

# Modern termination certificates

- A modern certificate = a **derivation tree**
- Sound Inferences
  - generic **deep** theorem (Coccinelle)
  - particular (Coq) **shallow** lemma (CiME)
- Leaves
  - empty relation
  - WF proof
    - **generic deep** ex: RPO (Coccinelle)
    - **particular shallow** ex: polynomial interpretation function (CiME).

# Termination Proof Sketch

$$\begin{array}{rcl} R : & f(f(x)) & \rightarrow h(f(x)) \\ & g(x) & \rightarrow f(x) \end{array} \quad \{ ffx \rightarrow hfx; gx \rightarrow fx \} \ SN$$

# Termination Proof Sketch

$$\begin{array}{rcl} R : & f(f(x)) & \rightarrow h(\textcolor{red}{f}(x)) \\ & g(x) & \rightarrow \textcolor{red}{f}(x) \end{array}$$

$$DP : \begin{array}{l} \langle g^\# x, f^\# x \rangle \\ \langle f^\# fx, f^\# x \rangle \end{array} \qquad \{ ffx \rightarrow hfx; \ gx \rightarrow fx \} \ SN$$

# Termination Proof Sketch

$$R : \begin{array}{rcl} f(f(x)) & \rightarrow & h(\textcolor{red}{f}(x)) \\ g(x) & \rightarrow & \textcolor{red}{f}(x) \end{array} \quad \text{DP } \frac{}{\{ffx \rightarrow hfx; gx \rightarrow fx\} \text{ SN}}$$
$$DP : \begin{array}{l} \langle g^\# x, f^\# x \rangle \\ \cancel{\langle f^\# fx, f^\# x \rangle} \end{array}$$

# Termination Proof Sketch

$$R : \begin{array}{rcl} f(f(x)) & \rightarrow & h(\textcolor{red}{f}(x)) \\ g(x) & \rightarrow & \textcolor{red}{f}(x) \end{array} \quad \text{DP } \frac{\{ \langle g^\# x, f^\# x \rangle \} \text{ SN}}{\{ ffx \rightarrow hfx; gx \rightarrow fx \} \text{ SN}}$$
$$DP : \langle g^\# x, f^\# x \rangle$$

# Termination Proof Sketch

$$\begin{array}{ll} R : & f(f(x)) \rightarrow h(\textcolor{red}{f}(x)) \\ & g(x) \rightarrow \textcolor{red}{f}(x) \\ DP : & \langle g^\# x, f^\# x \rangle \end{array} \quad \text{DP} \frac{\textcolor{red}{DPR\ SN}}{\{ffx \rightarrow hfx; gx \rightarrow fx\} SN}$$

Lemma wfR\_wfDPR: well\_founded DPR  $\rightarrow$  well\_founded R.

$\Rightarrow$  next step: prove **well\_founded DPR**

# Termination Proof Sketch

$$R : \begin{array}{rcl} f(f(x)) & \rightarrow & h(\textcolor{red}{f}(x)) \\ g(x) & \rightarrow & \textcolor{red}{f}(x) \end{array} \quad \text{GRAPH } \frac{\{\} \text{ SN}}{DPR \text{ SN}}$$
$$DP : \langle g^\# x, f^\# x \rangle \quad \text{DP } \frac{\{ffx \rightarrow hfx; gx \rightarrow fx\} \text{ SN}}{\{ffx \rightarrow hfx; gx \rightarrow fx\} \text{ SN}}$$

No cycle!

