 \\ \{0\} & \text{falls} \quad n = 0 \\ \{+\} & \text{falls} \quad n > 0 \end{cases}$$

Für beliebige Mengen $S \subseteq \boldsymbol{Z}$ definieren wir:

$$\alpha(S) = \bigcup_{n \in S} \alpha(\{n\}).$$

Entsprechend definieren wir die Konkretisierung γ durch

$$\begin{array}{lcl} \gamma(\{-\}) & = & \{\ldots, \text{-}3, \text{-}2, \text{-}1\} \\ \gamma(\{0\}) & = & \{0\} \\ \gamma(\{+\}) & = & \{1, 2, 3, \ldots\} \\ \gamma(S') & = & \bigcup_{s \in S'} \gamma(\{s\}). \end{array}$$

Z.B.

$$\gamma(\{-, 0, +\}) = \gamma(\{-\}) \cup \gamma(\{0\}) \cup \gamma(\{+\})$$
$$= \{\ldots, \text{-}3, \text{-}2, \text{-}1\} \cup \{0\} \cup \{1, 2, 3, \ldots\} = \boldsymbol{Z}.$$

Beispiel Vorzeichen

$M = \wp(\boldsymbol{Z})$ mit $(\subseteq)$, $\quad M' = \wp(\{-, 0, +\})$ mit $(\subseteq)$.

Wir definieren die Abstraktion α zunächst auf einelementigen Mengen:

$$\alpha(\{n\}) = \begin{cases} \{-\} & \text{falls} \quad n < 0 \\ \{0\} & \text{falls} \quad n = 0 \\ \{+\} & \text{falls} \quad n > 0 \end{cases}$$

Für beliebige Mengen $S \subseteq \boldsymbol{Z}$ definieren wir:

$$\alpha(S) = \bigcup_{n \in S} \alpha(\{n\}).$$

Entsprechend definieren wir die Konkretisierung γ durch

$$\begin{aligned} \gamma(\{-\}) &= \{\ldots, \text{-}3, \text{-}2, \text{-}1\} \\ \gamma(\{0\}) &= \{0\} \\ \gamma(\{+\}) &= \{1, 2, 3, \ldots\} \\ \gamma(S') &= \bigcup_{s \in S'} \gamma(\{s\}). \end{aligned}$$

Beispiel Vorzeichen

$M = \wp(\boldsymbol{Z})$ mit $(\subseteq)$, $\quad M' = \wp(\{-, 0, +\})$ mit $(\subseteq)$.

Wir definieren die Abstraktion α zunächst auf einelementigen Mengen:

$$\alpha(\{n\}) = \begin{cases} \{-\} & \text{falls} \quad n < 0 \\ \{0\} & \text{falls} \quad n = 0 \\ \{+\} & \text{falls} \quad n > 0 \end{cases}$$

Für beliebige Mengen $S \subseteq \boldsymbol{Z}$ definieren wir:

$$\alpha(S) = \bigcup_{n \in S} \alpha(\{n\}).$$

Entsprechend definieren wir die Konkretisierung γ durch

$$\begin{aligned} \gamma(\{-\}) &= \{\ldots, \text{-}3, \text{-}2, \text{-}1\} \\ \gamma(\{0\}) &= \{0\} \\ \gamma(\{+\}) &= \{1, 2, 3, \ldots\} \\ \gamma(S') &= \bigcup_{s \in S'} \gamma(\{s\}). \end{aligned}$$

Z.B.

$\alpha(\{\text{-}2, \text{-}1\}) = \alpha(\{\text{-}2\}) \cup \alpha(\{\text{-}1\}) = \{-\} \cup \{-\} = \{-\}$,

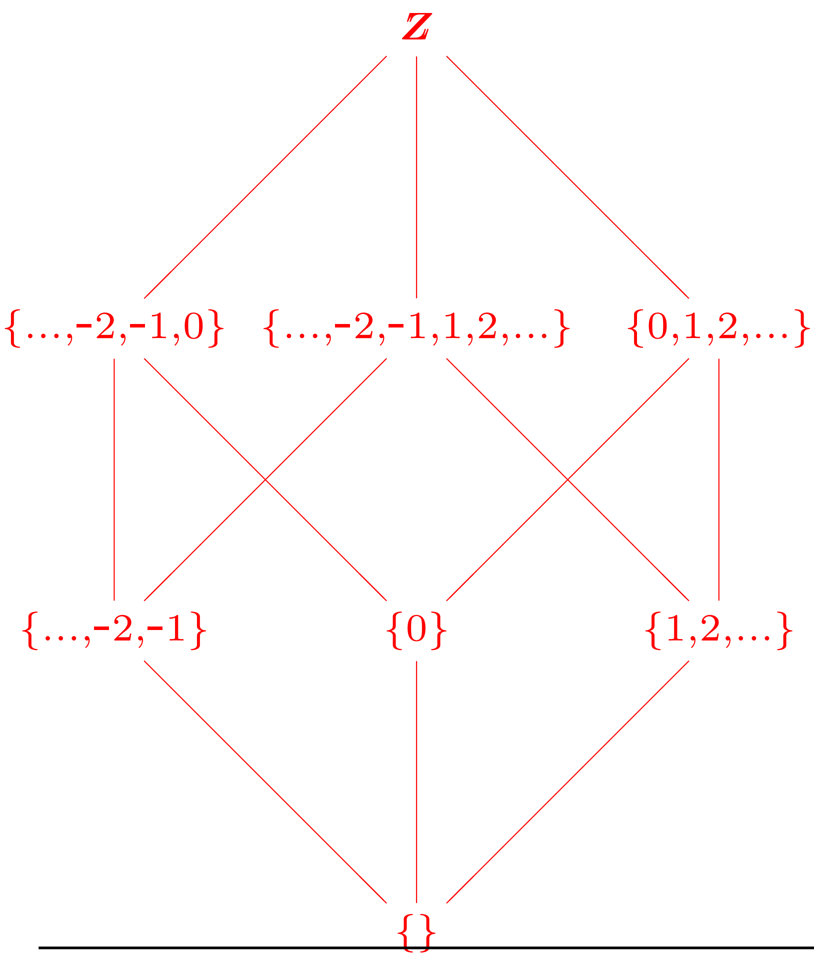
$\alpha(\{0, 2, 4, 6, \ldots\}) = \alpha(\{0\}) \cup \alpha(\{2\}) \cup \alpha(\{4\}) \cup \alpha(\{6\}) \cup \ldots = \{0, +\}$.

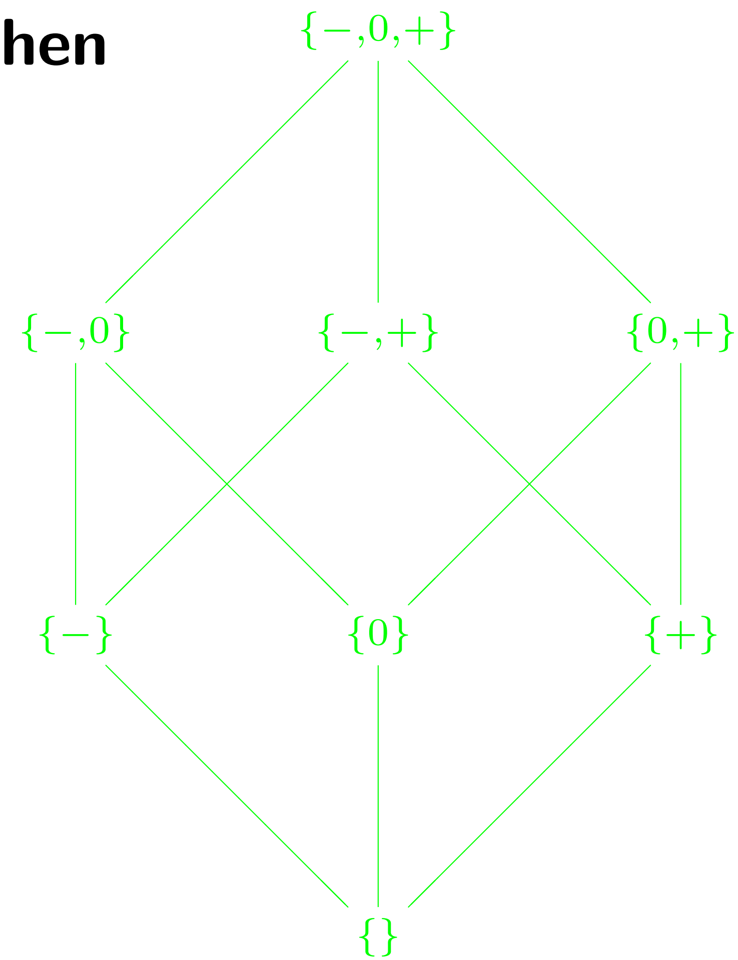
Z.B.

$\gamma(\{-, 0, +\}) = \gamma(\{-\}) \cup \gamma(\{0\}) \cup \gamma(\{+\})$

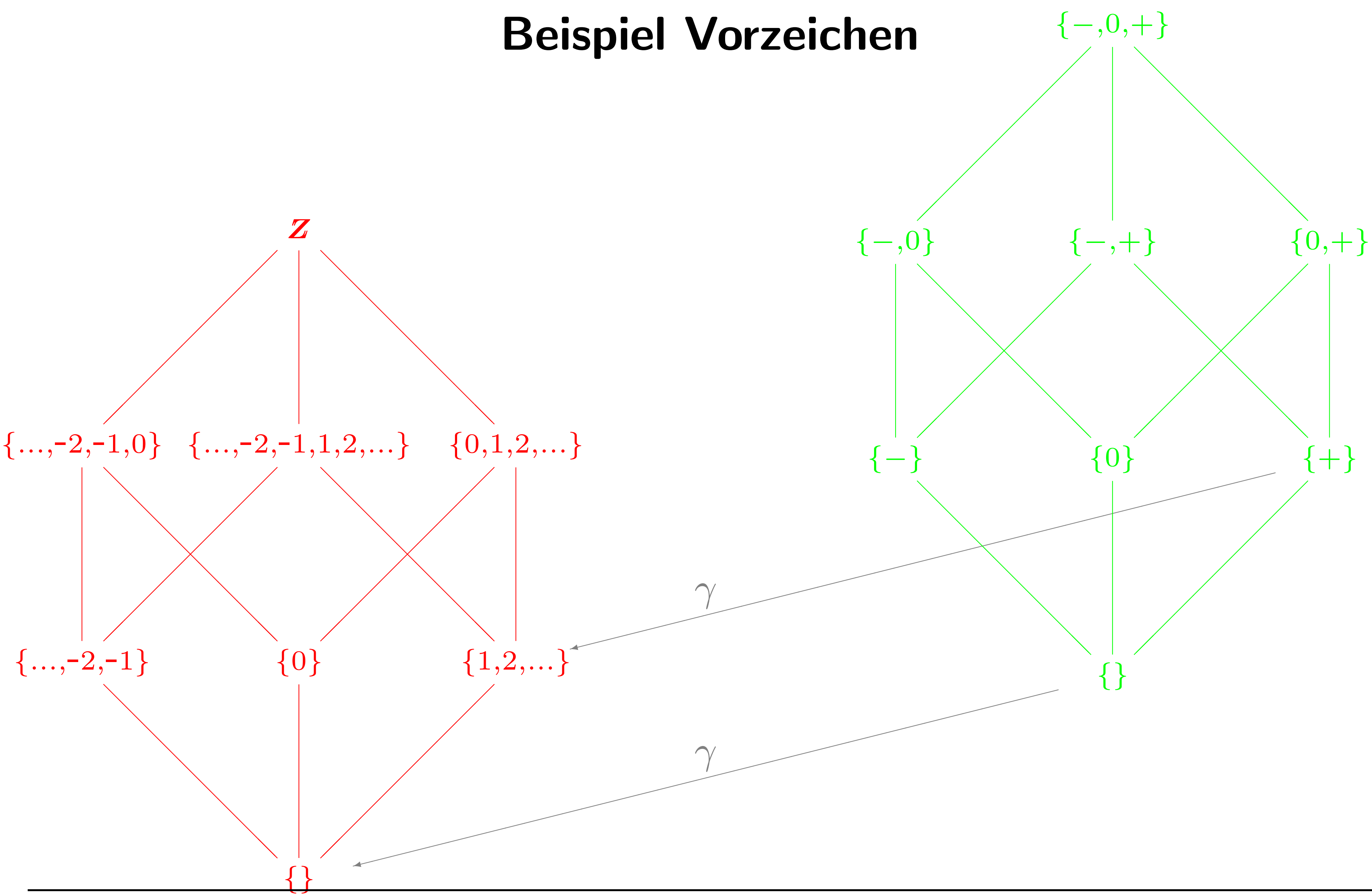
$= \{\ldots, \text{-}3, \text{-}2, \text{-}1\} \cup \{0\} \cup \{1, 2, 3, \ldots\} = \boldsymbol{Z}$.

Beispiel Vorzeichen

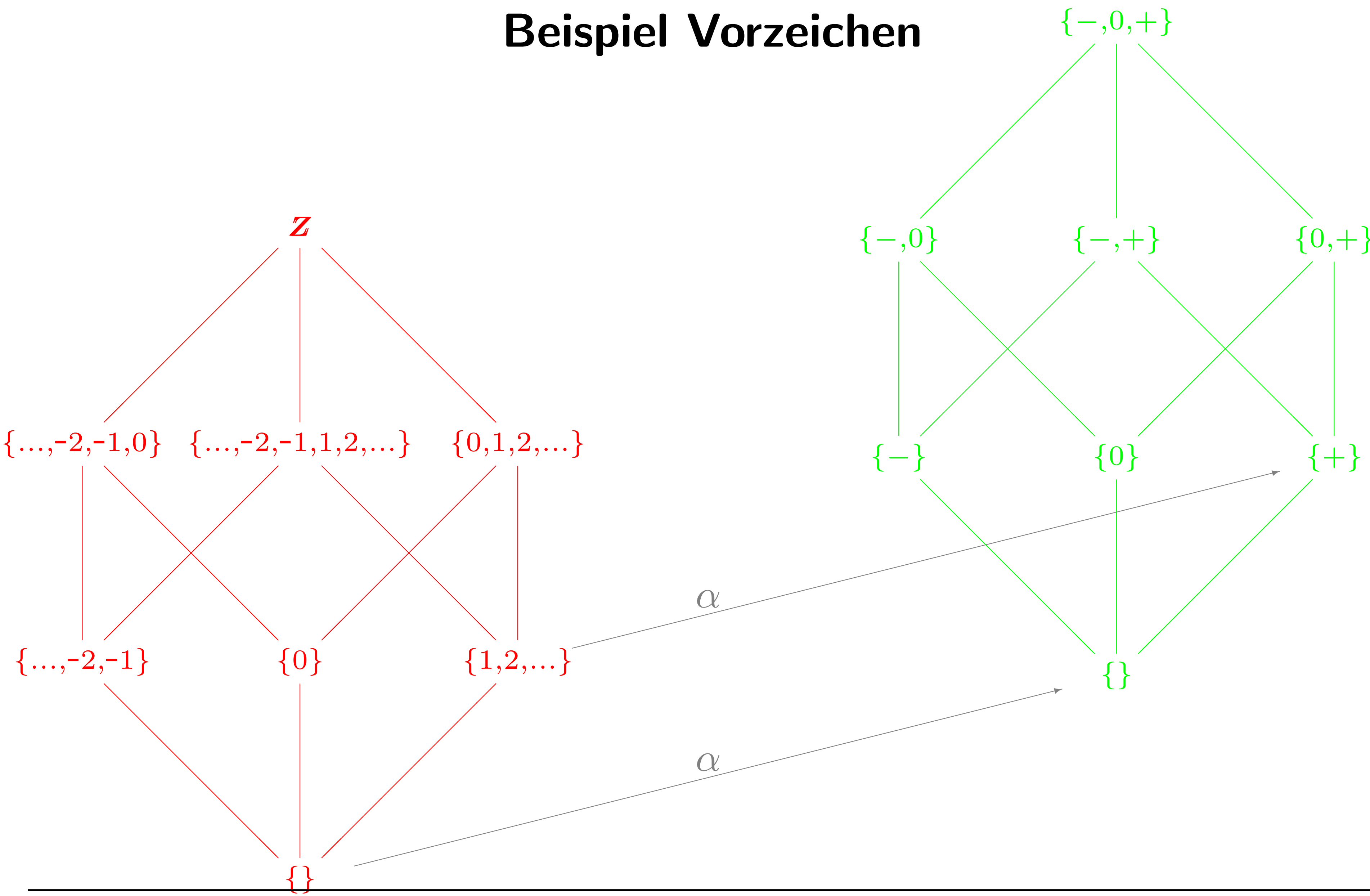




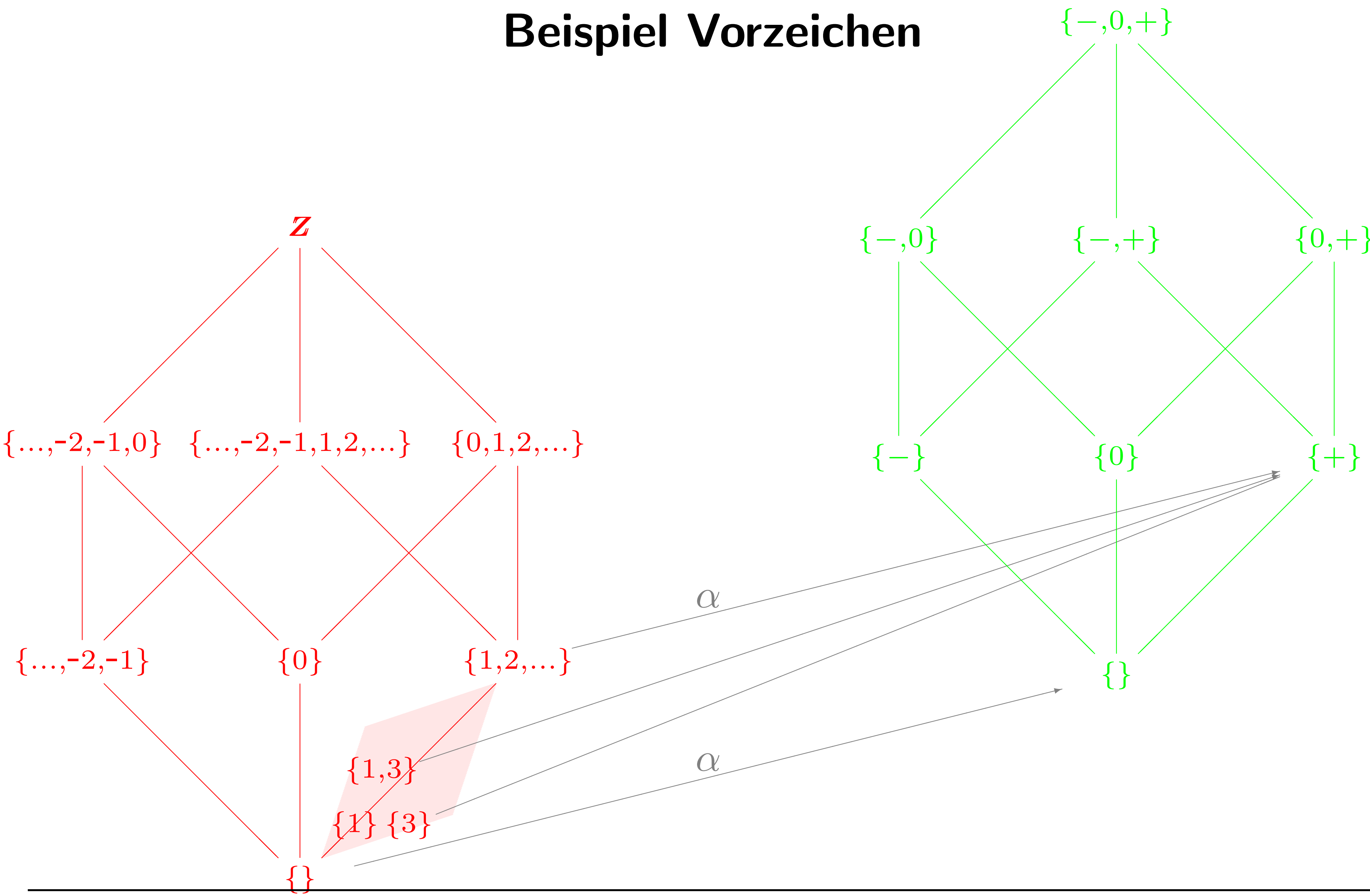
Beispiel Vorzeichen



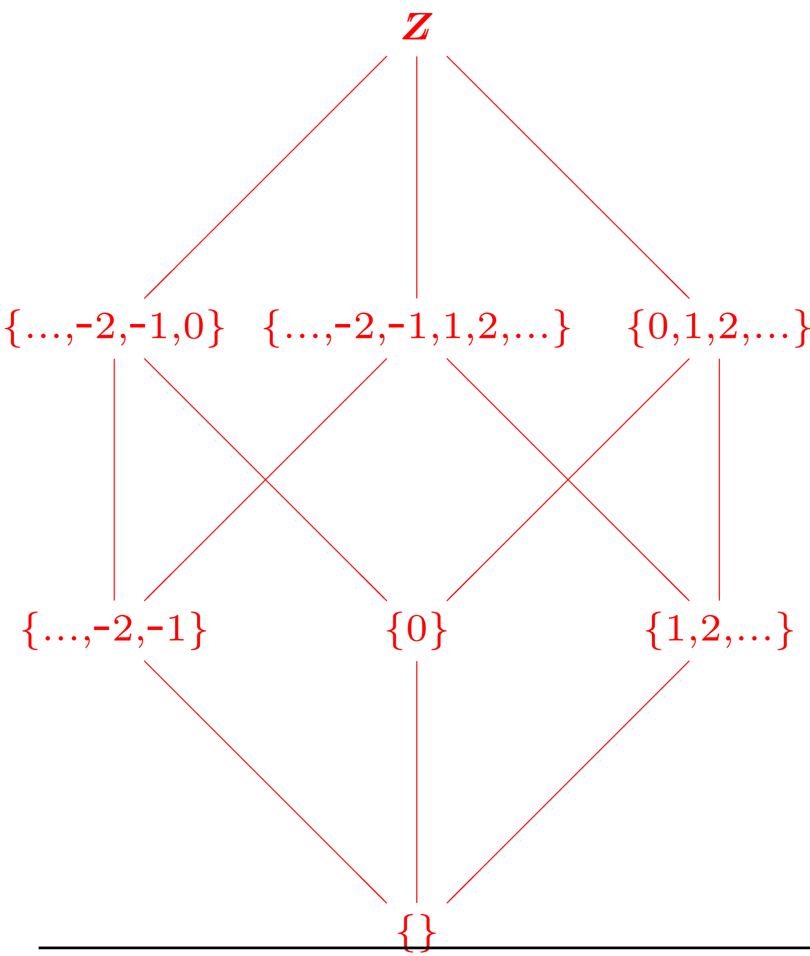
Beispiel Vorzeichen

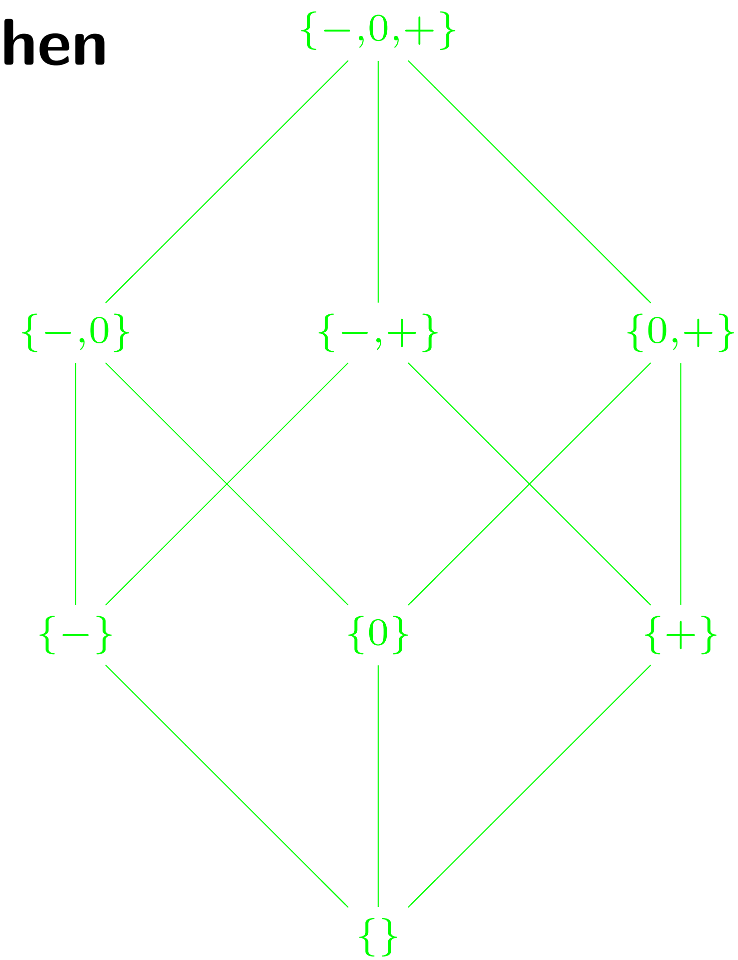


Beispiel Vorzeichen

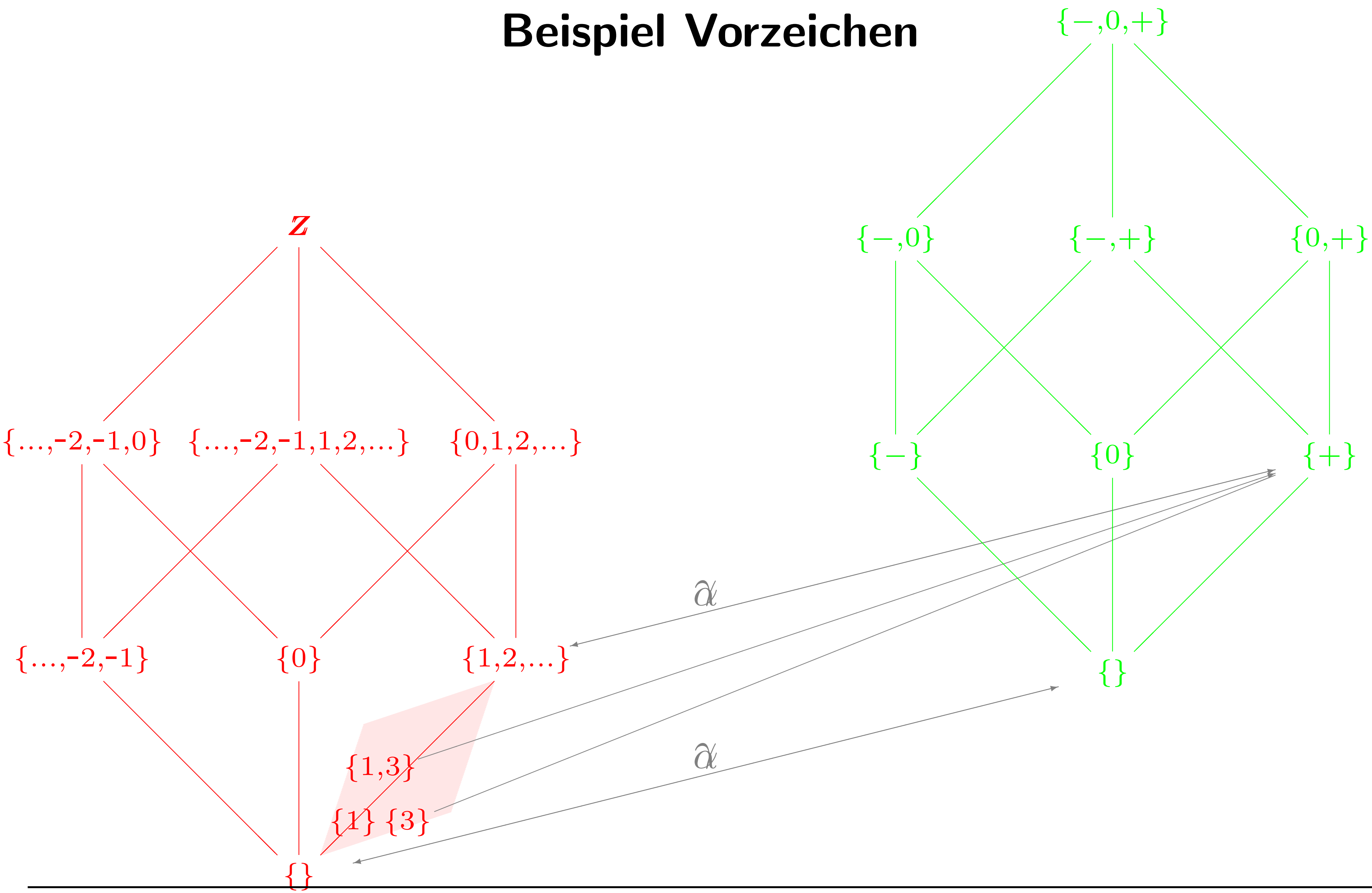


Beispiel Vorzeichen





Beispiel Vorzeichen



Beispiel Restklassen

$M = \wp(\mathbb{Z})$ mit $(\subseteq)$, $\quad M' = \wp(\{0, \ldots, m-1\})$ mit $(\subseteq)$ für ein festes $m \geq 2$.
Wir definieren $\alpha(\{n\}) = \{n\%m\}$ für einelementige,
$\alpha(S) = \bigcup_{n \in S} \alpha(\{n\})$ für beliebige Mengen;
sowie $\gamma(\{n'\}) = \{n \in \mathbb{N} \mid n\%m = n'\}$ und $\gamma(S') = \bigcup_{s \in S'} \gamma(\{s\})$.

Wir bilden also alle (konkreten) Zahlen, die denselben Rest mod. m haben, auf dieselbe (abstrakte) Zahl ab.

Für $m = 2$ ist $0 \in M'$ bzw. $1 \in M'$ die Abstraktion der geraden bzw. der ungeraden Zahlen.
Für $m = 256$ ist $0, \ldots, 255 \in M'$ jeweils die Abstraktion der Zahlen mit dem entsprechenden Wert des niederwertigsten Byte, z.B.
$\alpha(\{\texttt{0x2900}, \texttt{0x0a00}, \texttt{0x00fe}, \texttt{0x12fe}, \texttt{0x85fe}\}) = \{0, 254\}$.

Beipiel Restklassen: Eigenschaften

Name	Eigenschaft	
$\gamma\ \neq$	$\gamma(\{a'\}) \cap \gamma(\{b'\}) = \{\}$	für $a' \neq b'$
$\gamma\ \cap$	$\gamma(x' \cap y') = \gamma(x') \cap \gamma(y')$	
$\gamma\ \cup$	$\gamma(x' \cup y') = \gamma(x') \cup \gamma(y')$	
$\alpha\ \cup$	$\alpha(x \cup y) = \alpha(x) \cup \alpha(y)$	
$\alpha\ \gamma$	$\alpha(\gamma(x')) = x'$	

Nochmal: Korrektheit der abstrakten Interpretation

Satz (Cousot,Cousot 1976):

Nochmal: Korrektheit der abstrakten Interpretation

Satz (Cousot,Cousot 1976):
Seien M mit $(\sqsubseteq)$,$\perp$ und M' mit $(\sqsubseteq')$,$\perp'$ vollständige Verbände.
Sei $M \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} M'$ eine Galois-Verbindung.
Sei $\Phi : M \longrightarrow M$ monoton und stetig.
Sei $\Phi' : M' \longrightarrow M'$ monoton, so daß $\alpha(\Phi(\gamma(x'))) \sqsubseteq' \Phi'(x')$.
Nach dem Fixpunktsatz ist dann
$X = \bigsqcup \{\perp, \quad \Phi(\perp), \quad \Phi(\Phi(\perp)), \quad \ldots\}$ der kleinste Fixpunkt von Φ.
$X' = \bigsqcup' \{\perp', \ \Phi'(\perp'), \ \Phi'(\Phi'(\perp')), \ \ldots\}$ ist nur dann der kleinste Fixpunkt von Φ', wenn Φ' zusätzlich stetig ist.

Nochmal: Korrektheit der abstrakten Interpretation

Satz (Cousot,Cousot 1976):
Seien M mit $(\sqsubseteq)$,$\perp$ und M' mit $(\sqsubseteq')$,$\perp'$ vollständige Verbände.
Sei $M \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} M'$ eine Galois-Verbindung.
Sei $\Phi : M \longrightarrow M$ monoton und stetig.
Sei $\Phi' : M' \longrightarrow M'$ monoton, so daß $\alpha(\Phi(\gamma(x'))) \sqsubseteq' \Phi'(x')$.
Nach dem Fixpunktsatz ist dann
$X = \bigsqcup \{\perp, \quad \Phi(\perp), \quad \Phi(\Phi(\perp)), \quad \ldots\}$ der kleinste Fixpunkt von Φ.
$X' = \bigsqcup' \{\perp', \ \Phi'(\perp'), \ \Phi'(\Phi'(\perp')), \ \ldots\}$ ist nur dann der kleinste Fixpunkt von Φ',
wenn Φ' zusätzlich stetig ist. *In jedem Fall gilt aber $X \sqsubseteq \gamma(X')$.*

Nochmal: Korrektheit der abstrakten Interpretation

Satz (Cousot,Cousot 1976):
Seien M mit $(\sqsubseteq)$,$\bot$ und M' mit $(\sqsubseteq')$,$\bot'$ vollständige Verbände.
Sei $M \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} M'$ eine Galois-Verbindung.
Sei $\Phi : M \longrightarrow M$ monoton und stetig.
Sei $\Phi' : M' \longrightarrow M'$ monoton, so daß $\alpha(\Phi(\gamma(x'))) \sqsubseteq' \Phi'(x')$.
Nach dem Fixpunktsatz ist dann
$X = \bigsqcup \{\bot, \ \ \Phi(\bot), \ \ \ \Phi(\Phi(\bot)), \ \ \ \ldots\}$ der kleinste Fixpunkt von Φ.
$X' = \bigsqcup'\{\bot', \ \Phi'(\bot'), \ \Phi'(\Phi'(\bot')), \ \ldots\}$ ist nur dann der kleinste Fixpunkt von Φ',
wenn Φ' zusätzlich stetig ist. *In jedem Fall gilt aber* $X \sqsubseteq \gamma(X')$ *.*

D.h. wir können im abstrakten Verband (mit Φ') genauso rechnen
wie vorher im konkreten (mit Φ, "collecting semantics").

