Extensive, locally complete abstract interpretation

Flavio Ascari

✉ flavio.ascari@phd.unipi.it

Supervisors

Roberto Bruni Roberta Gori

University of Pisa

IN SUPREMÆ DIGNITATIS · 1343 ·

UNIVERSITÀ DI PISA

Overview

Static analysis

Get information on program behaviour without executing it.

```
int a[6], b[6];
for (int i = 0; i <= 5; ++i) {
    int j = i * 2;
    a[j] += 1;
    b[i] += i;
}
```

↓

Access to a happens out of bounds.
Access to b is always correct.

Abstract interpretation

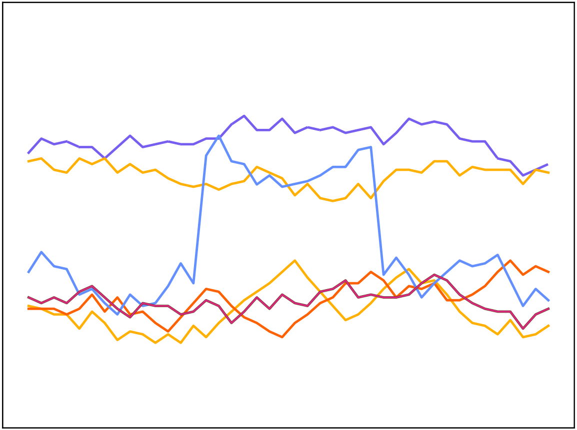
$$\begin{tikzcd} P^\sharp \arrow[r, "\llbracket \mathsf{r} \rrbracket^A"] & Q^\sharp \\ P \arrow[u] \arrow[r, "\llbracket \mathsf{r} \rrbracket"] & Q \arrow[u] \end{tikzcd}$$

Abstract interpretation

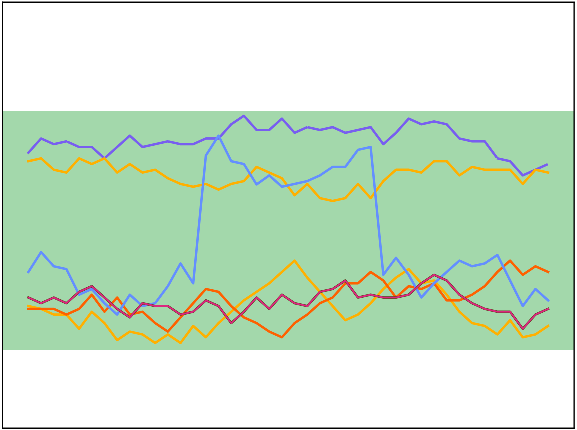
$$\begin{tikzcd} P^\sharp \arrow[r, "[\![\mathrm{r}]\!]^A"] & Q^\sharp \\ P \arrow[u] \arrow[r, "[\![\mathrm{r}]\!]"] & Q \arrow[u] \end{tikzcd}$$

```
int a[6], b[6];
for (int i = 0; i <= 5; ++i) {      // i in [0, 5]
    int j = i * 2;                  // j in [0, 5] * 2
                                    //      = [0, 10]
    a[j] += 1;
    b[i] += i;
}
```

