A Multilanguage Static Analysis of Python/C Programs with Mopsa

Raphaël Monat, Abdelraouf Ouadjaout, Antoine Miné

Dagstuhl
11 July 2023

Inria Université de Lille

Introduction

Static program analysis

average.py

```python
def average(l):
  m = 0
  for i in range(len(l)):
    m = m + l[i]
  m = m // (i + 1)
  return s

r1 = average([1, 2, 3])
r2 = average(['a', 'b', 'c'])
```

TypeError: unsupported operand type(s) for '+': 'int' and 'str'

argslen.c

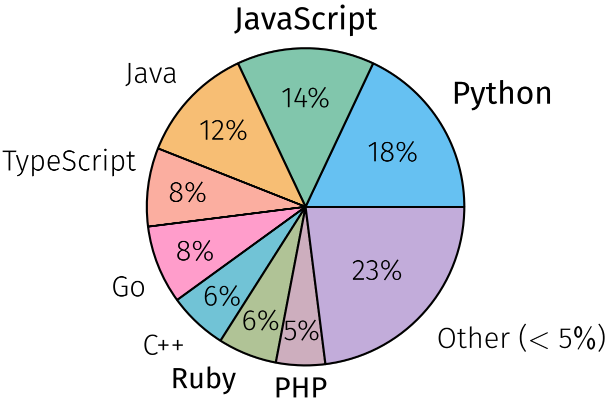
```c
#include <string.h>

int main(int argc, char *argv[]) {
  int i = 0;
  for (char **p = argv; *p; p++) {
    strlen(*p); // valid string
    i++; // no overflow
  }
  return 0;
}
```

No alarm

Specifications of the analyzer

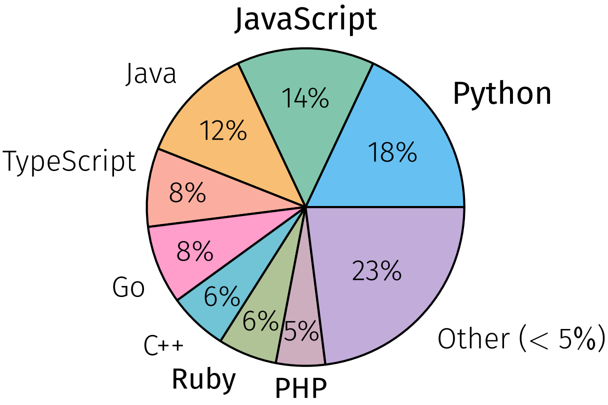
Inference	of program properties such as the absence of run-time errors.
Semantic	based on a formal modelization of the language.
Automatic	no expert knowledge required.
Sound	covers all possible executions.

Dynamic programming languages



Most popular languages on GitHub

Dynamic programming languages



Most popular languages on GitHub

Features

- Object orientation
- Dynamic typing
- Dynamic object structure
- Introspection operators
- `eval`

Combining C and Python – motivation

One in five of the top 200 Python libraries contains C code

Combining C and Python – motivation

One in five of the top 200 Python libraries contains C code

- To bring better performance (numpy)

Combining C and Python – motivation

One in five of the top 200 Python libraries contains C code

- To bring better performance (numpy)
- To provide library bindings (pygit2)

Combining C and Python – motivation

One in five of the top 200 Python libraries contains C code

- To bring better performance (numpy)
- To provide library bindings (pygit2)

Pitfalls

Combining C and Python – motivation

One in five of the top 200 Python libraries contains C code

- To bring better performance (numpy)
- To provide library bindings (pygit2)

Pitfalls

- Different values ($\mathbb{Z}$ vs. `Int32`)

Combining C and Python – motivation

One in five of the top 200 Python libraries contains C code

- To bring better performance (numpy)
- To provide library bindings (pygit2)

Pitfalls

- Different values ($\mathbb{Z}$ vs. `Int32`)
- Shared memory state

Outline

A Taste of Python

Python's specificities

No standard

- CPython is the reference

  $\Longrightarrow$ manual inspection of the source code and handcrafted tests

Python's specificities

No standard

- CPython is the reference

  $\Longrightarrow$ manual inspection of the source code and handcrafted tests

Operator redefinition

- Calls, additions, attribute accesses
- Operators eventually call overloaded `__methods__`

Protected attributes

```python
class Protected:
  def __init__(self, priv):
    self._priv = priv
  def __getattribute__(self, attr):
    if attr[0] == "_": raise AttributeError("...")
    return object.__getattribute__(self, attr)

a = Protected(42)
a._priv # AttributeError raised
```

Python's specificities (II)

Dual type system

- Nominal (classes, MRO)

Fspath (from standard library)

```python
class Path:
  def __fspath__(self): return 42

def fspath(p):
  if isinstance(p, (str, bytes)):
    return p
  elif hasattr(p, "__fspath__"):
    r = p.__fspath__()
    if isinstance(r, (str, bytes)):
      return r
  raise TypeError

fspath("/dev" if random() else Path())
```

Barrett, Cassels, Haahr, Moon, Playford, and Withington. "A Monotonic Superclass Linearization for Dylan". OOPSLA 1996

Python's specificities (II)

Dual type system

- Nominal (classes, MRO)
- **Structural (attributes)**

Fspath (from standard library)

```
class Path:
  def __fspath__(self): return 42

def fspath(p):
  if isinstance(p, (str, bytes)):
    return p
  elif hasattr(p, "__fspath__"):
    r = p.__fspath__()
    if isinstance(r, (str, bytes)):
      return r
  raise TypeError

fspath("/dev" if random() else Path())
```

Barrett, Cassels, Haahr, Moon, Playford, and Withington. "A Monotonic Superclass Linearization for Dylan". OOPSLA 1996

Python's specificities (II)

Dual type system

- Nominal (classes, MRO)
- Structural (attributes)

Exceptions

Exceptions rather than specific values

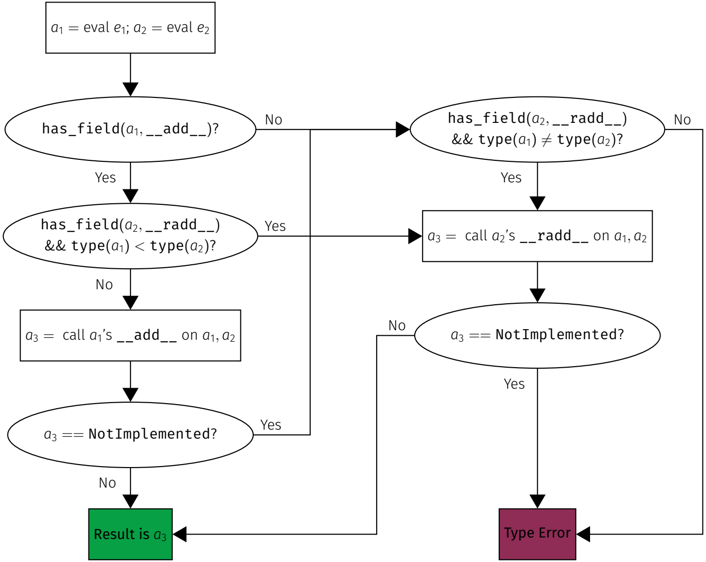
- `1 + "a"` ⇝ `TypeError`
- `l[len(l) + 1]` ⇝ `IndexError`

