Principles of Abstract Interpretation
MIT press
Ch. **23**, Abstract equational semantics

Patrick Cousot

pcousot.github.io

PrAbsInt@gmail.com github.com/PrAbsInt/

These slides are available at
http://github.com/PrAbsInt/slides/slides-23--equational-forward-abstract-semantics-PrAbsInt.pdf

Chapter 23

Ch. **23**, Abstract equational semantics

Traditional data flow analysis

- Traditional data flow analyses are expressed as solutions to systems of boolean equations attached to program graphs/flowcharts [Cocke and Schwartz, 1969, Second revised version, April 1970, pp. 429–461] [Hecht, 1977], not as an abstract structural semantics.
- These equations are abstractions of the structural semantics essentially loosing the structural information on programs.
- For example, circular dependencies appearing in equations because of iterations must be rebuilt [Cocke and Schwartz, 1969, Second revised version, April 1970, pp. 435–437] (nowadays using Tarjan's strongly connected components algorithm [Tarjan, 1972] and Bourdoncle's iteration algorithm [Bourdoncle, 1993]) whereas iterations are straightforward to locate knowing the program syntax.

Reachability proof methods

The traditional methods to prove reachability properties of programs are:

- Hoare logic
  - It is based on the structural reachability semantics of Chapter **19** (and so generalizes to the abstract semantics of Chapter **21**, see [P. Cousot, R. Cousot, Logozzo, and Barnett, 2012])
  - It will be developed in Chapter **26**
- Turing/Naur/Floyd invariance proof method
  - It is based on the equational semantics developed in this Chapter **23** (using fixpoint induction introduced in next Chapter **24**)
  - It will be developed in Chapter **25**

So although the two abstract structural and equational semantics are equivalent, they are both needed to explain verification and static analysis methods and prove them equivalent.

Principle of the equational semantics

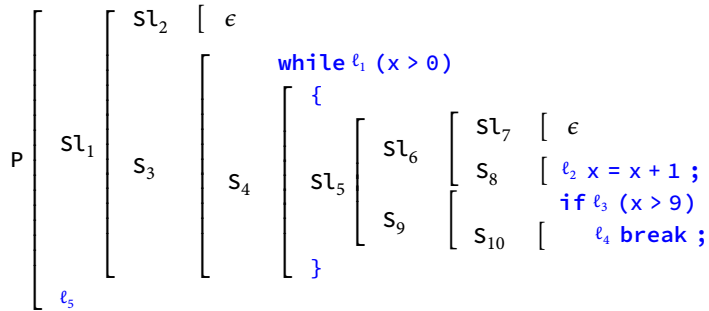
- A variable $\mathcal{X}_\ell$ is attached to each label ℓ of the program $\mathtt{P}$.
- The equations must be designed so that their solutions satisfy $\mathcal{X}_\ell = \widehat{\mathcal{S}}^{\,\natural}[\![\mathtt{P}]\!]\,\mathcal{R}_0\,\ell$ for all program labels ℓ.
- So the relations between the variables $\mathcal{X}_\ell$ of the equations directly follow from the structural definition of the semantics $\widehat{\mathcal{S}}^{\,\natural}[\![\mathtt{P}]\!]\,\mathcal{R}_0\,\ell$ by expressing the relationships between the abstract properties of the subcomponents of each program component.
- Then $\widehat{\mathcal{S}}^{\,\natural}[\![\mathtt{P}]\!]\,\mathcal{R}_0\,\ell$ corresponds to a particular iteration strategy for solving the equations by structural induction, all such strategies being equivalent by the chaotic iteration Theorem 22.4.

Example of equational semantics of a program

The program

```
while ℓ1 (x > 0) {
    ℓ2 x = x + 1 ;
    if ℓ3 (x > 9)
        ℓ4 break ;
    } ℓ5
```
(19.7) □

Grammatical structure:



(23.1)

Labelling

$$
\mathtt{P}\left[\begin{array}{l}
\mathtt{Sl}_1\left[\begin{array}{ll}
\mathtt{Sl}_2 & [\ \epsilon \\
\mathtt{S}_3 & \\
\end{array}\right. \\
\mathtt{S}_4\left[\begin{array}{l}
\texttt{while}\ \ell_1\ \texttt{(x > 0)} \\
\texttt{\{} \\
\mathtt{Sl}_5\left[\begin{array}{ll}
\mathtt{Sl}_6 & \left[\begin{array}{ll} \mathtt{Sl}_7 & [\ \epsilon \\ \mathtt{S}_8 & [\ \ell_2\ \texttt{x = x + 1 ;} \end{array}\right. \\
\mathtt{S}_9 & \left[\begin{array}{ll} \mathtt{S}_{10} & [\ \ell_4\ \texttt{break ;} \end{array}\right.
\end{array}\right. \\
\texttt{\}}
\end{array}\right. \\
\ell_5
\end{array}\right.
\qquad (23.1)
$$

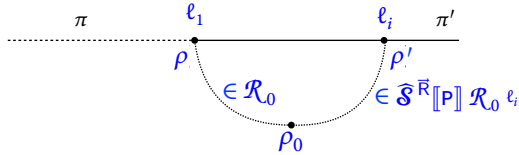
The labelling of program (23.1) is as follows.

$\mathtt{S}$	$\mathtt{P}, \mathtt{Sl}_1$	$\mathtt{Sl}_2$	$\mathtt{S}_3$	$\mathtt{S}_4, \mathtt{Sl}_5$	$\mathtt{Sl}_6, \mathtt{S}_8$	$\mathtt{Sl}_7$	$\mathtt{S}_9$	$\mathtt{S}_{10}$
at$[\![\mathtt{S}]\!]$	ℓ_1	ℓ_1	ℓ_1	ℓ_2	ℓ_2	ℓ_2	ℓ_3	ℓ_4
after$[\![\mathtt{S}]\!]$	ℓ_5	ℓ_1	ℓ_5	ℓ_1	ℓ_3	ℓ_2	ℓ_1	ℓ_1

and breaks-of$[\![\mathtt{S}_4]\!] = \{\ell_4\}$, breaks-of$[\![\mathtt{Sl}_1]\!] = \varnothing$.

The relational invariants

- The structural relational forward reachability semantics $\widehat{\mathcal{S}}^{\vec{\mathsf{R}}}[\![\mathsf{P}]\!]\,\mathcal{R}_0\,\ell_i$ is a relation between environments that can be encountered during an execution of program P starting from any initial environment statisfying $\mathcal{R}_0$ and reaching program label ℓ_i (see Chapter **19**).



- We denote by
  - x_0 the initial value of the variable x and by
  - x the value of this variable x during execution when reaching program label ℓ_i.

Relational invariants

P	ℓ_i	$\widehat{\mathcal{S}}^{\vec{\mathsf{R}}}[\![\mathsf{P}]\!]\mathcal{R}_0\ \ell_i, \quad i = 1, \ldots, 5$
/* $x = x_0$ */		$\mathcal{R}_0 = \{\langle \rho_0, \rho\rangle \mid \rho = \rho_0\}$
/* $x = x_0 \leqslant 0 \vee x_0 > 0$ */		
while ℓ_1 (x > 0)	ℓ_1	$\{\langle \rho_0, \rho\rangle \mid \rho(\mathsf{x}) = \rho_0(\mathsf{x}) \leqslant 0 \vee \rho_0(\mathsf{x}) > 0\}$
{		
ℓ_2 /* $x_0 > 0 \wedge x > 0$ */	ℓ_2	$\{\langle \rho_0, \rho\rangle \mid \rho_0(\mathsf{x}) > 0 \wedge \rho(\mathsf{x}) > 0\}$
x = x + 1 ;		
/* $x_0 > 0 \wedge x > 1$ */		
if ℓ_3 (x > 9)	ℓ_3	$\{\langle \rho_0, \rho\rangle \mid \rho_0(\mathsf{x}) > 0 \wedge \rho(\mathsf{x}) > 1\}$
ℓ_4 /* $x_0 > 0 \wedge x > 9$ */	ℓ_4	$\{\langle \rho_0, \rho\rangle \mid \rho_0(\mathsf{x}) > 0 \wedge \rho(\mathsf{x}) > 9\}$
break ;		
}		
ℓ_5 /* $(x = x_0 \leqslant 0) \vee (x_0 > 0 \wedge x > 9)$ */	ℓ_5	$\{(\langle \rho_0, \rho\rangle \mid \rho(\mathsf{x}) = \rho_0(\mathsf{x}) \leqslant 0) \vee (\rho_0(\mathsf{x}) > 0 \wedge \rho(\mathsf{x}) > 9)\}$

S_4

The system of equations

The system of equations $\vec{\mathscr{E}}^{\mathsf{R}}[\![\mathtt{P}]\!]\,\mathcal{R}_0$ for the program `P` (23.1) is

```
while ℓ1 (x > 0) {        (19.7)
    ℓ2 x = x + 1 ;
    if ℓ3 (x > 9)
        ℓ4 break ;
    } ℓ5
```

$$\begin{cases} \mathcal{X}_{\ell_1} &= \mathcal{R}_0 \cup \overleftarrow{\mathtt{test}}^{\mathsf{R}}[\![\mathtt{x > 9}]\!]\mathcal{X}_{\ell_3} \\ \mathcal{X}_{\ell_2} &= \mathtt{test}^{\mathsf{R}}[\![\mathtt{x > 0}]\!]\mathcal{X}_{\ell_1} \\ \mathcal{X}_{\ell_3} &= \mathtt{assign}_{\mathsf{R}}[\![\mathtt{x, x + 1}]\!]\,\mathcal{X}_{\ell_2} \\ \mathcal{X}_{\ell_4} &= \mathtt{test}^{\mathsf{R}}[\![\mathtt{x > 9}]\!]\mathcal{X}_{\ell_3} \\ \mathcal{X}_{\ell_5} &= \overleftarrow{\mathtt{test}}^{\mathsf{R}}[\![\mathtt{x > 0}]\!]\mathcal{X}_{\ell_1} \cup \mathcal{X}_{\ell_4} \end{cases} \qquad (23.2)$$

The equations express the fact that

- The values of x at ℓ_1 are the initial values of $\mathcal{R}_0$ or those after the loop body that is those at ℓ_3 that do not pass the test `(x > 9)`;
- The values of x at ℓ_2 are those at ℓ_1 that pass the test `(x > 0)`;
- The values of x at ℓ_3 are those at ℓ_2 after incrementation;
- The values of x at ℓ_4 are those at ℓ_3 that pass the test `(x > 9)`;
- The values of x at ℓ_5 are are those at ℓ_1 that do not pass the test `(x > 0)` or those at ℓ_4 when the **`break ;`** statement exists the loop.