Nochmal: Korrektheit der abstrakten Interpretation

Satz (Cousot,Cousot 1976):
Seien M mit $(\sqsubseteq)$,$\bot$ und M' mit $(\sqsubseteq')$,$\bot'$ vollständige Verbände.
Sei $M \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} M'$ eine Galois-Verbindung.
Sei $\Phi : M \longrightarrow M$ monoton und stetig.
Sei $\Phi' : M' \longrightarrow M'$ monoton, so daß $\alpha(\Phi(\gamma(x'))) \sqsubseteq' \Phi'(x')$.
Nach dem Fixpunktsatz ist dann
$X = \bigsqcup \{\bot, \quad \Phi(\bot), \quad \Phi(\Phi(\bot)), \quad \ldots\}$ der kleinste Fixpunkt von Φ.
$X' = \bigsqcup'\{\bot', \; \Phi'(\bot'), \; \Phi'(\Phi'(\bot')), \; \ldots\}$ ist nur dann der kleinste Fixpunkt von Φ',
wenn Φ' zusätzlich stetig ist. *In jedem Fall gilt aber* $X \sqsubseteq \gamma(X')$ *.*

D.h. wir können im abstrakten Verband (mit Φ') genauso rechnen
wie vorher im konkreten (mit Φ, “collecting semantics”).
Der abstrakte Punkt X' ist eine obere Approximation des konkreten Fixpunkts X.

Nochmal: Korrektheit der abstrakten Interpretation

Satz (Cousot,Cousot 1976):
Seien M mit $(\sqsubseteq)$,$\bot$ und M' mit $(\sqsubseteq')$,$\bot'$ vollständige Verbände.
Sei $M \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} M'$ eine Galois-Verbindung.
Sei $\Phi : M \longrightarrow M$ monoton und stetig.
Sei $\Phi' : M' \longrightarrow M'$ monoton, so daß $\alpha(\Phi(\gamma(x'))) \sqsubseteq' \Phi'(x')$.
Nach dem Fixpunktsatz ist dann
$X = \bigsqcup \{\bot, \quad \Phi(\bot), \quad \Phi(\Phi(\bot)), \quad \ldots\}$ der kleinste Fixpunkt von Φ.
$X' = \bigsqcup' \{\bot', \ \Phi'(\bot'), \ \Phi'(\Phi'(\bot')), \ \ldots\}$ ist nur dann der kleinste Fixpunkt von Φ',
wenn Φ' zusätzlich stetig ist. *In jedem Fall gilt aber* $X \sqsubseteq \gamma(X')$ *.*

D.h. wir können im abstrakten Verband (mit Φ') genauso rechnen
wie vorher im konkreten (mit Φ, "collecting semantics").
Der abstrakte Punkt X' ist eine obere Approximation des konkreten Fixpunkts X.
Wir haben ein Rezept bekommen für die Überführung der Programmkonstrukte.

Nochmal: Korrektheit der abstrakten Interpretation

Satz (Cousot,Cousot 1976):
Seien M mit $(\sqsubseteq)$,$\bot$ und M' mit $(\sqsubseteq')$,$\bot'$ vollständige Verbände.
Sei $M \overset{\gamma}{\underset{\alpha}{\leftrightarrows}} M'$ eine Galois-Verbindung.
Sei $\Phi : M \longrightarrow M$ monoton und stetig.
Sei $\Phi' : M' \longrightarrow M'$ monoton, so daß $\alpha(\Phi(\gamma(x'))) \sqsubseteq' \Phi'(x')$.
Nach dem Fixpunktsatz ist dann
$X = \bigsqcup \{\bot, \quad \Phi(\bot), \quad \Phi(\Phi(\bot)), \quad \ldots\}$ der kleinste Fixpunkt von Φ.
$X' = \bigsqcup' \{\bot', \ \Phi'(\bot'), \ \Phi'(\Phi'(\bot')), \ \ldots\}$ ist nur dann der kleinste Fixpunkt von Φ',
wenn Φ' zusätzlich stetig ist. *In jedem Fall gilt aber $X \sqsubseteq \gamma(X')$.*

D.h. wir können im abstrakten Verband (mit Φ') genauso rechnen
wie vorher im konkreten (mit Φ, “collecting semantics”).
Der abstrakte Punkt X' ist eine obere Approximation des konkreten Fixpunkts X.
Wir haben ein Rezept bekommen für die Überführung der Programmkonstrukte.

Anforderungen: Überführbarkeit

Jedes Programmkonstrukt (Verzweigung, Zusammenführung, Zuweisung, . . .) muß sich in eine abstrakte Operation / Gleichung überführen lassen. Insbesondere die im Programm auftretenden Operationen müssen eine abstrakte Entsprechung haben.

Überführung von Programmkonstrukten am Beispiel

Bei der Berechnung der collecting semantics in unserem Beispiel hatten wir als (konkreten) Verband $M = \wp(\boldsymbol{Z})^8$ gewählt, entsprechend den 8 Programmpunkten $A, \ldots, H$, an denen wir die Wertemengen der `int`-Variablen x bestimmen wollten.

Jetzt wollen wir z.B. nur wissen, welche Restklassen mod. 6 an einem Programmpunkt auftreten können
(daraus können wir die Reste mod. 2 und mod. 3 ablesen; 2 und 3 treten als einzige Konstanten im Programmtext auf).
Wir wählen daher als abstrakten Verband $M' = \wp(\{0, \ldots, 5\})^8$, dazu α und γ komponentenweise wie auf der obigen Folie.

Überführung von Programmkonstrukten am Beispiel

Damit können den Mindestwert von Φ' einfach ausrechnen:

$$
\begin{array}{lll}
 & \alpha(\Phi(\gamma(\langle A', \ldots, H' \rangle))) & \\
= & \alpha(\Phi(\langle \gamma(A'), \ldots, \gamma(H') \rangle)) & \gamma \text{ komponentenweise} \\
= & \alpha(\langle \{1, ..., 5\}, \ldots, \{3n{+}1 \mid n \in \gamma(F')\} \rangle) & \text{Def. } \Phi \\
= & \langle \alpha(\{1, ..., 5\}), & \\
 & \ \alpha(\gamma(A') \cup \gamma(G') \cup \gamma(H')), & \\
 & \ \alpha(\gamma(B') \cap \{2, 3, 4, ...\}), & \\
 & \ \alpha(\gamma(B') \cap \{..., \text{-}2, \text{-}1, 0, 1\}), & \\
 & \ \alpha(\gamma(C') \cap \{..., \text{-}4, \text{-}2, 0, 2, 4, ...\}), & \\
 & \ \alpha(\gamma(C') \cap \{..., \text{-}3, \text{-}1, 1, 3, ...\}), & \\
 & \ \alpha(\{n/2 \mid n \in \gamma(E')\}), & \\
 & \ \alpha(\{3n{+}1 \mid n \in \gamma(F')\}) \rangle & \alpha \text{ komponentenweise}
\end{array}
$$

Überführung von Programmkonstrukten am Beispiel

Jetzt schätzen wir die einzelnen Komponenten möglichst knapp nach oben ab:

$$
\begin{array}{lcll}
\alpha(\{1,...,5\}) & = & \{1,...,5\} & \text{Def. } \alpha \\
\alpha(\gamma(A') \cup \gamma(G') \cup \gamma(H')) & = & \alpha(\gamma(A' \cup G' \cup H')) & \gamma\ \cup \\
 & = & A' \cup G' \cup H' & \alpha\ \gamma \\
\alpha(\gamma(B') \cap \{2,3,4,...\}) & \sqsubseteq' & \alpha(\gamma(B')) & \\
 & = & B' & \alpha\ \gamma \\
\alpha(\gamma(B') \cap \{...,\text{-}2,\text{-}1,0,1\}) & \sqsubseteq' & \alpha(\gamma(B')) & \\
 & = & B' & \alpha\ \gamma \\
\alpha(\gamma(C') \cap \{...,\text{-}4,\text{-}2,0,2,4,...\}) & = & \alpha(\gamma(C' \cap \{0,2,4\})) & \gamma\ \cap \\
 & = & C' \cap \{0,2,4\} & \alpha\ \gamma \\
\alpha(\gamma(C') \cap \{...,\text{-}3,\text{-}1,1,3,...\}) & = & \alpha(\gamma(C' \cap \{1,3,5\})) & \gamma\ \cap \\
 & = & C' \cap \{1,3,5\} & \alpha\ \gamma
\end{array}
$$

Überführung von Programmkonstrukten am Beispiel

$$
\begin{array}{lcll}
\alpha(\{n/2 \mid n \in \gamma(E')\}) & \sqsubseteq' & \alpha(\boldsymbol{Z}) & \\
 & = & \{0, ..., 5\} & \\
\alpha(\{3n{+}1 \mid n \in \gamma(F')\}) & = & \alpha(\{3n{+}1 \mid n' \in F' \wedge n \in \gamma(\{n'\})\}) & \gamma \cup \\
 & = & \bigcup_{n' \in F'} \bigcup_{n \in \gamma(\{n'\})} \alpha(\{3n{+}1\}) & \alpha \cup \\
 & = & \bigcup_{n' \in F'} \bigcup_{n \in \gamma(\{n'\})} \{(3n{+}1)\%6\} & \alpha\ \{\cdot\} \\
 & = & \bigcup_{n' \in F'} \bigcup_{n \in \gamma(\{n'\})} \{(3(n\%6){+}1)\%6\} & \text{Arithmetik} \\
 & = & \bigcup_{n' \in F'} \bigcup_{n \in \gamma(\{n'\})} \{(3n'{+}1)\%6\} & \gamma\ \{\cdot\} \\
 & = & \bigcup_{n' \in F'} \{(3n'{+}1)\%6\} & \text{alle gleich} \\
 & = & \{(3n'{+}1)\%6 \mid n' \in F'\} &
\end{array}
$$

Überführung von Programmkonstrukten am Beispiel

Wir können also definieren:

$$\begin{aligned}\Phi'(A',\ldots,H') = \langle\ & \{1,...,5\},\\ & A' \cup G' \cup H',\\ & B',\\ & B',\\ & C' \cap \{0,2,4\},\\ & C' \cap \{1,3,5\},\\ & \{0,...,5\},\\ & \{(3n'+1)\%6 \mid n' \in F'\}\ \rangle\end{aligned}$$

Dabei müssen wir darauf achten, daß Φ' monoton wird (das ist hier der Fall).

Diese Definition von Φ' enthält nur noch abstrakte Konstrukte.

Anforderungen: Terminierung

nochmal Satz (Cousot,Cousot 1976):
Der kleinste Fixpunkt X der collecting semantics kann abgeschätzt werden durch
$X \sqsubseteq \gamma(X')$, wobei $X' = \bigsqcup'\{\perp', \; \Phi'(\perp'), \; \Phi'(\Phi'(\perp')), \; \ldots\}$.

Wir wollen also sicherstellen, daß die Berechnung von X' immer terminiert.
Dazu gibt es verschiedene Möglichkeiten:

1. Der abstrakte Verband M' hat nur endlich viele Elemente.
2. Jede unendlich lange aufsteigende Kette in M' wird irgendwann stationär („Ascending Chain Condition (ACC)", s.u.).
3. Wir können Φ' so konstruieren, daß die Terminierung gesichert ist („Widening", s.u.).

Terminierung: Ascending Chain Condition

ACC: jede unendlich lange aufsteigende Kette in M' wird irgendwann stationär.

Formal:
für jede aufsteigende Kette $x'_1 \sqsubseteq' x'_2 \sqsubseteq' \ldots \sqsubseteq' x'_i \sqsubseteq' \ldots$ existiert ein $n \in I\!N$, so daß $x'_n = x'_{n+1} = \ldots = x'_{n+j} = \ldots$.
Wir nennen die Kette in diesem Fall *stationär ab* n.
In diesem Fall ist $\bigsqcup' \{x'_1, x'_2, \ldots, x'_i, \ldots\} = x'_n$.

Da die Iterationen von Φ' eine aufsteigende Kette bilden
(wegen der Monotonie von Φ' ist $\bot' \sqsubseteq' \Phi'(\bot') \sqsubseteq' \Phi'(\Phi'(\bot')) \sqsubseteq' \ldots$),
garantiert ACC, daß sie irgendwann stationär wird und daher nach endlich vielen Iterationen der Maximalwert X' erreicht ist.

Ascending Chain Condition: Beispiele

$\{-\infty, \ldots, \text{-}4, \text{-}3, \text{-}2, \text{-}1, 0\}$ mit der üblichen Ordnung $(\leq)$.

$\{\{\}, I\!N\} \cup$
$\{\{0\}, \{1\}, \{2\}, \ldots\} \cup$
$\{\{0,1\}, \{0,2\}, \{0,3\}, \ldots, \{1,2\}, \{1,3\}, \ldots, \{2,3\}, \ldots\}$
mit $(\subseteq)$ (“ostfriesische Mengen”)

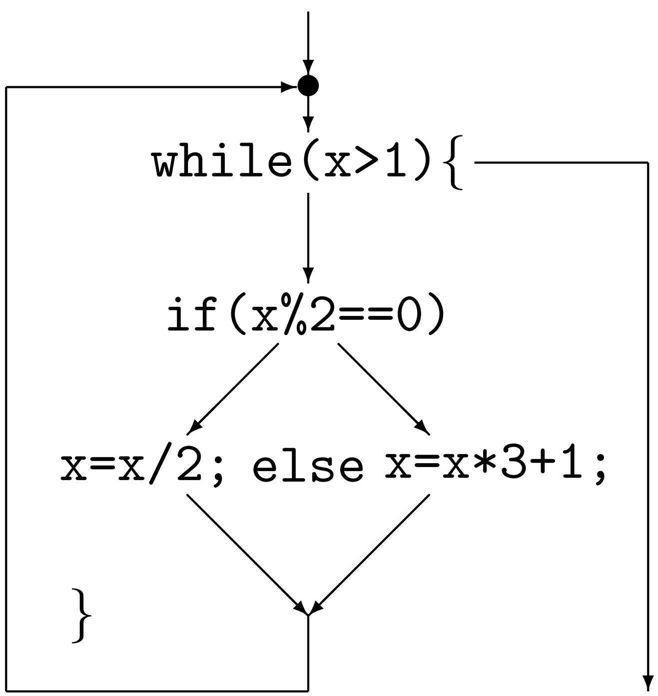
Terminierung: Widening

Der Verband der Intervalle ist aber weder endlich, noch erfüllt er ACC.

(z.B. $[1,2] \sqsubseteq' [1,3] \sqsubseteq' \ldots \sqsubseteq' [1,i] \sqsubseteq' \ldots$).

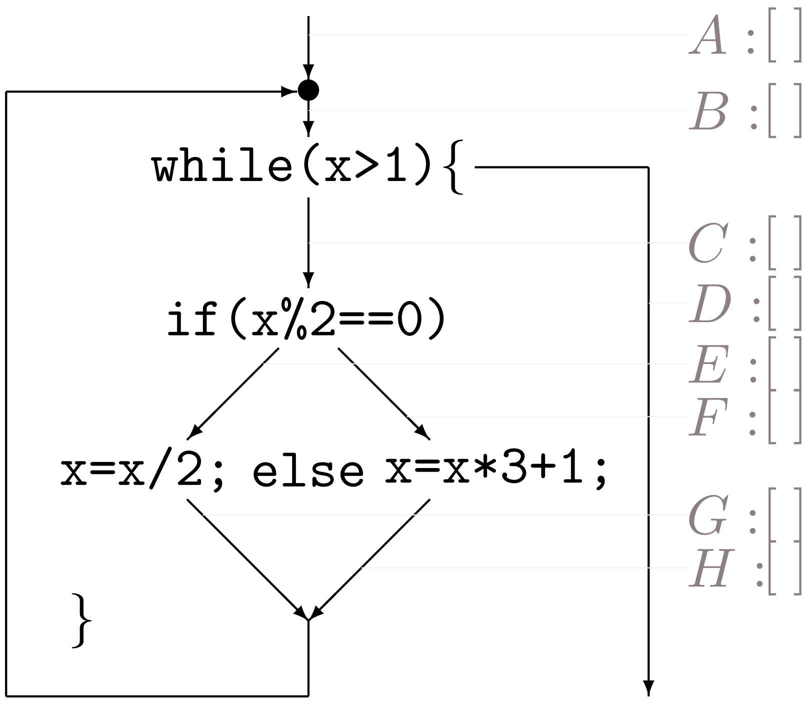
In unserem Beispiel terminiert die Berechnung der abstrakten Interpretation tatsächlich nicht (s.u.).

Beispiel

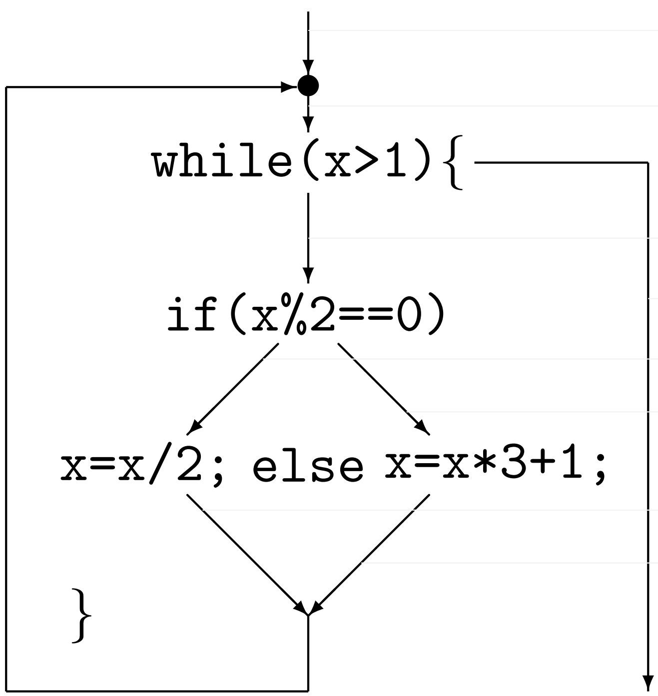


Beispiel

neu: $\bot$

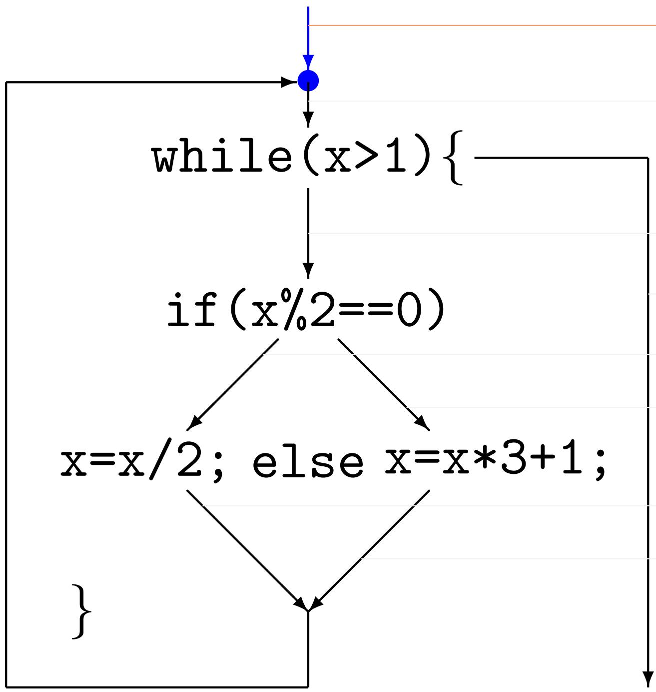


Beispiel



	neu: $\Phi(\perp)$	alt: $\perp$
A :		[ ]
B :		[ ]
C :		[ ]
D :		[ ]
E :		[ ]
F :		[ ]
G :		[ ]
H :		[ ]

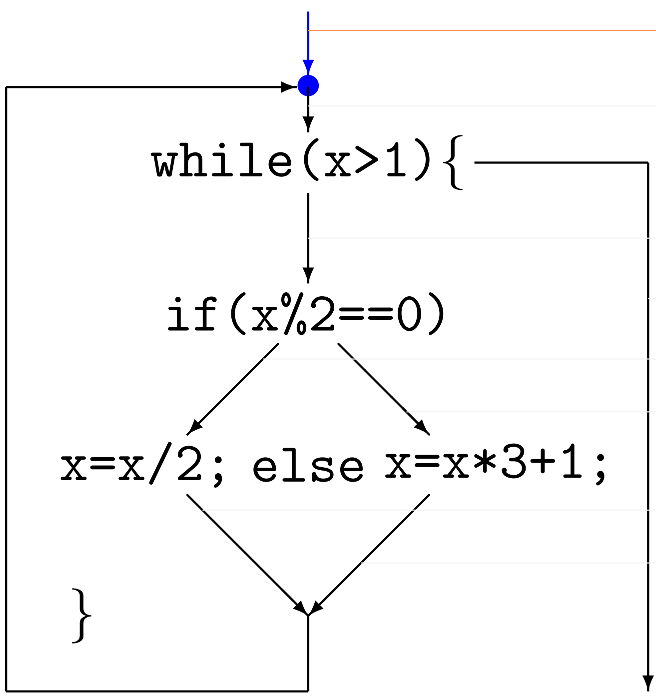
Beispiel



	neu: $\Phi(\perp)$	alt: $\perp$
A	$[1 \ldots 5]$	$[\,]$
B	$[\,]$	$[\,]$
C	$[\,]$	$[\,]$
D	$[\,]$	$[\,]$
E	$[\,]$	$[\,]$
F	$[\,]$	$[\,]$
G	$[\,]$	$[\,]$
H	$[\,]$	$[\,]$

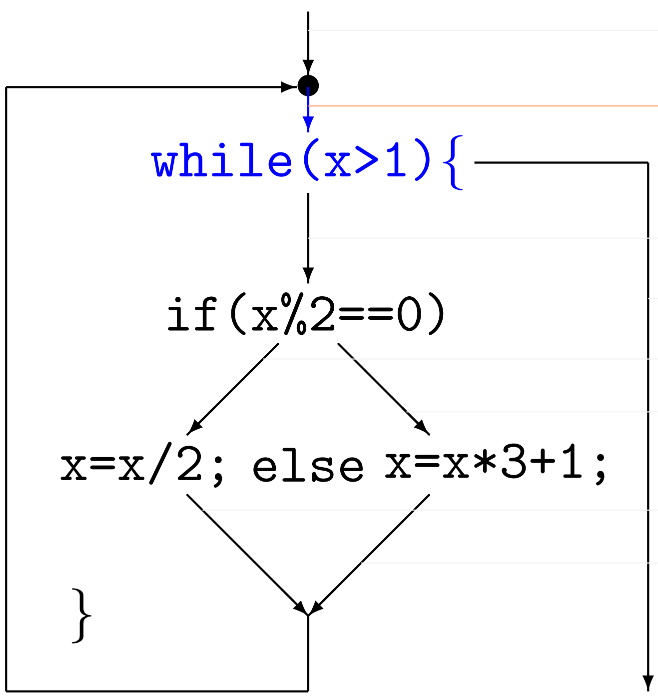
$$A = \{1, 2, 3, 4, 5\}$$

Beispiel



	neu: $\Phi(\Phi(\bot))$	alt: $\Phi(\bot)$
A :		$[1 \ldots 5]$
B :		$[\,]$
C :		$[\,]$
D :		$[\,]$
E :		$[\,]$
F :		$[\,]$
G :		$[\,]$
H :		$[\,]$

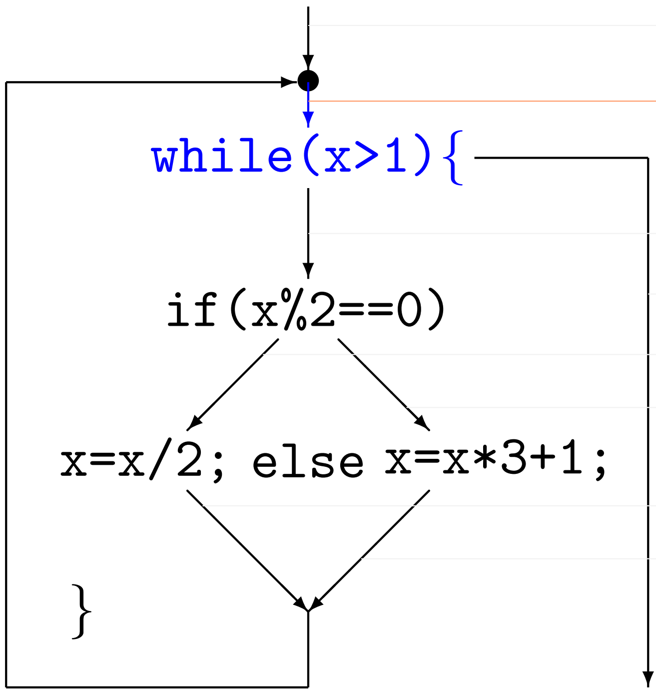
Beispiel



	neu: $\Phi(\Phi(\perp))$	alt: $\Phi(\perp)$
A :	$[1\ldots5]$	$[1\ldots5]$
B :	$[1\ldots5]$	$[\,]$
C :	$[\,]$	$[\,]$
D :	$[\,]$	$[\,]$
E :	$[\,]$	$[\,]$
F :	$[\,]$	$[\,]$
G :	$[\,]$	$[\,]$
H :	$[\,]$	$[\,]$

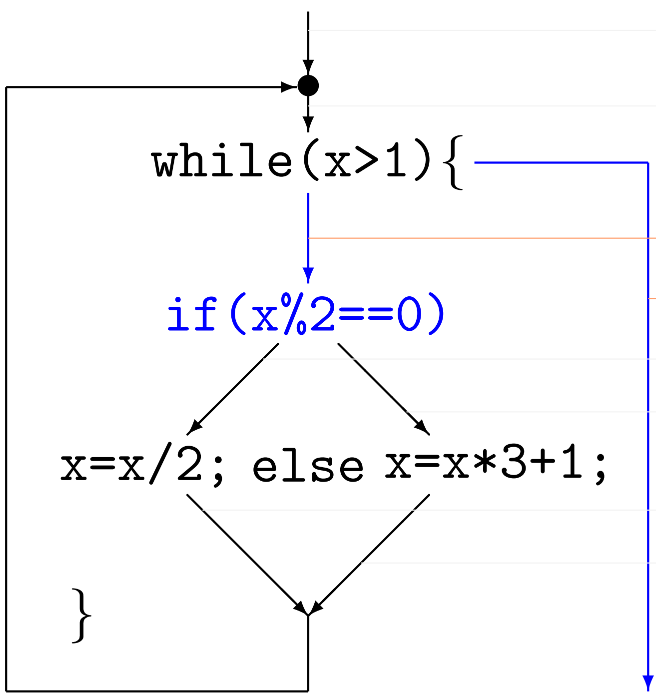
$$B = A \cup G \cup H$$

Beispiel



	neu: $\Phi^3(\perp)$	alt: $\Phi(\Phi(\perp))$
A :		$[1\ldots5]$
B :		$[1\ldots5]$
C :		$[\,]$
D :		$[\,]$
E :		$[\,]$
F :		$[\,]$
G :		$[\,]$
H :		$[\,]$

Beispiel

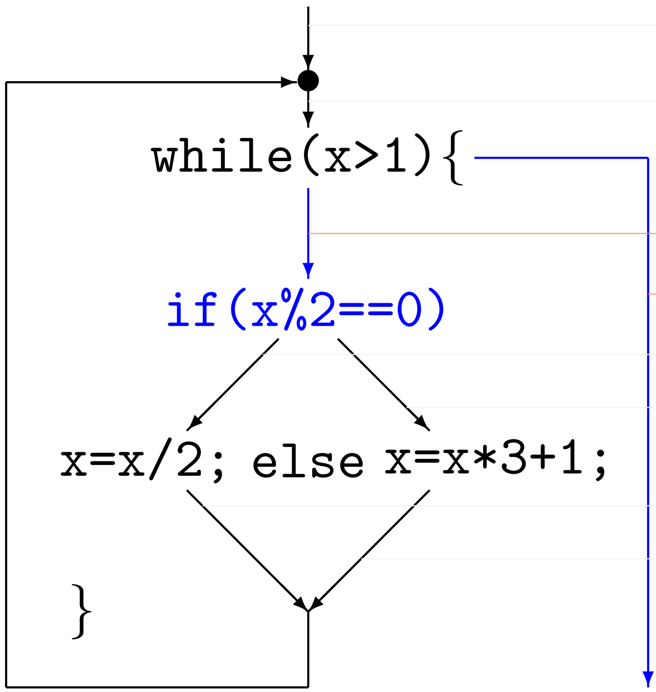


	neu: $\Phi^3(\bot)$	alt: $\Phi(\Phi(\bot))$
$A:$	$[1\dots5]$	$[1\dots5]$
$B:$	$[1\dots5]$	$[1\dots5]$
$C:$	$[2\dots5]$	$[\,]$
$D:$	$[1\dots1]$	$[\,]$
$E:$	$[\,]$	$[\,]$
$F:$	$[\,]$	$[\,]$
$G:$	$[\,]$	$[\,]$
$H:$	$[\,]$	$[\,]$

$$C = B \cap \{2, 3, 4, \dots\}$$

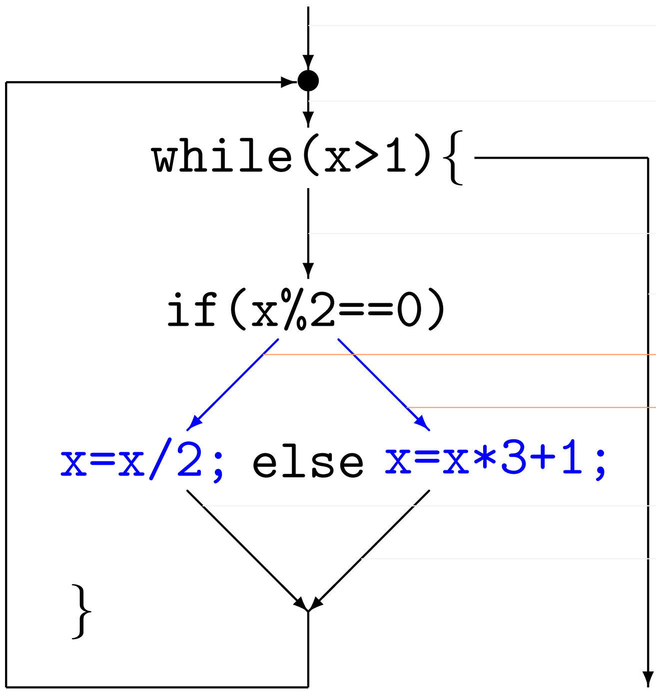
$$D = B \cap \{\dots, -2, -1, 0, 1\}$$

Beispiel



	neu: $\Phi^4(\bot)$	alt: $\Phi^3(\bot)$
A :		$[1 \ldots 5]$
B :		$[1 \ldots 5]$
C :		$[2 \ldots 5]$
D :		$[1 \ldots 1]$
E :		$[\,]$
F :		$[\,]$
G :		$[\,]$
H :		$[\,]$