Fspath (from standard library)

```
class Path:
  def __fspath__(self): return 42

def fspath(p):
  if isinstance(p, (str, bytes)):
    return p
  elif hasattr(p, "__fspath__"):
    r = p.__fspath__()
    if isinstance(r, (str, bytes)):
      return r
  raise TypeError

fspath("/dev" if random() else Path())
```

Barrett, Cassels, Haahr, Moon, Playford, and Withington. "A Monotonic Superclass Linearization for Dylan". OOPSLA 1996

Example Semantics – binary operators



Custom infix operators

```python
class Infix(object):
    def __init__(self, func): self.func = func
    def __or__(self, other): return self.func(other)
    def __ror__(self, other): return Infix(lambda x: self.func(other, x))

instanceof = Infix(isinstance)
b = 5 |instanceof| int

@Infix
def padd(x, y):
  print(f"{x} + {y} = {x + y}")
  return x + y
c = 2 |padd| 3
```

Credits `tomerfiliba.com/blog/Infix-Operators/`

Overview of our value analysis for Python

Goal

Detect runtime errors: uncaught raised exceptions

Overview of our value analysis for Python

Goal

Detect runtime errors: uncaught raised exceptions

Supported constructs

Our analysis supports:

- Objects
- Exceptions
- Dynamic typing
- Introspection
- Permissive semantics
- Dynamic attributes
- Generators
- `super`
- Metaclasses

Overview of our value analysis for Python

Goal

Detect runtime errors: uncaught raised exceptions

Supported constructs

Our analysis supports:

- Objects
- Exceptions
- Dynamic typing
- Introspection
- Permissive semantics
- Dynamic attributes
- Generators
- `super`
- Metaclasses

Unsupported constructs

- Recursive functions
- `eval`
- Finalizers

Mopsa

A program analysis workflow

Averaging numbers

```
def average(l):
  m = 0
  for i in range(len(l)):
    m = m + l[i]
  m = m // (i + 1)
  return m

l = [randint(0, 20)
  for i in range(randint(5, 10))]
m = average(l)
```

A program analysis workflow

Averaging numbers

```python
def average(l):
  m = 0
  for i in range(len(l)):
    m = m + l[i]
  m = m // (i + 1)
  return m

l = [randint(0, 20)
  for i in range(randint(5, 10))]
m = average(l)
```

Proved safe?

- `m // (i+1)`
- `l[i]`

Searching for a loop invariant (l. 4)

Environment abstraction

$m \mapsto @^\sharp_{\mathtt{int}^\sharp} \quad i \mapsto @^\sharp_{\mathtt{int}^\sharp}$

A program analysis workflow

Averaging numbers

```
1  def average(l):
2    m = 0
3    for i in range(len(l)):
4      m = m + l[i]
5    m = m // (i + 1)
6    return m
7
8  l = [randint(0, 20)
9    for i in range(randint(5, 10))]
10 m = average(l)
```

Proved safe?

- `m // (i+1)`
- `l[i]`

Searching for a loop invariant (l. 4)

Stateless domains: **list content**,

Environment abstraction

$m \mapsto @^\sharp_{\texttt{int}^\sharp}$ $\quad i \mapsto @^\sharp_{\texttt{int}^\sharp}$ $\quad \boldsymbol{\underline{\mathrm{els}}(l)} \mapsto \boldsymbol{@^\sharp_{\texttt{int}^\sharp}}$

A program analysis workflow

Averaging numbers

```
1  def average(l):
2    m = 0
3    for i in range(len(l)):
4      m = m + l[i]
5    m = m // (i + 1)
6    return m
7
8  l = [randint(0, 20)
9    for i in range(randint(5, 10))]
10 m = average(l)
```

Proved safe?

- `m // (i+1)`
- `l[i]`

Searching for a loop invariant (l. 4)

Stateless domains: list content,

Environment abstraction

$m \mapsto @^\sharp_{\texttt{int}^\sharp}$ $\quad i \mapsto @^\sharp_{\texttt{int}^\sharp}$ $\quad \underline{\text{els}}(l) \mapsto @^\sharp_{\texttt{int}^\sharp}$

Numeric abstraction (intervals)

$m \in [0, +\infty)$ $\quad \underline{\text{els}}(l) \in [0, 20]$ $\quad i \in [0, +\infty)$

A program analysis workflow

Averaging numbers

```
1  def average(l):
2    m = 0
3    for i in range(len(l)):
4      m = m + l[i]
5    m = m // (i + 1)
6    return m
7
8  l = [randint(0, 20)
9    for i in range(randint(5, 10))]
10 m = average(l)
```

Proved safe?

- `m // (i+1)`
- `l[i]`

Searching for a loop invariant (l. 4)

Stateless domains: list content, **list length**

Environment abstraction

$m \mapsto @^\sharp_{\mathtt{int}^\sharp}$ $\quad i \mapsto @^\sharp_{\mathtt{int}^\sharp}$ $\quad \underline{\mathrm{els}}(l) \mapsto @^\sharp_{\mathtt{int}^\sharp}$

Numeric abstraction (intervals)

$m \in [0, +\infty)$ $\quad \underline{\mathrm{els}}(l) \in [0, 20]$

$\boldsymbol{\underline{\mathrm{len}}(l) \in [5, 10]}$ $\quad \boldsymbol{i \in [0, 10]}$

A program analysis workflow

Averaging numbers

```
1  def average(l):
2    m = 0
3    for i in range(len(l)):
4      m = m + l[i]
5    m = m // (i + 1)
6    return m
7
8  l = [randint(0, 20)
9    for i in range(randint(5, 10))]
10 m = average(l)
```

Proved safe?

- `m // (i+1)`
- `l[i]`

Searching for a loop invariant (l. 4)

Stateless domains: list content, list length

Environment abstraction

$m \mapsto @^\sharp_{\texttt{int}^\sharp} \quad i \mapsto @^\sharp_{\texttt{int}^\sharp} \quad \underline{\mathsf{els}}(l) \mapsto @^\sharp_{\texttt{int}^\sharp}$

Numeric abstraction (polyhedra)

$m \in [0, +\infty) \quad \underline{\mathsf{els}}(l) \in [0, 20]$

$\mathbf{0 \leq \mathit{i} < \underline{len}(\mathit{l}) \quad 5 \leq \underline{len}(\mathit{l}) \leq 10}$

A program analysis workflow

Averaging tasks

```
1  class Task:
2    def __init__(self, weight):
3      if weight < 0: raise ValueError
4      self.weight = weight
5
6  def average(l):
7    m = 0
8    for i in range(len(l)):
9      m = m + l[i].weight
10   m = m // (i + 1)
11   return m
12
13 l = [Task(randint(0, 20))
14   for i in range(randint(5, 10))]
15 m = average(l)
```

Proved safe?

