New York University, CIMS, CS, Course CSCI-GA.3140-001, Spring 2024

“Abstract Interpretation”

Ch. 7, Maximal Trace Semantics

Patrick Cousot

pcousot@cs.nyu.edu cs.nyu.edu/~pcousot

Class 2, Monday, January 29th, 2024, 4:55-6:55 PM, WWH, Room CIWW 202

These slides are available at
http://cs.nyu.edu/~pcousot/courses/spring24/CSCI-GA.3140-001/slides/02--2024-01-29-syntax-semantics-traces-oo//slides-07--maximal-trace-semantics-AI.pdf

Chapter 7

Ch. 7, Maximal Trace Semantics

Finite maximal trace semantics

- $\boldsymbol{\mathcal{S}}^{+}[\![\mathsf{S}]\!](\pi_1\mathsf{at}[\![\mathsf{S}]\!]) \quad \triangleq \quad \{\pi_2\ell \in \boldsymbol{\mathcal{S}}^{*}[\![\mathsf{S}]\!](\pi_1\mathsf{at}[\![\mathsf{S}]\!]) \mid \ell = \mathsf{after}[\![\mathsf{S}]\!]\}$
- $\boldsymbol{\mathcal{S}}^{+}[\![\mathsf{S}]\!](\pi_1\ell) \quad = \quad \emptyset$ when $\ell \neq \mathsf{at}[\![\mathsf{S}]\!]$

- $\boldsymbol{\mathcal{S}}^{+}[\![\mathsf{S}]\!](\pi_1\mathsf{at}[\![\mathsf{S}]\!])$ is the set of maximal finite traces $\mathsf{at}[\![\mathsf{S}]\!]\pi_2\mathsf{after}[\![\mathsf{S}]\!]$ of S continuing the trace $\pi_1\mathsf{at}[\![\mathsf{S}]\!]$ and reaching $\mathsf{after}[\![\mathsf{S}]\!]$.
- Schematically,

$$\xrightarrow{\quad\pi_1\quad} \underbrace{\mathsf{at}[\![\mathsf{S}]\!] \xrightarrow{\quad\pi_2\quad} \mathsf{after}[\![\mathsf{S}]\!]}_{\in\ \boldsymbol{\mathcal{S}}^{+}[\![\mathsf{S}]\!](\pi_1\mathsf{at}[\![\mathsf{S}]\!])}$$

© P. Cousot, NYU, CIMS, CS, Monday, January 29th, 2024

Prefixes of a trace

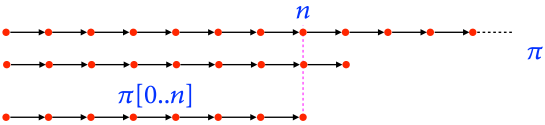
- If $\pi = \ell_0 \xrightarrow{e_0} \ldots \ell_i \xrightarrow{e_i} \ldots \ell_n$ is a finite trace then its prefix $\pi[0..p]$ at p is
  - π when $p \geqslant n$
  - $\ell_0 \xrightarrow{e_0} \ldots \ell_j \xrightarrow{e_j} \ldots \ell_p$ when $0 \leqslant p \leqslant n$.
- If $\pi = \ell_0 \xrightarrow{e_0} \ldots \ell_i \xrightarrow{e_i} \ldots$ is an infinite trace then its prefix $\pi[0..p]$ at p is

$\ell_0 \xrightarrow{e_0} \ldots \ell_j \xrightarrow{e_j} \ldots \ell_p$.

© P. Cousot, NYU, CIMS, CS, Monday, January 29th, 2024

Prefixes of a trace

- If $\pi = \ell_0 \xrightarrow{e_0} \ldots \ell_i \xrightarrow{e_i} \ldots \ell_n$ is a finite trace then its prefix $\pi[0..p]$ at p is
  - π when $p \geqslant n$
  - $\ell_0 \xrightarrow{e_0} \ldots \ell_j \xrightarrow{e_j} \ldots \ell_p$ when $0 \leqslant p \leqslant n$.
- If $\pi = \ell_0 \xrightarrow{e_0} \ldots \ell_i \xrightarrow{e_i} \ldots$ is an infinite trace then its prefix $\pi[0..p]$ at p is $\ell_0 \xrightarrow{e_0} \ldots \ell_j \xrightarrow{e_j} \ldots \ell_p$.



Limit of prefix traces (I)

- Given a set $\mathscr{T} \in \wp(\mathbb{T}^+)$ of finite traces, its limit $\lim \mathscr{T}$ is the set of infinite traces which prefixes are traces in $\mathscr{T}$.

$$\lim \mathscr{T} \quad \triangleq \quad \{\pi \in \mathbb{T}^\infty \mid \forall n \in \mathbb{N} \mathrel{.} \pi[0..n] \in \mathscr{T}\}\,.$$

- $\lim \varnothing = \varnothing$.
- Requires $\mathscr{T}$ to be prefix closed.