Lemma wfDPR : well\_founded DPR

# Modelling in Proof Assistant

Classical approaches:

## Deep embedding

- generic
- full theory encoding  $\rightsquigarrow$  instantiation difficult (premises)

## Shallow embedding

- no encoding of theory  $\rightsquigarrow$  possibly easier
- problem specific  $\rightsquigarrow$  one proof for each problem

Our approach: mixing embeddings

# Criteria as inference rules

| Deep                | Shallow  |
|---------------------|--|
| TRS $\mathcal{R}$   | $\rightsquigarrow$ relation $\rightarrow_R$                          |
| DP( $\mathcal{R}$ ) | $\rightsquigarrow$ relation $\rightarrow_{\text{DPR}(\text{DP}(R))}$ |

Ex: Dependency pair criterion:

$$\frac{\text{SN}(\rightarrow_{\text{DPR}(\text{DP}(R))})}{\text{SN}(\rightarrow_R)} \text{ DP}$$

# inference rules

Ex: proof by DP + ordering pair (axiom)

$$\frac{\begin{array}{c} WF(>, \geq) \quad \rightarrow_{DPR(DP(R))} \subset > \quad \rightarrow_R \subset \geq \\ \hline SN(\rightarrow_{DPR(DP(R))}) \end{array}}{SN(\rightarrow_R)} \text{ DP} \quad \text{ORD}$$

# Cime 3 (Cime 2.99)

Toplevel or Batchmode (from XML, to XML, to Coq...)

Certifies:

- (marked)DP (subterm enhanced)
- “Full” graph criteria (strong and weak)
- Polynomials
- RPO (partial prec.) + AFS

# XML Proof tree

```
<proof>
  <property prop="sntrs" criterion="dp">
    ...
    <property prop="sndp" criterion="ordering">
      ...
    </property>
  </property>
</proof>
```

# XML Proof tree

```
<property prop="snmp" criterion="component">
    <system>...</system>
    <criterion>...</criterion>
    <property ...> ... </property>
    <property ...> ... </property>
    ...
</property>
```

# Xml Proof tree

```
<system>
  <rewsys>
    <rule num="0"> ... </rule>
    ...
  </rewsys>
  <dplist>
    <dprule num="0"> ... </dprule>
    ...
  </dplist>
</system>
```

# Xml Proof tree

criterion = information mandatory for criterion certification

Ex: for the ORD rule:

```
<criterion>
  <ordering>
    ...
  </ordering>
</criterion>
```

# Graph criterion

## General rule:

$$\frac{\forall p \in \mathcal{SCP}(\mathcal{G}), \text{SN}(p)}{\text{SN}(\rightarrow_{\text{DPR}(\text{DP}(R))})} \text{ GRAPH}$$

- $\mathcal{G}$  is the (approximated) dependency graph of  $R$ ,
  - and  $SCP(\mathcal{G})$  is the set of strongly connected parts ( $\simeq$  circuits).
  - $SN(p)$  = there is no dependency chain crossing all nodes of  $p$  infinitely many times.

All graph criterion variants = instances of general rule  
= different ways to gather  $p$ 's

Powerful instance:

$$\frac{\text{SN}(\mathcal{G} \setminus \langle t, u \rangle) \quad \text{SNG} \left\{ \begin{array}{l} \mathcal{W}\mathcal{F}(>, \geq) \xrightarrow{\rightarrow_{\text{DPR}(\mathcal{G})}} \geq \\ \rightarrow_R \subset \geq \quad \color{red}{t > u} \end{array} \right\}}{\text{SN}(\mathcal{G})}$$

