

# Make FunBlocks alive

Marvin FOURASTIE

Master project

# Motivations



Educational purpose



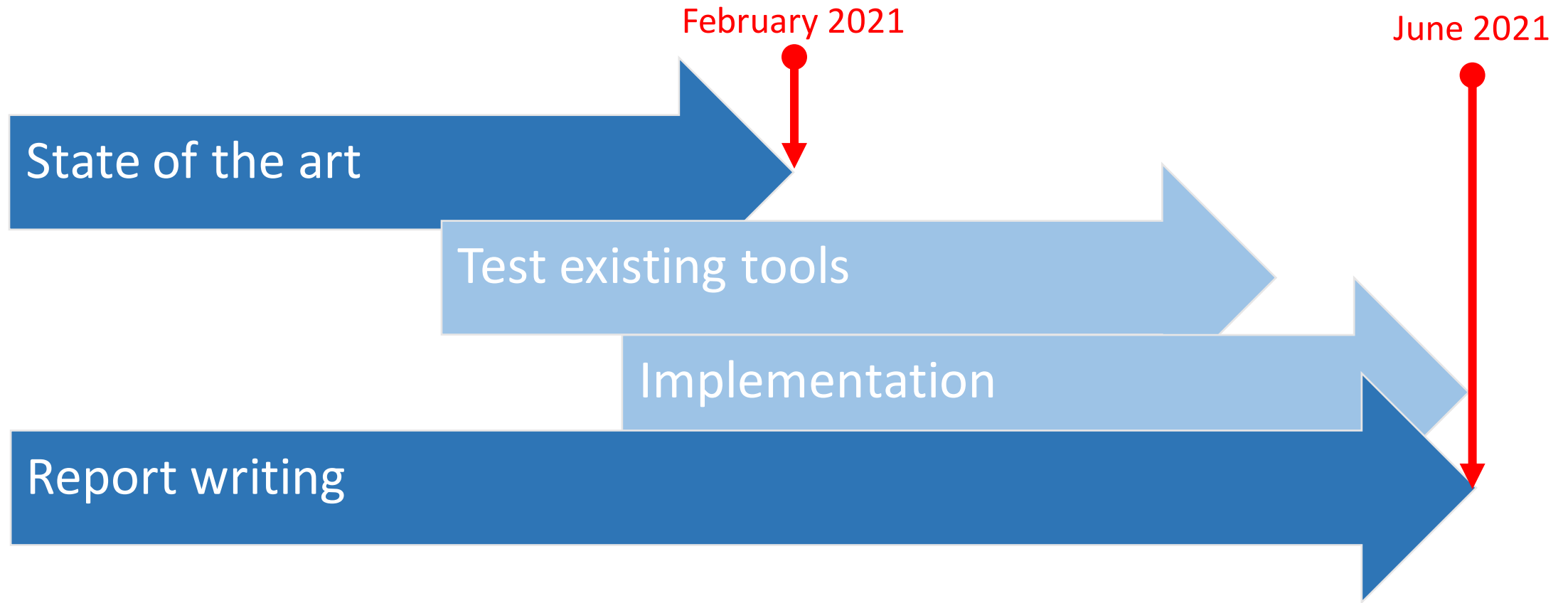
Imperative paradigm alternative



Based on rewrite systems

## FunBlocks

# Road Map



# FunBlocks

```
1  init area(disk(r))  
2  
3  case area(disk($d)) => mul(pi,square($d))
```

## PROGRAM STATE

area disk r

## RULES

▶ area disk < d > → mul pi square < d >

## PROGRAM STATE

mul pi square r

## RULES

▶ area disk < d > → mul pi square < d >

# FunBlocks

Declarative paradigm



```
area(disk(r))
```

Based on rewrite systems



```
case area(disk($d)) => mul(pi,square($d))
```

Static typing



```
type Tree $t :: empty | leaf $t | node (Tree $t) (Tree $t)
```

# Goals

Provide users with **valuable insights** about their program

→ Verification of rewrite systems

# Rewrite systems

## Stack operators

$\text{Zero} = \{0\}$

$\text{Nat} = \text{Zero} \cup \text{succ}(\text{Nat})$

$\text{Empty} = \Lambda$

$\text{Stack} = \text{Empty} \cup \text{push}(\text{Nat}, \text{Stack})$

$\text{top} : \text{Stack} \rightarrow \text{Nat}$

$\text{pop} : \text{Stack} \rightarrow \text{Stack}$

$\text{alternate} : \text{Stack} \times \text{Stack} \rightarrow \text{Stack}$

# Rewrite systems

## Canonical rewrite system

$\text{top}(\text{push}(x, y)) = x$

$\text{pop}(\text{push}(x, y)) = y$

$\text{alternate}(\Lambda, z) = z$

$\text{alternate}(\text{push}(x, y), z) = \text{push}(x, \text{alternate}(z, y))$



$\text{top}(\text{push}(x, y)) \rightarrow x$

$\text{pop}(\text{push}(x, y)) \rightarrow y$

$\text{alternate}(\Lambda, z) \rightarrow z$

$\text{alternate}(\text{push}(x, y), z) \rightarrow \text{push}(x, \text{alternate}(z, y))$



# Rewrite systems

Termination

Confluence

Soundness

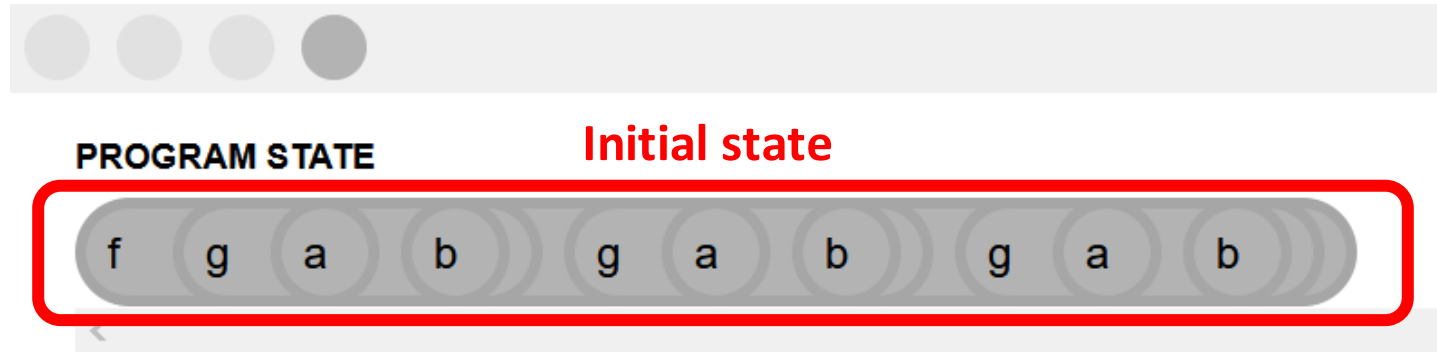
Completeness

Correctness

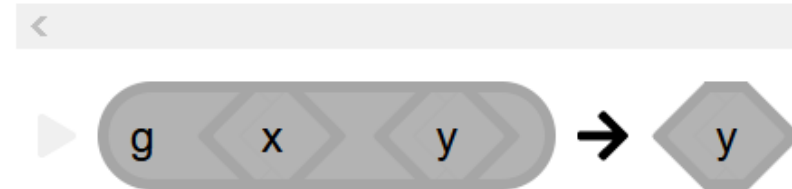
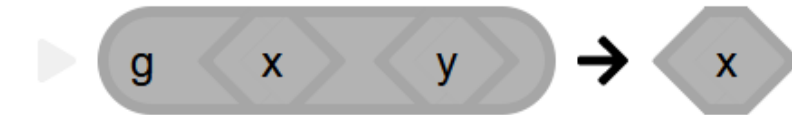
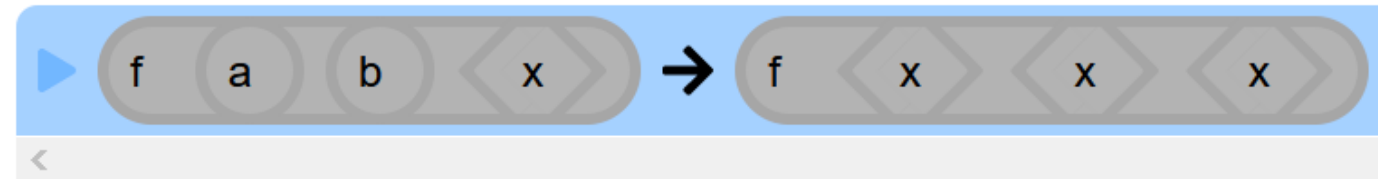


Undecidable in general

# Termination



## RULES



# Reduction order

Monotone



$s_i > t \rightarrow f(s_1, \dots, s_i, \dots, s_n) > f(s_1, \dots, t, \dots, s_n)$   
For  $f$  of arity  $n$

Close under substitution



$s > t \rightarrow \sigma s > \sigma t$ , for all substitution  $\sigma$

Well-founded



no infinite descending chain

$(\mathbb{N}, <)$  is well-founded

$(\mathbb{Z}, <)$  is not well-founded

# Termination

A term rewriting system is **terminating**

if and only if

it admits a **compatible reduction order**  $<$   
(if  $l > r$  for every rewrite rule  $l \rightarrow r$ )



Verification of termination

# Polynomial interpretation

$$f(a, x) \rightarrow x$$

$$f(g(x), y) \rightarrow g(f(x, y))$$

weight  
→

$$w(a) = 1$$

$$w(g(t)) = 1 + w(t)$$

$$w(f(t_1, t_2)) = 2w(t_1) + w(t_2)$$

# Polynomial interpretation

$$f(a, x) \rightarrow x$$

$$w(f(a, x)) = 2 + w(x)$$

$$w(x) = w(x)$$

$$w(f(a, x)) > w(x)$$

$$f(g(x), y) \rightarrow g(f(x, y))$$

$$w(f(g(x), y)) = 2 + 2w(x) + w(y)$$

$$w(g(f(x, y))) = 1 + 2w(x) + w(y)$$

$$w(f(g(x), y)) > w(g(f(x, y)))$$

Reduction order  $\rightarrow$  Termination

# Algorithms

Recursive Path Ordering



Order based on the mutisets

Knuth-Bendix Ordering



Based on weights assigned to operators

Dependency pairs



Prove innermost termination

# Termination

APROVE

=

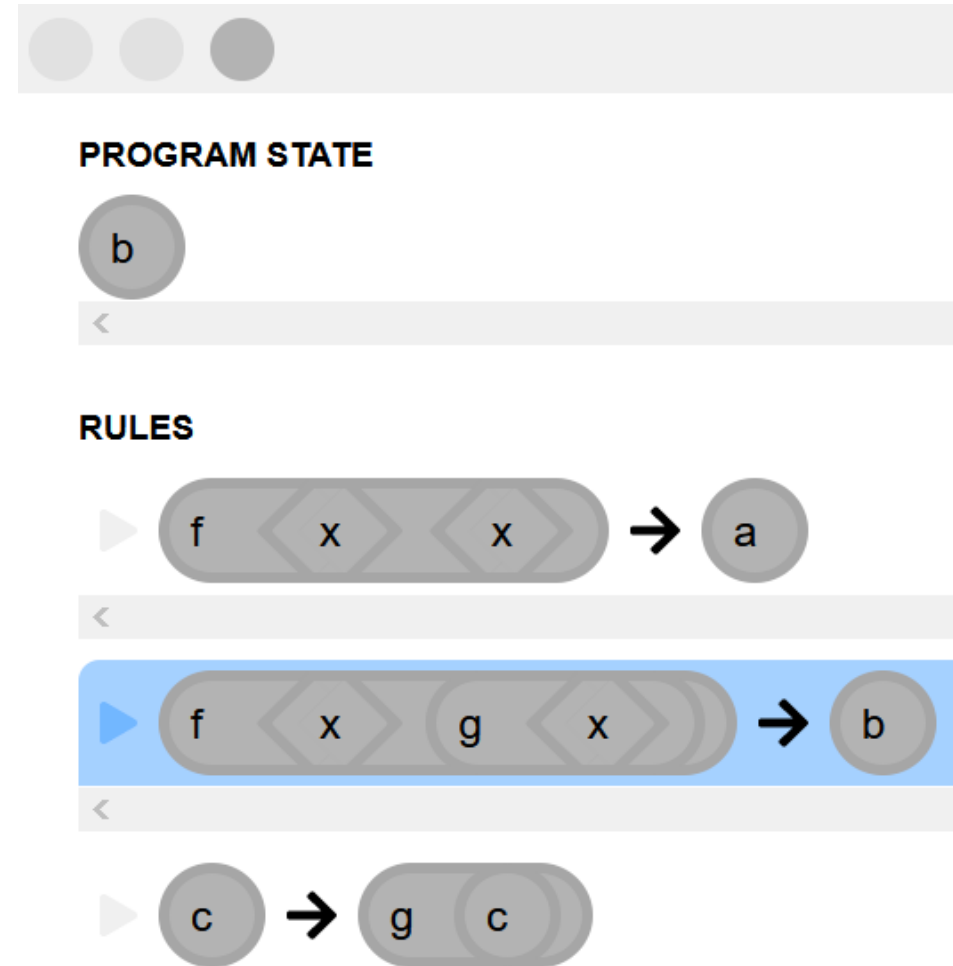
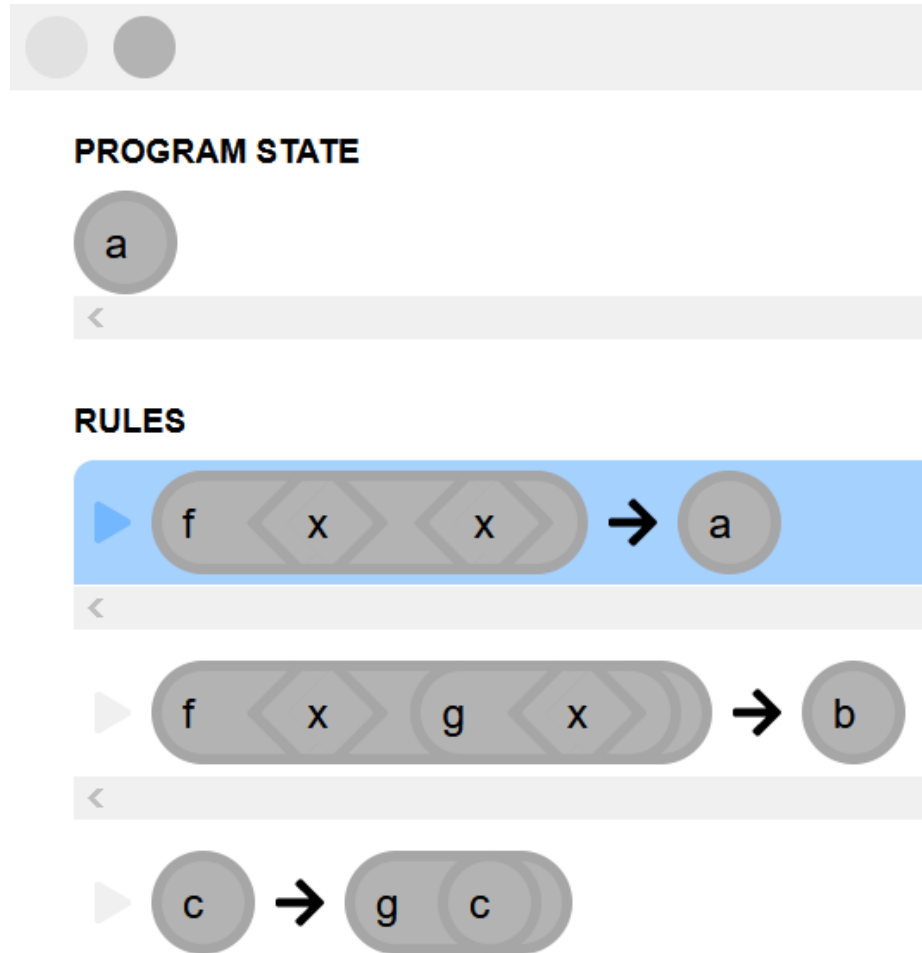
Direct proof  
(polynomial, LBO, KBO,...)

