Towards An Assume-Guarantee Theory for Adaptable Systems

Paola Inverardi, Patrizio Pelliccione, Massimo Tivoli

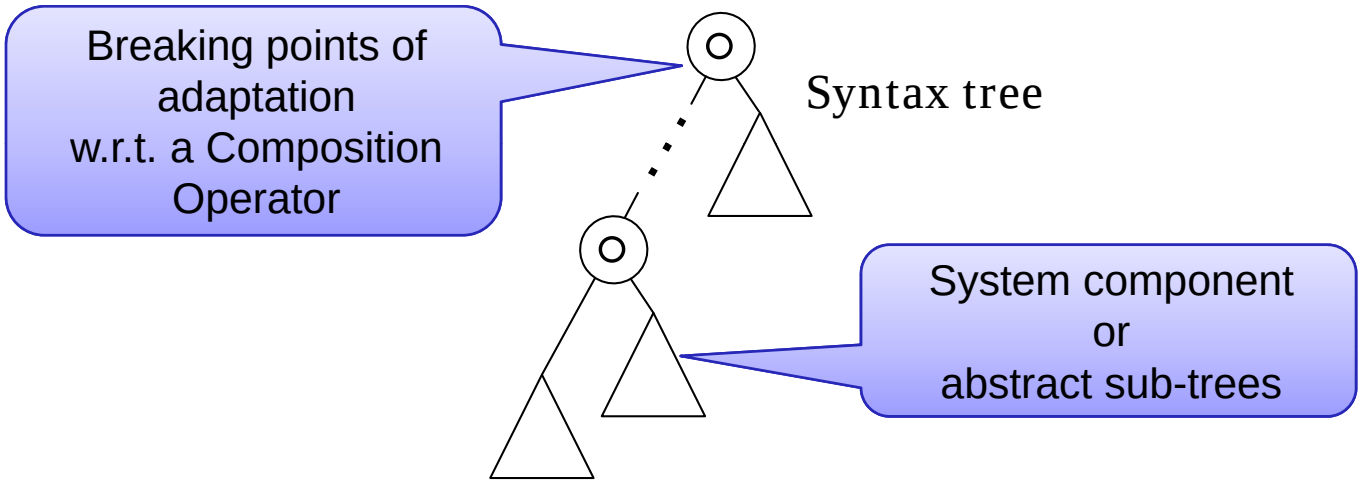
Dipartimento di Informatica
Università degli Studi dell'Aquila
Italy
{paola.inverardi,patrizio.pelliccione,massimo.tivoli}@di.univaq.it

Adaptation & Dependability

- Increasingly, software systems must adapt in response to
  - changing user needs
  - system intrusions or faults
  - changing operational environment
  - resource variability
- …but still preserving a certain degree of dependability characterized as ***Invariants***
  - invariants represent the system properties that should be maintained w.r.t. the adaptation to be performed
  - Instead, non-critical properties might be relaxed, hence increasing the degree of flexibility of the system during or after adaptation

Framework Idea

- Break up a system in parts that can be substituted or changed without hurting the invariant property



- Every node labeled with an assumption to be satisfied by the component in order to maintain the invariant
- These assumptions can be automatically generated by following a compositional approach
- The framework works at different levels of abstraction spanning from code to software architecture

Main motivations

- Ease the task of effectively breaking the system into parts
- Ease the task of correctly (with respect to the invariant) composing a system out of elementary components
- Support adaptability at different levels of system granularity
- Efficiently drive the compositional assumption generation
- Support reactions to unsuccessful (with respect to the invariant) adaptations

Assume-Guarantee Reasoning (AGR)