Solving the system of equations iteratively

- In the example (23.2), $\mathcal{X}_{\ell_1}$ recursively depends upon itself while all other $\mathcal{X}_{\ell_i}$, $i = 2, \ldots, 5$ depend only of this $\mathcal{X}_{\ell_1}$.
- So we first have to solve the fixpoint equation

$$\mathcal{X}_{\ell_1} \quad = \quad \mathcal{R}_0 \cup \overrightarrow{\overline{\mathsf{test}}^{\mathsf{R}}}[\![\mathtt{x} > 9]\!](\mathsf{assign}_{\mathsf{R}}[\![\mathtt{x}, \mathtt{x} + 1]\!]\ (\overrightarrow{\mathsf{test}^{\mathsf{R}}}[\![\mathtt{x} > 0]\!]\mathcal{X}_{\ell_1}))$$

that is (by definitions (19.12) and (19.16))

$$\mathcal{X}_{\ell_1} \quad = \quad \mathcal{R}_0 \cup \{\langle \rho_0, \rho[\mathtt{x} \leftarrow \rho(\mathtt{x}) + 1]\rangle \mid \langle \rho_0, \rho\rangle \in \mathcal{X}_{\ell_1} \wedge 0 < \rho(\mathtt{x}) \leqslant 9\} \tag{23.3}$$

- and then carry forward the result to all other $\mathcal{X}_{\ell_i}$, $i = 2, \ldots, 5$. The equation is solved iteratively using Tarski iterative fixpoint Theorem 15.21.

Iterates

The iterates $\mathcal{X}^n_{\ell_1}$, $n \geqslant 0$ are as follows.

$$\mathcal{X}^0_{\ell_1} = \varnothing$$

$$\begin{aligned}\mathcal{X}^1_{\ell_1} &= \mathcal{R}_0 \cup \{\langle \rho_0,\ \rho[\mathrm{x} \leftarrow \rho(\mathrm{x}) + 1]\rangle \mid \langle \rho_0,\ \rho\rangle \in \mathcal{X}^0_{\ell_1} \wedge 0 < \rho(\mathrm{x}) \leqslant 9\} \\ &= \mathcal{R}_0 \\ &= \{\langle \rho_0,\ \rho\rangle \mid \rho = \rho_0\}\end{aligned}$$

$$\begin{aligned}\mathcal{X}^2_{\ell_1} &= \mathcal{R}_0 \cup \{\langle \rho_0,\ \rho[\mathrm{x} \leftarrow \rho(\mathrm{x}) + 1]\rangle \mid \langle \rho_0,\ \rho\rangle \in \mathcal{X}^1_{\ell_1} \wedge 0 < \rho(\mathrm{x}) \leqslant 9\} \\ &= \{\langle \rho_0,\ \rho\rangle \mid \rho = \rho_0\} \cup \{\langle \rho_0,\ \rho_0[x \leftarrow \rho_0(\mathrm{x}) + 1]\rangle \mid 0 < \rho_0(\mathrm{x}) \leqslant 9\}\end{aligned}$$

.../...

$$
\begin{aligned}
\mathcal{X}^3_{\ell_1} &= \mathcal{R}_0 \cup \{\langle \rho_0,\ \rho[\mathtt{x} \leftarrow \rho(\mathtt{x}) + 1]\rangle \mid \langle \rho_0,\ \rho\rangle \in \mathcal{X}^2_{\ell_1} \wedge 0 < \rho(\mathtt{x}) \leqslant 9\} \\
&= \{\langle \rho_0,\ \rho\rangle \mid \rho = \rho_0\} \cup \{\langle \rho_0,\ \rho[\mathtt{x} \leftarrow \rho(\mathtt{x}) + 1]\rangle \mid \langle \rho_0,\ \rho\rangle \in (\{\langle \rho_0,\ \rho\rangle \mid \rho = \rho_0\} \cup \{\langle \rho_0, \\
&\quad \rho_0[x \leftarrow \rho_0(\mathtt{x}) + 1]\rangle \mid 0 < \rho_0(\mathtt{x}) \leqslant 9\}) \wedge 0 < \rho(\mathtt{x}) \leqslant 9\} \\
&= \{\langle \rho_0,\ \rho\rangle \mid \rho = \rho_0\} \cup \{\langle \rho_0,\ \rho[\mathtt{x} \leftarrow \rho(\mathtt{x}) + 1]\rangle \mid \rho = \rho_0 \wedge 0 < \rho_0(\mathtt{x}) \leqslant 9\} \cup \{\langle \rho_0, \\
&\quad \rho[\mathtt{x} \leftarrow \rho(\mathtt{x}) + 1]\rangle \mid \rho = \rho_0[x \leftarrow \rho_0(\mathtt{x}) + 1] \wedge 0 < \rho_0(\mathtt{x}) \leqslant 9 \wedge 0 < \rho(\mathtt{x}) \leqslant 9\} \\
&= \{\langle \rho_0,\ \rho\rangle \mid \rho = \rho_0\} \cup \{\langle \rho_0,\ \rho_0[x \leftarrow \rho_0(\mathtt{x}) + 1]\rangle \mid 0 < \rho_0(\mathtt{x}) \leqslant 9\} \cup \{\langle \rho_0,\ \rho_0[x \leftarrow \\
&\quad \rho_0(\mathtt{x}) + 2]\rangle \mid 0 < \rho_0(\mathtt{x}) \leqslant 8\}
\end{aligned}
$$

So we make the following induction hypothesis (which holds for $1 \leqslant n \leqslant 3$ where $\bigcup \varnothing = \varnothing$).

$$
\mathcal{X}^n_{\ell_1} \quad = \quad \{\langle \rho_0,\ \rho\rangle \mid \rho = \rho_0\} \cup \bigcup_{i=1}^{n-1} \{\langle \rho_0,\ \rho_0[x \leftarrow \rho_0(\mathtt{x}) + i]\rangle \mid 0 < \rho_0(\mathtt{x}) \leqslant (9 - i)\}
$$

.../...

Induction

We check that the hypothesis is inductive.

$$\mathcal{X}^{n+1}_{\ell_1} = \mathcal{R}_0 \cup \{\langle \rho_0,\ \rho[\mathtt{x} \leftarrow \rho(\mathtt{x}) + 1]\rangle \mid \langle \rho_0,\ \rho\rangle \in \mathcal{X}^n_{\ell_1} \wedge 0 < \rho(\mathtt{x}) \leqslant 9\}$$

$$= \{\langle \rho_0,\ \rho\rangle \mid \rho = \rho_0\} \cup \{\langle \rho_0,\ \rho[\mathtt{x} \leftarrow \rho(\mathtt{x}) + 1]\rangle \mid \langle \rho_0,\ \rho\rangle \in \{\langle \rho_0,\ \rho\rangle \mid \rho = \rho_0\} \cup \bigcup_{i=1}^{n-1}\{\langle \rho_0,\ \rho_0[x \leftarrow \rho_0(\mathtt{x}) + i]\rangle \mid 0 < \rho_0(\mathtt{x}) \leqslant (9 - i)\}) \wedge 0 < \rho(\mathtt{x}) \leqslant 9\}$$

$$= \{\langle \rho_0,\ \rho\rangle \mid \rho = \rho_0\} \cup \{\langle \rho_0,\ \rho_0[x \leftarrow \rho_0(\mathtt{x}) + 1]\rangle \mid \rho_0(\mathtt{x}) \leqslant 9\} \cup \{\langle \rho_0,\ \rho[\mathtt{x} \leftarrow \rho(\mathtt{x}) + 1]\rangle \mid \langle \rho_0,\ \rho\rangle \in \bigcup_{i=1}^{n-1}\{\langle \rho_0,\ \rho_0[x \leftarrow \rho_0(\mathtt{x}) + i]\rangle \mid 0 < \rho_0(\mathtt{x}) \leqslant (9 - i)\}) \wedge 0 < \rho(\mathtt{x}) \leqslant 9\}$$

$$= \{\langle \rho_0,\ \rho\rangle \mid \rho = \rho_0\} \cup \{\langle \rho_0,\ \rho_0[x \leftarrow \rho_0(\mathtt{x}) + 1]\rangle \mid \rho_0(\mathtt{x}) \leqslant 9\} \cup \bigcup_{i=1}^{n-1}\{\langle \rho_0,\ \rho_0[x \leftarrow \rho_0(\mathtt{x}) + i][x \leftarrow \rho_0[x \leftarrow \rho_0(\mathtt{x}) + i](\mathtt{x}) + 1]\rangle \mid 0 < \rho_0(\mathtt{x}) \leqslant (9 - i) \wedge 0 < \rho_0[x \leftarrow \rho_0(\mathtt{x}) + i](\mathtt{x}) \leqslant 9\}$$

.../...

$$= \{\langle \rho_0,\ \rho\rangle \mid \rho = \rho_0\} \cup \{\langle \rho_0,\ \rho_0[x \leftarrow \rho_0(\mathsf{x}) + 1]\rangle \mid \rho_0(\mathsf{x}) \leqslant 9\} \cup \bigcup_{i=1}^{n-1} \{\langle \rho_0,$$

$$\rho_0[x \leftarrow \rho_0(\mathsf{x}) + i + 1]\rangle \mid i + 1 < \rho_0(\mathsf{x}) + i + 1 \leqslant 10 \wedge 1 < \rho_0(\mathsf{x}) + i + 1 \leqslant 9\}$$

$$= \{\langle \rho_0,\ \rho\rangle \mid \rho = \rho_0\} \cup \bigcup_{j=1}^{(n+1)-1} \{\langle \rho_0,\ \rho_0[x \leftarrow \rho_0(\mathsf{x}) + j]\rangle \mid 0 < \rho_0(\mathsf{x}) \leqslant (9 - j)\}$$

(letting $j = i + 1$)

.../...

