J-P GALLOIS,E FIEVET , A LAPITRE

gallois@albatros.saclay.cea.fr

AGATHA

Statemate specification analysis and automated test generation

- Validation and Test from Specification
- Calculus Explosion : Problems and Solutions
- Architecture and Mechanism of AGATHA
- Examples
- STATEMATE/AGATHA connexion

AGATHA

Automata languages :

ESTELLE

SDL

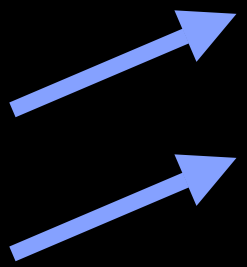
STATECHARTS

AGATHA

INDUSTRIAL TOOLS

ObjectGEODE & TAU

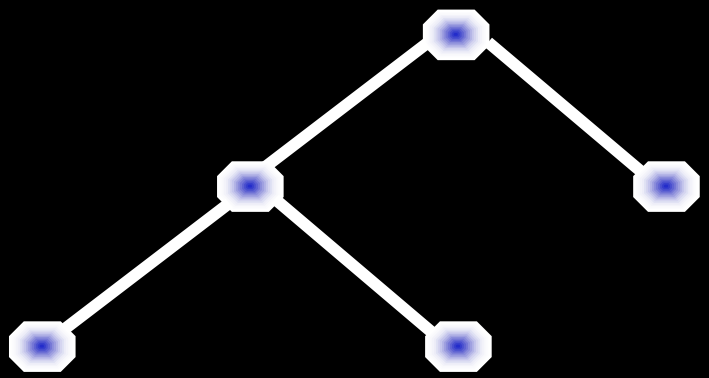
STATEMATE



AGATHA

Automata

Formal Model:
SDL, STATECHARTS...



Objectives :

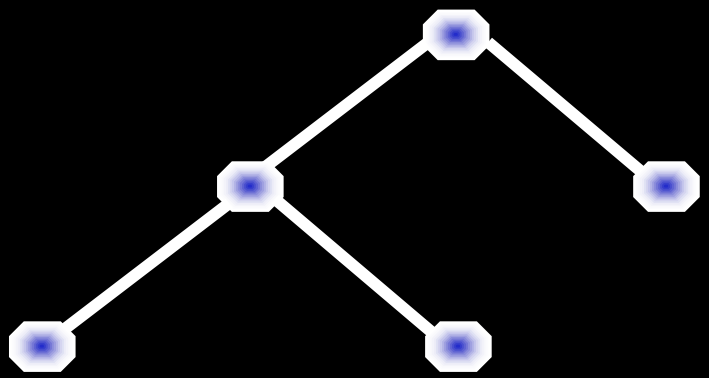
- **Validation**
- **Verification of Properties**
- **Test Generation**

AGATHA

Automata

Verification : Model-Checking

Reduction of State Number :



- **BDD (symbolic calculus : boolean, finite domains)**
- **Polyhedric (abstractions : integers)**

AGATHA

GOAL :Validation & Test Generation

To check Behaviours of the system :

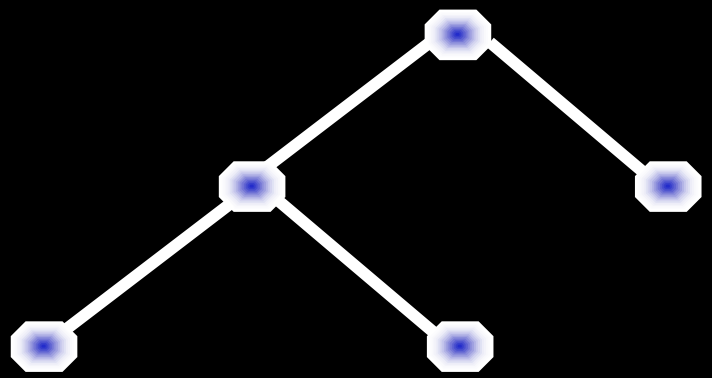
Validate them on specification (simulation)

Generate test to check the implementation (conformance testing)