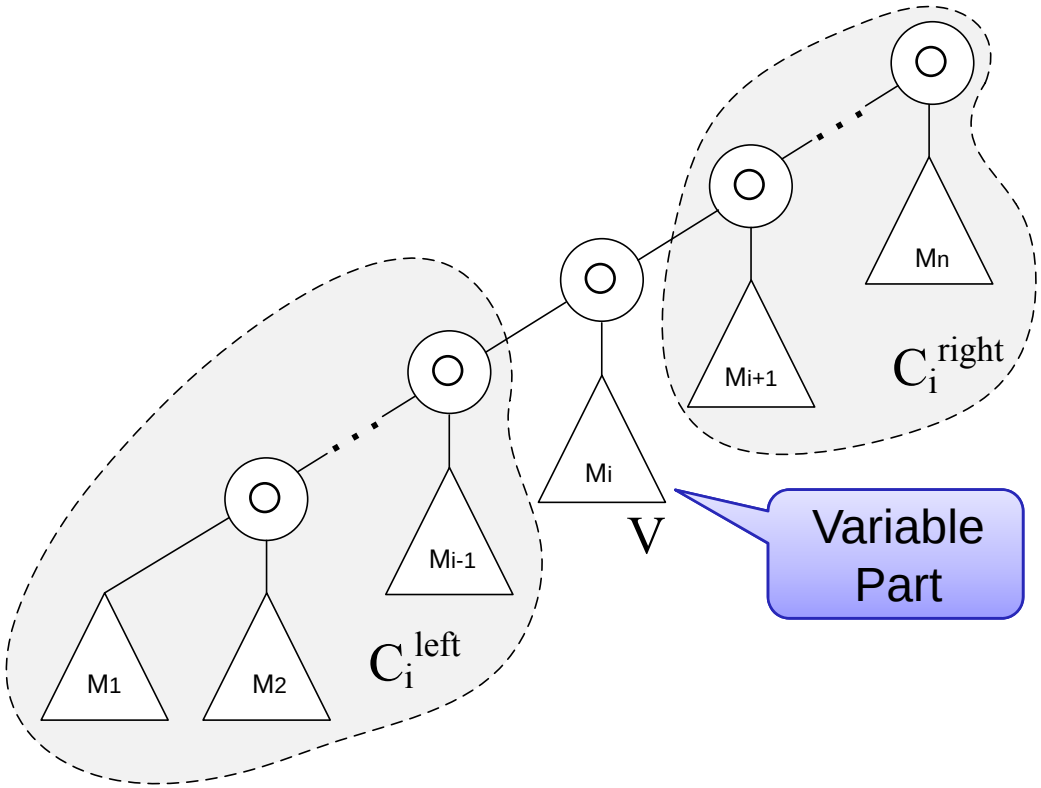
- By considering a system composed of several components, AGR aims at verifying the system through the separate verification of the single components

Assumption $< \varphi > M < \psi >$ Guarantee

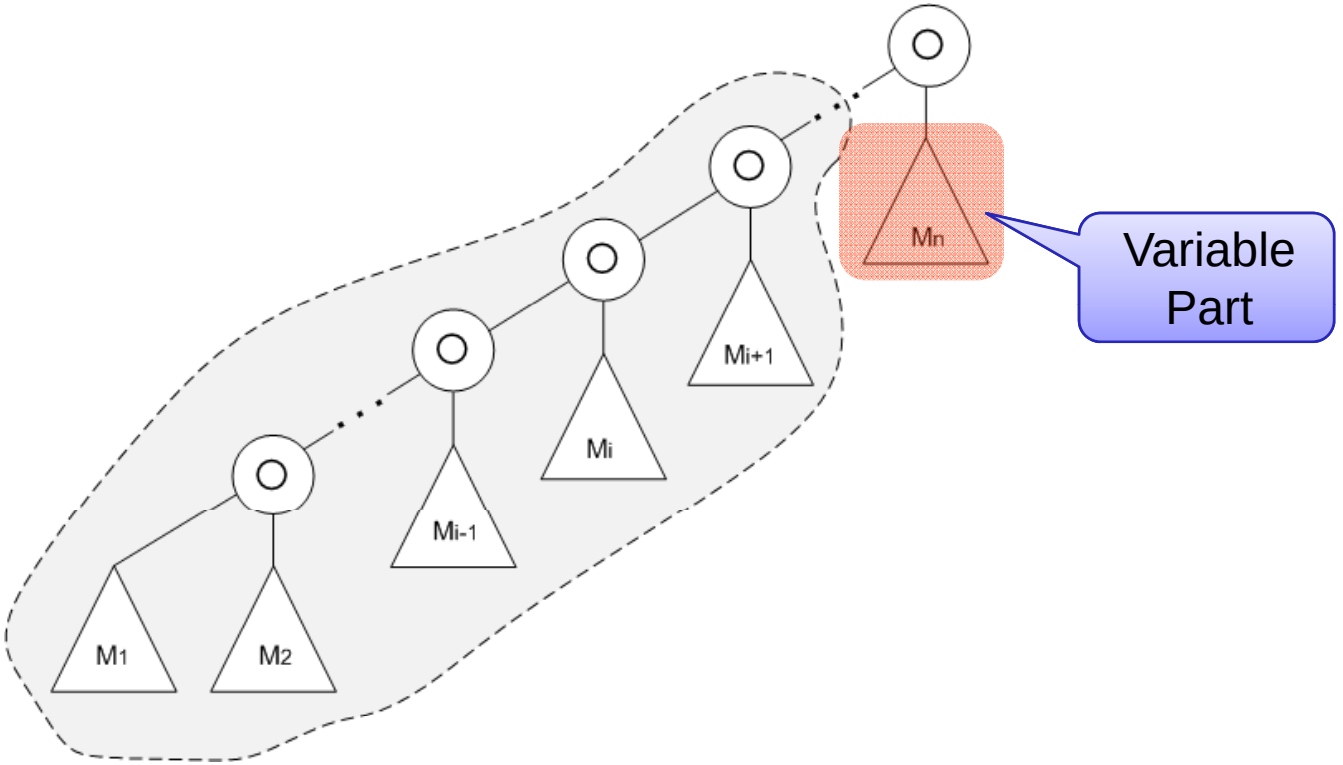
- Reasoning chain:

