

Motivations

« Basic Concepts of Abstract Interpretation »

Patrick Cousot

École normale supérieure
45 rue d'Ulm
75230 Paris cedex 05, France

Patrick.Cousot@ens.fr
www.di.ens.fr/~cousot

IFIP WCC — Topical day on Abstract Interpretation

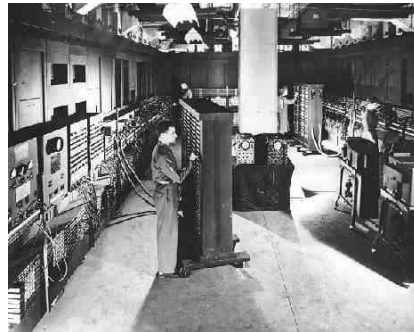
What is (or should be) the essential
preoccupation of computer scientists?

What is (or should be) the essential preoccupation of computer scientists?

The production of reliable software, its maintenance and safe evolution year after year (up to 20 even 30 years).

Computer hardware change of scale

The 25 last years, computer hardware has seen its performances multiplied by 10^4 to $10^6/10^9$;



ENIAC (5000 flops)



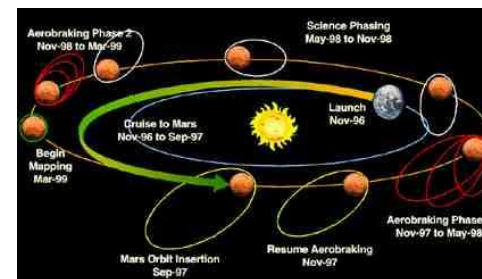
Intel/Sandia Teraflops System (10^{12} flops)

— 5 —

The information processing revolution

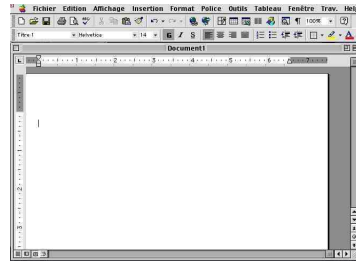
A scale of 10^6 is typical of a significant **revolution**:

- **Energy**: nuclear power station / Roman slave;
- **Transportation**: distance Earth — Mars / Paris — Toulouse



Computer software change of scale

- The size of the programs executed by these computers has grown up in similar proportions;
- **Example 1** (modern text editor for the general public):
 - > 1 700 000 lines of C¹;
 - 20 000 procedures;
 - 400 files;
 - > 15 years of development.



¹ full-time reading of the code (35 hours/week) would take at least 3 months!

Computer software change of scale (cont'd)

- Example 2 (professional computer system):
 - 30 000 000 lines of code;
 - 30 000 (known) bugs!



- 7 -

The estimated cost of an overflow

- 500 000 000 \$;
- Including indirect costs (delays, lost markets, etc):
2 000 000 000 \$;
- The financial results of Arianespace were **negative** in 2000, for the first time since 20 years.

- 9 -

Software bugs

Bugs



- whether anticipated (Y2K bug)
- or unforeseen (failure of the 5.01 flight of Ariane V launcher)
- are quite frequent;
- Bugs can be very difficult to discover in huge software;
- Bugs can have catastrophic consequences either very costly or inadmissible (embedded software in transportation systems);

Who cares?

- No one is legally responsible for bugs:
This software is distributed WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.
- So, no one cares about software verification
- And even more, one can even make money out of bugs (customers buy the next version to get around bugs in software)

Why no one cares?

- Software designers don't care because there is **no risk in writing bugged software**
- The law/judges can never enforce more than what is offered by the **state of the art**
- Automated software verification by formal methods is **undecidable** whence thought to be **impossible**
- Whence the state of the art is that **no one will ever be able to eliminate all bugs** at a reasonable price
- And so **no one ever bear any responsibility**

– 11 –

Current research results

- Research is presently changing the **state of the art** (e.g. ASTRÉE)
- We can **check for the absence of large categories of bugs** (may be not all of them but a significant portion of them)
- The verification can be made automatically by **mechanical tools**
- Some **bugs can be found completely automatically**, without any human intervention

The next step (5 years)

- If these tools are successful, their use can be enforced by quality **norms**
- Professionals have to **conform to such norms** (otherwise they are not credible)
- Because of complete tool automaticity, **no one can be discharged from the duty of applying such state of the art tools**
- Third parties of confidence can **check software a posteriori** to trace back bugs and prove responsibilities

– 13 –

A foreseeable future (10 years)

- The real take-off of software verification must be **enforced**
- **Development costs arguments** have shown to be **ineffective**
- **Norms/laws** might be much more **convincing**
- This requires **effectiveness and complete automation** (to avoid acquittal based on human capacity limitations arguments)

Why will “partial software verification” ultimately succeed?

- The **state of the art** will change toward complete automation, at least for common categories of bugs
- So **responsibilities** can be established (at least for automatically detectable bugs)
- Whence the **law** will change (by adjusting to the new state of the art)
- To ensure at least **partial software verification**
- For the **benefit** of all of us

– 15 –

Static analysis
by abstract interpretation

Example of static analysis (input)

```
n := n0;
i := n;
while (i <> 0 ) do
  j := 0;
  while (j <> i) do
    j := j + 1
  od;
  i := i - 1
od
```

– 17 –

Example of static analysis (output)

```
{n0>=0}
  n := n0;
{n0=n,n0>=0}
  i := n;
{n0=i,n0=n,n0>=0}
  while (i <> 0 ) do
    {n0=n,i>=1,n0>=i}
    j := 0;
    {n0=n,j=0,i>=1,n0>=i}
    while (j <> i) do
      {n0=n,j>=0,i>=j+1,n0>=i}
      j := j + 1
      {n0=n,j>=1,i>=j,n0>=i}
    od;
    {n0=n,i=j,i>=1,n0>=i}
    i := i - 1
    {i+1=j,n0=n,i>=0,n0>=i+1}
  od
{n0=n,i=0,n0>=0}
```

Example of static analysis (safety)

```

{n0>=0}
  n := n0;
{n0=n,n0>=0}
  i := n;
{n0=i,n0=n,n0>=0}
  while (i <> 0 ) do
    {n0=n,i>=1,n0>=i}
      j := 0;
    {n0=n,j=0,i>=1,n0>=i}
      while (j <> i) do
        {n0=n,j>=0,i>=j+1,n0>=i}
          j := j + 1
        {n0=n,j>=1,i>=j,n0>=i}
      od;
    {n0=n,i=j,i>=1,n0>=i}
      i := i - 1
    {i+1=j,n0=n,i>=0,n0>=i+1}
  od
{n0=n,i=0,n0>=0}

```

n0 must be initially nonnegative (otherwise the program does not terminate properly)

j < n0 so no upper overflow

i > 0 so no lower overflow

Static analysis by abstract interpretation

Verification: define and prove automatically a **property** of the **possible behaviors** of a complex computer program (example: program semantics);

Abstraction: the reasoning/calculus can be done on an **abstraction** of these behaviors dealing only with those elements of the behaviors related to the considered property;

Theory: abstract interpretation.

Example of static analysis

Verification: absence of runtime errors;

Abstraction: polyhedral abstraction (affine inequalities);

Theory: abstract interpretation.

A very informal introduction to the principles of abstract interpretation

Semantics

The *concrete semantics* of a program formalizes (is a mathematical model of) the set of all its possible executions in all possible execution environments.

— 21 —

Undecidability

- The concrete mathematical semantics of a program is an “infinite” mathematical object, *not computable*;
- All non trivial questions on the concrete program semantics are *undecidable*.

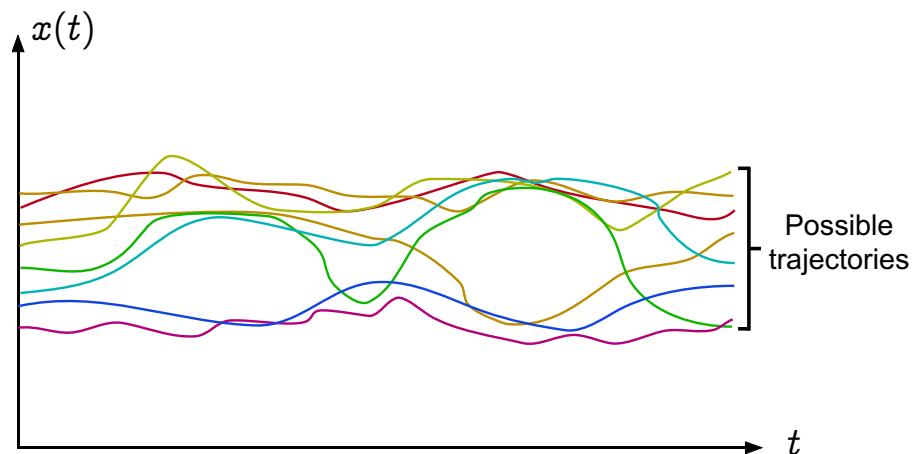
Example: termination

- Assume $\text{termination}(P)$ would always terminate and returns true iff P always terminates on all input data;
- The following program yields a contradiction

```
P ≡ while termination(P) do skip od.
```

— 23 —

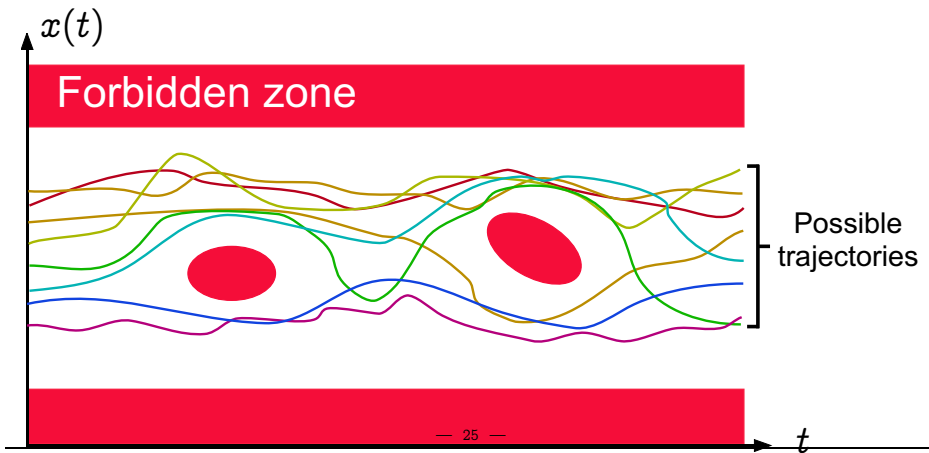
Graphic example: Possible behaviors



Graphic example: Safety properties

The *safety properties* of a program express that no possible execution in any possible execution environment can reach an erroneous state.

Graphic example: Safety property



Safety proofs

- A **safety proof** consists in proving that the intersection of the program concrete semantics and the forbidden zone is empty;
- **Undecidable** problem (the concrete semantics is not computable);
- Impossible to provide completely automatic answers with finite computer resources and neither human interaction nor uncertainty on the answer².

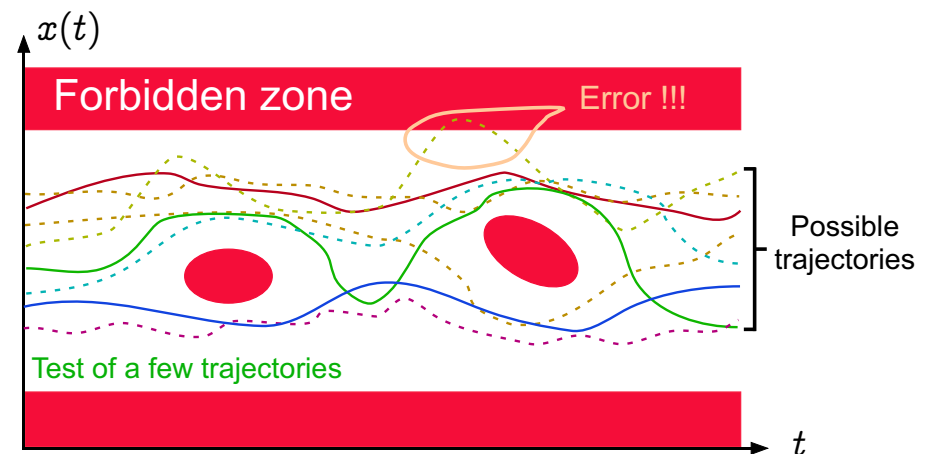
² e.g. probabilistic answer.

Test/debugging

- consists in considering a subset of the possible executions;
- not a correctness proof;
- **absence of coverage** is the main problem.

— 27 —

Graphic example: Property test/simulation



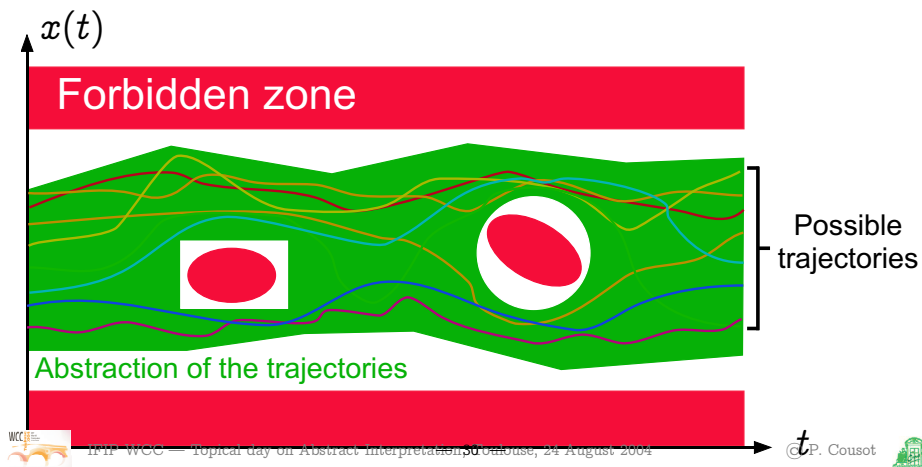
— 28 —

Abstract interpretation

- consists in considering an *abstract semantics*, that is to say a superset of the concrete semantics of the program;
- hence the abstract semantics *covers all possible concrete cases*;
- *correct*: if the abstract semantics is safe (does not intersect the forbidden zone) then so is the concrete semantics

– 29 –

Graphic example: Abstract interpretation



Formal methods

Formal methods are abstract interpretations, which differ in the way to obtain the abstract semantics:

- “*model checking*”:
 - the abstract semantics is given manually by the user;
 - in the form of a finitary model of the program execution;
 - can be computed automatically, by techniques relevant to static analysis.

– 31 –

- “*deductive methods*”:
 - the abstract semantics is specified by verification conditions;
 - the user must provide the abstract semantics in the form of inductive arguments (e.g. invariants);
 - can be computed automatically by methods relevant to static analysis.
- “*static analysis*”:
 - the abstract semantics is computed automatically from the program text according to pre-defined abstractions (that can sometimes be tailored automatically/manually by the user).

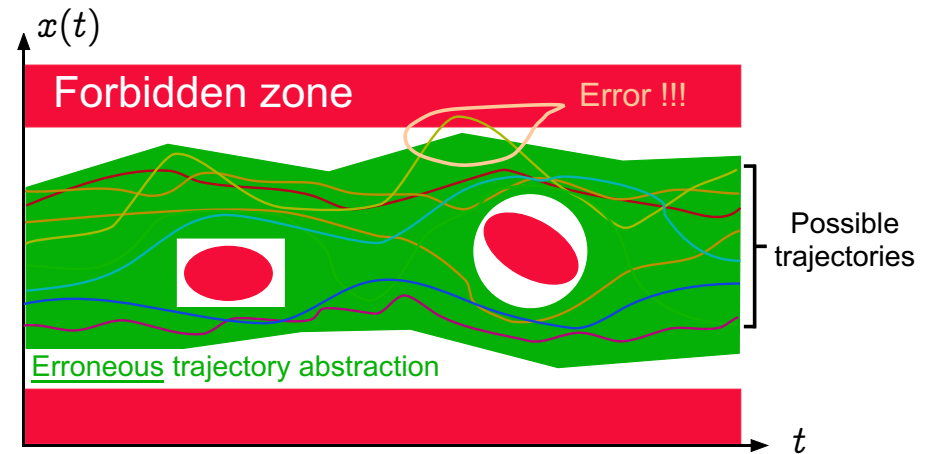
– 32 –

Required properties of the abstract semantics

- **sound** so that no possible error can be forgotten;
- **precise** enough (to avoid false alarms);
- as **simple/abstract** as possible (to avoid combinatorial explosion phenomena).