Beispiel

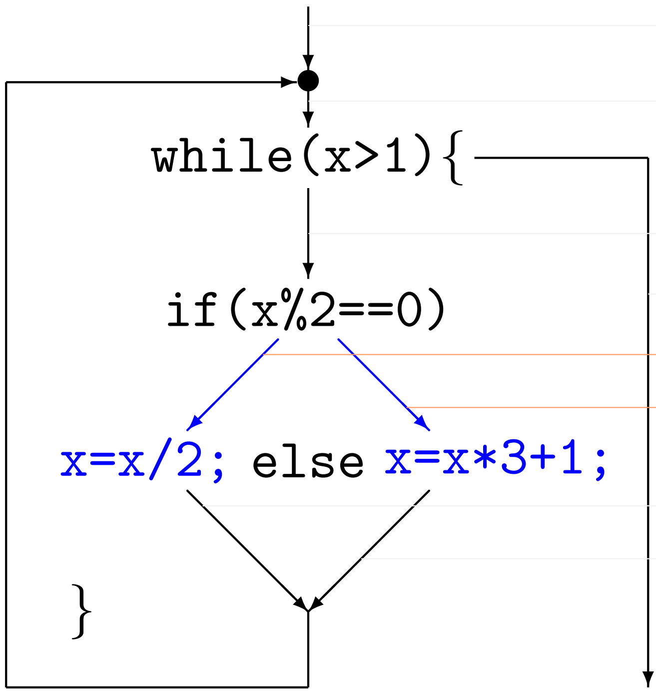


	neu: $\Phi^4(\perp)$	alt: $\Phi^3(\perp)$
A	$[1\ldots5]$	$[1\ldots5]$
B	$[1\ldots5]$	$[1\ldots5]$
C	$[2\ldots5]$	$[2\ldots5]$
D	$[1\ldots1]$	$[1\ldots1]$
E	$[2\ldots4]$	$[\,]$
F	$[3\ldots5]$	$[\,]$
G	$[\,]$	$[\,]$
H	$[\,]$	$[\,]$

$$E = C \cap \{\ldots, -4, -2, 0, 2, 4, \ldots\}$$

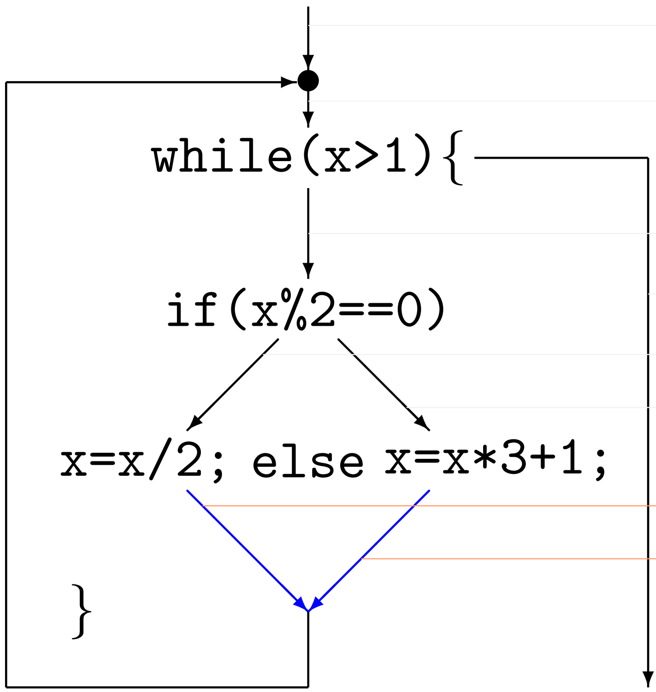
$$F = C \cap \{\ldots, -3, -1, 1, 3, \ldots\}$$

Beispiel



	neu: $\Phi^5(\perp)$	alt: $\Phi^4(\perp)$
A :		$[1\dots5]$
B :		$[1\dots5]$
C :		$[2\dots5]$
D :		$[1\dots1]$
E :		$[2\dots4]$
F :		$[3\dots5]$
G :		$[\,]$
H :		$[\,]$

Beispiel

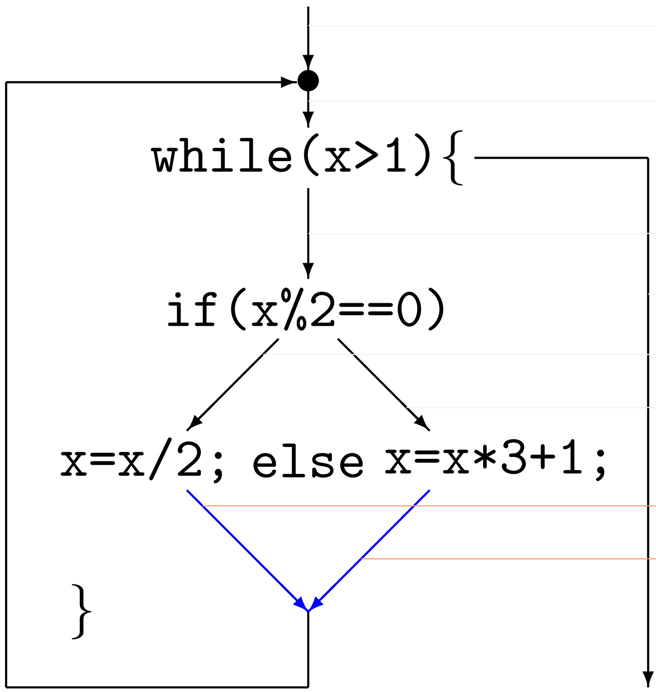


	neu: $\Phi^5(\perp)$	alt: $\Phi^4(\perp)$
A	$[1\ldots5]$	$[1\ldots5]$
B	$[1\ldots5]$	$[1\ldots5]$
C	$[2\ldots5]$	$[2\ldots5]$
D	$[1\ldots1]$	$[1\ldots1]$
E	$[2\ldots4]$	$[2\ldots4]$
F	$[3\ldots5]$	$[3\ldots5]$
G	$[1\ldots2]$	$[\,]$
H	$[10\ldots16]$	$[\,]$

$$G = \{n/2 \mid n \in E\}$$

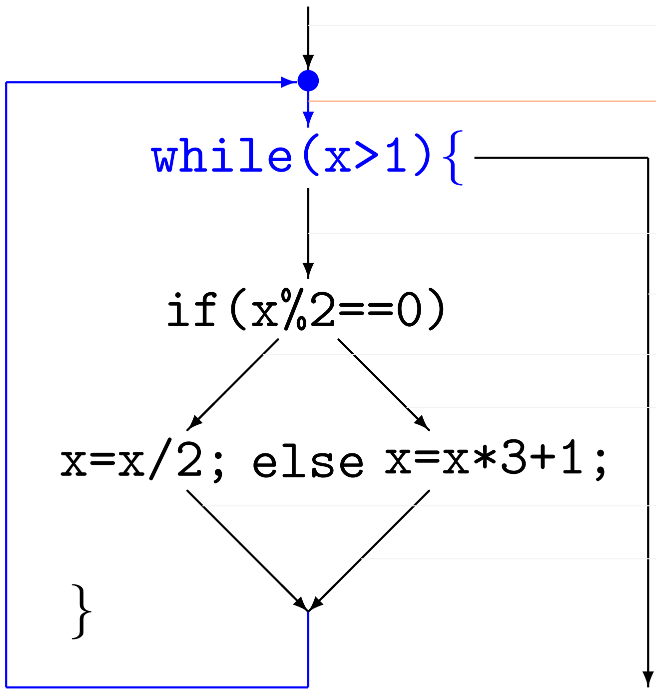
$$H = \{3 \cdot n + 1 \mid n \in F\}$$

Beispiel



	neu: $\Phi^6(\perp)$	alt: $\Phi^5(\perp)$
$A:$		$[1\dots5]$
$B:$		$[1\dots5]$
$C:$		$[2\dots5]$
$D:$		$[1\dots1]$
$E:$		$[2\dots4]$
$F:$		$[3\dots5]$
$G:$		$[1\dots2]$
$H:$		$[10\dots16]$

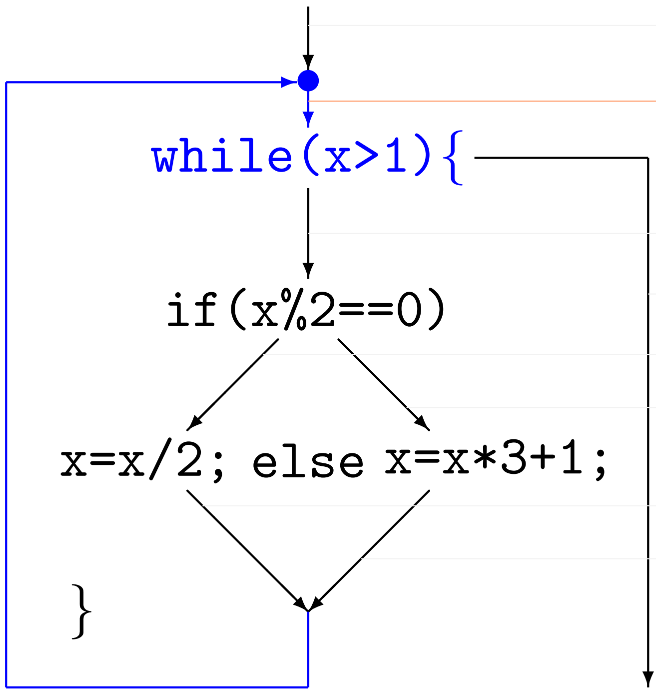
Beispiel



	neu: $\Phi^6(\perp)$	alt: $\Phi^5(\perp)$
A	$[1 \ldots 5]$	$[1 \ldots 5]$
B	$[1 \ldots 16]$	$[1 \ldots 5]$
C	$[2 \ldots 5]$	$[2 \ldots 5]$
D	$[1 \ldots 1]$	$[1 \ldots 1]$
E	$[2 \ldots 4]$	$[2 \ldots 4]$
F	$[3 \ldots 5]$	$[3 \ldots 5]$
G	$[1 \ldots 2]$	$[1 \ldots 2]$
H	$[10 \ldots 16]$	$[10 \ldots 16]$

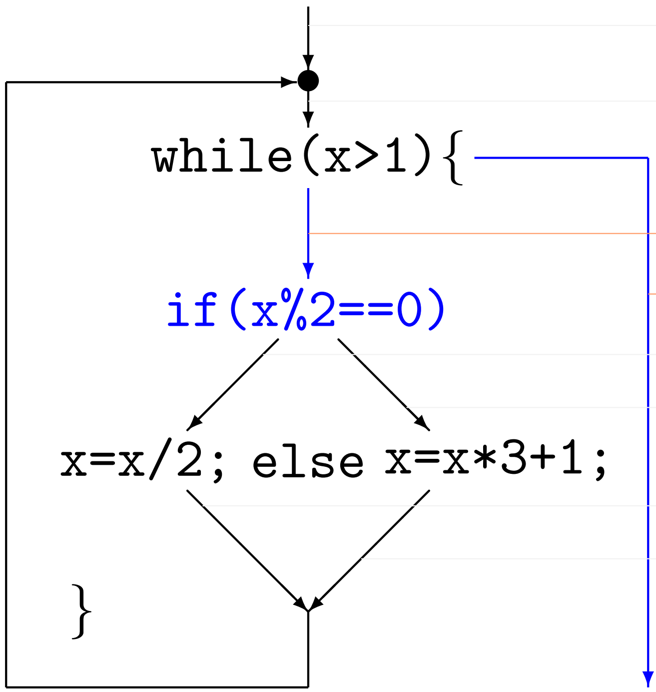
$$B = A \cup G \cup H$$

Beispiel



	neu: $\Phi^7(\perp)$	alt: $\Phi^6(\perp)$
A :		$[1 \dots 5]$
B :		$[1 \dots 16]$
C :		$[2 \dots 5]$
D :		$[1 \dots 1]$
E :		$[2 \dots 4]$
F :		$[3 \dots 5]$
G :		$[1 \dots 2]$
H :		$[10 \dots 16]$

Beispiel

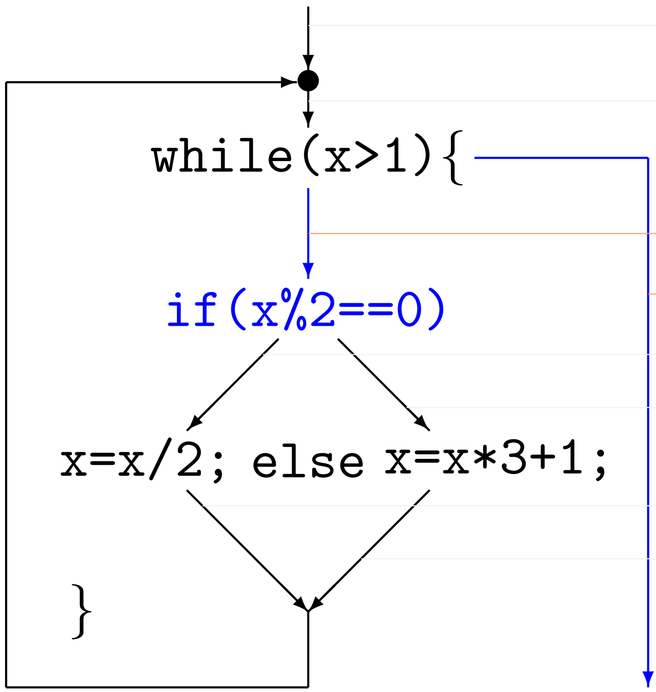


	neu: $\Phi^7(\bot)$	alt: $\Phi^6(\bot)$
A :	$[1 \ldots 5]$	$[1 \ldots 5]$
B :	$[1 \ldots 16]$	$[1 \ldots 16]$
C :	$[2 \ldots 16]$	$[2 \ldots 5]$
D :	$[1 \ldots 1]$	$[1 \ldots 1]$
E :	$[2 \ldots 4]$	$[2 \ldots 4]$
F :	$[3 \ldots 5]$	$[3 \ldots 5]$
G :	$[1 \ldots 2]$	$[1 \ldots 2]$
H :	$[10 \ldots 16]$	$[10 \ldots 16]$

$$C = B \cap \{2, 3, 4, \ldots\}$$

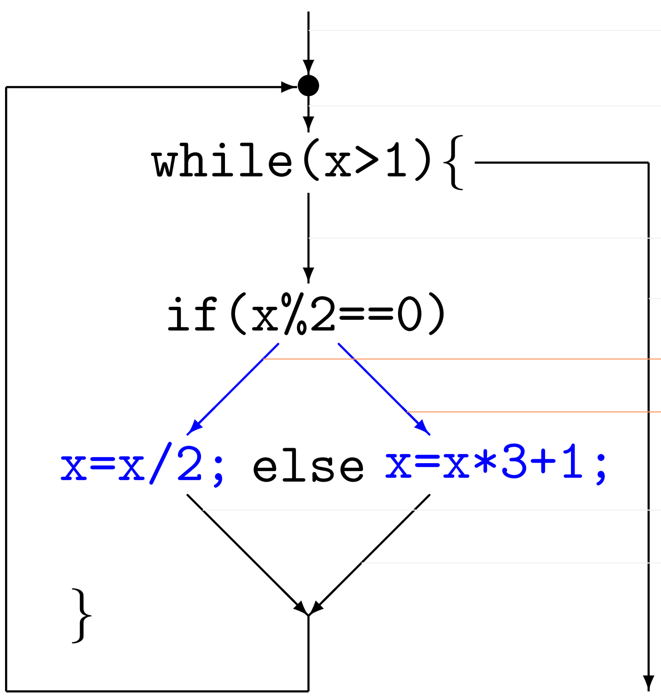
$$D = B \cap \{\ldots, -2, -1, 0, 1\}$$

Beispiel



	neu: $\Phi^8(\bot)$	alt: $\Phi^7(\bot)$
A :		$[1 \ldots 5]$
B :		$[1 \ldots 16]$
C :		$[2 \ldots 16]$
D :		$[1 \ldots 1]$
E :		$[2 \ldots 4]$
F :		$[3 \ldots 5]$
G :		$[1 \ldots 2]$
H :		$[10 \ldots 16]$

Beispiel

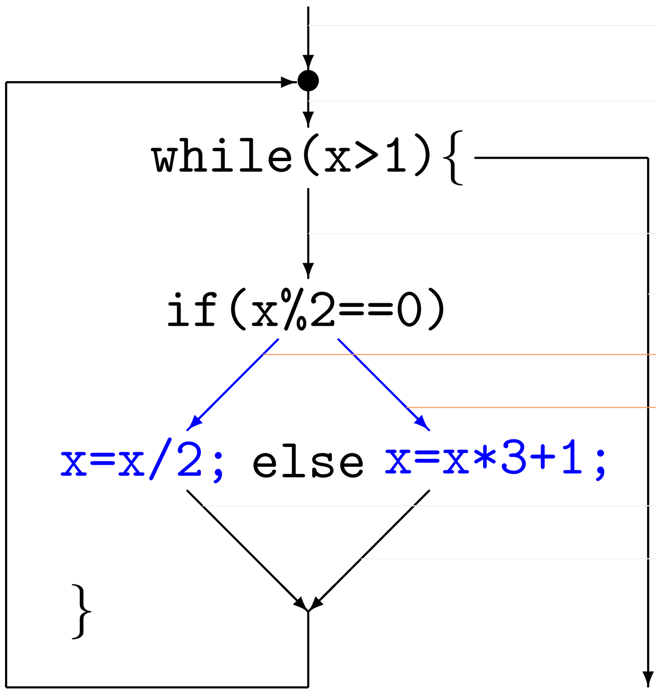


	neu: $\Phi^8(\bot)$	alt: $\Phi^7(\bot)$
A	$[1\ldots5]$	$[1\ldots5]$
B	$[1\ldots16]$	$[1\ldots16]$
C	$[2\ldots16]$	$[2\ldots16]$
D	$[1\ldots1]$	$[1\ldots1]$
E	$[2\ldots16]$	$[2\ldots4]$
F	$[3\ldots15]$	$[3\ldots5]$
G	$[1\ldots2]$	$[1\ldots2]$
H	$[10\ldots16]$	$[10\ldots16]$

$$E = C \cap \{\ldots, -4, -2, 0, 2, 4, \ldots\}$$

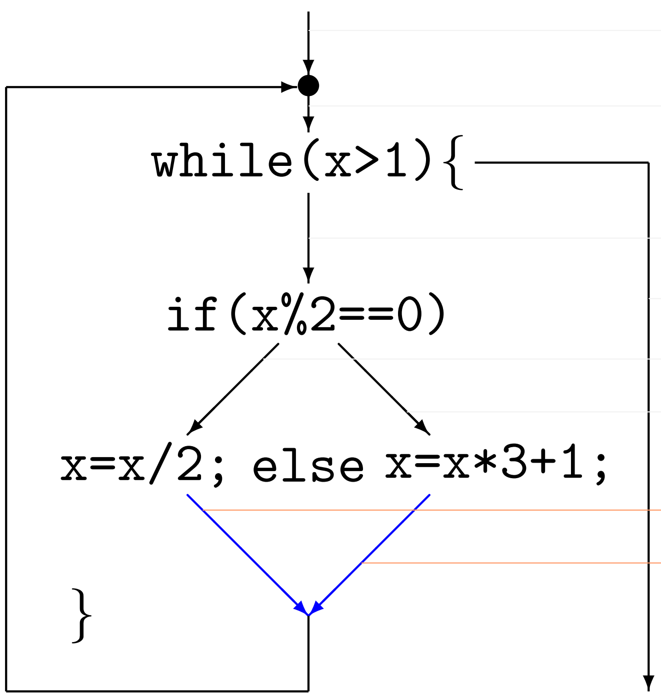
$$F = C \cap \{\ldots, -3, -1, 1, 3, \ldots\}$$

Beispiel



	neu: $\Phi^9(\perp)$	alt: $\Phi^8(\perp)$
A :		$[1 \ldots 5]$
B :		$[1 \ldots 16]$
C :		$[2 \ldots 16]$
D :		$[1 \ldots 1]$
E :		$[2 \ldots 16]$
F :		$[3 \ldots 15]$
G :		$[1 \ldots 2]$
H :		$[10 \ldots 16]$

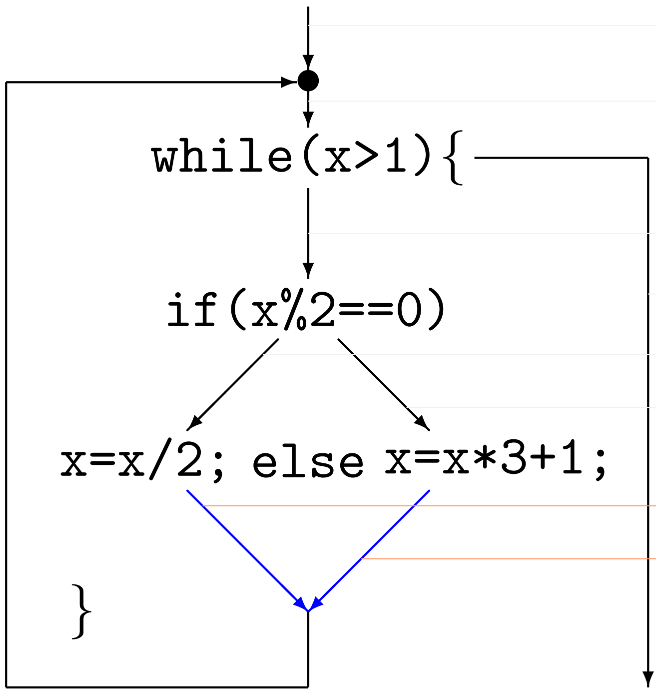
Beispiel



	neu: $\Phi^9(\perp)$	alt: $\Phi^8(\perp)$
A :	$[1\ldots5]$	$[1\ldots5]$
B :	$[1\ldots16]$	$[1\ldots16]$
C :	$[2\ldots16]$	$[2\ldots16]$
D :	$[1\ldots1]$	$[1\ldots1]$
E :	$[2\ldots16]$	$[2\ldots16]$
F :	$[3\ldots15]$	$[3\ldots15]$
G :	$[1\ldots8]$	$[1\ldots2]$
H :	$[10\ldots46]$	$[10\ldots16]$

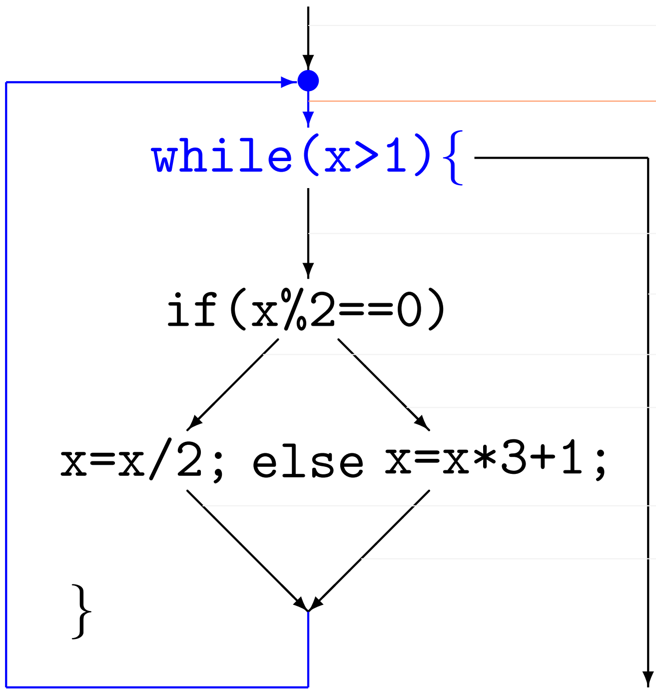
$$G = \{n/2 \mid n \in E\}$$
$$H = \{3 \cdot n + 1 \mid n \in F\}$$

Beispiel



	neu: $\Phi^{10}(\bot)$	alt: $\Phi^{9}(\bot)$
$A:$		$[1\ldots 5]$
$B:$		$[1\ldots 16]$
$C:$		$[2\ldots 16]$
$D:$		$[1\ldots 1]$
$E:$		$[2\ldots 16]$
$F:$		$[3\ldots 15]$
$G:$		$[1\ldots 8]$
$H:$		$[10\ldots 46]$

Beispiel



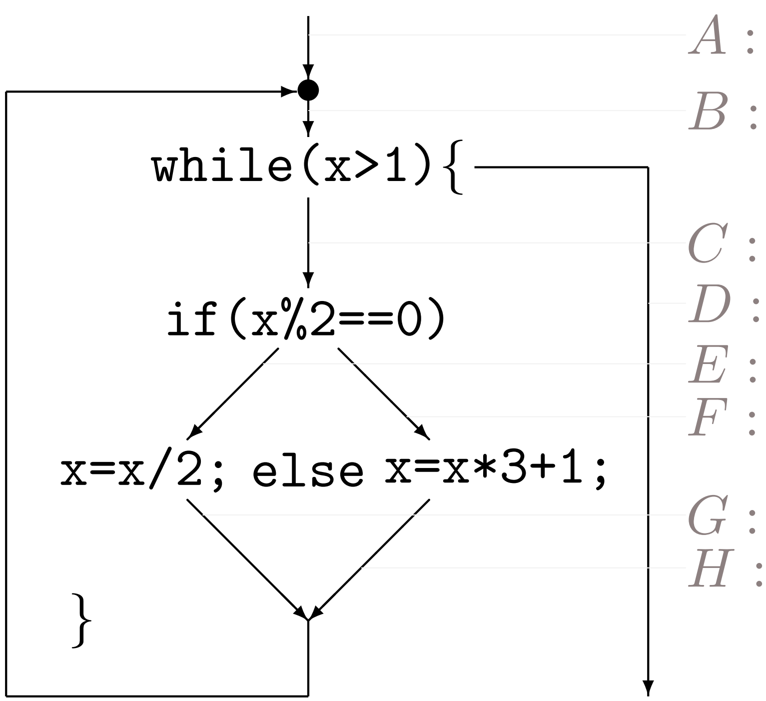
	neu: $\Phi^{10}(\perp)$	alt: $\Phi^{9}(\perp)$
A	$[1\ldots5]$	$[1\ldots5]$
B	$[1\ldots46]$	$[1\ldots16]$
C	$[2\ldots16]$	$[2\ldots16]$
D	$[1\ldots1]$	$[1\ldots1]$
E	$[2\ldots16]$	$[2\ldots16]$
F	$[3\ldots15]$	$[3\ldots15]$
G	$[1\ldots8]$	$[1\ldots8]$
H	$[10\ldots46]$	$[10\ldots46]$

$$B = A \cup G \cup H$$

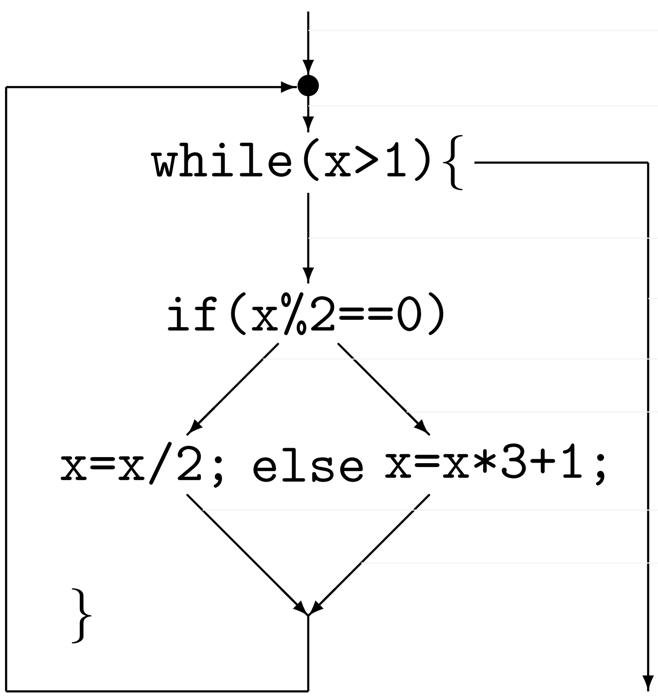
Beispiel

neu:

alt:



Beispiel



	neu: $\Phi^{n}(\underline{\perp})$	alt: $\Phi^{n-1}(\underline{\perp})$
A :	$[1 \ldots 5]$	$[1 \ldots 5]$
B :	$[1 \ldots 16]$	$[1 \ldots 16]$
C :	$[2 \ldots 16]$	$[2 \ldots 16]$
D :	$[1 \ldots 1]$	$[1 \ldots 1]$
E :	$[2 \ldots 16]$	$[2 \ldots 16]$
F :	$[3 \ldots 15]$	$[3 \ldots 15]$
G :	$[1 \ldots 8]$	$[1 \ldots 8]$
H :	$[10 \ldots 46]$	$[10 \ldots 46]$

Fixpunkt erreicht

$$E = C \cap \{\ldots, -2, 0, 2, 4, \ldots\}$$

$$H = \{3 \cdot x + 1 \mid x \in F\}$$

Terminierung: Widening

Andererseits ist es sehr wünschenswert, Informationen über die Grenzen, innerhalb derer sich ein Variablenwert an einer Programmstelle bewegen kann, zu bekommen.

Sofern Φ' zusätzlich stetig ist, kann man eine Methode aus (Cousot,Cousot 1992) anwenden, die Φ' so modifiziert, daß es nach endlich vielen Iterationen nichts mehr ändert, daß also die Kette $\perp' \sqsubseteq' \Phi'(\perp') \sqsubseteq' \Phi'(\Phi'(\perp')) \sqsubseteq' \ldots \sqsubseteq' \Phi'^i(\perp') \sqsubseteq' \ldots$ garantiert stationär wird.

Terminierung: Widening

Formal: Sei Φ' zusätzlich stetig.
Sei $\nabla : M' \times M' \longrightarrow M'$ eine Operation, so daß $x' \sqcup y' \sqsubseteq' x' \nabla y'$ und für jede

$$
\begin{array}{lccccccccc}
\text{aufsteigende Kette} & x'_1 & \sqsubseteq' & x'_2 & \sqsubseteq' & \ldots & \sqsubseteq' & x'_i & \sqsubseteq' & \ldots \\
\text{die Kette} & x'_1 & \sqsubseteq' & x'_1 \nabla x'_2 & \sqsubseteq' & \ldots & \sqsubseteq' & x'_1 \nabla \ldots \nabla x'_i & \sqsubseteq' & \ldots
\end{array}
$$

irgendwann stationär wird.

Definiere $\Phi''(x') = \begin{cases} x' & \text{für } \Phi'(x') = x' \\ x' \nabla \Phi'(x') & \text{sonst} \end{cases}$.

Dann ist die Kette $\bot' \sqsubseteq' \Phi''(\bot') \sqsubseteq' \Phi''(\Phi''(\bot')) \sqsubseteq' \ldots \sqsubseteq' \Phi''^i(\bot') \sqsubseteq' \ldots$
irgendwann stationär und ihre kleinste obere Schranke
$X'' = \bigsqcup'\{\bot', \Phi''(\bot'), \Phi''(\Phi''(\bot')), \ldots\}$ ist eine obere Abschätzung für den kleinsten Fixpunkt X' von Φ'.

Beispiel mit Widening

Definiere eine widening-Operation auf Intervallen durch
$[l \ldots u] \,\nabla [\,] = [\,] \,\nabla [l \ldots u] = [l \ldots u]$ sowie $[l_1 \ldots u_1] \,\nabla [l_2 \ldots u_2] = [l \ldots u]$ mit

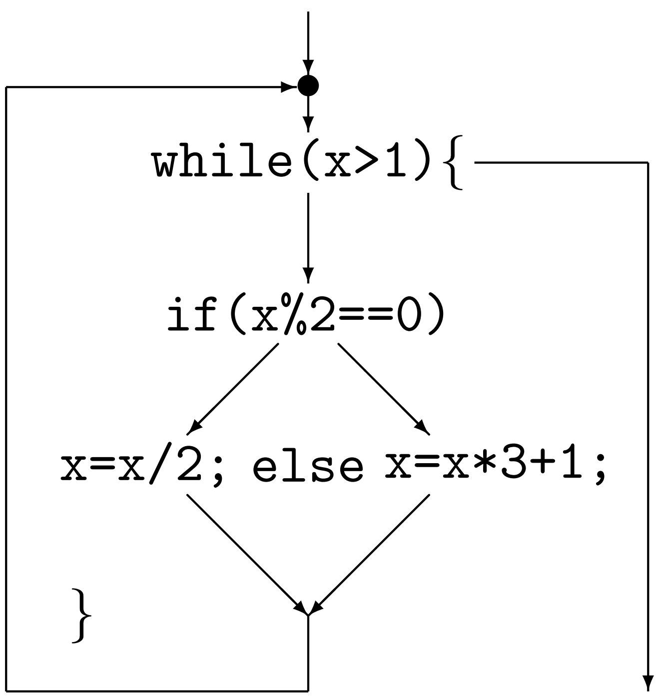
$$l = \begin{cases} -\infty & \text{für} \quad l_2 < l_1 \\ l_1 & \text{sonst} \end{cases} \quad \text{und} \quad u = \begin{cases} +\infty & \text{für} \quad u_2 > u_1 \\ u_1 & \text{sonst} \end{cases}$$

Anschaulich: Sobald sich eine Intervallgrenze verschlechtert, wird sie gleich auf den schlechtestmöglichen Wert gesetzt.

Z.B. $[1 \ldots 5] \,\nabla [1 \ldots 16] = [1 \ldots \infty]$, $[1 \ldots 16] \,\nabla [1 \ldots 5] = [1 \ldots 16]$.

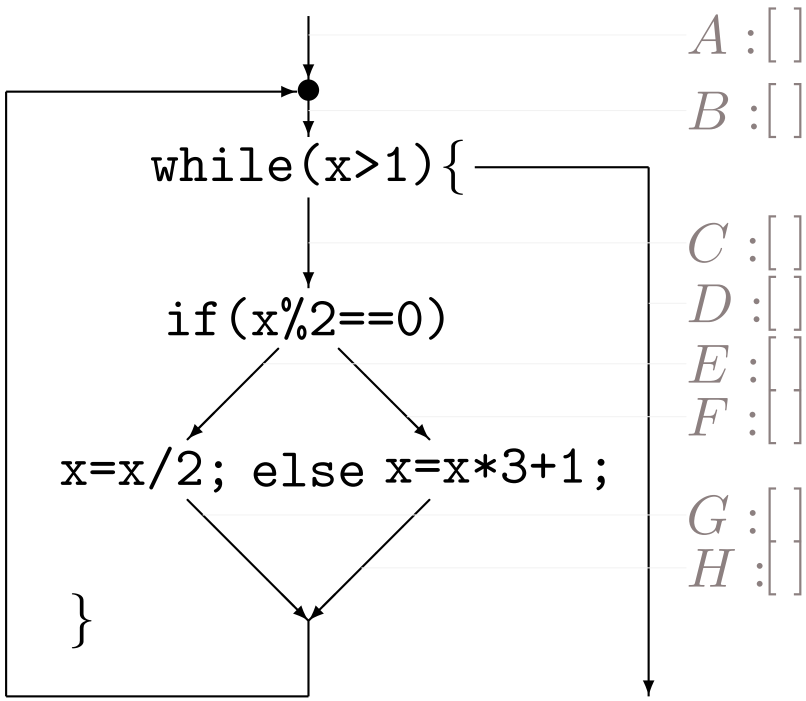
(∇) ist nicht kommutativ, da es die zeitliche Reihenfolge berücksichtigen soll.