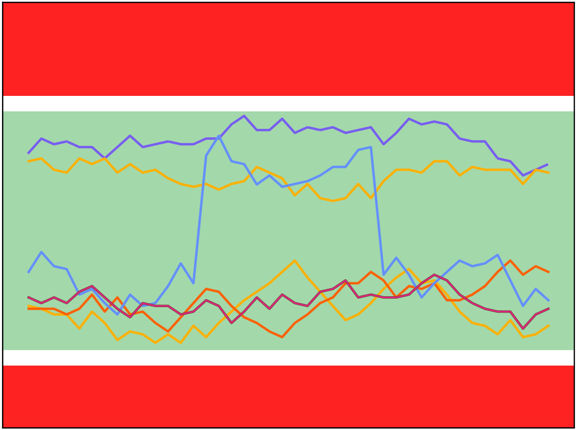
Static analysis - over-approximation



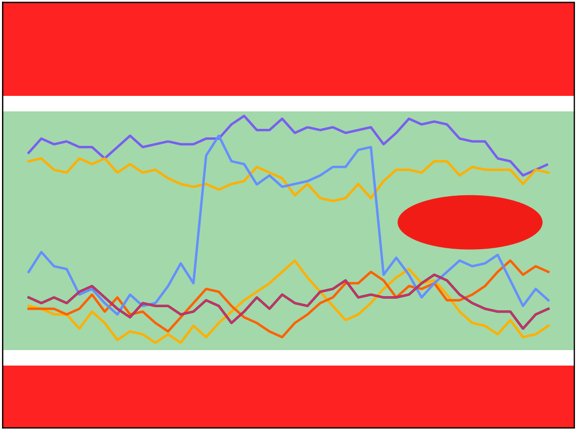
Static analysis - over-approximation



Static analysis - over-approximation

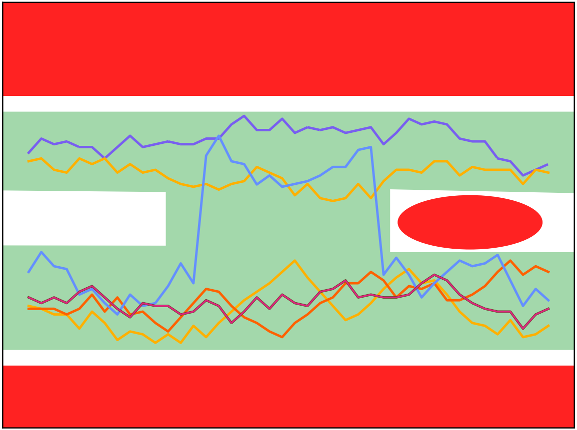


Static analysis - over-approximation



False alarm!

Static analysis - over-approximation



Completeness

Completeness

A is complete for r if

$$A[\![\mathsf{r}]\!]A = A[\![\mathsf{r}]\!]$$

Completeness

Completeness

A is complete for r if

$$A[\![\mathrm{r}]\!]A = A[\![\mathrm{r}]\!]$$

Local completeness

A is locally complete for r on P if

$$A[\![\mathrm{r}]\!]A(P) = A[\![\mathrm{r}]\!](P)$$

Completeness

Completeness

A is complete for r if

$$A[\![\mathsf{r}]\!]A = A[\![\mathsf{r}]\!]$$

Local completeness

A is locally complete for r on P if

$$A[\![\mathsf{r}]\!]A(P) = A[\![\mathsf{r}]\!](P)$$

Both *extensional* properties, only depending on $[\![\mathsf{r}]\!]$ and not r.

Completeness

Completeness

A is complete for r if

$$A[\![\mathsf{r}]\!]A = A[\![\mathsf{r}]\!]$$

Local completeness

A is locally complete for r on P if

$$A[\![\mathsf{r}]\!]A(P) = A[\![\mathsf{r}]\!](P)$$

Both *extensional* properties, only depending on $[\![\mathsf{r}]\!]$ and not r.
However state of the art techniques prove *intensional* properties such as

$$[\![\mathsf{r}]\!]^{\sharp}_{A} A = A[\![\mathsf{r}]\!]$$

$$[\![\mathsf{r}]\!]^{\sharp}_{A} A(P) = A[\![\mathsf{r}]\!](P)$$

Intensional vs extensional

$$\mathsf{r} = \mathtt{skip}$$

Intensional vs extensional

$$\mathsf{r} = \mathtt{skip}$$

$$\mathsf{r}' = \mathtt{x\ :=\ x\ +\ 1;\ x\ :=\ x\ -\ 1}$$

Intensional vs extensional

$$\mathsf{r} = \texttt{skip}$$

$$\mathsf{r}' = \texttt{x := x + 1; x := x - 1}$$

Different *syntax* $\mathsf{r} \neq \mathsf{r}'$

Intensional vs extensional

$$\mathsf{r} = \texttt{skip}$$

$$\mathsf{r}' = \texttt{x := x + 1; x := x - 1}$$

Different *syntax* $\mathsf{r} \neq \mathsf{r}'$ but same *semantics* $[\![\mathsf{r}]\!] = [\![\mathsf{r}']\!]$!

Example

Analysis in $A = \mathsf{Sign} = \{\bot, +, -, 0, \top\}$.

$\mathsf{r} = \texttt{skip}$ $\qquad$ $\mathsf{r}' = \texttt{x := x + 1; x := x - 1}$

Example

Analysis in $A = \text{Sign} = \{\bot, +, -, 0, \top\}$.

$\mathsf{r} = \texttt{skip}$

$\mathsf{r}' = \texttt{x := x + 1; x := x - 1}$

$[\![\mathsf{r}]\!]^\sharp_A A = \text{id} = A[\![\mathsf{r}]\!]$

Example

Analysis in $A = \text{Sign} = \{\bot, +, -, 0, \top\}$.