Limit

Passing to the limit, the solution to the fixpoint equation (23.3) is

$$\begin{aligned}\mathcal{X}_{\ell_1} &= \bigcup_{n\geqslant 0} \mathcal{X}^n_{\ell_1}\\ &= \{\langle \rho_0,\ \rho\rangle \mid \rho = \rho_0\} \cup \{\langle \rho_0,\ \rho_0[x \leftarrow \rho_0(\mathrm{x}) + i]\rangle \mid i \in [1,9] \wedge 0 < \rho_0(\mathrm{x}) \leqslant (9-i)\}\end{aligned}$$

(since the join is empty when $9 - i \leqslant 0$)

.../...

Propagation

We derive the other components of the equations (23.2).

$$\mathcal{X}_{\ell_2} = \{\langle \rho_0,\ \rho\rangle \in \mathcal{X}_{\ell_1} \mid \rho(\mathrm{x}) > 0\}$$
$$= \{\langle \rho_0,\ \rho_0\rangle \mid \rho_0(\mathrm{x}) > 0\} \cup \{\langle \rho_0,\ \rho_0[x \leftarrow \rho_0(\mathrm{x}) + i]\rangle \mid i \in [1,9] \wedge 0 < \rho_0(\mathrm{x}) \leqslant (9-i)\}$$

$$\mathcal{X}_{\ell_3} = \{\langle \rho_0,\ \rho[\mathrm{x} \leftarrow \rho(\mathrm{x}) + 1]\rangle \mid \langle \rho_0,\ \rho\rangle \in \mathcal{X}_{\ell_1} \wedge \rho(\mathrm{x}) > 0\}$$
$$= \{\langle \rho_0,\ \rho[\mathrm{x} \leftarrow \rho(\mathrm{x}) + 1]\rangle \mid \langle \rho_0,\ \rho\rangle \in (\{\langle \rho_0,\ \rho\rangle \mid \rho = \rho_0\} \cup \{\langle \rho_0,\ \rho_0[x \leftarrow \rho_0(\mathrm{x}) + i]\rangle \mid i \in [1,9] \wedge 0 < \rho_0(\mathrm{x}) \leqslant (9-i)\}) \wedge \rho(\mathrm{x}) > 0\}$$
$$= \{\langle \rho_0,\ \rho[\mathrm{x} \leftarrow \rho(\mathrm{x}) + 1]\rangle \mid \rho = \rho_0 \wedge \rho(\mathrm{x}) > 0\} \cup \{\langle \rho_0,\ \rho[\mathrm{x} \leftarrow \rho(\mathrm{x}) + 1]\rangle \mid \langle \rho_0,\ \rho\rangle \in \{\langle \rho_0,\ \rho_0[x \leftarrow \rho_0(\mathrm{x}) + i]\rangle \mid i \in [1,9] \wedge 0 < \rho_0(\mathrm{x}) \leqslant (9-i)\}) \wedge \rho(\mathrm{x}) > 0\}$$
$$= \{\langle \rho_0,\ \rho[\mathrm{x} \leftarrow \rho(\mathrm{x}) + 1]\rangle \mid \rho = \rho_0 \wedge \rho(\mathrm{x}) > 0\} \cup \{\langle \rho_0,\ \rho[\mathrm{x} \leftarrow \rho(\mathrm{x}) + 1]\rangle \mid \exists i \in [1,9]\ .\ \rho = \rho_0[x \leftarrow \rho_0(\mathrm{x}) + i] \wedge 0 < \rho_0(\mathrm{x}) \leqslant (9-i) \wedge \rho(\mathrm{x}) > 0\}$$
$$= \{\langle \rho_0,\ \rho[\mathrm{x} \leftarrow \rho(\mathrm{x}) + 1]\rangle \mid \rho = \rho_0 \wedge \rho(\mathrm{x}) > 0\} \cup \{\langle \rho_0,\ \rho_0[x \leftarrow \rho_0(\mathrm{x}) + i][x \leftarrow \rho_0[x \leftarrow \rho_0(\mathrm{x}) + i](\mathrm{x}) + 1]\rangle \mid i \in [1,9] \wedge 0 < \rho_0(\mathrm{x}) \leqslant (9-i) \wedge \rho_0[x \leftarrow \rho_0(\mathrm{x}) + i](\mathrm{x}) > 0\}$$
$$= \{\langle \rho_0,\ \rho_0[x \leftarrow \rho_0(\mathrm{x}) + 1]\rangle \mid \rho_0(\mathrm{x}) > 0\} \cup \{\langle \rho_0,\ \rho_0[x \leftarrow \rho_0(\mathrm{x}) + i]\rangle \mid i \in [1,9] \wedge 0 < \rho_0(\mathrm{x}) \leqslant (9-i)\}$$

$$\begin{aligned}
\mathcal{X}_{\ell_4} &= \{\langle \rho_0,\ \rho[\mathsf{x} \leftarrow \rho(\mathsf{x}) + 1]\rangle \mid \langle \rho_0,\ \rho\rangle \in \mathcal{X}_{\ell_1} \wedge \rho(\mathsf{x}) > 9\} \\
&= \{\langle \rho_0,\ \rho[\mathsf{x} \leftarrow \rho(\mathsf{x}) + 1]\rangle \mid \langle \rho_0,\ \rho\rangle \in (\{\langle \rho_0,\ \rho\rangle \mid \rho = \rho_0\} \cup \{\langle \rho_0,\ \rho_0[x \leftarrow \rho_0(\mathsf{x}) + i]\rangle \mid i \in [1, 9] \wedge 0 < \rho_0(\mathsf{x}) \leqslant (9 - i)\}) \wedge \rho(\mathsf{x}) > 9\} \\
&= \{\langle \rho_0, \rho_0[x \leftarrow \rho_0(\mathsf{x})+1]\rangle \mid \rho_0(\mathsf{x}) > 9\} \cup \{\langle \rho_0, \rho_0[x \leftarrow \rho_0(\mathsf{x})+i+1]\rangle \mid i \in [1, 9] \wedge \rho_0(\mathsf{x}) = (9 - i)\} \\
&= \{\langle \rho_0,\ \rho_0[x \leftarrow \rho_0(\mathsf{x}) + 1]\rangle \mid \rho_0(\mathsf{x}) > 9\} \cup \{\langle \rho_0,\ \rho_0[x \leftarrow 10]\rangle \mid 1 \leqslant \rho_0(\mathsf{x}) \leqslant 9\}
\end{aligned}$$

$$\begin{aligned}
\mathcal{X}_{\ell_5} &= \{\langle \rho_0,\ \rho[\mathsf{x} \leftarrow \rho(\mathsf{x}) + 1]\rangle \mid \langle \rho_0,\ \rho\rangle \in \mathcal{X}_{\ell_1} \wedge \rho(\mathsf{x}) > 9\} \cup \{\langle \rho_0,\ \rho\rangle \in \mathcal{R}_0 \mid \rho(\mathsf{x}) \leqslant 0\} \\
&= \{\langle \rho_0,\ \rho_0\rangle \mid \rho_0(\mathsf{x}) \leqslant 0\} \cup \{\langle \rho_0,\ \rho_0[x \leftarrow \rho_0(\mathsf{x}) + 1]\rangle \mid \rho_0(\mathsf{x}) > 9\} \cup \{\langle \rho_0,\ \rho_0[x \leftarrow 10]\rangle \mid 1 \leqslant \rho_0(\mathsf{x}) \leqslant 9\}
\end{aligned}$$

.../...

Least solution to the fixpoint equations

So the least solution $\mathcal{S}$ to the system of equations (23.2) is the following.

$$\begin{cases}
\mathcal{S}_{\ell_1} &= \{\langle \rho_0,\ \rho\rangle \mid \rho = \rho_0\} \cup \{\langle \rho_0,\ \rho_0[x \leftarrow \rho_0(x) + i]\rangle \mid i \in [1,9] \wedge 0 < \rho_0(x) \leqslant (9-i)\} \\
\mathcal{S}_{\ell_2} &= \{\langle \rho_0,\ \rho_0\rangle \mid \rho_0(x) > 0\} \cup \{\langle \rho_0,\ \rho_0[x \leftarrow \rho_0(x) + i]\rangle \mid i \in [1,9] \wedge 0 < \rho_0(x) \leqslant (9-i)\} \\
\mathcal{S}_{\ell_3} &= \{\langle \rho_0,\ \rho_0[x \leftarrow \rho_0(x) + 1]\rangle \mid \rho_0(x) > 0\} \cup \{\langle \rho_0,\ \rho_0[x \leftarrow \rho_0(x) + i]\rangle \mid i \in [1,9] \wedge 0 < \rho_0(x) \leqslant (9-i)\} \\
\mathcal{S}_{\ell_4} &= \{\langle \rho_0,\ \rho_0[x \leftarrow \rho_0(x) + 1]\rangle \mid \rho_0(x) > 9\} \cup \{\langle \rho_0,\ \rho_0[x \leftarrow \rho_0(x) + i + 1]\rangle \mid i \in [1,9] \wedge \rho_0(x) = (9-i)\} \\
\mathcal{S}_{\ell_5} &= \{\langle \rho_0,\ \rho_0\rangle \mid \rho_0(x) \leqslant 0\} \cup \{\langle \rho_0,\ \rho_0[x \leftarrow \rho_0(x) + 1]\rangle \mid \rho_0(x) > 9\} \cup \{\langle \rho_0,\ \rho_0[x \leftarrow 10]\rangle \mid 1 \leqslant \rho_0(x) \leqslant 9\}
\end{cases}$$

```
while ℓ1 (x > 0) {
    ℓ2 x = x + 1 ;
    if ℓ3 (x > 9)
        ℓ4 break ;
    } ℓ5
```
(19.7)

On program exit at ℓ_5, $\mathcal{S}_{\ell_5}$ environments that the value x of x is

- the initial value x_0 of x when x_0 is negative or zero (since the loop is never entered);
- or, the initial value x_0 of x plus 1 when x_0 is greater than 9;
- or 10, when the initial value x_0 of x is between 1 and 9 since in that case x is incremented by successive loop iterations until reaching 10 in which case the loop exits by the break statement.

Structural equational semantics

- The equational semantics of a program P is designed so that its least solution is the abstract interpreter of Chapter **21**.
- We define the equational semantics of a program P by structural induction on the syntax of program P.
- So the equational semantics (specifying how the equations are derived for a program) is structural but the equations are not (*i.e.* the program structure is not apparent in the equations).

