Comparing the Galois Connection and Widening/Narrowing Approaches to Abstract Interpretation

P. Cousot & R. Cousot

Abstract Interpretation (in theory)

Abstract Interpretation is method for deriving conservative approximations of the semantics of programming languages.

Abstract Interpretation is used to:

- Specify hierarchies of semantics of programming languages at different levels of abstraction.
- Design program proof methods.
- Specify automatic program analyzers (by interpretation of programs in abstract domains).
- Etc.

Abstract Interpretation (in Practice)

Abstract Interpretation is a method for the automatic, static and conservative determination of dynamic properties of programs:

- Automatic: no human intervention during the analysis (as opposed to proof methods).
- Static: without considering all possible runs (as opposed to model-checking).
- Conservative/sound: without omitting some runs (as opposed to debugging).
- Dynamic properties: semantic properties of the runtime behaviors (as opposed to program metrology).

Part 1

The Galois Connection Approach to Abstract Interpretation

Collecting Semantics

- For a given program, the problem is the effective computation of a sound approximation A of the collecting semantics, specifying the exact properties of concern. For simplicity:
  - The collecting semantics is $\mathrm{lfp}_{\perp}\, F$ where $\perp \in L$, $F \in L \xrightarrow{\mathrm{con}} L$ and $L(\sqsubseteq, \perp, \sqcup)$ is a cpo.
  - Soundness of the approximation A is defined by: $\mathrm{lfp}_{\perp}\, F \sqsubseteq A$.

Example: Declarative Semantics of a Logic Program

- B_P: Herbrand universe for program P.
- $\mathrm{ground}(P)$: set of all ground instances of clauses in P.
- The immediate consequence operator $T_P \in \wp(B_P) \xrightarrow{\mathrm{con}} \wp(B_P)$:

$$T_P(X) = \left\{A \;\middle|\; A \leftarrow B_1, \ldots, B_n \in \mathrm{ground}(P) \wedge \forall i = 1, \ldots, n : B_i \in X\right\}$$

- A model of P is $I \subseteq B_P$, such that $T_P(I) \subseteq I$.
- Characterization theorem of the least model M_P (van Emden and Kowalski):

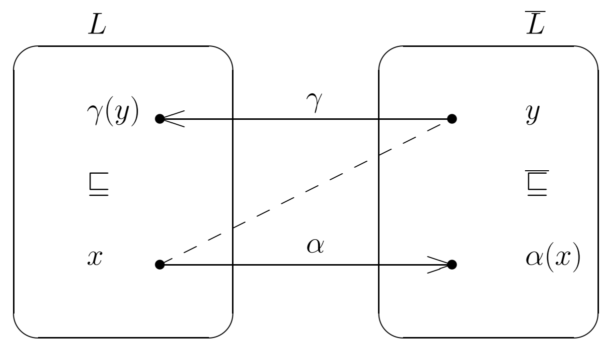
  $\wp(B_P)(\subseteq, \emptyset, \cup)$ is a complete lattice.

  $M_P = \mathrm{lfp}_{\emptyset}\, T_P = \cup_{n \in \mathbb{N}} {T_P}^n(\emptyset)$.

Property Approximation using Galois Connections

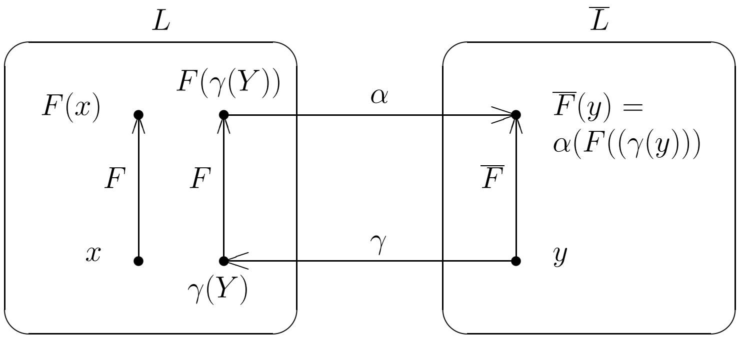
- Chose an abstract version $\overline{L}$ of the concrete properties L.
- Chose an abstract version $\overline{\sqsubseteq}$ of the concrete approximation relation $\sqsubseteq$.
- For each abstract property $y \in \overline{L}$ chose its concrete meaning $\gamma(y) \in L$.
- Decide once for all of the abstract approximation $\alpha(x) \in \overline{L}$ of any concrete property $x \in L$.

