CRISTAL

(2009-2012)
Contrôle des Ressources par Interprétations Sémantiques
et Théorie de la démonstrAtion Linéaire

Romain Péchoux

EPI Carte, Inria Nancy Grand-Est, Loria, and Université de Lorraine
romain.pechoux@loria.fr

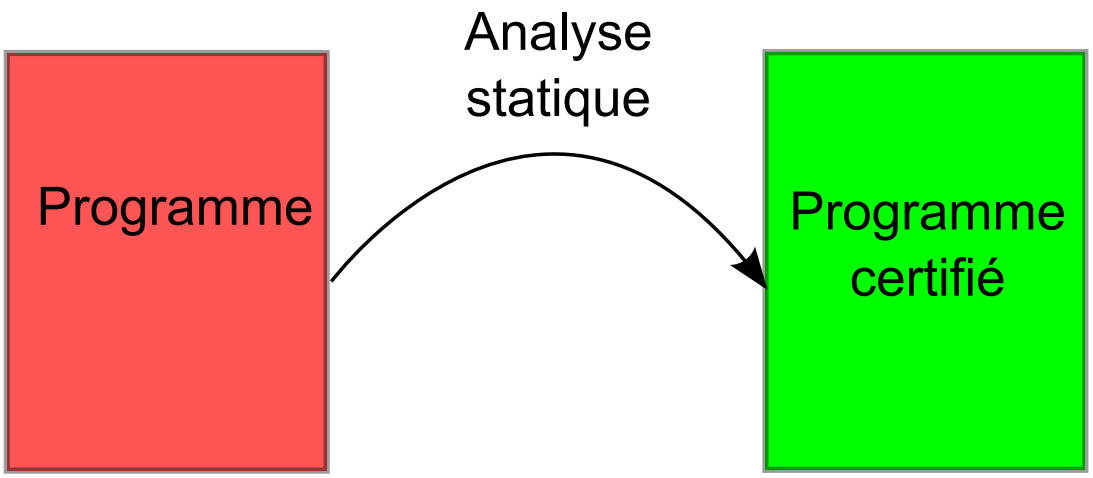
November 15, 2012

Motivations

Cristal belongs to Implicit Computational Complexity (ICC) that aims at:

- Providing machine independent characterizations of complexity classes
- Studying resource consumption on several programming paradigms:
  - Functional
  - Imperative and object-oriented
  - Concurrent (multi-threaded) calculi
  - ...

Applications



- space upper bounds (heap, stack, ...)
- time upper bounds (instructions, recursive calls, ...)

ICC Tools

- ICC uses distinct static analysis tools and methodologies:
  - Linear logic (Soft and Light logics)
  - Interpretations (abstract, quasi-and sup-interpretations)
  - Termination techniques for TRS
  - Type systems
  - Second order logic and function algebra
- Practical motivations:
  - Distributed systems have increased the need for program correctness and certification.
  - Certifying runtime properties is of central importance for small and mobile devices with bounded computational resources that receive programs to be executed.