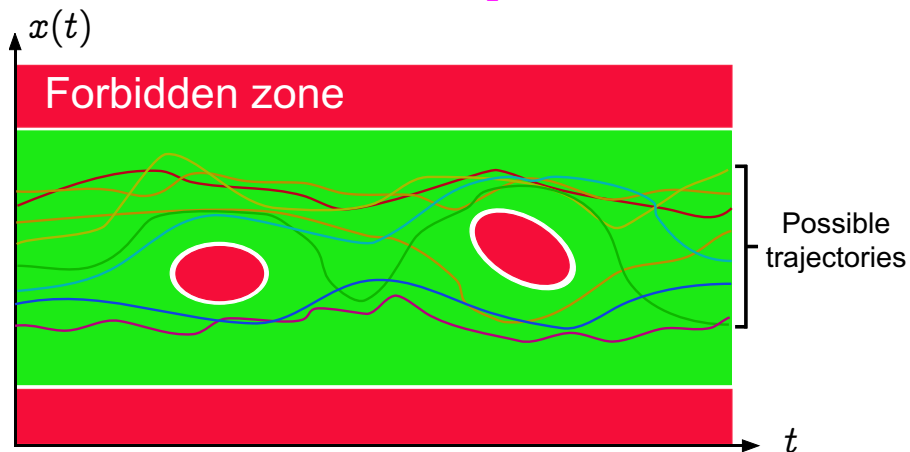
– 33 –

Graphic example: Erroneous abstraction — I

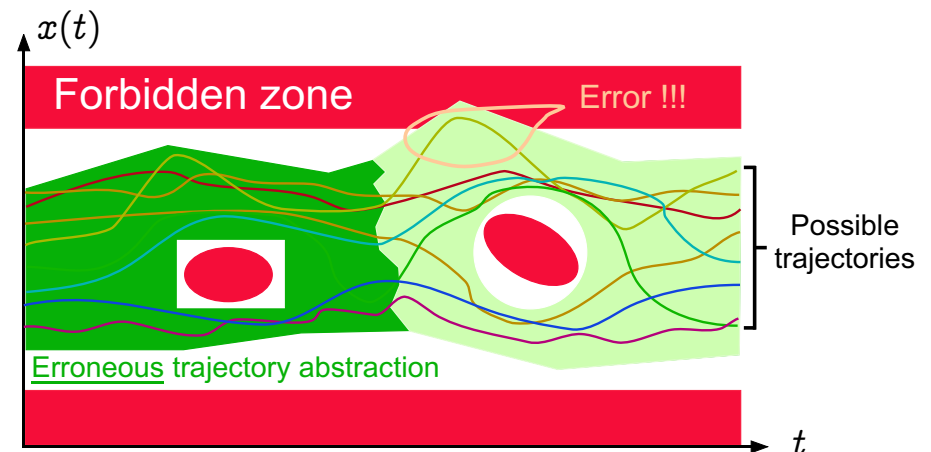


– 35 –

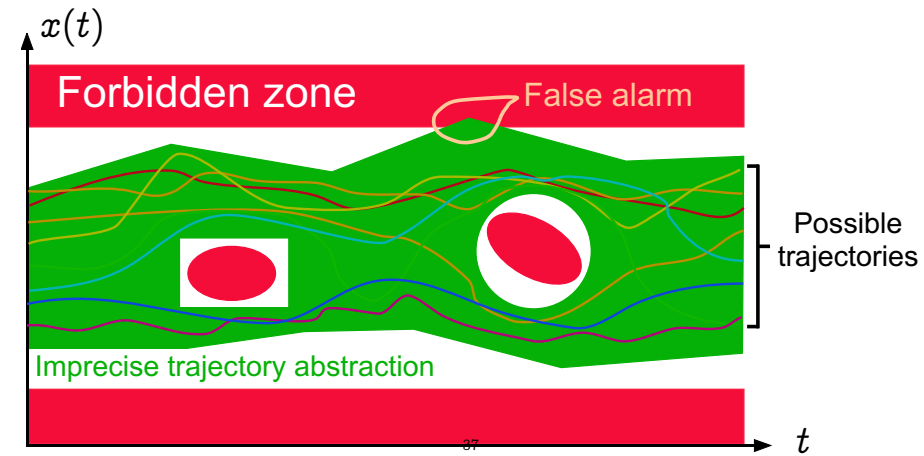
Graphic example: The most abstract correct and precise semantics



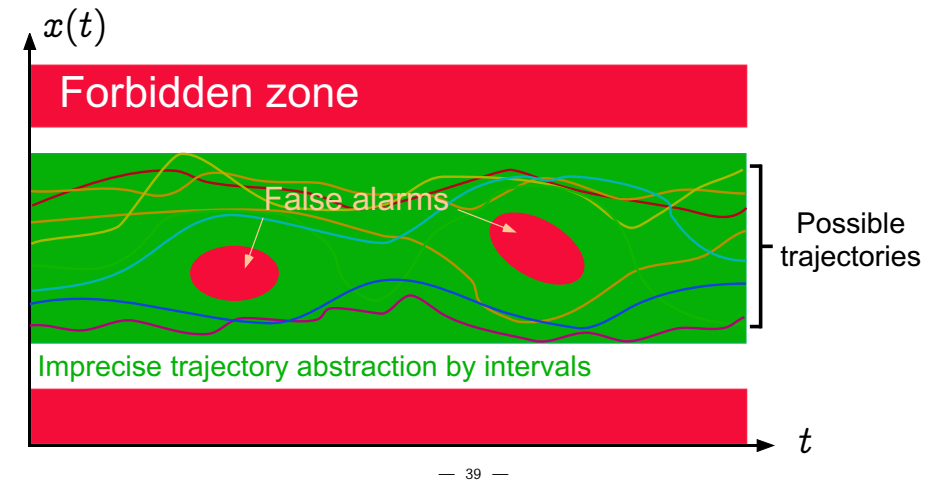
Graphic example: Erroneous abstraction — II



Graphic example: Imprecision \Rightarrow false alarms



Graphic example: Standard abstraction by intervals

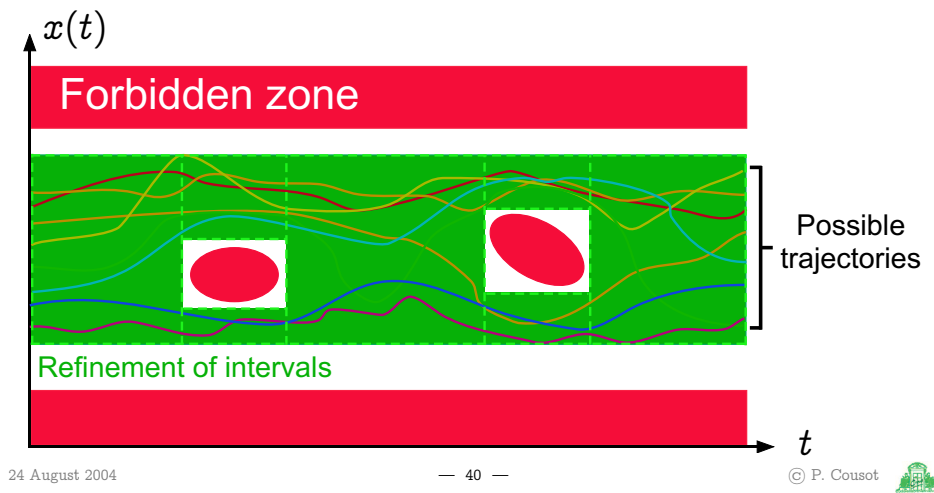


Abstract domains

Standard abstractions

- that serve as a **basis** for the design of static analyzers:
 - abstract program data,
 - abstract program basic operations;
 - abstract program control (iteration, procedure, concurrency, ...);
- can be **parametrized** to allow for manual adaptation to the application domains.

Graphic example: A more refined abstraction



Standard semantics

A very informal introduction
to static analysis
algorithms

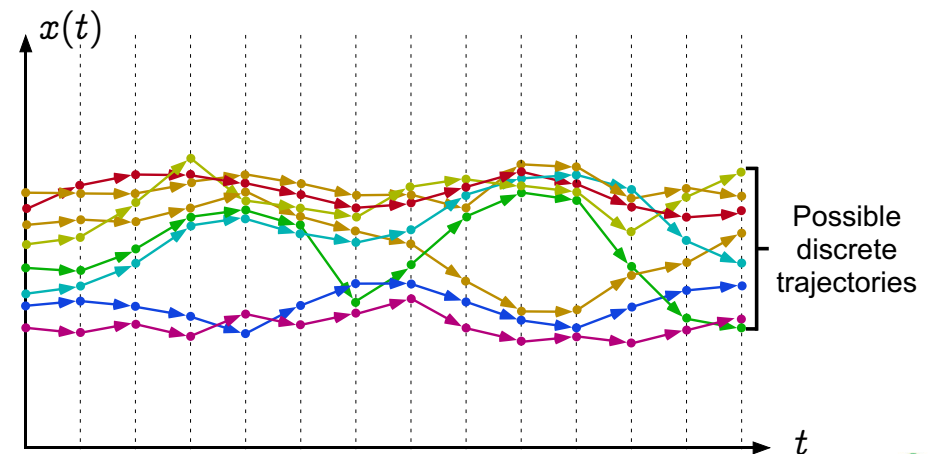
- Start from a **standard operational semantics** that describes formally:
 - **states** that is data values of program variables,
 - **transitions** that is elementary computation steps;
- Consider **traces** that is successions of states corresponding to executions described by transitions (possibly infinite).

— 43 —

— 41 —

Standard operational semantics

Graphic example: Small-steps transition semantics



24 August 2004

— 44 —

© P. Cousot

Example: Small-steps transition semantics of an assignment

```
int x;
...
l:
  x := x + 1;
l':
```

$$\{l : x = v \rightarrow l' : x = v + 1 \mid v \in [\text{min_int}, \text{max_int} - 1]\} \\ \cup \{l : x = \text{max_int} \rightarrow l' : x = \Omega\} \quad (\text{runt me error})$$

— 45 —

Example: Small-steps transition semantics of a loop

```

11: ...
11: x = -1
11: x = 0
11: x = 1
11: ...
12: x := 1;
12: while x < 10 do
13:   x := x + 1
14:
14: od
15:
14: x = 10
15: x = 10
...
14: x = 10
15: x = 10

```

Example: Trace semantics of loop

```

11: ...
11: x = -1
11: x = 0
11: x = 1
11: ...
13: x = 2
14: x = 3
...
14: x = 10
14: x = 10
15:

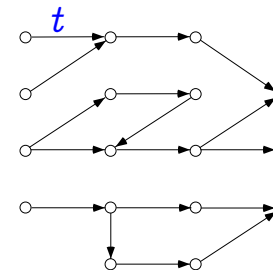
```

11: ~~x := 1;~~ →
 12: while x < 10 do
 13: x := x + 1
 14: od
 15:

— 47 —

Transition systems

- $\langle S, \overset{t}{\rightarrow} \rangle$ where:
 - S is a set of states/vertices/...
 - $\overset{t}{\rightarrow} \in \wp(S \times S)$ is a transition relation/set of arcs/...



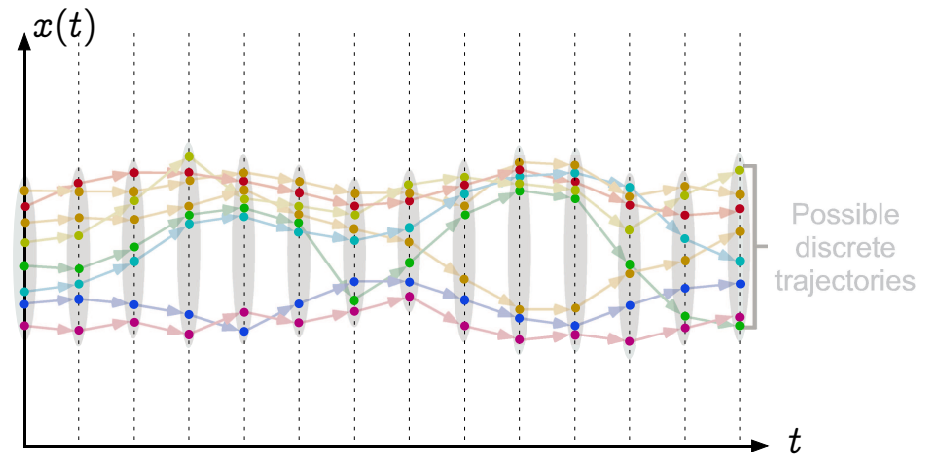
Collecting semantics in fixpoint form

— 49 —

Collecting semantics

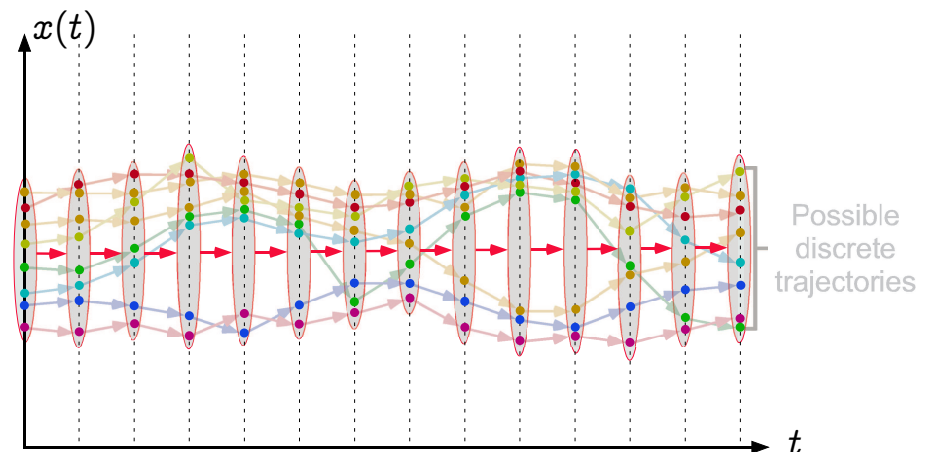
- consider all traces simultaneously;
- collecting semantics:
 - sets of states that describe data values of program variables on all possible trajectories;
 - set of states transitions that is simultaneous elementary computation steps on all possible trajectories;

Graphic example: sets of states



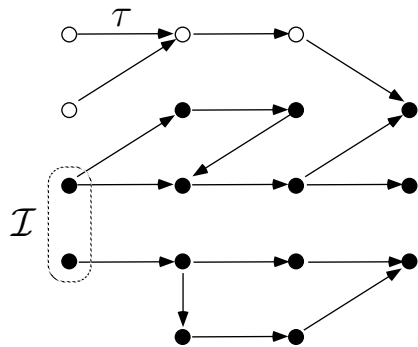
— 51 —

Graphic example: set of states transitions



— 52 —

Example: Reachable states of a transition system



— 53 —

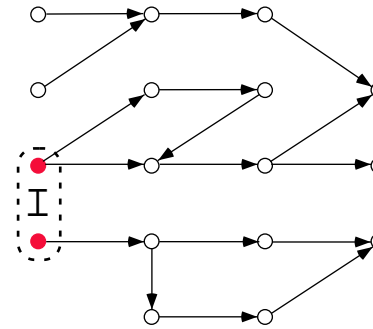
Reachable states in fixpoint form

$$F(X) = \mathcal{I} \cup \{s' \mid \exists s \in X : s \xrightarrow{t} s'\}$$

$$\mathcal{R} = \text{lfp}_{\emptyset}^{\subseteq} F$$

$$= \bigcup_{n=0}^{+\infty} F^n(\emptyset) \quad \text{where} \quad \begin{aligned} f^0(x) &= x \\ f^{n+1}(x) &= f(f^n(x)) \end{aligned}$$

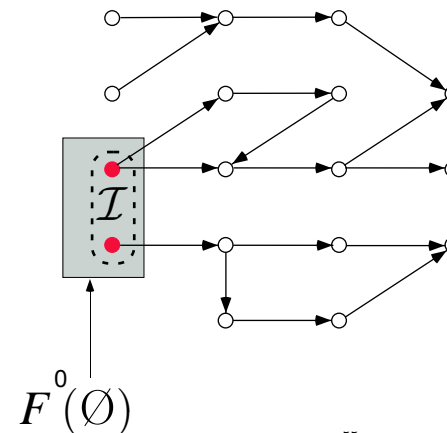
Example of fixpoint iteration for reachable states $\text{lfp}_{\emptyset}^{\subseteq} \lambda X. \mathcal{I} \cup \{s' \mid \exists s \in X : s \xrightarrow{t} s'\}$



\emptyset

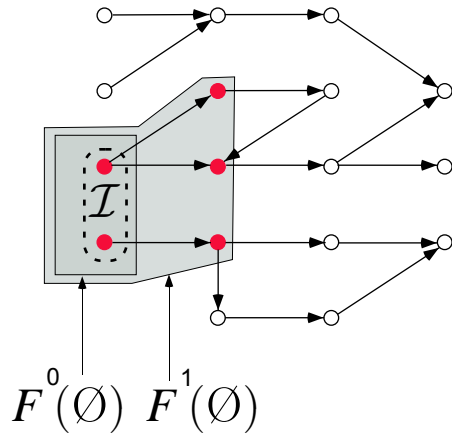
— 55 —

Example of fixpoint iteration for reachable states $\text{lfp}_{\emptyset}^{\subseteq} \lambda X. \mathcal{I} \cup \{s' \mid \exists s \in X : s \xrightarrow{t} s'\}$

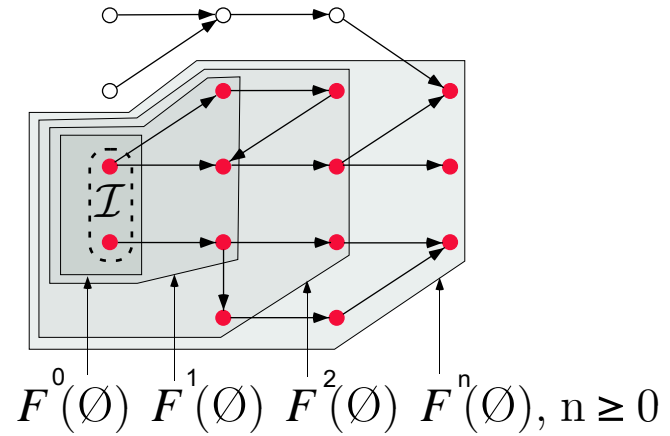


— 55 —

Example of fixpoint iteration for reachable states $\text{lfp}_{\emptyset}^{\subseteq} \lambda X. \mathcal{I} \cup \{s' \mid \exists s \in X : s \xrightarrow{t} s'\}$

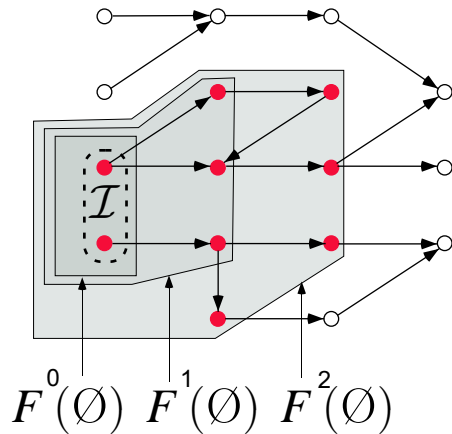


— 55 —



— 55 —

Example of fixpoint iteration
for reachable states $\text{fp}_\emptyset^{\subseteq} \lambda X. \mathcal{I} \cup \{s' \mid \exists s \in X : s \xrightarrow{t} s'\}$



— 55 —

Abstraction by Galois connections

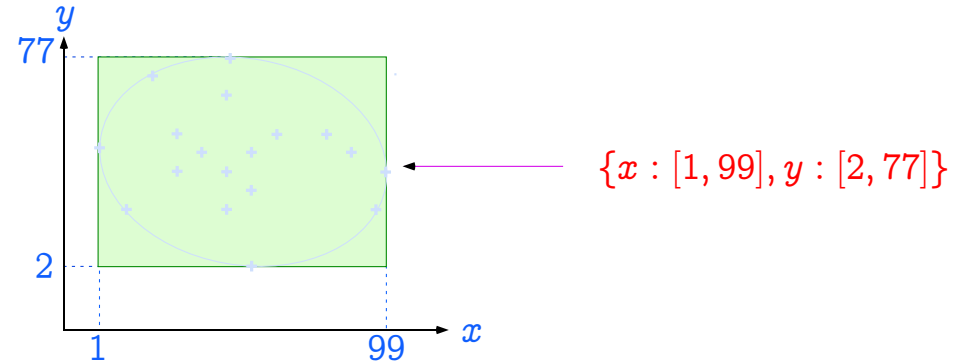
Example of fixpoint iteration
for reachable states $\text{fp}_\emptyset^{\subseteq} \lambda X. \mathcal{I} \cup \{s' \mid \exists s \in X : s \xrightarrow{t} s'\}$

Abstracting sets (i.e. properties)

- Choose an **abstract domain**, replacing sets of objects (states, traces, ...) S by their abstraction $\alpha(S)$
- The **abstraction function** α maps a set of concrete objects to its abstract interpretation;
- The inverse **concretization function** γ maps an abstract set of objects to concrete ones;
- **Forget no concrete objects**: (abstraction from above) $S \subseteq \gamma(\alpha(S))$.