+

Dependency pairs and  
size-change principle



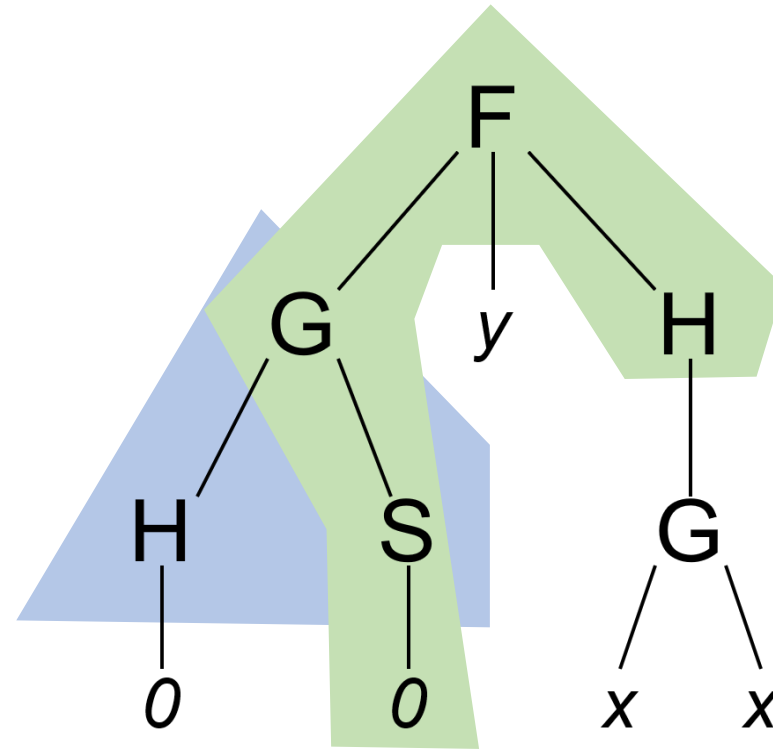
# Confluence



# Overlap and critical pairs

$$\rho_1 : F(G(x, S(0)), y, H(z)) \rightarrow x$$

$$\rho_2 : G(H(x), S(y)) \rightarrow y$$



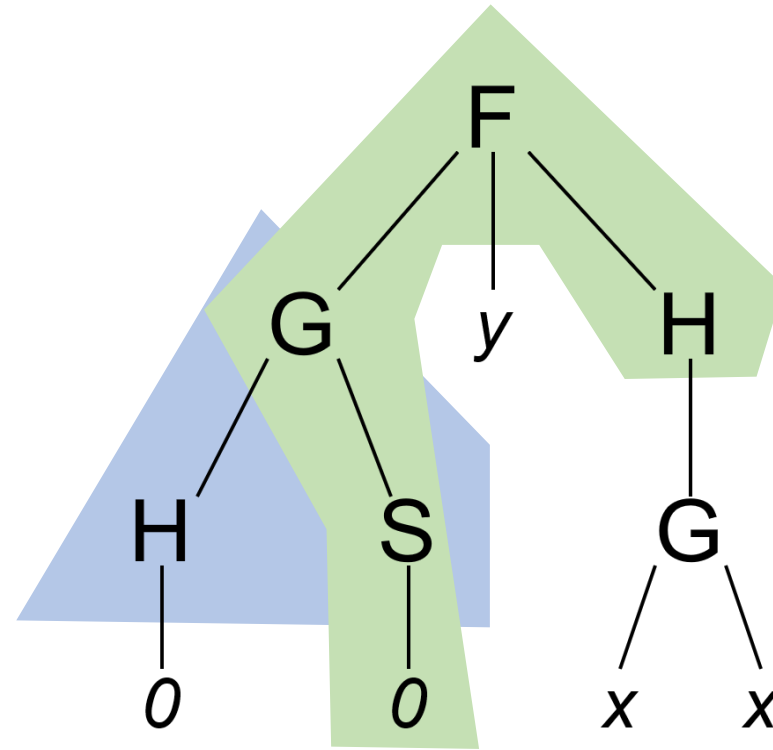
# Overlap and critical pairs

Overlapping:

Term:  $F(G(H(0), S(0)), y, H(z))$

$F(G(\square, S(0)), \square, H(\square))$

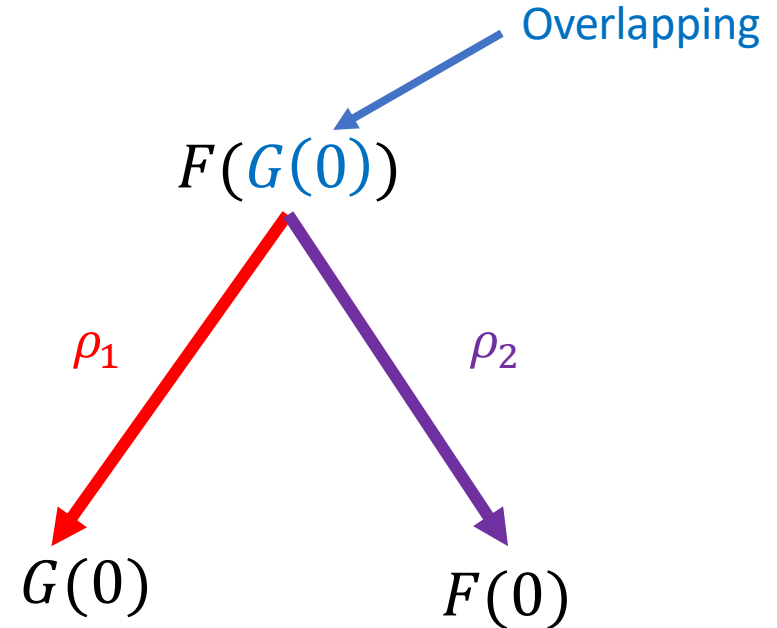
$G(H(\square), S(\square))$



# Overlap and critical pairs

$$\rho_1 : F(x) \rightarrow G(0)$$

$$\rho_2 : G(x) \rightarrow 0$$



$\langle G(x), F(x) \rangle$  is called **critical pair**

# Critical Pair Lemma

A terminating rewriting system is confluent

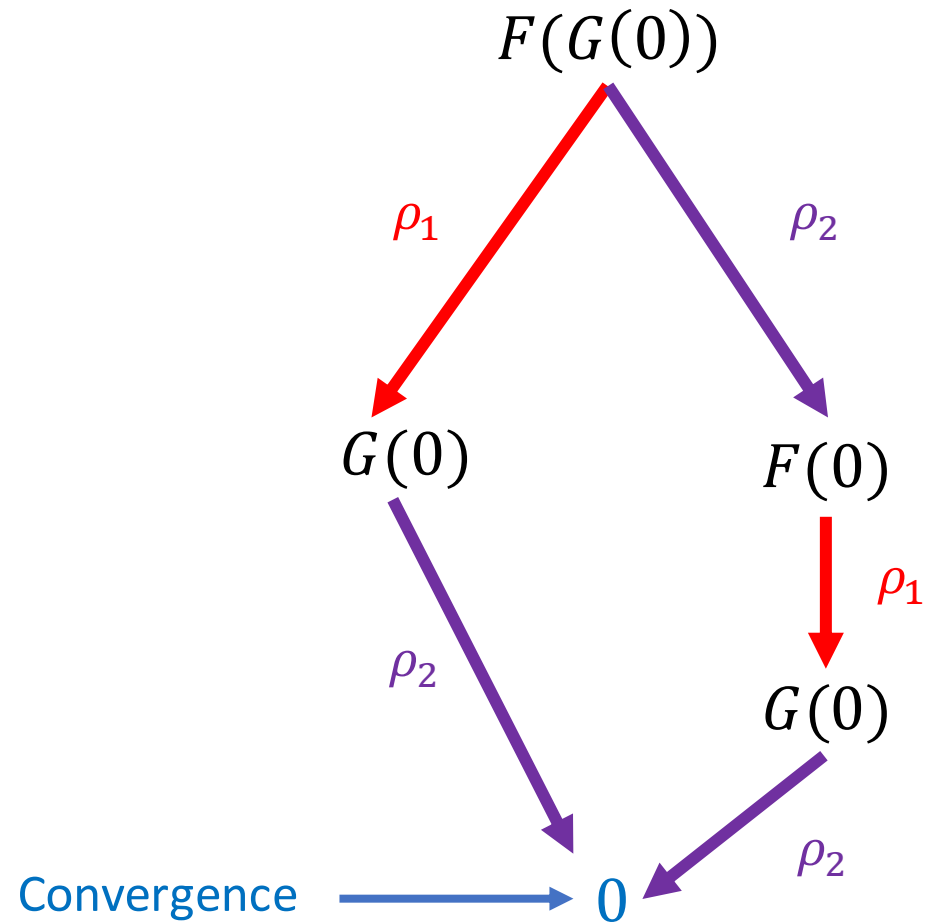
if and only if

all critical pairs are convergent

# Critical Pair Lemma

$$\rho_1 : F(x) \rightarrow G(0)$$

$$\rho_2 : G(x) \rightarrow 0$$



# Knuth-Bendix completion

Input:

A set of equation

A reduction ordering  $<$

$$1 \cdot x = x$$

$$x^{-1} \cdot x = 1$$

$$(x \cdot y) \cdot z = x \cdot (y \cdot z)$$

Non-confluent

# Knuth-Bendix completion

Output:

Terminate successfully



Terminating and confluent rewrite system

Loop indefinitely



Non-terminating rewrite system

Fail



Rule which cannot be ordered  
(i.e. commutative operator)



# Knuth-Bendix completion

Basic rules:

Orienting



Transform  $s = t$  to  $s \rightarrow t$

Adding



Add  $s = t$  in the set of equation

Simplifying



Simplify  $s = t$  in  $s' = t'$

Deleting



Delete trivial rules  $s = s$

# Knuth-Bendix completion

Adding



Add  $s = t$  in the set of equation

$$\begin{array}{lcl} (x * y) * z & \rightarrow & x * (y * z) \\ x * x & \rightarrow & x \end{array}$$



$$\begin{array}{c} (x * x) * z \\ \swarrow \quad \searrow \\ x * z \quad x * (x * z) \end{array}$$

No convergent

$$\begin{array}{lcl} (x * y) * z & \rightarrow & x * (y * z) \\ x * x & \rightarrow & x \\ x * (x * z) & \rightarrow & x * z \end{array}$$

New rule added

# Knuth-Bendix completion

Completion process:

1. For each equation  $s = t$  reduce  $s$  and  $t$  to normal form  $s'$  and  $t'$
2. Fill the set of rules using basic operators and reduction ordering
3. If the algorithm terminate successfully: terminating and confluent rewrite system

# Knuth-Bendix completion

Completion for axioms of groups:

$$\begin{array}{ll} 1 \cdot x & = x \\ x^{-1} \cdot x & = 1 \\ (x \cdot y) \cdot z & = x \cdot (y \cdot z) \end{array}$$



$$\begin{array}{ll} 1 \cdot x & \rightarrow x \\ x^{-1} \cdot x & \rightarrow 1 \\ (x \cdot y) \cdot z & \rightarrow x \cdot (y \cdot z) \\ x^{-1} \cdot (x \cdot y) & \rightarrow y \\ 1^{-1} & \rightarrow 1 \\ x \cdot 1 & \rightarrow x \\ (x^{-1})^{-1} & \rightarrow x \\ x \cdot x^{-1} & \rightarrow 1 \\ x \cdot (x^{-1} \cdot y) & \rightarrow y \\ (x \cdot y)^{-1} & \rightarrow y^{-1} x^{-1} \end{array}$$

# Educational tools

$T_T T_2 / \text{RS}^{\text{TOOL}}$

Termination

CSI

Confluence

KBCV

Completion

# TRS tool

Parcourir... Aucun fichier sélectionné.

Upload

```
(VAR x y)
(RULES
  f(x,y) -> x
  f(x,y) -> f(x,g(y))
  g(x) -> h(x)
  F(g(x),x) -> F(x,g(x))
  F(h(x),x) -> F(x,h(x))
)
(COMMENT Example 6 of \cite{AT97})
(COMMENT %% TagRevision: 1 %%)
(COMMENT %% Tags: [4ec3f85c01836]non_left_linear{};[4ec3f87f0f1e0]r
```

Go!

50



Rewrites Limit (Use with caution)

# TRS tool

$R_0 = f(x, y) \rightarrow x$
$R_0$ is Left-Linear
$R_0$ is Right-Linear
$R_0$ is Linear
$R_0$ is Collapsing
$R_0$ is not Duplicating
$R_0$ is not Conservative
$R_0$ is Destructive

TRS
The TRS is not Left-Linear
The TRS is not Right-Linear
The TRS is not Linear
The TRS is Collapsing
The TRS is not Duplicating
The TRS is not Conservative
The TRS is Destructive
The TRS is not Orthogonal
The TRS is not Almost Orthogonal
The TRS is not Weakly Orthogonal
The TRS is Locally Confluent
Unknown confluence for The TRS
The TRS is non terminating Infinite Loop: $f(x, g(y)) \rightarrow \underline{f(x, g(g(y)))}$

# TTT2

## Tyrolean Termination Tool 2 (1.20)

### 1. Input Term Rewrite System

For input use the **standard TRS format**.

select example ...

or upload file

Parcourir...