Galois Connections



- y is an approximation of x
- $\Leftrightarrow x \sqsubseteq \gamma(y)$
- $\Leftrightarrow \alpha(x)\ \overline{\sqsubseteq}\ y$

Extension of Galois Connections to Functions



- $\overline{F}$ is an approximation of F
- $\Leftrightarrow \alpha \circ F \circ \gamma \sqsubseteq \overline{F}$
- $\Leftrightarrow F \sqsubseteq \gamma \circ \overline{F} \circ \alpha$

Extension of Galois Connections from Properties to Higher-Order Property Transformers

- if $L \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} \overline{L}$ is a Galois connection, then:

$$\vec{\alpha} \in (L \longmapsto L) \longmapsto (\overline{L} \longmapsto \overline{L})$$
$$\vec{\alpha}(\varphi) \stackrel{\text{def}}{=} \alpha \circ \varphi \circ \gamma$$

$$\vec{\gamma} \in (\overline{L} \longmapsto \overline{L}) \longmapsto (L \longmapsto L)$$
$$\vec{\gamma}(\overline{\varphi}) \stackrel{\text{def}}{=} \gamma \circ \overline{\varphi} \circ \alpha$$

is a Galois connection:

$$(L \stackrel{\text{mon}}{\longmapsto} L) \underset{\vec{\alpha}}{\overset{\vec{\gamma}}{\leftrightarrows}} (\overline{L} \stackrel{\text{mon}}{\longmapsto} \overline{L})$$

Fixpoint Approximation using Galois Connections

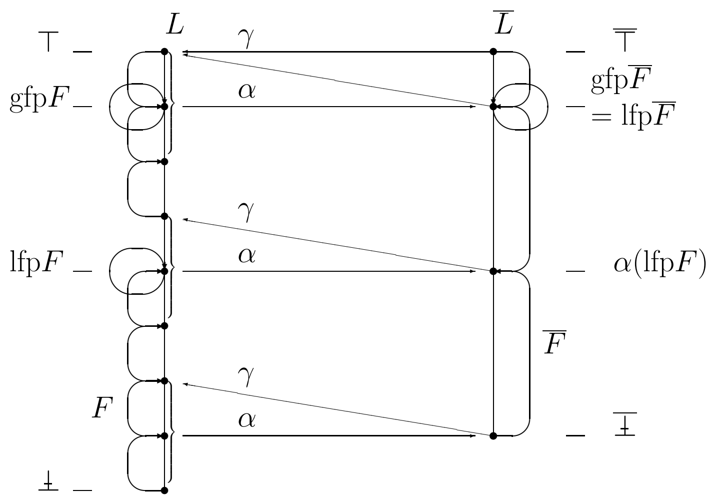
- $L(\sqsubseteq, \perp, \sqcup)$ is a cpo of concrete properties,
  $F \in (L \stackrel{\text{con}}{\longmapsto} L)$ is continuous,
  $\text{lfp}_{\perp} F = \sqcup_{n \geq 0} F^n(\perp)$ is not computable.
- Chose a cpo $\overline{L}(\overline{\sqsubseteq}, \overline{\perp}, \overline{\sqcup})$ of abstract properties such that $L \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} \overline{L}$.
- Define $\overline{F} = \alpha \circ F \circ \gamma$.
  and $\overline{\perp} = \alpha(\perp)$.
- then $\text{lfp}_{\perp} F \sqsubseteq \gamma(\text{lfp}_{\overline{\perp}}\ \overline{F})$.

Fixpoint Approximation Algorithm using Galois Connections

- If $\overline{L}$ is finite (or satisfies the ascending chain condition), you have got an effective program analysis algorithm:

$\langle \overline{\perp}, \overline{F} \rangle :=$ analysis(Program);
%% $\alpha(\perp) \,\overline{\sqsubseteq}\, \overline{\perp} \wedge \alpha \circ F \circ \gamma \,\overline{\sqsubseteq}\, \overline{F}$
$X := \overline{\perp}$;
repeat
  $Y := X$;
  $X := \overline{F}(X)$
until $Y = X$;
%% $\text{lfp}_{\perp} F \sqsubseteq \gamma(X) \wedge \text{lfp}_{\overline{\perp}} \overline{F} \,\overline{\sqsubseteq}\, X$