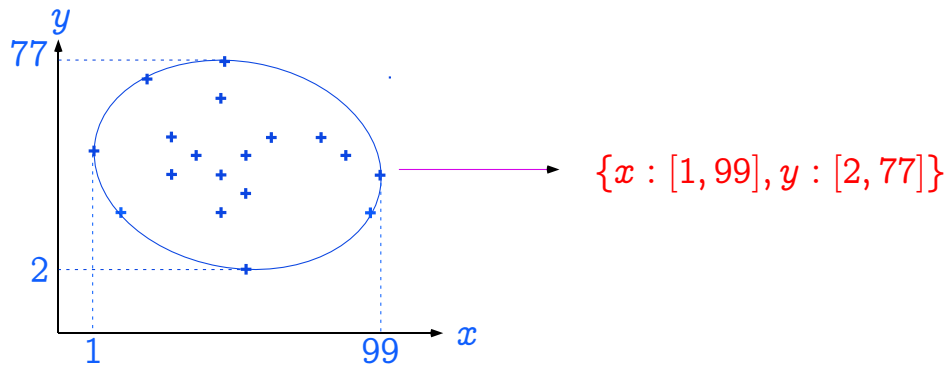
— 57 —

Interval concretization γ

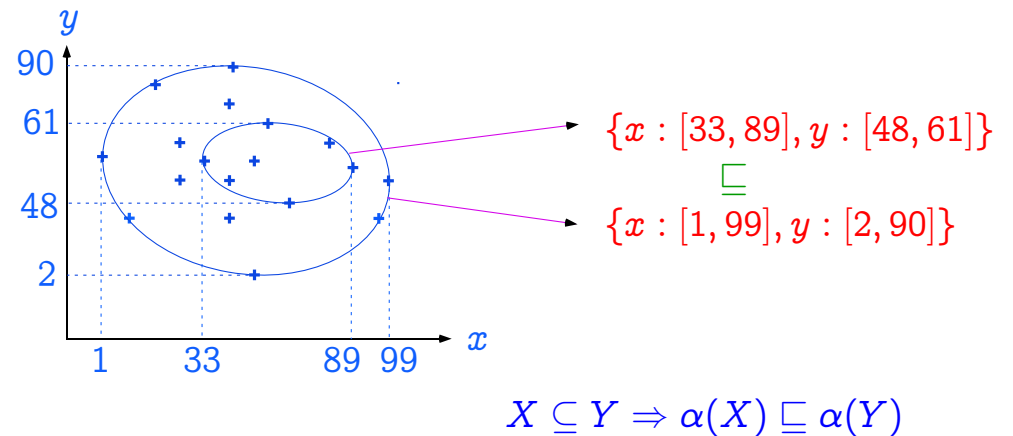


— 59 —

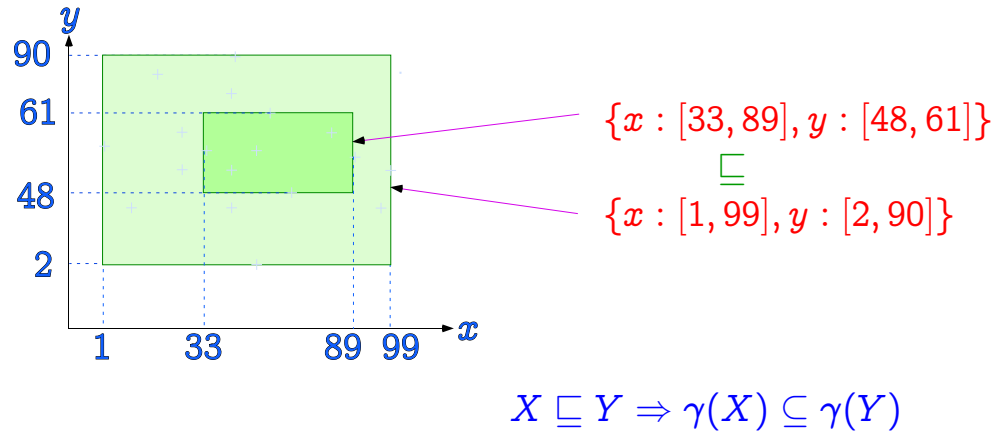
Interval abstraction α



The abstraction α is monotone

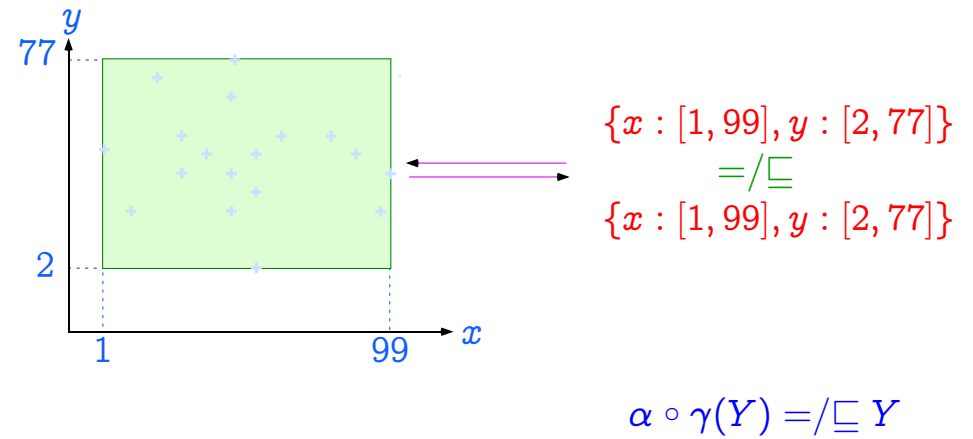


The concretization γ is monotone



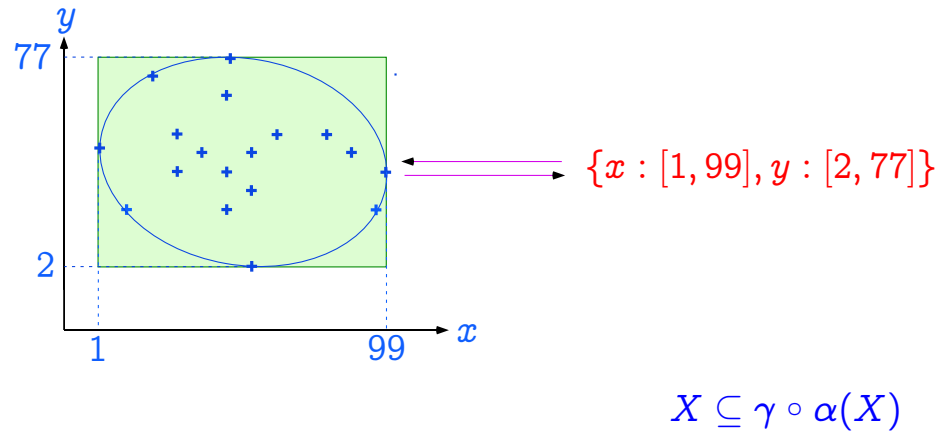
— 61 —

The $\alpha \circ \gamma$ composition is reductive



— 63 —

The $\gamma \circ \alpha$ composition is extensive



Correspondance between concrete and abstract properties

- The pair $\langle \alpha, \gamma \rangle$ is a **Galois connection**:

$$\langle \wp(S), \subseteq \rangle \xleftrightarrow[\alpha]{\gamma} \langle \mathcal{D}, \sqsubseteq \rangle$$

- $\langle \wp(S), \subseteq \rangle \xleftrightarrow[\alpha]{\gamma} \langle \mathcal{D}, \sqsubseteq \rangle$ when α is onto (equivalently $\alpha \circ \gamma = 1$ or γ is one-to-one).

Galois connection

$$\langle \mathcal{D}, \sqsubseteq \rangle \xleftrightarrow[\alpha]{\gamma} \langle \overline{\mathcal{D}}, \sqsubseteq \rangle$$

$$\text{iff } \forall x, y \in \mathcal{D} : x \sqsubseteq y \implies \alpha(x) \sqsubseteq \alpha(y)$$

$$\wedge \forall \overline{x}, \overline{y} \in \overline{\mathcal{D}} : \overline{x} \sqsubseteq \overline{y} \implies \gamma(\overline{x}) \sqsubseteq \gamma(\overline{y})$$

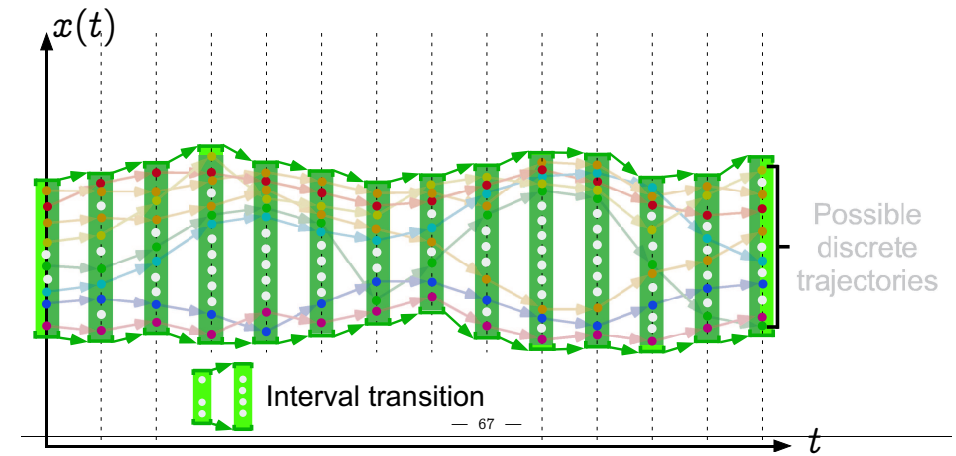
$$\wedge \forall x \in \mathcal{D} : x \sqsubseteq \gamma(\alpha(x))$$

$$\wedge \forall \overline{y} \in \overline{\mathcal{D}} : \alpha(\gamma(\overline{y})) \sqsubseteq \overline{y}$$

$$\text{iff } \forall x \in \mathcal{D}, \overline{y} \in \overline{\mathcal{D}} : \alpha(x) \sqsubseteq \overline{y} \iff x \sqsubseteq \gamma(\overline{y})$$

— 65 —

Graphic example: Abstract transitions



Example: Interval transition semantics of assignments

```
int x;
...
l:
    x := x + 1;
l':
```

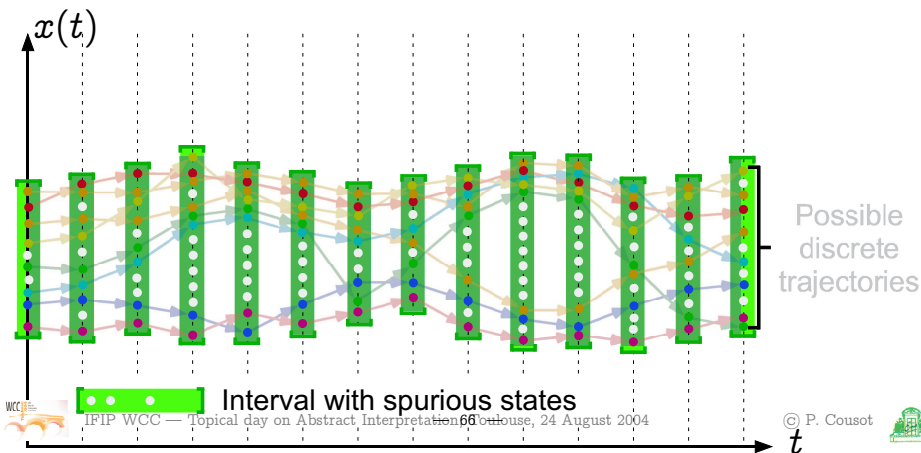
$$\{l : x \in [\ell, h] \rightarrow l' : x \in [l + 1, \min(h + 1, \max_int)] \cup \{\Omega \mid h = \max_int\} \mid \ell \leq h\}$$

where $[\ell, h] = \emptyset$ when $h < \ell$.

24 August 2004

— 68 —

Graphic example: Interval abstraction



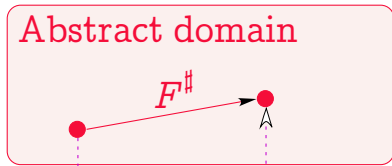
WCC — IFIP WCC — Topical day on Abstract Interpretation, P. Cousot, 24 August 2004

© P. Cousot

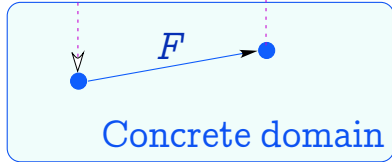


© P. Cousot





Function abstraction



$$F^\# = \alpha \circ F \circ \gamma$$

.e. $F^\# = \rho \circ F$

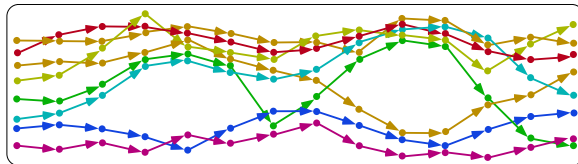
$$\langle P, \sqsubseteq \rangle \xleftrightarrow[\alpha]{\gamma} \langle Q, \sqsubseteq \rangle \Rightarrow$$

$$\langle P \xrightarrow{\text{mon}} P, \dot{\sqsubseteq} \rangle \xleftrightarrow[\lambda F \cdot \alpha \circ F \circ \gamma]{\lambda F^\# \cdot \gamma \circ F^\# \circ \alpha} \langle Q \xrightarrow{\text{mon}} Q, \dot{\sqsubseteq} \rangle$$

— 69 —

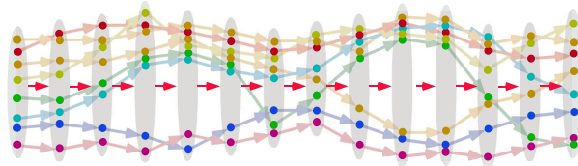
Example: Set of traces to trace of intervals abstraction

Set of traces:



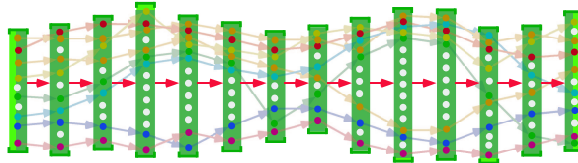
$\alpha_1 \downarrow$

Trace of sets:



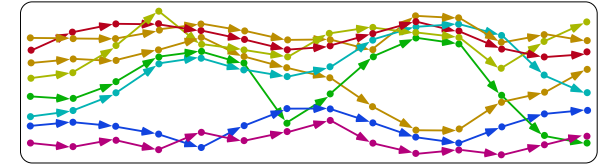
$\alpha_2 \downarrow$

Trace of intervals



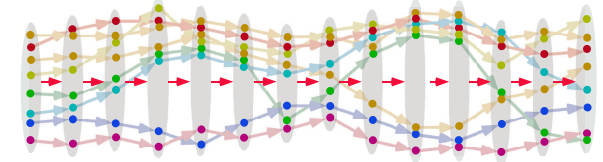
Example: Set of traces to reachable states abstraction

Set of traces:



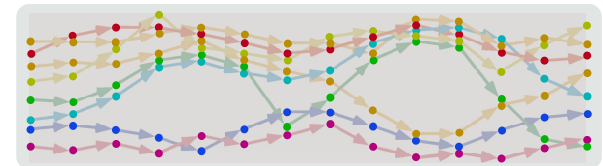
$\alpha_1 \downarrow$

Trace of sets:



$\alpha_3 \downarrow$

Reachable states



— 71 —

Composition of Galois Connections

The composition of Galois connections:

$$\langle L, \leq \rangle \xleftrightarrow[\alpha_1]{\gamma_1} \langle M, \sqsubseteq \rangle$$

and:

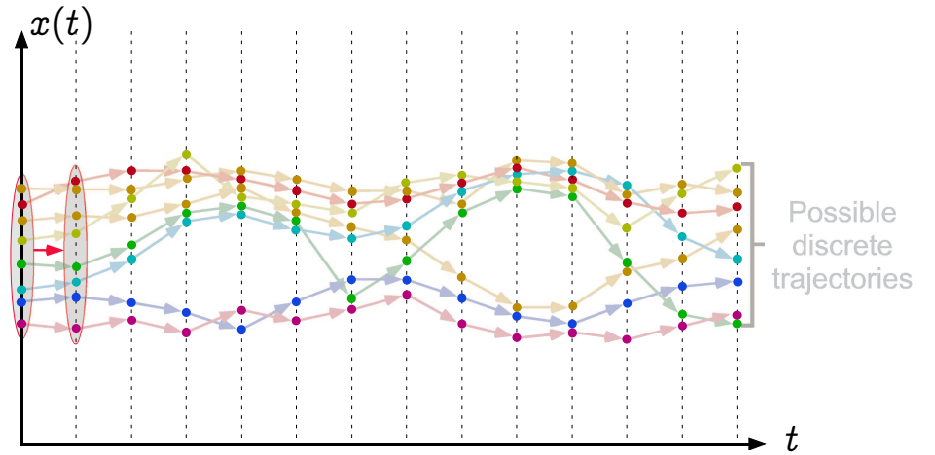
$$\langle M, \sqsubseteq \rangle \xleftrightarrow[\alpha_2]{\gamma_2} \langle N, \preceq \rangle$$

is a Galois connection:

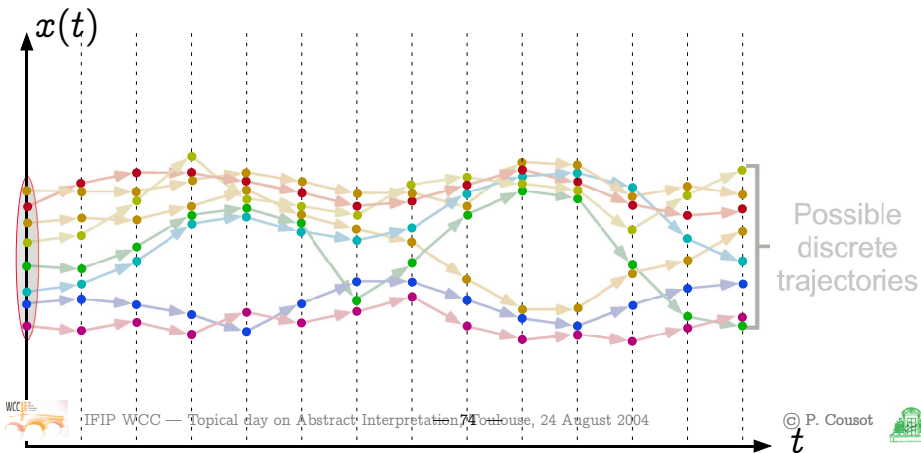
$$\langle L, \leq \rangle \xleftrightarrow[\alpha_2 \circ \alpha_1]{\gamma_1 \circ \gamma_2} \langle N, \preceq \rangle$$

Abstract semantics in fixpoint form

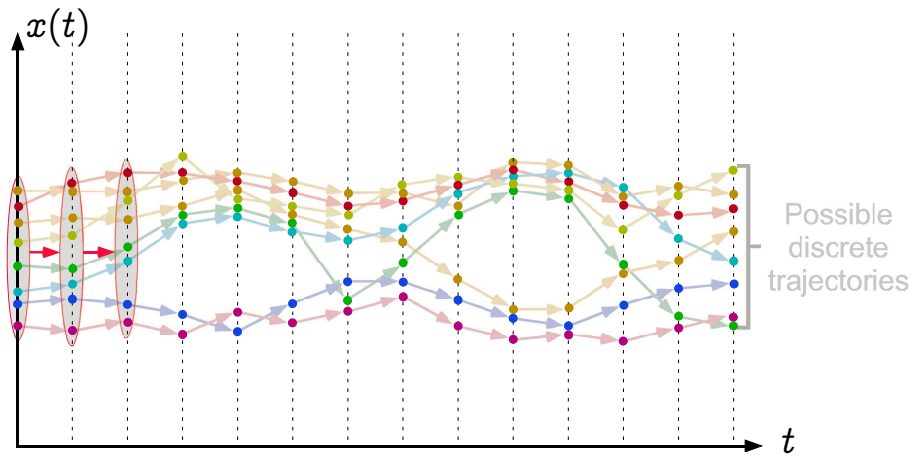
Graphic example: traces of sets of states in fixpoint form



