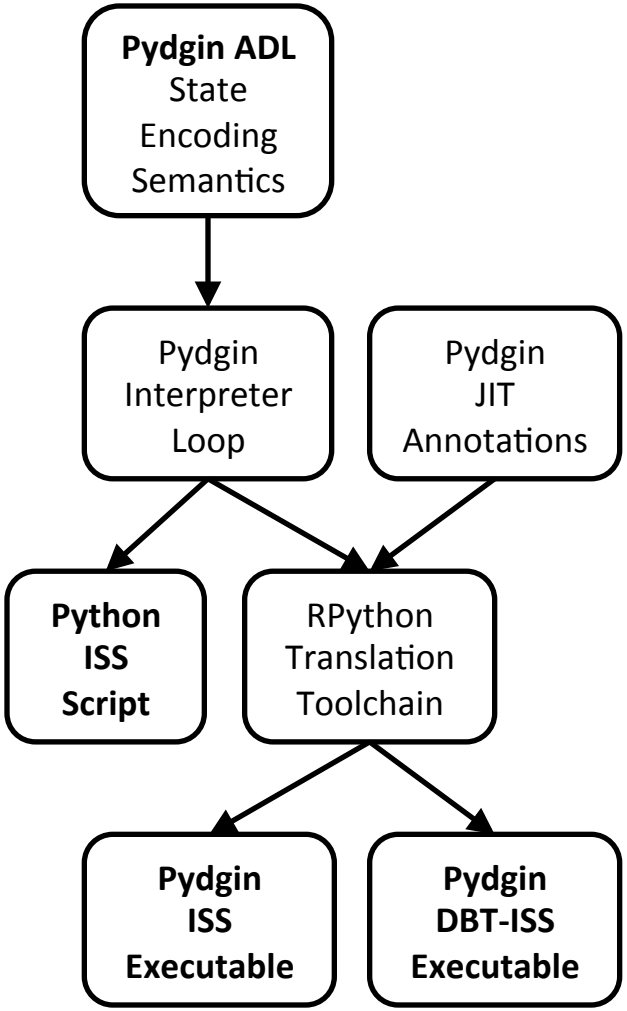
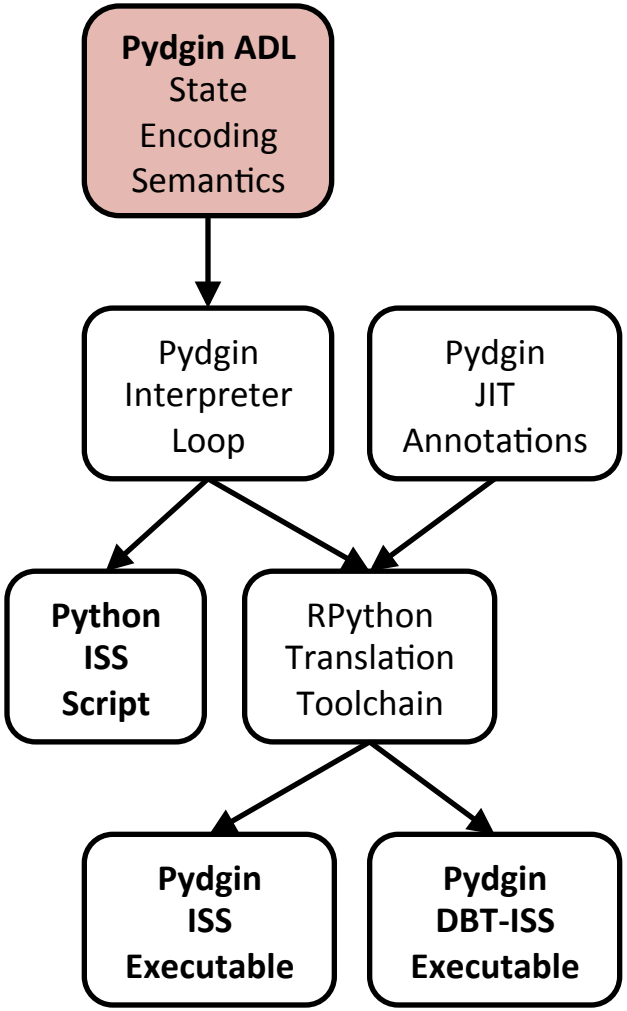
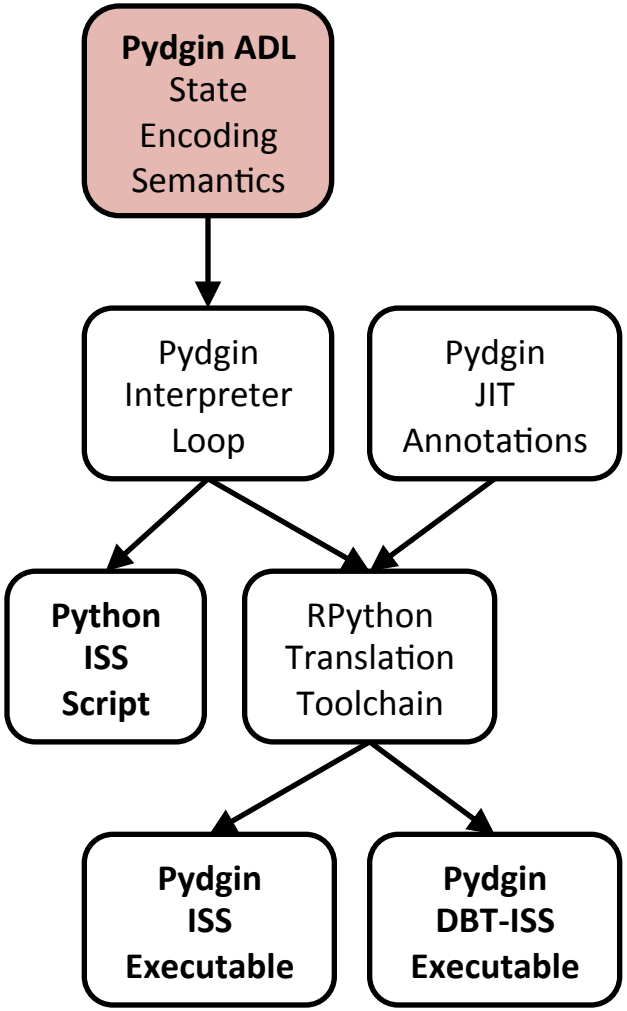
Pydgin Framework