- `m // (i+1)`
- `l[i].weight`

Searching for a loop invariant (l. 4)

Stateless domains: list content, list length

Environment abstraction

$m \mapsto @^\sharp_{\texttt{int}^\sharp}$ $\quad i \mapsto @^\sharp_{\texttt{int}^\sharp}$ $\quad \underline{\text{els}(l)} \mapsto @^\sharp_{\texttt{Task}}$

$\underline{@^\sharp_{\texttt{Task}} \cdot \texttt{weight}} \mapsto @^\sharp_{\texttt{int}^\sharp}$

Numeric abstraction (polyhedra)

$m \in [0, +\infty)$

$0 \leq i < \underline{\text{len}}(l) \quad 5 \leq \underline{\text{len}}(l) \leq 10$

$0 \leq \underline{@^\sharp_{\texttt{Task}} \cdot \texttt{weight}} \leq 20$

Attributes abstraction

$@^\sharp_{\texttt{Task}} \mapsto (\{\texttt{weight}\}, \emptyset)$

A program analysis workflow

Averaging tasks

```
1  class Task:
2    def __init__(self, weight):
3      if weight < 0: raise ValueError
4      self.weight = weight
5
6  def average(l):
7    m = 0
8    for i in range(l
9      m = m + l[i].w
10   m = m // (i + 1)
11   return m
12
13 l = [Task(randint(
14   for i in range(randint(5, 10))]
15 m = average(l)
```

Proved safe?

- `m // (i+1)`
- `l[i].weight`

Searching for a loop invariant (l. 4)

Stateless domains: list content, list length

Environment abstraction

$m \mapsto @^\sharp$ … $\mapsto @^\sharp_{\texttt{Task}}$

Conclusion

- Different domains depending on the precision
- Use of auxiliary variables (<u>underlined</u>)

…)

$[\ldots, +\infty)$

$0 \leq i < \underline{\mathrm{len}}(l) \quad 5 \leq \underline{\mathrm{len}}(l) \leq 10$

$0 \leq \underline{@^\sharp_{\texttt{Task}} \cdot \texttt{weight}} \leq 20$

Attributes abstraction

$@^\sharp_{\texttt{Task}} \mapsto (\{\,\texttt{weight}\,\}, \emptyset)$

Modular **O**pen **P**latform for **S**tatic **A**nalysis[1]

`gitlab.com/mopsa/mopsa-analyzer`

[1] Journault, Miné, Monat, and Ouadjaout. "Combinations of reusable abstract domains for a multilingual static analyzer". 2019.

Modular Open Platform for Static Analysis[1]

`gitlab.com/mopsa/mopsa-analyzer`

- One AST to analyze them all
  - Multilanguage support
  - Expressiveness
  - Reusability

[1] Journault, Miné, Monat, and Ouadjaout. "Combinations of reusable abstract domains for a multilingual static analyzer". 2019.

Modular Open Platform for Static Analysis[1]

`gitlab.com/mopsa/mopsa-analyzer`

- One AST to analyze them all
  - Multilanguage support
  - Expressiveness
  - Reusability
- Unified domain signature
  - Semantic rewriting
  - Loose coupling
  - Observability

[1] Journault, Miné, Monat, and Ouadjaout. "Combinations of reusable abstract domains for a multilingual static analyzer". 2019.

Modular Open Platform for Static Analysis[1]

`gitlab.com/mopsa/mopsa-analyzer`

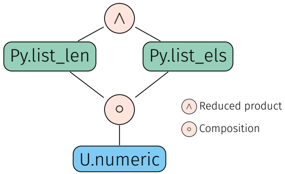
- One AST to analyze them all
  - Multilanguage support
  - Expressiveness
  - Reusability
- Unified domain signature
  - Semantic rewriting
  - Loose coupling
  - Observability
- DAG of abstract domains
  - Composition
  - Cooperation

[1] Journault, Miné, Monat, and Ouadjaout. "Combinations of reusable abstract domains for a multilingual static analyzer". 2019.

Modular Open Platform for Static Analysis[1]

`gitlab.com/mopsa/mopsa-analyzer`

- One AST to analyze them all
  - Multilanguage support
  - Expressiveness
  - Reusability
- Unified domain signature
  - Semantic rewriting
  - Loose coupling
  - Observability
- DAG of abstract domains
  - Composition
  - Cooperation



[1]Journault, Miné, Monat, and Ouadjaout. "Combinations of reusable abstract domains for a multilingual static analyzer". 2019.

Dynamic, semantic iterators with delegation

Universal.Iterators.Loops
Matches `while(...){...}`
Computes fixpoint using widening

Dynamic, semantic iterators with delegation

```
for(init; cond; incr) body
```

Universal.Iterators.Loops
Matches `while(...){...}`
Computes fixpoint using widening

Dynamic, semantic iterators with delegation

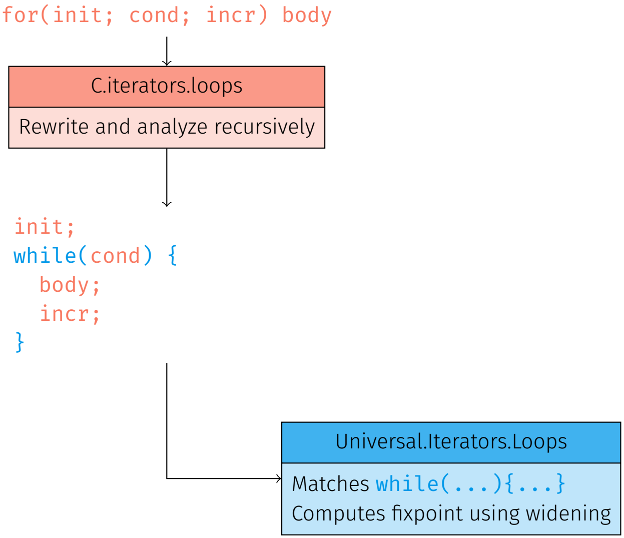
`for(init; cond; incr) body`

↓

C.iterators.loops
Rewrite and analyze recursively

Universal.Iterators.Loops
Matches `while(...){...}` Computes fixpoint using widening

Dynamic, semantic iterators with delegation



Dynamic, semantic iterators with delegation

```
for(init; cond; incr) body
```

```
for target in iterable: body
```

C.iterators.loops

Rewrite and analyze recursively

```
init;
while(cond) {
  body;
  incr;
}
```

Universal.Iterators.Loops

Matches `while(...){...}`

Computes fixpoint using widening

Dynamic, semantic iterators with delegation

`for(init; cond; incr) body`

C.iterators.loops

Rewrite and analyze recursively

```
init;
while(cond) {
  body;
  incr;
}
```

`for target in iterable: body`

Python.Desugar.Loops

- Rewrite and analyze recursively
- Optimize for some semantic cases

Universal.Iterators.Loops

Matches `while(...){...}`

Computes fixpoint using widening

Dynamic, semantic iterators with delegation

```
for(init; cond; incr) body
```

C.iterators.loops

Rewrite and analyze recursively

```
init;
while(cond) {
  body;
  incr;
}
```

```
for target in iterable: body
```

Python.Desugar.Loops

- Rewrite and analyze recursively
- Optimize for some <u>semantic</u> cases

```
it = iter(iterable)
while(1) {
 try: target = next(it)
 except StopIteration: break
 body
}
clean it
```

Universal.Iterators.Loops

Matches `while(...){...}`

Computes fixpoint using widening

Expression rewriting

$\mathbb{S}^{\#}_{env}[\![\, m = m + l[i].weight \,]\!]^{\#}_{env}\sigma^{\sharp}$