- The equations $\widehat{\mathscr{E}}^{\natural}[\![\mathsf{s}]\!]$ for a program component s have the form

$$\mathcal{X} \quad = \quad \mathsf{E}[\![\mathsf{s}]\!]\, \mathcal{R}_0\, \mathcal{X} \tag{23.4}$$

  which can be detailled as

$$\begin{cases} \mathcal{X}_\ell \quad = \quad \mathsf{E}[\![\mathsf{s}]\!]\, \mathcal{R}_0\, (\prod_{\ell' \in \mathsf{labs}[\![\mathsf{s}]\!]} \mathcal{X}_{\ell'})\, \ell \\ \ell \in \mathsf{labs}[\![\mathsf{s}]\!] \end{cases}$$

  so that the equational semantics is the set of equations

$$\widehat{\mathscr{E}}^{\natural}[\![\mathsf{s}]\!] = \{\mathcal{X}_\ell \quad = \quad \mathsf{E}[\![\mathsf{s}]\!]\, \mathcal{R}_0\, (\textstyle\prod_{\ell' \in \mathsf{labs}[\![\mathsf{s}]\!]} \mathcal{X}_{\ell'})\, \ell \mid \ell \in \mathsf{labs}[\![\mathsf{s}]\!]\}.$$

- By (19.30), the set of reachable environments of a statement s not at a label of that statement is empty, abstracted by $\bot^{\natural}$. So $\mathcal{X}^\ell = \bot^{\natural}$ for all $\ell \notin \mathsf{labs}[\![\mathsf{s}]\!]$ and to determine this no specific equation need to be considered.

Structural equational semantics

Equational semantics of a program $\mathtt{P} ::= \mathtt{Sl}\ \ell'$

$$\widehat{\mathscr{E}}^{\natural}[\![\mathtt{P}]\!] \triangleq \widehat{\mathscr{E}}^{\natural}[\![\mathtt{Sl}]\!] \tag{23.5}$$

- The equational semantics of a program $\mathtt{P} ::= \mathtt{Sl}\ \ell'$ with variables $\mathcal{X}^{\ell}$, $\ell \in \mathit{labs}[\![\mathtt{S}]\!]$ is that of its statement list $\mathtt{Sl}$.

Equational semantics of a skip statement $\mathtt{S} ::= \mathtt{;}$

$$\widehat{\mathscr{E}}^{\natural}[\![\mathtt{S}]\!]\,\mathcal{R}_0 = \{\mathcal{X}_{\mathit{at}[\![\mathtt{S}]\!]} = \mathcal{R}_0, \mathcal{X}_{\mathit{after}[\![\mathtt{S}]\!]} = \mathcal{X}_{\mathit{at}[\![\mathtt{S}]\!]}\} \tag{23.6}$$

- The equational semantics of a skip statement $\mathtt{S} ::= \mathtt{;}$ maps the (abstraction of the) initial environments to themselves since they are not modified.

Equational semantics of an assignment statement S ::= x = E ;

$$\mathscr{E}^{\natural}[\![\mathtt{S}]\!]\,\mathcal{R}_0 = \{\mathcal{X}_{\mathsf{at}[\![\mathtt{S}]\!]} = \mathcal{R}_0, \quad \mathcal{X}_{\mathsf{after}[\![\mathtt{S}]\!]} = \mathsf{assign}_{\natural}[\![\mathtt{x}, \mathtt{E}]\!]\,\mathcal{X}_{\mathsf{at}[\![\mathtt{S}]\!]}\} \tag{23.7}$$

- The equational semantics of an assignment statement S ::= x = E ; maps the (abstraction of the) initial environments to themselves on entry and to themselves as modified by the assignment on exit.

Equational semantics of a conditional statement $\mathtt{S} ::= \mathtt{if\ (B)\ S}_t$

$$\begin{aligned}\mathscr{E}^{\natural}[\![\mathtt{S}]\!]\,\mathcal{R}_0 \quad = \quad & \mathsf{let}\,\{\mathcal{X}_{\mathsf{after}[\![\mathtt{S}]\!]} = E\} \uplus \mathcal{E} = \mathscr{E}^{\natural}[\![\mathtt{S}_t]\!](\mathsf{test}^{\natural}[\![\mathtt{B}]\!]\mathcal{X}_{\mathsf{at}[\![\mathtt{S}]\!]})\ \mathsf{in} \\ & \{\mathcal{X}_{\mathsf{at}[\![\mathtt{S}]\!]} = \mathcal{R}_0\} \cup \mathcal{E} \cup \{\mathcal{X}_{\mathsf{after}[\![\mathtt{S}]\!]} = E \sqcup^{\natural} \overline{\mathsf{test}}^{\natural}[\![\mathtt{B}]\!]\mathcal{X}_{\mathsf{at}[\![\mathtt{S}]\!]}\}\end{aligned} \tag{23.8}$$

- We write $X \uplus Y = Z$ to mean that X, Y is a partition of Z that is $X \cap Y = \varnothing$ and $X \cup Y = Z$. This is essential to ensure that there is only one equation per variable $\mathcal{X}_\ell$, $\ell \in \mathsf{labs}[\![\mathtt{S}]\!]$
- The equational semantics of a conditional statement $\mathtt{S} ::= \mathtt{if\ (B)\ S}_t$ is the (abstraction of the) set of reachable environments in $\mathtt{S}_t$ under the hypothesis that the test B is true and, after the conditional statement, the union of the (abstraction of the) environments reaching the end of the true alternative $\mathtt{S}_t$ (as given by the equation for $\mathcal{X}_{\mathsf{after}[\![\mathtt{S}_t]\!]} = \mathcal{X}_{\mathsf{after}[\![\mathtt{S}]\!]}$ in the alternative $\mathtt{S}_t$) and those for which the conditional statement is skipped when the test B is false.

Equational semantics of a conditional statement $\mathtt{S} ::= \mathtt{if\ (B)\ S}_t\ \mathtt{else\ S}_f$

$$\begin{aligned}\widehat{\mathscr{E}}^{\natural}[\![\mathtt{S}]\!]\,\mathcal{R}_0 \quad = \quad & \mathsf{let}\,(\{\mathcal{X}_{\mathsf{after}[\![\mathtt{S}]\!]} = E_t\} \cup \mathcal{E}_t) = \widehat{\mathscr{E}}^{\natural}[\![\mathtt{S}_t]\!](\mathsf{test}^{\natural}[\![\mathtt{B}]\!]\mathcal{X}_{\mathsf{at}[\![\mathtt{S}]\!]}) \\ & \text{and}\ \ (\{\mathcal{X}_{\mathsf{after}[\![\mathtt{S}]\!]} = E_f\} \cup \mathcal{E}_f) = \widehat{\mathscr{E}}^{\natural}[\![\mathtt{S}_f]\!](\overline{\mathsf{test}}^{\natural}[\![\mathtt{B}]\!]\mathcal{X}_{\mathsf{at}[\![\mathtt{S}]\!]})\ \mathsf{in} \\ & \quad \{\mathcal{X}_{\mathsf{at}[\![\mathtt{S}]\!]} = \mathcal{R}_0\} \cup \\ & \quad \mathcal{E}_t \cup \mathcal{E}_f \cup \\ & \quad \{\mathcal{X}_{\mathsf{after}[\![\mathtt{S}]\!]} = E_t \sqcup^{\natural} E_f\}\end{aligned} \tag{23.9}$$

- The equational semantics of a conditional statement $\mathtt{S} ::= \mathtt{if\ (B)\ S}_t\ \mathtt{else\ S}_f$ is the (abstraction of the) set of reachable environments in $\mathtt{S}_t$ under the hypothesis that the test $\mathtt{B}$ is true, the set of reachable environments in $\mathtt{S}_f$ under the hypothesis that the test $\mathtt{B}$ is false, and, after the conditional statement, the union of the sets of environments reaching the end of the true and false alternatives $\mathtt{S}_t$ and $\mathtt{S}_f$.

Equational semantics of a statement list $\mathtt{sl} ::= \mathtt{sl}'\ \mathtt{s}$

$$\begin{array}{lcll} \widehat{\mathscr{E}}^{\natural}[\![\mathtt{sl}]\!]\mathcal{R}_0 & = & \widehat{\mathscr{E}}^{\natural}[\![\mathtt{s}]\!]\mathcal{R}_0 & \text{when} \quad \mathtt{sl}' ::= \epsilon \\ & = & \text{let } (\{\mathcal{X}_{\mathsf{after}[\![\mathtt{sl}']\!]} = E'\} \cup \mathcal{E}') = \widehat{\mathscr{E}}^{\natural}[\![\mathtt{sl}']\!]\mathcal{R}_0 & \text{otherwise} \\ & & \quad \text{and } (\{\mathcal{X}_{\mathsf{at}[\![\mathtt{s}]\!]} = E\} \cup \mathcal{E}) = \widehat{\mathscr{E}}^{\natural}[\![\mathtt{s}]\!]\mathcal{X}_{\mathsf{at}[\![\mathtt{s}]\!]} \text{ in} & \\ & & \quad\quad \{\mathcal{X}_{\mathsf{at}[\![\mathtt{s}]\!]} = E' \sqcup^{\natural} E\} \cup \mathcal{E}' \cup \mathcal{E} & \end{array} \tag{23.10}$$

- The equational semantics of a statement list $\mathtt{sl} ::= \mathtt{sl}'\ \mathtt{s}$ is the set of equations of $\mathtt{sl}'$ and those of $\mathtt{s}$ after executing $\mathtt{sl}'$ where the equation for $\mathcal{X}_{\mathsf{after}[\![\mathtt{sl}']\!]} = \mathcal{X}_{\mathsf{at}[\![\mathtt{s}]\!]}$ is shared.

Equational semantics of an empty statement list $\mathtt{sl} ::= \epsilon$

$$\widehat{\mathscr{E}}^{\natural}[\![\mathtt{sl}]\!]\mathcal{R}_0 = \{\mathcal{X}_{\mathsf{at}[\![\mathtt{sl}]\!]} = \mathcal{R}_0\} \tag{23.11}$$

- The empty statement list $\mathtt{sl} ::= \epsilon$ does not involve any computation so that the (abstraction of the) reachable environments are the initial environments.