AGATHA

Conformance testing : implementation

One test purpose = A property to test



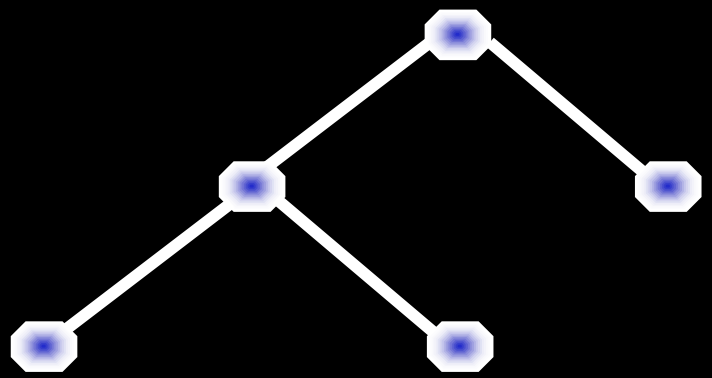
Test Purpose :
Reduce the State explosion

AGATHA

All systems behaviours : structural method

Branch coverage: possible but non exhaustive

Path coverage: exhaustive but impossible



To be Exhaustive :

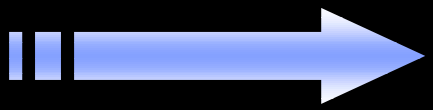
We need Path coverage

AGATHA

Path coverage => Big Calculus Explosion

Least Reduction: one test = one behaviour

Symbolic calculus (Automatic)



Abstractions (Manual & Automatic)

AGATHA

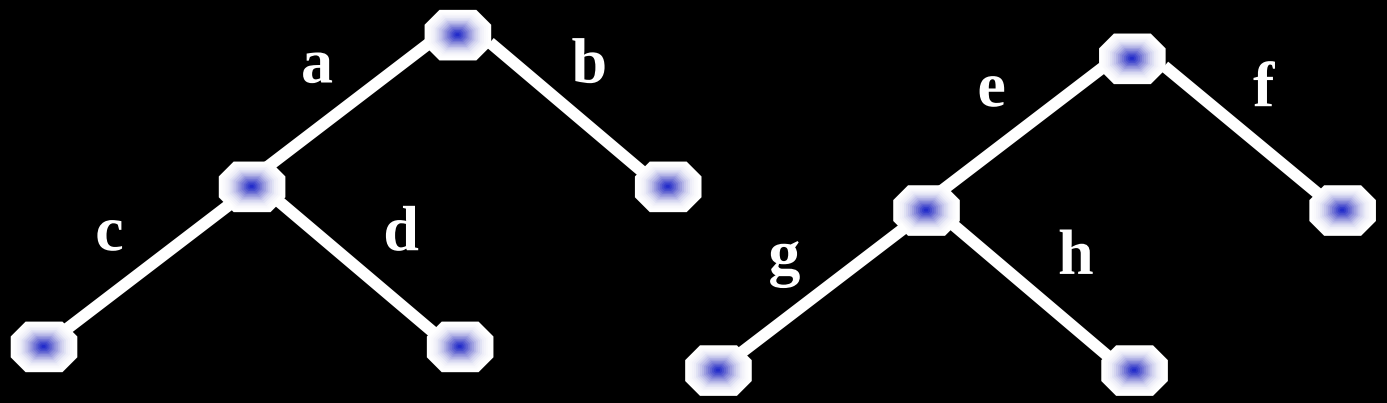
Path coverage

2 Factors of Calculus Explosion:

- **Parallelism**
- **Variables Impact**

AGATHA

Interleavings (Parallelism)



a c e g
or
a e c g
or
a e g c
Etc.