ORDPAIR  
GRAPH

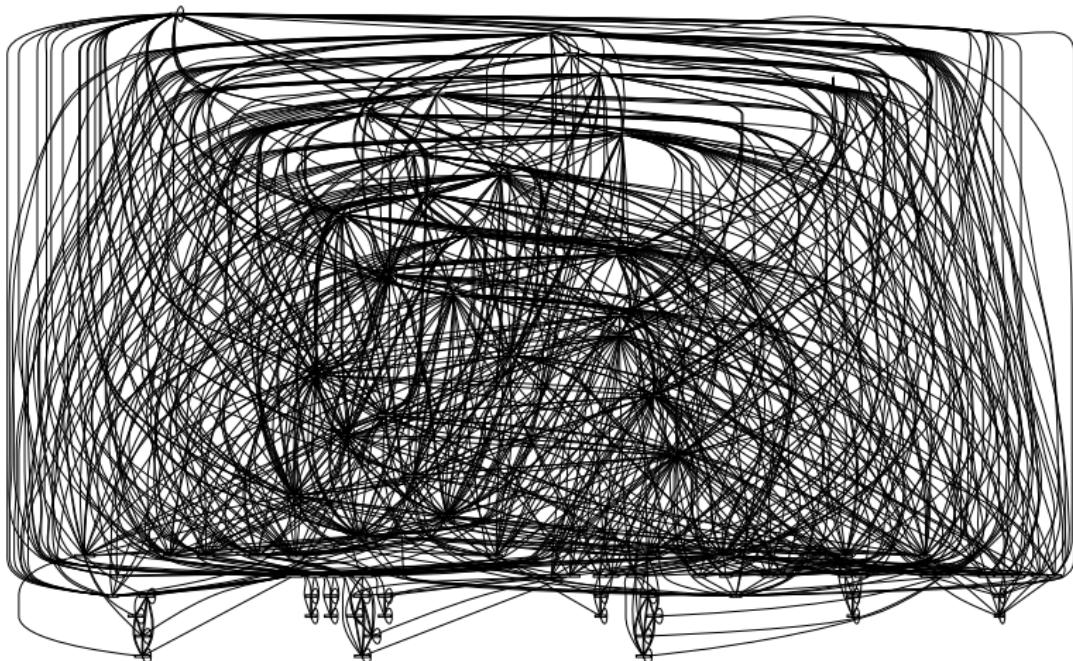
- $\mathcal{G}$  is a strongly connected component,
  - Each connected component of  $\text{SN}(\mathcal{G} \setminus \langle t, u \rangle)$  proved recursively with other orders.
- ~ Need to specify dags of strongly connected components of graphs.

# An Example

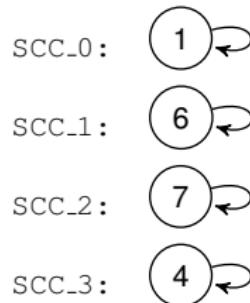
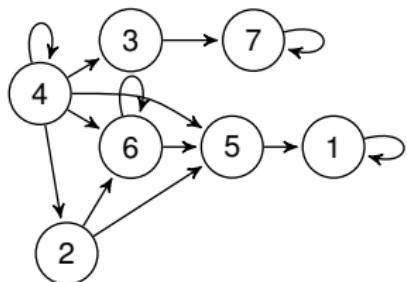
ExSec11\_1\_Luc02a\_iGM

47 rules, 85 vertices, 1015 arcs

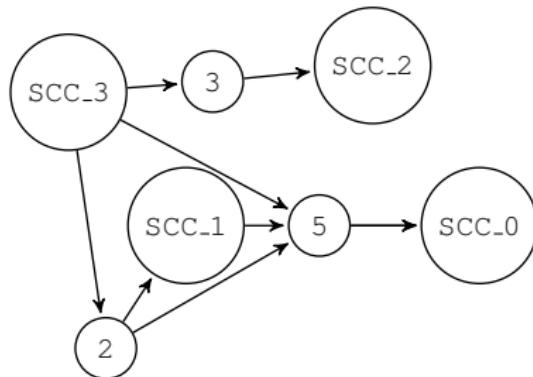
Compile time: 113s



# graph example



Information to store:



# Graph criterion in Xml

```
<criterion>
  <dag>
    <scc num="0"> ... </scc>
    ...
    <nonscc num="7"> ... </scc>
    ...
    <edges start="0" end="2">
      ...
  </dag>
</criterion>
```

# Graph criterion in Xml

```
<property prop="sndp" criterion="component">
    <system>...</system>
    <criterion><dag>...</dag></criterion>

    <-- SCC_0 -->
    <property prop="sndp" criterion="intracomponent">
        ...
    </property>

    <-- SCC_1 -->
    ...
</property>
```

# Resources

A3PAT project (CNAM & ENSIIE/Orsay/LaBRI/INRIA-Sophia)

Regarding termination:

All TRS proven to be SN by CiME (no usable rules, no eqth)

Give it a try

- CiME 3 soon
- CiME 2.99, Coccinelle library available from the A3PAT website:  
<http://a3pat.ensiie.fr>
- Try it online!