Pydgin Framework

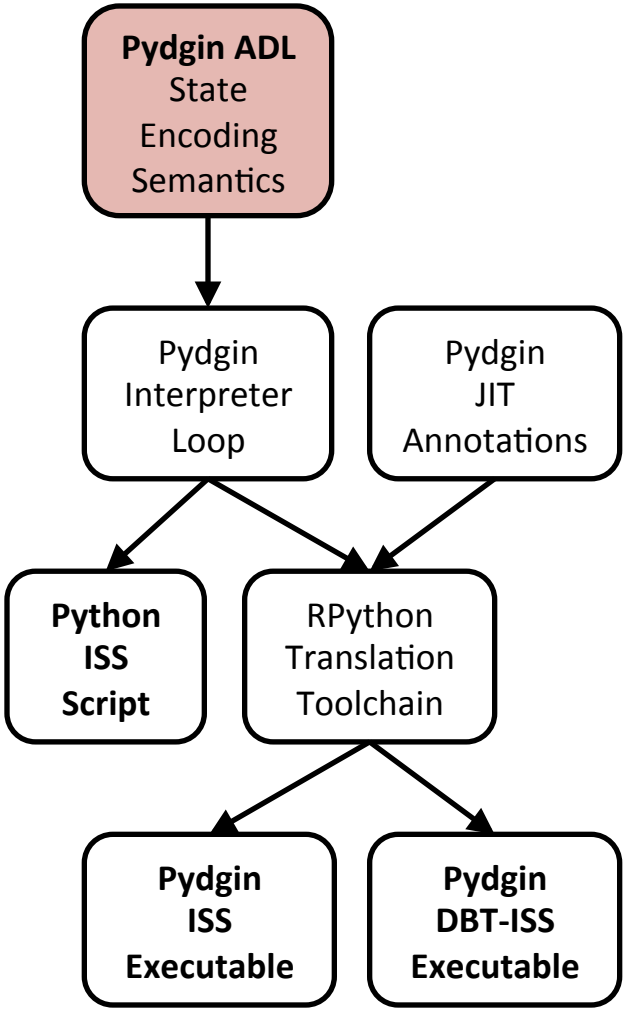


Pydgin ADL: ARMv5 Architectural State



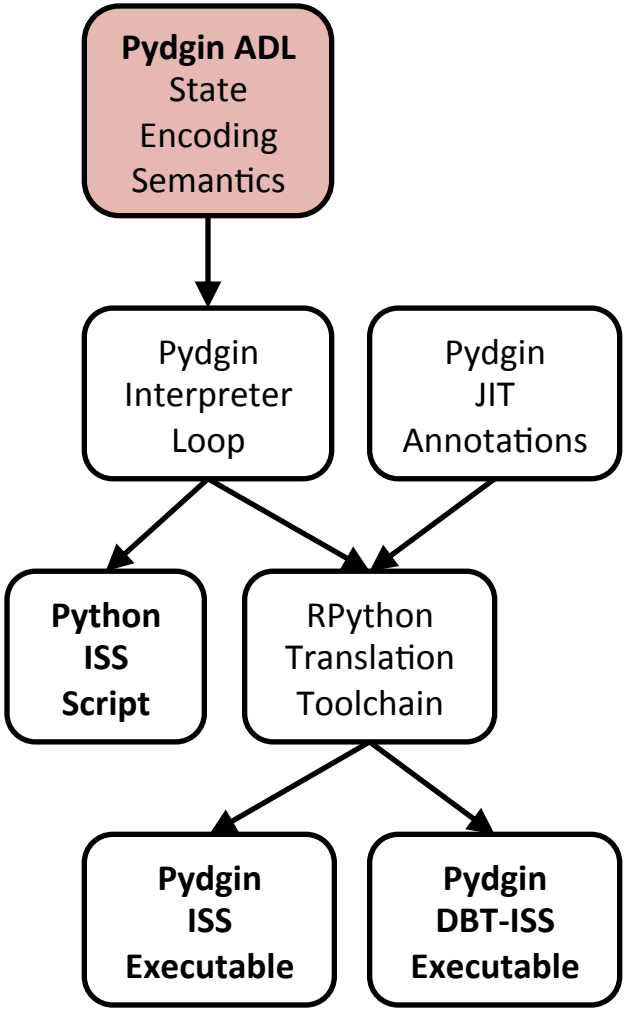

```
class State( object ):

  def __init__( self, memory, reset_addr=0x400 ):
    self.pc  = reset_addr
    self.rf  = ArmRegisterFile( self, num_regs=16 )
    self.mem = memory

    self.rf[ 15 ] = reset_addr

    # current program status register (CPSR)
    self.N    = 0b0      # Negative condition
    self.Z    = 0b0      # Zero condition
    self.C    = 0b0      # Carry condition
    self.V    = 0b0      # Overflow condition

  def fetch_pc( self ):
    return self.pc
```