Aucun fichier sélectionné.

```
(VAR x y)
(RULES
  add(0,y) -> y
  add(s(x),y) -> s(add(x,y))
  mul(0,y) -> 0
  mul(s(x),y) -> add(y,mul(x,y))
)
```

### 2. Select Strategy

☒ FAST ☐ FBI ☐ HYDRA ☐ LPO ☐ KBO ☐ POLY ☐ MAT(2) ☐ MAT(3) ☐ COMP ☐ COMPLEXITY  
☐ EXPERT

### 3. Encode State into URL (optional)

encode URL clear URL

### 4. Start TTT2

check ☐ use HTML output if available (*experimental feature*)



# CSI

Enter a **TRS** or **HRS** or upload a file

[browse...](#)

Examples:

[trs1](#)

[trs2](#)

[hrs1](#)

[hrs2](#)



CSI 0.1

CSI 0.6

CSI 1.1

CSI 1.1✓

UNR

UNC

CR

CSI 1.2.4

CSI 1.2.4✓

CSI^ho

[encode URL](#)

[clear URL](#)

[reset](#)

[submit](#)

# KBCV

Orient →

Orient ←

Simplify

Delete

Compose

Collapse

Deduce

Completion

Undo

Redo

Equations

from 1 to 500

1.  $f(f(x, y), z) \approx f(x, f(y, z))$

2.  $f(x, c) \approx x$

3.  $f(x, g(x)) \approx c$

Rules

from 1 to 500

LPO Precedence

Undo / Redo Stack

1. start : Welcome to the 'Knuth-Bendix Completion Visualizer'!

2. add : equations  $f(f(x,y),z)=f(x,f(y,z))$ ,  $f(x,c)=x$ ,  $f(x,g(x))=c$  were added

Status Messages

Welcome to the 'Knuth-Bendix Completion Visualizer'!

equations  $f(f(x,y),z)=f(x,f(y,z))$ ,  $f(x,c)=x$ ,  $f(x,g(x))=c$  were added

file '.kbcvinit' loaded!

# Performance tools

Termination

MU-TERM

NaTT

**APROVE**

Confluence

ACP

Saigawa

Completion

**Maxcomp**

Proof verification

**CoLoR**

**CeTA**

# Hybrid tools

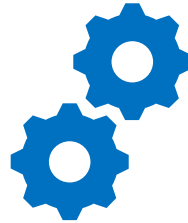


**MoudE3**

# CiME



Rewriting toolkit

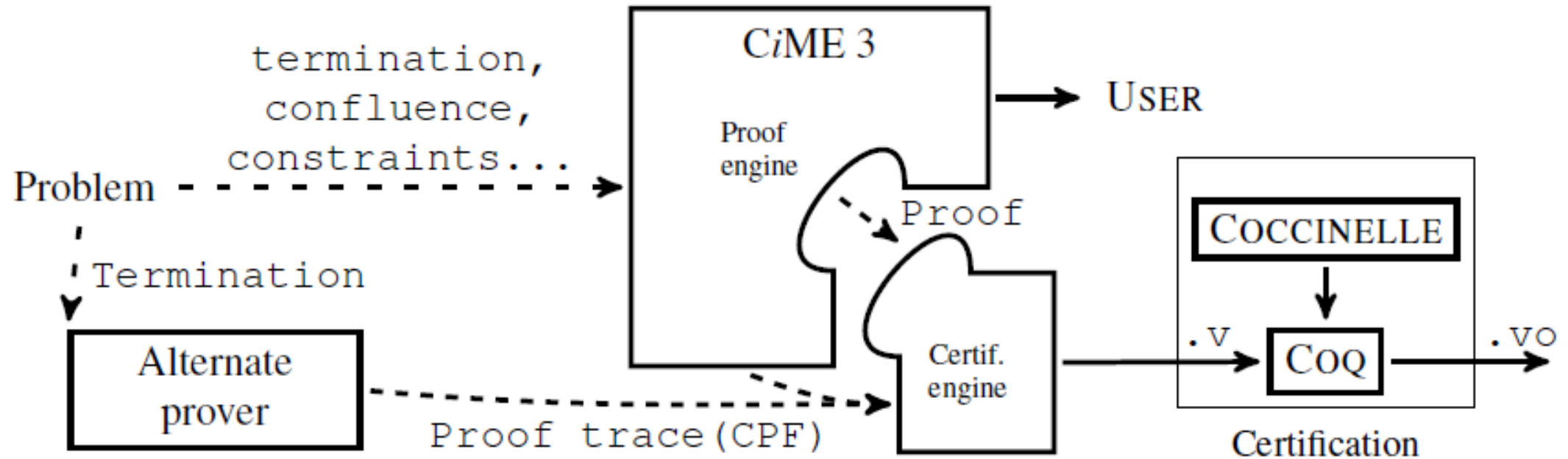


Proof engine



Proof certification

# CiME



# CiME

## Examples of declarations

```
let X = variables "x,y";  
  
let F = signature "plus : binary; 0:constant; S:unary;";  
  
let T = algebra F;  
  
let t1 = term T "S(0)";  
  
let R = trs T "plus(0,x) -> x; plus(S x, y) -> S(plus(x,y));";  
  
let c = order_constraints T "0 < S(0) /\ S(plus(x,y)) < plus(S(x),y)";
```

# CiME

## Definition of signatures

```
CiME> let F_peano = signature "  
    0 : constant; s : unary; +,* : infix binary;  
    ";
```

```
F_peano : signature = signature "* : 2; s : 1; + : 2; 0 : 0"
```

```
CiME>let X = variables "x,y,z";
```

```
X : variable_set = variables "z,x,y"
```



# CiME

## Definition of algebra and terms

```
CiME> let A_peano = algebra F_peano ;  
  
A_peano : F_peano algebra = algebra F_peano
```

```
CiME> let t = term A_peano "s(s(s(0)))*(s(0)+s(s(0)))";  
  
t : F_peano term = s(s(s(0))) * (s(0)+s(s(0)))
```

# CiME

## Term rewriting system

```
CiME> let R_peano = trs A_peano "  
  x+0 -> x;  
  x+s(y) -> s(x+y);  
  x*0 -> 0;  
  x*s(y) -> (x*y)+x;  
  ";  
  
R_peano : F_peano trs = trs A_peano "  
  x+0 -> x;  
  x+s(y) -> s(x+y);  
  x *0 -> 0;  
  x *s(y) -> (x *y)+x  "
```

```
CiME> termination R_peano;  
  
CiME> coq_certify_proof R_peano;  
  
CiME> convergence R_peano ;  
  
...
```

# Maude

## MoudE3



Simplicity



Expressiveness



Performance

# Maude

```
1  fmod BASIC-NAT is
2      sort Nat .
3
4      op 0 : -> Nat .
5      op s : Nat -> Nat .
6      op _+_ : Nat Nat -> Nat .
7
8      vars N M : Nat .
9
10     eq 0 + N = N .
11     eq s(M) + N = s(M + N) .
12 endfm
```

# Mauve

```
5      fmod FACTORIAL is
6      protecting NAT .
7      op _! : Nat -> NzNat .
8      var N : Nat .
9      eq 0 ! = 1 .
10     eq (s N) ! = (s N) * N ! .
11     endfm
```

```
> load factorial.maunder
```

```
> red 100 ! .
```

Reduce in FACTORIAL : 100 ! .

```
rewrites: 201 in 0ms cpu (0ms real) (~ rewrites/second)
```

```
result NzNAT:
```

9332621544394415268169923885626670049071596826438162146  
8592963895217599993229915608941463976156518286253697920  
827223758251185210916864000000000000000000000000

# Maude

```
7      mod VENDING-MACHINE is
8        including VENDING-MACHINE-SIGNATURE .
9        var M : Marking .
10       rl [add-q] : M => M q .
11       rl [add-$] : M => M $ .
12       rl [buy-c] : $ => c .
13       rl [buy-a] : $ => a q .
14       rl [change] : q q q q => $ .
15     endm
```

# Maude

Inductive Theorem Prover (ITP)

Sufficient Completeness Checker (SCC)

Church-Rosser Checker (CRC)

Coherence Checker (ChC)

Maude Termination Tool (MTT)



Maude Formal Environment (MFE)

# Tools overview

	Maude	CiME
Extensibility	+	≈
Still active	≈	—
I/O files	+	+
Syntax	+	+
Documentation	+	—



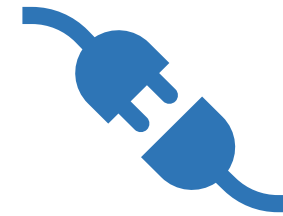
# I/O in Maude



Standard input/output



File handling



Sockets

# I/O in Maude

```
7      mod VENDING-MACHINE is
8        including VENDING-MACHINE-SIGNATURE .
9        var M : Marking .
10       rl [add-q] : M => M q .
11       rl [add-$] : M => M $ .
12       rl [buy-c] : $ => c .
13       rl [buy-a] : $ => a q .
14       rl [change] : q q q q => $ .
15     endm
```

# I/O in Maude

```
5   fmod VENDING-MACHINE-SIGNATURE is
6     sorts Coin Item Marking .
7     subsorts Coin Item < Marking .
8     op __ : Marking Marking -> Marking [assoc comm id: null] .
9     op null : -> Marking .
10    op $ : -> Coin [format (r! o)] .
11    op q : -> Coin [format (r! o)] .
12    op a : -> Item [format (b! o)] .
13    op c : -> Item [format (b! o)] .
14  endfm
```

# I/O in Maude

```
5    load vending-machine-signature.maude
6
7    fmod VENDING-MACHINE-GRAMMAR is
8      protecting VENDING-MACHINE-SIGNATURE .
9      protecting NAT .
10     sort Action .
11     op insert $ : -> Action .
12     op insert q : -> Action .
13     op show basket : -> Action .
14     op show credit : -> Action .
15     op buy__(s) : Nat Item -> Action .
16   endfm
```

# I/O in Maude

```
5  load vending-machine-grammar.maude
6  load buying-strats.maude
7  load file.maude
8
9  mod VENDING-MACHINE-IO is
10      .
11      .
12      .
95  rl < 0 : X | action : insert $, marking : M, Atts >
96  => < 0 : X | action : idle,
97      marking : downTerm(insertCoin('add-$, upTerm(M)), null), Atts >
98  write(stdout, 0, "one dollar introduced\n") .
```

# I/O in Maude

Enter in external environment  $\left\{ \begin{array}{l} \text{Maude> erew vending machine .} \\ \text{erewrite in VENDING-MACHINE-IO : vending machine .} \end{array} \right.$

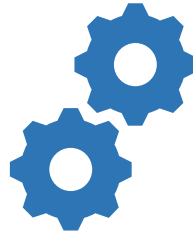
Input	> insert \$
Output	one dollar introduced
	> buy 1 a(s)
	1 apples bought

Parse input?

# META-LEVEL module



Parse input



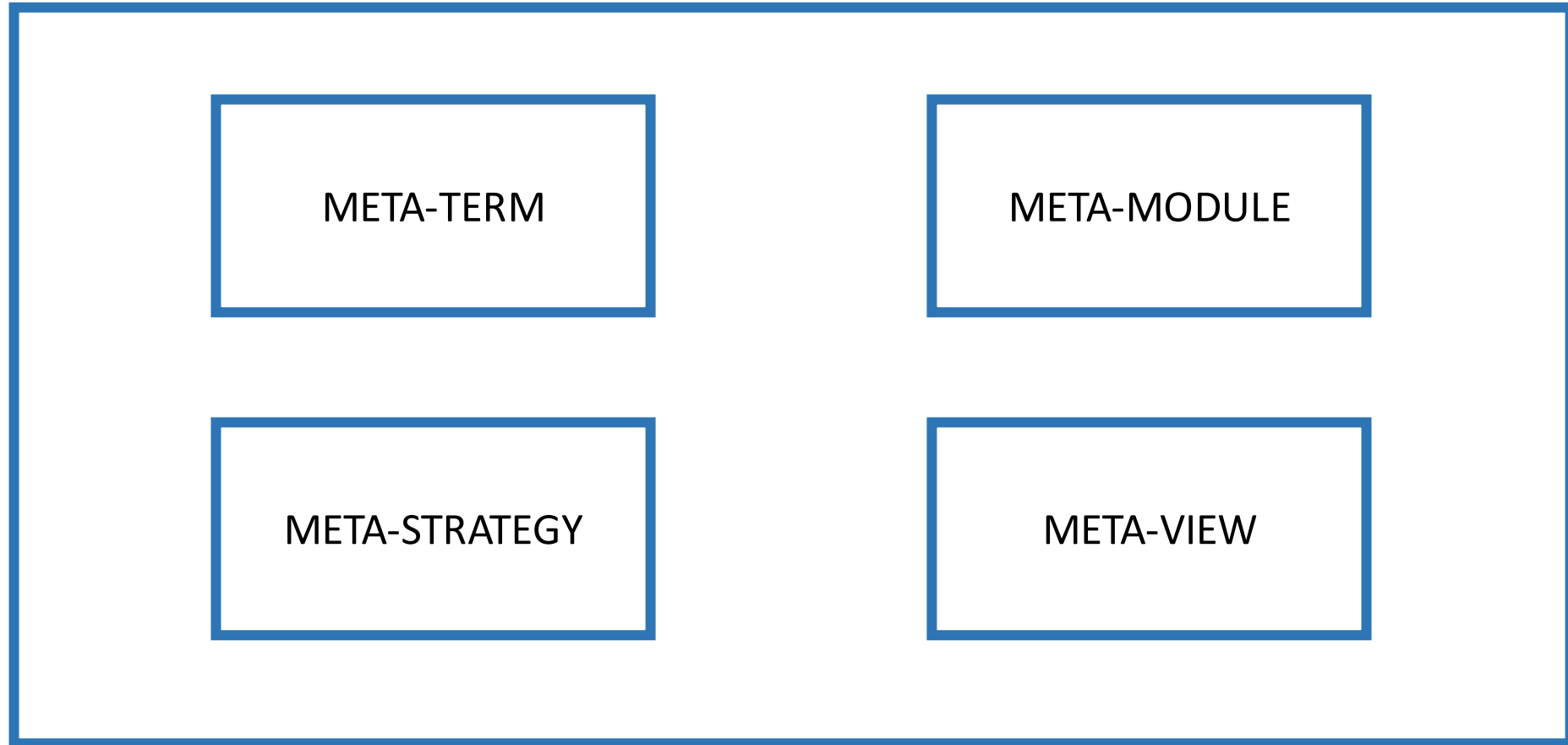
Execute



Print

# META-LEVEL module

META-LEVEL





# META-LEVEL operations

`metaParse()`



Parse a metarepresentation

`upModule()` / `downModule()`



Move through metarepresentations

Reduce in META-LEVEL



Use operation of the META-LEVEL module

# Metalinguage

Funblocks

```
init area(disk(r))
```

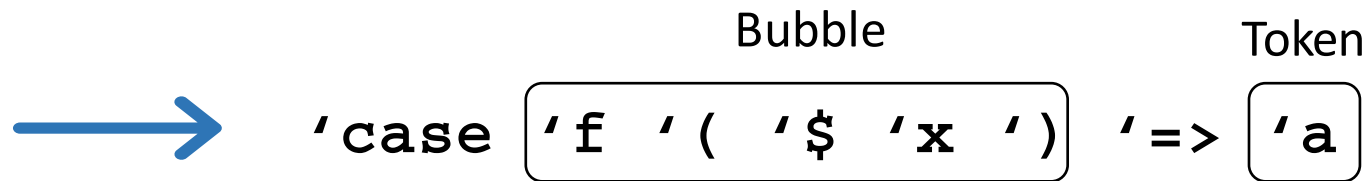
```
case area(disk($d)) => mul(pi, square($d))
```