Beispiel mit Widening

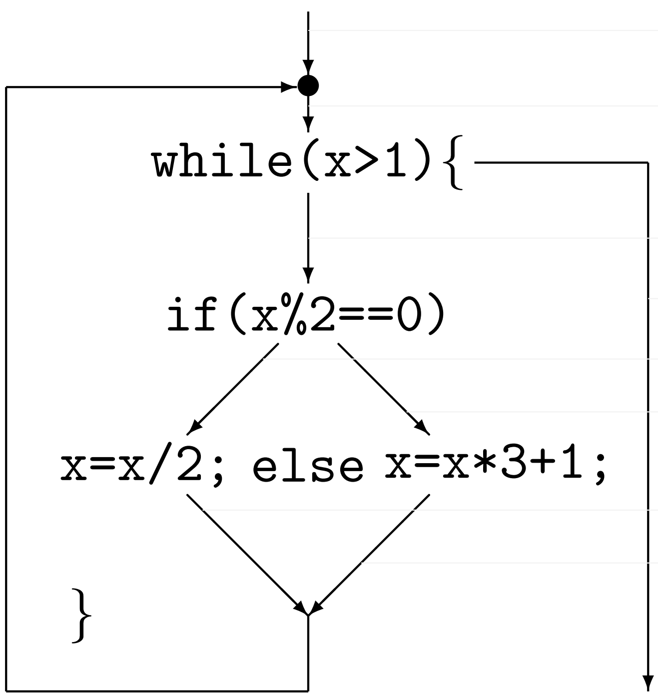


Beispiel mit Widening

neu: $\perp$

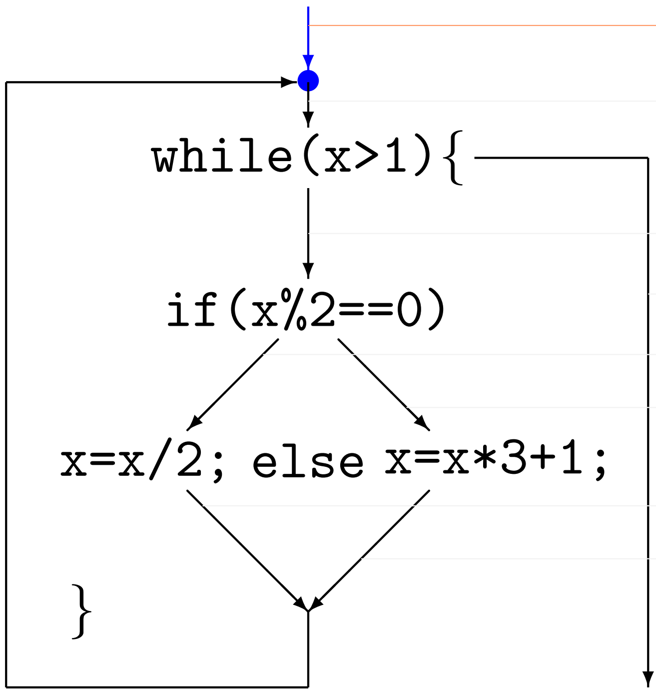


Beispiel mit Widening



	neu: $\Phi(\perp)$	alt: $\perp$
A :		[ ]
B :		[ ]
C :		[ ]
D :		[ ]
E :		[ ]
F :		[ ]
G :		[ ]
H :		[ ]

Beispiel mit Widening

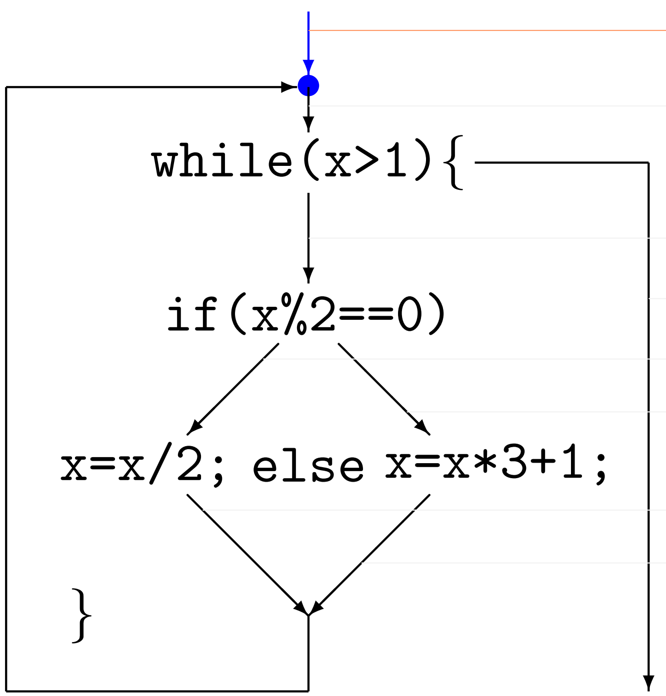


neu: $\Phi(\perp)$ alt: $\perp$

	neu	alt
A	$[1\ldots 5]$	$[\,]$
B	$[\,]$	$[\,]$
C	$[\,]$	$[\,]$
D	$[\,]$	$[\,]$
E	$[\,]$	$[\,]$
F	$[\,]$	$[\,]$
G	$[\,]$	$[\,]$
H	$[\,]$	$[\,]$

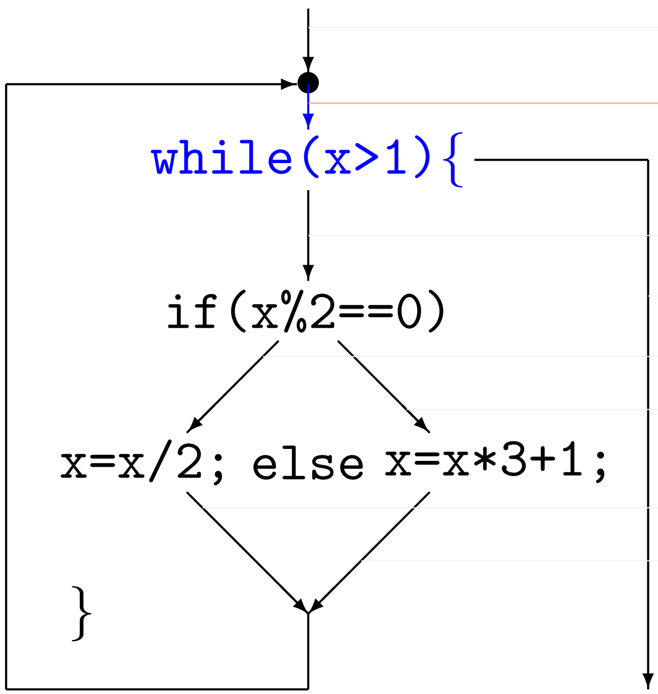
$$A = \{1, 2, 3, 4, 5\}$$

Beispiel mit Widening



	neu: $\Phi(\Phi(\perp))$	alt: $\Phi(\perp)$
A :		$[1\ldots5]$
B :		$[\,]$
C :		$[\,]$
D :		$[\,]$
E :		$[\,]$
F :		$[\,]$
G :		$[\,]$
H :		$[\,]$

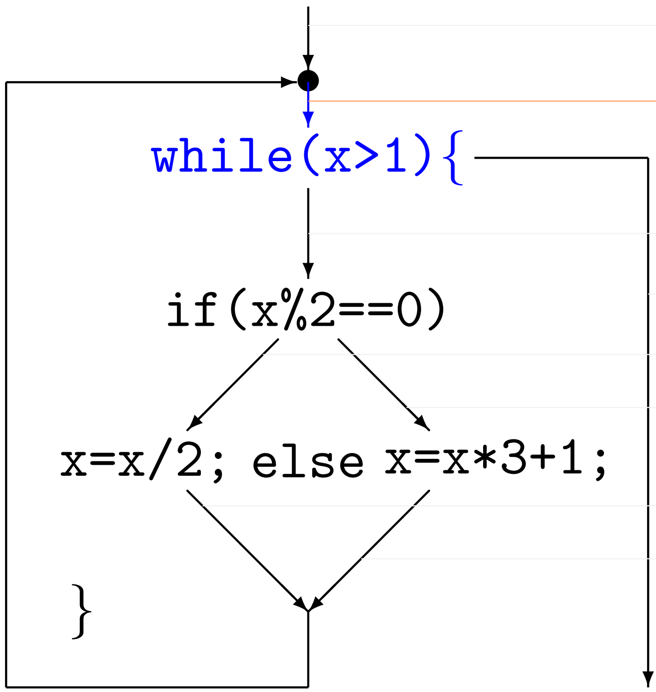
Beispiel mit Widening



	neu: $\Phi(\Phi(\perp))$	alt: $\Phi(\perp)$
A :	$[1\ldots5]$	$[1\ldots5]$
B :	$[1\ldots5]$	$[\,]$
C :	$[\,]$	$[\,]$
D :	$[\,]$	$[\,]$
E :	$[\,]$	$[\,]$
F :	$[\,]$	$[\,]$
G :	$[\,]$	$[\,]$
H :	$[\,]$	$[\,]$

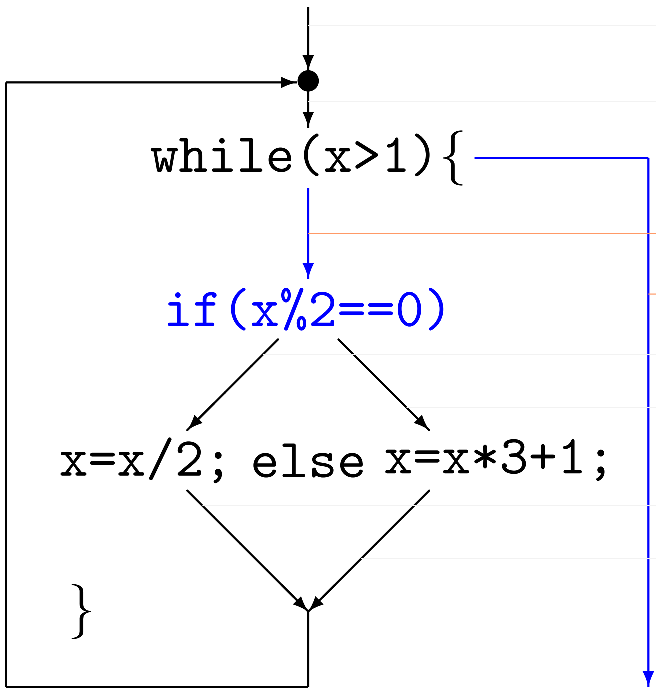
$$B = A \cup G \cup H$$

Beispiel mit Widening



	neu: $\Phi^3(\bot)$	alt: $\Phi(\Phi(\bot))$
A :		$[1 \ldots 5]$
B :		$[1 \ldots 5]$
C :		$[\,]$
D :		$[\,]$
E :		$[\,]$
F :		$[\,]$
G :		$[\,]$
H :		$[\,]$

Beispiel mit Widening

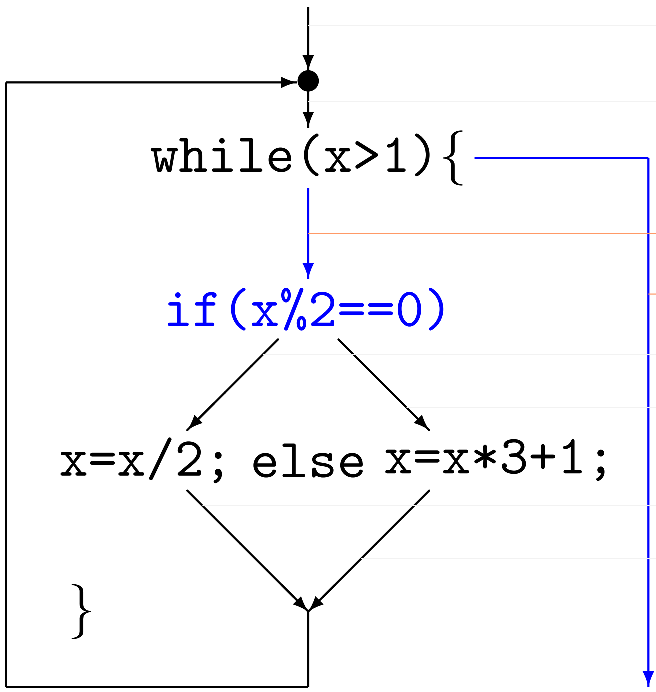


	neu: $\Phi^3(\perp)$	alt: $\Phi(\Phi(\perp))$
A	$[1 \ldots 5]$	$[1 \ldots 5]$
B	$[1 \ldots 5]$	$[1 \ldots 5]$
C	$[2 \ldots 5]$	$[\,]$
D	$[1 \ldots 1]$	$[\,]$
E	$[\,]$	$[\,]$
F	$[\,]$	$[\,]$
G	$[\,]$	$[\,]$
H	$[\,]$	$[\,]$

$$C = B \cap \{2, 3, 4, \ldots\}$$

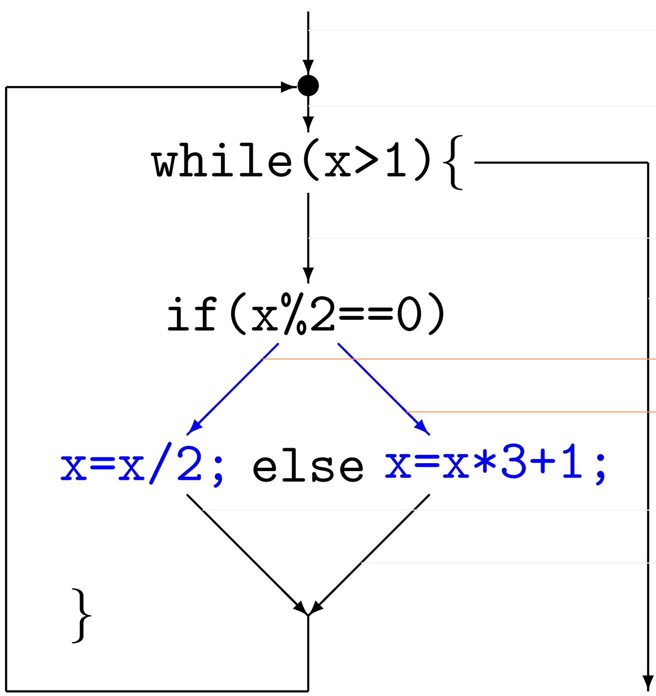
$$D = B \cap \{\ldots, -2, -1, 0, 1\}$$

Beispiel mit Widening



	neu: $\Phi^4(\perp)$	alt: $\Phi^3(\perp)$
A :		$[1 \ldots 5]$
B :		$[1 \ldots 5]$
C :		$[2 \ldots 5]$
D :		$[1 \ldots 1]$
E :		$[\,]$
F :		$[\,]$
G :		$[\,]$
H :		$[\,]$

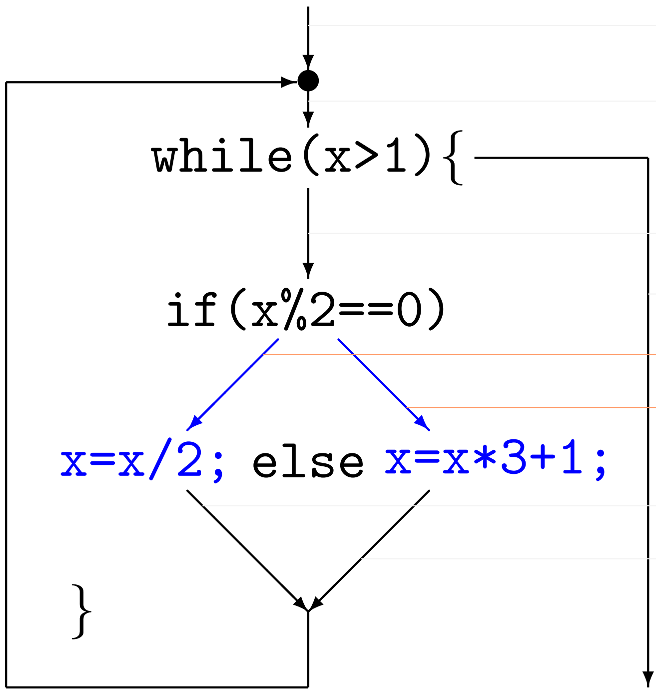
Beispiel mit Widening



	neu: $\Phi^4(\perp)$	alt: $\Phi^3(\perp)$
A :	$[1\ldots5]$	$[1\ldots5]$
B :	$[1\ldots5]$	$[1\ldots5]$
C :	$[2\ldots5]$	$[2\ldots5]$
D :	$[1\ldots1]$	$[1\ldots1]$
E :	$[2\ldots4]$	$[\,]$
F :	$[3\ldots5]$	$[\,]$
G :	$[\,]$	$[\,]$
H :	$[\,]$	$[\,]$

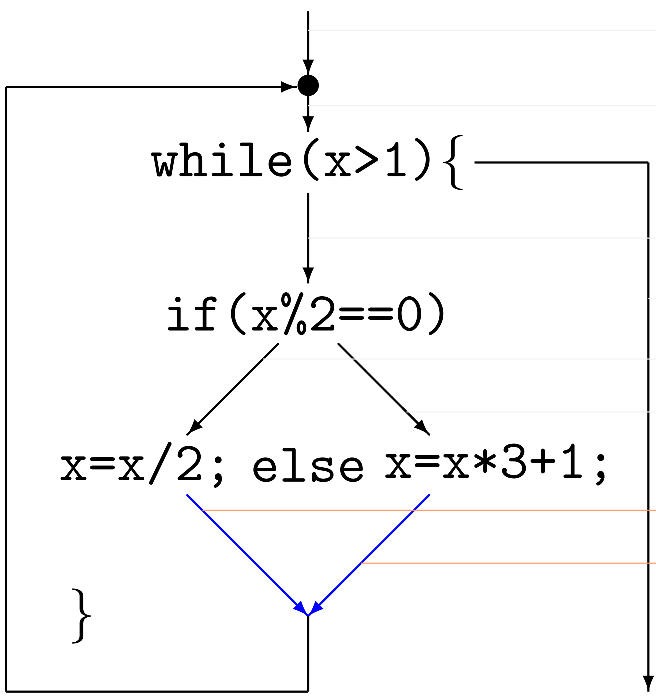
$$E = C \cap \{\ldots,-4,-2,0,2,4,\ldots\}$$
$$F = C \cap \{\ldots,-3,-1,1,3,\ldots\}$$

Beispiel mit Widening



	neu: $\Phi^5(\perp)$	alt: $\Phi^4(\perp)$
A :		$[1 \ldots 5]$
B :		$[1 \ldots 5]$
C :		$[2 \ldots 5]$
D :		$[1 \ldots 1]$
E :		$[2 \ldots 4]$
F :		$[3 \ldots 5]$
G :		$[\,]$
H :		$[\,]$

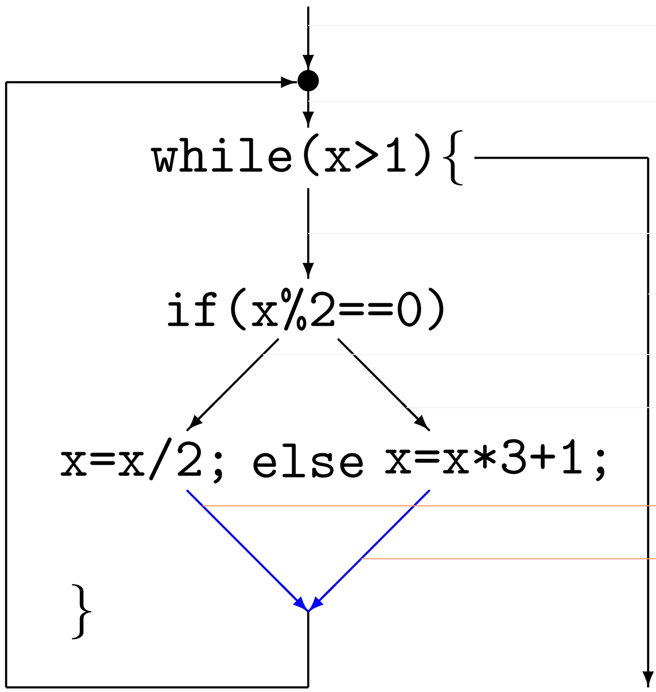
Beispiel mit Widening



	neu: $\Phi^5(\bot)$	alt: $\Phi^4(\bot)$
A	$[1\dots5]$	$[1\dots5]$
B	$[1\dots5]$	$[1\dots5]$
C	$[2\dots5]$	$[2\dots5]$
D	$[1\dots1]$	$[1\dots1]$
E	$[2\dots4]$	$[2\dots4]$
F	$[3\dots5]$	$[3\dots5]$
G	$[1\dots2]$	$[\,]$
H	$[10\dots16]$	$[\,]$

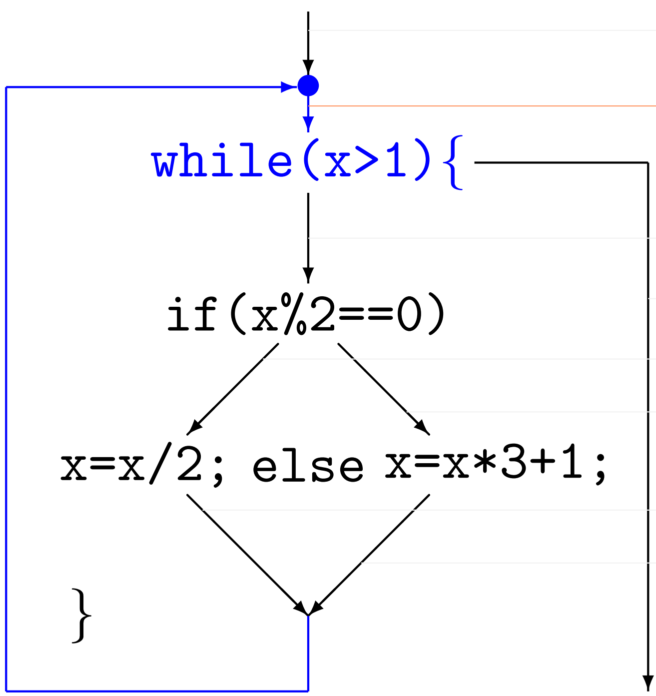
$$G = \{n/2 \mid n \in E\}$$
$$H = \{3 \cdot n + 1 \mid n \in F\}$$

Beispiel mit Widening



	neu: $\Phi^6(\bot)$	alt: $\Phi^5(\bot)$
A :		$[1 \ldots 5]$
B :		$[1 \ldots 5]$
C :		$[2 \ldots 5]$
D :		$[1 \ldots 1]$
E :		$[2 \ldots 4]$
F :		$[3 \ldots 5]$
G :		$[1 \ldots 2]$
H :		$[10 \ldots 16]$

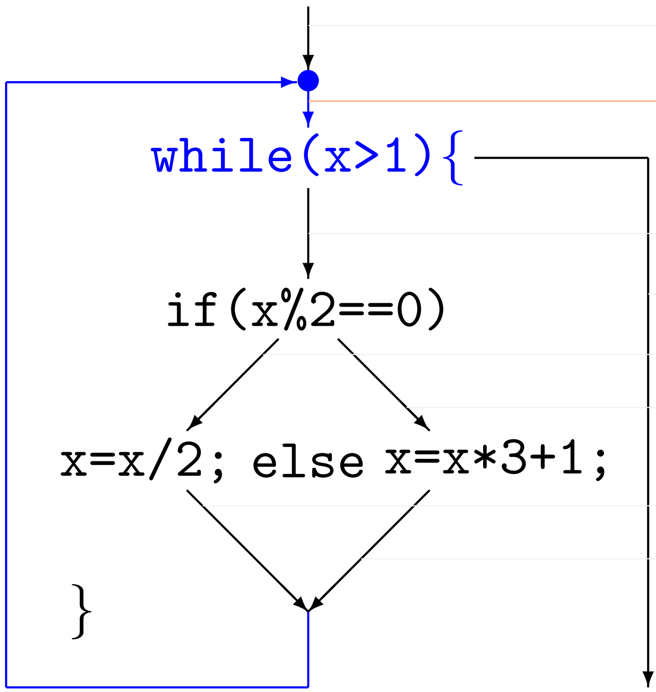
Beispiel mit Widening



	neu: $\Phi^6(\perp)$	alt: $\Phi^5(\perp)$
A :	$[1\ldots5]$	$[1\ldots5]$
B :	$[1\ldots\infty]$	$[1\ldots5]$
C :	$[2\ldots5]$	$[2\ldots5]$
D :	$[1\ldots1]$	$[1\ldots1]$
E :	$[2\ldots4]$	$[2\ldots4]$
F :	$[3\ldots5]$	$[3\ldots5]$
G :	$[1\ldots2]$	$[1\ldots2]$
H :	$[10\ldots16]$	$[10\ldots16]$

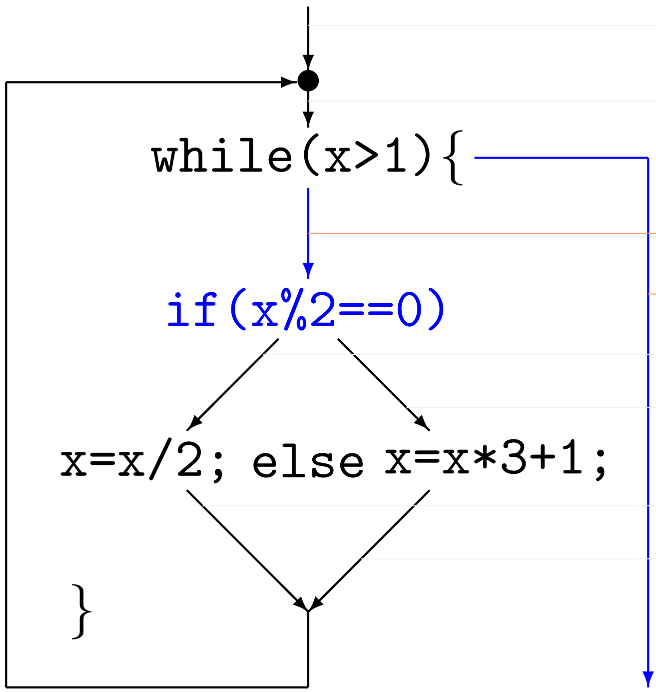
$$B = A \cup G \cup H$$

Beispiel mit Widening



	neu: $\Phi^7(\perp)$	alt: $\Phi^6(\perp)$
A :		$[1\ldots5]$
B :		$[1\ldots\infty]$
C :		$[2\ldots5]$
D :		$[1\ldots1]$
E :		$[2\ldots4]$
F :		$[3\ldots5]$
G :		$[1\ldots2]$
H :		$[10\ldots16]$

Beispiel mit Widening

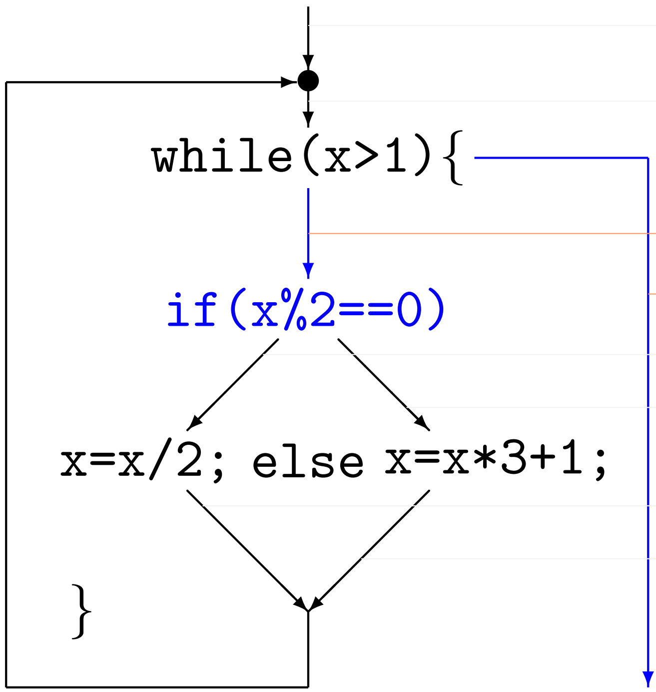


	neu: $\Phi^7(\perp)$	alt: $\Phi^6(\perp)$
A	$[1 \ldots 5]$	$[1 \ldots 5]$
B	$[1 \ldots \infty]$	$[1 \ldots \infty]$
C	$[2 \ldots \infty]$	$[2 \ldots 5]$
D	$[1 \ldots 1]$	$[1 \ldots 1]$
E	$[2 \ldots 4]$	$[2 \ldots 4]$
F	$[3 \ldots 5]$	$[3 \ldots 5]$
G	$[1 \ldots 2]$	$[1 \ldots 2]$
H	$[10 \ldots 16]$	$[10 \ldots 16]$

$$C = B \cap \{2, 3, 4, \ldots\}$$

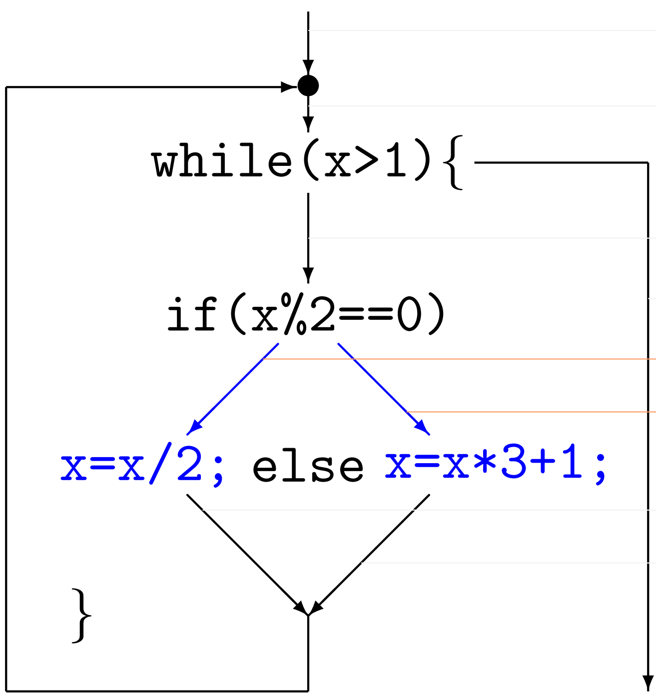
$$D = B \cap \{\ldots, -2, -1, 0, 1\}$$

Beispiel mit Widening



	neu: $\Phi^8(\perp)$	alt: $\Phi^7(\perp)$
A :		$[1 \ldots 5]$
B :		$[1 \ldots \infty]$
C :		$[2 \ldots \infty]$
D :		$[1 \ldots 1]$
E :		$[2 \ldots 4]$
F :		$[3 \ldots 5]$
G :		$[1 \ldots 2]$
H :		$[10 \ldots 16]$

Beispiel mit Widening

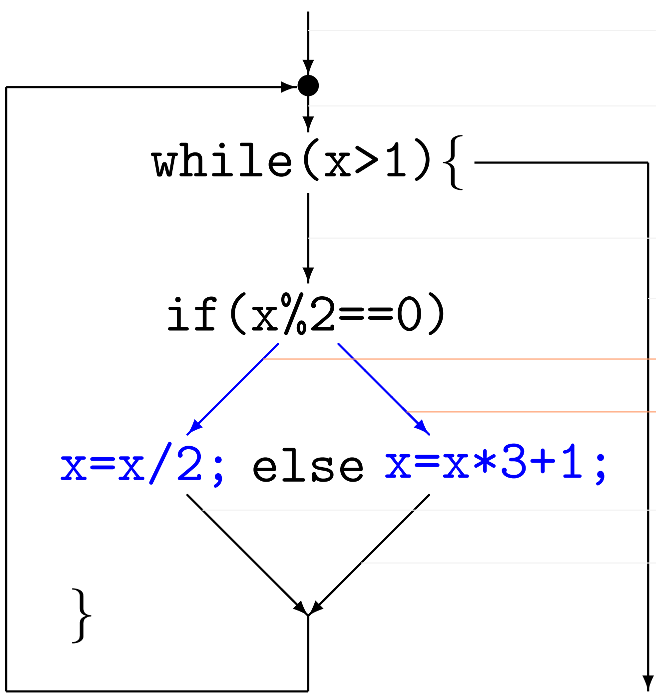


	neu: $\Phi^8(\perp)$	alt: $\Phi^7(\perp)$
A :	$[1\ldots5]$	$[1\ldots5]$
B :	$[1\ldots\infty]$	$[1\ldots\infty]$
C :	$[2\ldots\infty]$	$[2\ldots\infty]$
D :	$[1\ldots1]$	$[1\ldots1]$
E :	$[2\ldots\infty]$	$[2\ldots4]$
F :	$[3\ldots\infty]$	$[3\ldots5]$
G :	$[1\ldots2]$	$[1\ldots2]$
H :	$[10\ldots16]$	$[10\ldots16]$

$$E = C \cap \{\ldots, -4, -2, 0, 2, 4, \ldots\}$$

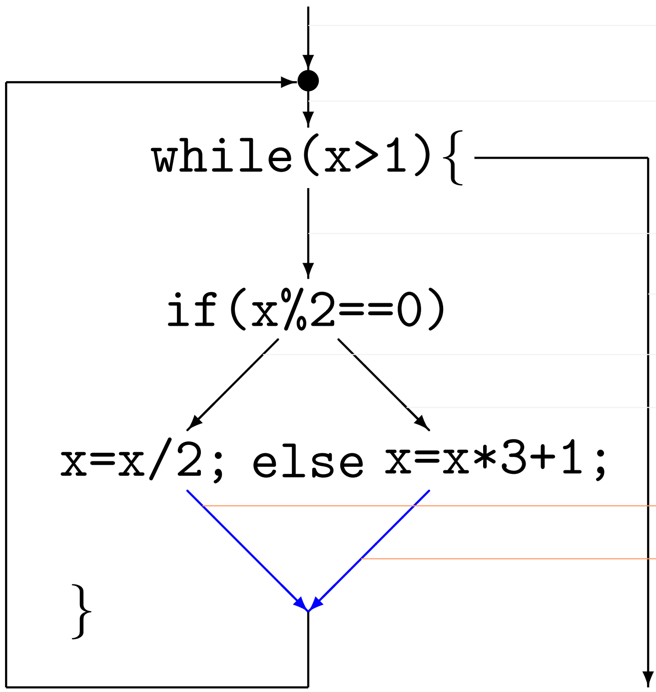
$$F = C \cap \{\ldots, -3, -1, 1, 3, \ldots\}$$

