Frama-C Day 2016

Temporal logic and C programs

How to model-check with uncertainty ?

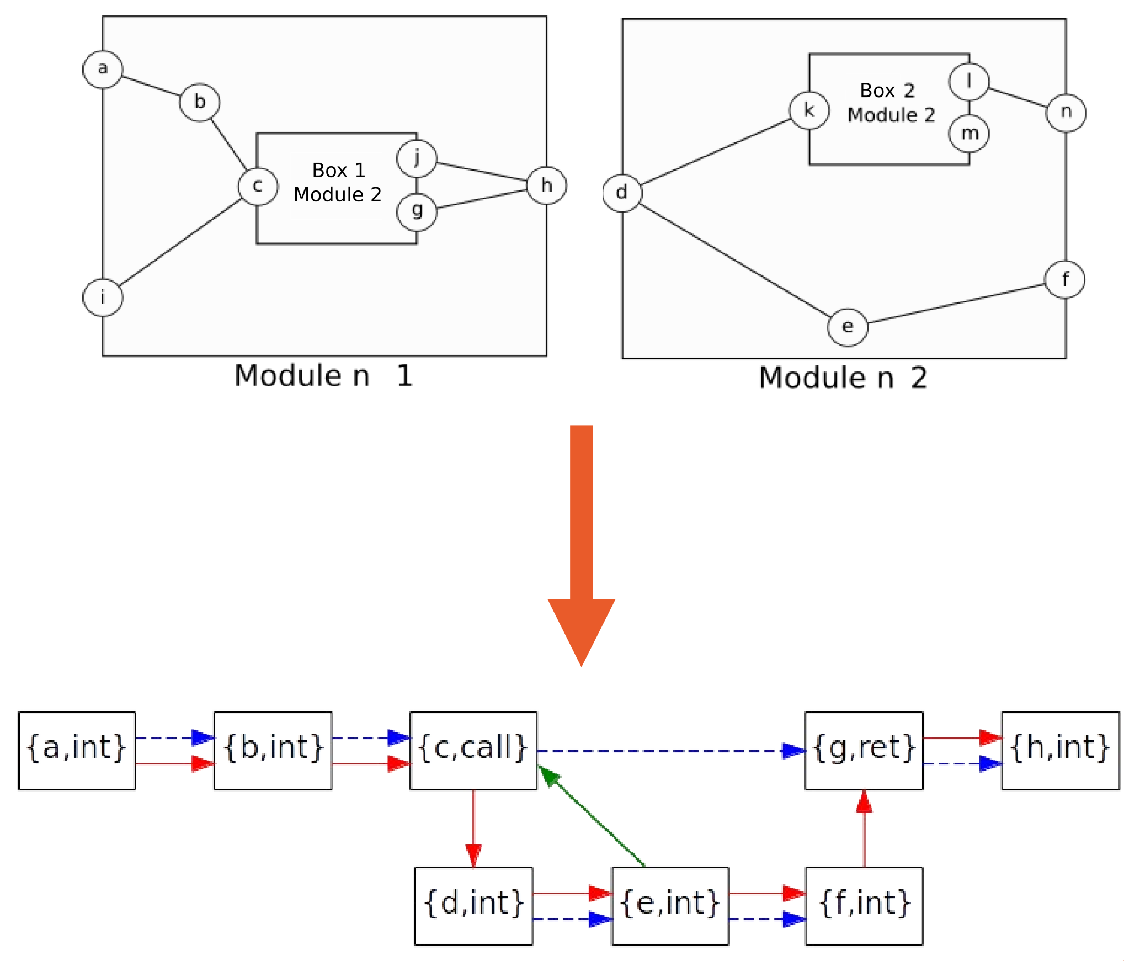
Context: Talking about time ?

CaRet temporal logic [Alur04]

- **3** discrete time measures in a **single** formula

- Expresses **safety**, **liveness**, **past** and **call context** properties

- Decidability procedure over **recursive state machines**



More expressive than PLTL and recursive state machines are well suited for C control flow graph representation