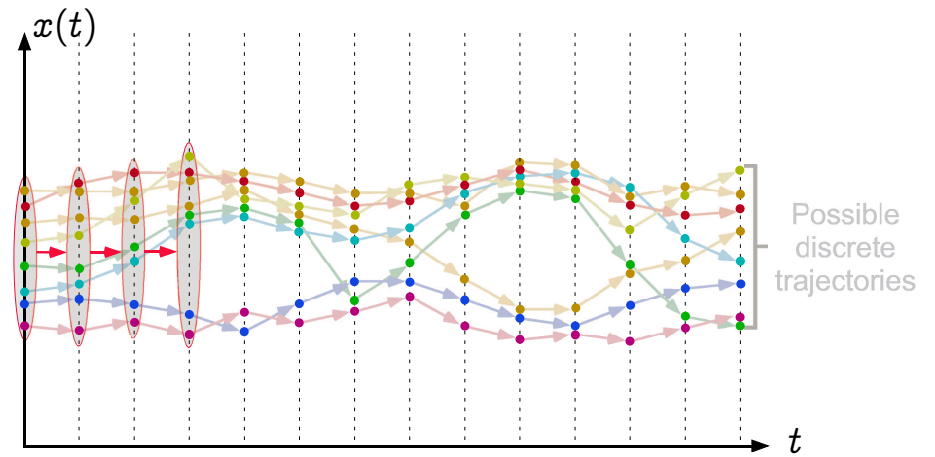
Graphic example: traces of sets of states in fixpoint form



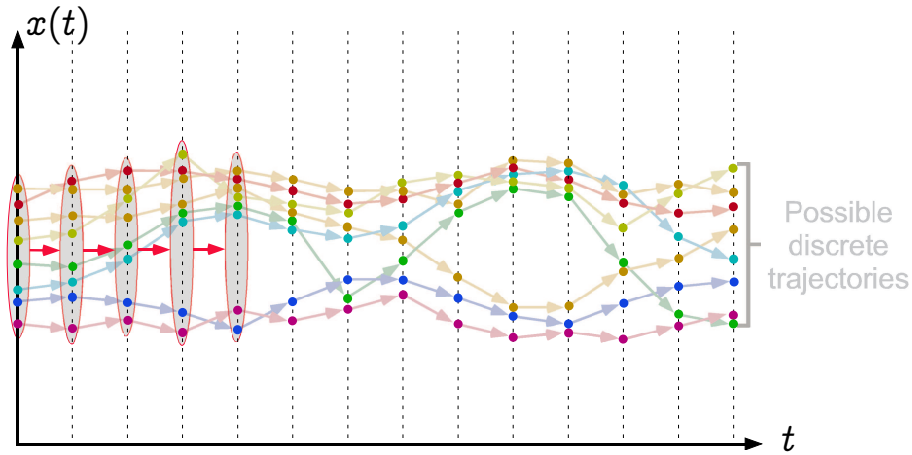
Graphic example: traces of sets of states
in fixpoint form



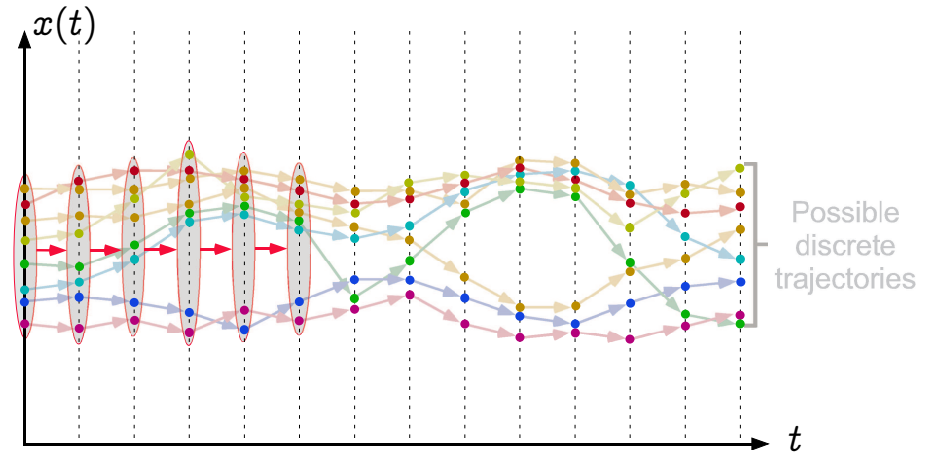
Graphic example: traces of sets of states
in fixpoint form



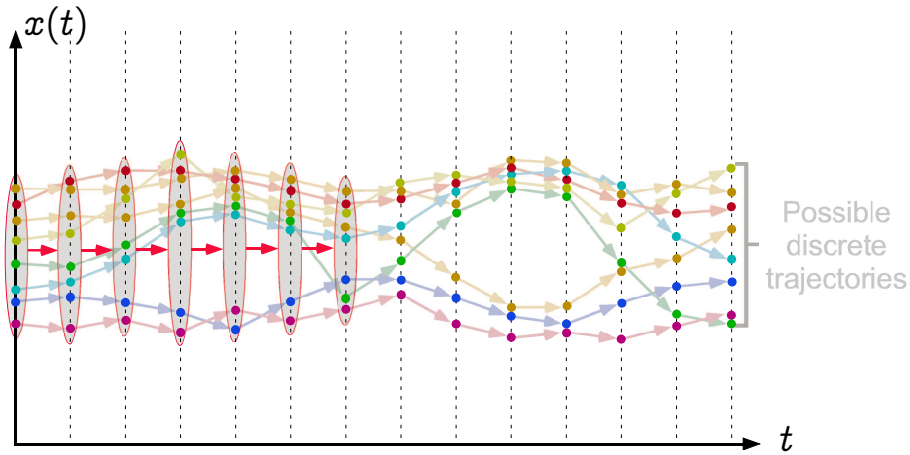
Graphic example: traces of sets of states
in fixpoint form



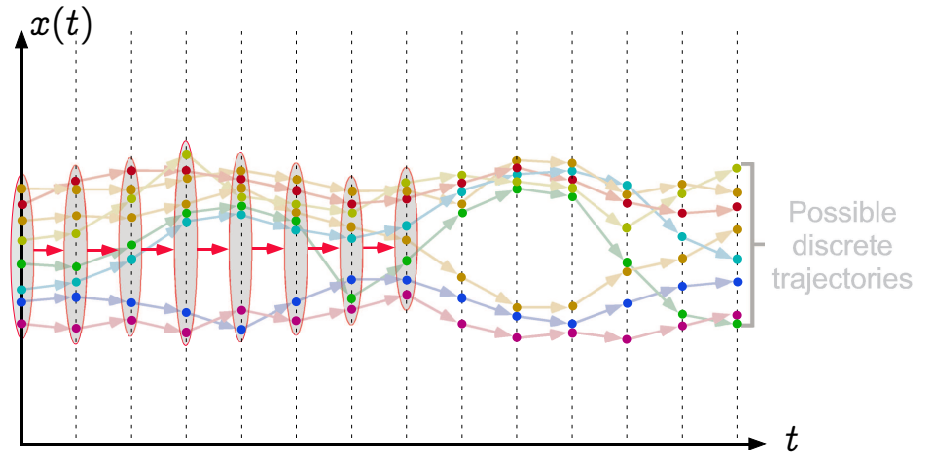
Graphic example: traces of sets of states
in fixpoint form



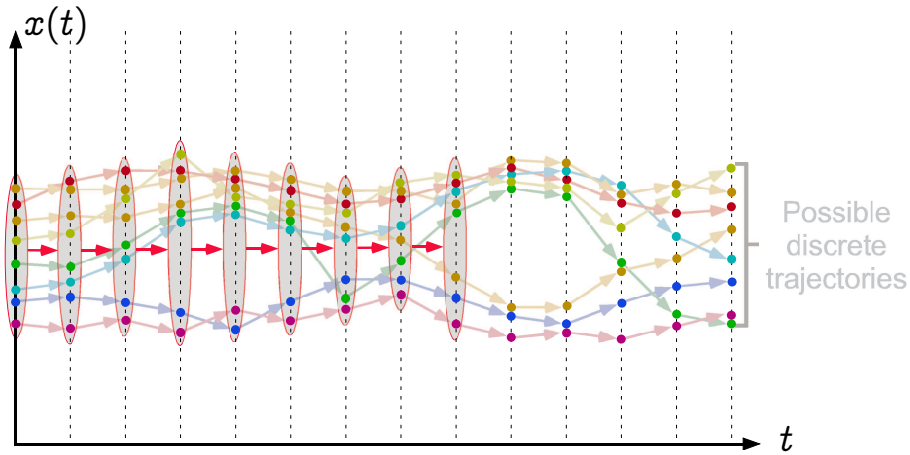
Graphic example: traces of sets of states
in fixpoint form



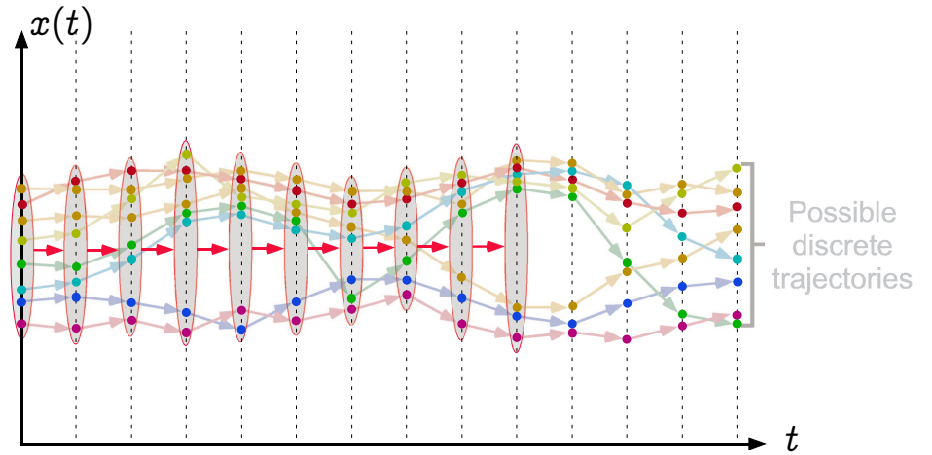
Graphic example: traces of sets of states
in fixpoint form



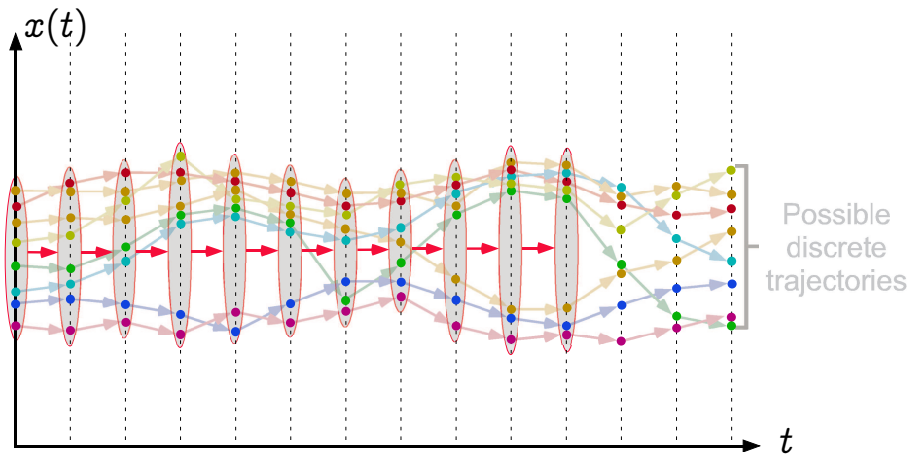
Graphic example: traces of sets of states
in fixpoint form



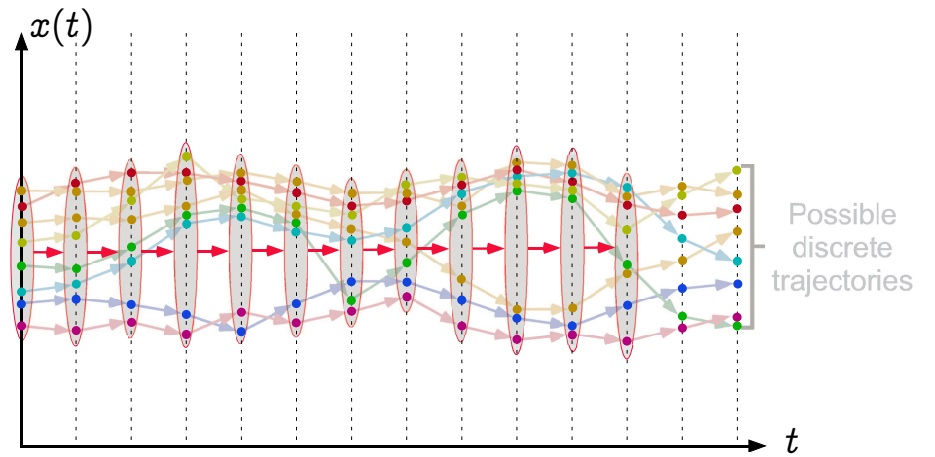
Graphic example: traces of sets of states
in fixpoint form



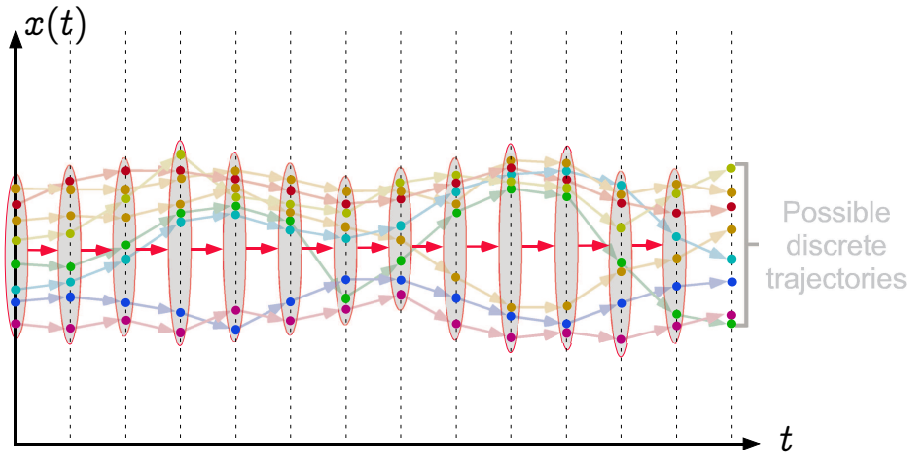
Graphic example: traces of sets of states
in fixpoint form



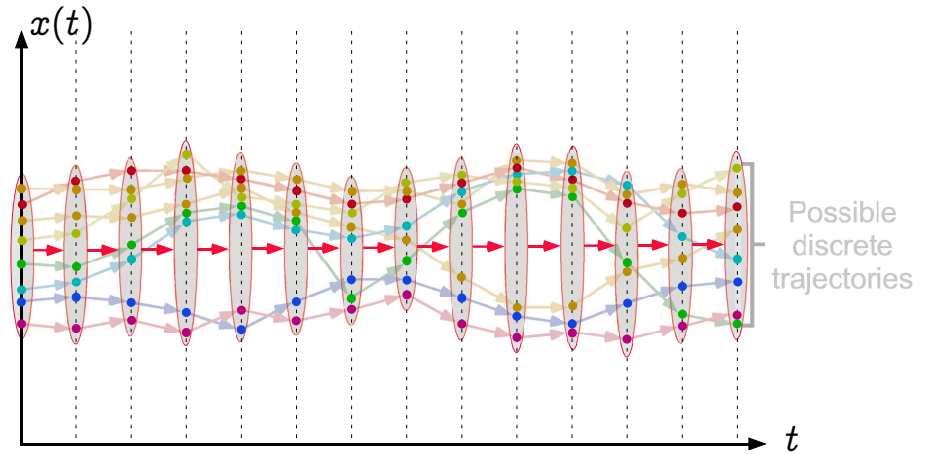
Graphic example: traces of sets of states
in fixpoint form



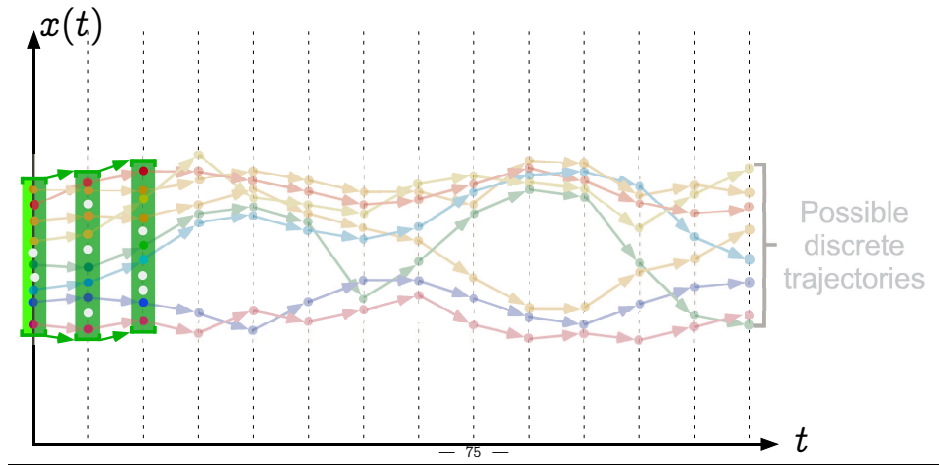
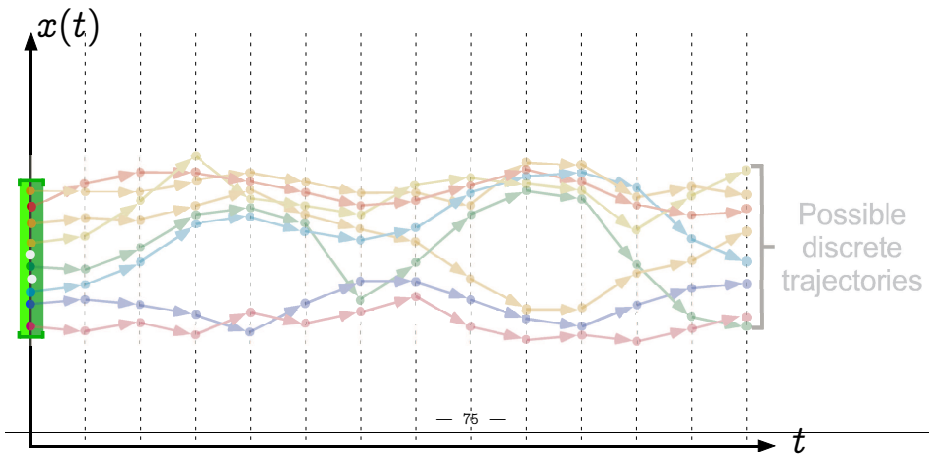
Graphic example: traces of sets of states
in fixpoint form