$$\frac{<> M' < \varphi > \quad < \varphi > M < \psi >}{<> M \cdot M' < \psi >}$$

Decorate the system with assumptions and guarantees

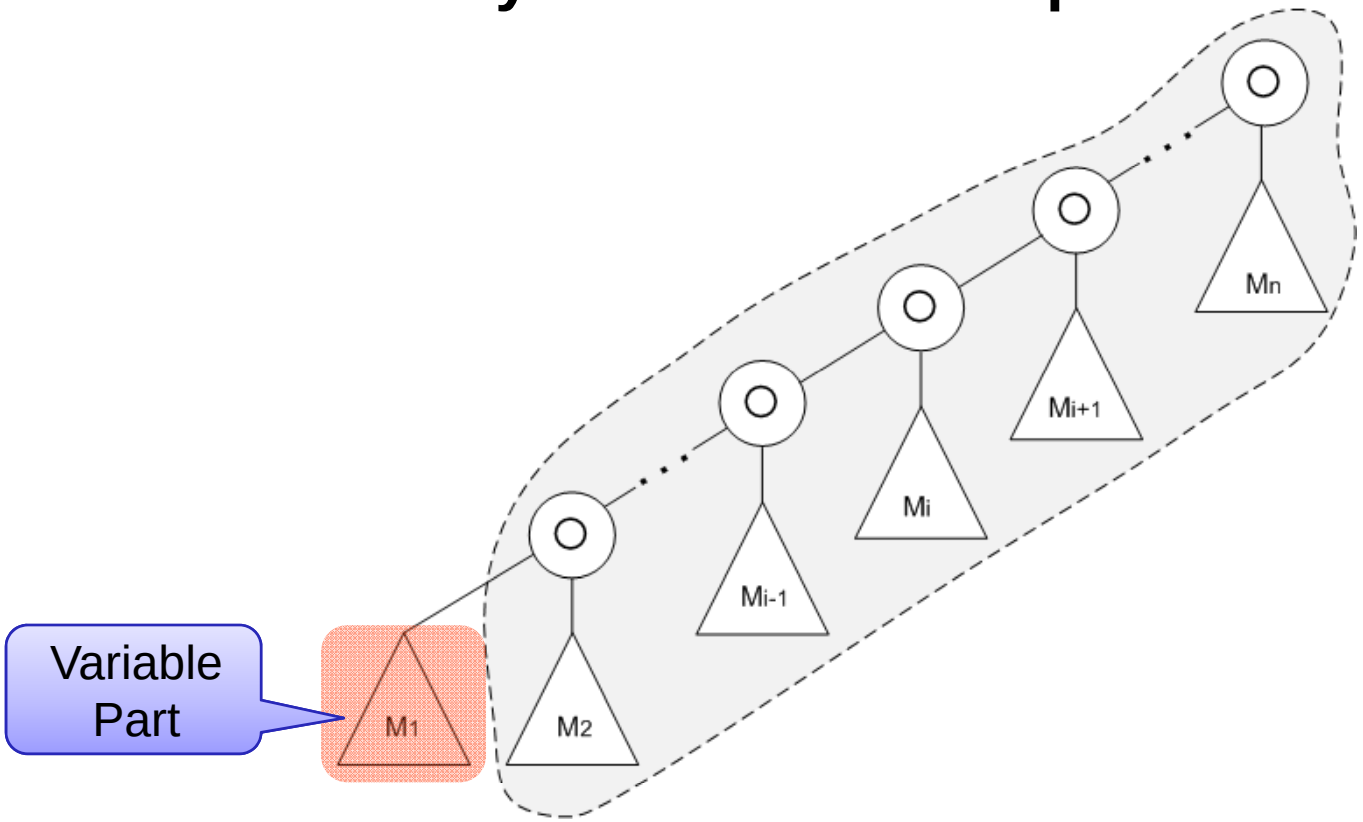


Decorate the system with assumptions and guarantees



$$\frac{\langle \phi_E \rangle \; \mathrm{C}_\mathrm{n}^{\mathrm{left}} \; \langle \mathrm{A_n} \rangle \quad \langle \mathrm{A_n} \rangle \; \mathrm{M_n} \; \langle \mathrm{I} \rangle}{\langle \phi_E \rangle \; \mathrm{C}_\mathrm{n}^{\mathrm{left}} \circ \mathrm{M_n} \; \langle \mathrm{I} \rangle}$$