Beispiel mit Widening



	neu: $\Phi^9(\perp)$	alt: $\Phi^8(\perp)$
A :		$[1\ldots5]$
B :		$[1\ldots\infty]$
C :		$[2\ldots\infty]$
D :		$[1\ldots1]$
E :		$[2\ldots\infty]$
F :		$[3\ldots\infty]$
G :		$[1\ldots2]$
H :		$[10\ldots16]$

Beispiel mit Widening

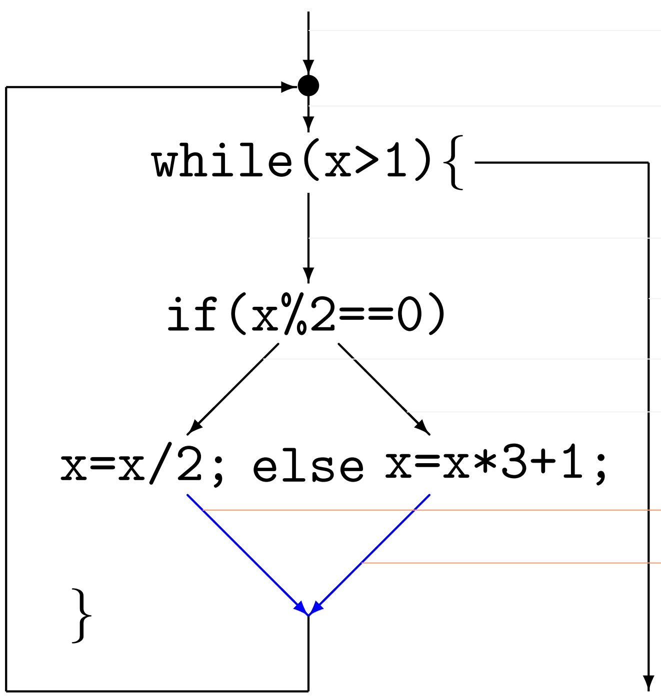


	neu: $\Phi^9(\bot)$	alt: $\Phi^8(\bot)$
A	$[1 \ldots 5]$	$[1 \ldots 5]$
B	$[1 \ldots \infty]$	$[1 \ldots \infty]$
C	$[2 \ldots \infty]$	$[2 \ldots \infty]$
D	$[1 \ldots 1]$	$[1 \ldots 1]$
E	$[2 \ldots \infty]$	$[2 \ldots \infty]$
F	$[3 \ldots \infty]$	$[3 \ldots \infty]$
G	$[1 \ldots \infty]$	$[1 \ldots 2]$
H	$[10 \ldots \infty]$	$[10 \ldots 16]$

$$G = \{n/2 \mid n \in E\}$$

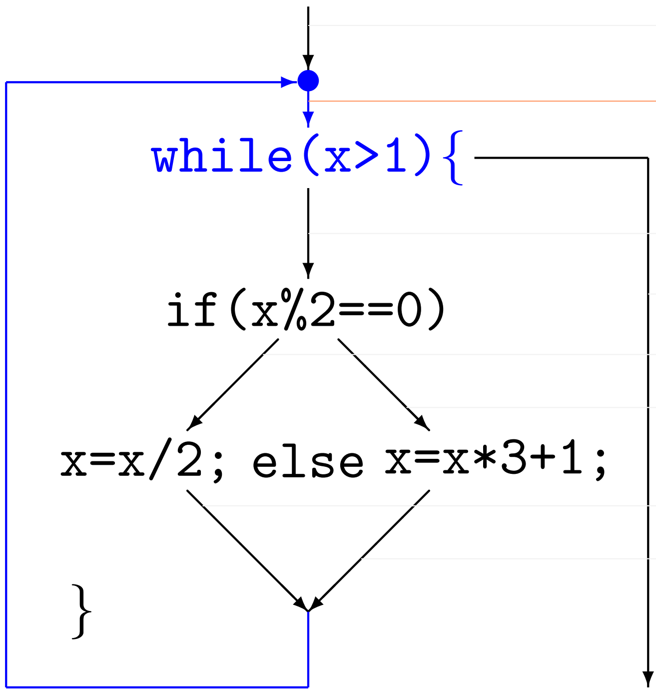
$$H = \{3 \cdot n + 1 \mid n \in F\}$$

Beispiel mit Widening



	neu: $\Phi^{10}(\bot)$	alt: $\Phi^{9}(\bot)$
A :		$[1\ldots5]$
B :		$[1\ldots\infty]$
C :		$[2\ldots\infty]$
D :		$[1\ldots1]$
E :		$[2\ldots\infty]$
F :		$[3\ldots\infty]$
G :		$[1\ldots\infty]$
H :		$[10\ldots\infty]$

Beispiel mit Widening

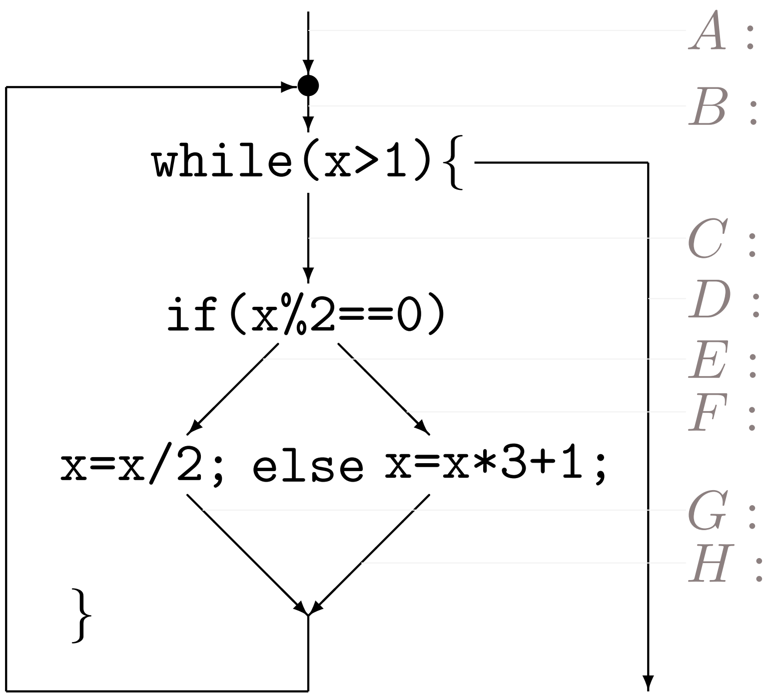


	neu: $\Phi^{10}(\bot)$	alt: $\Phi^{9}(\bot)$
A :	$[1 \ldots 5]$	$[1 \ldots 5]$
B :	$[1 \ldots \infty]$	$[1 \ldots \infty]$
C :	$[2 \ldots \infty]$	$[2 \ldots \infty]$
D :	$[1 \ldots 1]$	$[1 \ldots 1]$
E :	$[2 \ldots \infty]$	$[2 \ldots \infty]$
F :	$[3 \ldots \infty]$	$[3 \ldots \infty]$
G :	$[1 \ldots \infty]$	$[1 \ldots \infty]$
H :	$[10 \ldots \infty]$	$[10 \ldots \infty]$

$$B = A \cup G \cup H$$

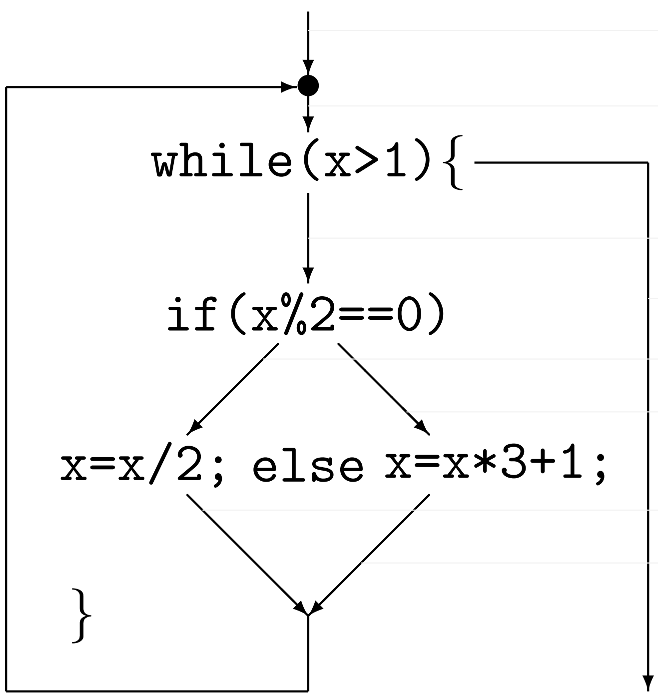
Beispiel mit Widening

neu: alt:



Beispiel mit Widening

neu: $\Phi^{\sharp}(\bot)$ alt: $\Phi^{\sharp}(\bot)$

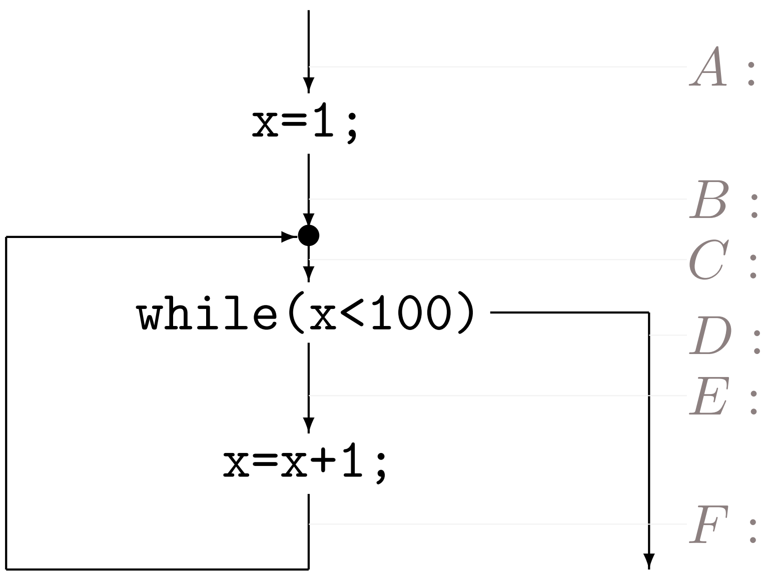


	neu	alt
A	$[1 \ldots 5]$	$[1 \ldots 5]$
B	$[1 \ldots \infty]$	$[1 \ldots \infty]$
C	$[2 \ldots \infty]$	$[2 \ldots \infty]$
D	$[1 \ldots 1]$	$[1 \ldots 1]$
E	$[2 \ldots \infty]$	$[2 \ldots \infty]$
F	$[3 \ldots \infty]$	$[3 \ldots \infty]$
G	$[1 \ldots \infty]$	$[1 \ldots \infty]$
H	$[10 \ldots \infty]$	$[10 \ldots \infty]$

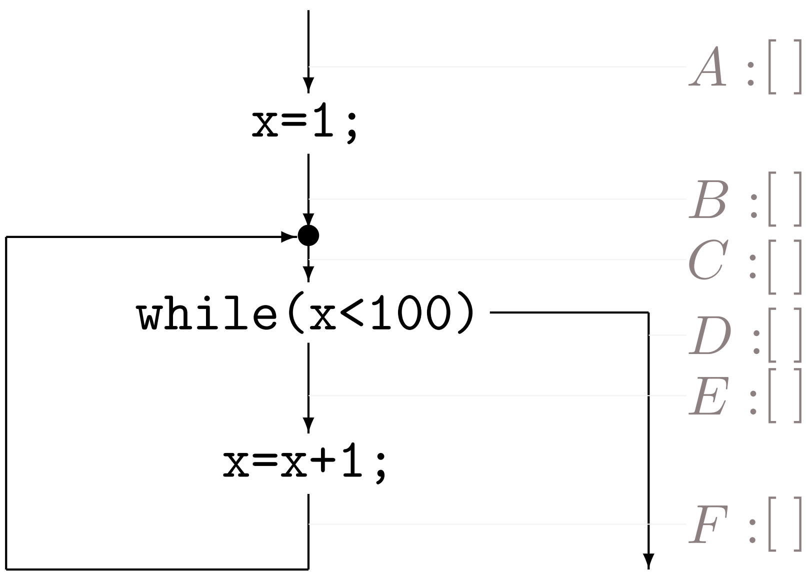
Fixpunkt erreicht

$$E = C \cap \{\ldots, -2, 0, 2, 4, \ldots\}$$
$$F = C \cap \{\ldots, -1, 1, 3, \ldots\}$$

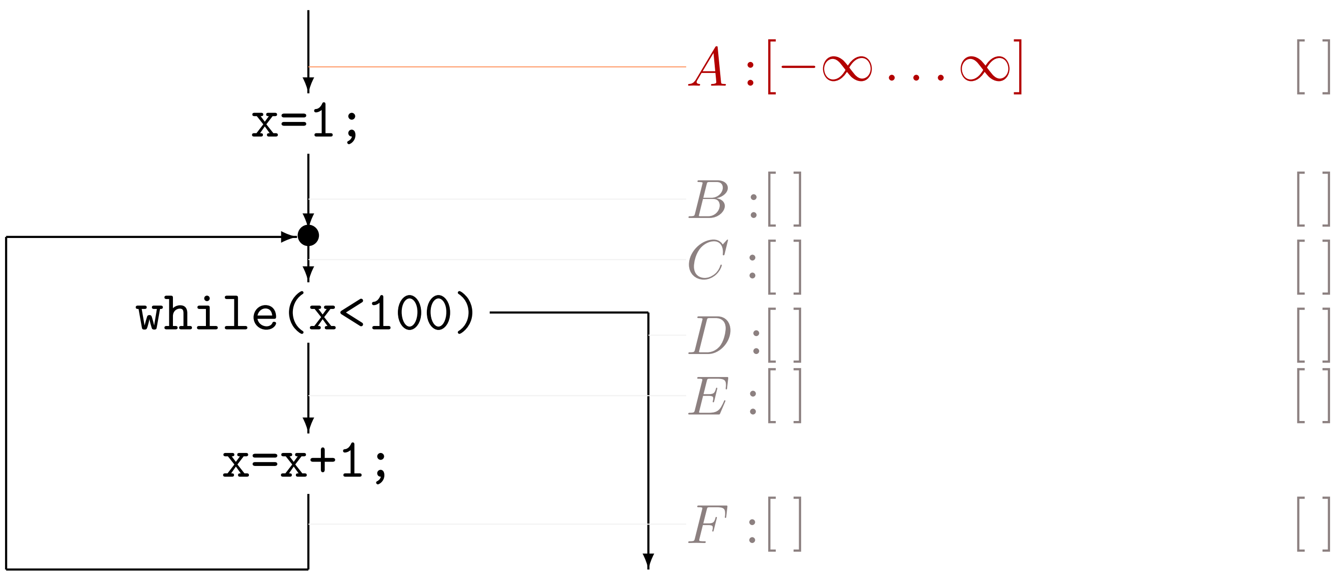
Genauigkeitsverlust durch Widening



Genauigkeitsverlust durch Widening

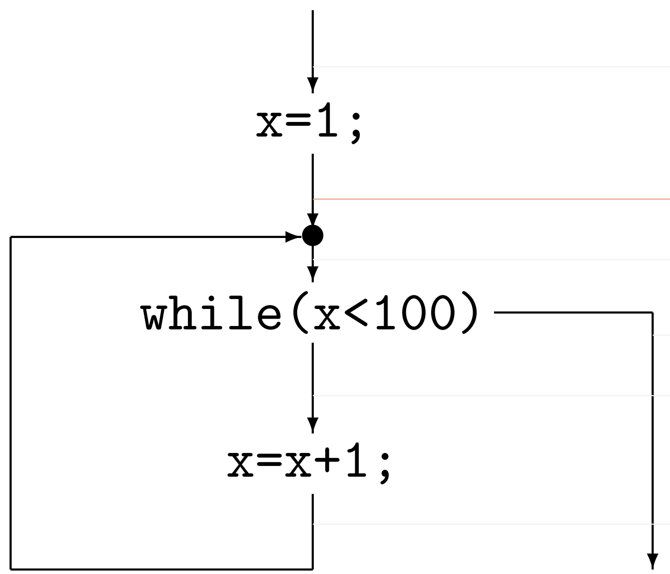


Genauigkeitsverlust durch Widening



$$A = [-\infty \ldots \infty]$$

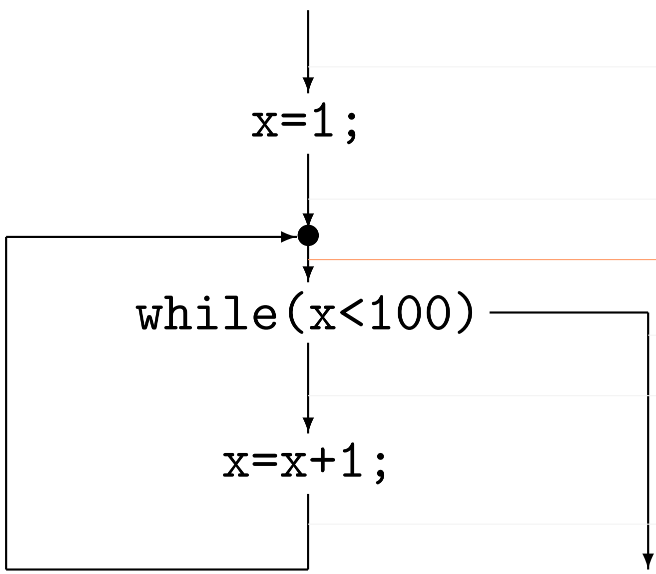
Genauigkeitsverlust durch Widening



$A : [-\infty \ldots \infty]$	$[-\infty \ldots \infty]$
$B : [1 \ldots 1]$	$[\,]$
$C : [\,]$	$[\,]$
$D : [\,]$	$[\,]$
$E : [\,]$	$[\,]$
$F : [\,]$	$[\,]$

$$B = [1 \ldots 1]$$

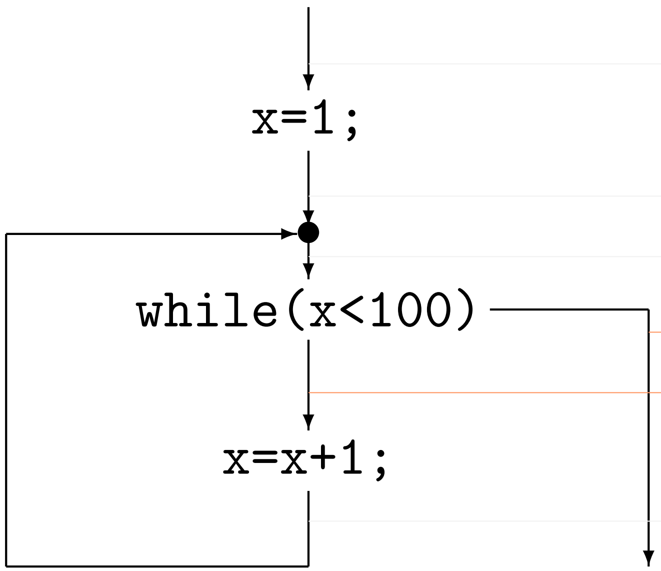
Genauigkeitsverlust durch Widening



A	$:[-\infty \ldots \infty]$	$[-\infty \ldots \infty]$
B	$:[1 \ldots 1]$	$[1 \ldots 1]$
C	$:[1 \ldots 1]$	$[\,]$
D	$:[\,]$	$[\,]$
E	$:[\,]$	$[\,]$
F	$:[\,]$	$[\,]$

$$C = B \cup F$$

Genauigkeitsverlust durch Widening

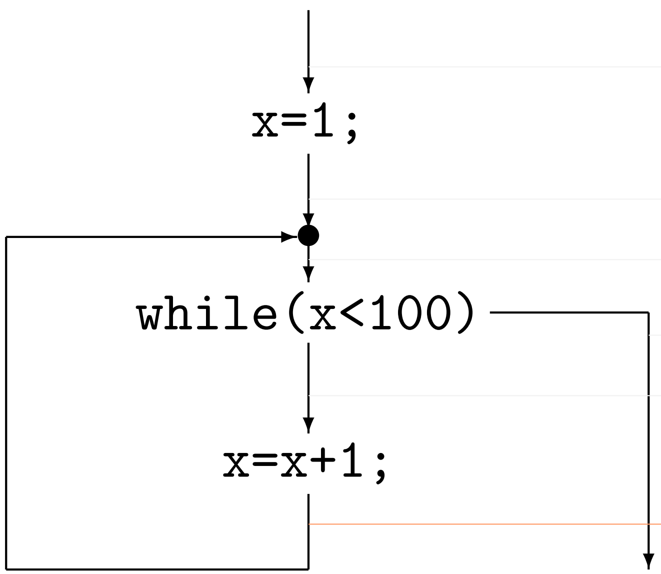


A :	$[-\infty \ldots \infty]$	$[-\infty \ldots \infty]$
B :	$[1 \ldots 1]$	$[1 \ldots 1]$
C :	$[1 \ldots 1]$	$[1 \ldots 1]$
D :	$[\,]$	$[\,]$
E :	$[1 \ldots 1]$	$[\,]$
F :	$[\,]$	$[\,]$

$$D = C \cap [100 \ldots \infty]$$

$$E = C \cap [-\infty \ldots 99]$$

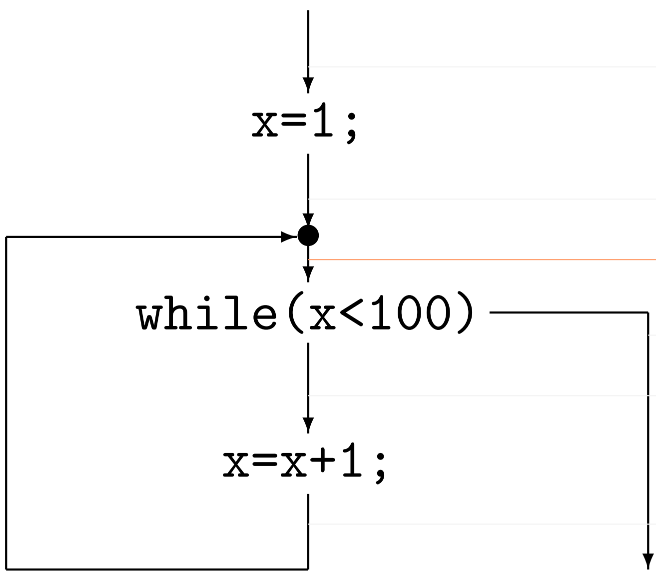
Genauigkeitsverlust durch Widening



A :	$[-\infty \ldots \infty]$	$[-\infty \ldots \infty]$
B :	$[1 \ldots 1]$	$[1 \ldots 1]$
C :	$[1 \ldots 1]$	$[1 \ldots 1]$
D :	$[\,]$	$[\,]$
E :	$[1 \ldots 1]$	$[1 \ldots 1]$
F :	$[2 \ldots 2]$	$[\,]$

$$F = \{n + 1 \mid n \in E\}$$

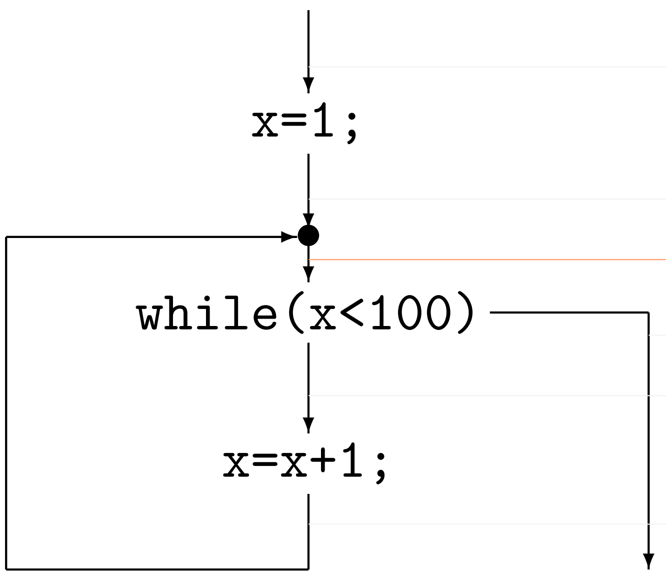
Genauigkeitsverlust durch Widening



A	$:[-\infty \ldots \infty]$	$[-\infty \ldots \infty]$
B	$:[1 \ldots 1]$	$[1 \ldots 1]$
C	$:[1 \ldots 2]$	$[1 \ldots 1]$
D	$:[\,]$	$[\,]$
E	$:[1 \ldots 1]$	$[1 \ldots 1]$
F	$:[2 \ldots 2]$	$[2 \ldots 2]$

$$C = B \cup F$$

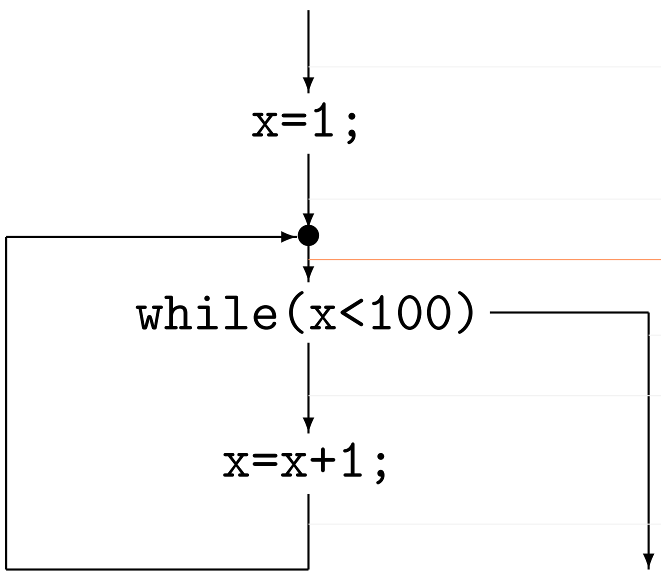
Genauigkeitsverlust durch Widening



A	$:[-\infty \ldots \infty]$	$[-\infty \ldots \infty]$
B	$:[1 \ldots 1]$	$[1 \ldots 1]$
C	$:[1 \ldots 2]$	$[1 \ldots 1]$
D	$:[\,]$	$[\,]$
E	$:[1 \ldots 1]$	$[1 \ldots 1]$
F	$:[2 \ldots 2]$	$[2 \ldots 2]$

$$[1 \ldots 1] \triangledown [1 \ldots 2] = [1 \ldots \infty]$$

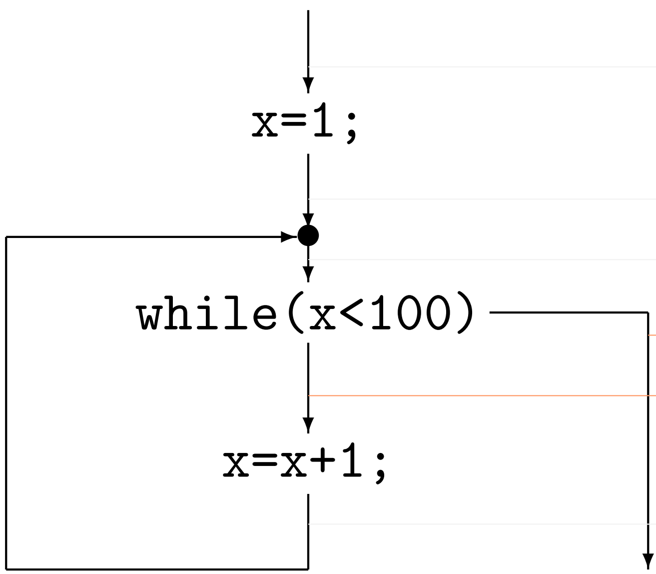
Genauigkeitsverlust durch Widening



A	$:[-\infty \ldots \infty]$	$[-\infty \ldots \infty]$
B	$:[1 \ldots 1]$	$[1 \ldots 1]$
C	$:[1 \ldots \infty]$	$[1 \ldots 1]$
D	$:[\,]$	$[\,]$
E	$:[1 \ldots 1]$	$[1 \ldots 1]$
F	$:[2 \ldots 2]$	$[2 \ldots 2]$

$$[1 \ldots 1] \,\nabla\, [1 \ldots 2] = [1 \ldots \infty]$$

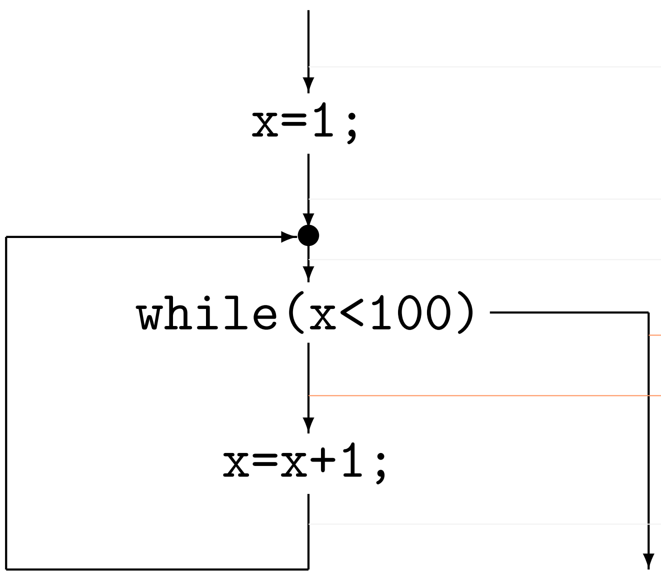
Genauigkeitsverlust durch Widening



A :	$[-\infty \ldots \infty]$	$[-\infty \ldots \infty]$
B :	$[1 \ldots 1]$	$[1 \ldots 1]$
C :	$[1 \ldots \infty]$	$[1 \ldots \infty]$
D :	$[100 \ldots \infty]$	$[\,]$
E :	$[1 \ldots 99]$	$[1 \ldots 1]$
F :	$[2 \ldots 2]$	$[2 \ldots 2]$

$$D = C \cap [100 \ldots \infty]$$
$$E = C \cap [-\infty \ldots 99]$$

Genauigkeitsverlust durch Widening

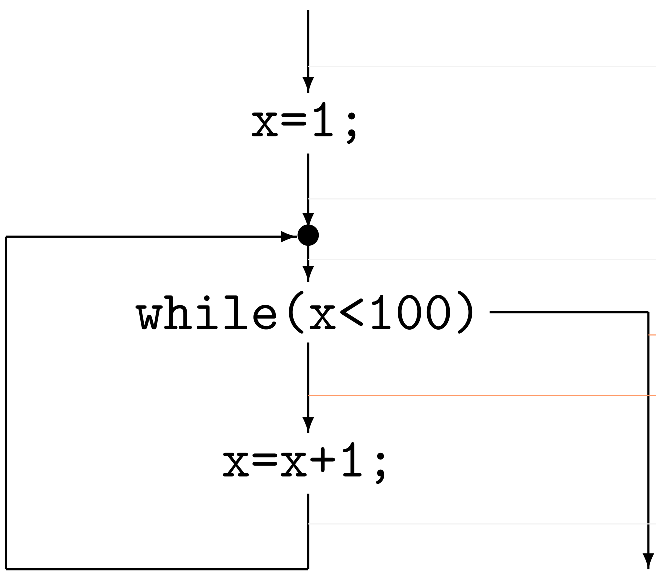


A	$[-\infty \ldots \infty]$	$[-\infty \ldots \infty]$
B	$[1 \ldots 1]$	$[1 \ldots 1]$
C	$[1 \ldots \infty]$	$[1 \ldots \infty]$
D	$[100 \ldots \infty]$	$[\,]$
E	$[1 \ldots 99]$	$[1 \ldots 1]$
F	$[2 \ldots 2]$	$[2 \ldots 2]$

$$[\,]\,\nabla\,[100 \ldots \infty] = [100 \ldots \infty]$$

$$[1 \ldots 1]\,\nabla\,[1 \ldots 99] = [1 \ldots \infty]$$

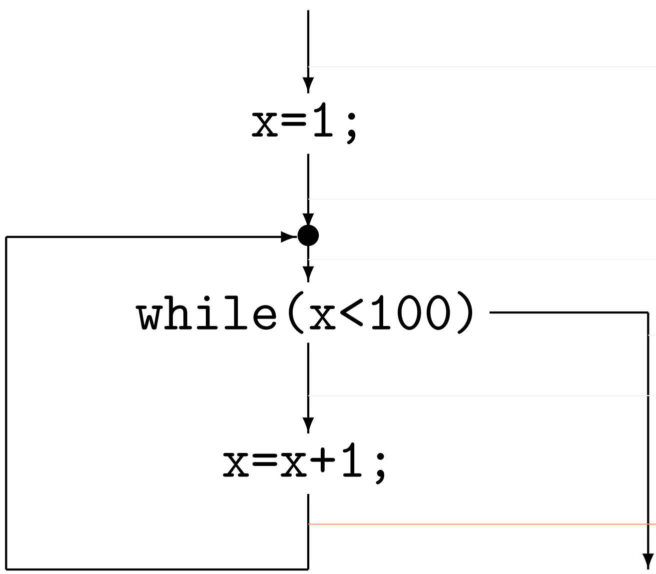
Genauigkeitsverlust durch Widening



A :	$[-\infty \ldots \infty]$	$[-\infty \ldots \infty]$
B :	$[1 \ldots 1]$	$[1 \ldots 1]$
C :	$[1 \ldots \infty]$	$[1 \ldots \infty]$
D :	$[100 \ldots \infty]$	$[\,]$
E :	$[1 \ldots \infty]$	$[1 \ldots 1]$
F :	$[2 \ldots 2]$	$[2 \ldots 2]$

$$[\,] \triangledown [100 \ldots \infty] = [100 \ldots \infty]$$
$$[1 \ldots 1] \triangledown [1 \ldots 99] = [1 \ldots \infty]$$