Pydgin ADL: ARMv5 Encodings



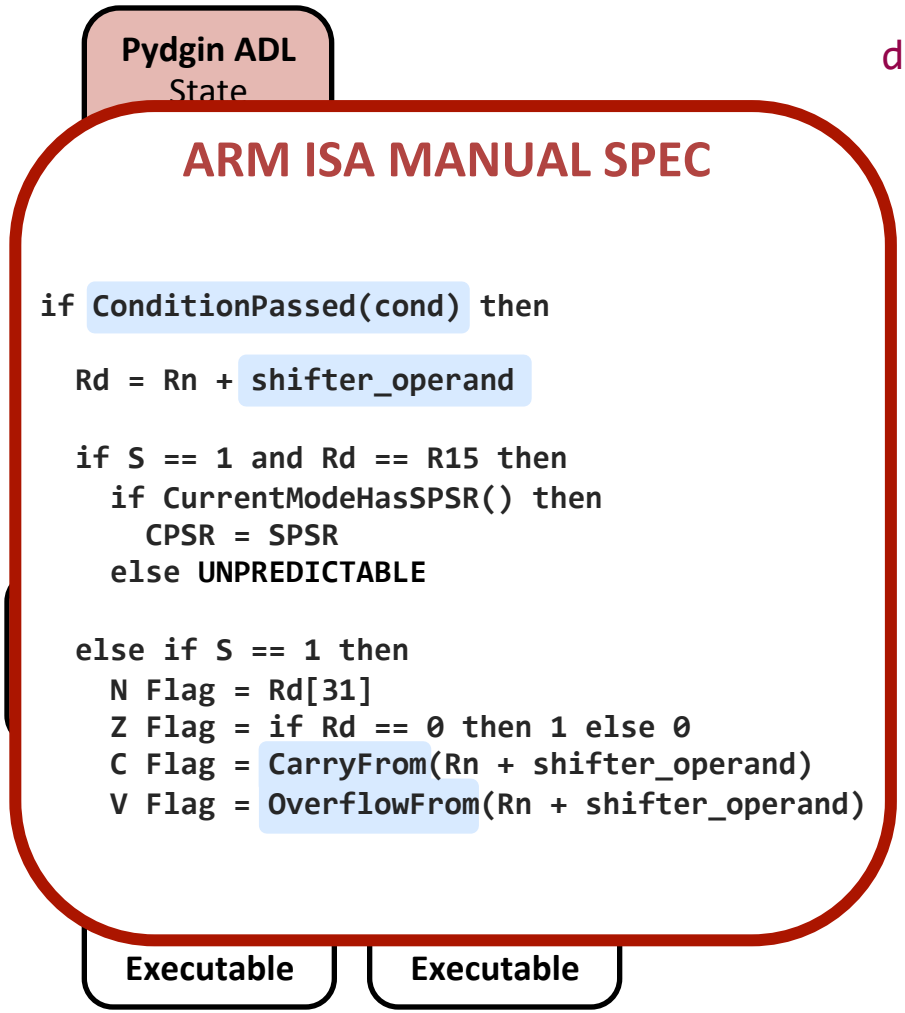

```
encodings = [

  ['nop',    '00000000000000000000000000000000'],
  ['mul',    'xxxx0000000xxxxxxxxxxxx1001xxxx'],
  ['umull',  'xxxx0000100xxxxxxxxxxxx1001xxxx'],
  ['adc',    'xxxx00x0101xxxxxxxxxxxxxxxxxxxx'],
  ['add',    'xxxx00x0100xxxxxxxxxxxxxxxxxxxx'],
  ['and',    'xxxx00x0000xxxxxxxxxxxxxxxxxxxx'],
  ['b',      'xxxx1010xxxxxxxxxxxxxxxxxxxxxxx'],
  ['bl',     'xxxx1011xxxxxxxxxxxxxxxxxxxxxxx'],
  ['bic',    'xxxx00x1110xxxxxxxxxxxxxxxxxxxx'],
  ['bkpt',   '111000010010xxxxxxxxxxxx0111xxxx'],

  # ...

  ['teq',    'xxxx00x10011xxxxxxxxxxxxxxxxxxx'],
  ['tst',    'xxxx00x10001xxxxxxxxxxxxxxxxxxx'],

]
```

Pydgin ADL: ARMv5 Instruction Semantics



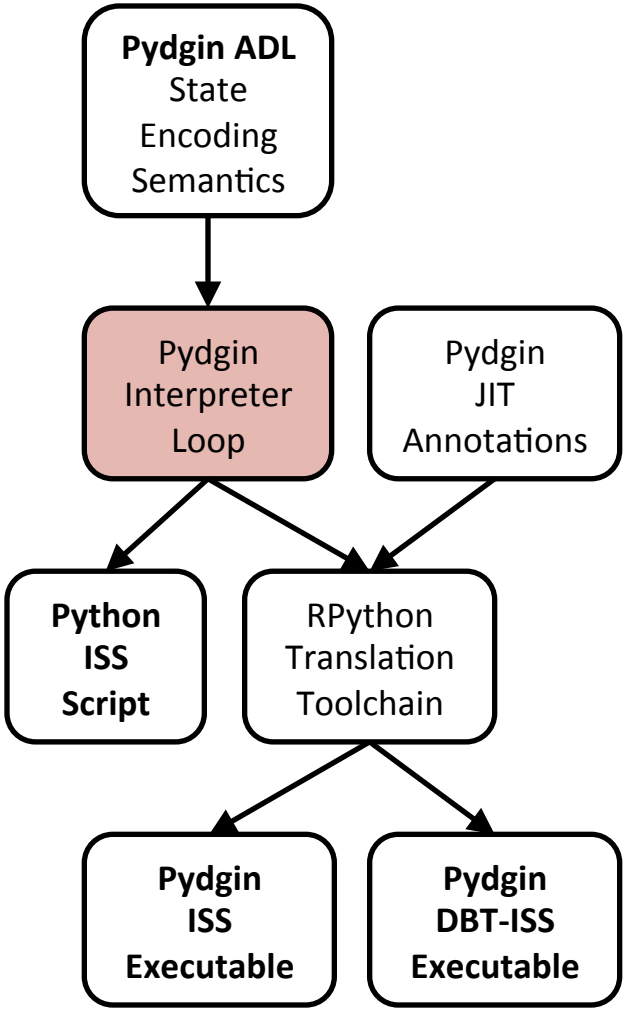

```
def execute_add( s, inst ):

  if condition_passed( s, inst.cond ):
    a,   = s.rf[ inst.rn ]
    b, _ = shifter_operand( s, inst )
    result = a + b
    s.rf[ inst.rd ] = trim_32(result)

    if inst.S:
      # ...
      s.N = (result >> 31)&1
      s.Z = trim_32(result) == 0
      s.C = carry_from(result)
      s.V = overflow_from(a, b, result)

    if inst.rd == 15:
      return
  s.rf[PC] = s.fetch_pc() + 4
```