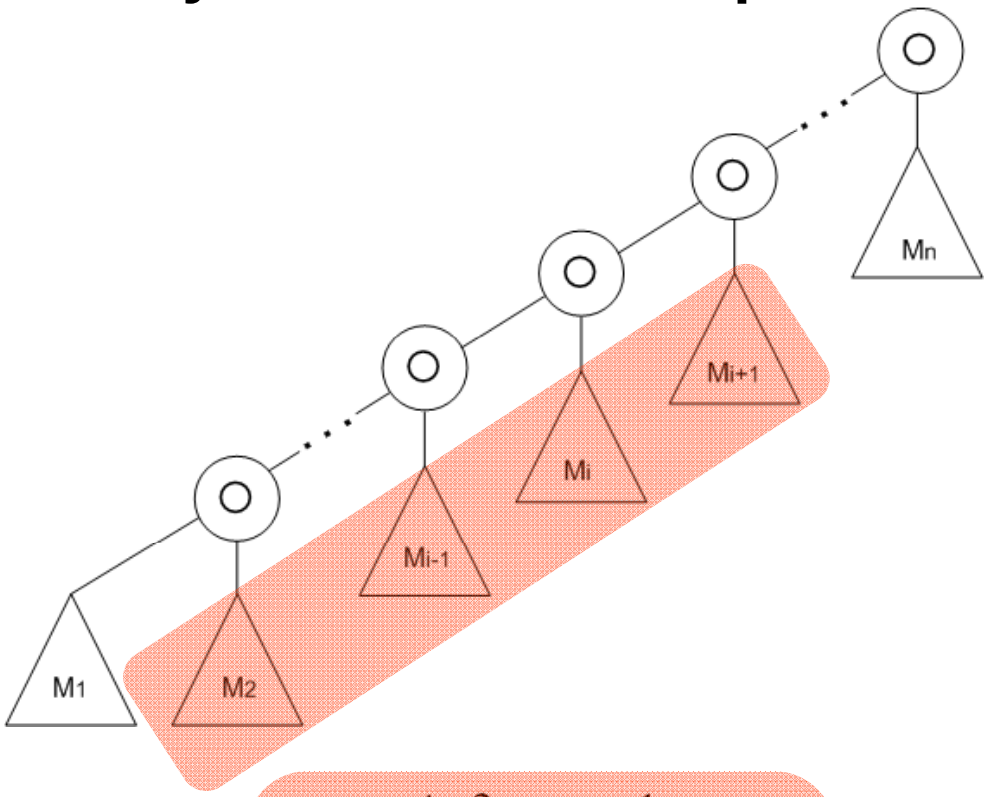
Decorate the system with assumptions and guarantees



$$\frac{\langle \phi_E \rangle \; \mathrm{M}_1 \; \langle \mathrm{G}_1 \rangle \qquad \langle \mathrm{G}_1 \rangle \; \mathrm{C}_1^{\mathrm{right}} \; \langle \mathrm{I} \rangle}{\langle \phi_E \rangle \; \mathrm{M}_1 \circ \mathrm{C}_1^{\mathrm{right}} \; \langle \mathrm{I} \rangle}$$

$$\frac{\langle \phi_E \rangle \; \mathrm{C}_{\mathrm{n}}^{\mathrm{left}} \; \langle \mathrm{A}_{\mathrm{n}} \rangle \qquad \langle \mathrm{A}_{\mathrm{n}} \rangle \; \mathrm{M}_{\mathrm{n}} \; \langle \mathrm{I} \rangle}{\langle \phi_E \rangle \; \mathrm{C}_{\mathrm{n}}^{\mathrm{left}} \circ \mathrm{M}_{\mathrm{n}} \; \langle \mathrm{I} \rangle}$$