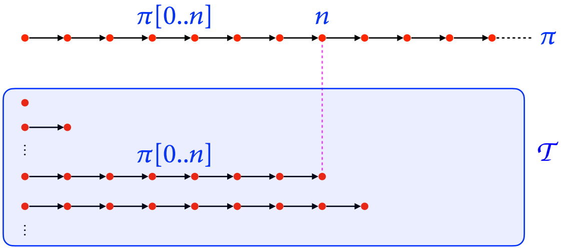
 © P. Cousot, NYU, CIMS, CS, Monday, January 29th, 2024

Limit of prefix traces (I)

- Given a set $\mathscr{T} \in \wp(\mathbb{T}^+)$ of finite traces, its limit $\lim \mathscr{T}$ is the set of infinite traces which prefixes are traces in $\mathscr{T}$.

$$\lim \mathscr{T} \quad \triangleq \quad \{\pi \in \mathbb{T}^\infty \mid \forall n \in \mathbb{N} \mathrel{.} \pi[0..n] \in \mathscr{T}\} .$$

- $\lim \varnothing = \varnothing$.
- Requires $\mathscr{T}$ to be prefix closed.



en.wikipedia.org/wiki/Inverse_limit

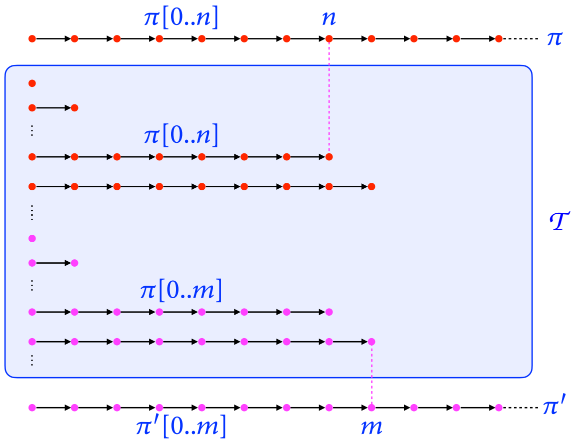
© P. Cousot, NYU, CIMS, CS, Monday, January 29th, 2024

Example I of limit of prefix traces

- The prefix semantics of the program $\mathsf{S} = \mathbf{while}\ ^{\ell_1}\ (\mathsf{tt})\ ^{\ell_2}\ \mathsf{x} = \mathsf{x} + 1\ ;^{\ell_3}$ is
$$\boldsymbol{\mathcal{S}}^*[\![\mathsf{S}]\!](\ell_1) = \Big\{\Big(\ell_1 \xrightarrow{\mathsf{tt}} \ell_2 \xrightarrow{\mathsf{x}\,=\,i} \ell_1\Big)_{i=1}^{n}, \Big(\ell_1 \xrightarrow{\mathsf{tt}} \ell_2 \xrightarrow{\mathsf{x}\,=\,i} \ell_1\Big)_{i=1}^{n} \xrightarrow{\mathsf{tt}} \ell_2 \;\Big|\; n \in \mathbb{N}\Big\}.$$
- Its limit is $\lim(\boldsymbol{\mathcal{S}}^*[\![\mathsf{S}]\!](\ell_1)) = \{\pi\}$ where the infinite trace is $\pi = \Big(\ell_1 \xrightarrow{\mathsf{tt}} \ell_2 \xrightarrow{\mathsf{x}\,=\,i}\Big)_{i=1}^{\infty}$.
- All prefixes of π belong to $\boldsymbol{\mathcal{S}}^*[\![\mathsf{S}]\!](\ell_1)$.

© P. Cousot, NYU, CIMS, CS, Monday, January 29th, 2024

Multiple limits



For a given set of prefixes, the limit is unique.

Limit of prefix traces (II)

- A general definition of the limit should not require the set $\mathscr{T} \in \wp(\mathbb{T}^{+})$ of finite traces to be closed by prefix
- It consists in defining limit $\lim \mathscr{T}$ as the set of infinite traces which prefixes can be extended to a trace in $\mathscr{T}$.

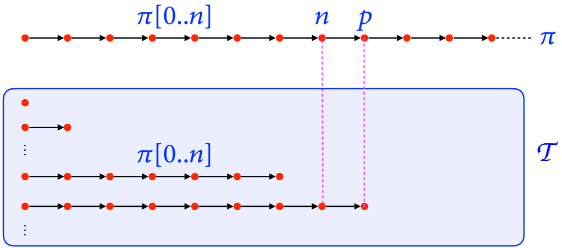
$$\lim \mathscr{T} \quad \triangleq \quad \{\pi \in \mathbb{T}^{\infty} \mid \forall n \in \mathbb{N} \mathrel{.} \exists p \geqslant n \mathrel{.} \pi[0..p] \in \mathscr{T}\}\,.$$

© P. Cousot, NYU, CIMS, CS, Monday, January 29th, 2024

Limit of prefix traces (II)