Pydgin ADL: ARMv5 Instruction Semantics

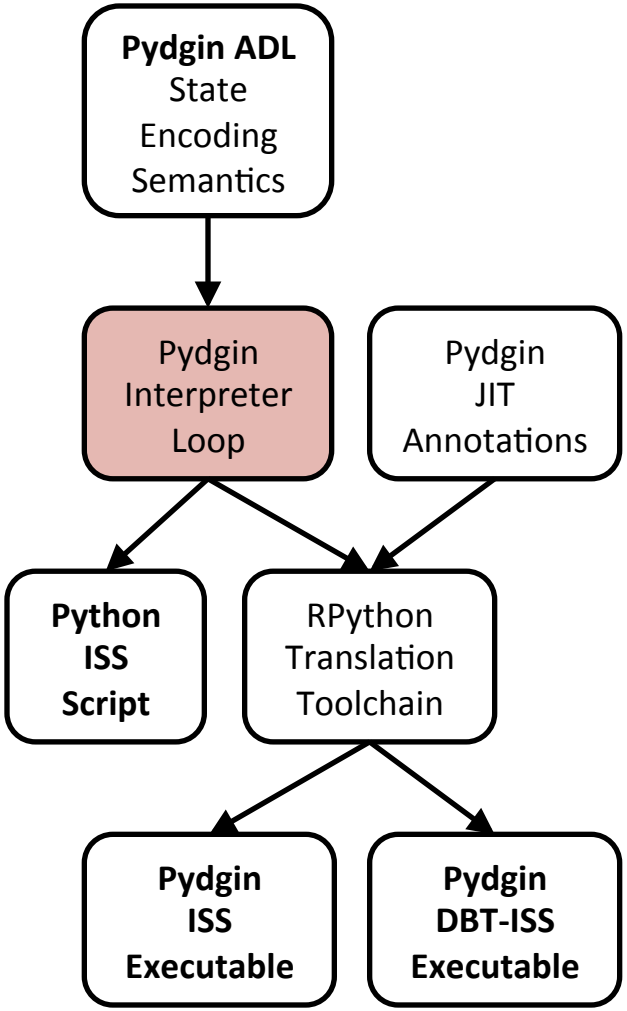



```python
def execute_add( s, inst ):

  if condition_passed( s, inst.cond ):
    a,   = s.rf[ inst.rn ]
    b, _ = shifter_operand( s, inst )
    result = a + b
    s.rf[ inst.rd ] = trim_32(result)

    if inst.S:
      # ...
      s.N = (result >> 31)&1
      s.Z = trim_32(result) == 0
      s.C = carry_from(result)
      s.V = overflow_from(a, b, result)

    if inst.rd == 15:
      return
  s.rf[PC] = s.fetch_pc() + 4
```

RPython ISS

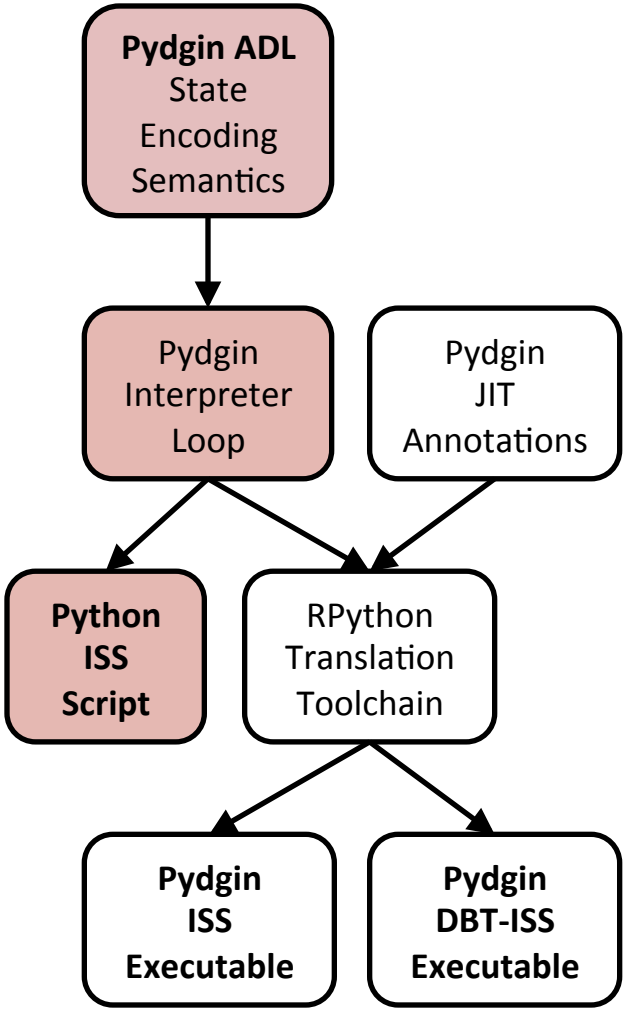

Pydgin ADL
State
Encoding
Semantics
Pydgin
Interpreter
Loop
Pydgin
JIT
Annotations
Python
ISS
Script
RPython
Translation
Toolchain
Pydgin
ISS
Executable
Pydgin
DBT-ISS
Executable

RPython ISS




```
def instruction_set_interpreter( memory ):
  state = State( memory )

  while True:


    pc      = state.fetch_pc()

    inst    = memory[ pc ]      # fetch
    execute = decode( inst )    # decode
    execute( state, inst )      # execute
```