Decorate the system with assumptions and guarantees



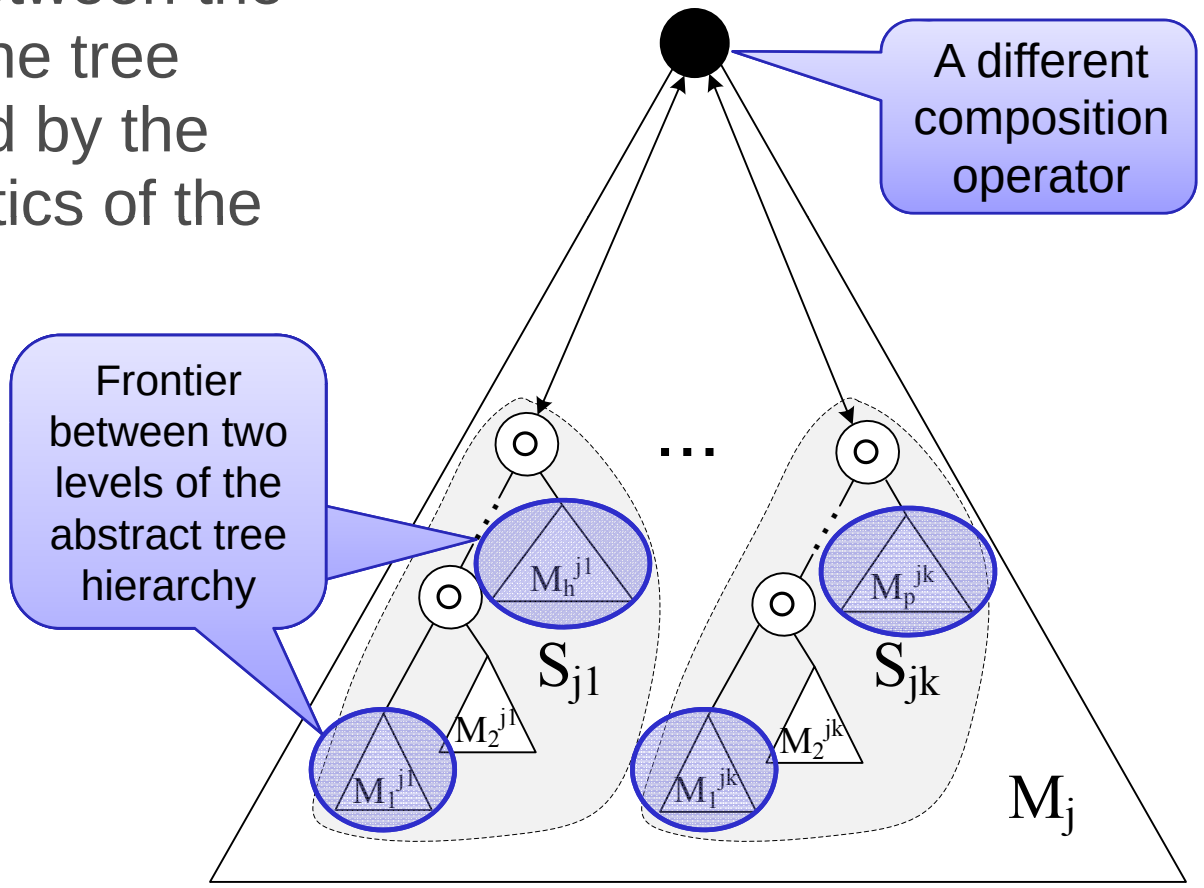
$$\frac{\langle \phi_E \rangle\ \mathrm{M}_1\ \langle \mathrm{G}_1 \rangle \qquad \langle \mathrm{G}_1 \rangle\ \mathrm{C}_1^{\mathrm{right}}\ \langle \mathrm{I} \rangle}{\langle \phi_E \rangle\ \mathrm{M}_1 \circ \mathrm{C}_1^{\mathrm{right}}\ \langle \mathrm{I} \rangle}$$

$$\frac{i{=}2,\cdots,n{-}1 \qquad \langle \phi_E \rangle\ \mathrm{C}_\mathrm{i}^{\mathrm{left}}\ \langle \mathrm{A}_\mathrm{i} \rangle \qquad \langle \mathrm{A}_\mathrm{i} \rangle\ \mathrm{M}_\mathrm{i}\ \langle \mathrm{G}_\mathrm{i} \rangle \qquad \langle \mathrm{G}_\mathrm{i} \rangle\ \mathrm{C}_\mathrm{i}^{\mathrm{right}}\ \langle \mathrm{I} \rangle}{\langle \phi_E \rangle\ \mathrm{C}_\mathrm{i}^{\mathrm{left}} \circ \mathrm{M}_\mathrm{i} \circ \mathrm{C}_\mathrm{i}^{\mathrm{right}}\ \langle \mathrm{I} \rangle}$$