Partial Order Method : Preserve deadlocks

AGATHA

Variables Explosion

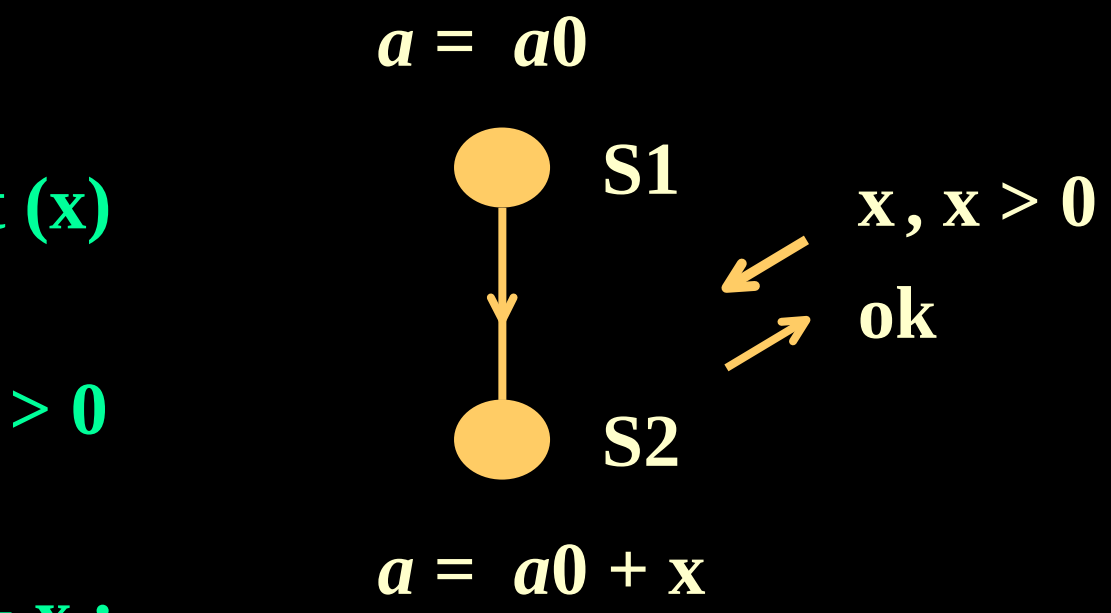
Symbolic calculus: SYMBOLIC EXECUTION

Symbolic Execution : Calculate symbolic states Tree (Lori Clarke, King, in years 70)

AGATHA

Example of Symbolic execution on a Transition

From S1
To S2
When input (x)
Output ok
Provided x > 0
Begin
    a : = *a* + x ;
End;



AGATHA

Extended Automata

Numerical State =

State
Numerical Values of Variables

Symbolic State =

State
Symbolic Values of Variables
Path Conditions

AGATHA

In the last example

For initial State :

Numerical = ***State*** **S1,** ***a*** **=** ***a*****0 = 0,**
Extended State = (S1, 0)

Symbolic = ***State*** **S1,** ***a*** **=** ***a*****0**
Extended State = (S1, ***a*****0)** → **include (S1,0)**

AGATHA

Extended State

Final State :