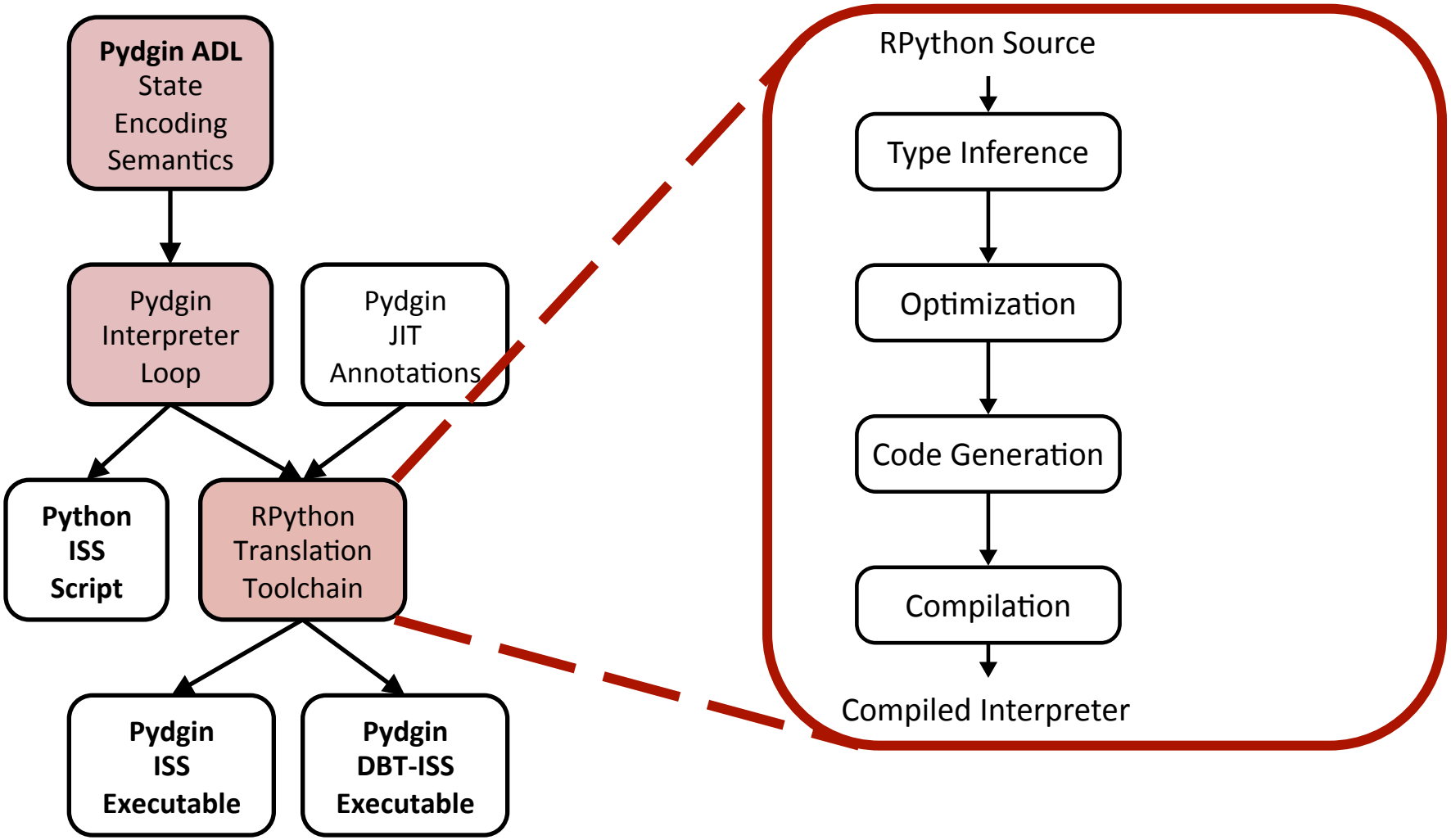
RPython ISS



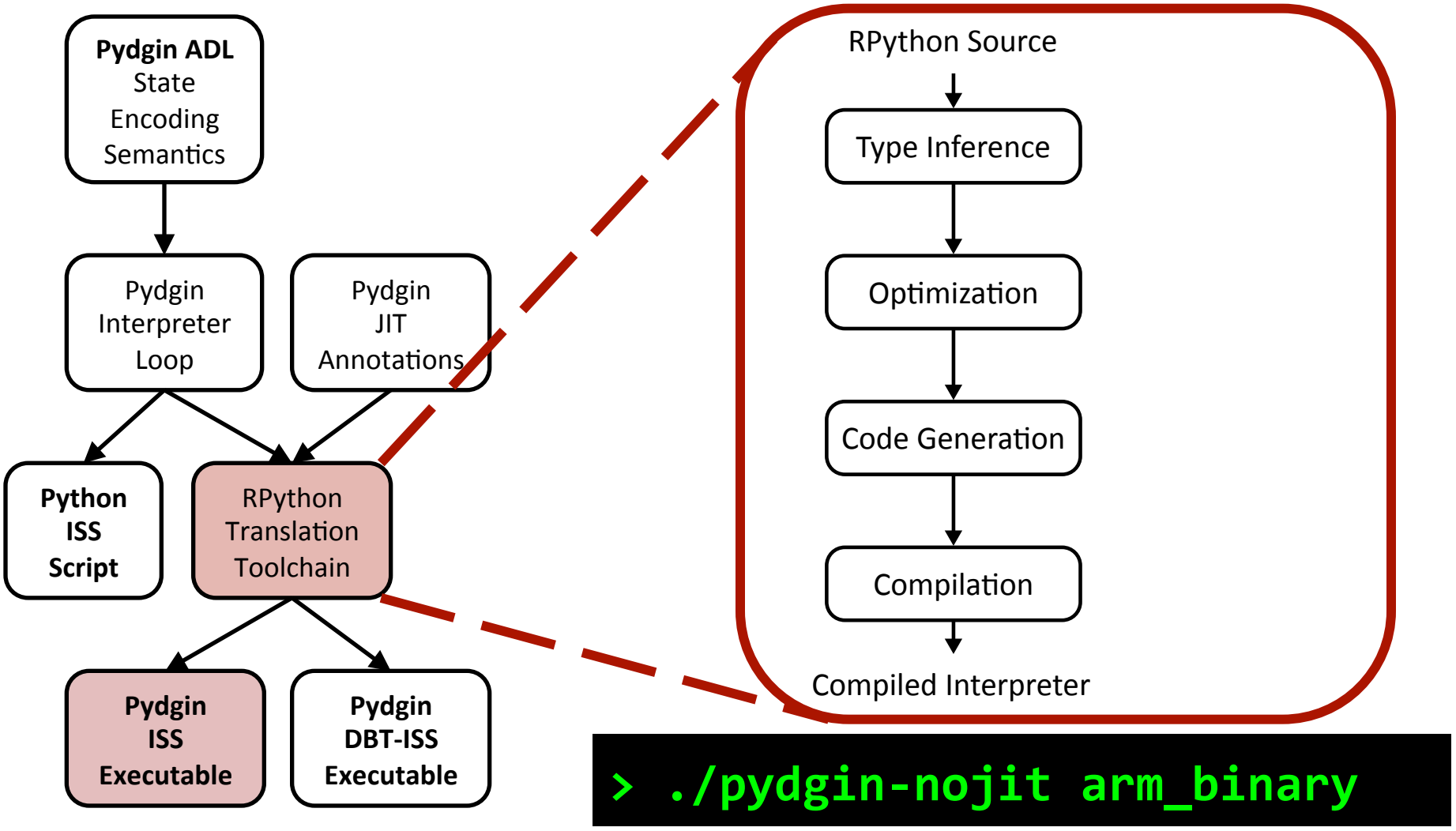

```
def instruction_set_interpreter( memory ):
  state = State( memory )

  while True:


    pc      = state.fetch_pc()

    inst    = memory[ pc ]      # fetch
    execute = decode( inst )    # decode
    execute( state, inst )      # execute
```

```
> python iss.py arm_binary
```