$$\frac{\langle \phi_E \rangle\ \mathrm{C}_\mathrm{n}^{\mathrm{left}}\ \langle \mathrm{A}_\mathrm{n} \rangle \qquad \langle \mathrm{A}_\mathrm{n} \rangle\ \mathrm{M}_\mathrm{n}\ \langle \mathrm{I} \rangle}{\langle \phi_E \rangle\ \mathrm{C}_\mathrm{n}^{\mathrm{left}} \circ \mathrm{M}_\mathrm{n}\ \langle \mathrm{I} \rangle}$$

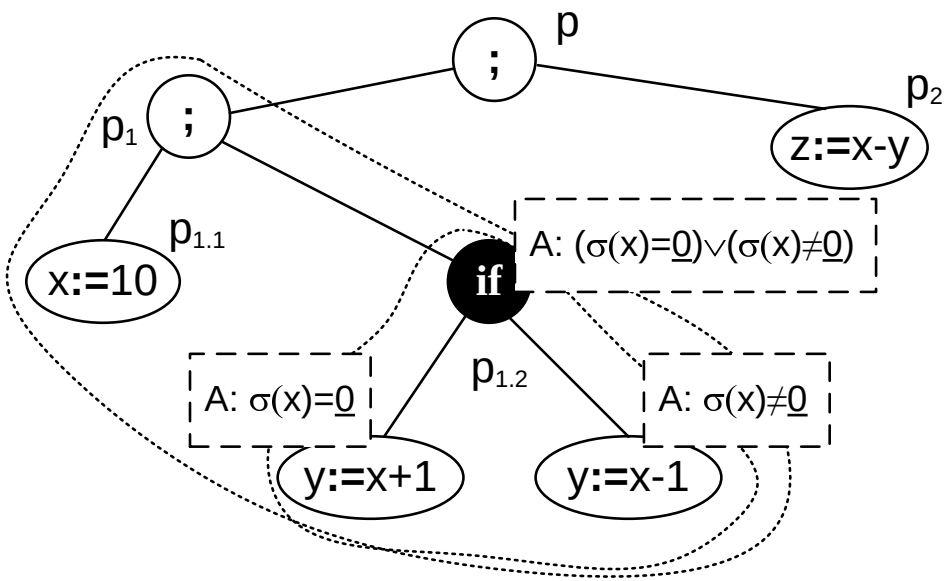
Sub-tree hierarchy of M_j

- The relationship between the different levels of the tree hierarchy is defined by the operational semantics of the operator ●



