Formal methods for public administrations

Raphaël Monat – SyCoMoRES team, Lille

rmonat.fr

COST proposal discussion
19 June 2025

Inria

whoami

Research Scientist at Inria Lille.

whoami

Research Scientist at Inria Lille.

Research Interests

whoami

Research Scientist at Inria Lille.

Research Interests

- Automated program analysis: C, Python, multi-language paradigms

whoami

Research Scientist at Inria Lille.

Research Interests

- Automated program analysis: C, Python, multi-language paradigms
- Formal methods for legal implementations (income taxes, social benefits, ...)

whoami

Research Scientist at Inria Lille.

Research Interests

- Automated program analysis: C, Python, multi-language paradigms
- Formal methods for legal implementations (income taxes, social benefits, ...)

Legal implementations are critical software!

whoami

Research Scientist at Inria Lille.

Research Interests

- Automated program analysis: C, Python, multi-language paradigms
- Formal methods for legal implementations (income taxes, social benefits, ...)

Legal implementations are critical software!

- Louvois: FR Army pay system from 2011-2021. 465M€ of errors in 2012 alone.

whoami

Research Scientist at Inria Lille.

Research Interests

- Automated program analysis: C, Python, multi-language paradigms
- Formal methods for legal implementations (income taxes, social benefits, ...)

Legal implementations are critical software!

- Louvois: FR Army pay system from 2011-2021. 465M€ of errors in 2012 alone.
- Phoenix: CA payroll for federal government since 2016. Pay problems for 80% of employees.

whoami

Research Scientist at Inria Lille.

Research Interests

- Automated program analysis: C, Python, multi-language paradigms
- Formal methods for legal implementations (income taxes, social benefits, ...)

Legal implementations are critical software!

- Louvois: FR Army pay system from 2011-2021. 465M€ of errors in 2012 alone.
- Phoenix: CA payroll for federal government since 2016. Pay problems for 80% of employees.

$\Longrightarrow$ High-assurance legal implementations?

whoami

Research Scientist at Inria Lille.

Research Interests

- Automated program analysis: C, Python, multi-language paradigms
- Formal methods for legal implementations (income taxes, social benefits, ...)

Legal implementations are critical software!

- Louvois: FR Army pay system from 2011-2021. 465M€ of errors in 2012 alone.
- Phoenix: CA payroll for federal government since 2016. Pay problems for 80% of employees.

$\Longrightarrow$ High-assurance legal implementations? Correctness, usability, trust, ...

Where it all started: the French tax code

Where it all started: the French tax code

2016 French law forces administration to $\simeq$ publish their source code.

Where it all started: the French tax code

2016 French law forces administration to $\simeq$ publish their source code.

04/2016 DGFiP releases the source code for income tax computation.

Where it all started: the French tax code

2016 French law forces administration to $\simeq$ publish their source code.

04/2016 DGFiP releases the source code for income tax computation.

02/2019 Denis Merigoux stumbles upon the codebase.

Where it all started: the French tax code

2016 French law forces administration to $\simeq$ publish their source code.

04/2016 DGFiP releases the source code for income tax computation.

02/2019 Denis Merigoux stumbles upon the codebase.

04-08/2019 On-the-side prototyping during our PhDs.

Where it all started: the French tax code

2016	French law forces administration to $\simeq$ publish their source code.
04/2016	DGFiP releases the source code for income tax computation.
02/2019	Denis Merigoux stumbles upon the codebase.
04-08/2019	On-the-side prototyping during our PhDs.
08/2019	Informal meeting with DGFiP. We discover some code is missing.

Where it all started: the French tax code

2016 French law forces administration to $\simeq$ publish their source code.

04/2016 DGFiP releases the source code for income tax computation.

02/2019 Denis Merigoux stumbles upon the codebase.

04-08/2019 On-the-side prototyping during our PhDs.

08/2019 Informal meeting with DGFiP. We discover some code is missing.

01/2020 Negotiations with DGFiP.

Where it all started: the French tax code

2016	French law forces administration to $\simeq$ publish their source code.
04/2016	DGFiP releases the source code for income tax computation.
02/2019	Denis Merigoux stumbles upon the codebase.
04-08/2019	On-the-side prototyping during our PhDs.
08/2019	Informal meeting with DGFiP. We discover some code is missing.
01/2020	Negotiations with DGFiP.
06/2020	At last, access to missing codebase!