Maude

```
sorts Const Var Func State Rule Term Expr .
```

# Metalanguage

case f(\$x) => a



**Tokens** are represented by **quoted identifiers (QID)**

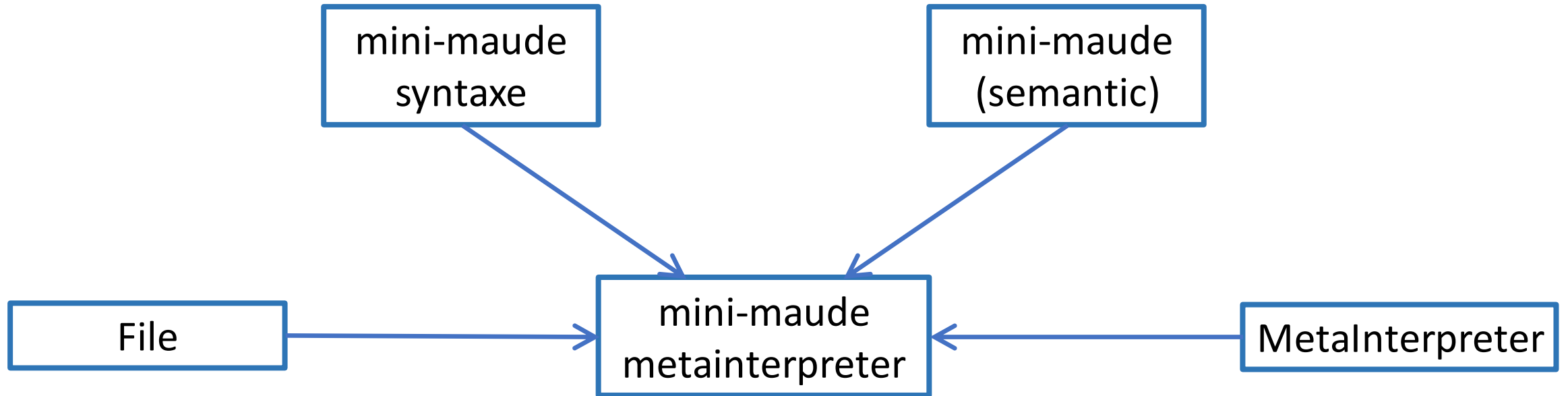
# Metalanguage

```
34     op init_ : Bubble -> State .
35     op case_=>_ : Bubble Bubble -> Rule .
36     op _(_) : Token Bubble -> Func .
37     op $_ : Token -> Var .

53     reduce in META-LEVEL :
54         metaParse(upModule('FUNBLOCKS-SYNTAX, false),
55             'case 'f '`( '$ 'x '` ) '=> 'a , anyType) .
```

```
> result: { 'case_=>_[bubble[...]],bubble['a.Qid]], 'Rule }
```

# MINI-MAUDE



# MINI-MAUDE

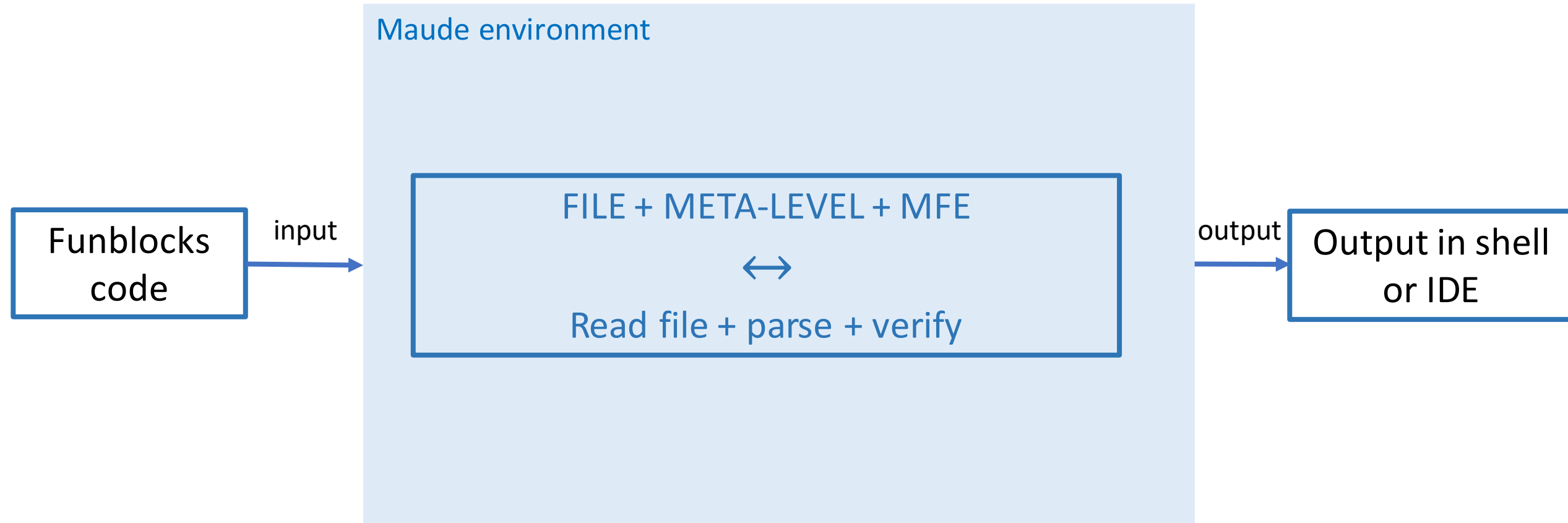
```
Maude> erew minimaude .  
erewrite in MINI-MAUDE-META-INTERPRETER : minimaude .  
MiniMaude Execution Environment
```

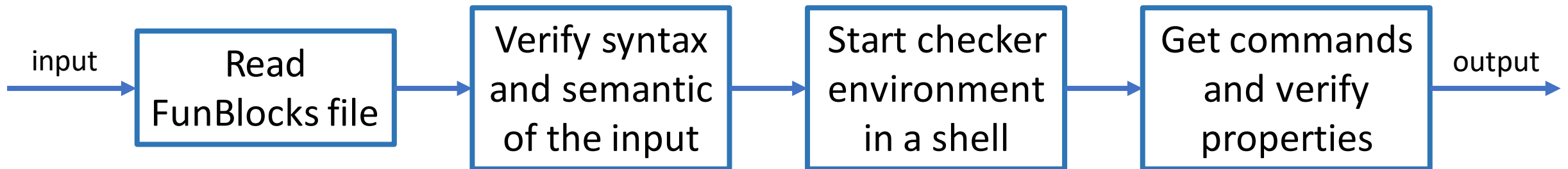
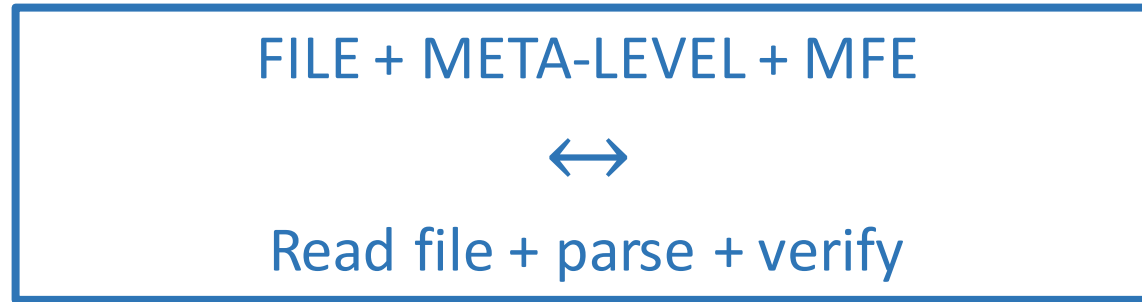
```
minimaude> fmod NAT3 is  
  > sort Nat3 .  
  > op s_ : Nat3 -> Nat3 .  
  > op 0 : -> Nat3 .  
  > eq s s s 0 = 0 .  
  > endfm
```

Module loaded successfully

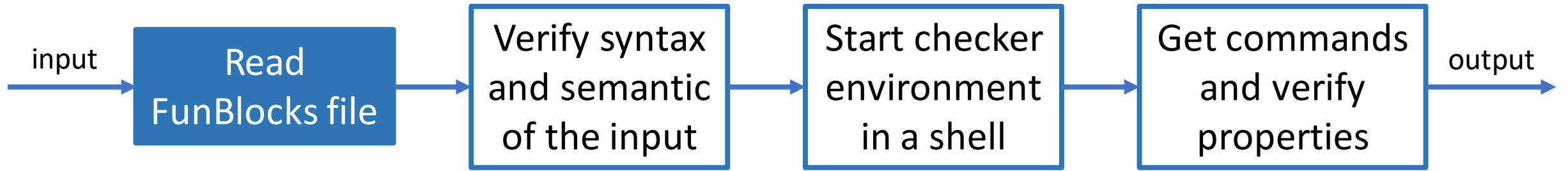
```
minimaude> reduce s s s s 0 .  
result Nat3: s 0
```

# System diagram









FunBlocks file

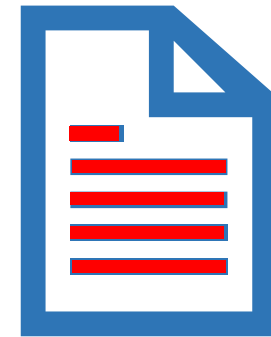


Input

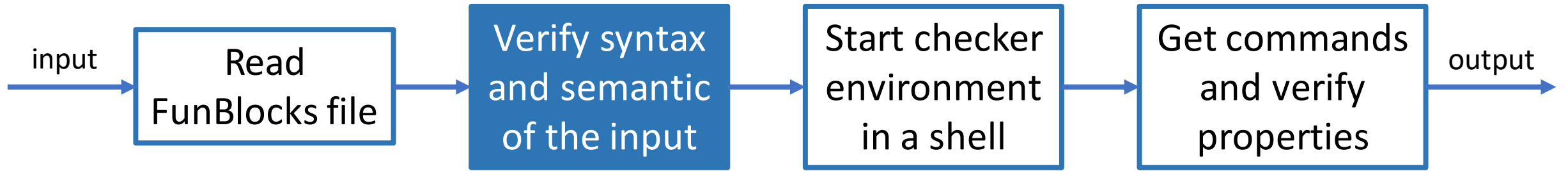
FILE

```
openFile()  
getLine()  
...
```

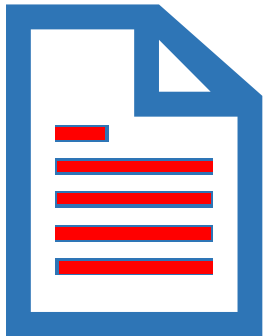
Read file



Output



Read file



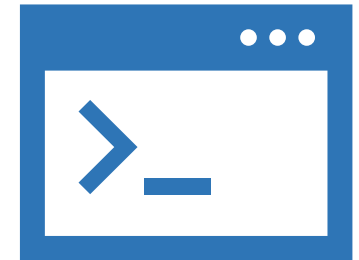
Input

META-LEVEL

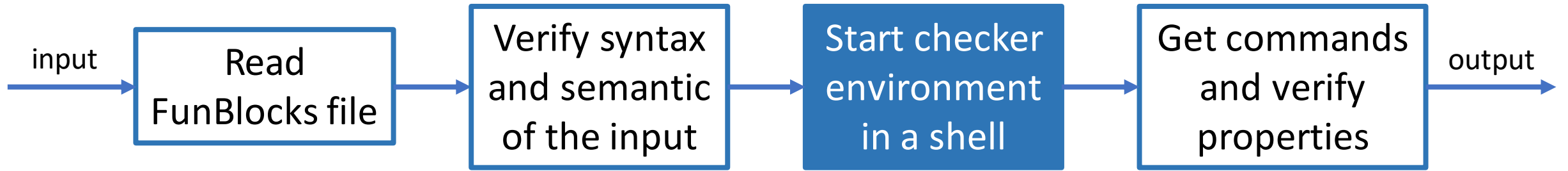
```
metaParse()  
upModule()  
...
```

```
load funblocks-syntax.maude  
load funblocks-semantic.maude
```