Expression rewriting

$\mathbb{S}^{\#}_{env}\llbracket\, m = m + l[i].weight \,\rrbracket^{\#}_{env}\sigma^{\sharp}$

$\hookrightarrow \mathbb{E}^{\#}_{binop}\llbracket\, m + l[i].weight \,\rrbracket\sigma^{\sharp}$

Expression rewriting

$\mathbb{S}^{\#}_{env}[\![\, m = m + l[i].weight \,]\!]^{\#}_{env}\sigma^{\sharp}$

$\quad\hookrightarrow \mathbb{E}^{\#}_{binop}[\![\, m + l[i].weight \,]\!]\sigma^{\sharp}$

$\qquad\hookrightarrow \mathbb{E}^{\#}_{env}[\![\, m \,]\!]\sigma^{\sharp}$

$\qquad\longleftarrow \langle @^{\sharp}_{\mathtt{int}^{\sharp}}, \underline{\mathrm{int}}(m)\rangle, \sigma^{\sharp}$

Expression rewriting

$\mathbb{S}^{\#}_{env}[\![\, m = m + l[i].weight \,]\!]^{\#}_{env} \sigma^{\sharp}$

$\hookrightarrow \mathbb{E}^{\#}_{binop}[\![\, m + l[i].weight \,]\!] \sigma^{\sharp}$

$\quad \hookrightarrow \mathbb{E}^{\#}_{env}[\![\, m \,]\!] \sigma^{\sharp}$

$\quad \longleftarrow \langle @^{\sharp}_{\mathtt{int}^{\sharp}}, \underline{\mathrm{int}}(m) \rangle, \sigma^{\sharp}$

$\quad \hookrightarrow \mathbb{E}^{\#}_{attrs}[\![\, l[i].weight \,]\!] \sigma^{\sharp}$

Expression rewriting

$\mathbb{S}^{\#}_{env}[\![\, m = m + l[i].weight \,]\!]^{\#}_{env}\sigma^{\sharp}$

$\hookrightarrow \mathbb{E}^{\#}_{binop}[\![\, m + l[i].weight \,]\!]\sigma^{\sharp}$

$\quad \hookrightarrow \mathbb{E}^{\#}_{env}[\![\, m \,]\!]\sigma^{\sharp}$

$\quad \longleftarrow \langle @^{\sharp}_{\mathtt{int}^{\sharp}}, \underline{\mathrm{int}}(m)\rangle, \sigma^{\sharp}$

$\quad \hookrightarrow \mathbb{E}^{\#}_{attrs}[\![\, l[i].weight \,]\!]\sigma^{\sharp}$

$\quad\quad \hookrightarrow \mathbb{E}^{\#}_{index}[\![\, l[i] \,]\!]\sigma^{\sharp}$

Expression rewriting

$\mathbb{S}^{\#}_{env}[\![\, m = m + l[i].weight \,]\!]^{\#}_{env}\sigma^{\sharp}$

$\quad\hookrightarrow \mathbb{E}^{\#}_{binop}[\![\, m + l[i].weight \,]\!]\sigma^{\sharp}$

$\qquad\mapsto \mathbb{E}^{\#}_{env}[\![\, m \,]\!]\sigma^{\sharp}$

$\qquad\longleftarrow \langle @^{\sharp}_{\mathtt{int}^{\sharp}}, \underline{\mathrm{int}}(m)\rangle, \sigma^{\sharp}$

$\qquad\hookrightarrow \mathbb{E}^{\#}_{attrs}[\![\, l[i].weight \,]\!]\sigma^{\sharp}$

$\qquad\quad\hookrightarrow \mathbb{E}^{\#}_{index}[\![\, l[i] \,]\!]\sigma^{\sharp}$

$\qquad\qquad\hookrightarrow \mathbb{E}^{\#}_{env}[\![\, l \,]\!]\sigma^{\sharp}$

$\qquad\qquad\longleftarrow \langle @^{\sharp}_{list,\mathbf{r}}, \perp\rangle, \sigma^{\sharp}$

Expression rewriting

$\mathbb{S}^{\#}_{env}[\![\, m = m + l[i].weight \,]\!]^{\#}_{env}\sigma^{\sharp}$

$\hookrightarrow \mathbb{E}^{\#}_{binop}[\![\, m + l[i].weight \,]\!]\sigma^{\sharp}$

$\quad \hookrightarrow \mathbb{E}^{\#}_{env}[\![\, m \,]\!]\sigma^{\sharp}$

$\quad \longleftarrow \langle @^{\sharp}_{\texttt{int}^{\sharp}}, \underline{\mathrm{int}}(m)\rangle, \sigma^{\sharp}$

$\quad \hookrightarrow \mathbb{E}^{\#}_{attrs}[\![\, l[i].weight \,]\!]\sigma^{\sharp}$

$\quad\quad \hookrightarrow \mathbb{E}^{\#}_{index}[\![\, l[i] \,]\!]\sigma^{\sharp}$

$\quad\quad\quad \hookrightarrow \mathbb{E}^{\#}_{env}[\![\, l \,]\!]\sigma^{\sharp}$

$\quad\quad\quad \longleftarrow \langle @^{\sharp}_{list,\mathbf{r}}, \perp\rangle, \sigma^{\sharp}$

$\quad\quad\quad \hookrightarrow \mathbb{E}^{\#}_{env}[\![\, i \,]\!]\sigma^{\sharp}$

$\quad\quad\quad \longleftarrow \langle @^{\sharp}_{\texttt{int}^{\sharp}}, \underline{\mathrm{int}}(i)\rangle, \sigma^{\sharp}$

Expression rewriting

$\mathbb{S}^{\#}_{env}[\![\, m = m + l[i].weight \,]\!]^{\#}_{env}\sigma^\sharp$

$\hookrightarrow \mathbb{E}^{\#}_{binop}[\![\, m + l[i].weight \,]\!]\sigma^\sharp$

$\hookrightarrow \mathbb{E}^{\#}_{env}[\![\, m \,]\!]\sigma^\sharp$

$\longleftarrow \langle @^\sharp_{\mathtt{int}^\sharp}, \underline{\mathrm{int}}(m)\rangle, \sigma^\sharp$

$\hookrightarrow \mathbb{E}^{\#}_{attrs}[\![\, l[i].weight \,]\!]\sigma^\sharp$

$\hookrightarrow \mathbb{E}^{\#}_{index}[\![\, l[i] \,]\!]\sigma^\sharp$

$\hookrightarrow \mathbb{E}^{\#}_{env}[\![\, l \,]\!]\sigma^\sharp$

$\longleftarrow \langle @^\sharp_{list,\mathrm{r}}, \bot\rangle, \sigma^\sharp$

$\hookrightarrow \mathbb{E}^{\#}_{env}[\![\, i \,]\!]\sigma^\sharp$

$\longleftarrow \langle @^\sharp_{\mathtt{int}^\sharp}, \underline{\mathrm{int}}(i)\rangle, \sigma^\sharp$

$\hookrightarrow \mathbb{E}^{\#}_{list}[\![\, \mathtt{list.\_\_getitem\_\_}(l, i) \,]\!]\sigma^\sharp$