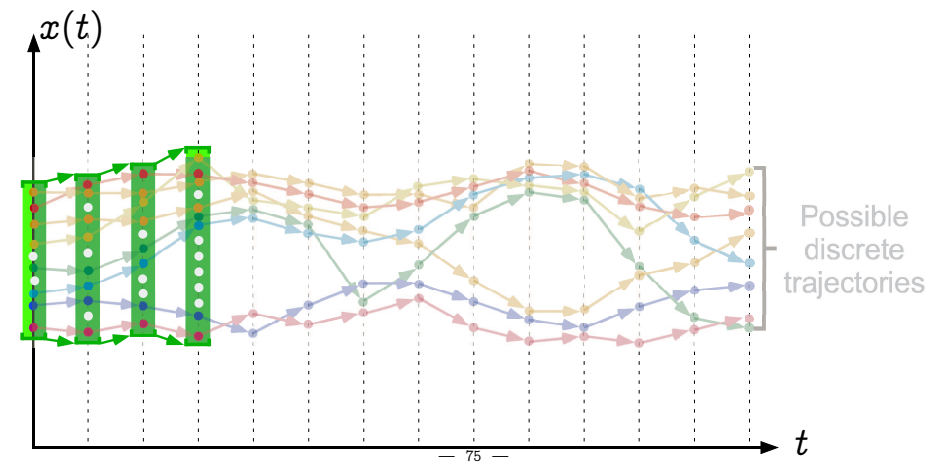
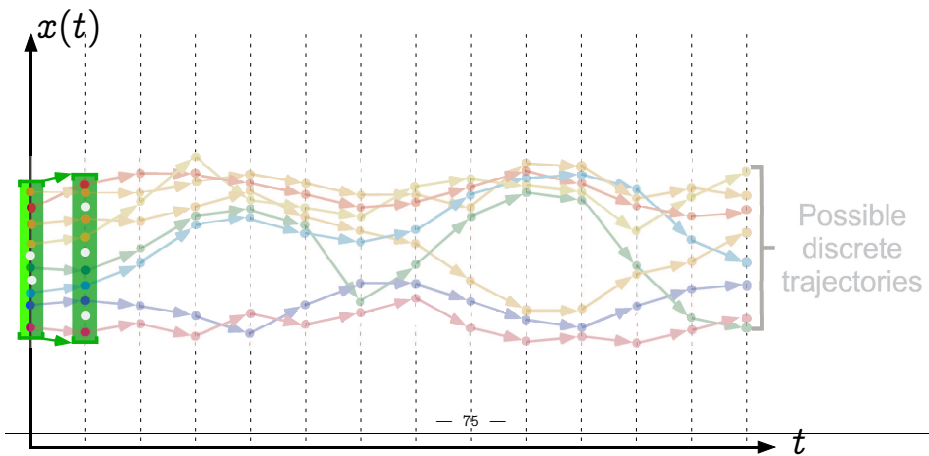
Graphic example: traces of sets of states
in fixpoint form



Graphic example: traces of intervals
in fixpoint form

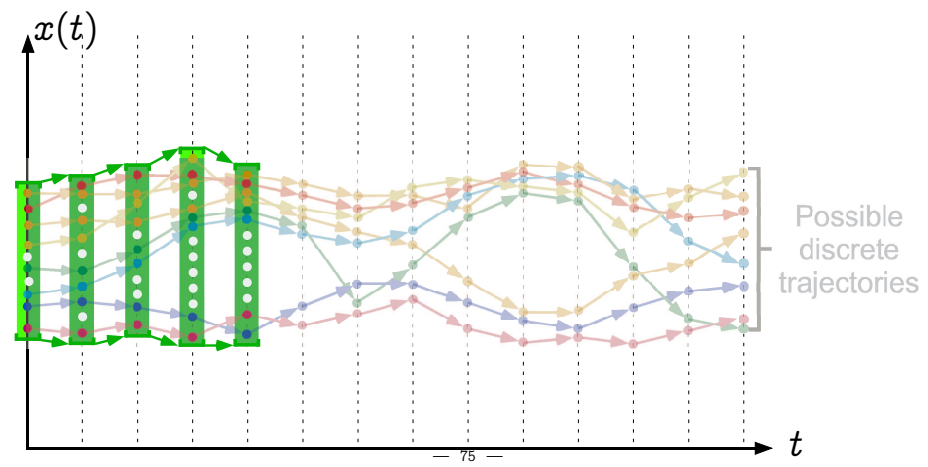


Graphic example: traces of intervals
in fixpoint form

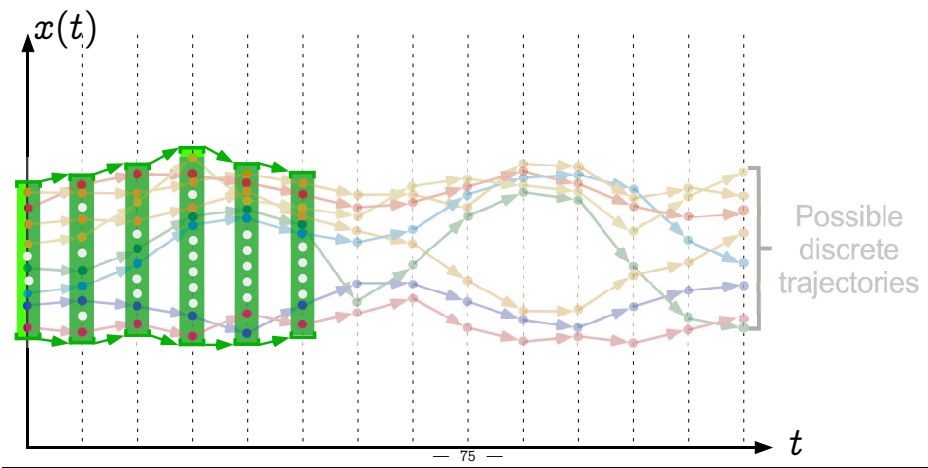


Graphic example: traces of intervals
in fixpoint form

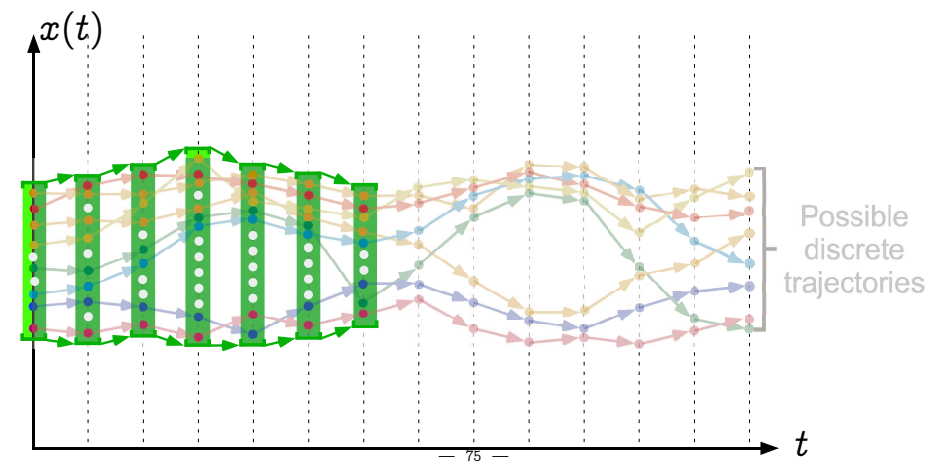
Graphic example: traces of intervals
in fixpoint form



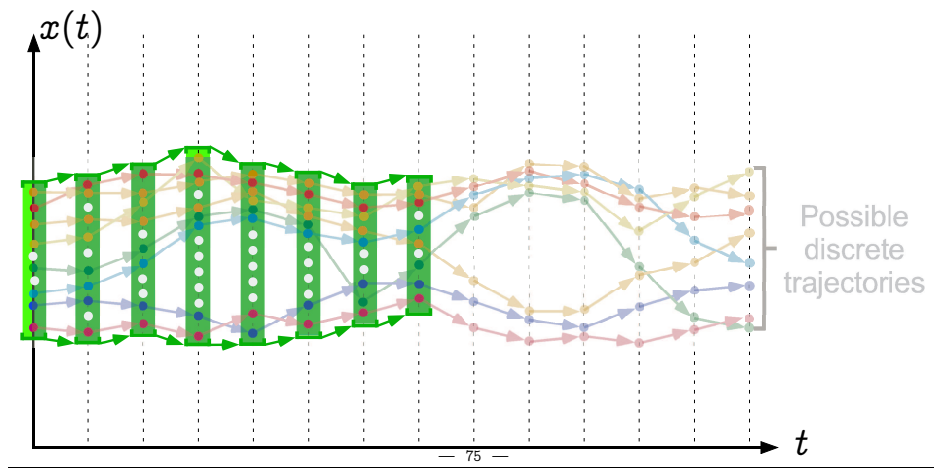
Graphic example: traces of intervals
in fixpoint form



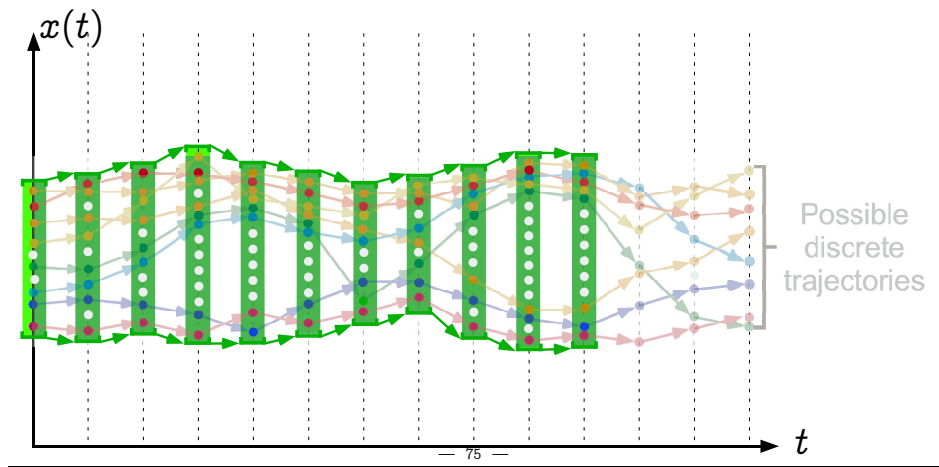
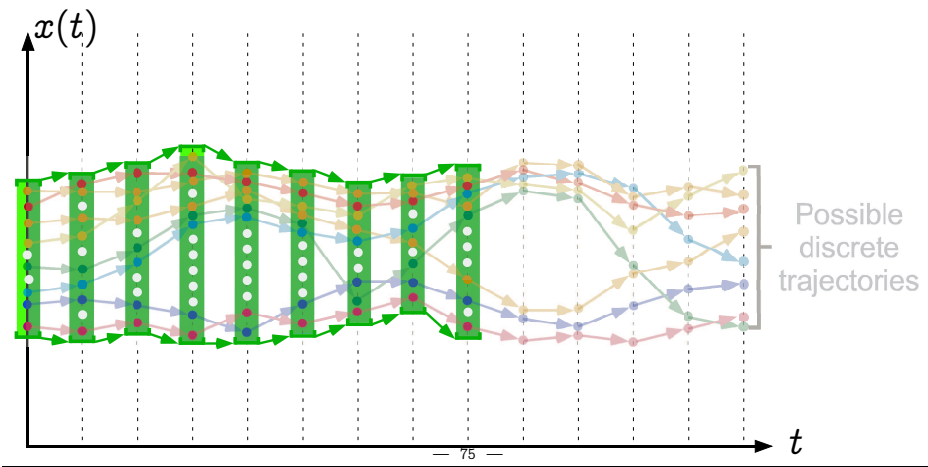
Graphic example: traces of intervals
in fixpoint form



Graphic example: traces of intervals
in fixpoint form

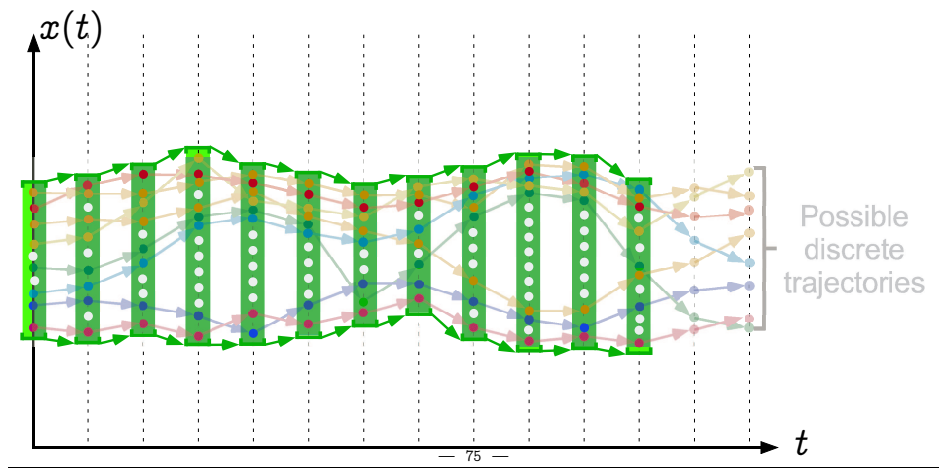
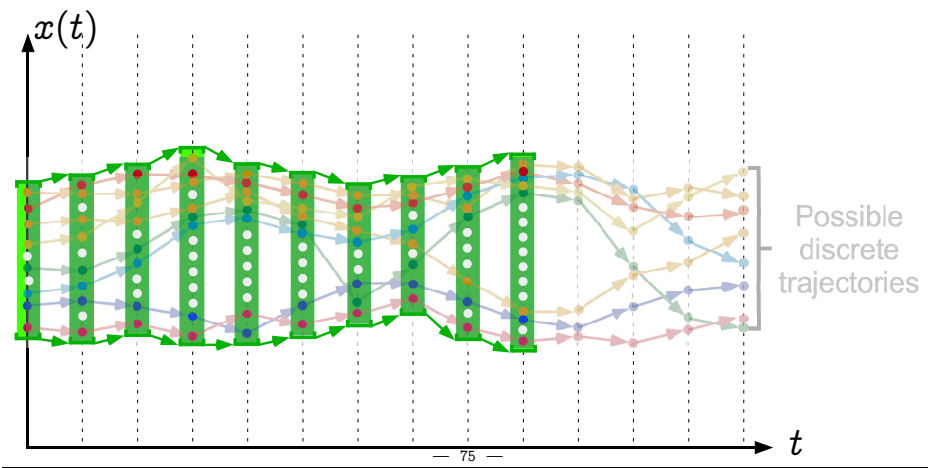


Graphic example: traces of intervals
in fixpoint form



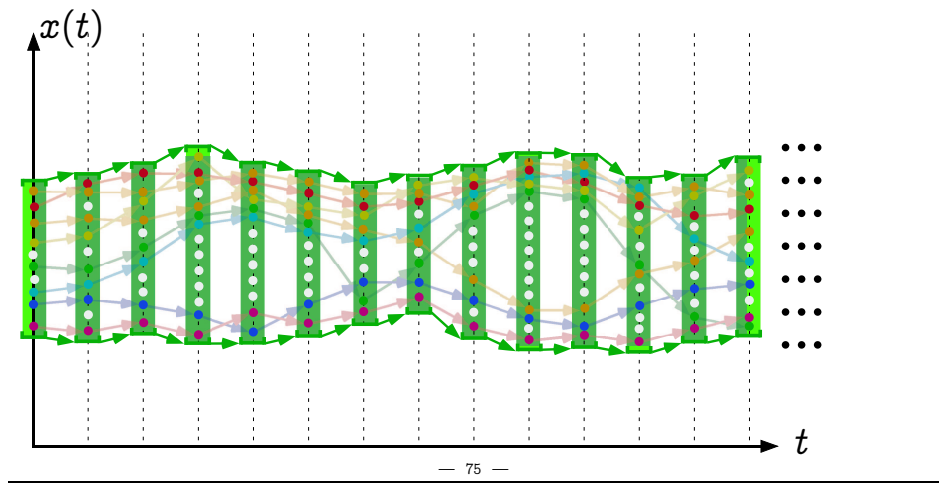
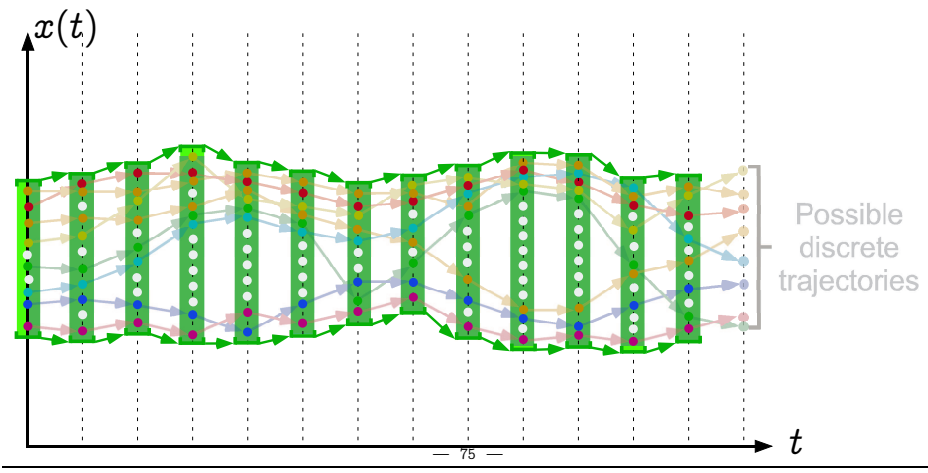
Graphic example: traces of intervals
in fixpoint form

Graphic example: traces of intervals
in fixpoint form

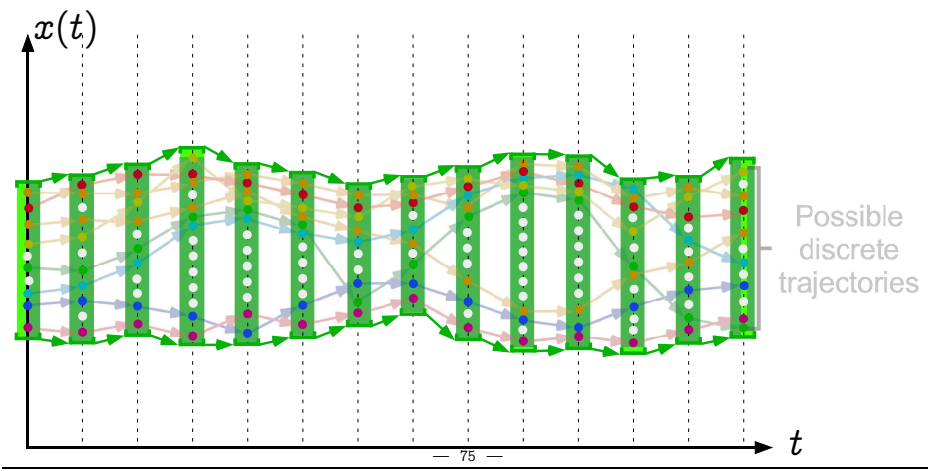


Graphic example: traces of intervals
in fixpoint form

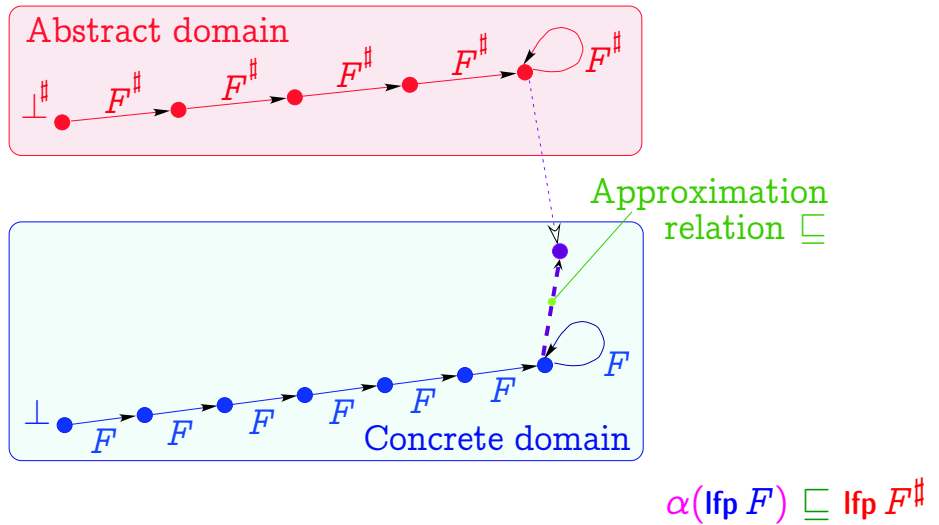
Graphic example: traces of intervals
in fixpoint form



