Principles of Abstract Interpretation
MIT press

Ch. **7**, Maximal trace semantics

Patrick Cousot

pcousot.github.io

PrAbsInt@gmail.com   github.com/PrAbsInt/

These slides are available at
http://github.com/PrAbsInt/slides/slides/slides-07--maximal-trace-semantics-PrAbsInt.pdf

Chapter 7

Ch. **7**, Maximal trace semantics

Finite maximal trace semantics

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

- $\mathcal{S}^+[\![\mathsf{S}]\!](\pi_1\mathsf{at}[\![\mathsf{S}]\!])$ 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,

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

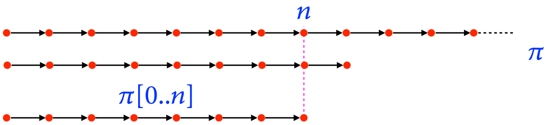
© P. Cousot, NYU, CIMS, CS

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

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

Limit of prefix traces (I)

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

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

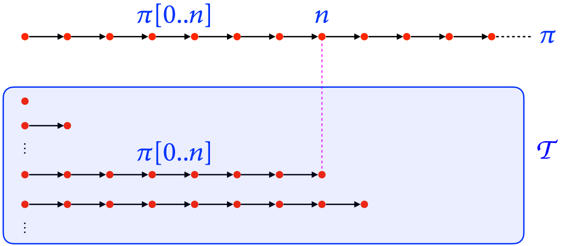
- $\lim \varnothing = \varnothing$.
- Requires $\mathcal{T}$ to be prefix closed.

Limit of prefix traces (I)

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

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

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



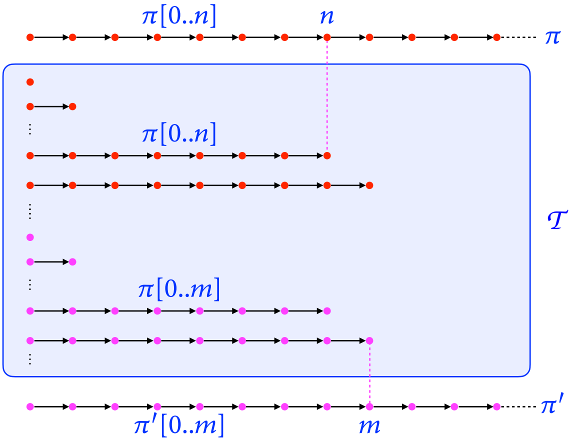
en.wikipedia.org/wiki/Inverse_limit

Example I of limit of prefix traces

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

© P. Cousot, NYU, CIMS, CS

Multiple limits



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

 © P. Cousot, NYU, CIMS, CS

Limit of prefix traces (II)

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

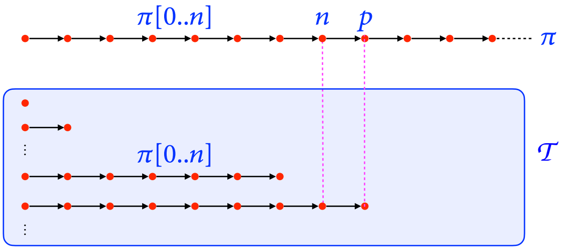
$$\lim \mathcal{T} \quad \triangleq \quad \{\pi \in \mathbb{T}^\infty \mid \forall n \in \mathbb{N} \,.\, \exists p \geqslant n \,.\, \pi[0..p] \in \mathcal{T}\} \;.$$

© P. Cousot, NYU, CIMS, CS

Limit of prefix traces (II)

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

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



 © P. Cousot, NYU, CIMS, CS

Example II of limit of prefix traces

- $\lim\left\{\left(\ell_1 \xrightarrow{\texttt{tt}} \ell_2 \xrightarrow{\texttt{x} = i} \ell_1\right)_{i=1}^{n} \;\middle|\; n \in \mathbb{N}\right\} = \{\pi\}$ where $\pi = \pi = \left(\ell_1 \xrightarrow{\texttt{tt}} \ell_2 \xrightarrow{\texttt{x} = i}\right)_{i=1}^{\infty}$.
- All prefixes of π are of the form $\left(\ell_1 \xrightarrow{\texttt{tt}} \ell_2 \xrightarrow{\texttt{x} = i} \ell_1\right)_{i=1}^{n}$ or $\left(\ell_1 \xrightarrow{\texttt{tt}} \ell_2 \xrightarrow{\texttt{x} = i} \ell_1\right)_{i=1}^{n} \xrightarrow{\texttt{tt}} \ell_2$ and this last one can be extended to a finite trace $\left(\ell_1 \xrightarrow{\texttt{tt}} \ell_2 \xrightarrow{\texttt{x} = i} \ell_1\right)_{i=1}^{n+1}$.

 © P. Cousot, NYU, CIMS, CS

Infinite maximal trace semantics

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

Maximal finite and infinite trace semantics

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

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

or infinite defined as limits of finite prefix traces.

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

 © P. Cousot, NYU, CIMS, CS

Example II of limit of prefix traces

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

© P. Cousot, NYU, CIMS, CS

Conclusion

© P. Cousot, NYU, CIMS, CS

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

Home work

- Read Ch. **7** "Maximal trace semantics" of

Principles of Abstract Interpretation
Patrick Cousot
MIT Press

The End, Thank you

© P. Cousot, NYU, CIMS, CS