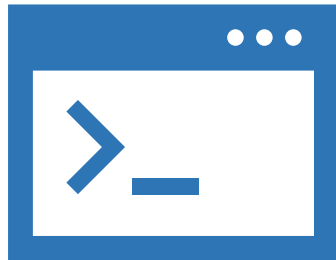
Module inserted



Output

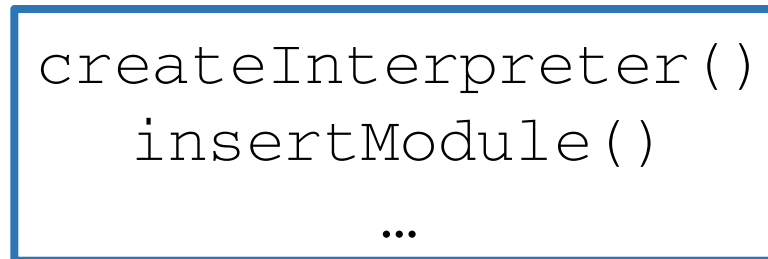


Module inserted

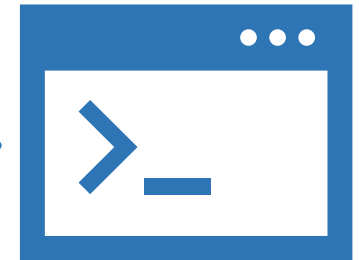


Input

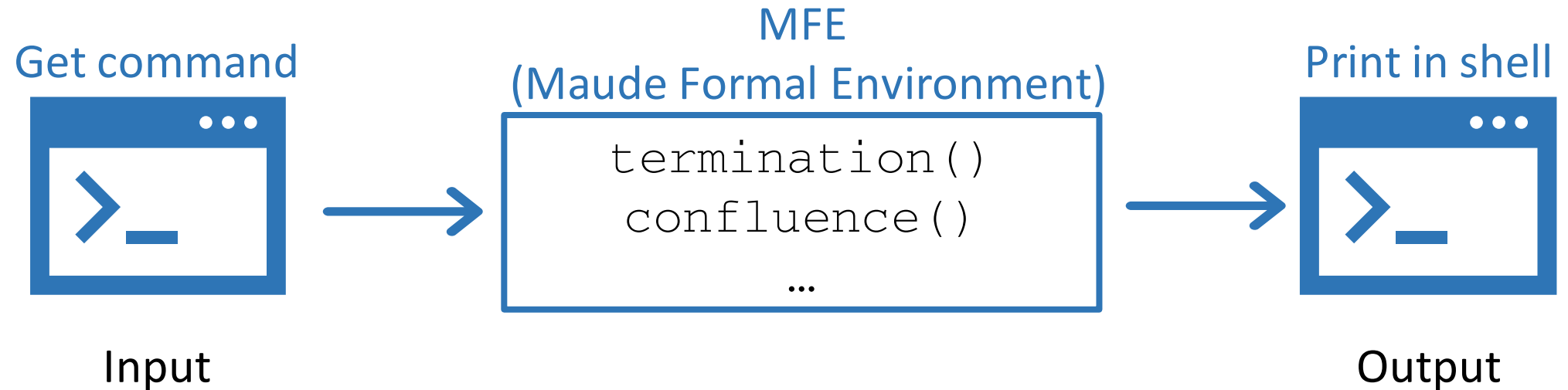
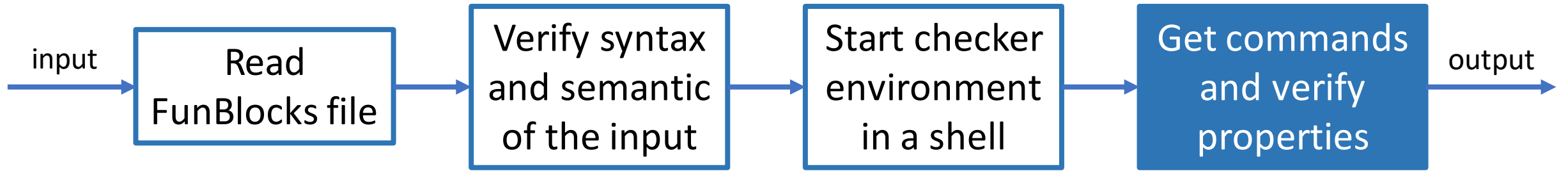
META-INTERPRETER



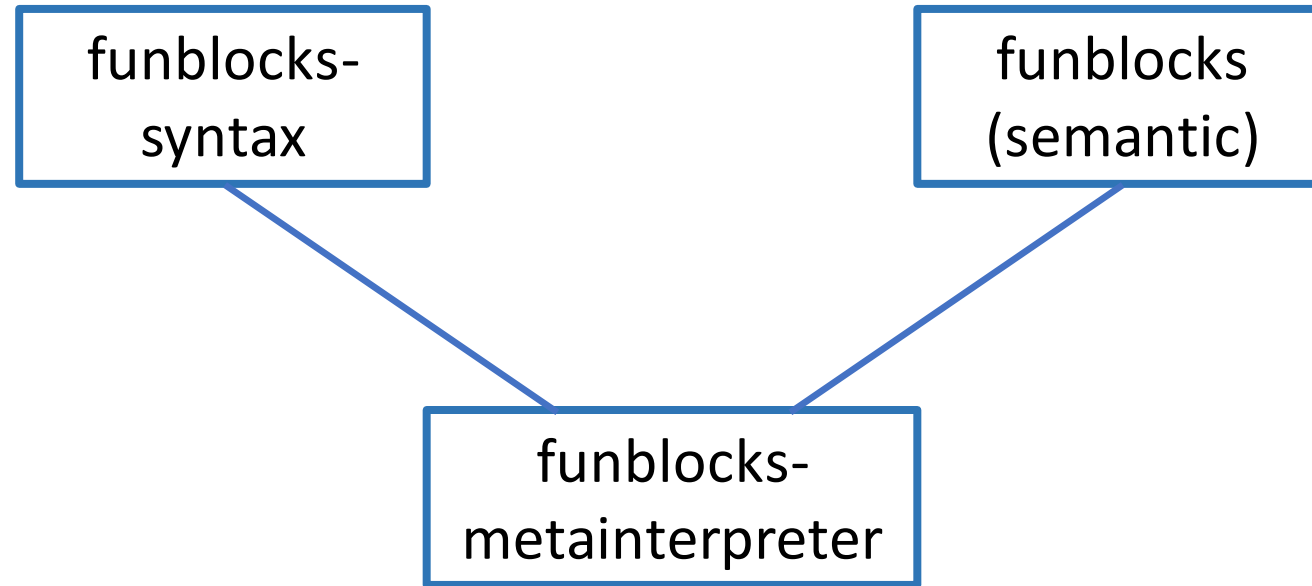
Wait for input



Output



# FunBlocks checker system



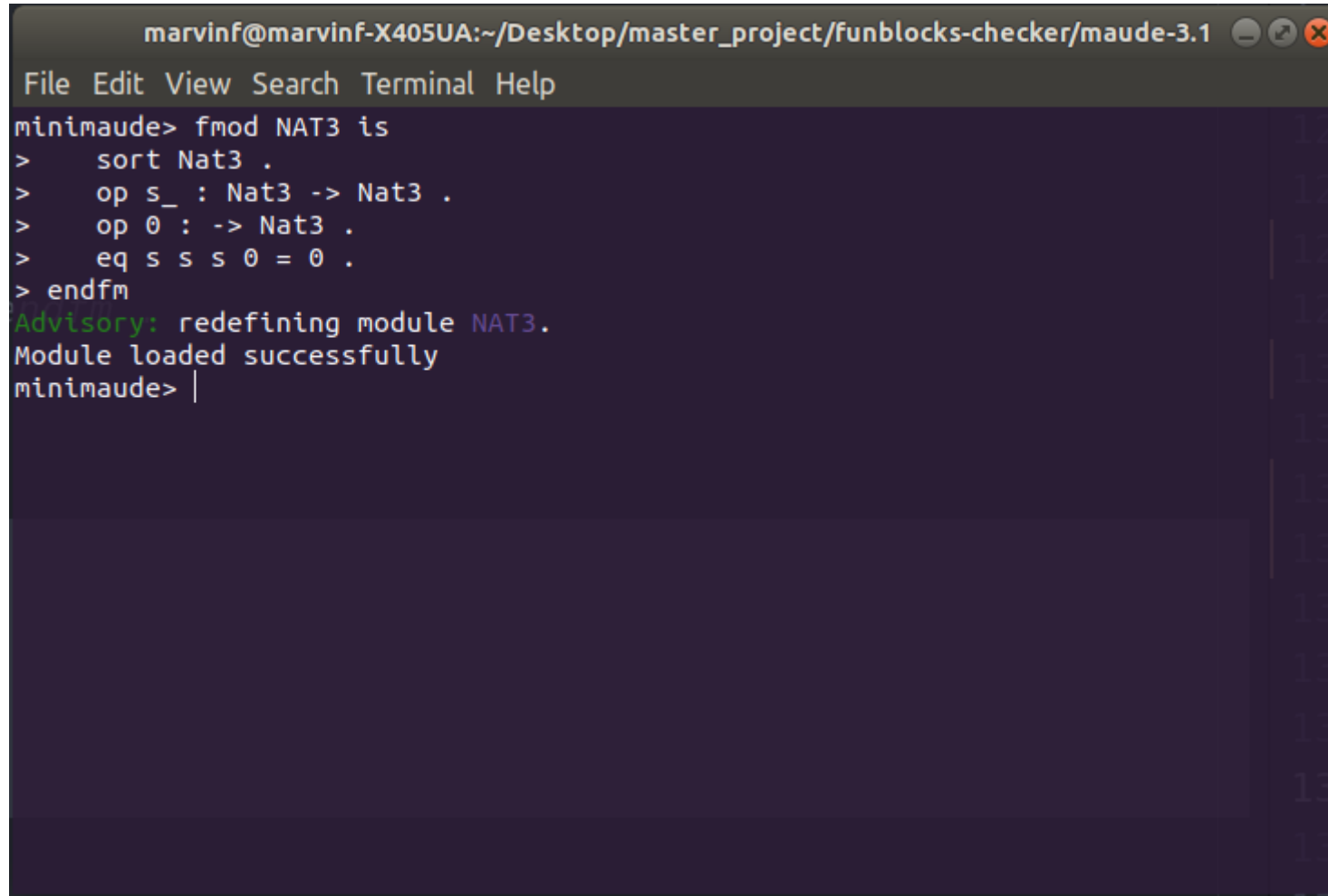
## funblocks- metainterpreter

```
3  rl < 0 : FunBlocks | mi: null, st: 0, Atts >
4      wrote(0, 0')
5      createdInterpreter(0, Y, MI)
6  => < 0 : FunBlocks | mi: MI, st: 1, Atts >
7      insertModule(MI, 0, upModule('FUNBLOCKS-SYNTAX, true)) .
8
9  rl < 0 : FunBlocks | mi: MI, st: 1, Atts >
10     insertedModule(0, 0')
11  => < 0 : FunBlocks | mi: MI, st: 2, Atts >
12     getLine(stdin, 0, "funblocks> ") .
```

## funblocks- metainterpreter

```
3  rl < 0 : FunBlocks | mi: null, st: 0, Atts >
4      wrote(0, 0')
5      createdInterpreter(0, Y, MI)
6  => < 0 : FunBlocks | mi: MI, st: 1, Atts >
7      insertModule(MI, 0, upModule('FUNBLOCKS-SYNTAX, true)) .
8
9  rl < 0 : FunBlocks | mi: MI, st: 1, Atts >
10     insertedModule(0, 0')
11  => < 0 : FunBlocks | mi: MI, st: 2, Atts >
12     getLine(stdin, 0, "funblocks> ") .
```