Graphic example: traces of intervals in fixpoint form



Approximate fixpoint abstraction



Graphic example: traces of intervals in fixpoint form

approximate/exact fixpoint abstraction

Exact Abstraction:

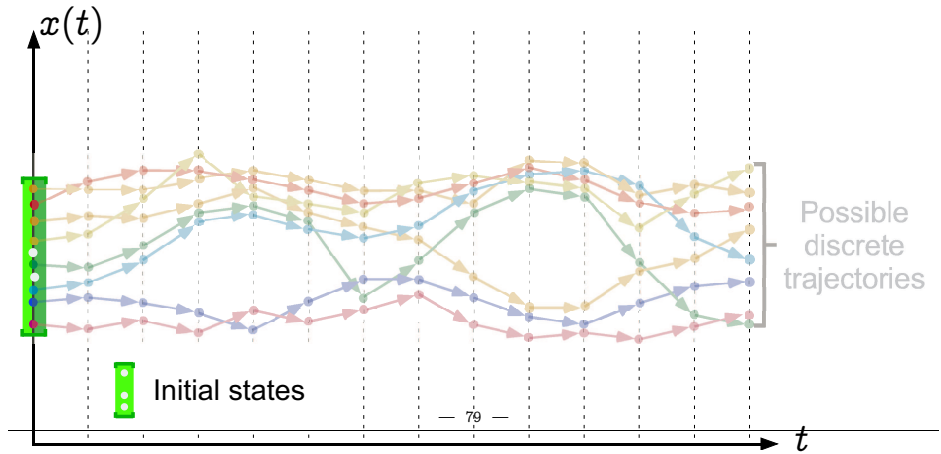
$$\alpha(\text{lfp } F) = \text{lfp } F^\sharp$$

Approximate Abstraction:

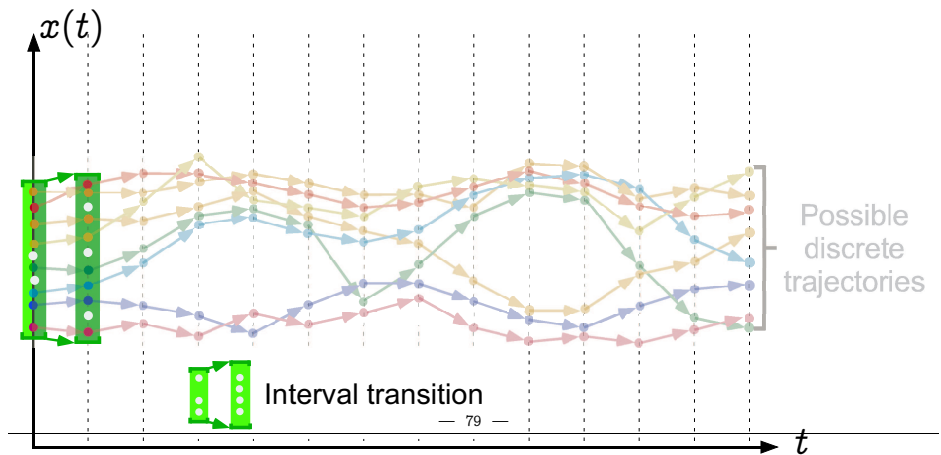
$$\alpha(\text{lfp } F) \sqsubseteq^\sharp \text{lfp } F^\sharp$$

Convergence acceleration
by widening/narrowing

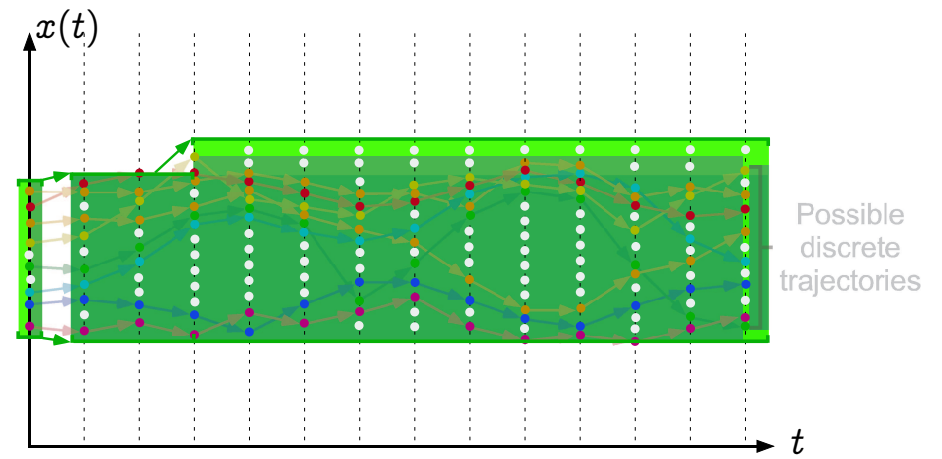
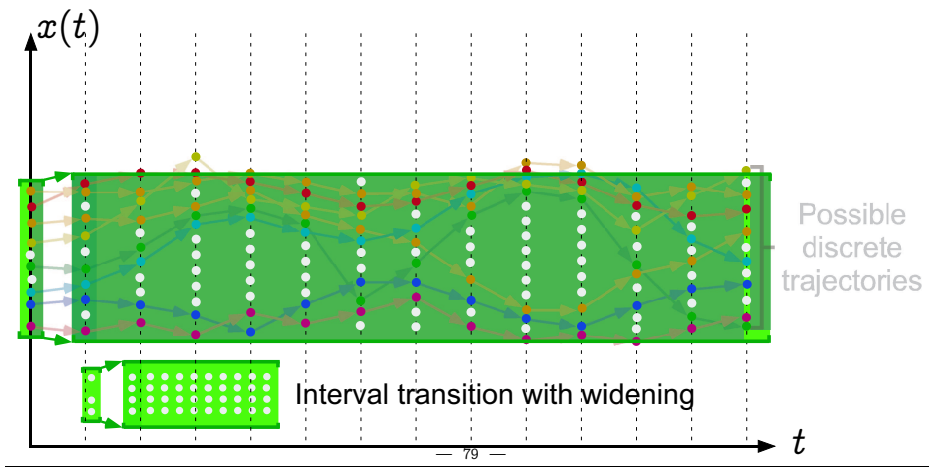
Graphic example: upward iteration with widening



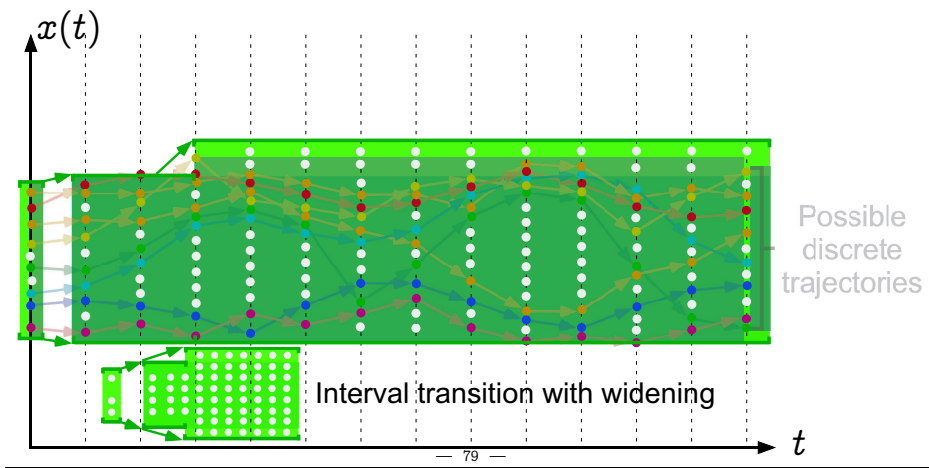
Graphic example: upward iteration with widening



Graphic example: upward iteration with widening



Graphic example: upward iteration with widening



Graphic example: stability of the upward iteration

Convergence acceleration with widening

— 81 —

Widening operator

A widening operator $\nabla \in \overline{L} \times \overline{L} \mapsto \overline{L}$ is such that:

- **Correctness:**
 - $\forall x, y \in \overline{L} : \gamma(x) \sqsubseteq \gamma(x \nabla y)$
 - $\forall x, y \in \overline{L} : \gamma(y) \sqsubseteq \gamma(x \nabla y)$
- **Convergence:**
 - for all increasing chains $x^0 \sqsubseteq x^1 \sqsubseteq \dots$, the increasing chain defined by $y^0 = x^0, \dots, y^{i+1} = y^i \nabla x^{i+1}, \dots$ is not strictly increasing.

Fixpoint approximation with widening

The upward iteration sequence with widening:

- $\hat{X}^0 = \perp$ (infimum)
- $\hat{X}^{i+1} = \hat{X}^i$ if $\overline{F}(\hat{X}^i) \sqsubseteq \hat{X}^i$
- = $\hat{X}^i \nabla F(\hat{X}^i)$ otherwise

is ultimately stationary and its limit \hat{A} is a sound upper approximation of $\text{lfp}^{\perp} \overline{F}$:

$$\text{lfp}^{\perp} \overline{F} \sqsubseteq \hat{A}$$

— 83 —

Interval widening

- $\overline{L} = \{\perp\} \cup \{[l, u] \mid l, u \in \mathbb{Z} \cup \{-\infty\} \wedge u \in \mathbb{Z} \cup \{\infty\} \wedge l \leq u\}$
- The **widening** extrapolates unstable bounds to infinity:

$$\begin{aligned} \perp \nabla X &= X \\ X \nabla \perp &= X \\ [l_0, u_0] \nabla [l_1, u_1] &= [f \ l_1 < l_0 \text{ then } -\infty \text{ else } l_0, \\ &\quad f \ u_1 > u_0 \text{ then } +\infty \text{ else } u_0] \end{aligned}$$

Not monotone. For example $[0, 1] \sqsubseteq [0, 2]$ but $[0, 1] \nabla [0, 2] = [0, +\infty] \not\sqsubseteq [0, 2] = [0, 2] \nabla [0, 2]$

Example: Interval analysis (1975)

Program to be analyzed:

```

x := 1;
1:
  while x < 10000 do
2:
    x := x + 1
3:
  od;
4:

```

— 85 —

Example: Interval analysis (1975)

Resolution by chaotic increasing iteration:

```

x := 1;
1:
  while x < 10000 do
2:
    x := x + 1
3:
  od;
4:

```

$$\begin{cases} X_1 = [1, 1] \\ X_2 = (X_1 \cup X_3) \cap [-\infty, 9999] \\ X_3 = X_2 \oplus [1, 1] \\ X_4 = (X_1 \cup X_3) \cap [10000, +\infty] \end{cases}$$

$$\begin{cases} X_1 = \emptyset \\ X_2 = \emptyset \\ X_3 = \emptyset \\ X_4 = \emptyset \end{cases}$$

— 87 —

Example: Interval analysis (1975)

Equations (abstract interpretation of the semantics):

```

x := 1;
1:
  while x < 10000 do
2:
    x := x + 1
3:
  od;
4:

```

$$\begin{cases} X_1 = [1, 1] \\ X_2 = (X_1 \cup X_3) \cap [-\infty, 9999] \\ X_3 = X_2 \oplus [1, 1] \\ X_4 = (X_1 \cup X_3) \cap [10000, +\infty] \end{cases}$$

Example: Interval analysis (1975)

Increasing chaotic iteration:

```

x := 1;
1:
  while x < 10000 do
2:
    x := x + 1
3:
  od;
4:

```

$$\begin{cases} X_1 = [1, 1] \\ X_2 = (X_1 \cup X_3) \cap [-\infty, 9999] \\ X_3 = X_2 \oplus [1, 1] \\ X_4 = (X_1 \cup X_3) \cap [10000, +\infty] \end{cases}$$

$$\begin{cases} X_1 = [1, 1] \\ X_2 = \emptyset \\ X_3 = \emptyset \\ X_4 = \emptyset \end{cases}$$

Example: Interval analysis (1975)

Increasing chaotic iteration:

```

x := 1;
1: while x < 10000 do
2:   x := x + 1
3:   od;
4:

```

$$\begin{cases} X_1 = [1, 1] \\ X_2 = (X_1 \cup X_3) \cap [-\infty, 9999] \\ X_3 = X_2 \oplus [1, 1] \\ X_4 = (X_1 \cup X_3) \cap [10000, +\infty] \end{cases}$$

Example: Interval analysis (1975)

Increasing chaotic iteration:

```

x := 1;
1: while x < 10000 do
2:   x := x + 1
3:   od;
4:

```

$$\begin{cases} X_1 = [1, 1] \\ X_2 = (X_1 \cup X_3) \cap [-\infty, 9999] \\ X_3 = X_2 \oplus [1, 1] \\ X_4 = (X_1 \cup X_3) \cap [10000, +\infty] \end{cases}$$

Example: Interval analysis (1975)

Increasing chaotic iteration:

```

x := 1;
1: while x < 10000 do
2:   x := x + 1
3:   od;
4:

```

$$\begin{cases} X_1 = [1, 1] \\ X_2 = (X_1 \cup X_3) \cap [-\infty, 9999] \\ X_3 = X_2 \oplus [1, 1] \\ X_4 = (X_1 \cup X_3) \cap [10000, +\infty] \end{cases}$$

Example: Interval analysis (1975)

Increasing chaotic iteration: **convergence !**

```

x := 1;
1: while x < 10000 do
2:   x := x + 1
3:   od;
4:

```

$$\begin{cases} X_1 = [1, 1] \\ X_2 = (X_1 \cup X_3) \cap [-\infty, 9999] \\ X_3 = X_2 \oplus [1, 1] \\ X_4 = (X_1 \cup X_3) \cap [10000, +\infty] \end{cases}$$

Example: Interval analysis (1975)

Increasing chaotic iteration: **convergence !!**

```

x := 1;
1: while x < 10000 do
2:     x := x + 1
3:     od;
4:

```

$$\begin{cases} X_1 = [1, 1] \\ X_2 = (X_1 \cup X_3) \cap [-\infty, 9999] \\ X_3 = X_2 \oplus [1, 1] \\ X_4 = (X_1 \cup X_3) \cap [10000, +\infty] \end{cases}$$

$$\begin{cases} X_1 = [1, 1] \\ X_2 = [1, 3] \\ X_3 = [2, 3] \\ X_4 = \emptyset \end{cases}$$

Example: Interval analysis (1975)

Increasing chaotic iteration: **convergence !!!**

```

x := 1;
1: while x < 10000 do
2:     x := x + 1
3:     od;
4:

```

$$\begin{cases} X_1 = [1, 1] \\ X_2 = (X_1 \cup X_3) \cap [-\infty, 9999] \\ X_3 = X_2 \oplus [1, 1] \\ X_4 = (X_1 \cup X_3) \cap [10000, +\infty] \end{cases}$$

$$\begin{cases} X_1 = [1, 1] \\ X_2 = [1, 3] \\ X_3 = [2, 4] \\ X_4 = \emptyset \end{cases}$$

Example: Interval analysis (1975)

Increasing chaotic iteration: **convergence !!!!**

```

x := 1;
1: while x < 10000 do
2:     x := x + 1
3:     od;
4:

```

$$\begin{cases} X_1 = [1, 1] \\ X_2 = (X_1 \cup X_3) \cap [-\infty, 9999] \\ X_3 = X_2 \oplus [1, 1] \\ X_4 = (X_1 \cup X_3) \cap [10000, +\infty] \end{cases}$$

$$\begin{cases} X_1 = [1, 1] \\ X_2 = [1, 4] \\ X_3 = [2, 4] \\ X_4 = \emptyset \end{cases}$$

Example: Interval analysis (1975)

Increasing chaotic iteration: **convergence !!!!!**

```

x := 1;
1: while x < 10000 do
2:     x := x + 1
3:     od;
4:

```

$$\begin{cases} X_1 = [1, 1] \\ X_2 = (X_1 \cup X_3) \cap [-\infty, 9999] \\ X_3 = X_2 \oplus [1, 1] \\ X_4 = (X_1 \cup X_3) \cap [10000, +\infty] \end{cases}$$

$$\begin{cases} X_1 = [1, 1] \\ X_2 = [1, 4] \\ X_3 = [2, 5] \\ X_4 = \emptyset \end{cases}$$

Example: Interval analysis (1975)

Increasing chaotic iteration: **convergence !!!!!**

```

x := 1;
1: while x < 10000 do
2:   x := x + 1
3:   od;
4:

```

$$\begin{cases} X_1 = [1, 1] \\ X_2 = (X_1 \cup X_3) \cap [-\infty, 9999] \\ X_3 = X_2 \oplus [1, 1] \\ X_4 = (X_1 \cup X_3) \cap [10000, +\infty] \end{cases}$$

$$\begin{cases} X_1 = [1, 1] \\ X_2 = [1, 5] \\ X_3 = [2, 5] \\ X_4 = \emptyset \end{cases}$$

Example: Interval analysis (1975)

Increasing chaotic iteration: **convergence !!!!!**

```

x := 1;
1: while x < 10000 do
2:   x := x + 1
3:   od;
4:

```

$$\begin{cases} X_1 = [1, 1] \\ X_2 = (X_1 \cup X_3) \cap [-\infty, 9999] \\ X_3 = X_2 \oplus [1, 1] \\ X_4 = (X_1 \cup X_3) \cap [10000, +\infty] \end{cases}$$

$$\begin{cases} X_1 = [1, 1] \\ X_2 = [1, 5] \\ X_3 = [2, 6] \\ X_4 = \emptyset \end{cases}$$

Example: Interval analysis (1975)

Convergence speed-up by widening:

```

x := 1;
1: while x < 10000 do
2:   x := x + 1
3:   od;
4:

```

$$\begin{cases} X_1 = [1, 1] \\ X_2 = (X_1 \cup X_3) \cap [-\infty, 9999] \\ X_3 = X_2 \oplus [1, 1] \\ X_4 = (X_1 \cup X_3) \cap [10000, +\infty] \end{cases}$$

$$\begin{cases} X_1 = [1, 1] \\ X_2 = [1, +\infty] \quad \Leftarrow \text{widening} \\ X_3 = [2, 6] \\ X_4 = \emptyset \end{cases}$$