$\hookrightarrow \mathbb{S}^{\#}_{num}[\![\, \mathtt{assume}\ 0 \le \underline{\mathrm{int}}(i) < \underline{\mathrm{len}}(@^\sharp_{list,\mathrm{r}}) \,]\!]^{\#}_{num}\sigma^\sharp$

$\hookrightarrow \mathbb{E}^{\#}_{env}[\![\, \underline{\mathrm{els}}(@^\sharp_{list,\mathrm{r}}) \,]\!]\sigma^\sharp$

$\longleftarrow \langle @^\sharp_{Task,\mathrm{r}}, \bot\rangle, \sigma^\sharp$

Expression rewriting

$\mathbb{S}^{\#}_{env}[\![\, m = m + l[i].weight \,]\!]^{\#}_{env}\sigma^{\sharp}$

$\hookrightarrow \mathbb{E}^{\#}_{binop}[\![\, m + l[i].weight \,]\!]\sigma^{\sharp}$

$\rightarrow \mathbb{E}^{\#}_{env}[\![\, m \,]\!]\sigma^{\sharp}$

$\longleftarrow \langle @^{\sharp}_{\mathtt{int}^{\sharp}}, \underline{\mathrm{int}}(m)\rangle, \sigma^{\sharp}$

$\rightarrow \mathbb{E}^{\#}_{attrs}[\![\, l[i].weight \,]\!]\sigma^{\sharp}$

$\rightarrow \mathbb{E}^{\#}_{index}[\![\, l[i] \,]\!]\sigma^{\sharp}$

$\rightarrow \mathbb{E}^{\#}_{env}[\![\, l \,]\!]\sigma^{\sharp}$

$\longleftarrow \langle @^{\sharp}_{list,\mathsf{r}}, \perp\rangle, \sigma^{\sharp}$

$\rightarrow \mathbb{E}^{\#}_{env}[\![\, i \,]\!]\sigma^{\sharp}$

$\longleftarrow \langle @^{\sharp}_{\mathtt{int}^{\sharp}}, \underline{\mathrm{int}}(i)\rangle, \sigma^{\sharp}$

$\rightarrow \mathbb{E}^{\#}_{list}[\![\, \mathtt{list.\_\_getitem\_\_}(l, i) \,]\!]\sigma^{\sharp}$

$\rightarrow \mathbb{S}^{\#}_{num}[\![\, \mathtt{assume}\ 0 \leq \underline{\mathrm{int}}(i) < \underline{\mathrm{len}}(@^{\sharp}_{list,\mathsf{r}}) \,]\!]^{\#}_{num}\sigma^{\sharp}$

$\rightarrow \mathbb{E}^{\#}_{env}[\![\, \underline{\mathrm{els}}(@^{\sharp}_{list,\mathsf{r}}) \,]\!]\sigma^{\sharp}$

$\longleftarrow \langle @^{\sharp}_{Task,\mathsf{r}}, \perp\rangle, \sigma^{\sharp}$

$\rightarrow \mathbb{E}^{\#}_{object}[\![\, \mathtt{object.\_\_getattribute\_\_}(l[i], "weight") \,]\!]\sigma^{\sharp}$

$\rightarrow \mathbb{E}^{\#}_{heap}[\![\, get\_field(l[i], "weight") \,]\!]\sigma^{\sharp}$

$\rightarrow \mathbb{E}^{\#}_{env}[\![\, l[i] \cdot weight \,]\!]\sigma^{\sharp}$

$\longleftarrow \langle @^{\sharp}_{\mathtt{int}^{\sharp}}, \underline{\mathrm{int}}(\underline{@^{\sharp}_{Task,\mathsf{r}} \cdot weight})\rangle, \sigma^{\sharp}$

Towards a Multilanguage Analysis

Multilanguage code – example

counter.c

```c
typedef struct {
    PyObject_HEAD;
    int count;
} Counter;

static PyObject*
CounterIncr(Counter *self, PyObject *args)
{
    int i = 1;
    if(!PyArg_ParseTuple(args, "|i", &i))
        return NULL;

    self->count += i;
    Py_RETURN_NONE;
}

static PyObject*
CounterGet(Counter *self)
{
    return Py_BuildValue("i", self->count);
}
```

count.py

```python
from counter import Counter
from random import randrange

c = Counter()
power = randrange(128)
c.incr(2**power-1)
c.incr()
r = c.get()
```

Multilanguage code – example

counter.c

```c
typedef struct {
    PyObject_HEAD;
    int count;
} Counter;

static PyObject*
CounterIncr(Counter *self, PyObject *args)
{
    int i = 1;
    if(!PyArg_ParseTuple(args, "|i", &i))
        return NULL;

    self->count += i;
    Py_RETURN_NONE;
}

static PyObject*
CounterGet(Counter *self)
{
    return Py_BuildValue("i", self->count);
}
```

count.py

```python
from counter import Counter
from random import randrange

c = Counter()
power = randrange(128)
c.incr(2**power-1)
c.incr()
r = c.get()
```

Multilanguage code – example

counter.c

```c
typedef struct {
    PyObject_HEAD;
    int count;
} Counter;

static PyObject*
CounterIncr(Counter *self, PyObject *args)
{
    int i = 1;
    if(!PyArg_ParseTuple(args, "|i", &i))
        return NULL;

    self->count += i;
    Py_RETURN_NONE;
}

static PyObject*
CounterGet(Counter *self)
{
    return Py_BuildValue("i", self->count);
}
```

count.py

```python
from counter import Counter
from random import randrange

c = Counter()
power = randrange(128)
c.incr(2**power-1)
c.incr()
r = c.get()
```

Multilanguage code – example

counter.c

```c
typedef struct {
    PyObject_HEAD;
    int count;
} Counter;

static PyObject*
CounterIncr(Counter *self, PyObject *args)
{
    int i = 1;
    if(!PyArg_ParseTuple(args, "|i", &i))
        return NULL;

    self->count += i;
    Py_RETURN_NONE;
}

static PyObject*
CounterGet(Counter *self)
{
    return Py_BuildValue("i", self->count);
}
```

count.py

```python
from counter import Counter
from random import randrange

c = Counter()
power = randrange(128)
c.incr(2**power-1)
c.incr()
r = c.get()
```

Multilanguage code – example

counter.c

```c
typedef struct {
    PyObject_HEAD;
    int count;
} Counter;

static PyObject*
CounterIncr(Counter *self, PyObject *args)
{
    int i = 1;
    if(!PyArg_ParseTuple(args, "|i", &i))
        return NULL;

    self->count += i;
    Py_RETURN_NONE;
}

static PyObject*
CounterGet(Counter *self)
{
    return Py_BuildValue("i", self->count);
}
```

count.py

```python
from counter import Counter
from random import randrange

c = Counter()
power = randrange(128)
c.incr(2**power-1)
c.incr()
r = c.get()
```

Multilanguage code – example

counter.c

```c
typedef struct {
    PyObject_HEAD;
    int count;
} Counter;

static PyObject*
CounterIncr(Counter *self, PyObject *args)
{
    int i = 1;
    if(!PyArg_ParseTuple(args, "|i", &i))
        return NULL;

    self->count += i;
    Py_RETURN_NONE;
}

static PyObject*
CounterGet(Counter *self)
{
    return Py_BuildValue("i", self->count);
}
```

count.py

```python
from counter import Counter
from random import randrange

c = Counter()
power = randrange(128)
c.incr(2**power-1)
c.incr()
r = c.get()
```