Equational semantics of an iteration statement $\mathtt{S} ::= \mathtt{while}^{\ell}\ \mathtt{(B)}\ \mathtt{S}_b$

$$
\begin{aligned}
\widehat{\mathscr{E}}^{\natural}[\![\mathtt{S}]\!]\,\mathcal{R}_0 \quad = \quad & \mathsf{let}\,(\{\mathcal{X}_{\mathsf{at}[\![\mathtt{S}]\!]} = E\} \cup \mathcal{E}) = \widehat{\mathscr{E}}^{\natural}[\![\mathtt{S}_b]\!](\mathsf{test}^{\natural}[\![\mathtt{B}]\!]\mathcal{X}_{\mathsf{at}[\![\mathtt{S}]\!]})\ \ \mathsf{in} \\
& \{\mathcal{X}_{\mathsf{at}[\![\mathtt{S}]\!]} = \mathcal{R}_0 \sqcup^{\natural} E\} \cup \\
& \mathcal{E} \cup \\
& \{\mathcal{X}_{\mathsf{after}[\![\mathtt{S}]\!]} = \overline{\mathsf{test}}^{\natural}[\![\mathtt{B}]\!]\mathcal{X}_{\mathsf{at}[\![\mathtt{S}]\!]} \sqcup^{\natural} \bigsqcup_{\ell \in \mathsf{breaks\text{-}of}[\![\mathtt{S}_b]\!]}^{\natural} \mathcal{X}_{\ell}\}
\end{aligned}
\tag{23.12}
$$

- The equational semantics of an iteration statement $\texttt{S} ::= \texttt{while}^{\ell}\ \texttt{(B)}\ \texttt{S}_b$, is a fixpoint which successive iterates provide the (abstraction of the) reachable environments after at most 0, 1, ...or more iterations in the loop.
- If the loop terminates, the fixpoint iterates beyond the maximal number of iterations add no new reachable environment.
- If the loop does not terminate the (abstraction of the) reachable environments after any number of iterations (is) are obtained by passing to the limit in the fixpoint iterates.
- The reachable environments $\mathcal{X}_{\mathsf{at}[\![\texttt{S}]\!]}$ are the entry environments or the reachable environments after one more iteration from reachable states with test true.
- The reachable environments $\mathcal{X}_{\mathsf{after}[\![\texttt{S}]\!]}$ on loop exit, are those $\mathsf{at}[\![\texttt{S}]\!]$ for which the test is false or the breaking environments reachable from reachable environments in an iteration with test true.

Equational semantics of a break statement $\mathtt{S} ::= \ell\ \mathtt{break}\ ;$

$$\mathscr{E}^{\natural}[\![\mathtt{S}]\!]\,\mathcal{R}_0 \quad = \quad \{\mathcal{X}_{\mathsf{at}[\![\mathtt{S}]\!]} = \mathcal{R}_0,\ \mathcal{X}_{\mathsf{after}[\![\mathtt{S}]\!]} = \bot^{\natural}\} \tag{23.13}$$

- The equational semantics of a break statement $\mathtt{S} ::= \mathtt{break}\ ;$ states that execution never goes after the break at $\mathsf{after}[\![\mathtt{S}]\!]$.

Equational semantics of a compound statement $\mathtt{S} ::= \{\ \mathtt{Sl}\ \}$

$$\mathscr{E}^{\natural}[\![\mathtt{S}]\!] \quad = \quad \mathscr{E}^{\natural}[\![\mathtt{Sl}]\!] \tag{23.14}$$

- The equational semantics of a compound statement $\mathtt{S} ::= \{\ \mathtt{Sl}\ \}$ is that of the statement list $\mathtt{Sl}$.

Theorem (23.20) The equations $\widehat{\mathscr{E}}^{\natural}[\![\mathsf{P}]\!]\,\mathcal{R}_0$ have the form

$$\begin{cases} \mathcal{X}_\ell \;=\; \mathsf{E}[\![\mathsf{P}]\!]\,\mathcal{R}_0\Big(\prod_{\ell' \in \mathsf{labs}[\![\mathsf{P}]\!]} \mathcal{X}_{\ell'}\Big)\,\ell \\ \ell \in \mathsf{labs}[\![\mathsf{P}]\!] \end{cases}$$

such that

- there is exactly one equation $\mathcal{X}_\ell = \mathsf{E}[\![\mathsf{P}]\!]\,\mathcal{R}_0\,(\prod_{\ell' \in \mathsf{labs}[\![\mathsf{P}]\!]} \mathcal{X}_{\ell'})\,\ell$ for each program point $\ell \in \mathsf{labs}[\![\mathsf{P}]\!]$;
- $\mathsf{E}[\![\mathsf{P}]\!]\,\mathcal{R}_0 \in \prod_{\ell \in \mathsf{labs}[\![\mathsf{P}]\!]} \mathbb{P}^{\natural} \xrightarrow{uc} \prod_{\ell \in \mathsf{labs}[\![\mathsf{P}]\!]} \mathbb{P}^{\natural}$ is well-defined and continuous;
- The equations have a least pointwise fixpoint $\mathsf{lfp}^{\dot{\sqsubseteq}^{\natural}}\,\mathsf{E}[\![\mathsf{P}]\!]\,\mathcal{R}_0 = \widehat{\mathscr{S}}^{\natural}[\![\mathsf{P}]\!]\,\mathcal{R}_0$, as defined in Section **21.2**.

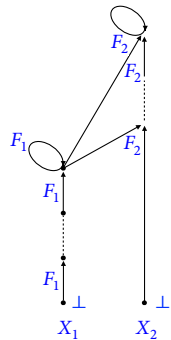
Theorem 23.20 shows that the equational definition of the semantics is exactly the same as the structural functional one of Chapter **21**. The idea is that the abstract interpreter is a function f which can be abstracted by an equation $\mathcal{X} = F(\mathcal{X})$ which least solution is $f = \mathsf{lfp}\,F$, and conversely.

Transfinite chaotic iterations

Equations:

$$\begin{cases} X_1 &= F_1(X_1) \\ X_2 &= F_2(X_1, X_2) \end{cases}$$

Example transfinite chaotic iterations [P. Cousot, 1977, 1978]:



Properties of the system of equations

(1) The variables of equations $\widehat{\mathscr{E}}^{\,\natural}[\![\mathtt{S}]\!]\,\mathcal{R}_0$ for a program component $\mathtt{S} \in \mathbb{P}\mathtt{c}$ are in $\{\mathcal{X}_\ell \mid \ell \in \mathsf{labs}[\![\mathtt{S}]\!]\}$

(2) No system of equations for a program component $\mathtt{S} \in \mathbb{P}\mathtt{c}$ has any equations depending on $\mathcal{X}_{\mathsf{after}[\![\mathtt{S}]\!]}$.

(3) For all program components $\mathtt{S}$, $\underline{\underline{NOT}}$ starting with an iteration, the equation for $\mathcal{X}_{\mathsf{at}[\![\mathtt{S}]\!]}$ is

$$\mathcal{X}_{\mathsf{at}[\![\mathtt{S}]\!]} = \mathcal{R}_0$$

The proofs are by structural induction

- Base cases, *e.g.* assignment (23.7)
- Induction cases, *e.g.* iteration (23.12) or statement list (23.10)

Proof of Theorem 23.20 — I

We prove the theorem for all program components $\mathsf{s} \in \mathbb{P}c$, by structural induction of s.

The equations $\widehat{\mathscr{E}}^{\,\natural}[\![\mathsf{s}]\!]\,\mathcal{R}_0$ have the form $\mathcal{X} = E(\mathcal{X})$, that is componenwise

$$\begin{cases} \mathcal{X}_\ell = \mathsf{E}[\![\mathsf{s}]\!]\,\mathcal{R}_0\,(\prod_{\ell' \in \mathsf{labs}[\![\mathsf{s}]\!]} \mathcal{X}_{\ell'})\,\ell \\ \\ \ell \in \mathsf{labs}[\![\mathsf{s}]\!] \end{cases}$$

— The upper continuity of these equations follows pointwise from the continuity of each equation $\mathcal{X} \mapsto \mathsf{E}[\![\mathsf{P}]\!]\,\mathcal{R}_0\,\mathcal{X}\,\ell$, $\ell \in \mathsf{labs}[\![\mathsf{P}]\!]$ which itself follows from

- the continuity of the identity and constant function,
- of the primitives of the abstract domain (including the join) in Definition 21.1,
- of the conditional with continuous alternatives, and
- the fact that the composition of continuous functions is continuous.

Proof of Theorem 23.20 — II

— The fact that there is one equation per program label is proved by structural induction.

- For the basis, this is true for the assignment, empty statement list, skip, and break statement.
- For the induction step,
  - for a program component made of several subcomponents, this remains true, by structural induction, for disjoint labels;
  - moreover, when a label is shared between subcomponents their equations are regrouped into one single equation.

Proof of Theorem 23.20 — III

For example, for the statement list $\mathtt{Sl} ::= \mathtt{Sl}'\ \mathtt{S}$, $\mathtt{Sl}' \neq \epsilon$,

- the equations $\widehat{\mathscr{E}}^{\,\natural}[\![\mathtt{Sl}']\!]\mathcal{R}_0$ and $\widehat{\mathscr{E}}^{\,\natural}[\![\mathtt{S}]\!]\mathcal{R}_0$ share, by definition of labs in Section **4.2.7**, only one common variable $\mathcal{X}_{\mathsf{after}[\![\mathtt{Sl}']\!]} = \mathcal{X}_{\mathsf{at}[\![\mathtt{S}]\!]}$
- the equation $\mathcal{X}_{\mathsf{after}[\![\mathtt{Sl}']\!]} = \mathrm{RHS}'$ for $\mathtt{Sl}'$ and the equation $\mathcal{X}_{\mathsf{at}[\![\mathtt{S}]\!]} = \mathrm{RHS}$ for $\mathtt{S}$ are grouped into a single equation $\mathcal{X}_{\mathsf{at}[\![\mathtt{S}]\!]} = \mathrm{RHS}' \sqcup^{\natural} \mathrm{RHS}$ for $\mathtt{Sl}$.
- so, by (23.10), the system of equation for $\mathtt{Sl} ::= \mathtt{Sl}'\ \mathtt{S}$ has exactly one equation for each program point of $\mathtt{Sl}$

The reasoning is the same for the conditional, iteration, *etc*.