Where it all started: the French tax code

2016	French law forces administration to $\simeq$ publish their source code.
04/2016	DGFiP releases the source code for income tax computation.
02/2019	Denis Merigoux stumbles upon the codebase.
04-08/2019	On-the-side prototyping during our PhDs.
08/2019	Informal meeting with DGFiP. We discover some code is missing.
01/2020	Negotiations with DGFiP.
06/2020	At last, access to missing codebase!
10/2020	Modern compiler, Mlang, ready. Paper submitted [MMP21]

Where it all started: the French tax code

2016	French law forces administration to $\simeq$ publish their source code.
04/2016	DGFiP releases the source code for income tax computation.
02/2019	Denis Merigoux stumbles upon the codebase.
04-08/2019	On-the-side prototyping during our PhDs.
08/2019	Informal meeting with DGFiP. We discover some code is missing.
01/2020	Negotiations with DGFiP.
06/2020	At last, access to missing codebase!
10/2020	Modern compiler, Mlang, ready. Paper submitted [MMP21]

Ongoing transfer of Mlang to be used in production at DGFiP

How to ensure an implementation complies with the law?

How to ensure an implementation complies with the law?

Catala, another DSL to the rescue [MCP21]

Article D823-20 of the French building regulations

The moving allowance is awarded to individuals or households with at least three children born or to be born and who move into a new home entitled to one of the personal housing allowances during a period between the first day of the calendar month following the third month of pregnancy for a child of rank three or more and the last day of the month preceding that in which the child reaches his or her second birthday.
This allowance is payable if the right to assistance is acquired within six months of the date of moving in.

```
```catala
scope MovingAllowanceEligibility:
 definition condition_moving_period under condition
  (match form.birthdate_third_child_or_more with pattern
  -- MoreThan3Children of date_of_birth_or_pregnancy:
   (match date_of_birth_or_pregnancy with pattern
    -- DateOfBirth of birthday
     current_date < (first_day_of_month of (birthday + 2 year))
    # ...
   )
  )
consequence fulfilled
```
```

How to ensure an implementation complies with the law?

Catala, another DSL to the rescue [MCP21]

Article D823-20 of the French building regulations

The moving allowance is awarded to individuals or households with at least three children born or to be born and who move into a new home entitled to one of the personal housing allowances during a period between the first day of the calendar month following the third month of pregnancy for a child of rank three or more and the last day of the month preceding that in which the child reaches his or her second birthday.
This allowance is payable if the right to assistance is acquired within six months of the date of moving in.

```catala
scope MovingAllowanceEligibility:
 definition condition_moving_period under condition
  (match form.birthdate_third_child_or_more with pattern
  -- MoreThan3Children of date_of_birth_or_pregnancy:
   (match date_of_birth_or_pregnancy with pattern
    -- DateOfBirth of birthday
     current_date < (first_day_of_month of (birthday + 2 year))
    # ...
   )
  )
consequence fulfilled
```

- Interdisciplinary work

How to ensure an implementation complies with the law?

Catala, another DSL to the rescue [MCP21]

Article D823-20 of the French building regulations

The moving allowance is awarded to individuals or households with at least three children born or to be born and who move into a new home entitled to one of the personal housing allowances during a period between the first day of the calendar month following the third month of pregnancy for a child of rank three or more and the last day of the month preceding that in which the child reaches his or her second birthday.
This allowance is payable if the right to assistance is acquired within six months of the date of moving in.

```
```catala
scope MovingAllowanceEligibility:
 definition condition_moving_period under condition
  (match form.birthdate_third_child_or_more with pattern
  -- MoreThan3Children of date_of_birth_or_pregnancy:
   (match date_of_birth_or_pregnancy with pattern
    -- DateOfBirth of birthday
     current_date < (first_day_of_month of (birthday + 2 year))
    # ...
   )
  )
consequence fulfilled
```

- Interdisciplinary work
- Literal programming
```

How to ensure an implementation complies with the law?

Catala, another DSL to the rescue [MCP21]

Article D823-20 of the French building regulations

The moving allowance is awarded to individuals or households with at least three children born or to be born and who move into a new home entitled to one of the personal housing allowances during a period between the first day of the calendar month following the third month of pregnancy for a child of rank three or more and the last day of the month preceding that in which the child reaches his or her second birthday.
This allowance is payable if the right to assistance is acquired within six months of the date of moving in.

```catala
scope MovingAllowanceEligibility:
 definition condition_moving_period under condition
  (match form.birthdate_third_child_or_more with pattern
  -- MoreThan3Children of date_of_birth_or_pregnancy:
   (match date_of_birth_or_pregnancy with pattern
    -- DateOfBirth of birthday
     current_date < (first_day_of_month of (birthday + 2 year))
    # ...
   )
  )
consequence fulfilled
```

- Interdisciplinary work
- Literal programming
- Default logic

Ongoing work around Catala

Proof of concept for public administrations (Merigoux, Gesbert, Primet, Botbol)