Multilanguage code – example

counter.c

```c
typedef struct {
    PyObject_HEAD;
    int count;
} Counter;

static PyObject*
CounterIncr(Counter *self, PyObject *args)
{
    int i = 1;
    if(!PyArg_ParseTuple(args, "|i", &i))
        return NULL;

    self->count += i;
    Py_RETURN_NONE;
}

static PyObject*
CounterGet(Counter *self)
{
    return Py_BuildValue("i", self->count);
}
```

count.py

```python
from counter import Counter
from random import randrange

c = Counter()
power = randrange(128)
c.incr(2**power-1)
c.incr()
r = c.get()
```

- $\texttt{power} \leq 30 \Rightarrow \texttt{r} = 2^{\texttt{power}}$

Multilanguage code – example

counter.c

```c
typedef struct {
    PyObject_HEAD;
    int count;
} Counter;

static PyObject*
CounterIncr(Counter *self, PyObject *args)
{
    int i = 1;
    if(!PyArg_ParseTuple(args, "|i", &i))
        return NULL;

    self->count += i;
    Py_RETURN_NONE;
}

static PyObject*
CounterGet(Counter *self)
{
    return Py_BuildValue("i", self->count);
}
```

count.py

```python
from counter import Counter
from random import randrange

c = Counter()
power = randrange(128)
c.incr(2**power-1)
c.incr()
r = c.get()
```

- $\texttt{power} \leq 30 \Rightarrow \texttt{r} = 2^{\texttt{power}}$
- $32 \leq \texttt{power} \leq 64$: OverflowError: signed integer is greater than maximum
- $\texttt{power} \geq 64$: OverflowError: Python int too large to convert to C long

Multilanguage code – example

counter.c

```c
typedef struct {
    PyObject_HEAD;
    int count;
} Counter;

static PyObject*
CounterIncr(Counter *self, PyObject *args)
{
    int i = 1;
    if(!PyArg_ParseTuple(args, "|i", &i))
        return NULL;

    self->count += i;
    Py_RETURN_NONE;
}

static PyObject*
CounterGet(Counter *self)
{
    return Py_BuildValue("i", self->count);
}
```

count.py

```python
from counter import Counter
from random import randrange

c = Counter()
power = randrange(128)
c.incr(2**power-1)
c.incr()
r = c.get()
```

- $\texttt{power} \leq 30 \Rightarrow \texttt{r} = 2^{\texttt{power}}$
- $\texttt{power} = 31 \Rightarrow \texttt{r} = -2^{31}$
- $32 \leq \texttt{power} \leq 64$: OverflowError: signed integer is greater than maximum
- $\texttt{power} \geq 64$: OverflowError: Python int too large to convert to C long

How to analyze multilanguage programs?

Type annotations

```python
class Counter:
  def __init__(self): ...
  def incr(self, i: int = 1): ...
  def get(self) -> int: ...
```

How to analyze multilanguage programs?

Type annotations

```
class Counter:
  def __init__(self): ...
  def incr(self, i: int = 1): ...
  def get(self) -> int: ...
```

- No raised exceptions $\Longrightarrow$ missed errors

How to analyze multilanguage programs?

Type annotations

```
class Counter:
  def __init__(self): ...
  def incr(self, i: int = 1): ...
  def get(self) -> int: ...
```

- No raised exceptions $\implies$ missed errors
- Only types

How to analyze multilanguage programs?

Type annotations

```python
class Counter:
  def __init__(self): ...
  def incr(self, i: int = 1): ...
  def get(self) -> int: ...
```

- No raised exceptions $\implies$ missed errors
- Only types
- Typeshed: type annotations for the standard library

How to analyze multilanguage programs?

Type annotations

```python
class Counter:
  def __init__(self): ...
  def incr(self, i: int = 1): ...
  def get(self) -> int: ...
```

- No raised exceptions $\implies$ missed errors
- Only types
- Typeshed: type annotations for the standard library, used in previous work: Monat, Ouadjaout, and Miné. "Static Type Analysis by Abstract Interpretation of Python Programs". ECOOP 2020.

How to analyze multilanguage programs?

Type annotations

Rewrite into Python code

```
class Counter:
  def __init__(self):
    self.count = 0
  def get(self):
    return self.count
  def incr(self, i=1):
    self.count += i
```

How to analyze multilanguage programs?

Type annotations

Rewrite into Python code

```
class Counter:
  def __init__(self):
    self.count = 0
  def get(self):
    return self.count
  def incr(self, i=1):
    self.count += i
```

- No integer wrap-around in Python

How to analyze multilanguage programs?

Type annotations

Rewrite into Python code

```
class Counter:
  def __init__(self):
    self.count = 0
  def get(self):
    return self.count
  def incr(self, i=1):
    self.count += i
```

- No integer wrap-around in Python
- Some effects can't be written in pure Python (e.g., read-only attributes)

How to analyze multilanguage programs?

Type annotations

Rewrite into Python code

Drawbacks of the current approaches

How to analyze multilanguage programs?

Type annotations

Rewrite into Python code

Drawbacks of the current approaches

- Not the real code

How to analyze multilanguage programs?

Type annotations

Rewrite into Python code

Drawbacks of the current approaches

- Not the real code
- Not automatic: manual conversion

How to analyze multilanguage programs?

Type annotations

Rewrite into Python code

Drawbacks of the current approaches

- Not the real code
- Not automatic: manual conversion
- Not sound: some effects are not taken into account

How to analyze multilanguage programs?

Type annotations

Rewrite into Python code

Drawbacks of the current approaches

- Not the real code
- Not automatic: manual conversion
- Not sound: some effects are not taken into account

Our approach

How to analyze multilanguage programs?

Type annotations

Rewrite into Python code

Drawbacks of the current approaches

- Not the real code
- Not automatic: manual conversion
- Not sound: some effects are not taken into account

Our approach

- Analyze both the C and Python sources

How to analyze multilanguage programs?

Type annotations

Rewrite into Python code

Drawbacks of the current approaches

- Not the real code
- Not automatic: manual conversion
- Not sound: some effects are not taken into account

Our approach

- Analyze both the C and Python sources
- Switch from one language to the other just as the program does

How to analyze multilanguage programs?

Type annotations

Rewrite into Python code

Drawbacks of the current approaches

- Not the real code
- Not automatic: manual conversion
- Not sound: some effects are not taken into account

Our approach

- Analyze both the C and Python sources
- Switch from one language to the other just as the program does
- Reuse previous analyses of C and Python

How to analyze multilanguage programs?