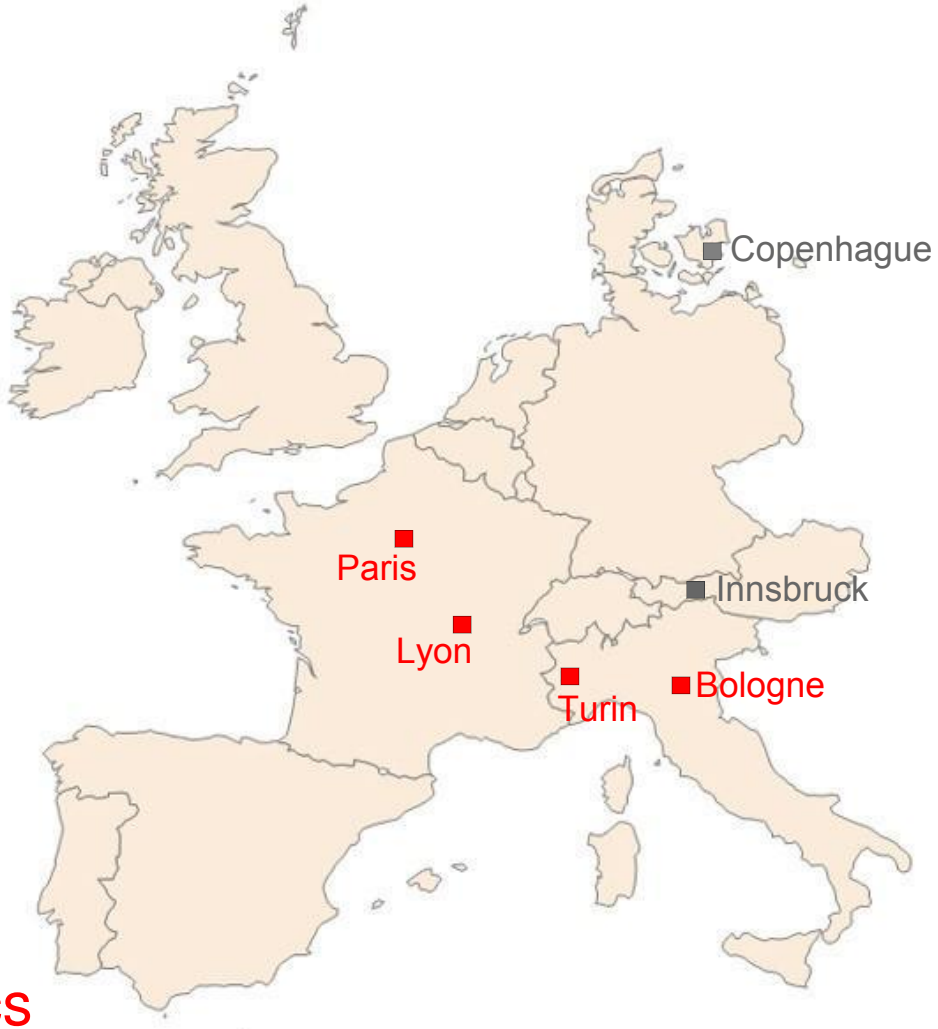
ICC European map

-
-
-
-
-

ICC European map

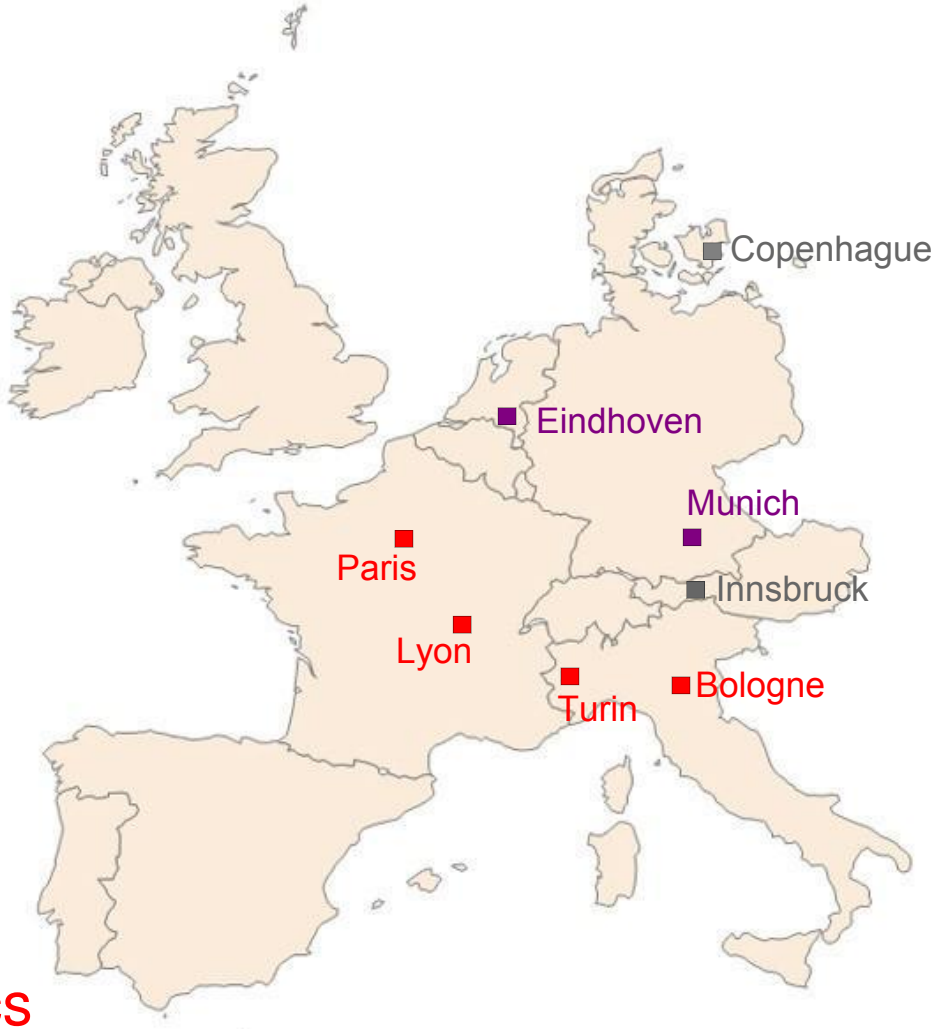
- Light logics
-
-
-
-

ICC European map



- Light logics
- TRS based techniques
-
-
-

ICC European map



- Light logics
- TRS based techniques
- Type systems
-
-

ICC European map

- Light logics
- TRS based techniques
- Type systems
- Abstract interpretations
-

ICC European map

- Light logics
- TRS based techniques
- Type systems
- Abstract interpretations
- Quasi and sup-interpretations

ICC European map

- Light logics : Turin
- TRS based techniques
- Type systems
- Abstract interpretations
- Quasi and sup-interpretations : Nancy

Italian participants

- Formal methods in computing, Dipartimento di informatica, Universita degli Studi di Torino:
  - Simona Ronchi Della Rocca, PR, principal investigator
  - Luca Roversi, assistant PR
  - Marco Gaboardi, postdoc (now in U. Penn.)
  - Mauro Piccolo, postdoc
  - Luca Vercelli, PhD student (has left CRISTAL in 2010)
  - Maurizio Dominici, PhD student since 09/2010
  - Erika De Benedetti, PhD student since 09/2011

French participants