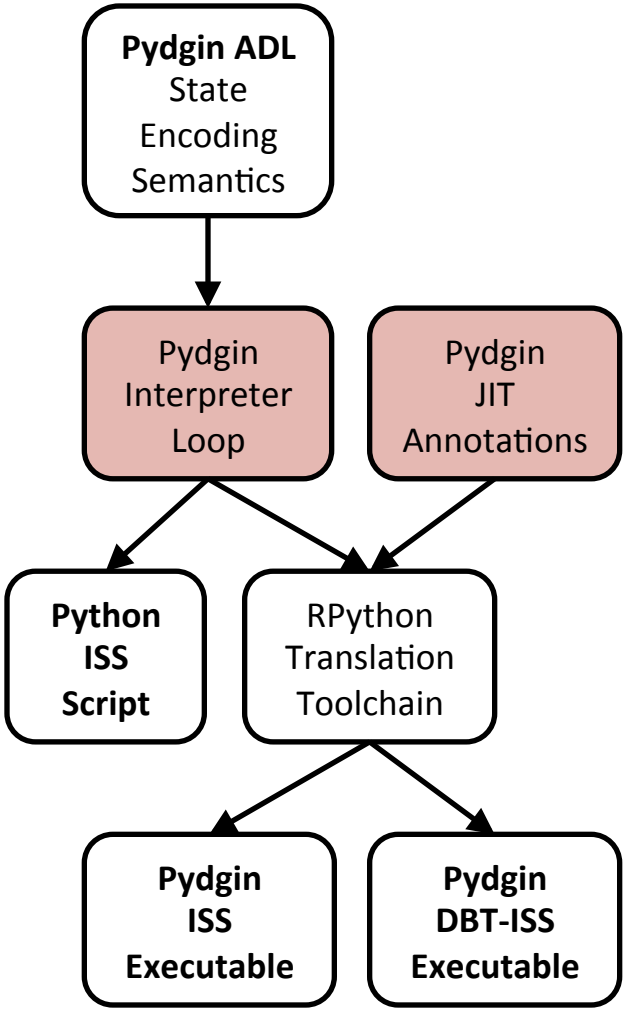
The RPython Translation Toolchain



The RPython Translation Toolchain

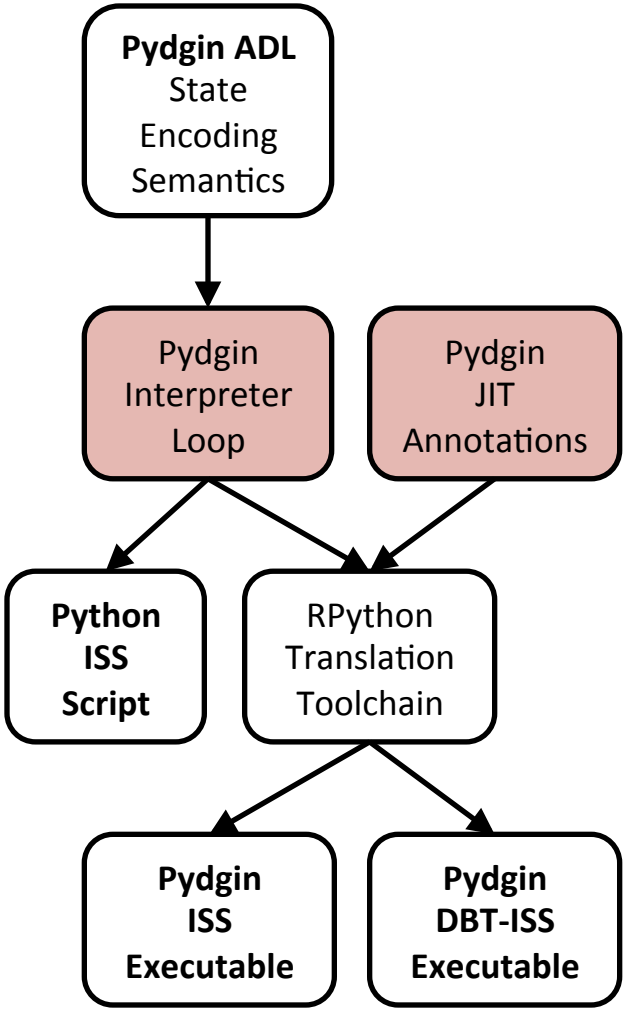


RPython ISS with JIT Annotations



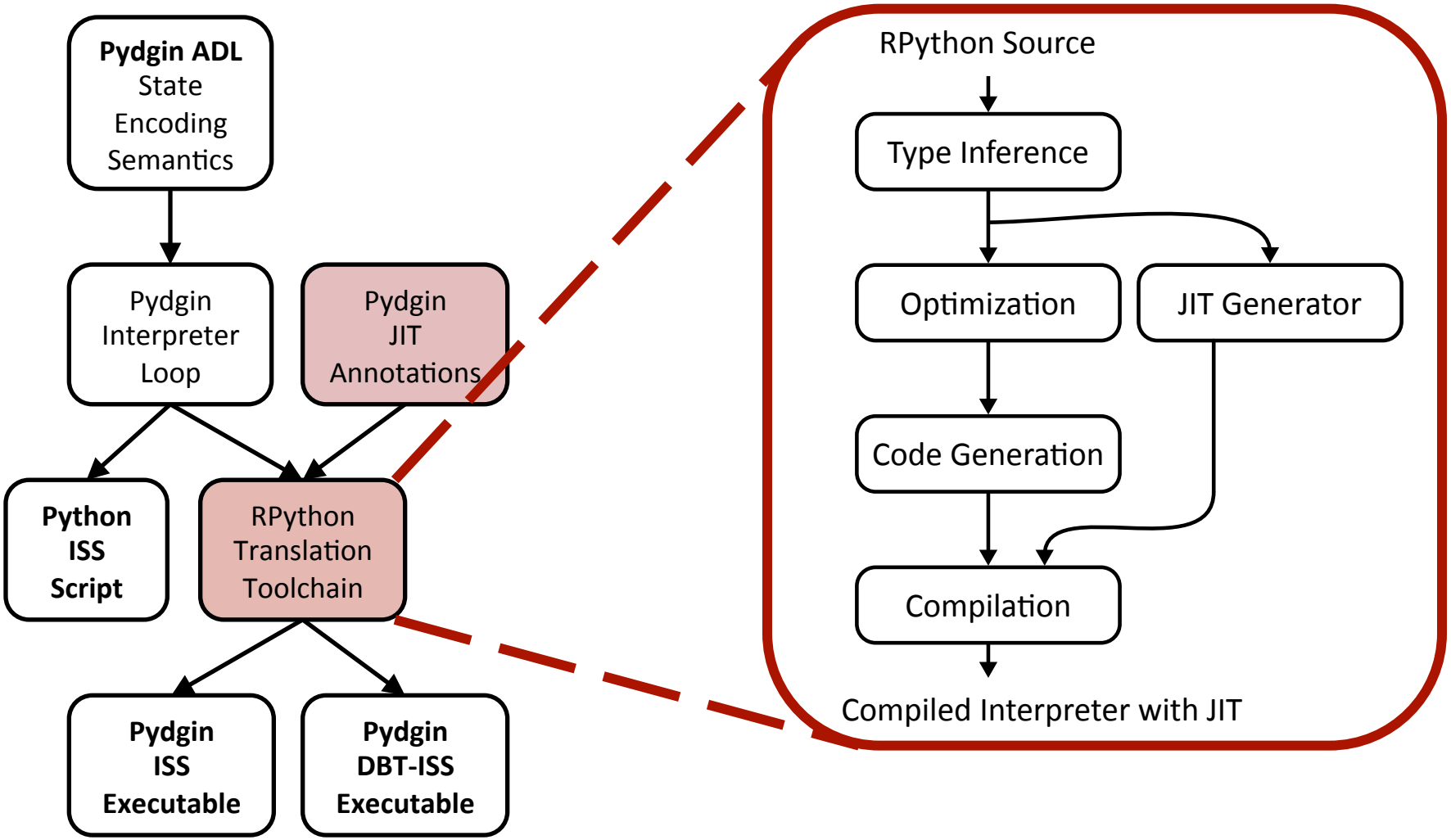

```
def instruction_set_interpreter( memory ):
  state = State( memory )

  while True:


    pc      = state.fetch_pc()

    inst    = memory[ pc ]      # fetch
    execute = decode( inst )    # decode
    execute( state, inst )      # execute
```