Type annotations

Rewrite into Python code

Drawbacks of the current approaches

- Not the real code
- Not automatic: manual conversion
- Not sound: some effects are not taken into account

Our approach

- Analyze both the C and Python sources
- Switch from one language to the other just as the program does
- Reuse previous analyses of C and Python
- Detect runtime errors in Python, in C, and at the boundary

High-level idea

Difficulty: shared memory

- Two distinct visions of a shared state
- Synchronization? We could perform a full state translation, but
  - the cost would be high in the analysis
  - <u>some</u> abstractions can be shared between Python and C

High-level idea

Difficulty: shared memory

- Two distinct visions of a shared state
- Synchronization? We could perform a full state translation, but
  - the cost would be high in the analysis
  - <u>some</u> abstractions can be shared between Python and C

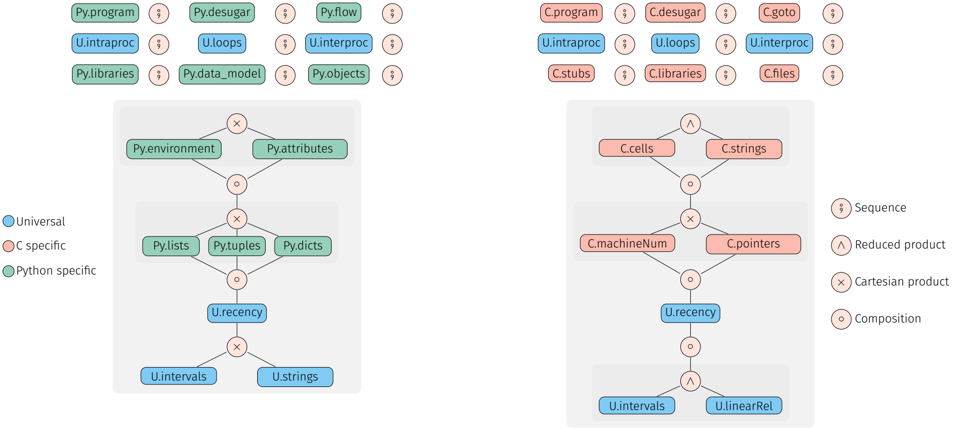
State separation $\leadsto$ reduced synchronization

- Observation: structures are directly dereferenceable by one language only
- Switch to other language otherwise (`c.incr()` $\leadsto$ `self->count += 1`)

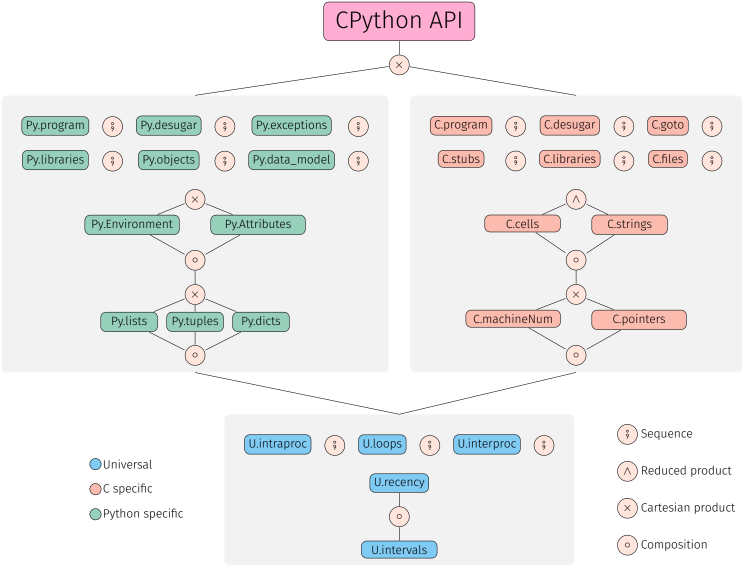
  Additional hypothesis: C accesses to Python objects through the API
- Synchronization: only when objects change language for the first time

Implementation & Experimental Evaluation

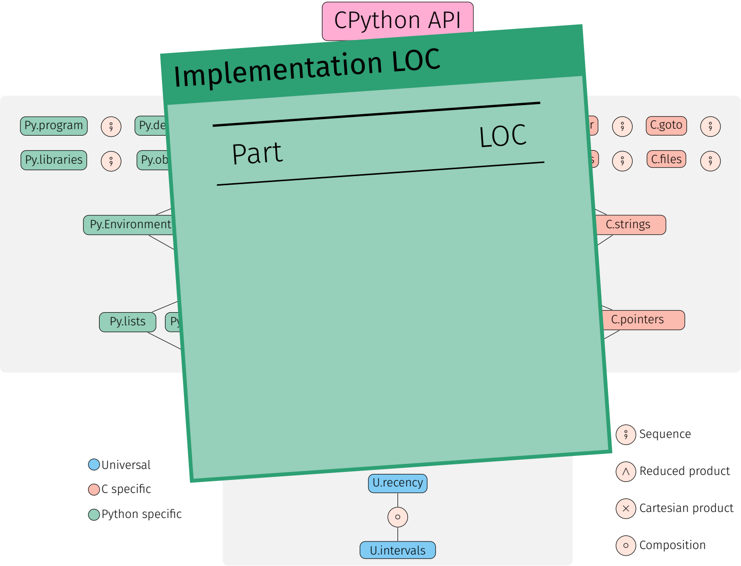
From distinct Python and C analyses...



... to a multilanguage analysis!



… to a multilanguage analysis!



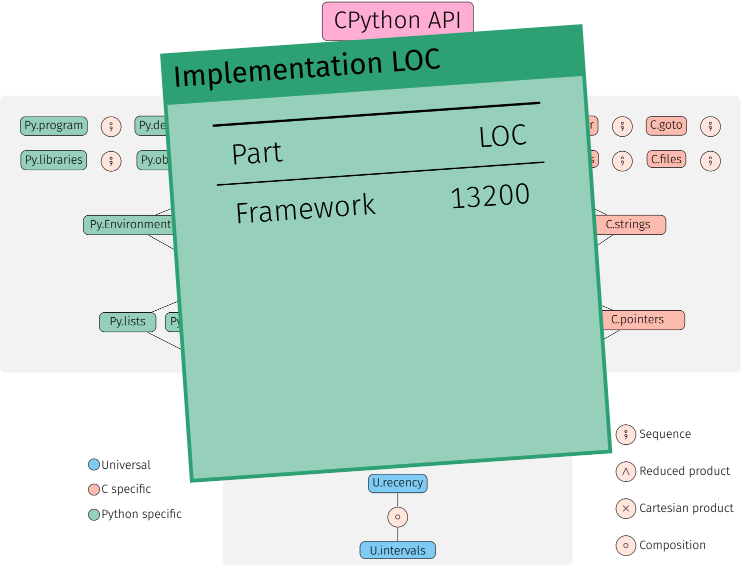
Implementation LOC

Part	LOC

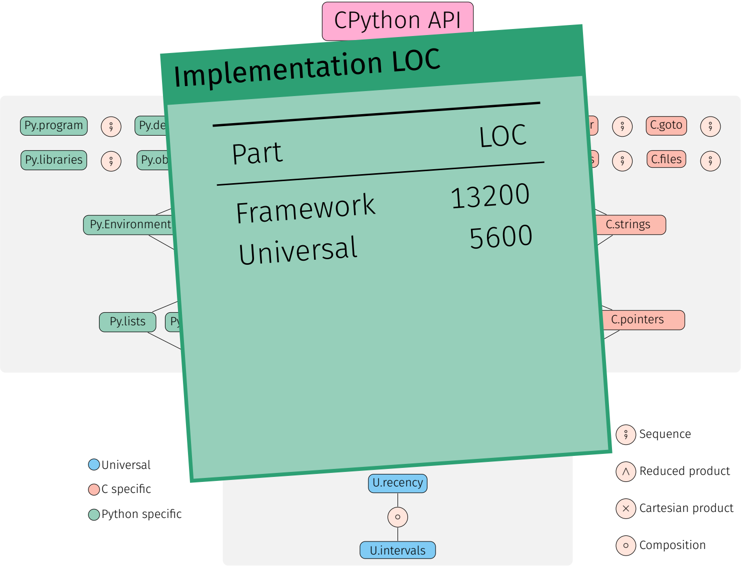
... to a multilanguage analysis!