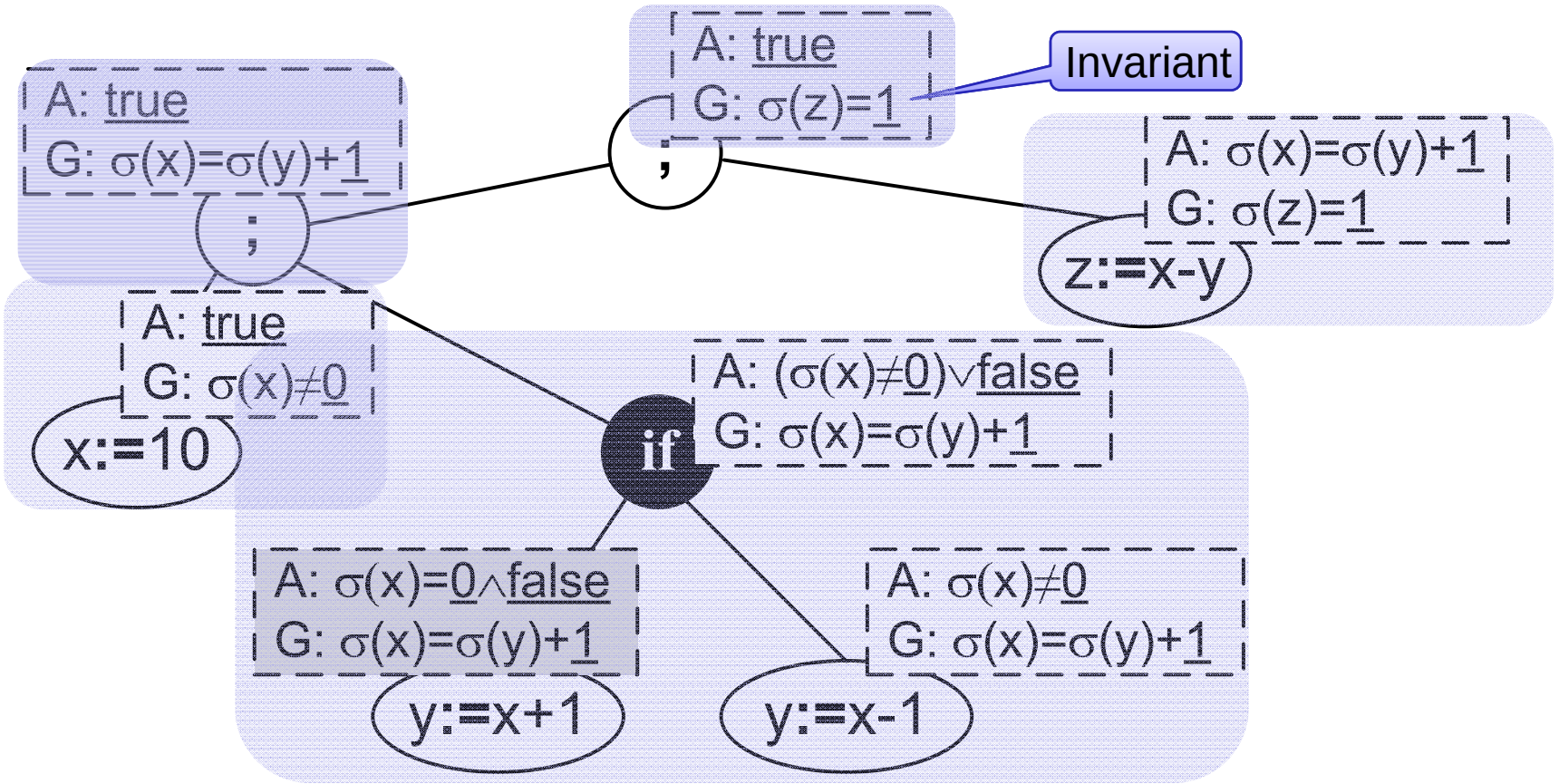
A simple programming language p

```
x:=10;
if x==0 then y:=x+1 else y:=x-1 fi;
z:=x-y
```