Fixpoint Approximation using Galois Connections



A Few Classical Examples: Example 1: Rule of Signs

- $L = \wp(\mathbb{Z})$ set of possible values of an integer variable.
- $\overline{L} =$
- $\alpha(X) = \sqcup\{\text{sign}(x) \mid x \in X\}$

Example 2: Mycroft's Strictness Analysis in Functional Programming

- $\mathbb{Z}_\bot = \mathbb{Z} \cup \bot$ $\quad\bot$ represent non-termination
- f is strict $\Leftrightarrow f(\bot) = \bot$
- $\Leftrightarrow f^*(\{\bot\}) \subseteq \{\bot\}$ where $f^*(X) = \{f(x) \mid x \in X\}$
- $L = \wp(\mathbb{Z}_\bot) \mapsto \wp(\mathbb{Z}_\bot)$
- $\overline{L} = \mathbb{B} \mapsto \mathbb{B}$ where $\mathbb{B} = \{0, 1\}$

Soundness of Strictness Analysis

- $\alpha(X) = 0$ if $X \subseteq \{\bot\}$
  $= 1$ if $X \not\subseteq \{\bot\}$
- $\gamma(0) = \{\bot\}$
  $\gamma(1) = \mathbb{Z}_\bot$
- $\vec{\alpha}(f^*) = \alpha \circ f^* \circ \gamma$
  $\vec{\gamma}(\overline{f}) = \gamma \circ \overline{f} \circ \alpha$
- $\overline{f}(0) = 0 \Rightarrow \alpha \circ f^* \circ \gamma(0) = 0 \Rightarrow \alpha \circ f^*(\{\bot\}) = 0 \Rightarrow f^*(\{\bot\}) \subseteq \{\bot\} \Leftrightarrow f$ is strict.

Example 3 : Mannila and Ukkonen Groundness Analysis in Logic Programming

- $\alpha(S) \;=\; \{\alpha_S(s) \mid s \in S\}$ set of states
- $\alpha_S(\langle g, \theta\rangle) \;=\; \alpha_g(g)$ state
- $\alpha_g(\Box) \;=\; \emptyset$ goal
- $\alpha_g(a_1 \ldots a_n\Box) \;=\; \{\alpha_a(a_i) \mid i = 1, \ldots, n\}$
- $\alpha_a(\mathtt{p}(t_1, \ldots, t_n)) \;=\; \mathtt{p}(\alpha_t(t_1), \ldots, \alpha_t(t_n))$ predicate
- $\alpha_t(\mathtt{X}) = \mathrm{NG}$ variable
- $\alpha_t(\mathtt{c}) = \mathrm{G}$ constant
- $\alpha_t(\mathtt{f}(t_1, \ldots, t_n)) = \mathrm{G}$ if $\forall i = 1, \ldots, n : \alpha_t(t_i) = \mathrm{G}$ term

  $= \mathrm{NG}$ if $\exists i = 1, \ldots, n : \alpha_t(t_i) = \mathrm{NG}$

On the Galois Connection Approach to abstract interpretation

- The approximation is done a priori, once for all $(L \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} \overline{L})$.
- The approximation α may be very rough.
- Usefulness of the approximation is shown by experience.
- The approximation is applied at each iteration step for $\overline{F} = \alpha \circ F \circ \gamma$.
- The approximation is independent of the iterates.
- $\overline{L}$ must satisfy the ascending chain condition.

Part 2

The Widening/Narrowing Approach

to Abstract Interpretation

Widening Operator

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

- $\forall x, y \in L : x \;\sqsubseteq\; x \nabla y$
- $\forall x, y \in L : y \;\sqsubseteq\; x \nabla y$
- for all increasing chains $x^0 \sqsubseteq x^1 \sqsubseteq \ldots$, the increasing chain defined by $y^0 = x^0, \ldots, y^{i+1} = y^i \nabla x^{i+1}, \ldots$ is not strictly increasing

Fixpoint Approximation with Widening

The upward iteration sequence with widening:

- $\hat{X}^0 = \overline{\bot}$
- $\hat{X}^{i+1} = \hat{X}^i$ if $\overline{F}(\hat{X}^i) \sqsubseteq \hat{X}^i$