Ongoing work with CAF & DGFIP

Ongoing work around Catala

Proof of concept for public administrations (Merigoux, Gesbert, Primet, Botbol)

Ongoing work with CAF & DGFIP

AVoCat: Automated Verification of Catala Programs (Fromherz, Monat, Goutagny)

Ongoing work around Catala

Proof of concept for public administrations (Merigoux, Gesbert, Primet, Botbol)

Ongoing work with CAF & DGFIP

AVoCat: Automated Verification of Catala Programs (Fromherz, Monat, Goutagny)

- Formal semantics for date arithmetic [MFM24]

Ongoing work around Catala

Proof of concept for public administrations (Merigoux, Gesbert, Primet, Botbol)

Ongoing work with CAF & DGFIP

AVoCat: Automated Verification of Catala Programs (Fromherz, Monat, Goutagny)

- Formal semantics for date arithmetic [MFM24] `2025-01-31 + 1 mo = ?`

Ongoing work around Catala

Proof of concept for public administrations (Merigoux, Gesbert, Primet, Botbol)

Ongoing work with CAF & DGFIP

AVoCat: Automated Verification of Catala Programs (Fromherz, Monat, Goutagny)

- Formal semantics for date arithmetic [MFM24] `2025-01-31 + 1 mo = ?`
- Automatic, exhaustive* testcase generation [GFM25]

Ongoing work around Catala

Proof of concept for public administrations (Merigoux, Gesbert, Primet, Botbol)

Ongoing work with CAF & DGFIP

AVoCat: Automated Verification of Catala Programs (Fromherz, Monat, Goutagny)

- Formal semantics for date arithmetic [MFM24] `2025-01-31 + 1 mo = ?`
- Automatic, exhaustive* testcase generation [GFM25]
  - Detection of legal ambiguities + standard errors

Ongoing work around Catala

Proof of concept for public administrations (Merigoux, Gesbert, Primet, Botbol)

Ongoing work with CAF & DGFIP

AVoCat: Automated Verification of Catala Programs (Fromherz, Monat, Goutagny)

- Formal semantics for date arithmetic [MFM24] `2025-01-31 + 1 mo = ?`
- Automatic, exhaustive* testcase generation [GFM25]
  - Detection of legal ambiguities + standard errors
  - 186,390 testcases for French housing benefits

Ongoing work around Catala

Proof of concept for public administrations (Merigoux, Gesbert, Primet, Botbol)

Ongoing work with CAF & DGFIP

AVoCat: Automated Verification of Catala Programs (Fromherz, Monat, Goutagny)

- Formal semantics for date arithmetic [MFM24] `2025-01-31 + 1 mo = ?`
- Automatic, exhaustive* testcase generation [GFM25]
  - Detection of legal ambiguities + standard errors
  - 186,390 testcases for French housing benefits
  - Known inconsistency detected by our tool

Wrap-up

My work: new solutions for legal implementations, public administrations

Wrap-up

My work: new solutions for legal implementations, public administrations

- ✓ Based on interdisciplinary collaboration.

Wrap-up

My work: new solutions for legal implementations, public administrations

- ✓ Based on interdisciplinary collaboration.
- ✗ “Move fast and break things”

Wrap-up

My work: new solutions for legal implementations, public administrations

✓ Based on interdisciplinary collaboration.

✗ “Move fast and break things”

Happy to contribute to COST proposal!

Interests: A, B, C, D, $A \to C$, $B \to C$, $C \leftrightarrow C$, $D \to B$, $D \leftrightarrow D$.

Discussion:

- sovereignty?
- open-source, transparency, accountability?
- digital public services?

References – I

[GFM25] Pierre Goutagny, Aymeric Fromherz, and Raphaël Monat. **“CUTECat: Concolic Execution for Computational Law”.** In: ed. by Viktor Vafeiadis. Lecture Notes in Computer Science. Springer, 2025, pp. 31–61. DOI: 10.1007/978-3-031-91121-7_2.

[MCP21] Denis Merigoux, Nicolas Chataing, and Jonathan Protzenko. **“Catala: a programming language for the law”.** In: 2021.

[MFM24] Raphaël Monat, Aymeric Fromherz, and Denis Merigoux. **“Formalizing Date Arithmetic and Statically Detecting Ambiguities for the Law”.** In: ed. by Stephanie Weirich. Lecture Notes in Computer Science. Springer, 2024, pp. 421–450. DOI: 10.1007/978-3-031-57267-8_16.

References – II

[MMP21] Denis Merigoux, Raphaël Monat, and Jonathan Protzenko. **“A modern compiler for the French tax code”.** In: ed. by Aaron Smith, Delphine Demange, and Rajiv Gupta. ACM, 2021, pp. 71–82. DOI: 10.1145/3446804.3446850.