$\mathsf{r} = \texttt{skip}$

$\mathsf{r}' = \texttt{x := x + 1; x := x - 1}$

$[\![\mathsf{r}]\!]^\sharp_A A = \text{id} = A[\![\mathsf{r}]\!]$

$[\![\mathsf{r}']\!]^\sharp_A A \neq \text{id} = A[\![\mathsf{r}']\!]$

$$\begin{aligned}
&[\![\mathsf{r}']\!]^\sharp_A A(0) \\
&= [\![\texttt{x := x - 1}]\!]^\sharp_A [\![\texttt{x := x + 1}]\!]^\sharp_A (0) \\
&= [\![\texttt{x := x - 1}]\!]^\sharp_A (+) \\
&= \top
\end{aligned}$$

Local Completeness Logic

$$\frac{\mathbb{C}^A_P(\llbracket \mathsf{e} \rrbracket)}{\vdash_A [P]\ \mathsf{e}\ [\llbracket \mathsf{e} \rrbracket P]}\ \text{(transfer)} \qquad \frac{P' \le P \le A(P') \quad \vdash_A [P']\ \mathsf{r}\ [Q'] \quad Q \le Q' \le A(Q)}{\vdash_A [P]\ \mathsf{r}\ [Q]}\ \text{(relax)}$$

$$\frac{\vdash_A [P]\ \mathsf{r}_1\ [R] \quad \vdash_A [R]\ \mathsf{r}_2\ [Q]}{\vdash_A [P]\ \mathsf{r}_1; \mathsf{r}_2\ [Q]}\ \text{(seq)} \qquad \frac{\vdash_A [P]\ \mathsf{r}_1\ [Q_1] \quad \vdash_A [P]\ \mathsf{r}_2\ [Q_2]}{\vdash_A [P]\ \mathsf{r}_1 \oplus \mathsf{r}_2\ [Q_1 \vee Q_2]}\ \text{(join)}$$

$$\frac{\vdash_A [P]\ \mathsf{r}\ [R] \quad \vdash_A [P \vee R]\ \mathsf{r}^*\ [Q]}{\vdash_A [P]\ \mathsf{r}^*\ [Q]}\ \text{(rec)} \qquad \frac{\vdash_A [P]\ \mathsf{r}\ [Q] \quad Q \le A(P)}{\vdash_A [P]\ \mathsf{r}^*\ [P \vee Q]}\ \text{(iterate)}$$

The proof system LCL_A[1].

A triple $\vdash_A [P]\ \mathsf{r}\ [Q]$ of the logic means that $\llbracket \mathsf{r} \rrbracket^\sharp_A A(P) = A \llbracket \mathsf{r} \rrbracket (P)$.
Depends on $\llbracket \mathsf{r} \rrbracket^\sharp_A$: intensional property.

[1] Roberto Bruni et al. "A Logic for Locally Complete Abstract Interpretations". In: *Logic in Computer Science, 2021*.

Refinement rule

$$\frac{\vdash_{A'} [P]\ \mathsf{r}\ [Q] \quad A' \preceq A \quad A[\![\mathsf{r}]\!]^{A'} A(P) = A(Q)}{\vdash_A [P]\ \mathsf{r}\ [Q]}\ \text{(refine-ext)}$$

The novel rule (refine-ext).

With this rule, $\vdash_A [P]\ \mathsf{r}\ [Q]$ means that $A[\![\mathsf{r}]\!]A(P) = A[\![\mathsf{r}]\!](P)$.
Only depends on $[\![\mathsf{r}]\!]$: extensional property!

Logical completeness

Theorem

If $A[\![r]\!]A(P) = A[\![r]\!](P)$ then $\vdash_A [P]\ r\ [Q]$.

This statement actually lacks some of the hypotheses, omitted for the sake of presentation.

Derived rules

$$\frac{\vdash_{A'} [P]\ \mathsf{r}\ [Q] \quad A' \preceq A \quad A[\![\mathsf{r}]\!]^{\sharp}_{A'} A(P) = A(Q)}{\vdash_{A} [P]\ \mathsf{r}\ [Q]}\ \text{(refine-int)}$$

$$\frac{\vdash_{A'} [P]\ \mathsf{r}\ [Q] \quad A' \preceq A \quad A'(P) = A(P)}{\vdash_{A} [P]\ \mathsf{r}\ [Q]}\ \text{(refine-pre)}$$

Future works

- Heuristics (when and how to refine)
- Relations to model checking (CEGAR)
- Simplification (simplify instead of refining)
- Metrics (eg. partial completeness)
- ...

Thanks for your attention!

Flavio Ascari
✉ flavio.ascari@phd.unipi.it