- EPI Carte, Inria Nancy Grand-Est and UL:
  - Romain Péchoux, assistant PR, principal investigator
  - Guillaume Bonfante, assistant PR
  - Jean-Yves Marion, PR, team leader
  - Hugo Férée, PhD student since 9/2011

Results summary

The collaboration has led us to several results:

1. Characterizations of complexity classes based on Lafont's Soft Linear Logic (SLL)
2. Development and study of a resource lambda-calculus
3. Interpretations for studying stream complexity
4. Non-interference based type systems

1. SLL based characterizations

Linear Logic (LL) is a modal logic where premises are interpreted as physical resources having the same power as System F.

Soft Linear Logic (SLL) is a restriction to PTIME extended by:

- STA $\equiv$ (F)PTIME [TYPES 08]
- ISTA $\equiv$ (F)PTIME and SN with intersection types [ITRS12]
- PSTA $\equiv$ NPTIME [LSFA 08]
- BSTA $\equiv$ PSPACE [POPL 09, ACM TOCL 11]

2. Theoretical study of a resource lambda-calculus

Syntax introduced in [FOSSACS 10]:

$$M, N, \ldots ::= x \mid \lambda x.M \mid (M\ P) \mid M + N \qquad \text{(terms)}$$
$$P, Q, \ldots ::= [M_1, \ldots, M_n] \qquad \text{(bags)}$$