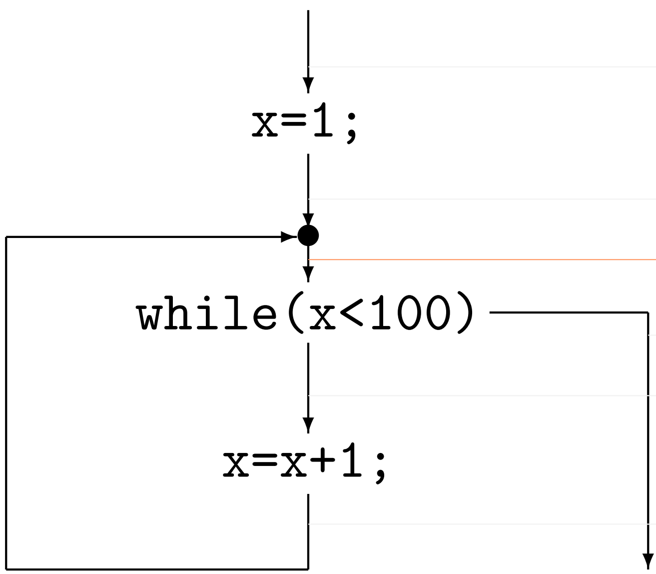
Genauigkeitsverlust durch Widening



$A : [-\infty \ldots \infty]$	$[-\infty \ldots \infty]$
$B : [1 \ldots 1]$	$[1 \ldots 1]$
$C : [1 \ldots \infty]$	$[1 \ldots \infty]$
$D : [100 \ldots \infty]$	$[100 \ldots \infty]$
$E : [1 \ldots \infty]$	$[1 \ldots \infty]$
$F : [2 \ldots \infty]$	$[2 \ldots 2]$

$$F = \{n + 1 \mid n \in E\}$$

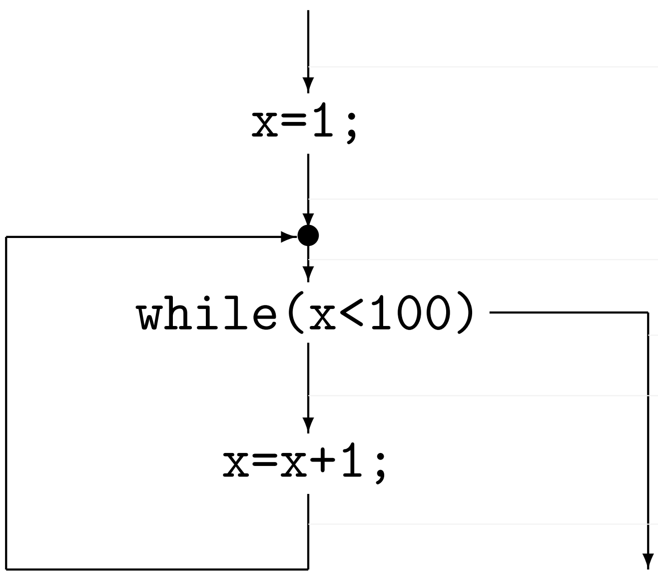
Genauigkeitsverlust durch Widening



$A: [-\infty \ldots \infty]$	$[-\infty \ldots \infty]$
$B: [1 \ldots 1]$	$[1 \ldots 1]$
$C: [1 \ldots \infty]$	$[1 \ldots \infty]$
$D: [100 \ldots \infty]$	$[100 \ldots \infty]$
$E: [1 \ldots \infty]$	$[1 \ldots \infty]$
$F: [2 \ldots \infty]$	$[2 \ldots \infty]$

$$C = B \cup F$$

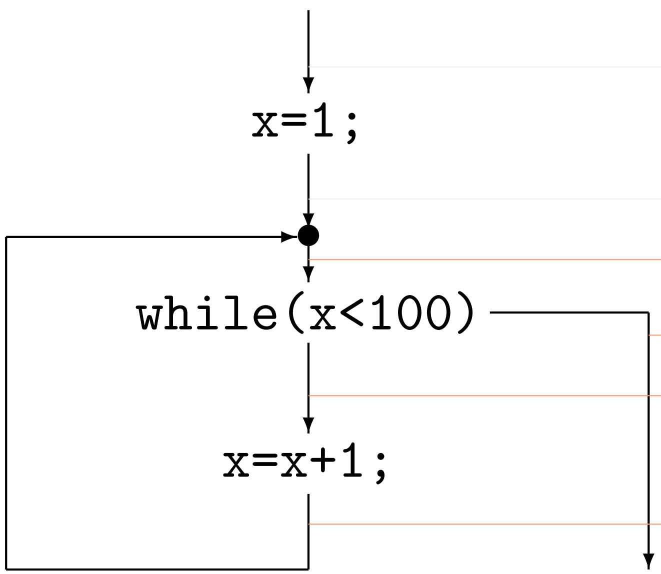
Genauigkeitsverlust durch Widening



A	$[-\infty \ldots \infty]$	$[-\infty \ldots \infty]$
B	$[1 \ldots 1]$	$[1 \ldots 1]$
C	$[1 \ldots \infty]$	$[1 \ldots \infty]$
D	$[100 \ldots \infty]$	$[100 \ldots \infty]$
E	$[1 \ldots \infty]$	$[1 \ldots \infty]$
F	$[2 \ldots \infty]$	$[2 \ldots \infty]$

Fixpunkt erreicht

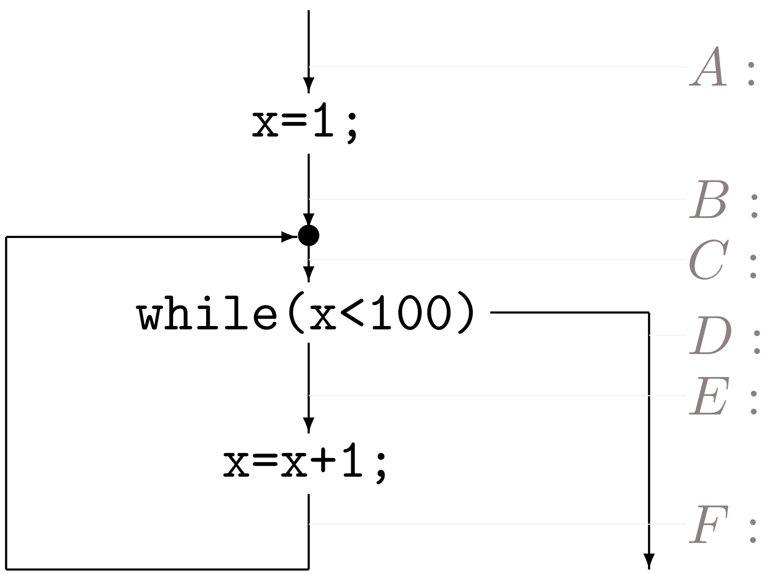
Genauigkeitsverlust durch Widening



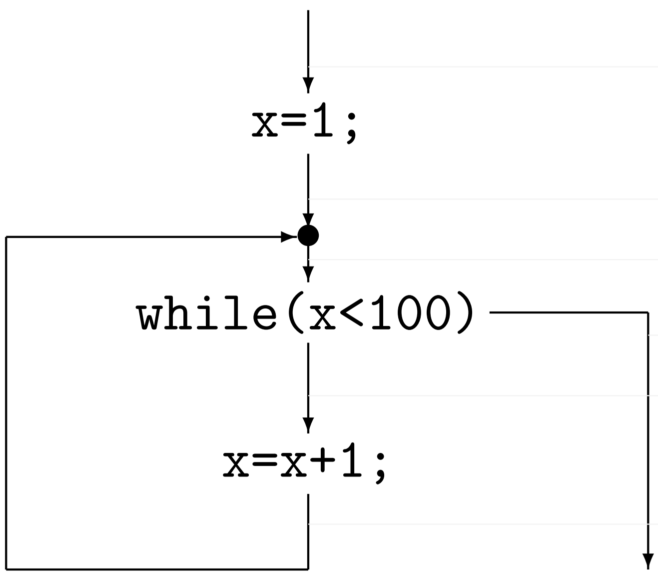
A	$:[-\infty \ldots \infty]$	$[-\infty \ldots \infty]$
B	$:[1 \ldots 1]$	$[1 \ldots 1]$
C	$:[1 \ldots \infty]$	$[1 \ldots \infty]$
D	$:[100 \ldots \infty]$	$[100 \ldots \infty]$
E	$:[1 \ldots \infty]$	$[1 \ldots \infty]$
F	$:[2 \ldots \infty]$	$[2 \ldots \infty]$

Fixpunkt erreicht, aber zu grob

Genauigkeitsverlust durch Widening



Genauigkeitsverlust durch Widening



A :	$[-\infty \dots \infty]$	$[-\infty \dots \infty]$
B :	$[1 \dots 1]$	$[1 \dots 1]$
C :	$[1 \dots \infty]$	$[1 \dots \infty]$
D :	$[100 \dots \infty]$	$[100 \dots \infty]$
E :	$[1 \dots 99]$	$[1 \dots 99]$
F :	$[2 \dots \infty]$	$[2 \dots \infty]$

Fixpunkt erreicht, aber zu grob

$C = C \,\nabla\, (B \sqcup F) = [1 \dots \infty]$; $D = C \sqcap [100 \dots \infty]$

$E = C \sqcap [-\infty \dots 99] = [1 \dots 99]$

Genauigkeitssteigerung durch nachgeschaltetes Narrowing

Sei $\vartriangle : M' \times M' \longrightarrow M'$ eine Operation,
so daß $y' \sqsubseteq' x' \vartriangle y' \sqsubseteq' x'$ für alle $y' \sqsubseteq' x'$ gilt, und
so daß für jede

absteigende Kette	x'_1	$\sqsupseteq'$	x'_2	$\sqsupseteq'$	$\ldots$	$\sqsupseteq'$	x'_i	$\sqsupseteq'$	$\ldots$
die Kette	x'_1	$\sqsupseteq'$	$x'_1 \vartriangle x'_2$	$\sqsupseteq'$	$\ldots$	$\sqsupseteq'$	$x'_1 \vartriangle \ldots \vartriangle x'_i$	$\sqsupseteq'$	$\ldots$

irgendwann stationär wird.

Definiere $\Phi'''(x') = x' \vartriangle \Phi'(x')$.

Dann ist die Kette $X'' \sqsupseteq' \Phi'''(X'') \sqsupseteq' \Phi'''(\Phi'''(X'')) \sqsupseteq' \ldots \sqsupseteq' \Phi'''^{i}(X'') \sqsupseteq' \ldots$
irgendwann stationär und ihre größte untere Schranke
$X''' = \prod'\{X'', \Phi'''(X''), \Phi'''(\Phi'''(X'')), \ldots\}$ ist immer noch eine obere
Abschätzung für den kleinsten Fixpunkt X' von Φ'.

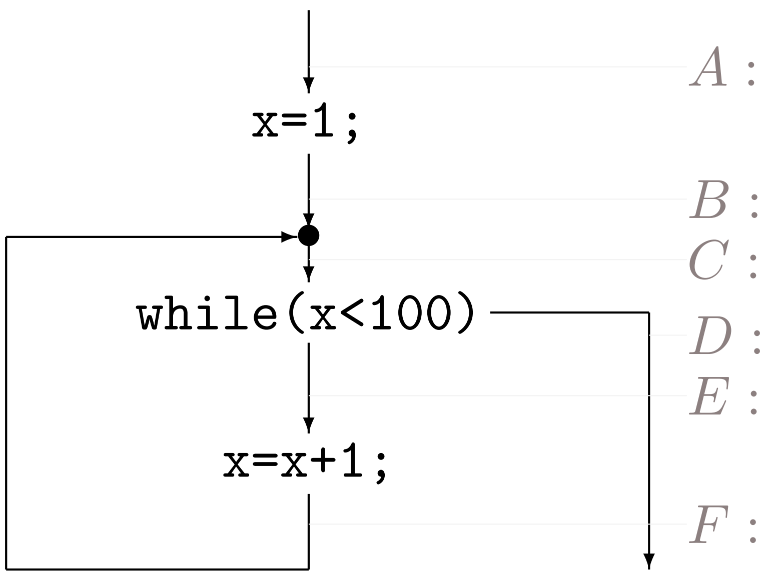
Beispiel mit nachgeschaltetem Narrowing

Definiere eine norrowing-Operation auf Intervallen durch
$[l \dots u] \vartriangle [\,] = [\,] \vartriangle [l \dots u] = [l \dots u]$ sowie $[l_1 \dots u_1] \vartriangle [l_2 \dots u_2] = [l \dots u]$ mit
$l = \begin{cases} l_2 & \text{für} \quad l_1 = -\infty \\ l_1 & \text{sonst} \end{cases}$ und $u = \begin{cases} u_2 & \text{für} \quad u_1 = +\infty \\ u_1 & \text{sonst} \end{cases}$

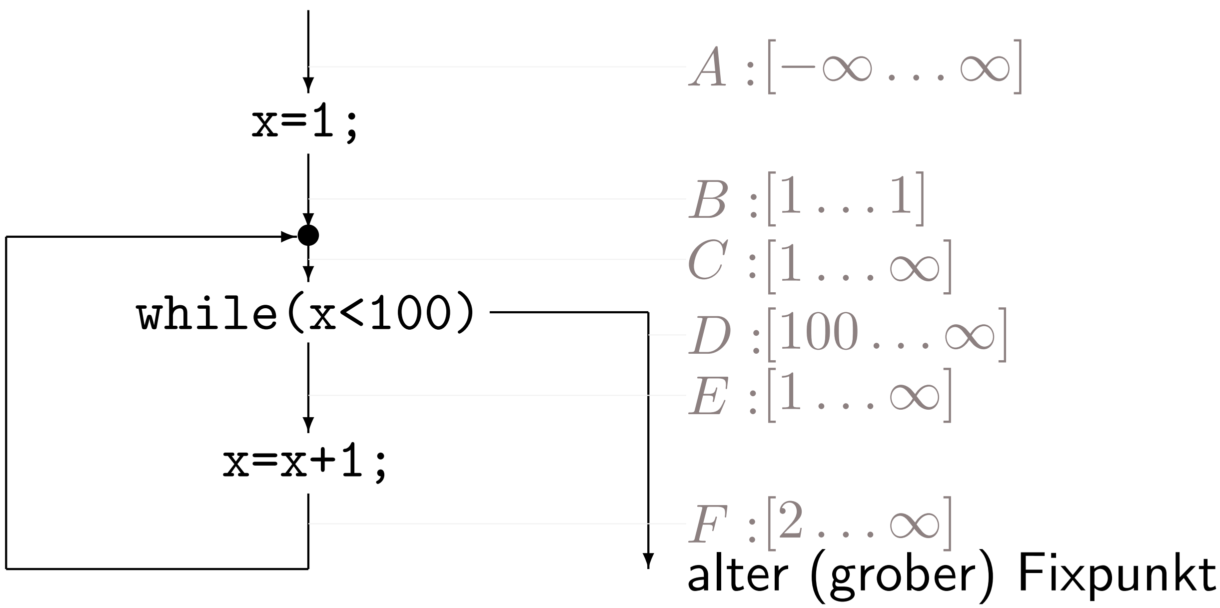
Anschaulich: Schlechteste Intervallgrenzen werden durch neue Werte ersetzt.

Z.B.
$[1 \dots \infty] \vartriangle [1 \dots 16] = [1 \dots 16]$,
$[1 \dots 16] \vartriangle [1 \dots \infty] = [1 \dots 16]$.
$[1 \dots 16] \vartriangle [1 \dots 17] = [1 \dots 16]$.

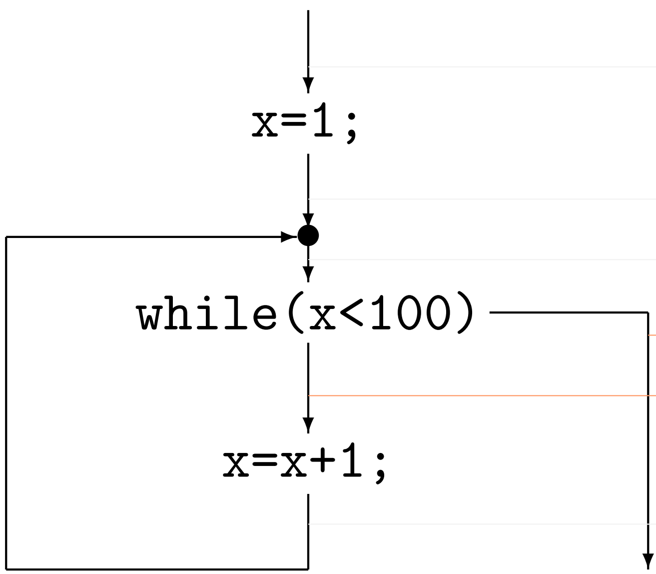
Beispiel mit nachgeschaltetem Narrowing



Beispiel mit nachgeschaltetem Narrowing



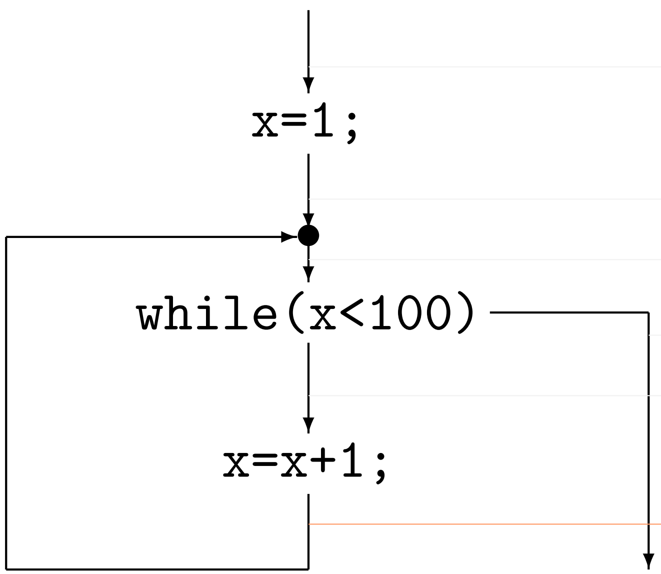
Beispiel mit nachgeschaltetem Narrowing



A :	$[-\infty \ldots \infty]$	$[-\infty \ldots \infty]$
B :	$[1 \ldots 1]$	$[1 \ldots 1]$
C :	$[1 \ldots \infty]$	$[1 \ldots \infty]$
D :	$[100 \ldots \infty]$	$[100 \ldots \infty]$
E :	$[1 \ldots 99]$	$[1 \ldots \infty]$
F :	$[2 \ldots \infty]$	$[2 \ldots \infty]$

$$D = C \cap [100 \ldots \infty]$$
$$E = C \cap [-\infty \ldots 99]$$

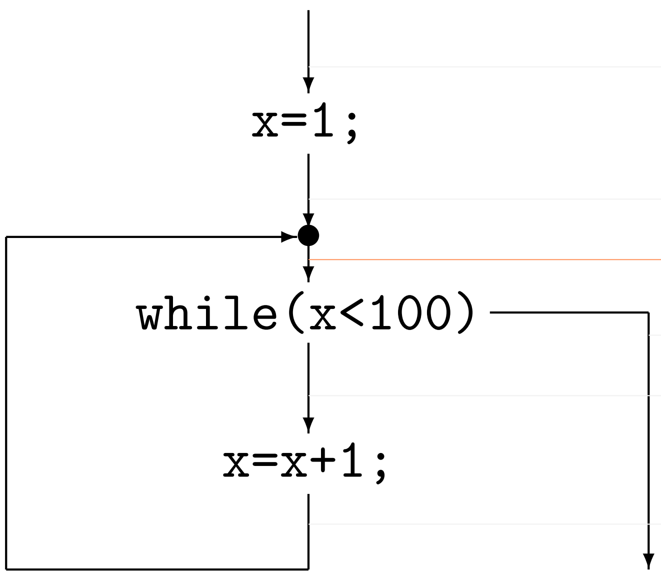
Beispiel mit nachgeschaltetem Narrowing



A	$[-\infty \ldots \infty]$	$[-\infty \ldots \infty]$
B	$[1 \ldots 1]$	$[1 \ldots 1]$
C	$[1 \ldots \infty]$	$[1 \ldots \infty]$
D	$[100 \ldots \infty]$	$[100 \ldots \infty]$
E	$[1 \ldots 99]$	$[1 \ldots 99]$
F	$[2 \ldots 100]$	$[2 \ldots \infty]$

$$F = \{n + 1 \mid n \in E\}$$

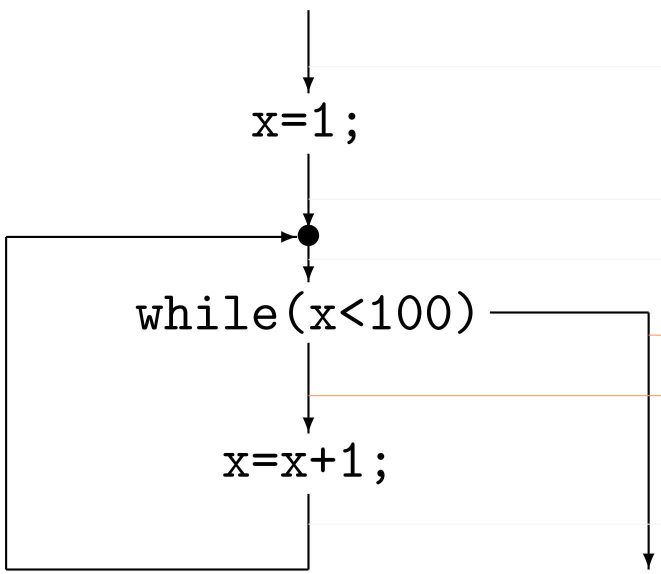
Beispiel mit nachgeschaltetem Narrowing



A	$:[-\infty \ldots \infty]$	$[-\infty \ldots \infty]$
B	$:[1 \ldots 1]$	$[1 \ldots 1]$
C	$:[1 \ldots 100]$	$[1 \ldots \infty]$
D	$:[100 \ldots \infty]$	$[100 \ldots \infty]$
E	$:[1 \ldots 99]$	$[1 \ldots 99]$
F	$:[2 \ldots 100]$	$[2 \ldots 100]$

$$C = B \cup F$$

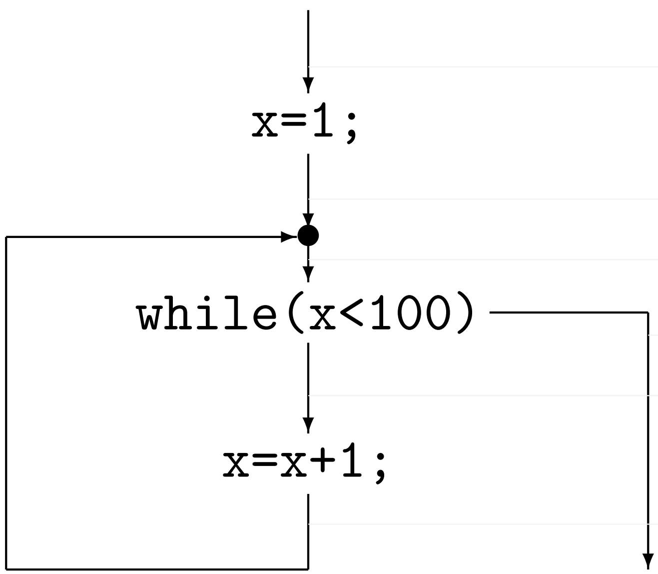
Beispiel mit nachgeschaltetem Narrowing



A :	$[-\infty \ldots \infty]$	$[-\infty \ldots \infty]$
B :	$[1 \ldots 1]$	$[1 \ldots 1]$
C :	$[1 \ldots 100]$	$[1 \ldots 100]$
D :	$[100 \ldots 100]$	$[100 \ldots \infty]$
E :	$[1 \ldots 99]$	$[1 \ldots 99]$
F :	$[2 \ldots 100]$	$[2 \ldots 100]$

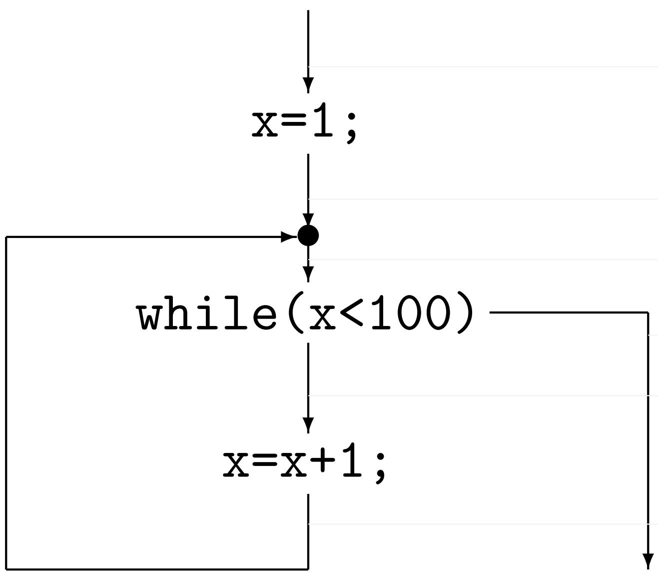
$$D = C \cap [100 \ldots \infty]$$
$$E = C \cap [-\infty \ldots 99]$$

Beispiel mit nachgeschaltetem Narrowing



A	$:[-\infty \dots \infty]$	$[-\infty \dots \infty]$
B	$:[1 \dots 1]$	$[1 \dots 1]$
C	$:[1 \dots 100]$	$[1 \dots 100]$
D	$:[100 \dots 100]$	$[100 \dots 100]$
E	$:[1 \dots 99]$	$[1 \dots 99]$
F	$:[2 \dots 100]$	$[2 \dots 100]$

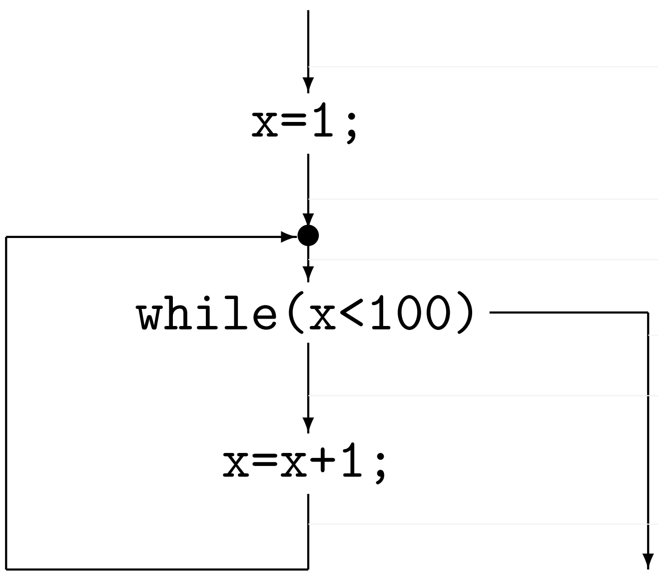
Beispiel mit nachgeschaltetem Narrowing



A	$:[-\infty \ldots \infty]$	$[-\infty \ldots \infty]$
B	$:[1 \ldots 1]$	$[1 \ldots 1]$
C	$:[1 \ldots 100]$	$[1 \ldots 100]$
D	$:[100 \ldots 100]$	$[100 \ldots 100]$
E	$:[1 \ldots 99]$	$[1 \ldots 99]$
F	$:[2 \ldots 100]$	$[2 \ldots 100]$

neuer (genauerer) Fixpunkt erreicht

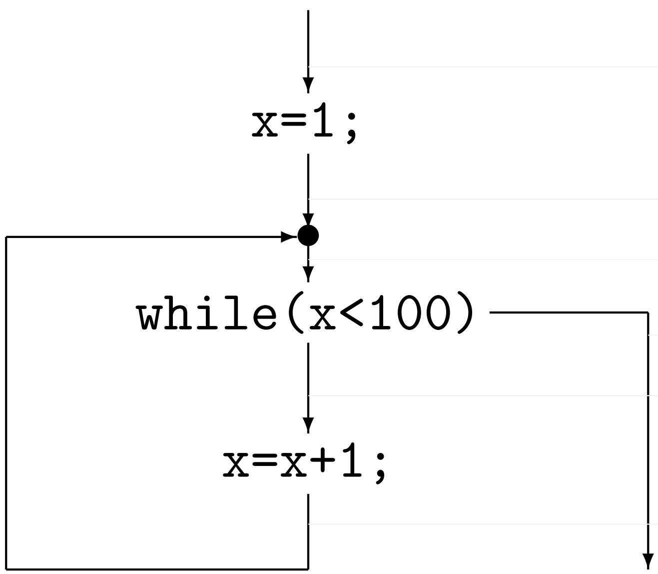
Beispiel mit nachgeschaltetem Narrowing



A	$:[-\infty \ldots \infty]$	$[-\infty \ldots \infty]$
B	$:[1 \ldots 1]$	$[1 \ldots 1]$
C	$:[1 \ldots 100]$	$[1 \ldots 100]$
D	$:[100 \ldots 100]$	$[100 \ldots 100]$
E	$:[1 \ldots 99]$	$[1 \ldots 99]$
F	$:[2 \ldots 100]$	$[2 \ldots 100]$

Schleifeninvariante automatisch berechnet

Beispiel mit nachgeschaltetem Narrowing



$A:$

$B:$

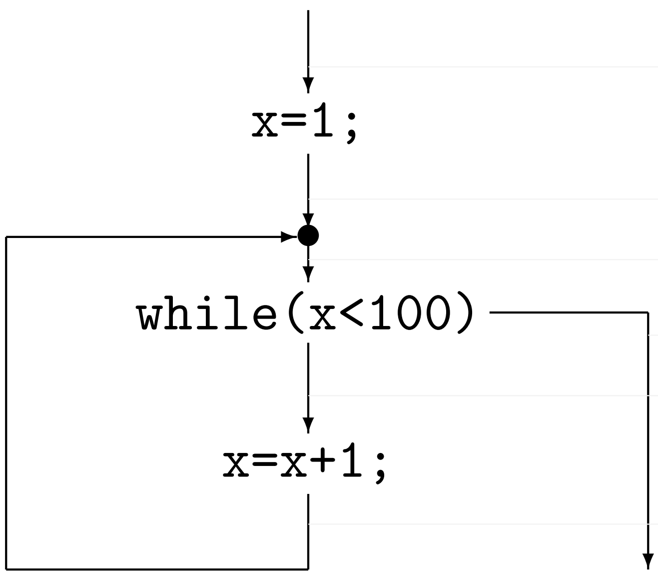
$C:$

$D:$

$E:$

$F:$

Beispiel mit nachgeschaltetem Narrowing



$A : [-\infty \ldots \infty]$	$A : [-\infty \ldots \infty]$
$B : [1 \ldots 1]$	$B : [1 \ldots 1]$
$C : [1 \ldots 100]$ / $[1 \ldots \infty]$	$C : [1 \ldots 100]$ / $[1 \ldots \infty]$
$D : [100 \ldots 100]$ / $[100 \ldots \infty]$	$D : [100 \ldots 100]$ / $[100 \ldots \infty]$
$E : [1 \ldots 99]$ / $[1 \ldots \infty]$	$E : [1 \ldots 99]$ / $[1 \ldots \infty]$
$F : [2 \ldots 100]$ / $[2 \ldots \infty]$	$F : [2 \ldots 100]$ / $[2 \ldots \infty]$

Erster (grober) Fixpunkt erreicht

Schleifeninvariante automatisch berechnet

$D = C \sqcap [100 \ldots \infty]$

$E = C \sqcap [-\infty \ldots 99]$

Widening und Narrowing: Übersicht

Konkreter Verband — Abstrakter Verband

$$\begin{array}{rccl}
 & \gamma(X'') & \xleftarrow{\gamma} & X'' = \bigsqcup'_n \Phi''^n(\bot') \\
 & | & & | \\
 & \gamma(X''') & \xleftarrow{\gamma} & X''' = \bigsqcup'_n \Phi'''^n(X'') \\
 & | & & | \\
 & \gamma(X') & \xleftarrow{\gamma} & X' = \bigsqcup'_n \Phi'^n(\bot') \\
 & | & & \\
\bigsqcup_n \Phi^n(\bot) = & X & &
\end{array}$$

Widening
$\Phi''(x') = x' \triangledown \Phi'(x')$ für . . .