Proof of Theorem 23.20 — IV

— It remains to prove that the equations $\widehat{\mathscr{E}}^{\,\natural}[\![\mathsf{S}]\!]\,\mathcal{R}_0$ for a statement S have a least pointwise fixpoint equal to the structural abstract semantics defined in Section **21.2**

$$\mathrm{lfp}^{\dot{\subseteq}^{\natural}}\, \mathsf{E}[\![\mathsf{P}]\!]\,\mathcal{R}_0 \quad = \quad \widehat{\mathcal{S}}^{\,\natural}[\![\mathsf{P}]\!]\,\mathcal{R}_0$$

— The proof is by structural induction

Proof of Theorem 23.20 — V

— For the basis, consider the assignment, (23.7) the equations are

$$\{\mathcal{X}_{\mathsf{at}[\![\mathsf{s}]\!]} = \mathcal{R}_0, \mathcal{X}_{\mathsf{after}[\![\mathsf{s}]\!]} = \mathsf{assign}^{\natural}[\![\mathsf{x}, \mathsf{E}]\!]\, \mathcal{X}_{\mathsf{at}[\![\mathsf{s}]\!]}\}$$

The unique solution (hence $\dot{\sqsubseteq}^{\natural}$-solution) is

$$\mathcal{S}_{\mathsf{at}[\![\mathsf{s}]\!]} = \mathcal{R}_0, \quad \mathcal{S}_{\mathsf{after}[\![\mathsf{s}]\!]} = \mathsf{assign}^{\natural}[\![\mathsf{x}, \mathsf{E}]\!]\, \mathcal{R}_0$$

and, by convention, $\mathcal{S}_\ell = \bot^{\natural}$ when $\ell \notin \{\mathsf{at}[\![\mathsf{S}]\!], \mathsf{after}[\![\mathsf{S}]\!]\}$.
By (21.7), this solution is

$$\mathcal{S} = \widehat{\mathcal{S}}^{\natural}[\![\mathsf{S}]\!]\, \mathcal{R}_0$$

The proof is similar for an empty statement list (23.11), a skip statement (23.6), a break statement (23.13), and it is trivial, by structural induction, for a compound statement (23.14).

Proof of Theorem 23.20 — VI

For the induction step of the proof.

— The equations for a program $\mathtt{P} ::= \mathtt{Sl}\ \ell'$ are the same as those for the statement list $\mathtt{Sl}$ since $\mathsf{labs}[\![\mathtt{P}]\!] = \mathsf{in}[\![\mathtt{Sl}]\!] \cup \{\mathsf{after}[\![\mathtt{Sl}]\!]\}$.

- By structural induction the equations $\widehat{\mathscr{E}}^{\,\natural}[\![\mathtt{Sl}]\!]$ have solution $\mathscr{S} = \widehat{\mathscr{S}}^{\,\natural}[\![\mathtt{Sl}]\!]\,\mathcal{R}_0$
- So the solution is the same for the program in accordance with (21.4).

— For the statement list $\mathtt{Sl} ::= \epsilon\ \mathtt{S}$, reduced to a statement $\mathtt{S}$, the result directly follows from $\mathsf{in}[\![\mathtt{Sl}]\!] = \mathsf{in}[\![\mathtt{S}]\!]$ and $\mathsf{after}[\![\mathtt{Sl}]\!] = \mathsf{after}[\![\mathtt{S}]\!]$, (21.5), (23.10), and the induction hypothesis.

Proof of Theorem 23.20 — VII

— For the statement list $\mathtt{sl} ::= \mathtt{sl}'\ \mathtt{s}$

$$\widehat{\mathscr{E}}^{\,\natural}[\![\mathtt{sl}]\!]\mathcal{R}_0 \quad = \quad \begin{array}{l}\text{let } (\{\mathcal{X}_{\mathsf{after}[\![\mathtt{sl}']\!]} = \mathrm{RHS}'\} \cup \mathcal{E}') = \widehat{\mathscr{E}}^{\,\natural}[\![\mathtt{sl}']\!]\mathcal{R}_0 \\ \quad \text{and } (\{\mathcal{X}_{\mathsf{at}[\![\mathtt{s}]\!]} = \mathrm{RHS}\} \cup \mathcal{E}) = \widehat{\mathscr{E}}^{\,\natural}[\![\mathtt{s}]\!]\mathcal{X}_{\mathsf{at}[\![\mathtt{s}]\!]} \text{ in} \\ \quad\quad \{\mathcal{X}_{\mathsf{at}[\![\mathtt{s}]\!]} = \mathrm{RHS}' \sqcup^{\natural} \mathrm{RHS}\} \cup \mathcal{E}' \cup \mathcal{E}\end{array} \tag{23.10}$$

- By induction hypothesis, the equations $\{\mathcal{X}_{\mathsf{after}[\![\mathtt{sl}']\!]} = \mathrm{RHS}'\} \cup \mathcal{E}' = \widehat{\mathscr{E}}^{\,\natural}[\![\mathtt{sl}']\!]\mathcal{R}_0$ have solution $\mathcal{S}'_{\ell'} = \widehat{\mathcal{S}}^{\,\natural}[\![\mathtt{sl}']\!]\,\mathcal{R}_0\,\ell'$ for $\ell' \in \mathsf{labs}[\![\mathtt{sl}']\!]$
- So the value of $\mathcal{X}_{\mathsf{at}[\![\mathtt{s}]\!]} = \mathcal{X}_{\mathsf{after}[\![\mathtt{sl}']\!]}$ is $\mathcal{S}'_{\mathsf{at}[\![\mathtt{s}]\!]} = \widehat{\mathcal{S}}^{\,\natural}[\![\mathtt{sl}']\!]\,\mathcal{R}_0\,\mathsf{at}[\![\mathtt{s}]\!]$.
- By induction hypothesis, the equations

$$\{\mathcal{X}_{\mathsf{at}[\![\mathtt{s}]\!]} = \mathrm{RHS}\} \cup \mathcal{E} = \widehat{\mathscr{E}}^{\,\natural}[\![\mathtt{s}]\!]\mathcal{X}_{\mathsf{at}[\![\mathtt{s}]\!]}$$

have therefore solution

$$\widehat{\mathcal{S}}^{\,\natural}[\![\mathtt{s}]\!]\,\mathcal{S}'_{\mathsf{at}[\![\mathtt{s}]\!]}\,\ell \quad = \quad \widehat{\mathcal{S}}^{\,\natural}[\![\mathtt{s}]\!]\,(\widehat{\mathcal{S}}^{\,\natural}[\![\mathtt{sl}']\!]\,\mathcal{R}_0\,\mathsf{at}[\![\mathtt{s}]\!])\,\ell \quad = \quad \widehat{\mathcal{S}}^{\,\natural}[\![\mathtt{sl}]\!]\,\mathcal{R}_0\,\ell \quad \text{by (21.5)}$$

for $\ell \in \mathsf{labs}[\![\mathtt{s}]\!]$

Proof of Theorem 23.20 — VIII

It remains to show that the equations $\{\mathcal{X}_{\mathsf{at}[\![\mathtt{S}]\!]} = \mathrm{RHS}' \sqcup^{\natural} \mathrm{RHS}\} \cup \mathcal{E}' \cup \mathcal{E} = \widehat{\mathscr{E}}^{\natural}[\![\mathtt{Sl}]\!]\mathcal{R}_0$ for $\mathtt{Sl}$ have the same solution.

- Remember that no system of equations for a program component $\mathtt{S} \in \mathbb{P}\mathrm{c}$ has any equations depending on $\mathcal{X}_{\mathsf{after}[\![\mathtt{S}]\!]}$.
- This means that a chaotic iteration strategy can solve $\mathcal{E}'$ first to get the solution $\mathcal{S}'_{\ell'} = \widehat{\mathscr{E}}^{\natural}[\![\mathtt{Sl}]\!]\mathcal{R}_0\ \ell'$ for $\mathcal{X}_{\ell'}$ when $\ell' \in \mathsf{labs}[\![\mathtt{Sl}']\!] \setminus \{\mathsf{after}[\![\mathtt{Sl}']\!]\}$.
- Then, we can calculate the value of RHS' which depends only on $\mathcal{S}'_{\ell'}$, $\ell' \in \mathsf{labs}[\![\mathtt{Sl}']\!] \setminus \{\mathsf{after}[\![\mathtt{Sl}']\!]\}$ and is

$$\widehat{\mathcal{S}}^{\natural}[\![\mathtt{Sl}']\!]\ \mathcal{R}_0\ \mathsf{after}[\![\mathtt{Sl}']\!] = \widehat{\mathcal{S}}^{\natural}[\![\mathtt{Sl}']\!]\ \mathcal{R}_0\ \mathsf{at}[\![\mathtt{S}]\!]$$

- So the chaotic iteration strategy is left with solving

$$\{\mathcal{X}_{\mathsf{at}[\![\mathtt{S}]\!]} = \widehat{\mathcal{S}}^{\natural}[\![\mathtt{Sl}']\!]\ \mathcal{R}_0\ \mathsf{at}[\![\mathtt{S}]\!] \sqcup^{\natural} \mathrm{RHS}\} \cup \mathcal{E}$$

- There are two subcases.