- A general definition of the limit should not require the set $\mathscr{T} \in \wp(\mathbb{T}^+)$ of finite traces to be closed by prefix
- It consists in defining limit $\lim \mathscr{T}$ as the set of infinite traces which prefixes can be extended to a trace in $\mathscr{T}$.

$$\lim \mathscr{T} \quad \triangleq \quad \{\pi \in \mathbb{T}^\infty \mid \forall n \in \mathbb{N} \,.\, \exists p \geqslant n \,.\, \pi[0..p] \in \mathscr{T}\}\,.$$



Example II of limit of prefix traces

- $\lim\left\{\left(\ell_1 \xrightarrow{\mathtt{tt}} \ell_2 \xrightarrow{\mathsf{x} = i} \ell_1\right)_{i=1}^{n} \;\Big|\; n \in \mathbb{N}\right\} = \{\pi\}$ where $\pi = \pi = \left(\ell_1 \xrightarrow{\mathtt{tt}} \ell_2 \xrightarrow{\mathsf{x} = i} \right)_{i=1}^{\infty}$.
- All prefixes of π are of the form $\left(\ell_1 \xrightarrow{\mathtt{tt}} \ell_2 \xrightarrow{\mathsf{x} = i} \ell_1\right)_{i=1}^{n}$ or $\left(\ell_1 \xrightarrow{\mathtt{tt}} \ell_2 \xrightarrow{\mathsf{x} = i} \ell_1\right)_{i=1}^{n} \xrightarrow{\mathtt{tt}} \ell_2$

  and this last one can be extended to a finite trace $\left(\ell_1 \xrightarrow{\mathtt{tt}} \ell_2 \xrightarrow{\mathsf{x} = i} \ell_1\right)_{i=1}^{n+1}$.

Infinite maximal trace semantics

$$\mathcal{S}^{\infty}[\![\mathsf{S}]\!](\pi^{\ell}) \quad \triangleq \quad \lim(\mathcal{S}^{*}[\![\mathsf{S}]\!](\pi^{\ell})).$$

Maximal finite and infinite trace semantics

- The maximal trace semantics is the set of traces which are either finite

$$\boldsymbol{\mathcal{S}}^{+}[\![\mathsf{S}]\!](\pi_1\mathsf{at}[\![\mathsf{S}]\!]) \quad \triangleq \quad \{\pi_2{}^{\ell} \in \boldsymbol{\mathcal{S}}^{*}[\![\mathsf{S}]\!](\pi_1\mathsf{at}[\![\mathsf{S}]\!]) \mid \ell = \mathsf{after}[\![\mathsf{S}]\!]\} \tag{6.9}$$

or infinite defined as limits of finite prefix traces.

$$\begin{aligned}
\boldsymbol{\mathcal{S}}^{+\infty}[\![\mathsf{S}]\!](\pi^{\ell}) \quad &\triangleq \quad \boldsymbol{\mathcal{S}}^{+}[\![\mathsf{S}]\!](\pi^{\ell}) \cup \boldsymbol{\mathcal{S}}^{\infty}[\![\mathsf{S}]\!](\pi^{\ell}) && (7.7)\\
\boldsymbol{\mathcal{S}}^{+\infty}[\![\mathsf{S}]\!]\Pi \quad &\triangleq \quad \bigcup\{\boldsymbol{\mathcal{S}}^{+\infty}[\![\mathsf{S}]\!](\pi^{\ell}) \mid \pi^{\ell} \in \Pi\}\\
\boldsymbol{\mathcal{S}}^{+\infty}[\![\mathsf{S}]\!] \quad &\triangleq \quad \boldsymbol{\mathcal{S}}^{+\infty}[\![\mathsf{S}]\!](\mathbb{T}^{+})\\
\boldsymbol{\mathcal{S}}^{+\infty}[\![\mathsf{P}]\!] \quad &\triangleq \quad \boldsymbol{\mathcal{S}}^{+\infty}[\![\mathsf{P}]\!](\{\mathsf{at}[\![\mathsf{P}]\!]\}).
\end{aligned}$$

© P. Cousot, NYU, CIMS, CS, Monday, January 29th, 2024

Example II of limit of prefix traces

- The maximal trace semantics of the program $\mathtt{S} = \mathtt{while}\ ^{\ell_1}\ (\mathtt{tt})\ ^{\ell_2}\ \mathtt{x = x + 1}\ ;^{\ell_3}$ is $\mathcal{S}^{+\infty}[\![\mathtt{S}]\!](\ell_1) = \left\{\left(\ell_1 \xrightarrow{\ \mathtt{tt}\ } \ell_2 \xrightarrow{\ \mathtt{x} = i\ }\right)_{i=1}^{\infty}\right\}$.

© P. Cousot, NYU, CIMS, CS, Monday, January 29th, 2024

Conclusion

Conclusion

- We have defined the maximal trace semantics of a subset of C
- Its abstractions will yield verification and static analysis methods for safety and security

The End, Thank you