Narrowing
$\Phi'''(x') = x' \vartriangle \Phi'(x')$

Abstrakte Interpretation
$\Phi'(x') \sqsupseteq' \alpha(\Phi(\gamma(x')))$

Collecting Semantics
Φ aus Programm

Anforderungen: Aussagekraft

Die abstrakten Mengen sollen genügend präzise sein, um die (benutzergegebenen) Eigenschaften an den Programmpunkten entscheiden zu können.

Ein Indiz für zusätzliche Ungenauigkeit ist das Auftreten von Abschätzungen bei der Berechnung von Φ' aus Φ.

Manchmal kann dann der abstrakte Verband so erweitert werden $^{(*)}$, daß genügend Information für eine genaueres Φ' zur Verfügung steht.

$^{(*)}$ durch Bildung kartesischer Produkte aus bekannten Einzelverbänden

Beispiel

$\mathbb{Z}$

$[-\infty, \infty], \{0, 1\}$

```
if(x>0)
```

↙ ↘

then		else
$\{1, 2, 3, ...\}$		$\{..., \text{-}2, \text{-}1, 0\}$
$[1, \infty], \{0, 1\}$		$[-\infty, 0], \{0, 1\}$
`x=2*x+1;`	else	`x=1-4*x;`
$\{3, 5, 7, ...\}$		$\{1, 3, 5, ...\}$
$[3, \infty], \{1\}$		$[1, \infty], \{1\}$

↘ ↙

$\{1, 3, 5, ...\}$

$[1, \infty], \{1\}$

```
x=8/(x%2);
```

- Abstrakter Verband: nur Intervalle
  - Information über Rest mod. 2 geht verloren
  - Nulldivision scheint möglich
- Abstrakter Verband: zusätzlich Reste mod. 2 (kartesisches Produkt)
  - Φ' für `then`- und `else`-Anweisung präziser
  - Nulldivision ausgeschlossen

Aussagekraft

Für die praktische Anwendung der abstrakten Interpretation ist es hinderlich, wenn für jedes zu analysierende Programm zuerst ein eigener abstrakter Verband ausgewählt und ein eigenes Φ' berechnet werden muß.

Das Werkzeug PolySpace, das von Cousot-Schülern entwickelt wurde, arbeitet vorwiegend mit dem Verband der n-dimensionalen Polyeder (s.u.).

Bei `int`-Variablen wird, soweit möglich, zusätzlich Restklasseninformation mitgeführt (rationale Kongruenzen, s.u.).

Polyeder-Verband

Der Polyeder-Verband ergibt sich als Verallgemeinerung des Intervall-Verbands auf mehrere Variablen.

Ein Element im Polyeder-Verband wird dargestellt durch eine Konjunktion linearer Ungleichungen.

Dadurch lassen sich lineare Abhängigkeiten zwischen Variablen noch berücksichtigen.

(In den Beispielen treten nur zwei Variablen auf, um eine geometrische Veranschaulichung zu ermöglichen.
Im allgemeinen Fall wird mit n-dimensionalen Polyedern gerechnet.)

Polyeder-Verband: Beispiel

```
x=80-2*y;
```

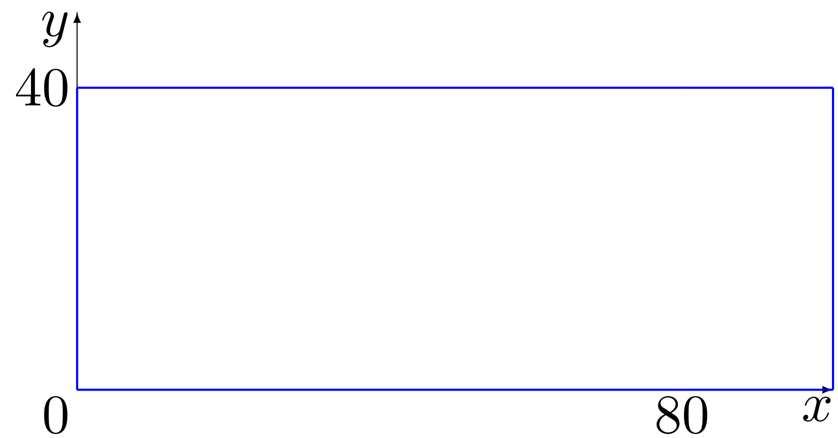
```
y=80/(x+y);
```

Polyeder-Verband: Beispiel

$x \in [0, 99] \wedge y \in [0, 40]$

```
x=80-2*y;
```

```
y=80/(x+y);
```



Im kartesischen Produkt aus zwei Intervallverbänden lassen sich nur Rechtecke darstellen.

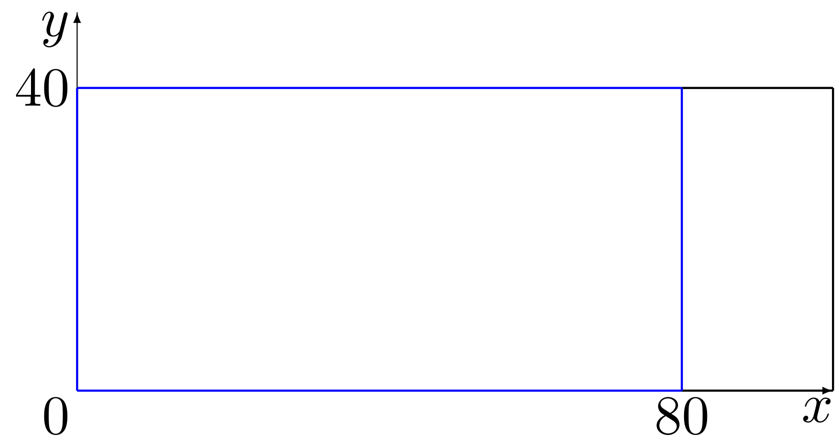
Polyeder-Verband: Beispiel

$x \in [0, 99] \wedge y \in [0, 40]$

```
x=80-2*y;
```

$x \in [0, 80] \wedge y \in [0, 40]$

```
y=80/(x+y);
```



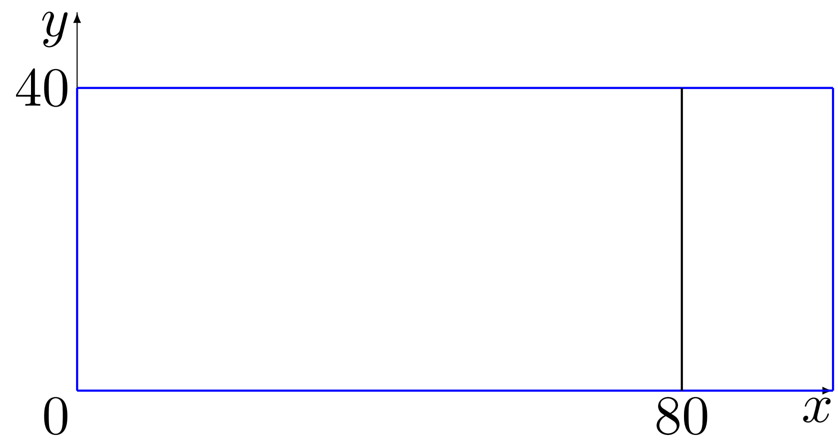
Im kartesischen Produkt aus zwei Intervallverbänden lassen sich nur Rechtecke darstellen.

Das Ergebnis der Zuweisung `x=80-2*y;` muß durch ein 80×40-Rechteck approximiert werden.

Polyeder-Verband: Beispiel

$x \in [0, 99] \wedge y \in [0, 40]$
$\{0 \leq x \leq 99 \wedge 0 \leq y \leq 40\}$
`x=80-2*y;`
$x \in [0, 80] \wedge y \in [0, 40]$

`y=80/(x+y);`

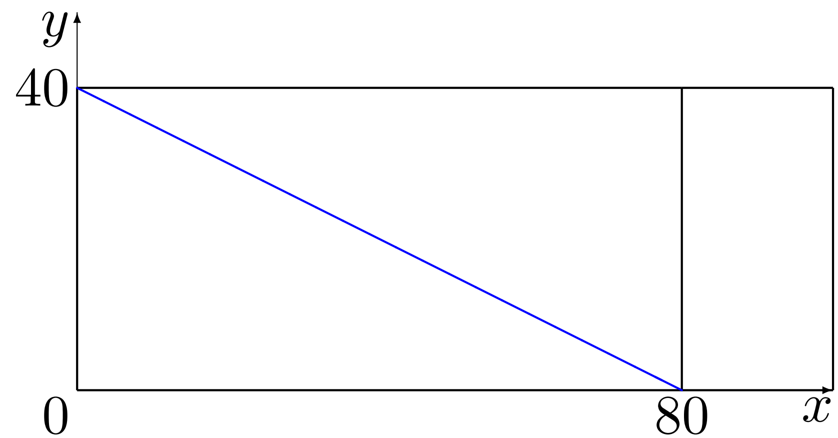


Im kartesischen Produkt aus zwei Intervallverbänden lassen sich nur Rechtecke darstellen.
Das Ergebnis der Zuweisung `x=80-2*y;` muß durch ein 80×40-Rechteck approximiert werden.

Im Polyeder-Verband können beliebige konvexe n-Ecke dargestellt werden.

Polyeder-Verband: Beispiel

$x \in [0, 99] \wedge y \in [0, 40]$
$\{0 \leq x \leq 99 \wedge 0 \leq y \leq 40\}$
```
x=80-2*y;
```
$x \in [0, 80] \wedge y \in [0, 40]$
$\{x = 80 - 2y \wedge 0 \leq y \leq 40\}$
```
y=80/(x+y);
```

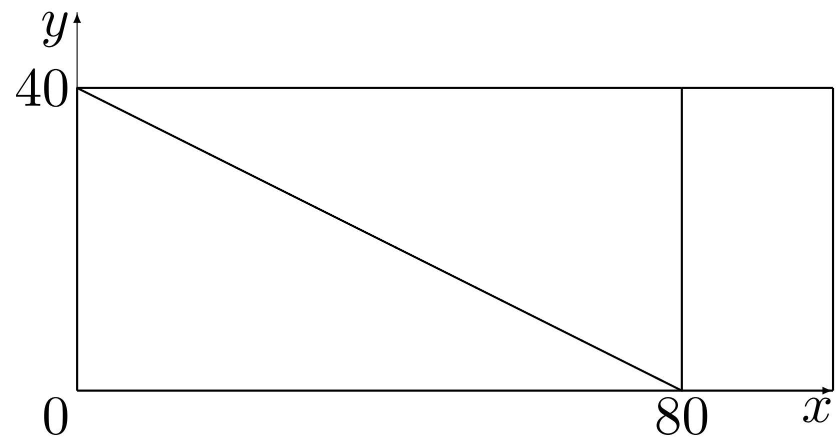


Im kartesischen Produkt aus zwei Intervallverbänden lassen sich nur Rechtecke darstellen.
Das Ergebnis der Zuweisung `x=80-2*y;` muß durch ein 80×40-Rechteck approximiert werden.

Im Polyeder-Verband können beliebige konvexe n-Ecke dargestellt werden.
Das Zuweisungsergebnis kann durch eine Linie exakt wiedergegeben werden.

Polyeder-Verband: Beispiel

$x \in [0, 99] \wedge y \in [0, 40]$
$\{0 \leq x \leq 99 \wedge 0 \leq y \leq 40\}$
```
x=80-2*y;
```
$x \in [0, 80] \wedge y \in [0, 40]$
$\{x = 80 - 2y \wedge 0 \leq y \leq 40\}$
```
y=80/(x+y);
```

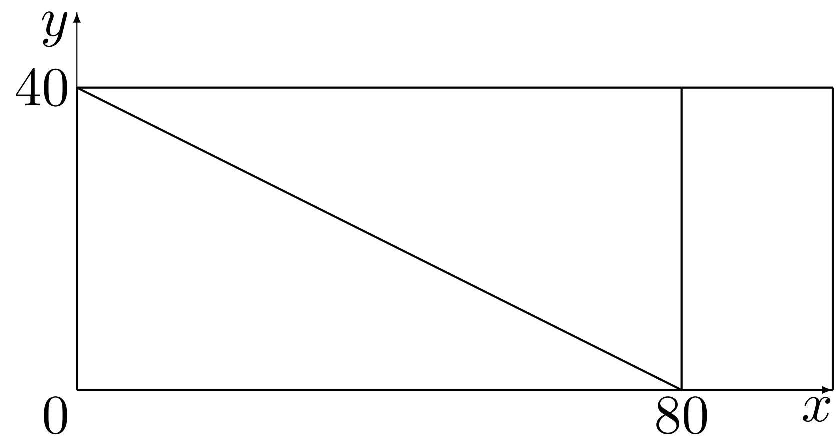


Im kartesischen Produkt aus zwei Intervallverbänden lassen sich nur Rechtecke darstellen.
Das Ergebnis der Zuweisung `x=80-2*y;` muß durch ein 80×40-Rechteck approximiert werden.

Im Polyeder-Verband können beliebige konvexe n-Ecke dargestellt werden.
Das Zuweisungsergebnis kann durch eine Linie exakt wiedergegeben werden.
Eine Nulldivision in der folgenden Zuweisung kann damit ausgeschlossen werden.

Polyeder-Verband: Beispiel

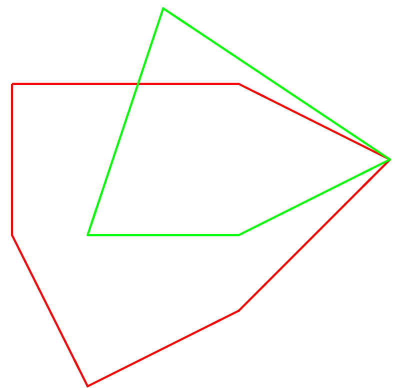
$x \in [0, 99] \wedge y \in [0, 40]$
$\{0 \leq x \leq 99 \wedge 0 \leq y \leq 40\}$
`x=80-2*y;`
$x \in [0, 80] \wedge y \in [0, 40]$
$\{x = 80 - 2y \wedge 0 \leq y \leq 40\}$
`y=80/(x+y);`



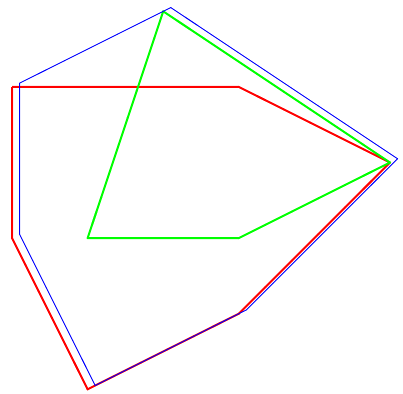
Im kartesischen Produkt aus zwei Intervallverbänden lassen sich nur Rechtecke darstellen.
Das Ergebnis der Zuweisung `x=80-2*y;` muß durch ein 80×40-Rechteck approximiert werden.

Im Polyeder-Verband können beliebige konvexe n-Ecke dargestellt werden.
Das Zuweisungsergebnis kann durch eine Linie exakt wiedergegeben werden.
Eine Nulldivision in der folgenden Zuweisung kann damit ausgeschlossen werden.

Polyeder-Verband: Verbandsoperationen

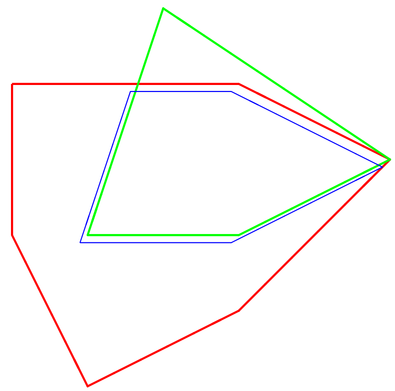


Polyeder-Verband: Verbandsoperationen



Die größte obere Schranke zweier Polyeder ist die konvexe Hülle ihrer Vereinigung.

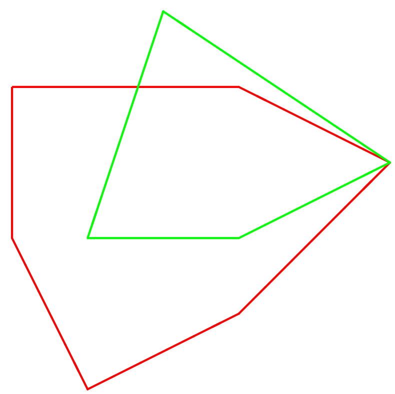
Polyeder-Verband: Verbandsoperationen



Die größte obere Schranke zweier Polyeder ist die konvexe Hülle ihrer Vereinigung.

Die kleinste untere Schranke ist ihr Durchschnitt; er ist stets bereits konvex.

Polyeder-Verband: Verbandsoperationen

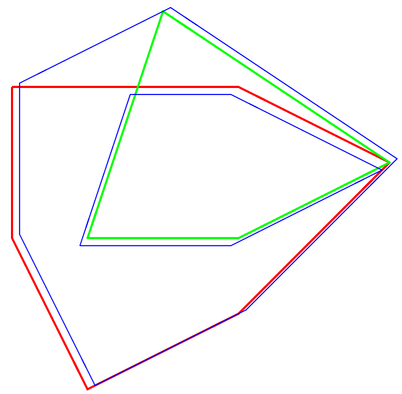


Die größte obere Schranke zweier Polyeder ist die konvexe Hülle ihrer Vereinigung.

Die kleinste untere Schranke ist ihr Durchschnitt; er ist stets bereits konvex.

Durchschnitt und konvexe Hülle der Vereinigung werden mit Hilfe geometrischer Algorithmen als neue Konjunktionen linearer Ungleichungen berechnet.

Polyeder-Verband: Verbandsoperationen



Die größte obere Schranke zweier Polyeder ist die konvexe Hülle ihrer Vereinigung.

Die kleinste untere Schranke ist ihr Durchschnitt; er ist stets bereits konvex.

Durchschnitt und konvexe Hülle der Vereinigung werden mit Hilfe geometrischer Algorithmen als neue Konjunktionen linearer Ungleichungen berechnet.

Polyeder-Verband: Analysebeispiel

```
i=2;
j=0;
while (...) {
        {2j + 2 ≤ i ∧ 0 ≤ j}
        if (...) {
                i=i+4;
                {2j + 6 ≤ i ∧ 0 ≤ j}
        } else {
                i=i+2;
                j=j+1;
                {2j + 2 ≤ i ∧ 1 ≤ j}
        }
        {2j + 2 ≤ i ∧ 6 ≤ i + 2j ∧ 0 ≤ j}
}
```

Verband der Rationalen Kongruenzen

Verband der rationalen Kongruenzen: $\{\bot, \top\} \cup (\mathbb{Q} \times \mathbb{Q})$,

wobei $\langle p, q\rangle \in \mathbb{Q} \times \mathbb{Q}$ intuitiv für $\{p + k \cdot q \mid k \in \mathbb{Z}\} = \gamma(\langle p, q\rangle)$ steht.

Z.B.

$$\begin{array}{lcl}
\gamma(\langle 1.0, 10\rangle) & = & \{\ldots, \text{-19},\ \text{-9},\ 1,\ 11,\ 21,\ 31, \ldots\} \\
\gamma(\langle 0.5, 1.0\rangle) & = & \{\ldots, \text{-1.5},\ \text{-0.5},\ 0.5,\ 1.5,\ 2.5, \ldots\} \\
\gamma(\langle 0.0, 0.1\rangle) & = & \{\ldots, \text{-0.2},\ \text{-0.1},\ 0,\ 0.1,\ 0.2,\ 0.3, \ldots\}
\end{array}$$

Dieser Verband ist unendlich groß und erfüllt nicht die ACC-Bedingung, so daß mit Widening und Narrowing gearbeitet werden muß.

Das Gleiche gilt für den Polyeder-Verband.

Cousot, Cousot 1992 gibt für jeden der beiden Verbände ein geeignetes Widening und Narrowing an.

Statische Analyse mit PolySpace

(Werbefolien für Industriekunden)

- Code wird analysiert, nicht ausgeführt
- prüft minimale semantische Kriterien
  (z.B. NULL–Pointer–Zugriffe)
- vollautomatisch, Rechenzeit im Stundenbereich

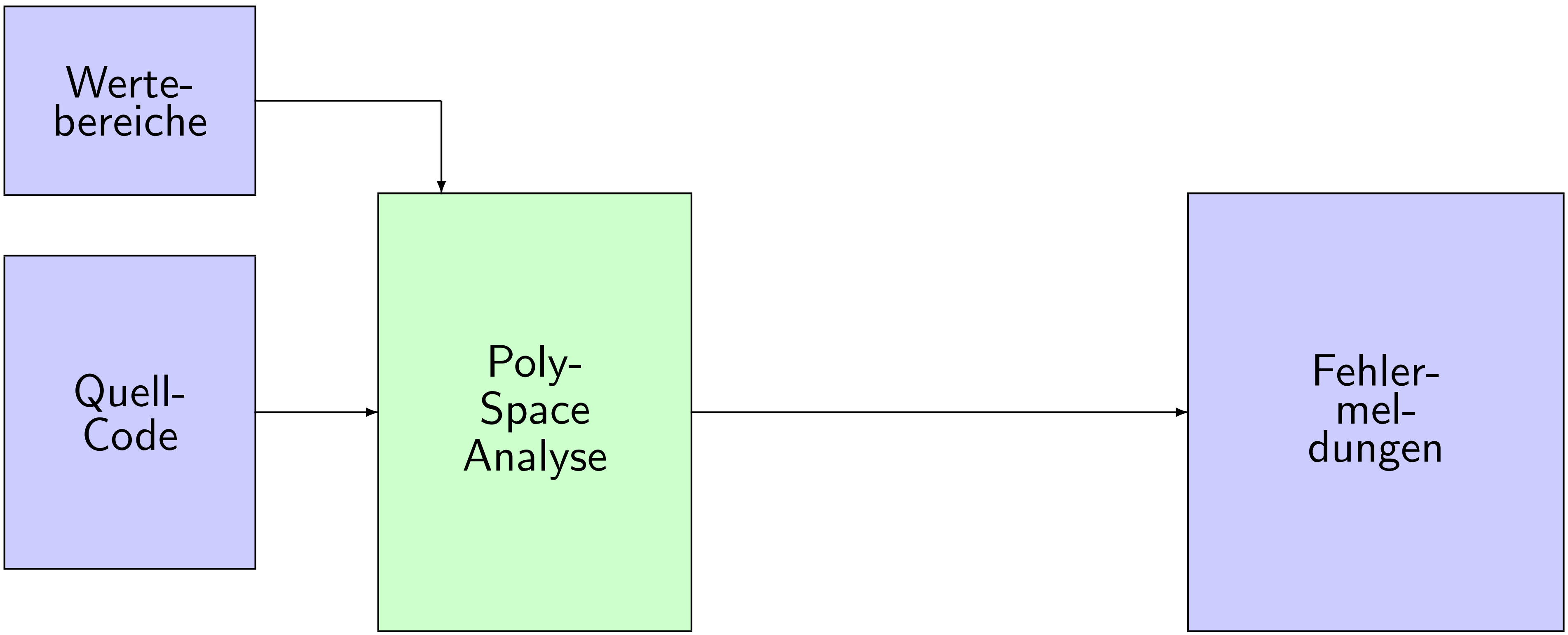
Statische Analyse

- unabhängig von Programm–Funktionalität
- benötigt keine Anforderungsspezifikation
- Aufwand und Nutzen zwischen Compiler und Test
- führt zu robusterem Code

Statische Analyse

- Grundlage: Wertebereichsanalyse
- an ca. 0.1% der Codestellen Fehler gefunden
- an ca. 10% der Codestellen Fehler nur vermutet
- manuelle Nachkontrolle unabhängig von Entwicklern

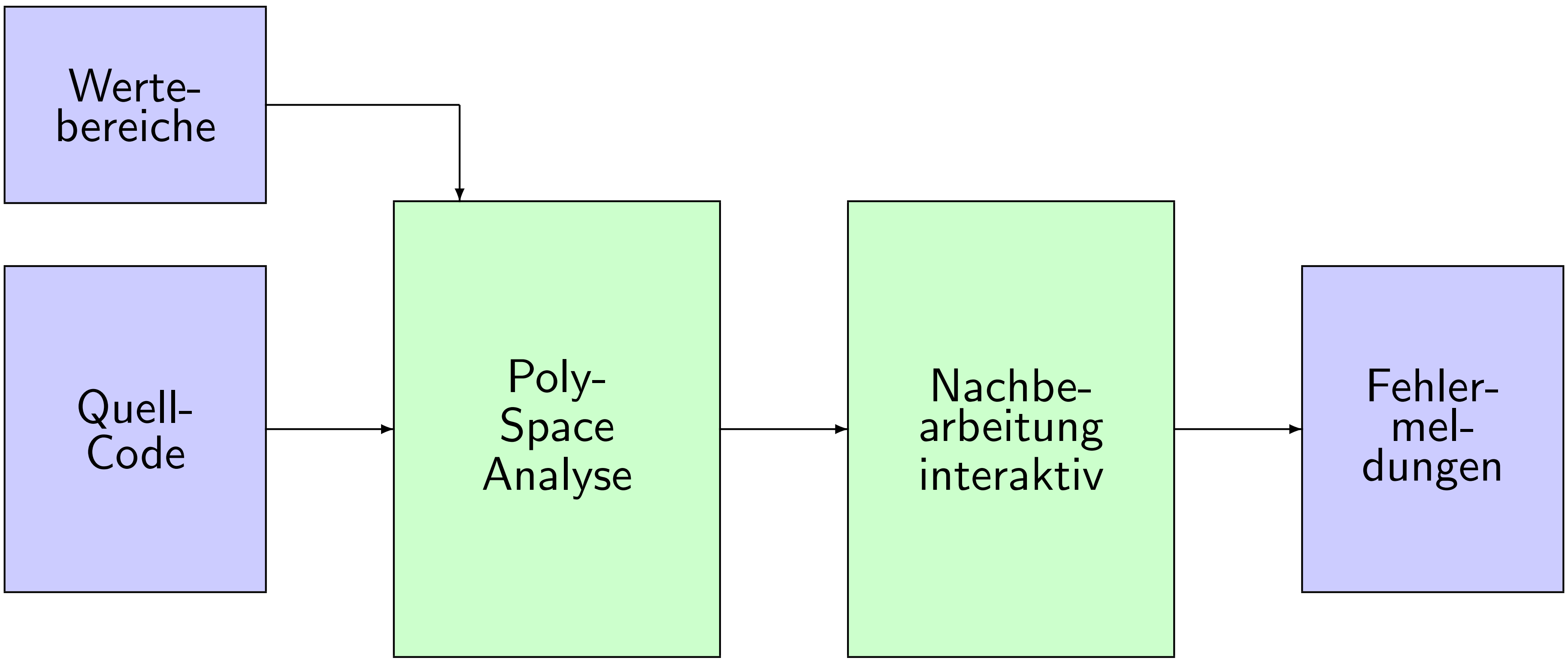
Vorgehen



20000 loc

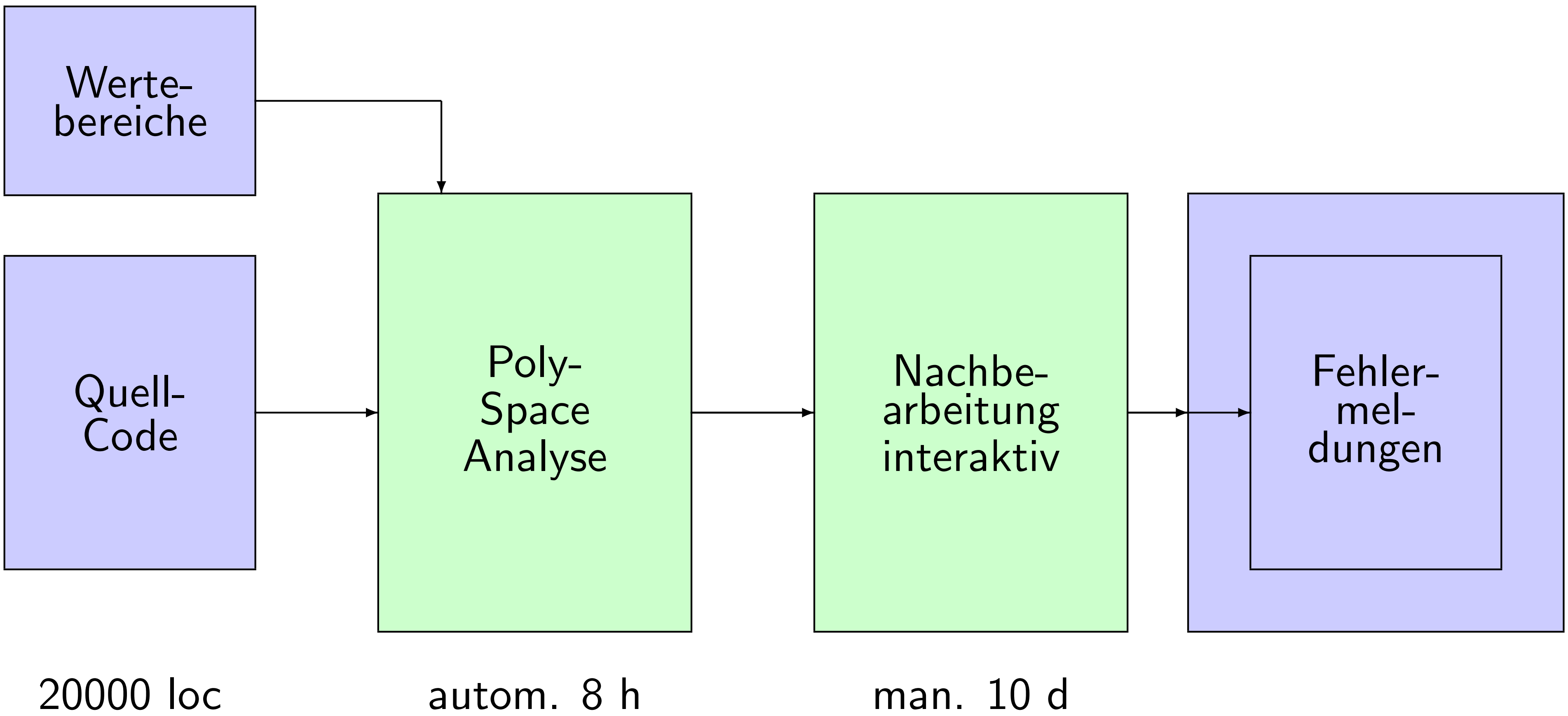
autom. 8 h

Vorgehen



20000 loc   autom. 8 h   man. 10 d

Vorgehen



Werte-bereiche
Quell-Code
Poly-Space Analyse
Nachbe-arbeitung interaktiv
Fehler-mel-dungen
20000 loc
autom. 8 h
man. 10 d

Untersuchte Fehlerarten

- Uninitialisierte Variablen
- Zugriff über ungültigen Zeiger
- Unerreichbarer Code
- Wertebereichsüberlauf
- Indexüberlauf
- Nulldivision
- Endlosschleife
- Endlosrekursion

Indexüberlauf — sicher

```
int a[10];

...

for (i=0; i<10; ++i)
    a[i] = a[i+1];
```

Indexüberlauf — sicher

```
int a[10];

...

for (i=0; i<10; ++i)
    a[i] = a[i+1];
```

$\longleftarrow$ index out of bounds !

Indexüberlauf — sicher

```
int a[10];

...

for (i=0; i<10; ++i)
    a[i] = a[i+1];
```

Indexüberlauf — sicher

```
int a[10];

...

for (i=0; i<10; ++i)
    a[i] = a[i+1];
```

Indexüberlauf — vermutet

```
int a[10];

...

for (i=0; a[i]>0; ++i)
    a[i] = a[i+1];
```

Indexüberlauf — vermutet

```
int a[10];

...

for (i=0; a[i]>0; ++i)
    a[i] = a[i+1];
```

⟵ index out of bounds ?

← ⟵ index out of bounds ?

Indexüberlauf — vermutet

```
int a[10];

...

for (i=0; a[i]>0; ++i)
    a[i] = a[i+1];
```

$\longleftarrow$ index out of bounds ?

$\leftarrow \longleftarrow$ index out of bounds ?

- Manuelle Nachkontrolle notwendig

Indexüberlauf — vermutet

```
int a[10];

...

for (i=0; a[i]>0; ++i)
    a[i] = a[i+1];
```

$\longleftarrow$ index out of bounds ?

$\leftarrow \longleftarrow$ index out of bounds ?