Proof of Theorem 23.20 — IX

– (First subcase) For all program components $\mathsf{s} \in \mathcal{PC}$ but the iteration,

- The equations $\widehat{\mathscr{E}}^{\,\natural}[\![\mathsf{s}]\!]\,\mathcal{R}_0$ have an entry equation of the form $\mathcal{X}_{\mathsf{at}[\![\mathsf{s}]\!]} = \mathcal{R}_0$.
- Therefore, $\mathcal{X}_{\mathsf{at}[\![\mathsf{s}]\!]} = \mathrm{RHS}$ is $\mathcal{X}_{\mathsf{at}[\![\mathsf{s}]\!]} = \mathcal{X}_{\mathsf{after}[\![\mathsf{s}\mathfrak{l}']\!]}$.
- Then the equations $\{\mathcal{X}_{\mathsf{at}[\![\mathsf{s}]\!]} = \widehat{\mathcal{S}}^{\,\natural}[\![\mathsf{s}\mathfrak{l}']\!]\,\mathcal{R}_0\,\mathsf{at}[\![\mathsf{s}]\!] \sqcup^{\natural} \mathrm{RHS}\} \cup \mathcal{E}$ are

  $$\{\mathcal{X}_{\mathsf{at}[\![\mathsf{s}]\!]} = \widehat{\mathcal{S}}^{\,\natural}[\![\mathsf{s}\mathfrak{l}']\!]\,\mathcal{R}_0\,\mathsf{at}[\![\mathsf{s}]\!] \sqcup^{\natural} \mathcal{X}_{\mathsf{after}[\![\mathsf{s}\mathfrak{l}']\!]}\} \cup \mathcal{E}$$

  that is $\{\mathcal{X}_{\mathsf{at}[\![\mathsf{s}]\!]} = \widehat{\mathcal{S}}^{\,\natural}[\![\mathsf{s}\mathfrak{l}']\!]\,\mathcal{R}_0\,\mathsf{at}[\![\mathsf{s}]\!] \sqcup^{\natural} \mathcal{X}_{\mathsf{at}[\![\mathsf{s}]\!]}\} \cup \mathcal{E}$,
- Their least solution is, by def. of the lub, the same as

  $$\{\mathcal{X}_{\mathsf{at}[\![\mathsf{s}]\!]} = \widehat{\mathcal{S}}^{\,\natural}[\![\mathsf{s}\mathfrak{l}']\!]\,\mathcal{R}_0\,\mathsf{at}[\![\mathsf{s}]\!]\} \cup \mathcal{E}$$

  which we have shown to have solution

  $$\widehat{\mathcal{S}}^{\,\natural}[\![\mathsf{s}]\!]\,(\widehat{\mathcal{S}}^{\,\natural}[\![\mathsf{s}\mathfrak{l}']\!]\,\mathcal{R}_0\,\mathsf{at}[\![\mathsf{s}]\!])\,\ell \quad = \quad \widehat{\mathcal{S}}^{\,\natural}[\![\mathsf{s}\mathfrak{l}]\!]\,\mathcal{R}_0\,\ell, \qquad \ell \in \mathsf{labs}[\![\mathsf{s}]\!]$$

Proof of Theorem 23.20 — X

– (Second subcase) Otherwise, $\mathtt{S} ::= \mathtt{while}^{\ell}\ \mathtt{(B)}\ \mathtt{S}_b$ is an iteration.

- By (23.12), the entry equation is $\mathcal{X}_{\mathsf{at}[\![\mathtt{S}]\!]} = \mathcal{X}_{\mathsf{after}[\![\mathtt{Sl}']\!]} \sqcup^{\natural} \mathrm{RHS}''$ where
$$\{\mathcal{X}_{\mathsf{at}[\![\mathtt{S}]\!]} = \mathrm{RHS}''\} \cup \mathcal{E}'' = \widehat{\mathscr{E}}^{\natural}[\![\mathtt{S}_b]\!](\mathsf{test}^{\natural}[\![\mathtt{B}]\!]\mathcal{X}_{\mathsf{at}[\![\mathtt{S}]\!]})$$
(where $\mathsf{after}[\![\mathtt{Sl}']\!] = \mathsf{at}[\![\mathtt{S}]\!] = \mathsf{after}[\![\mathtt{S}_b]\!]$ is the iteration label).
- So $\mathrm{RHS} = \mathcal{X}_{\mathsf{after}[\![\mathtt{Sl}']\!]} \sqcup^{\natural} \mathrm{RHS}''$ and the chaotic iterations are left to solve
$$\{\mathcal{X}_{\mathsf{at}[\![\mathtt{S}]\!]} = \widehat{\mathscr{S}}^{\natural}[\![\mathtt{Sl}']\!]\,\mathcal{R}_0\,\mathsf{at}[\![\mathtt{S}]\!] \sqcup^{\natural} \mathrm{RHS}\} \cup \mathcal{E}$$
that is
$$\{\mathcal{X}_{\mathsf{at}[\![\mathtt{S}]\!]} = \widehat{\mathscr{S}}^{\natural}[\![\mathtt{Sl}']\!]\,\mathcal{R}_0\,\mathsf{at}[\![\mathtt{S}]\!] \sqcup^{\natural} \mathcal{X}_{\mathsf{after}[\![\mathtt{Sl}']\!]} \sqcup^{\natural} \mathrm{RHS}''\} \cup \mathcal{E}$$
which simplifies to
$$\{\mathcal{X}_{\mathsf{at}[\![\mathtt{S}]\!]} = \widehat{\mathscr{S}}^{\natural}[\![\mathtt{Sl}']\!]\,\mathcal{R}_0\,\mathsf{at}[\![\mathtt{S}]\!] \sqcup^{\natural} \mathrm{RHS}''\} \cup \mathcal{E}$$
since the solution to $\mathcal{X}_{\mathsf{after}[\![\mathtt{Sl}']\!]}$ is $\widehat{\mathscr{S}}^{\natural}[\![\mathtt{Sl}']\!]\,\mathcal{R}_0\,\mathsf{at}[\![\mathtt{S}]\!]$ and $\sqcup^{\natural}$ is idempotent.
- This is exactly the equations $\widehat{\mathscr{E}}^{\natural}[\![\mathtt{S}]\!]\mathcal{X}_{\mathsf{at}[\![\mathtt{S}]\!]}$ which we have shown to have solution $\widehat{\mathscr{S}}^{\natural}[\![\mathtt{S}]\!]\,(\widehat{\mathscr{S}}^{\natural}[\![\mathtt{Sl}']\!]\,\mathcal{R}_0\,\mathsf{at}[\![\mathtt{S}]\!])\,\ell = \widehat{\mathscr{S}}^{\natural}[\![\mathtt{Sl}]\!]\,\mathcal{R}_0\,\ell$ for $\ell \in \mathsf{labs}[\![\mathtt{S}]\!]$.
- By Theorem 22.4, all chaotic iterations are equivalent and yields the least fixpoint proving that, in case of a statement list, $\mathsf{lfp}^{\dot{\sqsubseteq}^{\natural}}\,\widehat{\mathscr{E}}^{\natural}[\![\mathtt{Sl}]\!]\,\mathcal{R}_0 = \widehat{\mathscr{S}}^{\natural}[\![\mathtt{Sl}]\!]\,\mathcal{R}_0$.

Proof of Theorem 23.20 — XI

— The proof for the conditionals (23.8) and (23.9) is very similar.

Proof of Theorem 23.20 — XII

— For the iteration $\mathtt{S} ::= \mathtt{while}^{\ell}\ \mathtt{(B)}\ \mathtt{S}_b$ (23.12), the Jacobi calculation of the least fixpoint $\widehat{\mathscr{S}}^{\natural}[\![\mathtt{S}]\!]\,\mathcal{R}_0 \;=\; \mathrm{lfp}^{\sqsubseteq}(\mathscr{F}^{\natural}[\![\mathtt{while}^{\ell}\ \mathtt{(B)}\ \mathtt{S}_b]\!]\,\mathcal{R}_0)$ corresponds to a specific chaotic iteration strategy for the loop equations

$$\begin{array}{rcl}
\widehat{\mathscr{E}}^{\natural}[\![\mathtt{S}]\!]\,\mathcal{R}_0 & = & \mathsf{let}\,(\{\mathcal{X}_{\mathsf{at}[\![\mathtt{S}]\!]} = E\} \cup \mathcal{E}) = \widehat{\mathscr{E}}^{\natural}[\![\mathtt{S}_b]\!](\mathsf{test}^{\natural}[\![\mathtt{B}]\!]\mathcal{X}_{\mathsf{at}[\![\mathtt{S}]\!]})\ \mathsf{in} \\
& & \quad \{\mathcal{X}_{\mathsf{at}[\![\mathtt{S}]\!]} = \mathcal{R}_0 \sqcup^{\natural} E\} \cup \\
& & \quad \mathcal{E} \cup \\
& & \quad \{\mathcal{X}_{\mathsf{after}[\![\mathtt{S}]\!]} = \overline{\mathsf{test}}^{\natural}[\![\mathtt{B}]\!]\mathcal{X}_{\mathsf{at}[\![\mathtt{S}]\!]} \sqcup^{\natural} \bigsqcup_{\ell \in \mathsf{breaks\text{-}of}[\![\mathtt{S}_b]\!]}^{\natural} \mathcal{X}_{\ell}\}
\end{array} \qquad (23.12)$$

where the equations $\widehat{\mathscr{E}}^{\natural}[\![\mathtt{S}_b]\!](\mathsf{test}^{\natural}[\![\mathtt{B}]\!]\mathcal{X}_{\mathsf{at}[\![\mathtt{S}]\!]})$ for the loop body are solved by iteration before considering another iteration of the loop fixpoint $\widehat{\mathscr{E}}^{\natural}[\![\mathtt{S}]\!]\,\mathcal{R}_0$.

Proof of Theorem 23.20 — XIII

More precisely, by (21.11), $\widehat{\mathcal{S}}^{\natural}[\![\mathtt{S}]\!]\,\mathcal{R}_0$ is the least solution to the system of equations

$$\begin{cases} X(\ell') & = & \mathcal{F}^{\natural}[\![\mathtt{while}\ \ell\ \mathtt{(B)}\ \mathtt{S}_b]\!]\,\mathcal{R}_0\,X\,\ell' \\ \ell' \in \mathsf{labs}[\![\mathtt{S}]\!] \end{cases}$$

(where $\mathsf{labs}[\![\mathtt{S}]\!] = \mathsf{labs}[\![\mathtt{S}_b]\!] \cup \{\mathsf{after}[\![\mathtt{S}]\!]\}$ for iteration) that is

$$\begin{cases} X(\ell') & = & (\!|\ \ell' = \ell\ ?\ \mathcal{R}_0 \sqcup^{\natural} \widehat{\mathcal{S}}^{\natural}[\![\mathtt{S}_b]\!]\,(\mathsf{test}^{\natural}[\![\mathtt{B}]\!]X(\ell))\,\ell \\ & & \ |\ \ell' \in \mathsf{in}[\![\mathtt{S}_b]\!] \setminus \{\ell\}\ ?\ \widehat{\mathcal{S}}^{\natural}[\![\mathtt{S}_b]\!]\,(\mathsf{test}^{\natural}[\![\mathtt{B}]\!]X(\ell))\,\ell' \\ & & \ |\ \ell' = \mathsf{after}[\![\mathtt{S}]\!]\ ?\ \overline{\mathsf{test}}^{\natural}[\![\mathtt{B}]\!]X(\ell) \sqcup^{\natural} \bigsqcup_{\ell'' \in \mathsf{breaks\text{-}of}[\![\mathtt{S}_b]\!]}^{\natural} \widehat{\mathcal{S}}^{\natural}[\![\mathtt{S}_b]\!]\,(\mathsf{test}^{\natural}[\![\mathtt{B}]\!]X(\ell))\,\ell'' \\ & & \ :\ \bot^{\natural}\ |\!) \\ \ell' \in \mathsf{labs}[\![\mathtt{S}]\!] \end{cases} \qquad \text{(a)}$$

We let X^k, $k \in \mathbb{N}$ be the Jacobi iterations for this system of equations (a).