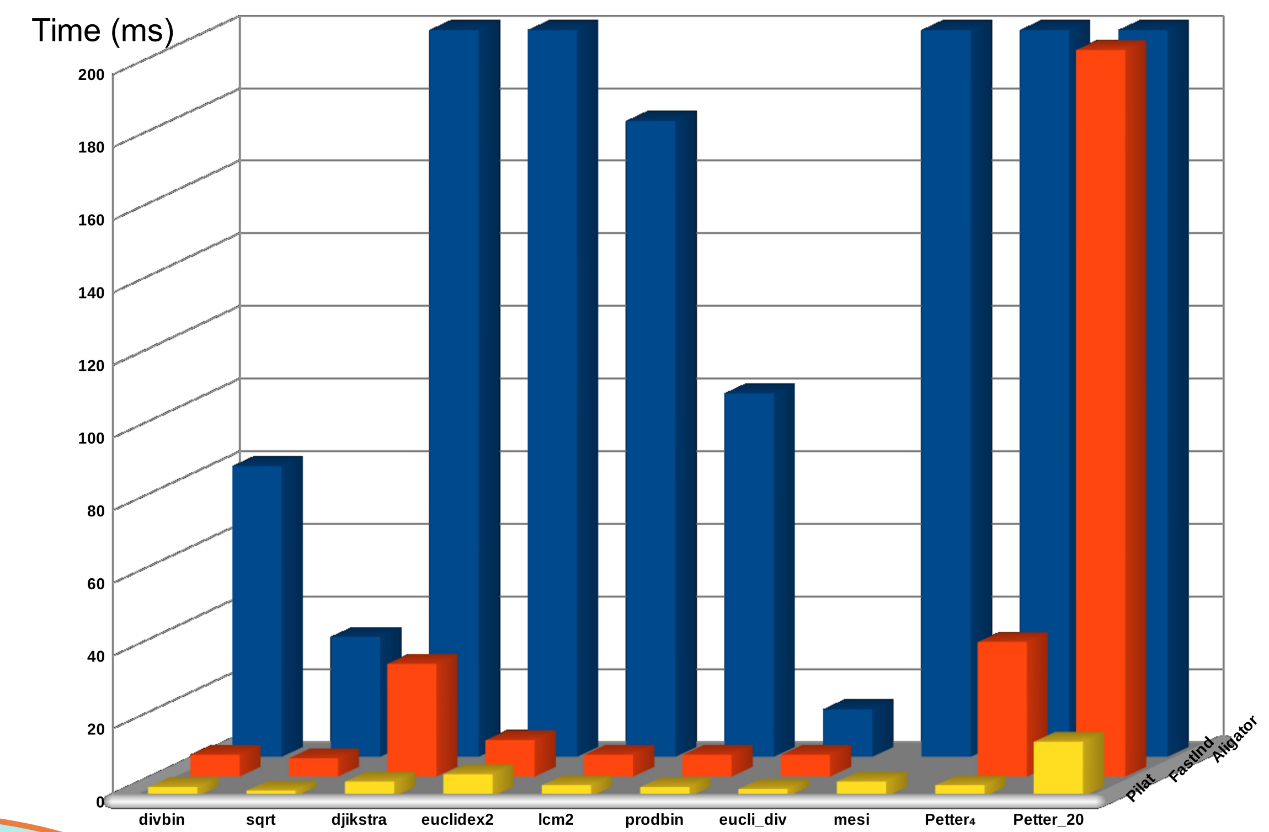
Issue: Avoiding undecidability ?