RPython ISS with JIT Annotations

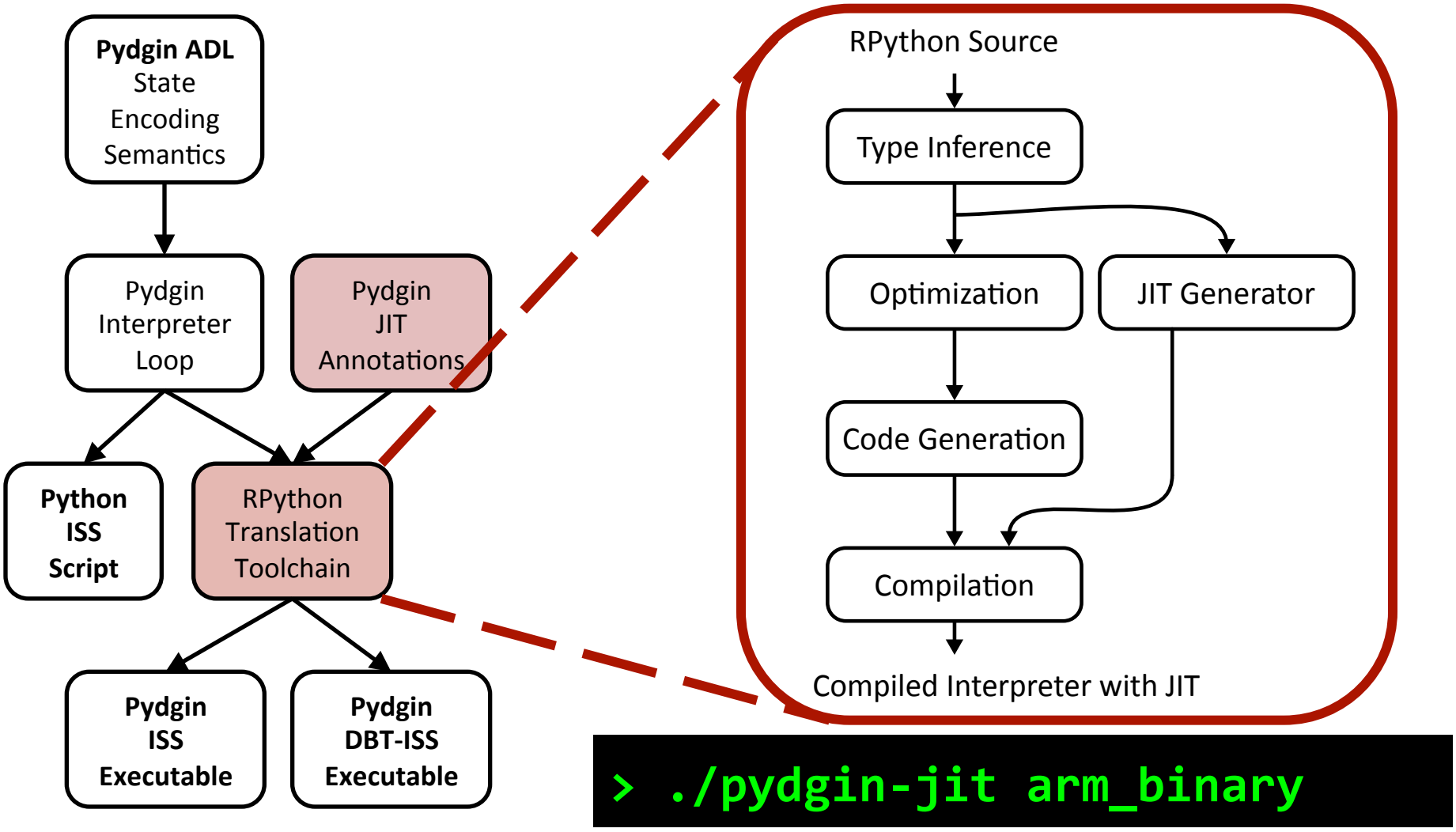



```
jd = JitDriver( greens = ['pc'],
                reds   = ['state'] )

def instruction_set_interpreter( memory ):
  state = State( memory )

  while True:
    jd.jit_merge_point( s.fetch_pc(), state )

    pc      = state.fetch_pc()

    inst    = memory[ pc ]      # fetch
    execute = decode( inst )    # decode
    execute( state, inst )      # execute

    if state.fetch_pc() < pc:
      jd.can_enter_jit( s.fetch_pc(), state )
```