- Manuelle Nachkontrolle notwendig
- Programmablauf muß lokal verstanden werden

Indexüberlauf — vermutet

```
int a[10];

...

for (i=0; a[i]>0; ++i)
    a[i] = a[i+1];
```

- Manuelle Nachkontrolle notwendig
- Programmablauf muß lokal verstanden werden

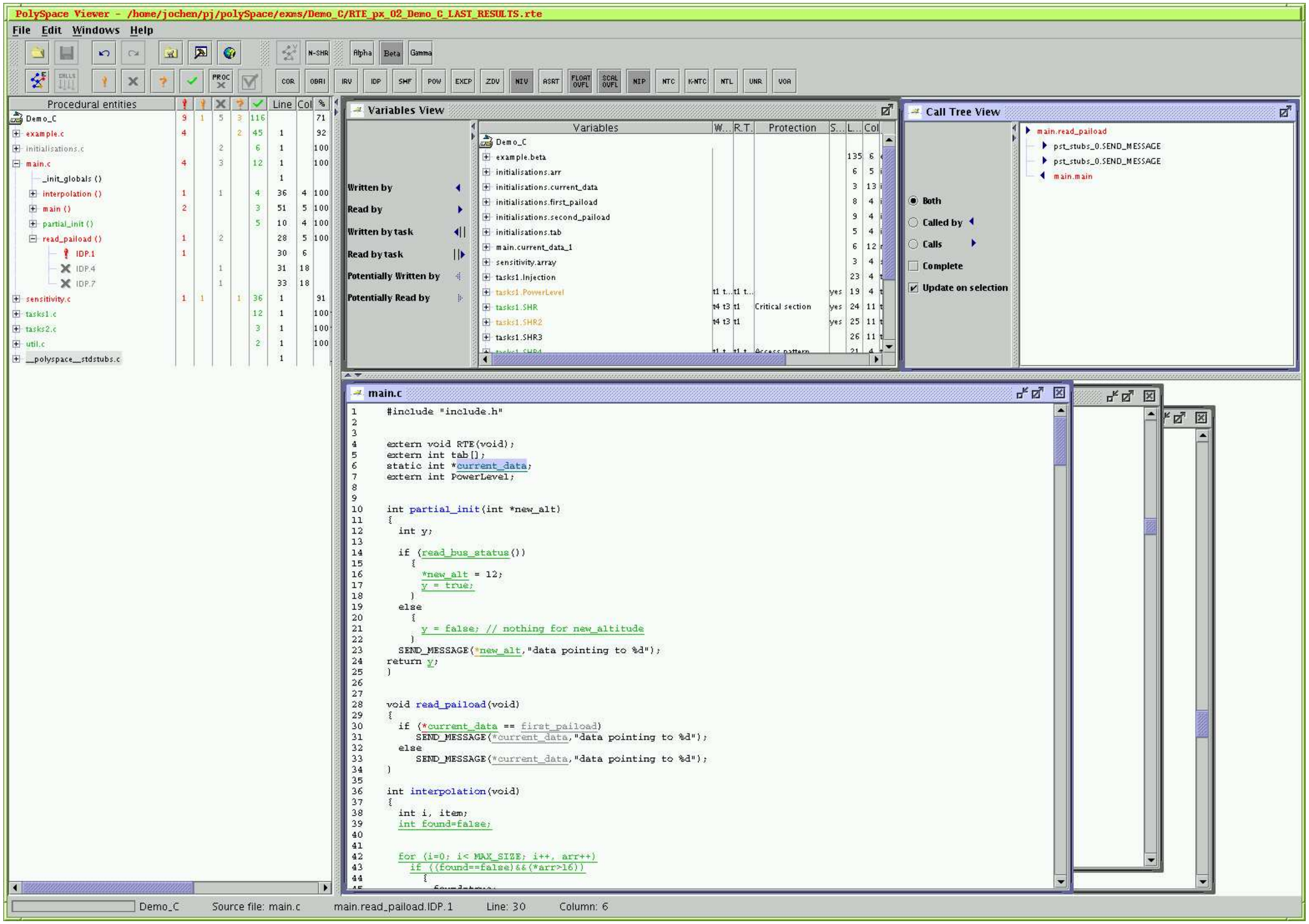
Uninitialisierte Variablen

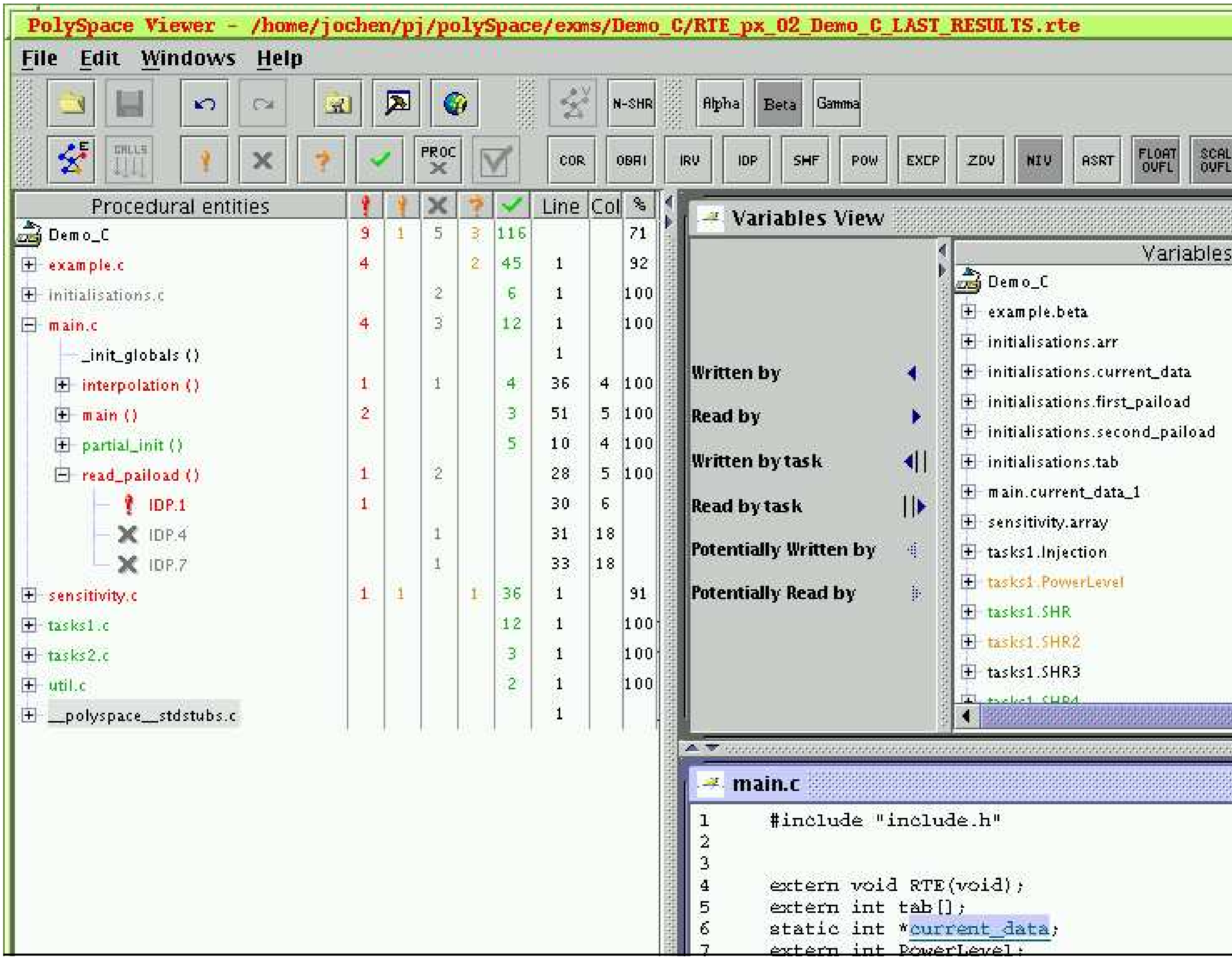
```
int search(int a[],int f,int t,int v) {     int m;
    while (f < t) {
        m = (f + t) / 2;
        if (v<a[m]) t=m; else if ...
    }
    return m;
}
```

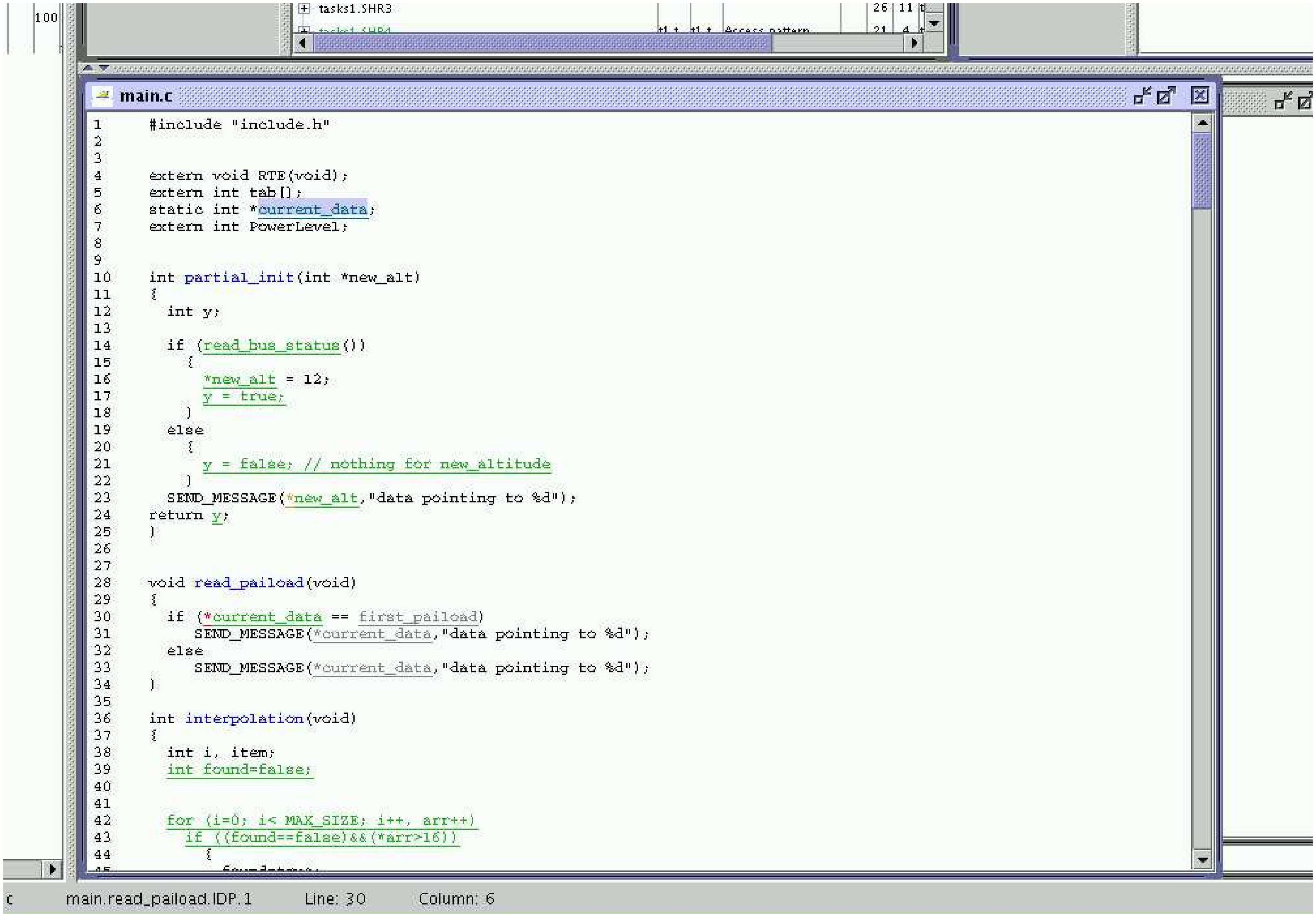
Uninitialisierte Variablen

```
int search(int a[],int f,int t,int v) {      int m;
    while (f < t) {
        m = (f + t) / 2;
        if (v<a[m]) t=m; else if ...
    }
    return m;                                   ⟵ uninitialized !
}
```

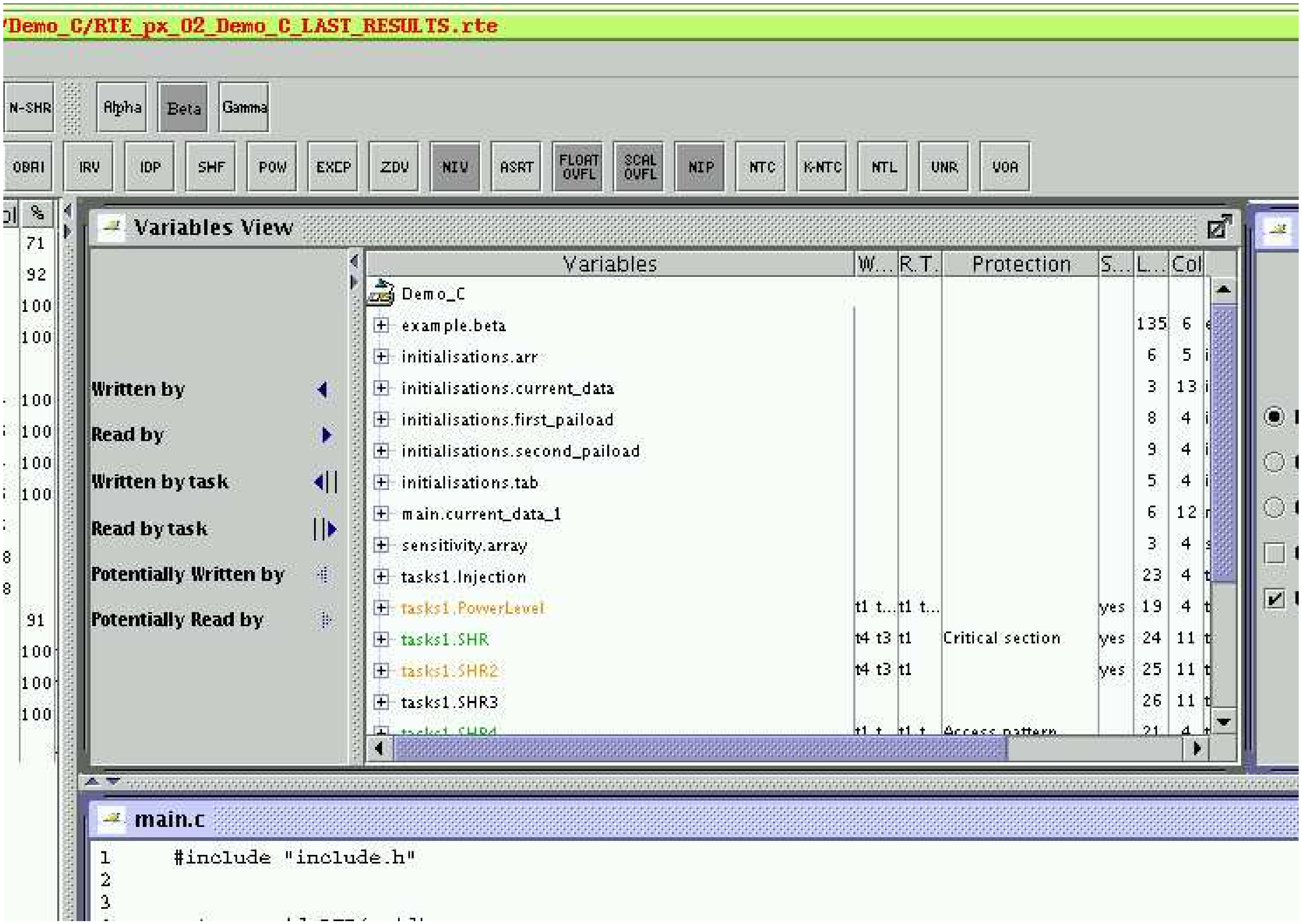
Werkzeugoberfläche



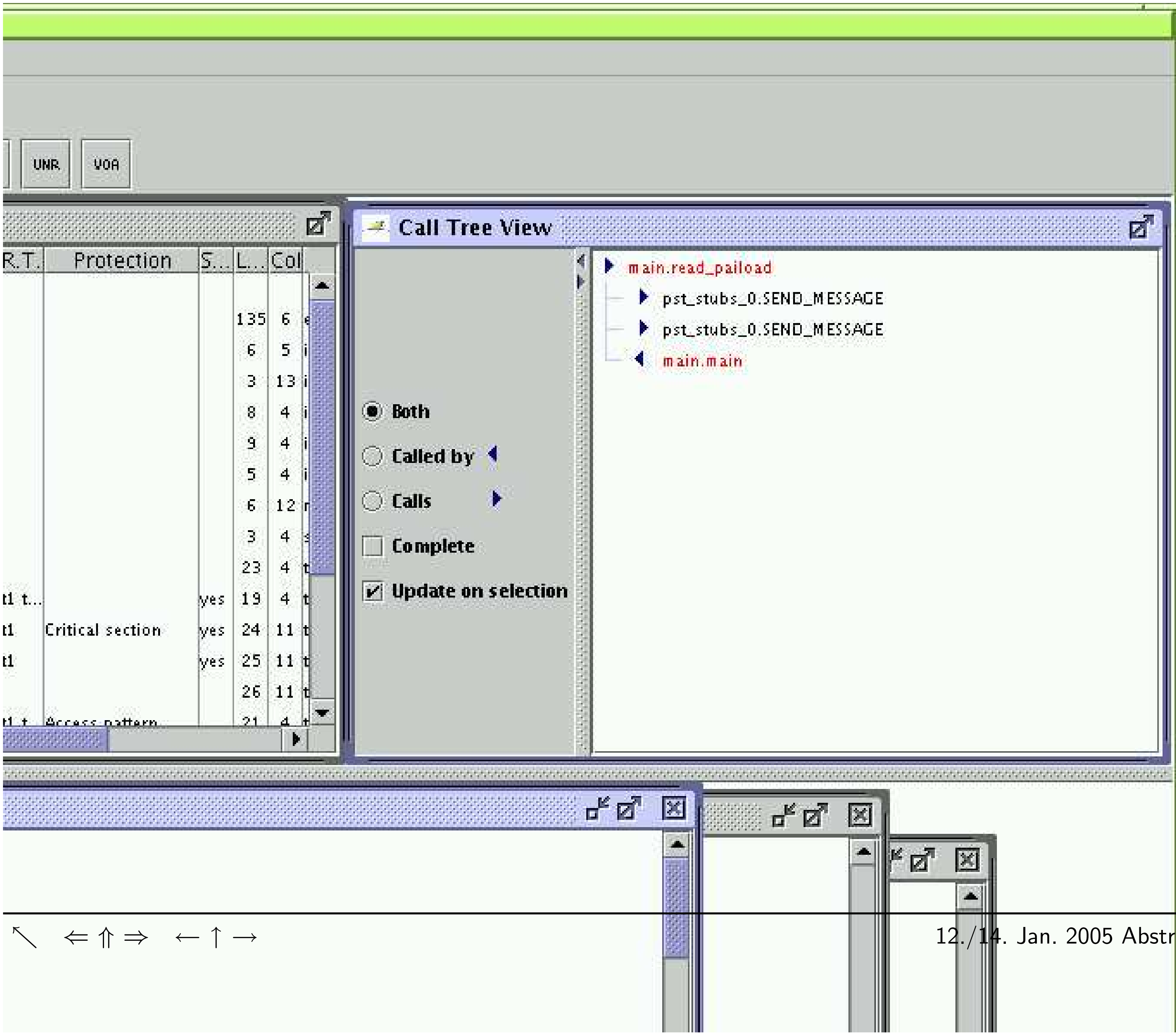

PolySpace Viewer - /home/jochen/pj/polySpace/exms/Demo_C/RTE_px_02_Demo_C_LAST_RESULTS.rte
File
Edit
Windows
Help
N-SHR
Alpha
Beta
Gamma
CALLS
PROC
COR
OBAI
IRV
IDP
SHF
POW
EXCP
ZDV
NIV
ASRT
FLOAT OVFL
SCAL OVFL
Procedural entities
Line
Col
%
Demo_C
example.c
initialisations.c
main.c
_init_globals ()
interpolation ()
main ()
partial_init ()
read_paiload ()
IDP.1
IDP.4
IDP.7
sensitivity.c
tasks1.c
tasks2.c
util.c
__polyspace__stdstubs.c
Variables View
Variables
Written by
Read by
Written by task
Read by task
Potentially Written by
Potentially Read by
Demo_C
example.beta
initialisations.arr
initialisations.current_data
initialisations.first_paiload
initialisations.second_paiload
initialisations.tab
main.current_data_1
sensitivity.array
tasks1.Injection
tasks1.PowerLevel
tasks1.SHR
tasks1.SHR2
tasks1.SHR3
main.c
1 #include "include.h"
2
3
4 extern void RTE(void);
5 extern int tab[];
6 static int *current_data;

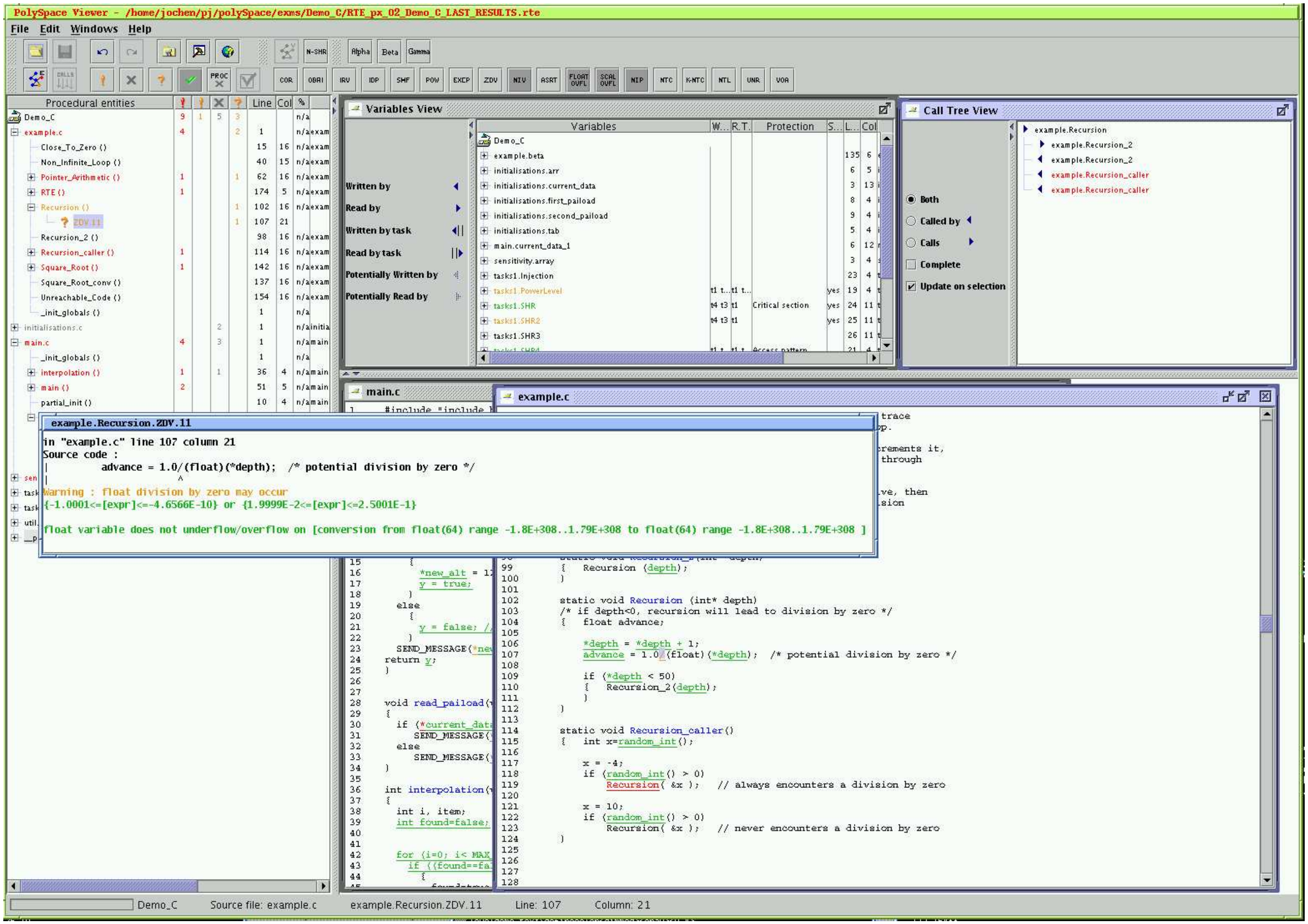


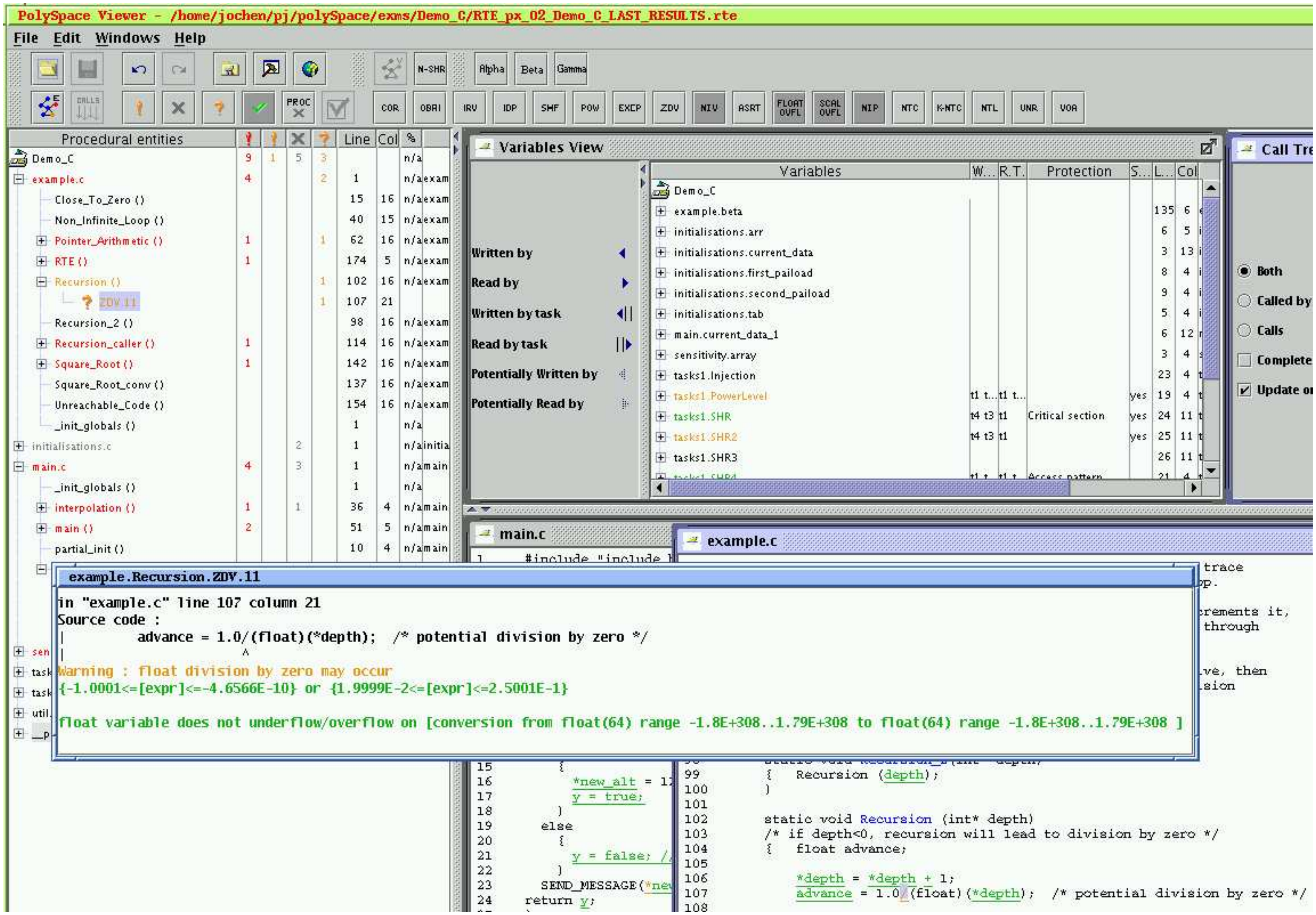
main.c
#include "include.h"
extern void RTE(void);
extern int tab[];
static int *current_data;
extern int PowerLevel;
int partial_init(int *new_alt)
{
int y;
if (read_bus_status())
{
*new_alt = 12;
y = true;
}
else
{
y = false; // nothing for new_altitude
}
SEND_MESSAGE(*new_alt,"data pointing to %d");
return y;
}
void read_paiload(void)
{
if (*current_data == first_paiload)
SEND_MESSAGE(*current_data,"data pointing to %d");
else
SEND_MESSAGE(*current_data,"data pointing to %d");
}
int interpolation(void)
{
int i, item;
int found=false;
for (i=0; i< MAX_SIZE; i++, arr++)
if ((found==false)&&(*arr>16))
{
main.read_paiload.IDP.1
Line: 30
Column: 6



Demo_C/RTE_px_02_Demo_C_LAST_RESULTS.rte
N-SHR
Alpha
Beta
Gamma
OBAI
IRV
IDP
SHF
POW
EXCP
ZDV
NIV
ASRT
FLOAT OVFL
SCAL OVFL
NIP
NTC
K-NTC
NTL
UNR
VOA
Variables View
Written by
Read by
Written by task
Read by task
Potentially Written by
Potentially Read by
Variables
W...
R.T.
Protection
S...
L...
Col
Demo_C
example.beta
initialisations.arr
initialisations.current_data
initialisations.first_paiload
initialisations.second_paiload
initialisations.tab
main.current_data_1
sensitivity.array
tasks1.Injection
tasks1.PowerLevel
tasks1.SHR
tasks1.SHR2
tasks1.SHR3
Critical section
Access pattern
main.c
1 #include "include.h"
2
3


UNR
VOA
R.T.
Protection
S...
L...
Col
Call Tree View
main.read_paiload
pst_stubs_0.SEND_MESSAGE
pst_stubs_0.SEND_MESSAGE
main.main
Both
Called by
Calls
Complete
Update on selection
Critical section
Access pattern


PolySpace Viewer - /home/jochen/pj/polySpace/exms/Demo_C/RTE_px_02_Demo_C_LAST_RESULTS.rte
File Edit Windows Help
Procedural entities
Variables View
Call Tree View
example.Recursion.ZDV.11
in "example.c" line 107 column 21
Source code :
advance = 1.0/(float)(*depth); /* potential division by zero */
Warning : float division by zero may occur
{-1.0001<=[expr]<=-4.6566E-10} or {1.9999E-2<=[expr]<=2.5001E-1}
float variable does not underflow/overflow on [conversion from float(64) range -1.8E+308..1.79E+308 to float(64) range -1.8E+308..1.79E+308]
main.c
example.c
static void Recursion (int* depth)
/* if depth<0, recursion will lead to division by zero */
float advance;
*depth = *depth + 1;
advance = 1.0/(float)(*depth); /* potential division by zero */
if (*depth < 50)
Recursion_2(depth);
static void Recursion_caller()
int x=random_int();
x = -4;
if (random_int() > 0)
Recursion(&x); // always encounters a division by zero
x = 10;
if (random_int() > 0)
Recursion(&x); // never encounters a division by zero
Demo_C
Source file: example.c
example.Recursion.ZDV.11
Line: 107
Column: 21


PolySpace Viewer - /home/jochen/pj/polySpace/exms/Demo_C/RTE_px_02_Demo_C_LAST_RESULTS.rte
File Edit Windows Help
Procedural entities
Variables View
Call Tree
main.c
example.c
example.Recursion.ZDV.11
in "example.c" line 107 column 21
Source code :
advance = 1.0/(float)(*depth); /* potential division by zero */
Warning : float division by zero may occur
{-1.0001<=[expr]<=-4.6566E-10} or {1.9999E-2<=[expr]<=2.5001E-1}
float variable does not underflow/overflow on [conversion from float(64) range -1.8E+308..1.79E+308 to float(64) range -1.8E+308..1.79E+308]
static void Recursion (int* depth)
/* if depth<0, recursion will lead to division by zero */
float advance;
*depth = *depth + 1;
advance = 1.0/(float)(*depth); /* potential division by zero */

Ergänzungen

Abstrakte Interpretation für nicht imperative Programme:

Voraussetzung ist, daß sich aus einem gegebenen Programm der Operator Φ bestimmen läßt.

(Auch bei imperativen Programmen sind noch viele Verallgemeinerungen möglich. Wir haben nur ein spezielles Φ betrachtet, nämlich das, das zur collecting semantics führt. Z.B. Datenflußanalyse ist mit einem anderen Φ möglich.)

Anwendungen in Übersetzerbau und Verifikation

- Unbenutzte Programmabschnitte
- Feldgrenzenüberwachung
- Vorzeichen
- Datenflußanalyse
- Auslagerung aus Schleifen

Anwendungen in Übersetzerbau und Verifikation

- Reference counting
- Slicing
- Erzeugung von Schleifeninvarianten
- Terminierung von Schleifen
- Worst case execution time

Werdegang

- 1960er Jahre: “Symbolic execution” (P. Naur)
- danach: viele ad-hoc-Verfahren, mehrere fehlerhaft
- 1976 / 1977: Cousot, Cousot
  Allgemeine Methodik für abstrakte Interpretation von Flowchart-Programmen
- danach: Erweiterung auf funktionale und logische Programme
- 1990er Jahre: Kombination mit Model-Checking

Literatur

References

[CC76] P. Cousot and R. Cousot. Static determination of dynamic properties of programs. In *Proc. 2nd Int. Symp. on Programming*, pages 106–130, Paris, 1976. Dunot.

[CC92] P. Cousot and R. Cousot. Comapring the Galois connection and widening / narrowing approaches to abstract interpretation. In Maurice Bruynooghe and Martin Wirsing, editors, *Proc. 4th Int. Symp. on Programming Language Implementation and Logic Programming (PLILP)*, volume 631 of *LNCS*, pages 269–296, Heidelberg, Aug. 1992. Springer.