  $= \hat{X}^i \triangledown F(\hat{X}^i)$ otherwise

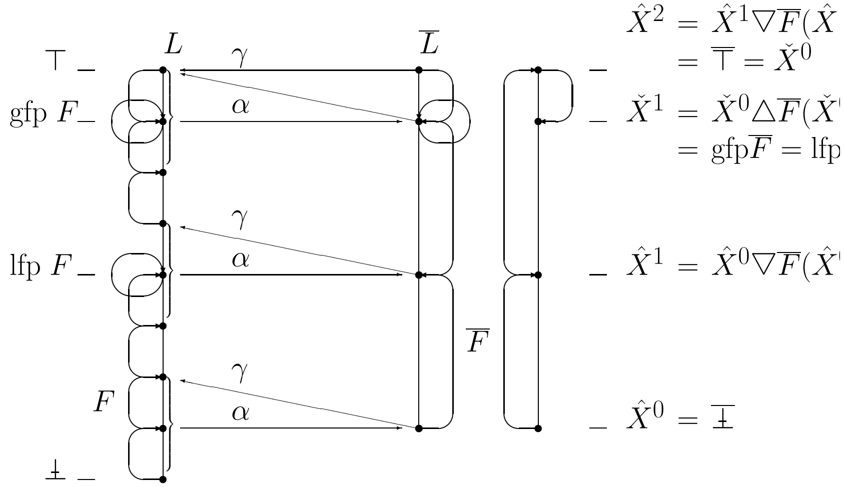
is ultimately stationary and its limit $\hat{A}$ is a sound upper approximation of $\mathrm{lfp}_{\overline{\bot}}$1.2cm25.0pt1.2cm1.2cm- $\overline{F}$:

$$\mathrm{lfp}_{\overline{\bot}}\text{1.2cm25.0pt1.2cm1.2cm-}\ \overline{F} \sqsubseteq \hat{A}$$

Program Analysis Algorithm with Widening

$\langle \overline{\bot}, \overline{F} \rangle :=$ analysis(Program);
%% $\alpha(\bot) \overline{\sqsubseteq}\, \overline{\bot} \wedge \alpha \circ F \circ \gamma \overline{\sqsubseteq}\, \overline{F}$
$X := \overline{\bot}$;
repeat
  $Y := X$;
  $X := \overline{F}(X)$
  if $X \overline{\sqsubseteq} Y$ **then** $C :=$ true
  else $C :=$ false; $X := Y \triangledown X$
until C;
%% $\mathrm{lfp}_{\bot} F \sqsubseteq \gamma(Y) \wedge \mathrm{lfp}_{\overline{\bot}} \overline{F} \overline{\sqsubseteq} Y$

Fixpoint Approximation with Widening/Narrowing



A Few Classical Examples: Example 1: Interval Analysis

Interval Analysis (Continued)

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

$$\begin{aligned} \bot \bigtriangledown X &= X \\ X \bigtriangledown \bot &= X \\ [\ell_0,\, u_0] \bigtriangledown [\ell_1,\, u_1] &= [\text{if } \ell_1 < \ell_0 \text{ then } -\infty \text{ else } \ell_0, \\ &\quad\ \ \text{if } \mathrm{u}_1 > \mathrm{u}_0 \text{ then } +\infty \text{ else } \mathrm{u}_0] \end{aligned}$$

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

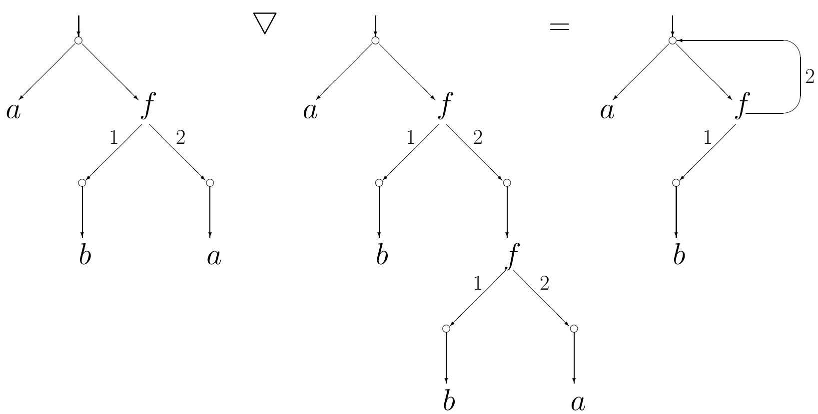
Improved Widening for Interval Analysis

- Extrapolate to zero, one or infinity:

$$\begin{aligned} \bot \bigtriangledown X &= X \\ X \bigtriangledown \bot &= X \\ [\ell_0,\, u_0] \bigtriangledown [\ell_1,\, u_1] &= [\text{if } \ell \leq \ell_1 < \ell_0 \ \wedge\ \ell \in \{1, 0, -1\} \text{ then } \mathrm{l} \\ &\quad\ \text{elsif } \ell_1 < \ell_0 \text{ then } -\infty \\ &\quad\ \text{else } \ell_0, \\ &\quad\ \text{if } \mathrm{u}_0 < \mathrm{u}_1 \leq \mathrm{u} \ \wedge\ \mathrm{u} \in \{-1, 0, 1\} \text{ then } \mathrm{u} \\ &\quad\ \text{elsif } \mathrm{u}_0 < \mathrm{u}_1 \text{ then } +\infty \\ &\quad\ \text{else } \mathrm{u}_0] \end{aligned}$$

- So the analysis is always as good as the sign analysis.

Example 2: Bruynooghe's Type Graph Widening



Example 3: Linear Inequalities & Application to Argument Size Analysis in Logic Programming

- Approximation of a term by its size:

$$\begin{aligned} \sigma(\mathtt{c}) \;=\; \sigma(\mathtt{X}) &= 1 \\ \sigma(\mathtt{f}(\mathtt{t}_1, \ldots, \mathtt{t}_n)) &= 1 + \Sigma_{i=1}^{n}\, \sigma(\mathtt{t}_i) \end{aligned}$$

- Approximation a set of points in $\mathbb{Z}^n$ by its convex hull:
  $\alpha_{\mathrm{A}}(X) = \lambda\mathtt{p}.\mathrm{ConvexHull}(\{\langle\sigma(\mathtt{t}_1), \ldots, \sigma(\mathtt{t}_\mathrm{n})\rangle \mid \mathtt{p}(\mathtt{t}_1, \ldots, \mathtt{t}_\mathrm{n}) \in \mathrm{X}\}$
- Approximation of a set of states by upper bounds of the argument sizes of the atoms occurring in these states:

$$\begin{aligned} \alpha_{\mathrm{g}}(\mathtt{a}_1 \ldots \mathtt{a}_n\Box) &= \{\mathtt{a}_i \mid i = 1, \ldots, n\} \qquad (\emptyset \text{ if } n = 0) \\ \alpha_{\mathrm{S}}(\langle \mathtt{g},\, \theta \rangle) &= \alpha_{\mathrm{g}}(\mathtt{g}) \\ \alpha(S) &= \alpha_{\mathrm{A}}\big(\cup\{\alpha_{\mathrm{S}}(s) \mid s \in S\}\big) \end{aligned}$$

Example of Argument Size Analysis

- Program testing for inequality of natural numbers $n \geq 0$ represented as successors $\texttt{s}^n\texttt{(0)}$ of zero:

```
p(X,X)     -> ;
p(X,s(Y)) -> p(X,Y) ;
```

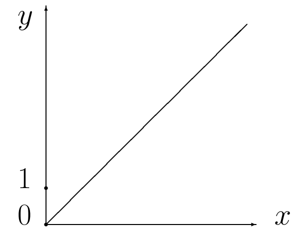
- Set of atoms: $\{\texttt{p(X,s}^n\texttt{(X))} \mid n \geq 0\}$
- Approximation: $\{\texttt{p(}x\texttt{,}y\texttt{)} \mid x \geq 0 \wedge y \geq 0 \wedge x \leq y\}$
- Fixpoint equation:

$$F(X) = \left\{\langle x,\, y\rangle \;\middle|\; x \geq 0 \wedge y \geq 0 \wedge ((x = y) \vee (\langle x,\, y-1\rangle \in X))\right\}$$

- The iterative computation of the least fixpoint does not converge in finitely many steps.

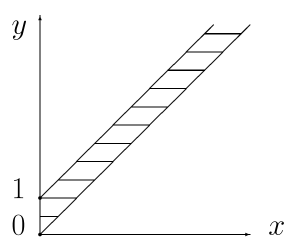
iteration with widening (1)

- $\hat{X}^0 = \emptyset$
- $\hat{X}^1 = F(\hat{X}^0)$
  $= \{\langle x,\, y\rangle \mid x \geq 0 \wedge x = y\}$



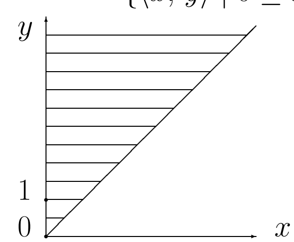
iteration with widening (2)