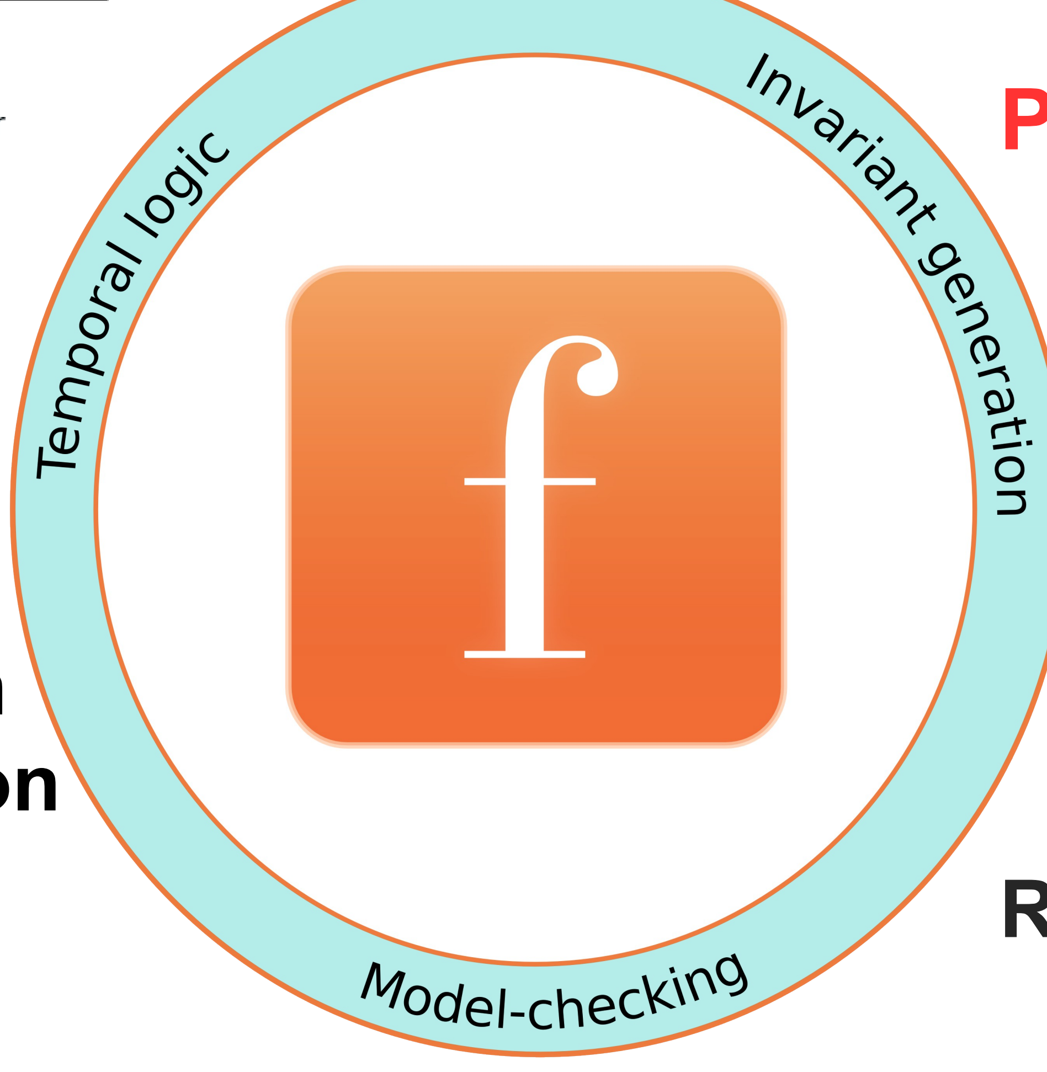
Polynomial invariants by linear algebra

- Reduction of **solvable** polynomials to **Presburger** arithmetic

- Eigenvectors of a linear application dual are **invariants**

- Decidability of **all** polynomial relations with a **polynomial complexity**





Pilat, a new tool for C invariant generation

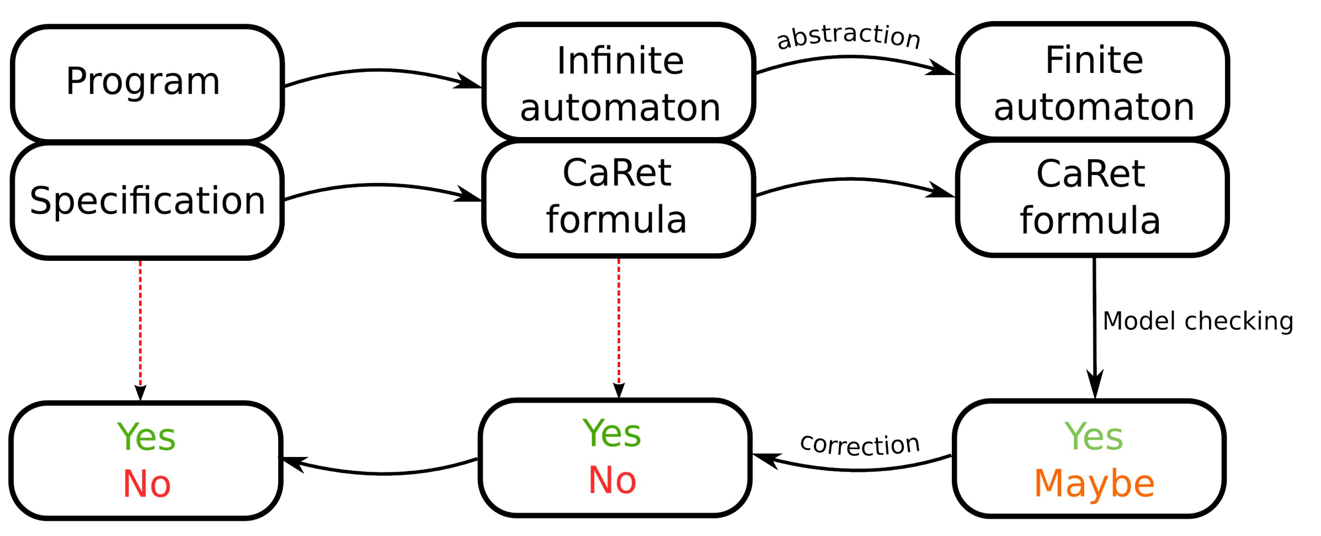
At least 5 times faster than Aligator and from 2 to 2700 times faster than FastInd

Release : June 2016

CaFE, a new model checker for C

- Based on a CaRet-like **three-valued** temporal logic

- Dealing with **uncertainty** by correction



Release : planned for 2017

Objectives :

- **Scalability** of the method for large examples

- Merging **CaFE** with **Pilat** and **Abstract domains analysis**

Steven de Oliveira | steven.deoliveira@cea.fr

Supervisors | Saddek Bensalem
| Virgile Prevosto