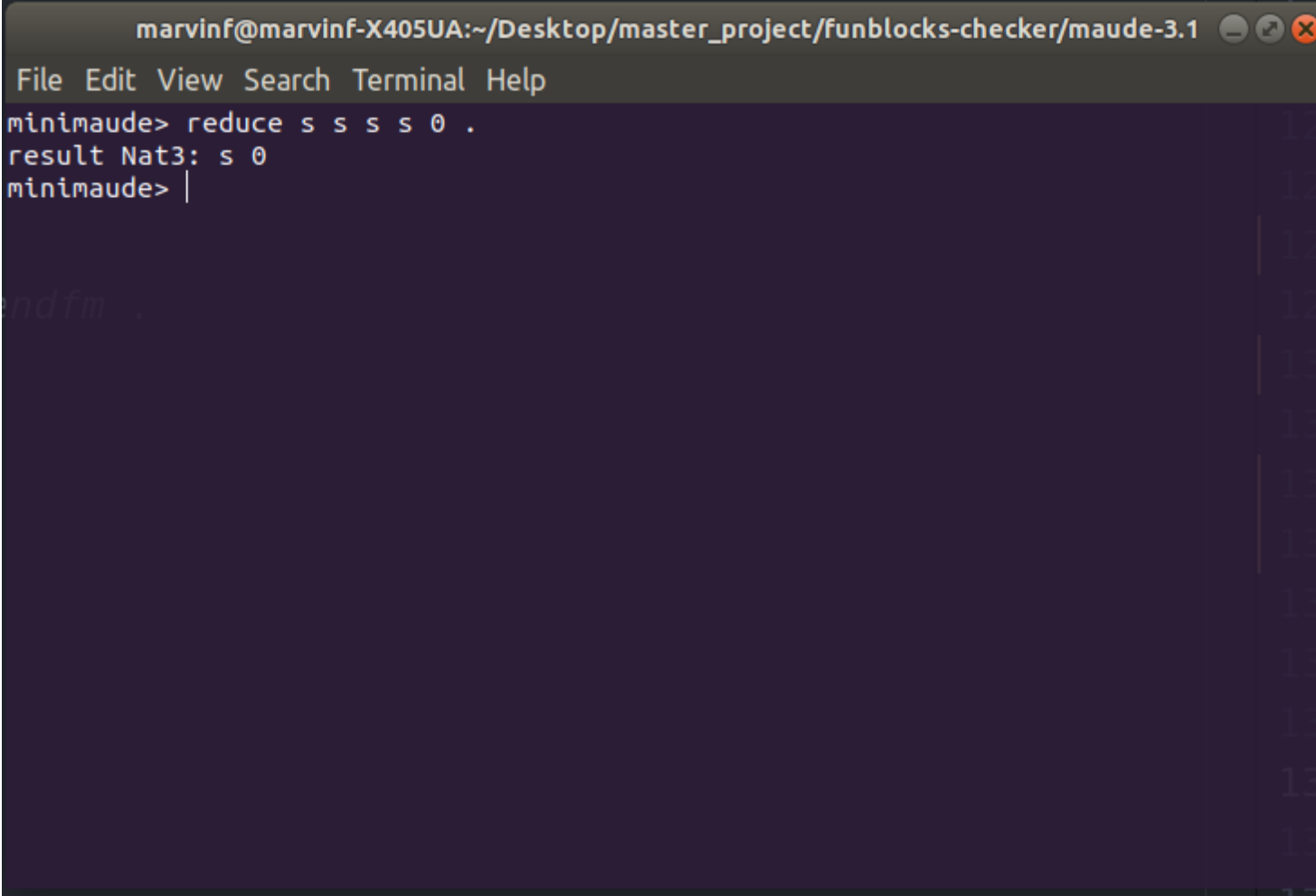
# Mini-Maude: insert module

A screenshot of a terminal window titled 'marvinf@marvinf-X405UA:~/Desktop/master\_project/funblocks-checker/maude-3.1'. The window has a menu bar with 'File', 'Edit', 'View', 'Search', 'Terminal', and 'Help'. The terminal shows the 'minimaude' prompt, followed by the command 'fmod NAT3 is'. Then, several lines of module code are entered: 'sort Nat3 .', 'op s\_ : Nat3 -> Nat3 .', 'op 0 : -> Nat3 .', and 'eq s s s 0 = 0 .', followed by 'endfm'. The terminal then displays the message 'Advisory: redefining module NAT3.' and 'Module loaded successfully'. The prompt 'minimaude>' is shown again with a cursor. On the right side of the terminal, there is a vertical scrollbar and a list of line numbers (12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 83, 84, 85, 86, 87, 88, 89, 90, 91, 92, 93, 94, 95, 96, 97, 98, 99, 100, 101, 102, 103, 104, 105, 106, 107, 108, 109, 110, 111, 112, 113, 114, 115, 116, 117, 118, 119, 120, 121, 122, 123, 124, 125, 126, 127, 128, 129, 130, 131, 132, 133, 134, 135, 136, 137, 138, 139, 140, 141, 142, 143, 144, 145, 146, 147, 148, 149, 150, 151, 152, 153, 154, 155, 156, 157, 158, 159, 160, 161, 162, 163, 164, 165, 166, 167, 168, 169, 170, 171, 172, 173, 174, 175, 176, 177, 178, 179, 180, 181, 182, 183, 184, 185, 186, 187, 188, 189, 190, 191, 192, 193, 194, 195, 196, 197, 198, 199, 200, 201, 202, 203, 204, 205, 206, 207, 208, 209, 210, 211, 212, 213, 214, 215, 216, 217, 218, 219, 220, 221, 222, 223, 224, 225, 226, 227, 228, 229, 230, 231, 232, 233, 234, 235, 236, 237, 238, 239, 240, 241, 242, 243, 244, 245, 246, 247, 248, 249, 250, 251, 252, 253, 254, 255, 256, 257, 258, 259, 260, 261, 262, 263, 264, 265, 266, 267, 268, 269, 270, 271, 272, 273, 274, 275, 276, 277, 278, 279, 280, 281, 282, 283, 284, 285, 286, 287, 288, 289, 290, 291, 292, 293, 294, 295, 296, 297, 298, 299, 300, 301, 302, 303, 304, 305, 306, 307, 308, 309, 310, 311, 312, 313, 314, 315, 316, 317, 318, 319, 320, 321, 322, 323, 324, 325, 326, 327, 328, 329, 330, 331, 332, 333, 334, 335, 336, 337, 338, 339, 340, 341, 342, 343, 344, 345, 346, 347, 348, 349, 350, 351, 352, 353, 354, 355, 356, 357, 358, 359, 360, 361, 362, 363, 364, 365, 366, 367, 368, 369, 370, 371, 372, 373, 374, 375, 376, 377, 378, 379, 380, 381, 382, 383, 384, 385, 386, 387, 388, 389, 390, 391, 392, 393, 394, 395, 396, 397, 398, 399, 400, 401, 402, 403, 404, 405, 406, 407, 408, 409, 410, 411, 412, 413, 414, 415, 416, 417, 418, 419, 420, 421, 422, 423, 424, 425, 426, 427, 428, 429, 430, 431, 432, 433, 434, 435, 436, 437, 438, 439, 440, 441, 442, 443, 444, 445, 446, 447, 448, 449, 450, 451, 452, 453, 454, 455, 456, 457, 458, 459, 460, 461, 462, 463, 464, 465, 466, 467, 468, 469, 470, 471, 472, 473, 474, 475, 476, 477, 478, 479, 480, 481, 482, 483, 484, 485, 486, 487, 488, 489, 490, 491, 492, 493, 494, 495, 496, 497, 498, 499, 500, 501, 502, 503, 504, 505, 506, 507, 508, 509, 510, 511, 512, 513, 514, 515, 516, 517, 518, 519, 520, 521, 522, 523, 524, 525, 526, 527, 528, 529, 530, 531, 532, 533, 534, 535, 536, 537, 538, 539, 540, 541, 542, 543, 544, 545, 546, 547, 548, 549, 550, 551, 552, 553, 554, 555, 556, 557, 558, 559, 560, 561, 562, 563, 564, 565, 566, 567, 568, 569, 570, 571, 572, 573, 574, 575, 576, 577, 578, 579, 580, 581, 582, 583, 584, 585, 586, 587, 588, 589, 590, 591, 592, 593, 594, 595, 596, 597, 598, 599, 600, 601, 602, 603, 604, 605, 606, 607, 608, 609, 610, 611, 612, 613, 614, 615, 616, 617, 618, 619, 620, 621, 622, 623, 624, 625, 626, 627, 628, 629, 630, 631, 632, 633, 634, 635, 636, 637, 638, 639, 640, 641, 642, 643, 644, 645, 646, 647, 648, 649, 650, 651, 652, 653, 654, 655, 656, 657, 658, 659, 660, 661, 662, 663, 664, 665, 666, 667, 668, 669, 670, 671, 672, 673, 674, 675, 676, 677, 678, 679, 680, 681, 682, 683, 684, 685, 686, 687, 688, 689, 690, 691, 692, 693, 694, 695, 696, 697, 698, 699, 700, 701, 702, 703, 704, 705, 706, 707, 708, 709, 710, 711, 712, 713, 714, 715, 716, 717, 718, 719, 720, 721, 722, 723, 724, 725, 726, 727, 728, 729, 730, 731, 732, 733, 734, 735, 736, 737, 738, 739, 740, 741, 742, 743, 744, 745, 746, 747, 748, 749, 750, 751, 752, 753, 754, 755, 756, 757, 758, 759, 760, 761, 762, 763, 764, 765, 766, 767, 768, 769, 770, 771, 772, 773, 774, 775, 776, 777, 778, 779, 780, 781, 782, 783, 784, 785, 786, 787, 788, 789, 790, 791, 792, 793, 794, 795, 796, 797, 798, 799, 800, 801, 802, 803, 804, 805, 806, 807, 808, 809, 810, 811, 812, 813, 814, 815, 816, 817, 818, 819, 820, 821, 822, 823, 824, 825, 826, 827, 828, 829, 830, 831, 832, 833, 834, 835, 836, 837, 838, 839, 840, 841, 842, 843, 844, 845, 846, 847, 848, 849, 850, 851, 852, 853, 854, 855, 856, 857, 858, 859, 860, 861, 862, 863, 864, 865, 866, 867, 868, 869, 870, 871, 872, 873, 874, 875, 876, 877, 878, 879, 880, 881, 882, 883, 884, 885, 886, 887, 888, 889, 890, 891, 892, 893, 894, 895, 896, 897, 898, 899, 900, 901, 902, 903, 904, 905, 906, 907, 908, 909, 910, 911, 912, 913, 914, 915, 916, 917, 918, 919, 920, 921, 922, 923, 924, 925, 926, 927, 928, 929, 930, 931, 932, 933, 934, 935, 936, 937, 938, 939, 940, 941, 942, 943, 944, 945, 946, 947, 948, 949, 950, 951, 952, 953, 954, 955, 956, 957, 958, 959, 960, 961, 962, 963, 964, 965, 966, 967, 968, 969, 970, 971, 972, 973, 974, 975, 976, 977, 978, 979, 980, 981, 982, 983, 984, 985, 986, 987, 988, 989, 990, 991, 992, 993, 994, 995, 996, 997, 998, 999, 1000).

```
marvinf@marvinf-X405UA:~/Desktop/master_project/funblocks-checker/maude-3.1
File Edit View Search Terminal Help
minimaude> fmod NAT3 is
>   sort Nat3 .
>   op s_ : Nat3 -> Nat3 .
>   op 0 : -> Nat3 .
>   eq s s s 0 = 0 .
> endfm
Advisory: redefining module NAT3.
Module loaded successfully
minimaude> |
```



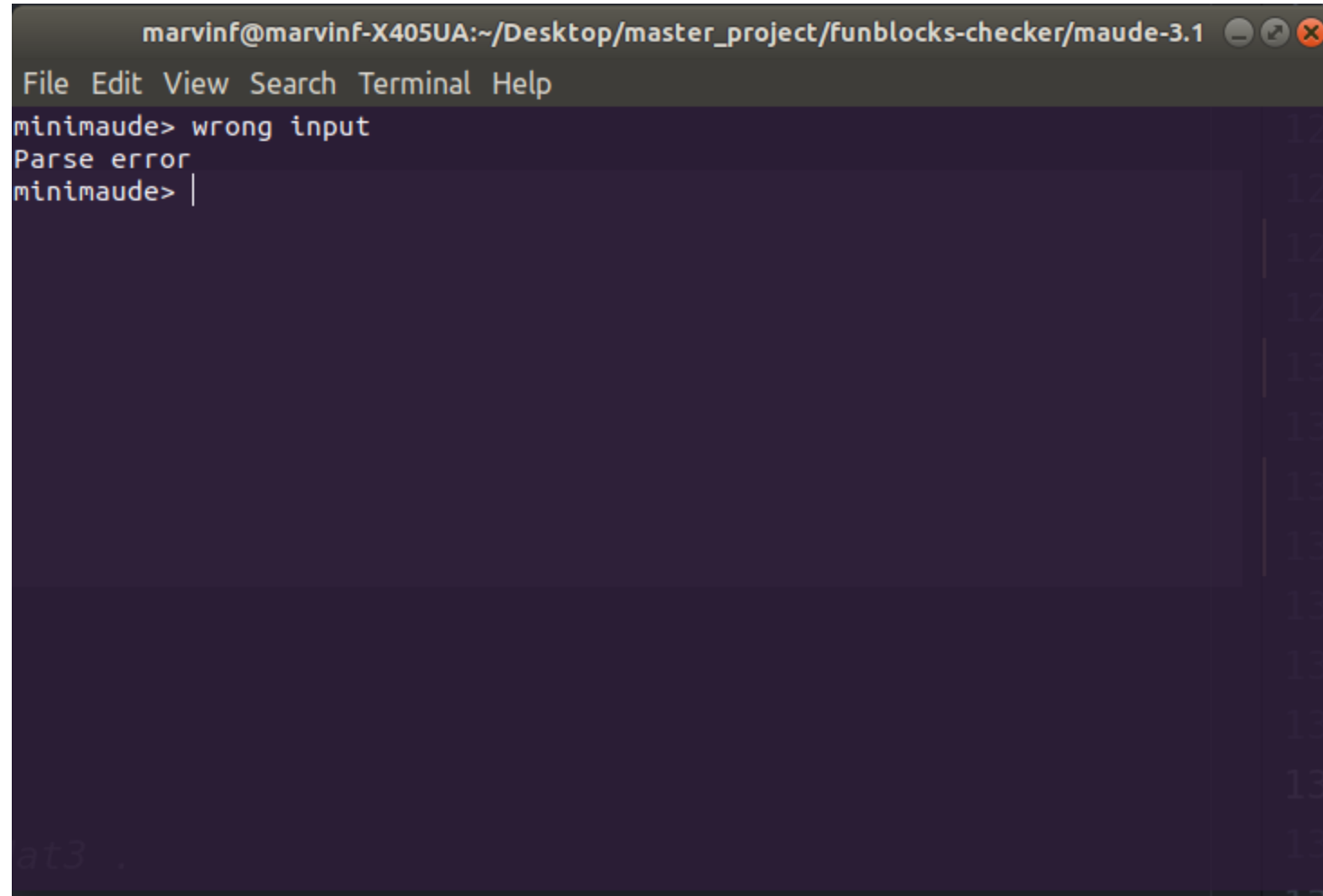
# Mini-Maude: use « reduce » command



```
marvinf@marvinf-X405UA:~/Desktop/master_project/funblocks-checker/maude-3.1
File Edit View Search Terminal Help
minimaude> reduce s s s s 0 .
result Nat3: s 0
minimaude> |
```

The screenshot shows a terminal window titled "marvinf@marvinf-X405UA:~/Desktop/master\_project/funblocks-checker/maude-3.1". The window has a menu bar with "File", "Edit", "View", "Search", "Terminal", and "Help". The terminal content shows the command "reduce s s s s 0 ." being entered, followed by the output "result Nat3: s 0". The prompt "minimaude>" is visible on the next line, with a cursor character "|".

# Mini-Maude: wrong command



The screenshot shows a terminal window with a dark background. The title bar at the top reads "marvinf@marvinf-X405UA:~/Desktop/master\_project/funblocks-checker/maude-3.1" and includes standard window control buttons. Below the title bar is a menu bar with the options "File", "Edit", "View", "Search", "Terminal", and "Help". The main area of the terminal displays the following text:

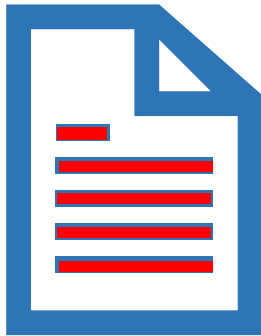
```
minimaude> wrong input
Parse error
minimaude> |
```

The text "at3 ." is partially visible at the bottom left of the terminal window. On the right side, there is a vertical scrollbar with a list of line numbers, including 12, 13, and 14.

# Mini-Maude: quit environment

```
marvinf@marvinf-X405UA:~/Desktop/master_project/funblocks-checker/maude-3.1
File Edit View Search Terminal Help
minimaude> q
goodbye
rewrites: 300 in 20ms cpu (185349ms real) (15000 rewrites/second)
result Portal: <>
=====
reduce in NAT3 : s s s s 0 .
rewrites: 1 in 0ms cpu (0ms real) (~ rewrites/second)
result Nat3: s 0
Maude> |
```

# Funblocks checker



## Module inserted



```
load funblocks-syntax.mauve
load funblocks-semantic.mauve
```

# Funblocks checker

```
1 case f => g
```

Input

FUN-TO-MAUDE



```
1 mod FUN-RULES is
2   sort Term .
3   op f : -> Term .
4   op g : -> Term .
5   rl f => g .
6 endm
```

Output

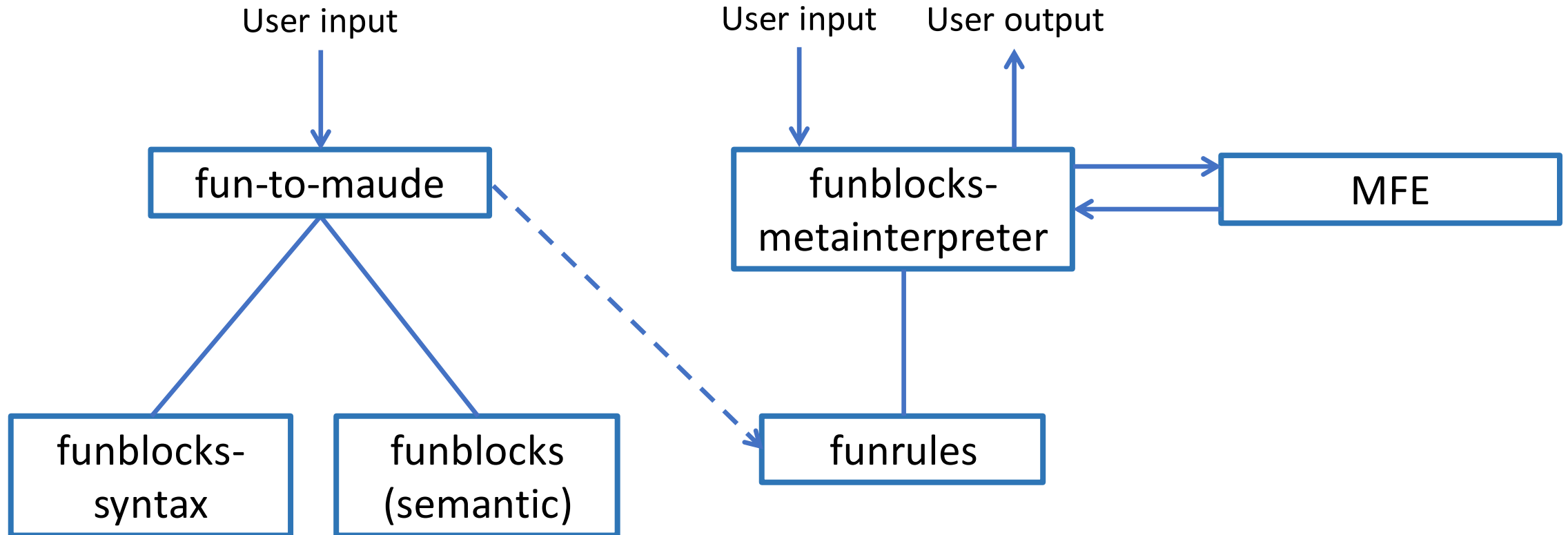
# What's next ?

```
1  mod FUN-RULES is
2    sort Term .
3    op f : -> Term .
4    op g : -> Term .
5    rl f => g .
6  endm
```

→ Typing ?