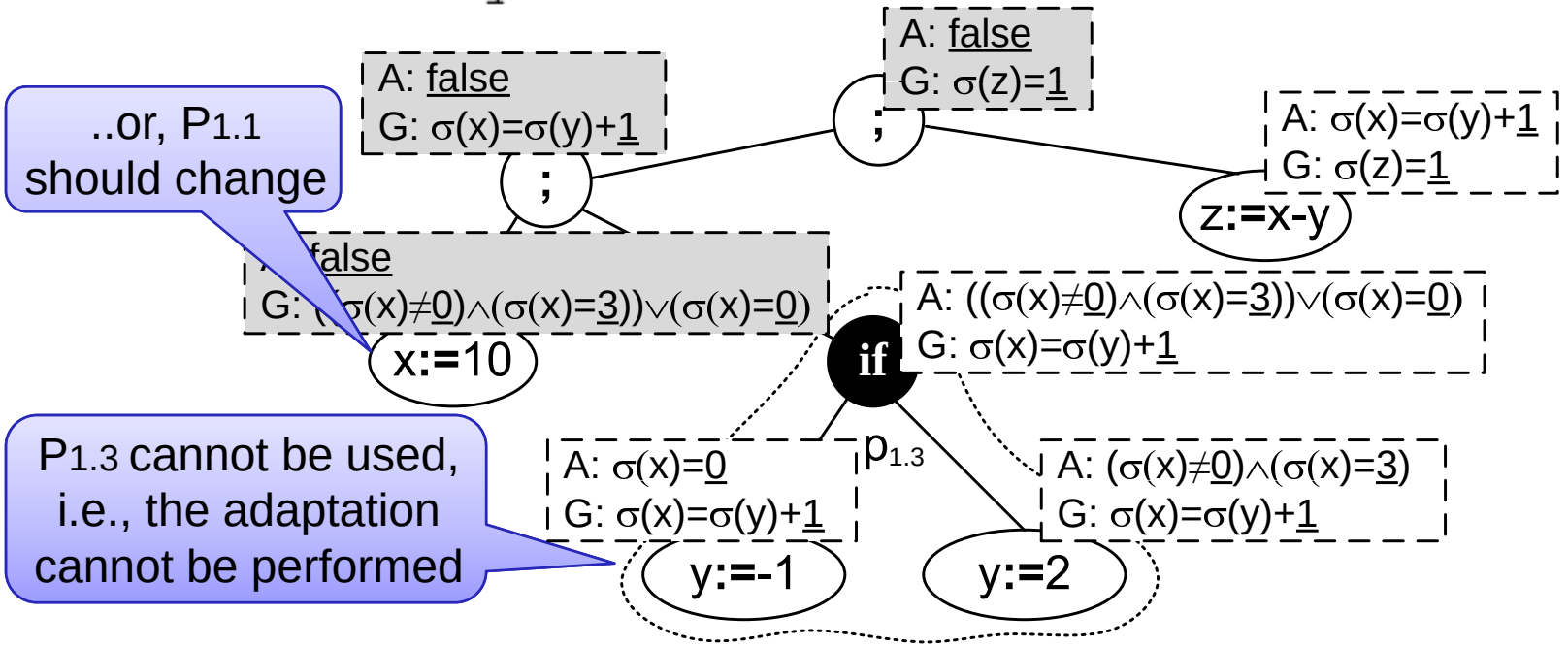
Decomposition of p

Assume-guarantee annotations of p



Adaptation

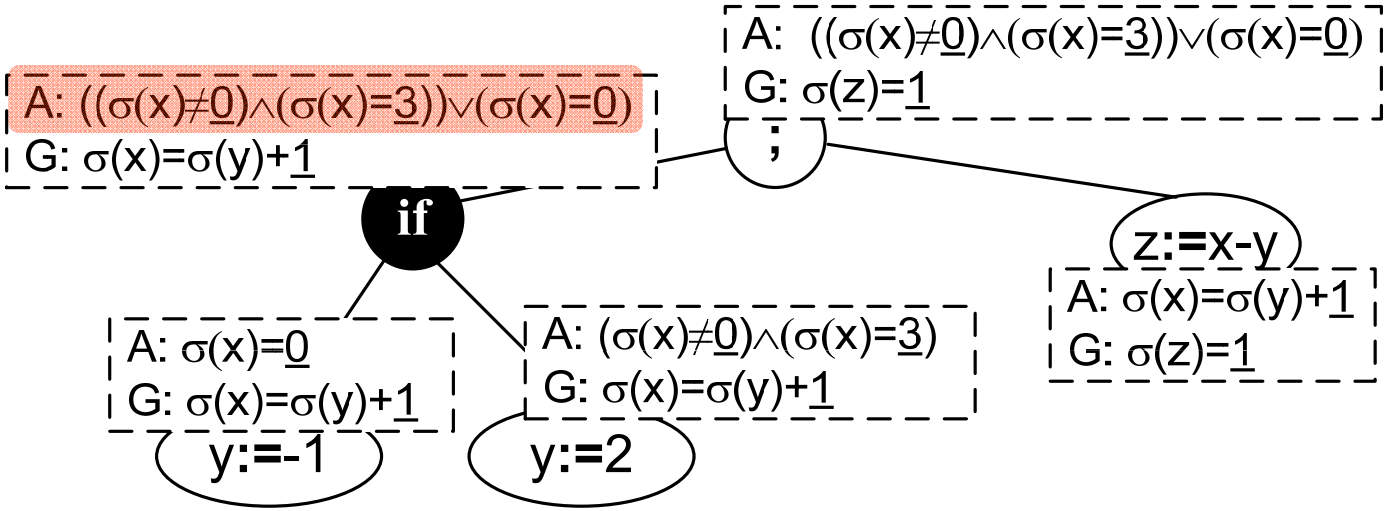
```
x:=10;
if x==0 then y:=-1 else y:=2 fi;
z:=x-y
```



Assume-guarantee re-computation after adaptation

What are the possible P1.1s that guarantee the invariant?

```
if x==0 then y:=-1 else y:=2 fi;
z:=x-y
```



Main dimensions to be considered when dealing with AGR

- Composition operator: the composition operator should be carefully selected and must be associative
- Assumptions generation: a suitable assumption generation technique should be defined
- System and property decomposition: the property definition should be decomposable w.r.t. the AGR
  - What's about deadlock?
- Languages selection: to support automated assumption generation a semantic relationship between the language used to write the system and the language used to specify the properties must exist

Future work

- Fully formalize the framework in order to give a proof of its soundness and provide a basis for its automation
- Experiment it on case studies that belong to different application domains and that specify adaptation at different levels of system granularity
- Last but not least….rebuild L'Aquila:

Please sign the petition at http://ideasforlaquila.org

Towards An Assume-Guarantee Theory for Adaptable Systems

Paola Inverardi, Patrizio Pelliccione, Massimo Tivoli

Thank you for the attention!

Questions?