Proof of Theorem 23.20 — XIV

- Let
$$\{\mathcal{X}_{\mathsf{at}[\![\mathtt{s}]\!]} = \mathrm{RHS}\} \cup \mathcal{E} = \widehat{\mathscr{E}}^{\,\natural}[\![\mathtt{s}_b]\!](\mathsf{test}^{\natural}[\![\mathtt{B}]\!]\mathcal{X}_{\mathsf{at}[\![\mathtt{s}]\!]})$$
be the equations of the loop body $\mathtt{s}_b$.
- By (23.12), the equations $\widehat{\mathscr{E}}^{\,\natural}[\![\mathtt{S}]\!]\,\mathcal{R}_0$ for the iteration $\mathtt{S} ::= \mathtt{while}^{\,\ell}\ \mathtt{(B)}\ \mathtt{s}_b$ are
$$\{\mathcal{X}_{\mathsf{at}[\![\mathtt{s}]\!]} = \mathcal{R}_0 \sqcup^{\natural} \mathrm{RHS}\} \cup \mathcal{E} \cup \{\mathcal{X}_{\mathsf{after}[\![\mathtt{s}]\!]} = \overline{\mathsf{test}}^{\natural}[\![\mathtt{B}]\!]\mathcal{X}_{\mathsf{at}[\![\mathtt{s}]\!]} \sqcup^{\natural} \bigsqcup_{\ell \in \mathsf{breaks\text{-}of}[\![\mathtt{s}_b]\!]}^{\natural} \mathcal{X}_\ell\} \qquad \text{(b)}$$
- We consider a chaotic iteration (generalized to transfinite iteration [P. Cousot, 1977, 1978]) for these equations (b) with a subsequence $\mathcal{X}^k$, $k \in \mathbb{N}$ defined as follows.

Proof of Theorem 23.20 — XV

- The initialization is the infimum $\mathcal{X}^0 = X^0 = \bot$;
- Assume, by recurrence hypothesis, that $\mathcal{X}^k = X^k$;
- We next iterate the subequations

$$\{\mathcal{X}_{\mathsf{at}[\![\mathsf{S}]\!]} = \mathcal{R}_0 \sqcup^\natural \mathrm{RHS}\} \cup \mathcal{E}$$

  in (b) and pass to the limit.
  - By $\mathcal{R}_0 \sqsubseteq^\natural \mathcal{X}^k_{\mathsf{at}[\![\mathsf{S}]\!]}$ the limit is the least solution to $\widehat{\mathscr{E}}^\natural[\![\mathsf{S}_b]\!](\mathsf{test}^\natural[\![\mathsf{B}]\!]\mathcal{X}^k_{\mathsf{at}[\![\mathsf{S}]\!]})$
  - By structural induction, it is $\widehat{\mathscr{S}}^\natural[\![\mathsf{S}_b]\!]\,(\mathsf{test}^\natural[\![\mathsf{B}]\!]\mathcal{X}^k(\mathsf{at}[\![\mathsf{S}]\!])) = \widehat{\mathscr{S}}^\natural[\![\mathsf{S}_b]\!]\,(\mathsf{test}^\natural[\![\mathsf{B}]\!]X^k(\mathsf{at}[\![\mathsf{S}]\!]))$ since $\mathcal{X}^k = X^k$ by recurrence hypothesis.
- Then we do a Jacobi iteration on the remaining equations in (b) which is then exactly the same as the Jacobi iteration in (a) so we get $\mathcal{X}^{k+1} = X^{k+1}$.

Proof of Theorem 23.20 — XVI

- By recurrence, $\forall k \in \mathbb{N} \,.\, \mathcal{X}^k = X^k$
- So the infinite increasing chaotic iterations for (b) contains as a subsequence the infinite increasing Jacobi iteration for (a)
- So the limits are the same (see Exercise 10.11) that is, by Theorem 22.4 and (21.11), $\widehat{\mathcal{S}}^{\,\natural}[\![\mathsf{s}]\!]\,\mathcal{R}_0$. □

Constraints

Constraints versus equations

- Many static program analysis methods solve inequations instead of equations (*e.g.* [P. Cousot and R. Cousot, 1995; Heintze and Jaffar, 1994]).
- This follows from the fact that the least solution $\mathrm{lfp}^{\dot{\sqsubseteq}}\, \vec{F}$ to the system of equations $\vec{X} = \vec{F}(\vec{X})$ that is

$$\left\{ \begin{array}{l} X_i \quad = \quad F_i(X_1, \ldots, X_n) \\ \mathrm{i}{=}1, \ldots, \mathrm{n} \end{array} \right.$$

on the cartesian product $\vec{D} = \prod_{i=1}^{n} D_i$ of complete lattices $\langle D_i, \sqsubseteq_i \rangle, i = 1, \ldots, n$, $n \geqslant 1$ ordered pointwise is also, by Tarski's fixpoint Theorem 15.6, the least solution to the inequations $\vec{F}(\vec{X}) \mathrel{\dot{\sqsubseteq}} \vec{X}$ that is

$$\left\{ \begin{array}{l} F_i(X_1, \ldots, X_n) \quad \sqsubseteq_i \quad X_i. \\ \mathrm{i}{=}1, \ldots, \mathrm{n} \end{array} \right.$$

Constraints versus equations

- It is trivial to modify Section **22** to generate such inequations from the program text.
- When the complete lattices $\langle D_i, \sqsubseteq_i \rangle, i = 1, \ldots, n$ are powersets,
  - $\{x\} \subseteq X$ can be rewritten $x \in X$,
  - $X \cup Y \subseteq Z$ as $X \subseteq Z \wedge Y \subseteq Z$,
  - $X \subseteq Y$ as $\forall x \in X \,.\, x \in Y$, *etc*.
- Solving such inequations is a problem that looks like quite different from solving equations iteratively, but it is not!
- Static analysis by constraint resolution fits perfectly in the abstract interpretation framework.

Conclusion

Conclusion on the structural equational semantics

- The understanding of static program analysis as solving fixpoint equations associated to the program (graph) dates back from the origin of dataflow analysis [Allen, 1971; Cocke and Schwartz, 1969, Second revised version, April 1970].
- This point of view is much broader and applies equally well to semantics, verification, and static analysis.
- We give more importance to the functional semantics $\widehat{\mathcal{S}}^{\natural}[\![\mathsf{s}]\!]$ over the equational semantics $\widehat{\mathscr{E}}^{\natural}[\![\mathsf{s}]\!]$ because we prefer to reason on the solution $\widehat{\mathcal{S}}^{\natural}[\![\mathsf{s}]\!]$ of the equations rather than on the equations $\widehat{\mathscr{E}}^{\natural}[\![\mathsf{s}]\!]$.
- The abstract interpreter $\widehat{\mathcal{S}}^{\natural}[\![\mathsf{s}]\!]$ is simpler, can be reasoned upon by structural induction, and does not introduce an intermediate step of building equations before solving them.
- However, $\mathcal{X} = \mathscr{F}^{\natural}(\mathcal{X})$, $\mathscr{F}^{\natural}(\mathcal{X}) \sqsubseteq^{\natural} \mathcal{X}$ and $\mathsf{lfp}^{\sqsubseteq^{\natural}} \mathscr{F}^{\natural}$ are perfectly interchangeable since they only depend on the choice of the abstract domain of Definition 21.1 and its soundness (and completeness) of Definition 27.1.

Bibliography I

Allen, Frances E. (1971). "A Basis for Program Optimization". In: *IFIP Congress (1)*, pp. 385–390.

Bourdoncle, François (1993). "Efficient chaotic iteration strategies with widenings". In: *Formal Methods in Programming and Their Applications*. Vol. 735. Lecture Notes in Computer Science. Springer, pp. 128–141.

Cocke, John and Jacob T. Schwartz (1969, Second revised version, April 1970). *Programming languages and their compilers : preliminary notes*. Courant Institute of Mathematical Sciences, New York University, New York, USA.

Cousot, Patrick (Sept. 1977). *Asynchronous iterative methods for solving a fixed point system of monotone equations in a complete lattice*. Tech. rep. R.R. 88. 15 p. Grenoble, France: Laboratoire IMAG, Université scientifique et médicale de Grenoble.

Bibliography II

Cousot, Patrick (Mar. 21, 1978). "Méthodes itératives de construction et d'approximation de points fixes d'opérateurs monotones sur un treillis, analyse sémantique de programmes (in French)". Thèse d'État ès sciences mathématiques. Grenoble, France: Université de Grenoble Alpes.

Cousot, Patrick and Radhia Cousot (1995). "Formal Language, Grammar and Set-Constraint-Based Program Analysis by Abstract Interpretation". In: *FPCA*. ACM, pp. 170–181.

Cousot, Patrick, Radhia Cousot, Francesco Logozzo, and Michael Barnett (2012). "An abstract interpretation framework for refactoring with application to extract methods with contracts". In: *OOPSLA*. ACM, pp. 213–232.

Hecht, Matthew S. (1977). *Global data flow analysis of computer programs*. Elsevier North-Holland Pub. Co.

Bibliography III

Heintze, Nevin and Joxan Jaffar (1994). "Set Constraints and Set-Based Analysis". In: *PPCP*. Vol. 874. Lecture Notes in Computer Science. Springer, pp. 281–298.

Tarjan, Robert Endre (1972). "Depth-First Search and Linear Graph Algorithms". *SIAM J. Comput.* 1.2, pp. 146–160.

Home work

Read Ch. **23** "Abstract equational semantics" of

Principles of Abstract Interpretation
Patrick Cousot
MIT Press

The End, Thank you