— 89 —

Example: Interval analysis (1975)

Decreasing chaotic iteration:

```

x := 1;
1: while x < 10000 do
2:   x := x + 1
3:   od;
4:

```

$$\begin{cases} X_1 = [1, 1] \\ X_2 = (X_1 \cup X_3) \cap [-\infty, 9999] \\ X_3 = X_2 \oplus [1, 1] \\ X_4 = (X_1 \cup X_3) \cap [10000, +\infty] \end{cases}$$

$$\begin{cases} X_1 = [1, 1] \\ X_2 = [1, +\infty] \\ X_3 = [2, +\infty] \\ X_4 = \emptyset \end{cases}$$

Example: Interval analysis (1975)

Decreasing chaotic iteration:

```

x := 1;
1: while x < 10000 do
2:   x := x + 1
3:   od;
4:

```

$$\begin{cases} X_1 = [1, 1] \\ X_2 = (X_1 \cup X_3) \cap [-\infty, 9999] \\ X_3 = X_2 \oplus [1, 1] \\ X_4 = (X_1 \cup X_3) \cap [10000, +\infty] \end{cases}$$

$$\begin{cases} X_1 = [1, 1] \\ X_2 = [1, 9999] \\ X_3 = [2, +\infty] \\ X_4 = \emptyset \end{cases}$$

Example: Interval analysis (1975)

Decreasing chaotic iteration:

```

x := 1;
1: while x < 10000 do
2:   x := x + 1
3:   od;
4:

```

$$\begin{cases} X_1 = [1, 1] \\ X_2 = (X_1 \cup X_3) \cap [-\infty, 9999] \\ X_3 = X_2 \oplus [1, 1] \\ X_4 = (X_1 \cup X_3) \cap [10000, +\infty] \end{cases}$$

$$\begin{cases} X_1 = [1, 1] \\ X_2 = [1, 9999] \\ X_3 = [2, +10000] \\ X_4 = \emptyset \end{cases}$$

Example: Interval analysis (1975)

Final solution:

```

x := 1;
1: while x < 10000 do
2:   x := x + 1
3:   od;
4:

```

$$\begin{cases} X_1 = [1, 1] \\ X_2 = (X_1 \cup X_3) \cap [-\infty, 9999] \\ X_3 = X_2 \oplus [1, 1] \\ X_4 = (X_1 \cup X_3) \cap [10000, +\infty] \end{cases}$$

$$\begin{cases} X_1 = [1, 1] \\ X_2 = [1, 9999] \\ X_3 = [2, +10000] \\ X_4 = [+10000, +10000] \end{cases}$$

— 91 —

Example: Interval analysis (1975)

Result of the interval analysis:

```

x := 1;
1: {x = 1}
   while x < 10000 do
2: {x ∈ [1, 9999]}
   x := x + 1
3: {x ∈ [2, +10000]}
   od;
4: {x = 10000}

```

$$\begin{cases} X_1 = [1, 1] \\ X_2 = (X_1 \cup X_3) \cap [-\infty, 9999] \\ X_3 = X_2 \oplus [1, 1] \\ X_4 = (X_1 \cup X_3) \cap [10000, +\infty] \end{cases}$$

$$\begin{cases} X_1 = [1, 1] \\ X_2 = [1, 9999] \\ X_3 = [2, +10000] \\ X_4 = [+10000, +10000] \end{cases}$$

Example: Interval analysis (1975)

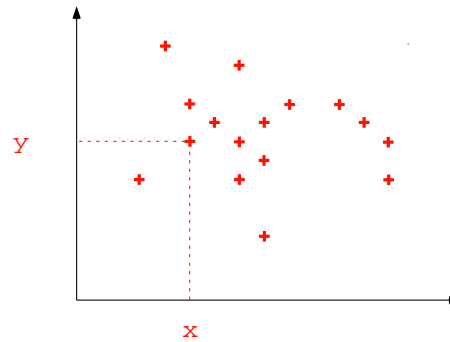
Checking absence of runtime errors with interval analysis:

```

x := 1;
1: {x = 1}
   while x < 10000 do
2: {x ∈ [1, 9999]}           ← no overflow
   x := x + 1
3: {x ∈ [2, +10000]}
   od;
4: {x = 10000}
    
```

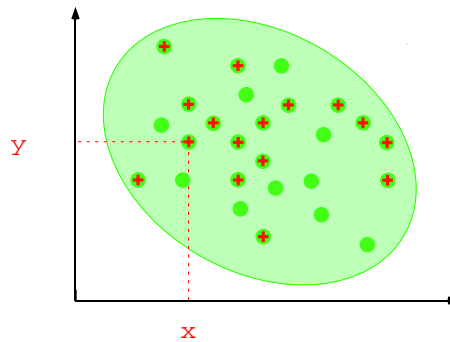
Refinement of abstractions

Approximations of an [in]finite set of points:



$\{\dots, \langle 19, 77 \rangle, \dots, \langle 20, 03 \rangle, \dots\}$

Approximations of an [in]finite set of points: from above

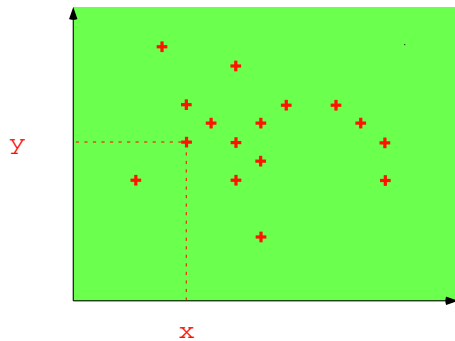


$\{\dots, \langle 19, 77 \rangle, \dots, \langle 20, 03 \rangle, \langle ?, ? \rangle, \dots\}$

From Below: dual³ + combinations.

³ Trivial for finite states (liveness model-checking), more difficult for infinite states (variant functions).

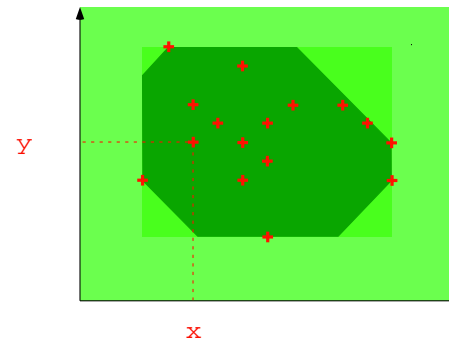
Effective computable approximations of an [in]finite set of points; Signs⁴



$$\begin{cases} x \geq 0 \\ y \geq 0 \end{cases}$$

— 97 —

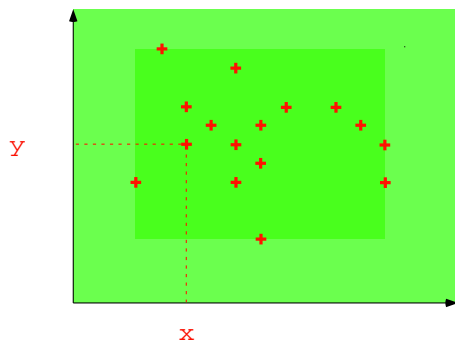
Effective computable approximations of an [in]finite set of points; Octagons⁶



$$\begin{cases} 1 \leq x \leq 9 \\ x + y \leq 77 \\ 1 \leq y \leq 9 \\ x - y \leq 99 \end{cases}$$

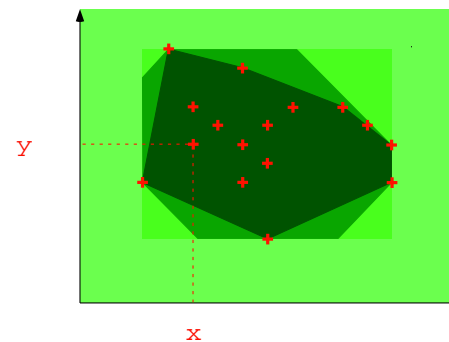
— 99 —

Effective computable approximations of an [in]finite set of points; Intervals⁵



$$\begin{cases} x \in [19, 77] \\ y \in [20, 03] \end{cases}$$

Effective computable approximations of an [in]finite set of points; Polyhedra⁷



$$\begin{cases} 19x + 77y \leq 2004 \\ 20x + 03y \geq 0 \end{cases}$$

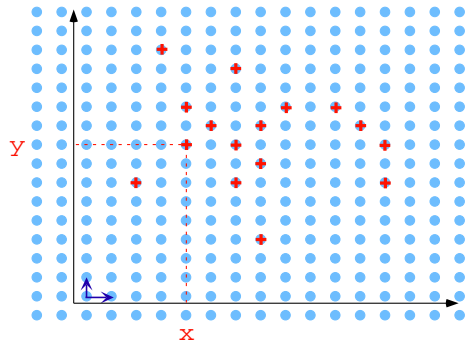
⁴ P. Cousot & R. Cousot. *Systematic design of program analysis frameworks*. ACM POPL'79, pp. 269–282, 1979.

⁵ P. Cousot & R. Cousot. *Static determination of dynamic properties of programs*. Proc. 2nd Int. Symp. on Programming, Dunod, 1976.

⁶ A. Miné. *A New Numerical Abstract Domain Based on Difference-Bound Matrices*. PADO'2001. LNCS 2053, pp. 155–172. Springer 2001. See the *The Octagon Abstract Domain Library* on <http://www.di.ens.fr/~mine/oct/>

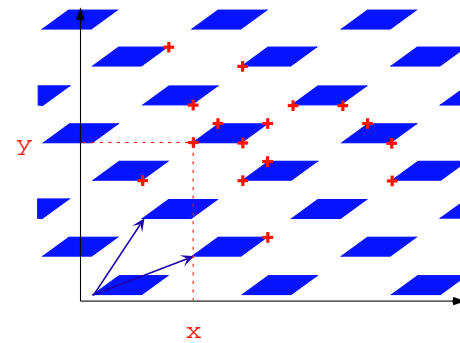
⁷ P. Cousot & N. Halbwachs. *Automatic discovery of linear restraints among variables of a program*. ACM POPL, 1978, pp. 84–97.

Effective computable approximations of an [in]finite set of points; Simple congruences⁸



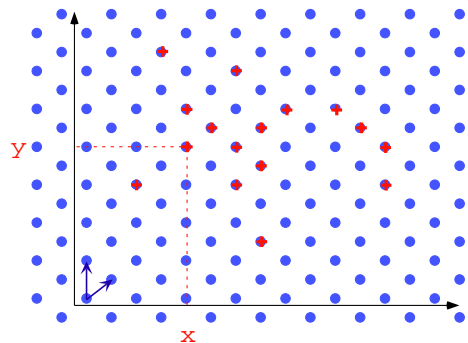
$$\begin{cases} x = 19 \pmod{77} \\ y = 20 \pmod{99} \end{cases}$$

Effective computable approximations of an [in]finite set of points; Trapezoidal linear congruences¹⁰



$$\begin{cases} 1x + 9y \in [0, 77] \pmod{10} \\ 2x - 1y \in [0, 99] \pmod{11} \end{cases}$$

Effective computable approximations of an [in]finite set of points; Linear congruences⁹



$$\begin{cases} 1x + 9y = 7 \pmod{8} \\ 2x - 1y = 9 \pmod{9} \end{cases}$$

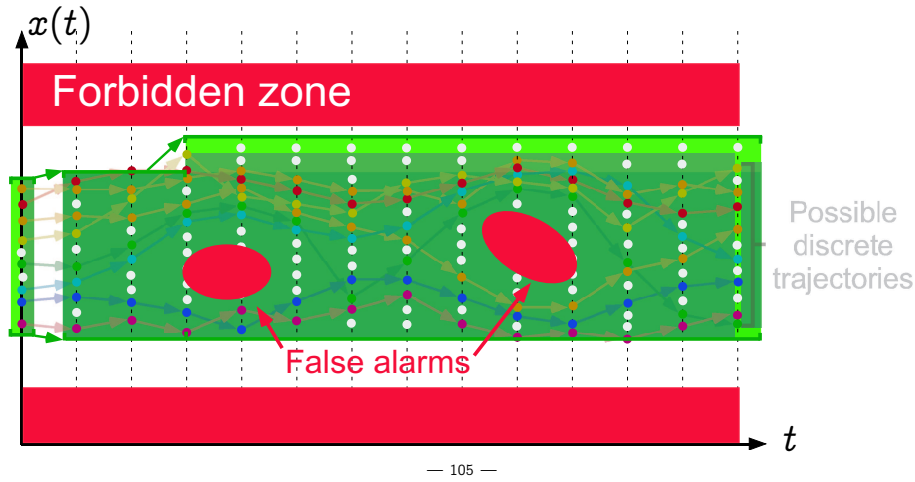
Refinement of iterates

⁸ Ph. Granger. *Static Analysis of Arithmetical Congruences*. Int. J. Comput. Math. 30, 1989, pp. 165–190.

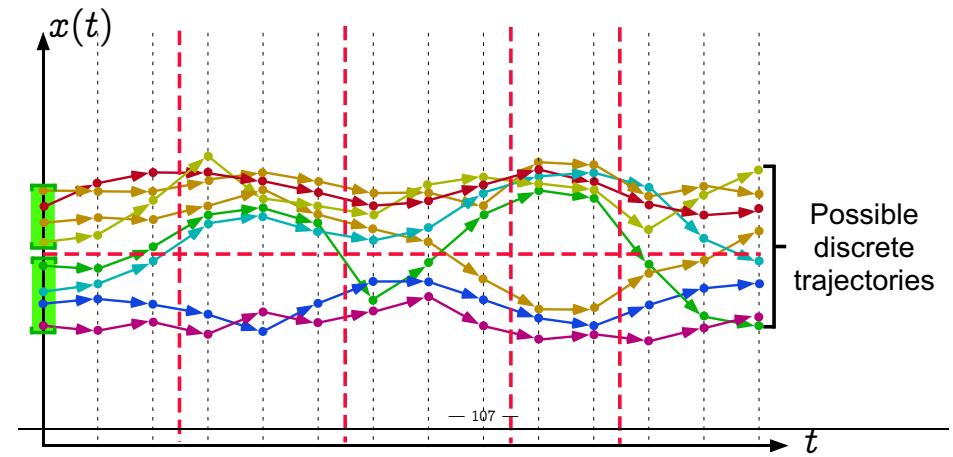
⁹ Ph. Granger. *Static Analysis of Linear Congruence Equalities among Variables of a Program*. TAPSOFT '91, pp. 169–192. LNCS 493, Springer, 1991.

¹⁰ F. Masdupuy. *Array Operations Abstraction Using Semantic Analysis of Trapezoid Congruences*. ACM ICS '92.

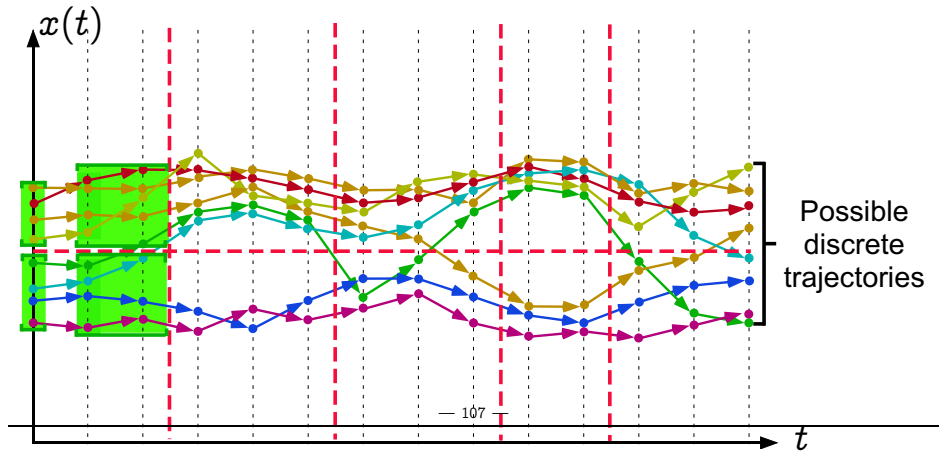
Graphic example: Refinement required by false alarms



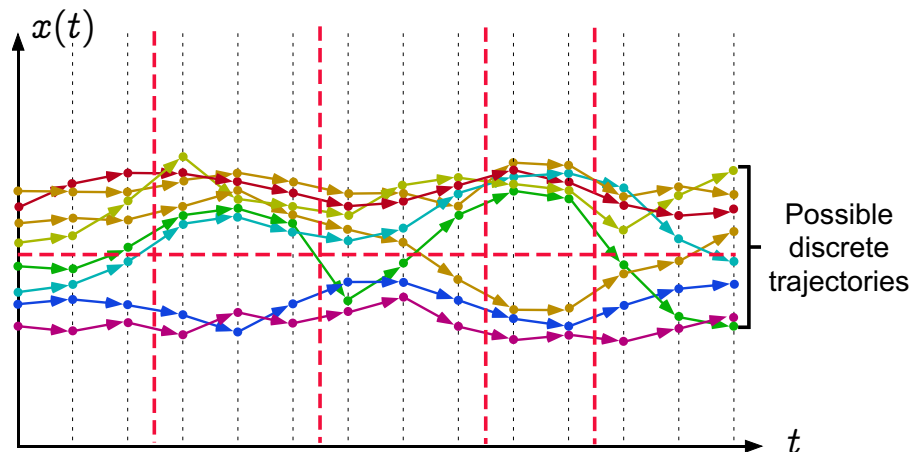
Graphic example: partitionned upward iteration with widening



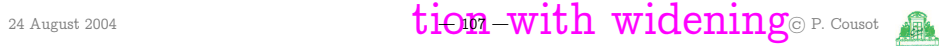
Graphic example: partitionned upward iteration with widening