→ Type checking

# FunBlocks checker system



# FUNBLOCK-SYNTAX

```
25  sorts Term Var Const Func Decl .
26  subsort Var Func Const < Term .
27
28  op case_=>_ : Term Term -> Decl .
29  op $_ : Token -> Var .
30  op _(_) : Token Token -> Func .
31  op _(_) : Token Term -> Func .
```



# FUNBLOCKS

```
'case '$ 'x' => 'id' ( 'a' )
```

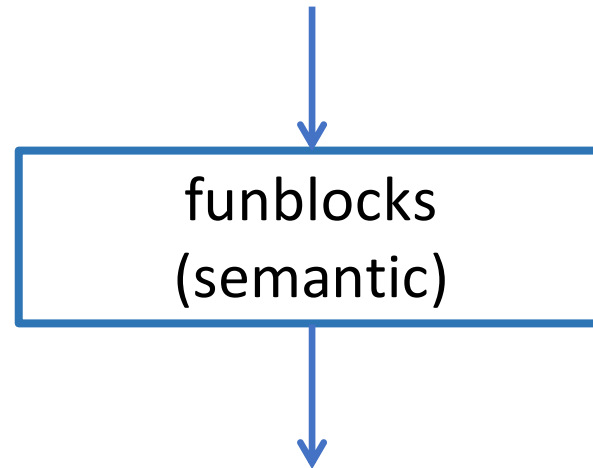


funblocks  
(semantic)

```
'var '$ 'x' : 'Untyped' . '\n  
'op 'id' : 'Untyped' -> 'Untyped' . '\n  
'op 'a' : '-> 'Untyped' . '\n  
'r1 '$ 'x' => ''id' ( ''a' ) ' . '\n
```

# FUNBLOCKS

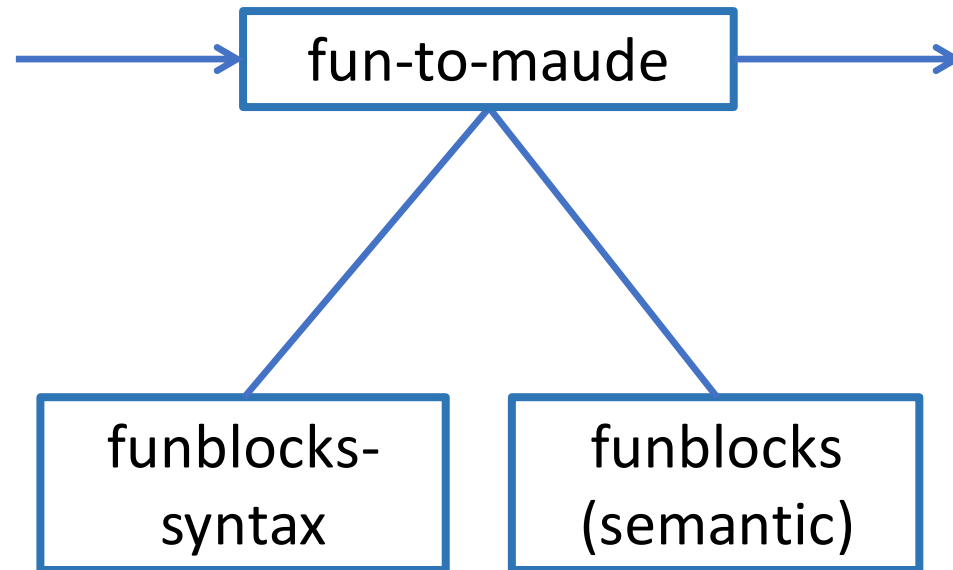
`'case 'compose '( 'f ', 'g ', '$ 'x ') '=> 'f '( 'g '( '$ 'x ') ')`



`noParse()`

# FUN-TO-MAUDE

```
init dist(a,d)  
case $ x => id(a)
```



```
1  mod FUN-RULES is  
2  var '$x' : Untyped .  
3  op 'id' : Untyped -> Untyped .  
4  op 'a' : -> Untyped .  
5  rl '$x' => 'id('a) .  
6  endm
```

# FUNRULES

```
1  mod FUN-RULES is
2  var '$x : Untyped .
3  op 'id : Untyped -> Untyped .
4  op 'a : -> Untyped .
5  rl '$x => 'id('a) .
6  endm
```



```
1  mod FUN-RULES is
2  inc FUNTYPES .
3  sorts Numbers String .
4  var '$x : Untyped .
5  op 'id : Untyped -> Untyped .
6  op 'a : -> Untyped .
7  rl '$x => 'id('a) .
8  endm
```

# Pre-processing (script)

case id(\$x) => \$x



case id(\$ x) => \$ x

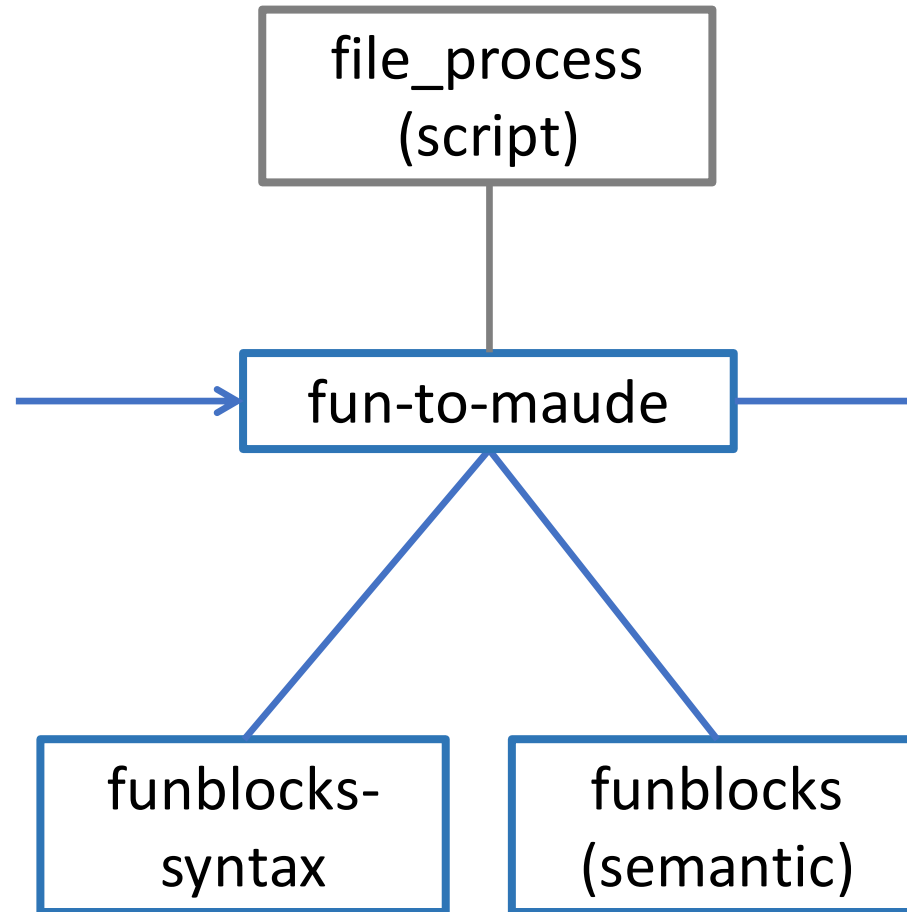
# Post-processing (script)

`case id($'x) => $('x`  `case id($x) => $x`

`op a : -> Nat`  
`op a : -> Nat`  `op a : -> Nat`

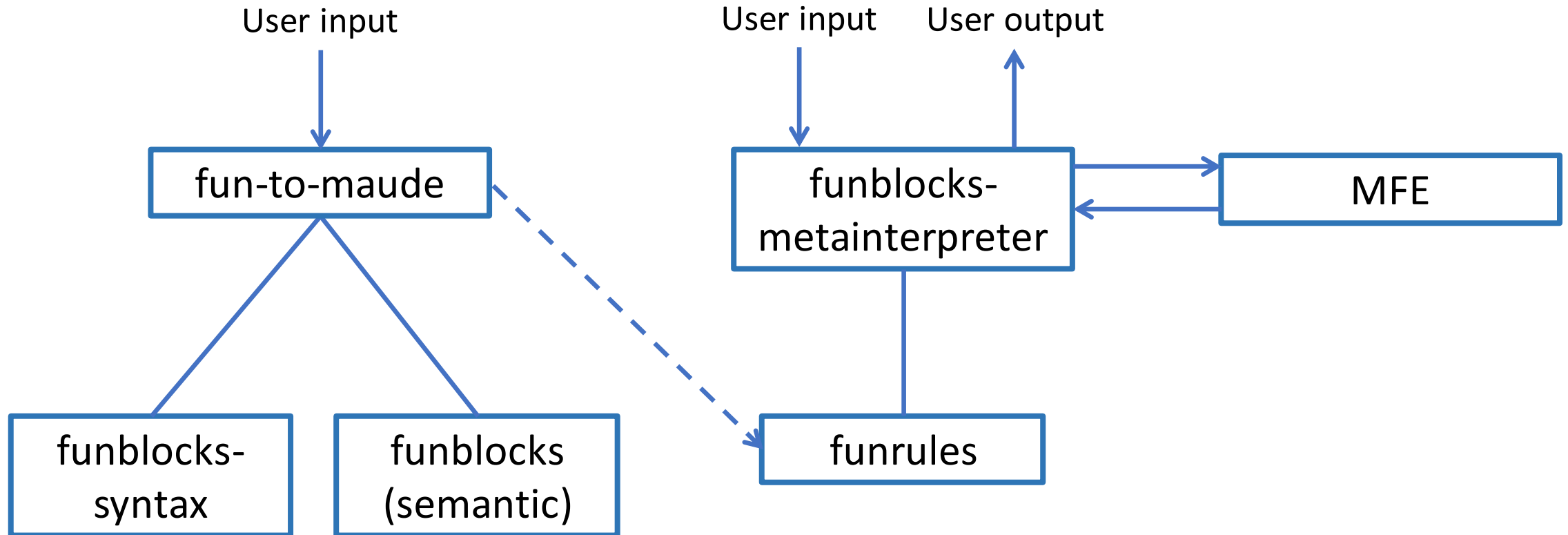
# FUN-TO-MAUDE

```
init dist(a,d)  
case $x => id(a)
```



```
1  mod FUN-RULES is  
2    var $x : Untyped .  
3    op id : Untyped -> Untyped .  
4    op a : -> Untyped .  
5    rl $x => id(a) .  
6  endm
```

# FunBlocks checker system





# Static Typing

```
type List $T :: empty | cons $T (List $T)
rule ajoute $T :: $T -> List $T => List $T
case ajoute($x, cons($y, $tail)) => cons($y, $tail)
```

```
{ ajoute:
  [ TypeVarRef { range: [Object], label: 'T' },
    TypeDeclRef { range: [Object], name: 'List', arguments: [Array] },
    TypeDeclRef { range: [Object], name: 'List', arguments: [Array] } ] }
```