Implementation LOC

Part	LOC
Framework	13200



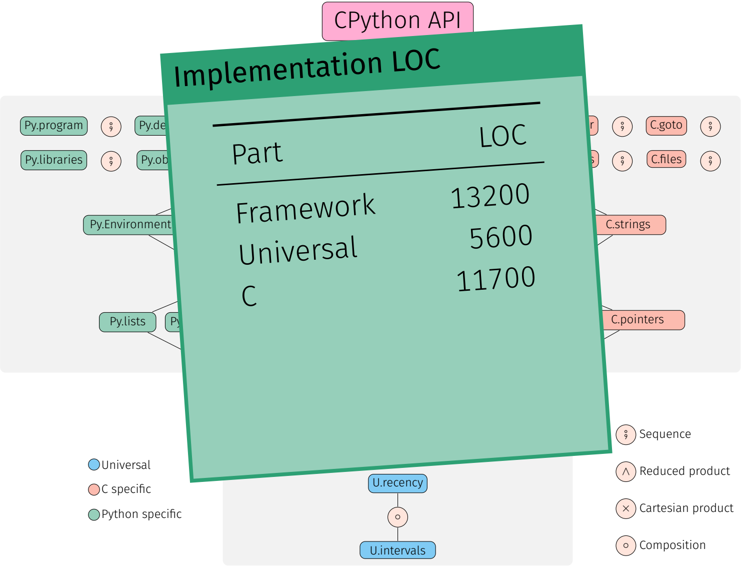
... to a multilanguage analysis!



Implementation LOC

Part	LOC
Framework	13200
Universal	5600

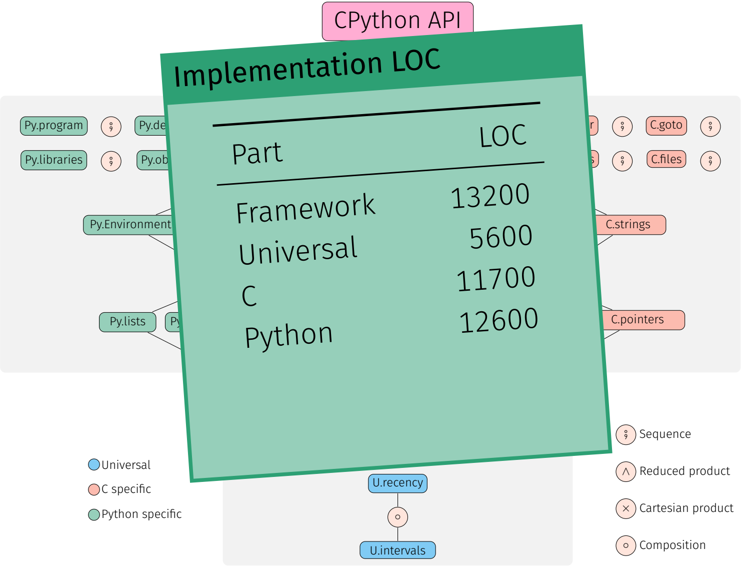
… to a multilanguage analysis!



Implementation LOC

Part	LOC
Framework	13200
Universal	5600
C	11700

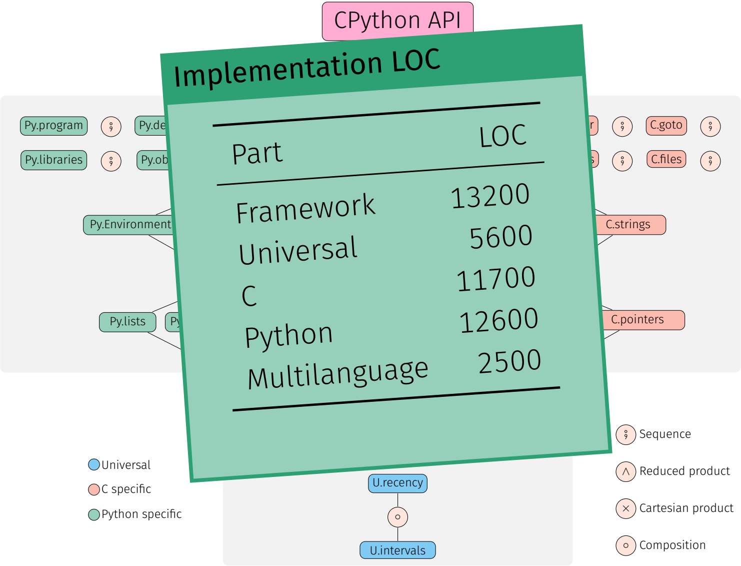
… to a multilanguage analysis!



Implementation LOC

Part	LOC
Framework	13200
Universal	5600
C	11700
Python	12600

… to a multilanguage analysis!



Implementation LOC

Part	LOC
Framework	13200
Universal	5600
C	11700
Python	12600
Multilanguage	2500

Benchmarks

Corpus selection

- Popular, real-world libraries available on GitHub, averaging 412 stars.
- Whole-program analysis: we use the tests provided by the libraries.

Library	C + Py. Loc	Tests	/test	$\frac{\text{\# proved checks}}{\text{\# checks}}$ %	# checks
`noise`	1397	15/15	1.2s	99.7%	6690
`cdistance`	2345	28/28	4.1s	98.0%	13716
`llist`	4515	167/194	1.5s	98.8%	36255
`ahocorasick`	4877	46/92	1.2s	96.7%	6722
`levenshtein`	5798	17/17	5.3s	84.6%	4825
`bitarray`	5841	159/216	1.6s	94.9%	25566

Conclusion

Conclusion

Difficulties

- Concrete semantics
- Memory interaction

Monat, Ouadjaout, and Miné. “A Multilanguage Static Analysis of Python Programs with Native C Extensions”. SAS 2021

Conclusion

Difficulties

- Concrete semantics
- Memory interaction

Previous works

- Type/exceptions analyses for the JNI
- No detection of runtime errors in C

Monat, Ouadjaout, and Miné. "A Multilanguage Static Analysis of Python Programs with Native C Extensions". SAS 2021

Conclusion

Difficulties

- Concrete semantics
- Memory interaction

Previous works

- Type/exceptions analyses for the JNI
- No detection of runtime errors in C

Results

- Careful separation of the states and modelization of the API
- Lightweight domain on top of off-the-shelf C and Python analyses
- Shared underlying abstractions (numeric, recency)
- Scale to small, real-world libraries (using client code)

Monat, Ouadjaout, and Miné. "A Multilanguage Static Analysis of Python Programs with Native C Extensions". SAS 2021

A Multilanguage Static Analysis of Python/C Programs with Mopsa

Questions

Raphaël Monat, Abdelraouf Ouadjaout, Antoine Miné

Dagstuhl
11 July 2023