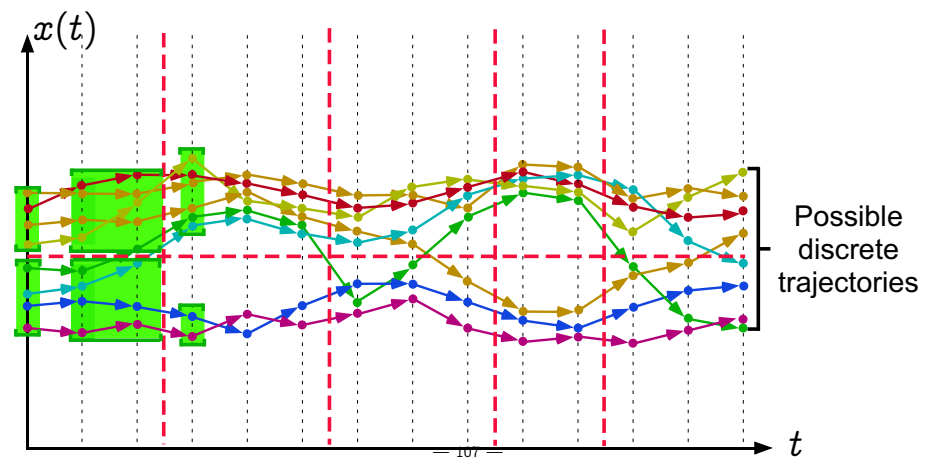


Graphic example: Partitionning

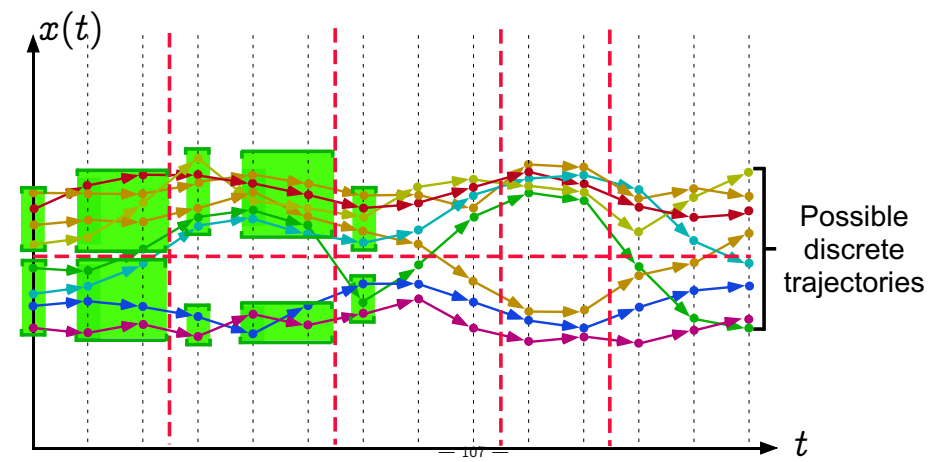


Graphic example: partitionned upward iteration with widening

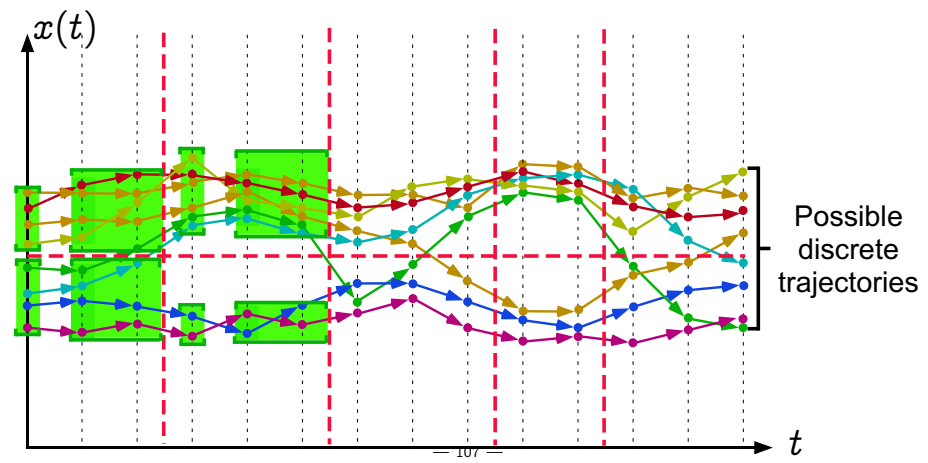




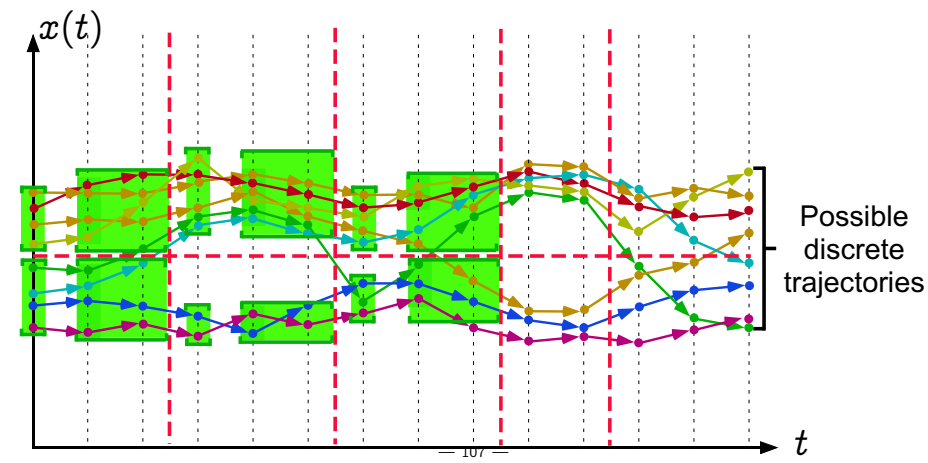
Graphic example: partitionned upward iteration with widening



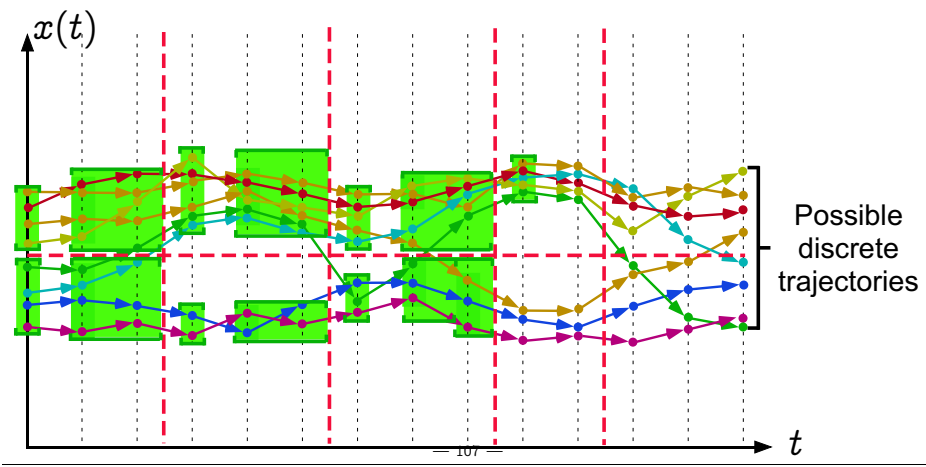
Graphic example: partitionned upward iteration with widening



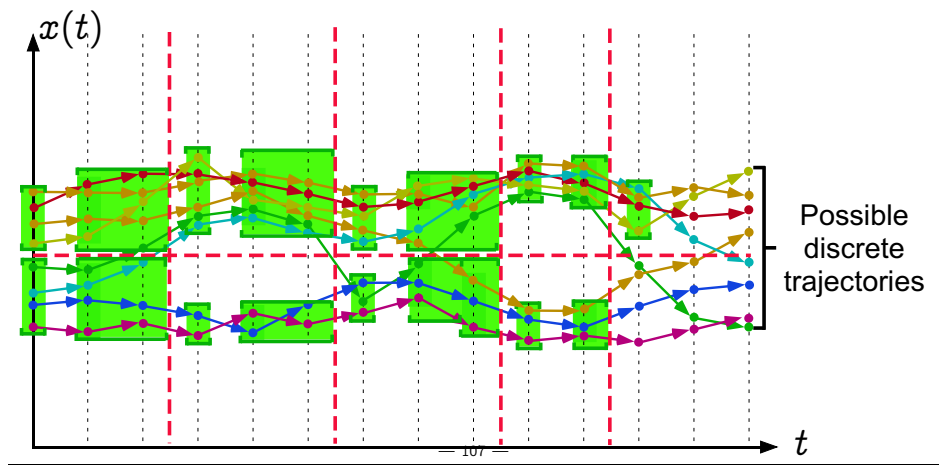
Graphic example: partitionned upward iteration with widening



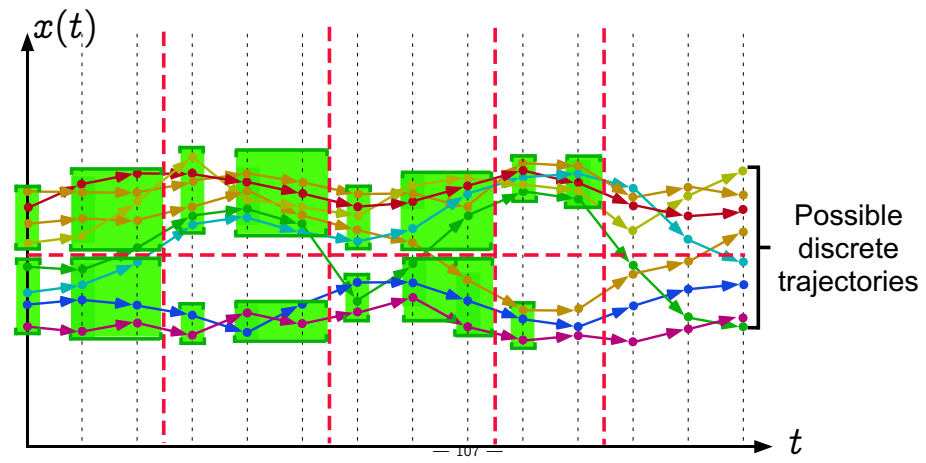
Graphic example: partitionned upward iteration with widening



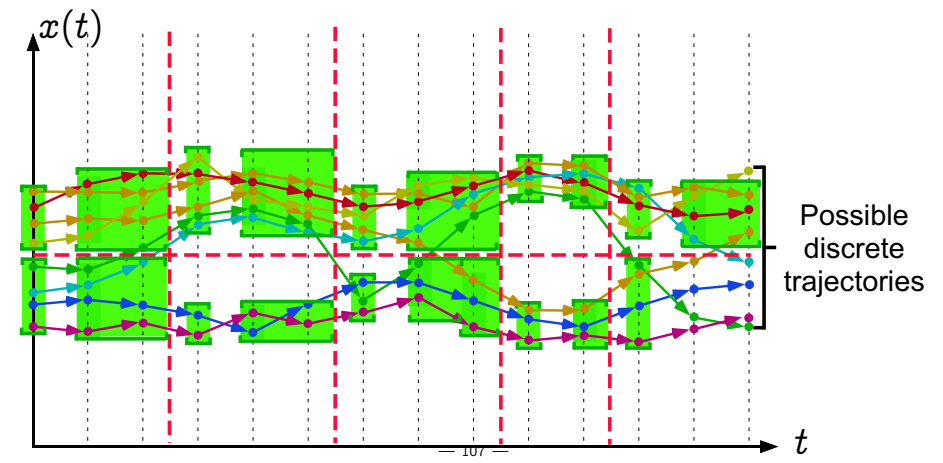
Graphic example: partitioned upward iteration with widening



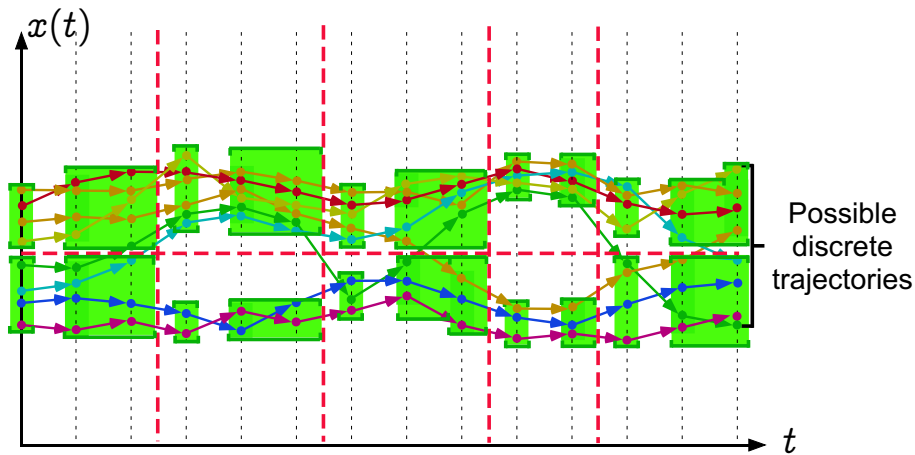
Graphic example: partitioned upward iteration with widening



Graphic example: partitioned upward iteration with widening



Graphic example: partitioned upward iteration with widening



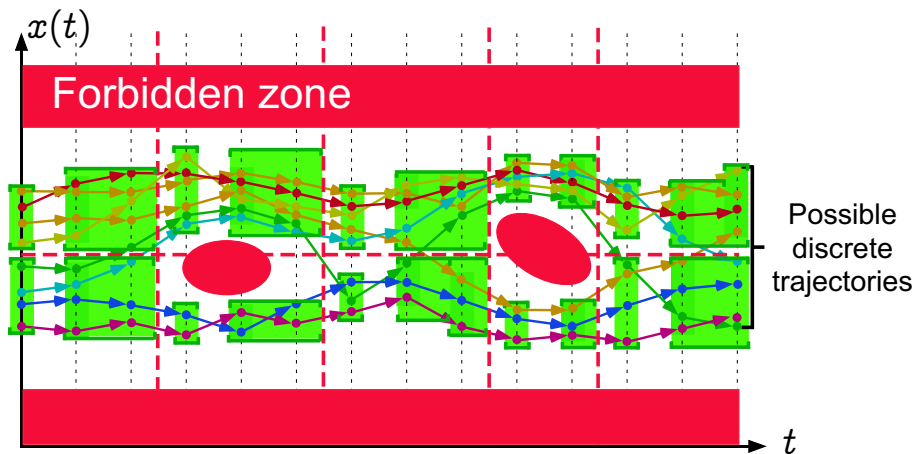
— 107 —

Examples of partitionnings

- sets of control states: attach local information to program points instead of global information for the whole program/procedure/loop
- sets of data states:
 - case analysis (test, switches)
- fixpoint iterates:
 - widening with threshold set

— 109 —

Graphic example: safety verification

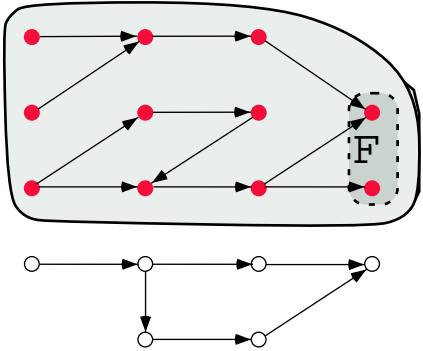


Interval widening with threshold set

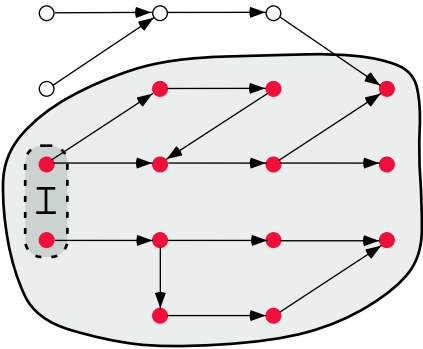
- The threshold set T is a finite set of numbers (plus $+\infty$ and $-\infty$),
- $[a, b] \nabla_T [a', b'] = [\text{if } a' < a \text{ then } \max\{\ell \in T \mid \ell \leq a'\} \text{ else } a, \\ \text{if } b' > b \text{ then } \min\{h \in T \mid h \geq b'\} \text{ else } b] .$
- Examples (intervals):
 - sign analysis: $T = \{-\infty, 0, +\infty\}$;
 - strict sign analysis: $T = \{-\infty, -1, 0, +1, +\infty\}$;
- T is a parameter of the analysis.

Combinations of abstractions

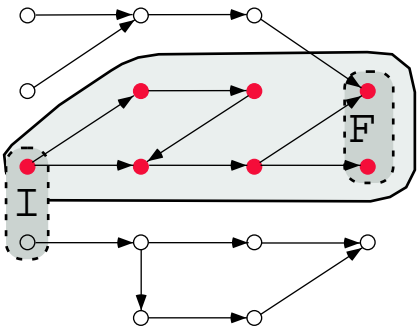
Backward/ancestry analysis



Forward/reachability analysis



Iterated forward/backward analysis



Example of iterated forward/backward analysis

Arithmetical mean of two integers x and y :

```
{x>=y}
while (x <> y) do
  {x>=y+2}
  x := x - 1;
  {x>=y+1}
  y := y + 1
  {x>=y}
od
{x=y}
```

Necessarily $x \geq y$ for proper termination

— 115 —

Example of iterated forward/backward analysis

Adding an auxiliary counter k decremented in the loop body and asserted to be null on loop exit:

```
{x=y+2k, x>=y}
while (x <> y) do
  {x=y+2k, x>=y+2}
  k := k - 1;
  {x=y+2k+2, x>=y+2}
  x := x - 1;
  {x=y+2k+1, x>=y+1}
  y := y + 1
  {x=y+2k, x>=y}
od
{x=y, k=0}
assume (k = 0)
{x=y, k=0}
```

Moreover **the difference of x and y must be even** for proper termination

Bibliography

— 117 —

Seminal papers

- Patrick Cousot & Radhia Cousot. [Abstract interpretation: a unified lattice model for static analysis of programs by construction or approximation of fixpoints](#). In 4th Symp. on Principles of Programming Languages, pages 238—252. ACM Press, 1977.
- Patrick Cousot & Nicolas Halbwachs. [Automatic discovery of linear restraints among variables of a program](#). In 5th Symp. on Principles of Programming Languages, pages 84—97. ACM Press, 1978.
- Patrick Cousot & Radhia Cousot. [Systematic design of program analysis frameworks](#). In 6th Symp. on Principles of Programming Languages pages 269—282. ACM Press, 1979.

Recent surveys

- Patrick Cousot. [Interprétation abstraite](#). Technique et Science Informatique, Vol. 19, Nb 1-2-3. Janvier 2000, Hermès, Paris, France. pp. 155-164. ■■
- Patrick Cousot. [Abstract Interpretation Based Formal Methods and Future Challenges](#). In Informatics, 10 Years Back — 10 Years Ahead, R. Wilhelm (Ed.), LNCS 2000, pp. 138-156, 2001.
- Patrick Cousot & Radhia Cousot. [Abstract Interpretation Based Verification of Embedded Software: Problems and Perspectives](#). In Proc. 1st Int. Workshop on Embedded Software, EMSOFT 2001, T.A. Henzinger & C.M. Kirsch (Eds.), LNCS 2211, pp. 97–113. Springer, 2001.

— 119 —

Conclusion

Theoretical applications of abstract interpretation

- [Static Program Analysis](#) [POPL '77,78,79] including [Data-flow Analysis](#) [POPL '79,00], [Set-based Analysis](#) [FPCA '95], etc
- [Syntax Analysis](#) [TCS 290(1) 2002]
- [Hierarchies of Semantics \(including Proofs\)](#) [POPL '92, TCS 277(1–2) 2002]
- [Typing](#) [POPL '97]
- [Model Checking](#) [POPL '00]
- [Program Transformation](#) [POPL '02]
- [Software watermarking](#) [POPL '04]

— 121 —

Practical applications of abstract interpretation

- [Program analysis and manipulation](#): a small rate of false alarms is acceptable
 - [AiT](#): [worst case execution time](#) – Christian Ferdinand
- [Program verification](#): no false alarms is acceptable
 - [TVLA](#): [A system for generating abstract interpreters](#) – Mooly Sagiv
 - [Astrée](#): [verification of absence of run-time errors](#) – Laurent Mauborgne

Industrial applications of abstract interpretation

- Both to **Program analysis and verification**
- **Experience with the industrial use of abstract interpretation-based static analysis tools** – Jean Souyris (Airbus France)

— 123 —

THE END

More references at URL www.di.ens.fr/~cousot.



IFIP WCC — Topical day on Abstract Interpretation, 24 August 2004

© P. Cousot



24 August 2004

— 124 —

© P. Cousot