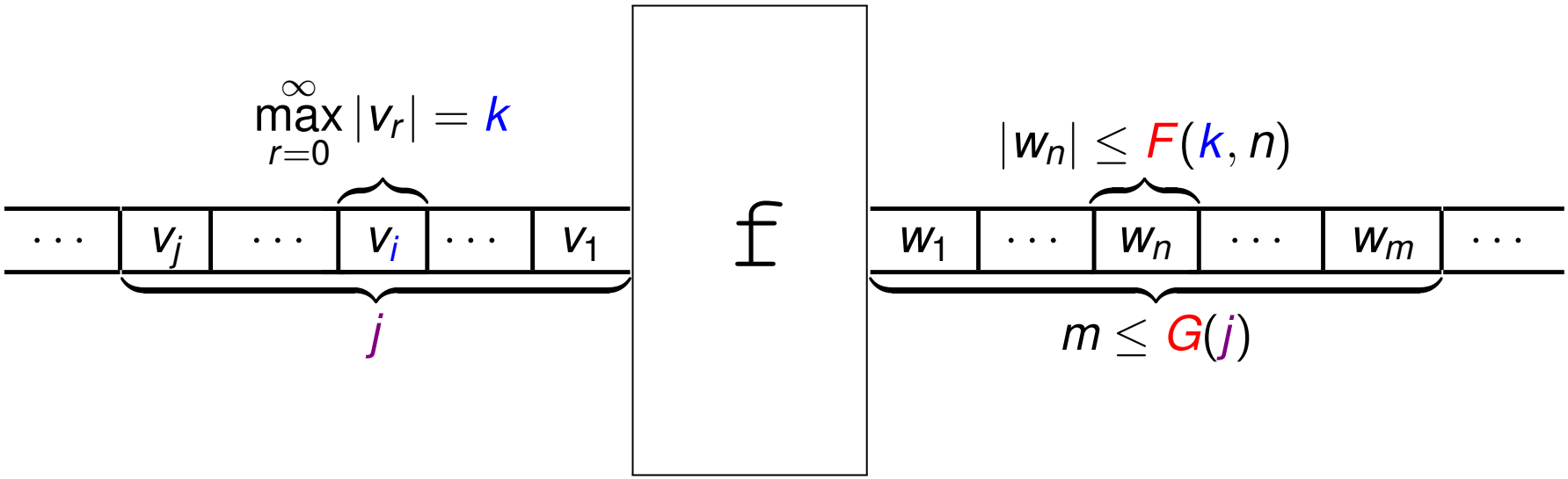
The β-rule becomes:

$$(\lambda x.M)[] \to_\beta M\{0/x\} \qquad (\lambda x.M)[N] \cdot P \to_\beta (\lambda x.M\langle N/x\rangle)P$$

- 0 is the neutral element of the sum
- $\{0/x\}$ is the usual λ-calculus substitution
- $\langle N/x\rangle$ i is the linear substitution , i.e., replacing one occurrence of x at a time.

This calculus has also been extended to a non-linear fragment.

3. Interpretations for studying stream complexity



- Criteria based on interpretations ensuring:
  - A local (global) upper bound F in [CSL 09], [I&C 2012]
  - A synchrony upper bound G in [FOPARA 10]
- Characterization of type-2 polynomial time complexity (related to BFF) in [ISAAC 10]

4. Non-interference based type systems

The type system [LICS 10] captures FPtime on an imperative language using:

- Non-interference type system by Volpano and Smith
- Tiering techniques by Leivant-Marion and Bellantoni-Cook

The essence is as follows:

$$\frac{X : \alpha \quad E : \beta}{X := E : \alpha}\ \alpha \leq \beta \qquad \frac{E : \mathbf{1} \quad C : \alpha}{\mathit{while}(E)\mathit{do}\{C\} : \mathbf{1}}\ \alpha, \beta \in \{\mathbf{0}, \mathbf{1}\}$$

Extended to:

- FPspace with processes using fork/wait instructions
- Multi-threads working in polynomial time

Publications (2009-2012):

24 publications in ICC (16 conferences and 8 journals):

- 3 journal co-publications:
  - An implicit characterization of pspace. ACM Transactions on Computational Logic, 2012.
  - Synthesis of sup-interpretations: a survey. Accepted to Theoretical Computer Science, 2012.
  - Space analysis of stream programs using interpretations. Submitted to Information & Computation. Under revision.
- 3 conference co-publications:
  - Global and local space properties of stream programs. In FOPARA 2010.
  - Upper bounds on stream I/O using semantic interpretations. In CSL 2009.
  - A Logical Account of PSPACE. In POPL 2009.
- Good publication record in:
  - conferences like POPL, LICS, ICFP, ESOP,...
  - journals like TCS, I&C, ACM TOCL, ...

Conclusion:

- An active community with two main annual events:
  - DICE, ETAPS affiliated workshop
  - LCC, LICS affiliated workshop
- In particular, the EA helped to:
  - fund and organize DICE 2011.
  - fund members travels and stays between distinct sites (Torino, Bologna, U. Penn. and Nancy).
  - fund PhD students (there were 5 students from 2009 to 2012).

Future ?

Complexity of stream programs...