# Static Typing

```
case ajoute($x, cons($y, $tail)) => cons($y, $tail)
```

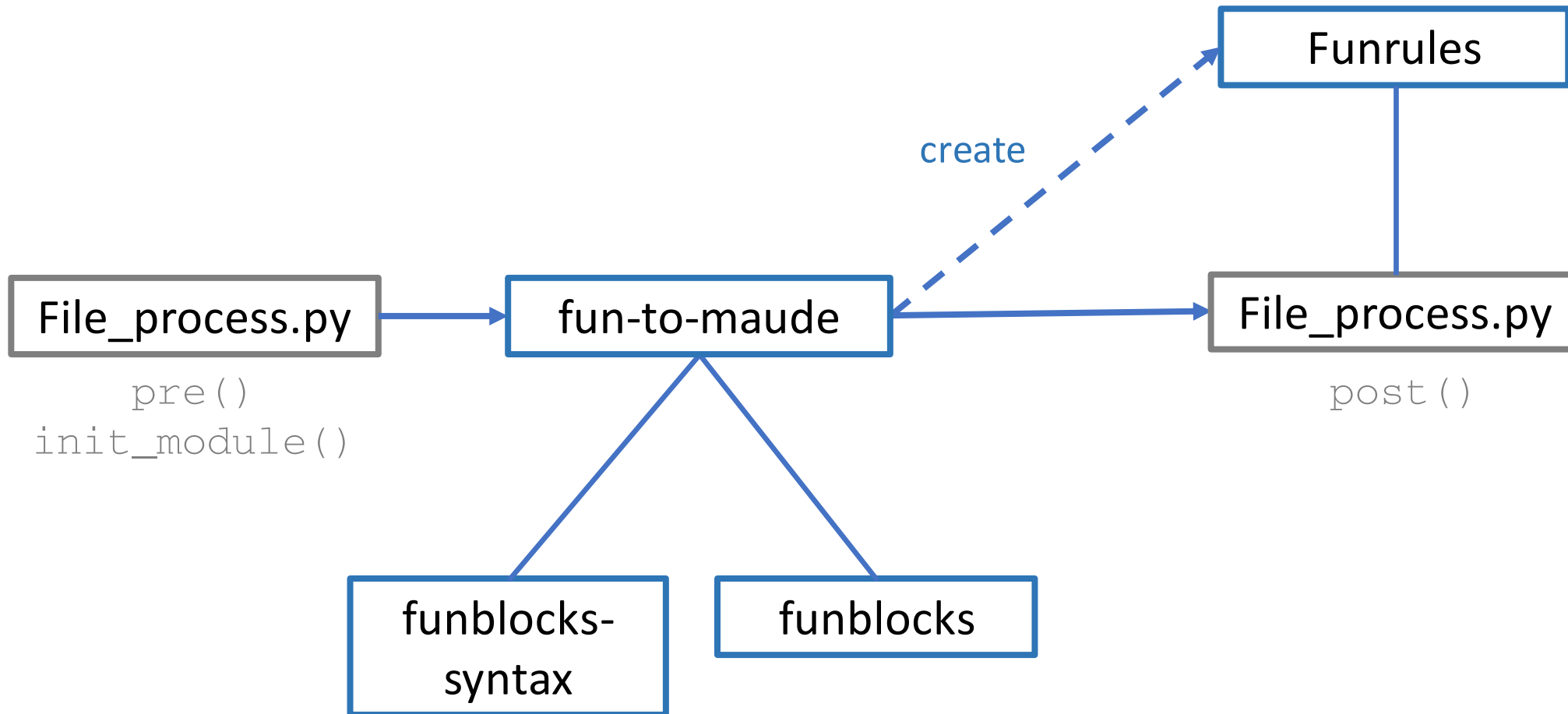
```
{ ajoute: [ TypeVarRef { range: null, label: 'T0' }, <2 empty items> ] }
```

```

5  fmod MY-LIST{T :: TRIV} is
6
7  protecting LIST{T} .
8  protecting NAT .
9  protecting QID .
10
11  subsort Qid < T$Elt < List{T} .
12  vars $x $y : T$Elt .
13  vars $tail : List{T} .
14
15  --- constructed with 'type'
16  op empty : -> List{T} .
17  op ajoute : T$Elt List{T} -> List{T} .
18  op cons : T$Elt List{T} -> List{T} .
19
20  --- constructed with 'case'
21  eq ajoute($x, cons($y, $tail)) = cons($y, ajoute($x, $tail)) .
22  eq ajoute($x, empty) = cons($x, empty) .
23
24  endfm

```

# Execution



# Maude tools

Inductive Theorem Prover (ITP)

Sufficient Completeness Checker (SCC)

Church-Rosser Checker (CRC)

Coherence Checker (ChC)

Maude Termination Tool (MTT)



Maude Formal Environment (MFE)

# Maude Formal Environment

Maude 3.1 (last version)

Inductive Theorem Prover (ITP)

**Church-Rosser Checker (CRC)**

Coherence Checker (ChC)

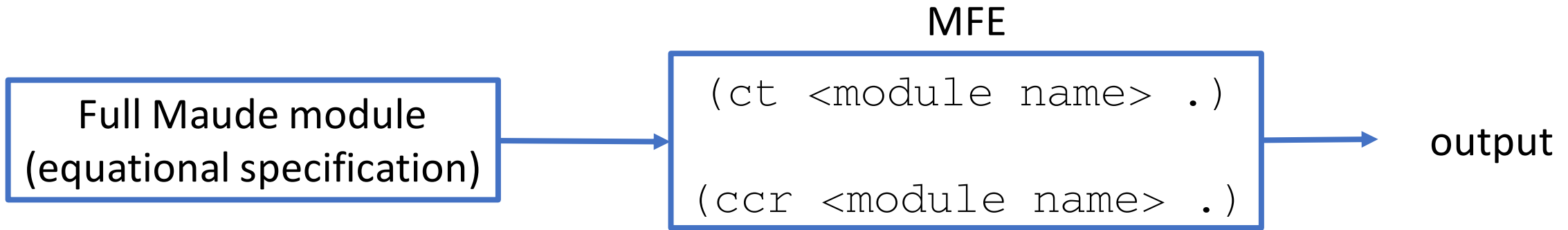
Maude++ 2.7

Sufficient Completeness Checker (SCC)

**Maude Termination Tool (MTT)**

↕  
AProVE

# Maude Formal Environment



Works only with equational specifications

# Church-Rosser Checker

```
1  mod TEST2 is
2    sort Generic .
3    op id : Nat -> Nat .
4    var x : Nat .
5    op a : -> Nat .
6    eq id(x) = x .
7    eq id(x) = a .
8  endm
```

```
Maude> (ccr TEST2 .)
rewrites: 36429 in 4ms cpu (3ms real) (9107250 rewrites/second)
Church-Rosser check for TEST2
The following critical pairs must be proved joinable:
  cp TEST21
    a
  = x:Nat .
    The module is sort-decreasing.
```



# Church-Rosser Checker

```
1  mod TEST3 is
2    sort Generic .
3    op id : Nat -> Nat .
4    var x : Nat .
5    op a : -> Nat .
6    eq id(x) = x .
7  endm
```

```
Maude> (ccr TEST3 .)
rewrites: 36299 in 4ms cpu (3ms real) (9074750 rewrites/second)
Church-Rosser check for TEST3
  All critical pairs have been joined.
  The specification is locally-confluent.
  The module is sort-decreasing.
```

# Church-Rosser Checker

```
1  mod TEST3 is
2    sort Generic .
3    op id : Nat -> Nat .
4    var x : Nat .
5    op a : -> Nat .
6    eq id(x) = x .
7  endm
```

```
Maude> (ccr TEST3 .)
rewrites: 36299 in 4ms cpu (3ms real) (9074750 rewrites/second)
Church-Rosser check for TEST3
  All critical pairs have been joined.
  The specification is locally-confluent.
  The module is sort-decreasing.
```

# Termination tool

```
14 (fmod TEST2 is
15   sort Nat .
16   vars x y : Nat .
17   op a : -> Nat .
18   op b : -> Nat .
19   op f : Nat Nat Nat -> Nat .
20   op g : Nat Nat -> Nat .
21
22   eq f(a,b,x) = f(x,x,x) .
23   eq g(x,y) = x .
24   eq g(x,y) = y .
25 endfm)
```

```
rewrites: 66 in 4ms cpu (4ms real) (16500 rewrites/second)
The MTT has been set as current tool.

rewrites: 29 in 4ms cpu (4ms real) (7250 rewrites/second)
aprove is now the current external tool.

rewrites: 75 in 0ms cpu (1ms real) (~ rewrites/second)
Success: The module TEST2 is non-terminating.

rewrites: 66 in 4ms cpu (0ms real) (16500 rewrites/second)
The CRC has been set as current tool.

rewrites: 126 in 0ms cpu (3ms real) (~ rewrites/second)
Church-Rosser check for TEST2
The following critical pairs must be proved joinable:
  cp TEST22
    x:Nat
    = y:Nat .
    The module is sort-decreasing.
```

# Equation vs rules (in Maude)



Equations

Represent theory

Terminating and confluent



Rules

Represent states changes

No constraints on termination and confluence

Reductions using rewrite logic

# Parsing in Maude

reduce

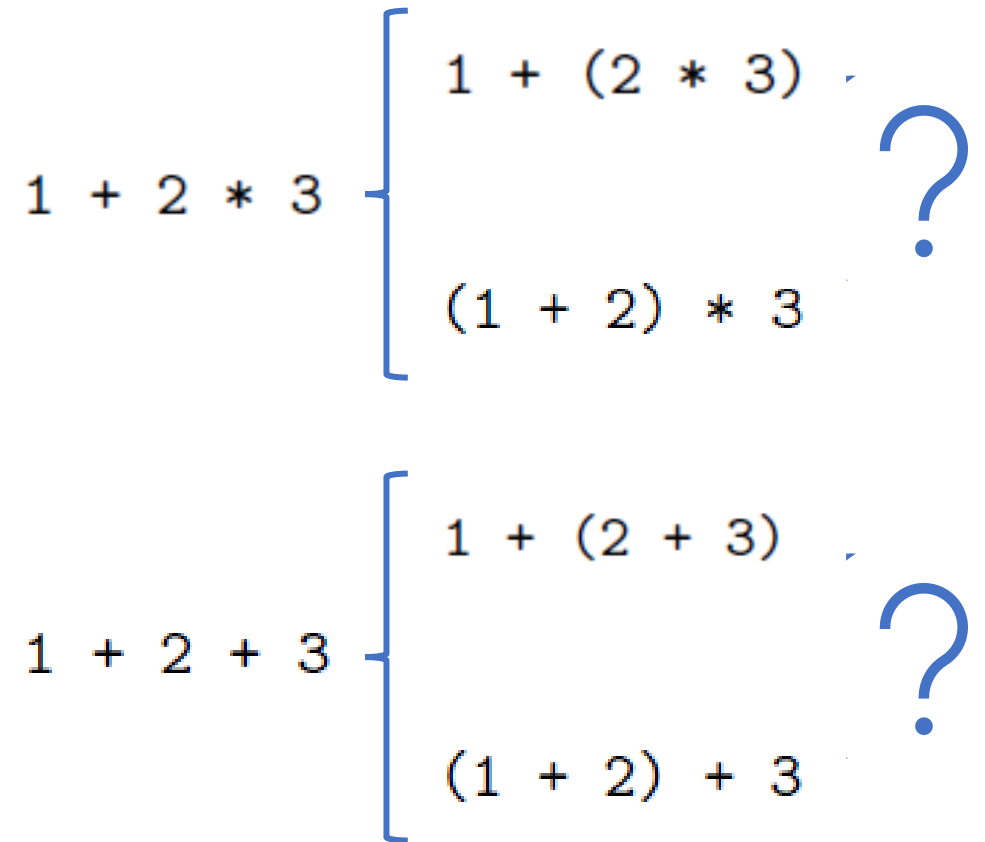
```
red 1 + (1 + 1) .
```

rewrite

```
rew [6] $ $ q q .
```

# Precedence and gathering

```
sort Nat .  
ops 1 2 3 : -> Nat .  
ops _+_ *_ : Nat Nat -> Nat .
```




# Precedence and gathering

prec  $\longrightarrow$  Indication of « priority » using a natural number

gather  $\longrightarrow$  E : precedence value  $\leq$  precedence value of the operator  
e : precedence value  $<$  precedence value of the operator  
& : any precedence value

# Precedence and gathering

```
op _+_ : Nat Nat -> Nat [prec 33 gather (E e)] .  
op _*_ : Nat Nat -> Nat [prec 31 gather (E e)] .
```


$$\begin{array}{lcl} 1 + 2 * 3 & = & 1 + (2 * 3) \\ 1 + 2 + 3 & = & (1 + 2) + 3 \end{array}$$



# Default precedence values

prec



0 for the constants (`zero`)

0 for mixfix operator which not begin **nor** end with `_ ( ( _ ) )`

41 for mixfix operator which begin **or** and with `_ ( to _ : _ )`  
-> 15 for unary operator ( `not _` )

41 : for mixfix operator which begin **and** end with `_ ( _ + _ )`

# Default gathering values

gather  $\longrightarrow$  & for default prefix operators  
& for operator which not begin nor end with  $\_ ( \_ )$   
E for adjacent  $\_$  or  $\_$  at the edges  $( \_? \_ : \_$  is  $( E \ \& \ E )$



Special cases of **binary** operators which **start and end with  $\_$**  and have **precedence value  $> 0$**  :

**(e E)** if it has the `assoc` attribute

If not, we have to look at the subsorts relationship...

# Default gathering values

If we have `Int < IntList`

<code>op _&lt;:_ : Int IntList -&gt; IntList .</code>		<code>(e E)</code>
<code>op _:&gt;_ : IntList Int -&gt; IntList .</code>		<code>(E e)</code>

# What's next ?



Demo

# References

1. Didier Buchs, modelisation verification course material, 2018
2. Dimitri Racordon, Emmanouela Stachtiri, Damien Morard, Didier Buchs, Functional Block Programming and Debugging, 2020
3. Nachum Dershowitz, Jean-Pierre Jouannaud, Rewrite Systems, 1990
4. Nachum Dershowitz, Computing with Rewrite Systems, 1985
5. Terese, Term Rewriting Systems, 2003
6. Thomas Sternagel and Harald Zankl, KBCV-Knuth-Bendix Completion Visualizer, 2012
7. Thomas Artsa, Jürgen Giesl, Termination of term rewriting using dependency pairs, 2000

# References

8. Jürgen Giesl, René Thiemann, Peter Schneider-Kamp, Stephan Falke, Automated Termination Proofs with AProVE, 2004
9. D. Kapur, P. Narendran, Path ordering for proving termination of term rewriting systems, 1985
10. Jeremy Dick, John Kalmus and Ursula Martin, Automating the Knuth Bendix ordering, 1990
11. E. Contejean, P. Courtieu, J. Forest, O. Pons, X. Urbain, Automated Certified Proofs with CiME3, 2011
12. F. Chalub, C. Braga, Maude MSOS Tool, 2005
13. S. Winkler, A. Middeldorp, Tools in Term Rewriting for Education, 2020
14. A. Salvador, L. Salvador, Term Rewriting Systems .Net Framework, 2013

# References (links)

## Database of Rewriting Systems

- <http://rewriting.loria.fr/systems.html>
- <http://www.jaist.ac.jp/~hirokawa/tool/>

## Knuth-Bendix Completion Visualizer

- <http://cl-informatik.uibk.ac.at/software/kbcv/>

## Knuth-Bendix Completion subject-based thesis

- <https://homepage.divms.uiowa.edu/~astump/papers/thesis-wehrman.pdf>

# References (links)

Prolog implementation of the Knuth-Bendix completion procedure

- <https://www.metalevel.at/trs/>

Maude tools

- <http://maude.lcc.uma.es/CRChC/>
- <http://www.lcc.uma.es/%7Eduran/MTT/>
- <http://maude.sip.ucm.es/debugging/>

Wikipedia

- [https://fr.wikipedia.org/wiki/Compl%C3%A9tion\\_de\\_Knuth-Bendix](https://fr.wikipedia.org/wiki/Compl%C3%A9tion_de_Knuth-Bendix)
- [https://fr.wikipedia.org/wiki/Paire\\_critique](https://fr.wikipedia.org/wiki/Paire_critique)



# References (links)

TRS tool:

- <http://tfmserver.dsic.upv.es:8080/Home.html>

# Make FunBlocks alive

Marvin FOURASTIE

Master project