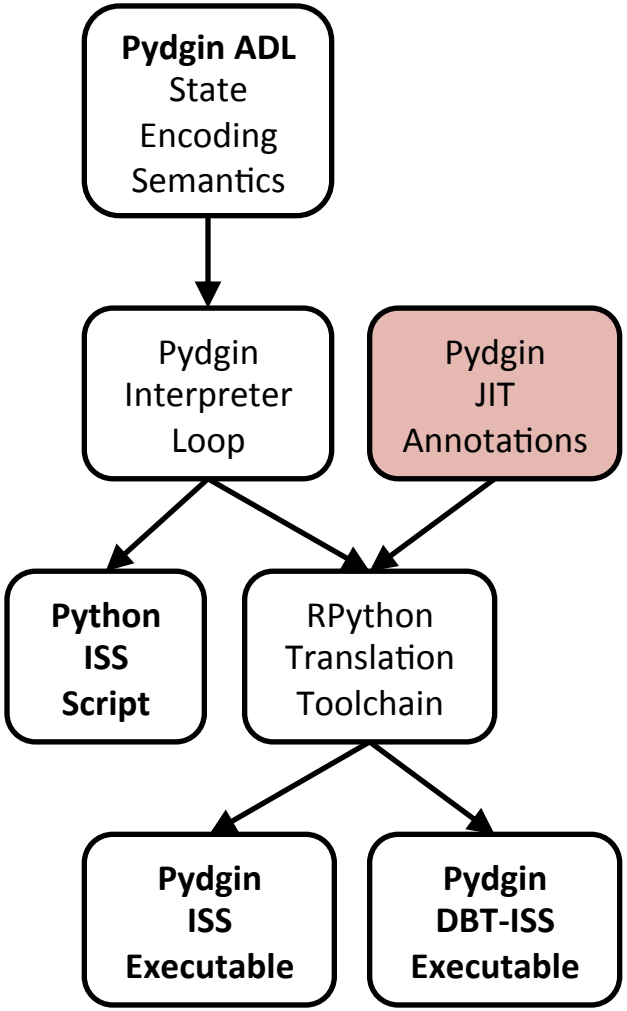
The RPython Translation Toolchain JIT Generator



The RPython Translation Toolchain JIT Generator

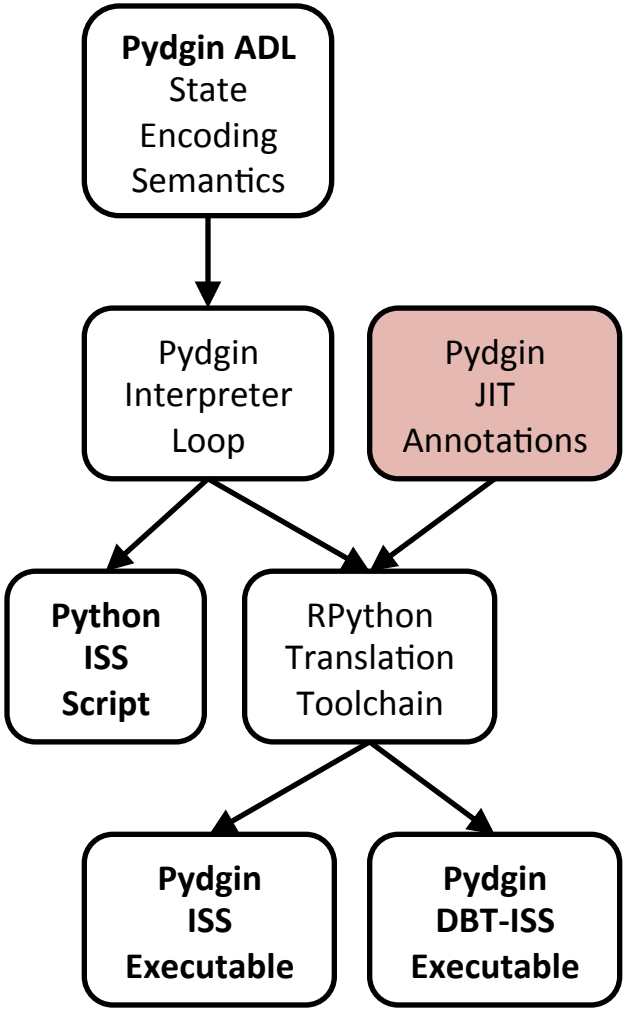


JIT Annotations



Creating a competitive JIT requires additional RPython JIT hints:

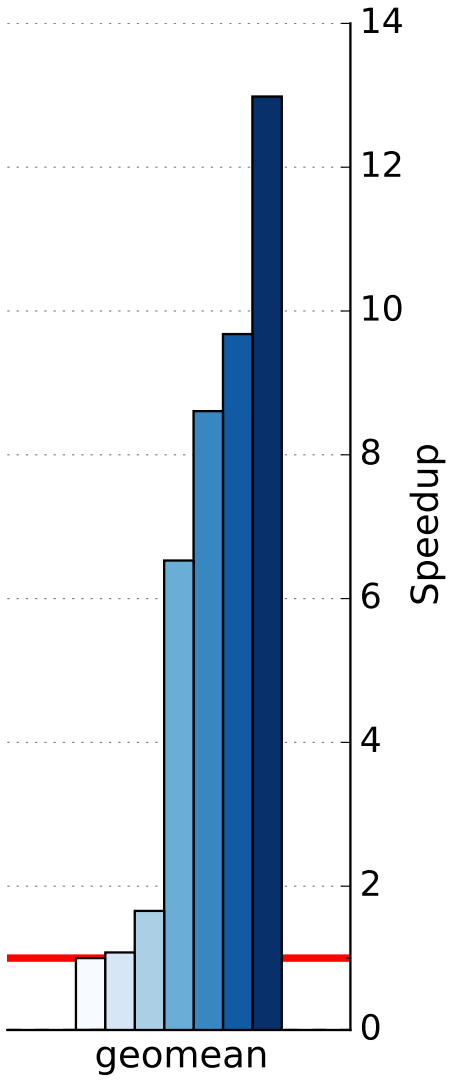
JIT Annotations



Creating a competitive JIT requires additional RPython JIT hints:

+ Minimal JIT Annotations
+ Elidable Instruction Fetch
+ Elidable Decode
+ Constant Promotion of PC and Memory
+ Word-Based Target Memory
+ Loop Unrolling in Instruction Semantics
+ Virtualizable PC and Statistics

JIT Annotations



Creating a competitive JIT requires additional RPython JIT hints:

+ Minimal JIT Annotations
+ Elidable Instruction Fetch
+ Elidable Decode
+ Constant Promotion of PC and Memory
+ Word-Based Target Memory
+ Loop Unrolling in Instruction Semantics
+ Virtualizable PC and Statistics

See our paper in ISPASS2015 for performance results!