- $F(\hat{X}^1) = \{\langle x,\, y\rangle \mid 0 \leq x \leq y \leq x+1\}$



iteration with widening (3)

- $\hat{X}^2 = \hat{X}^1 \triangledown F(\hat{X}^1)$
  $= \{\langle x,\, y\rangle \mid 0 \leq x \leq y\}$



- $\hat{X}^3 = F(\hat{X}^2) = \hat{X}^2$

Widening of polyhedra

- Polyhedron P_1 is given by inequalities $S_1 = \{\beta_1, \ldots \beta_n\}$
- P_2 is represented by $S_2 = \{\gamma_1, \ldots \gamma_m\}$
- $P_1 \triangledown P_2$ is $S'_1 \cup S'_2$ where:
  - S'_1 is the set of inequalities $\beta_i \in S_1$ satisfied by all points of P_2
  - S'_2 is the set of linear inequalities $\gamma_i \in S_2$ which can replace some $\beta_j \in S_1$ without changing polyhedron P_1

Example:

$P_1 = \{\langle x, y\rangle \mid x \geq 0 \wedge x \leq y \wedge y \leq x\}$
$P_2 = \{\langle x, y\rangle \mid 0 \leq x \leq y \leq x + 1\}$
$P_1 \triangledown P_2 = \{\langle x, y\rangle \mid 0 \leq x \leq y\}$

On the Fixpoint Approximation using Widening Operators

- The approximation is done a priori, once for all ($L \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} \overline{L}$ and $\triangledown$).
- The approximation α may be precise while $\triangledown$ may be very rough.
- Usefulness of the approximation is shown by experience (precision/cos can be tuned with $\triangledown$).
- The approximation is applied at each iteration step for $\overline{F}$.
- The approximation is dependent of the iterates.
- $\overline{L}$ need not satisfy the ascending chain condition (since $\triangledown$ will be used to enforce convergence).

Part 3

Comparing

the Galois Connection

and

The Widening/Narrowing

Approaches to Abstract Interpretation

A Common Believe about Widenings

- Given an infinite abstract domain together with specific widening (and narrowing) operators, it is possible to find a finite lattice and a Galois connection which will give the same results.
- Hence the widening/narrowing approach to abstract interpretation is a useless trick.

What is Proved in the Paper ?

1. For each program there exists a finite lattice which can be used for this program to obtain results equivalent to those obtained using widening/narrowing operators;
2. No such a finite lattice will do for all programs;
3. For all programs, infinitely many abstract values are necessary;
4. For a particular program it is not possible to infer the set of needed abstract values by a simple inspection of the text of the program.

Example 1 : Linear inequality analysis

```
program PL;
    var I, J : integer;
begin
    I := 2; J := 0;
    while ... do begin
        { 2J+2 ≤ I ∧ 0 ≤ J }
        if ... then begin
            I := I + 4;
            { 2J+6 ≤ I ∧ 0 ≤ J }
        end else begin
            I := I + 2; J := J + 1;
            { 2J+2 ≤ I ∧ 1 ≤ J }
        end;
        { 2J+2 ≤ I ∧ 6 ≤ I+2J ∧ 0 ≤ J }
    end;
end.
```


Example 2 : Rational congruence analysis (Granger)

```
program PC;
    var X : real;
begin
    X := 2.8542;
    while ... do begin
        { X ≡ 1/5000 [1/500] }
        X := X + 1/500;
    end;
end.
```


Example 3 : Interval Analysis

```
program Function91ofMcCarthy;
    var X, Y : integer;
    function F(X : integer) : integer;
    begin
        if X > n then
            F := X − 10
        else
            F := F(F(X + 11));
    end;
begin
    readln(X);
    Y := F(X);
    { Y ∈ [n−9, maxint − 10] }
end.
```

```
program Function91ofMcCarthy;
    var X, Y : integer;
    function F(X : integer) : integer;
    begin
        if X > 100 then
            F := X − 10
            { F ∈ [91, maxint - 10] }
        else
            F := F(F(F(F(X + 33))));
            { F ∈ [91, 93] }
        { F ∈ [91, maxint - 10] }
  end;
begin
    readln(X);
    Y := F(X);
    { Y ∈ [91, maxint - 10] }
end.
```


Conclusion

- The Galois connection approach is the basic method of abstract interpretation.
- Combination with the widening/narrowing is the key to practical success:
  - Rich domain of information,
  - Convergence acceleration.
- Ideas for designing widenings/narrowings are given in the paper together with examples.