Numerical =

***State* S2, *a* = *a*0 + 1 = 1**
Extended State = (S1, 1)

Symbolic =

***State* S2, *a* = *a*0 + x, x > 0**
Extended State
(S1, *a*0 + x, x > 0)

→ **include (S1,1)**

AGATHA

Path Condition PC

PC = x > 0 → Condition on the entries

Second transition *a = a + y, y < 0*

a = *a*0 + x + y, x > 0, y < 0

PC = x > 0 *and* y < 0

IF y = x THEN

PC = *(* x > 0) *and* (x< 0) = FALSE

→ This branch is suppressed

AGATHA

Symbolic execution

Symbolic Tree

→ Set of Symbolic States

Symbolic States

→ State,Symbolic values of variables, Path Condition

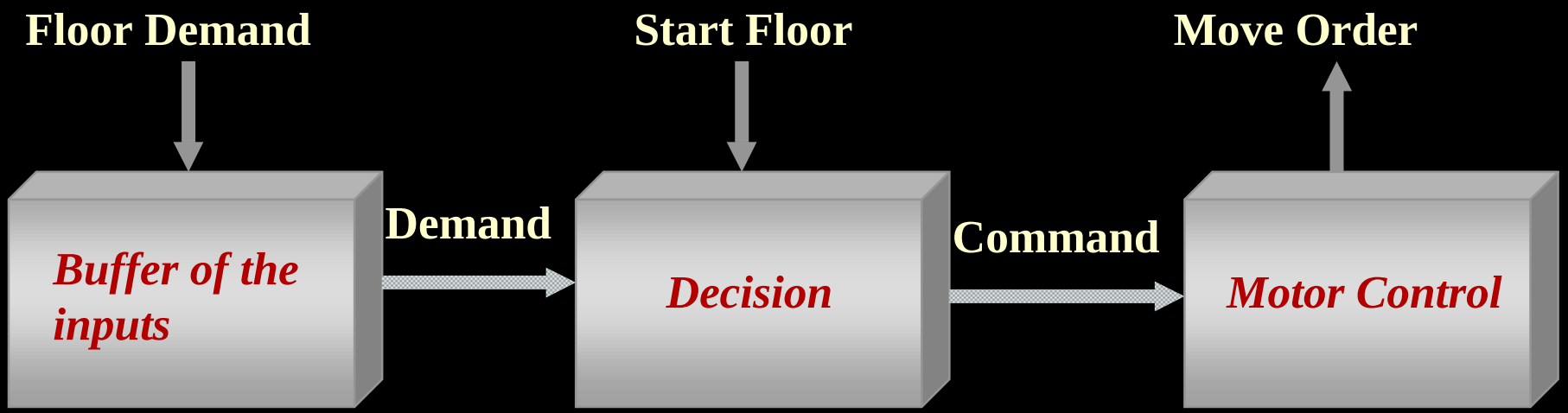
Criteria of Stop

→ Symbolic State Loop

AGATHA

The Elevator

3 Parallel Automatas communicating



AGATHA

The Elevator

Two parameters

Start Floor

Required Floor

Domain of variation

Set of Floors, which cardinality is N

AGATHA

The Elevator

Enumerated Calculus

If FIFO size = 1

Law in N^2

If FIFO size = P

Law in N^{P+1}

AGATHA

The Elevator

Symbolic Calculus

FIFO size = 1

Constant

FIFO size = P

Law in P^2

AGATHA

PCCN

Protection and Numerical Control and Command

Electrical Distribution

- Circuit Breakers
- Set of Circuit Breakers

Their number are variable

- Explosive Numerical Calculus

AGATHA

PCCN

5 Modules - 50 Variables – 1500 lines of ESTELLE

Solution : Abstract Circuit Breakers and Sets (permutations)

Numéric

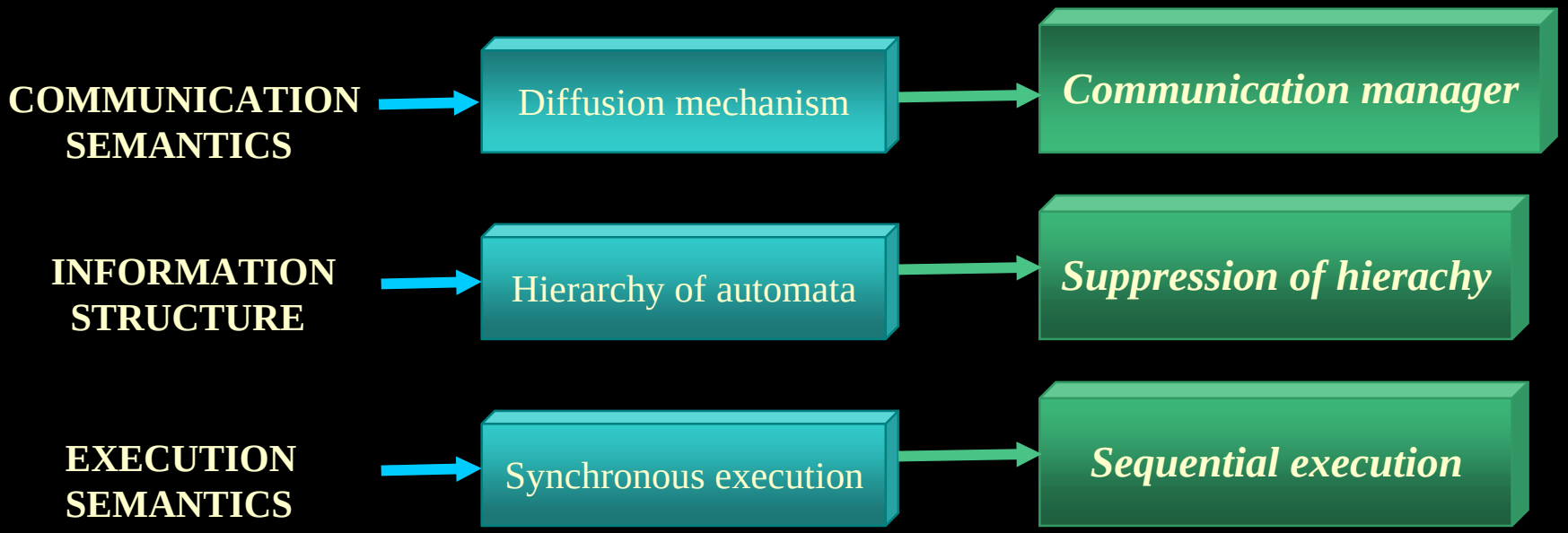
10^{13} States

Symbolic

28 Pathes of a few 10 States, which means
less than 1000 symbolic states

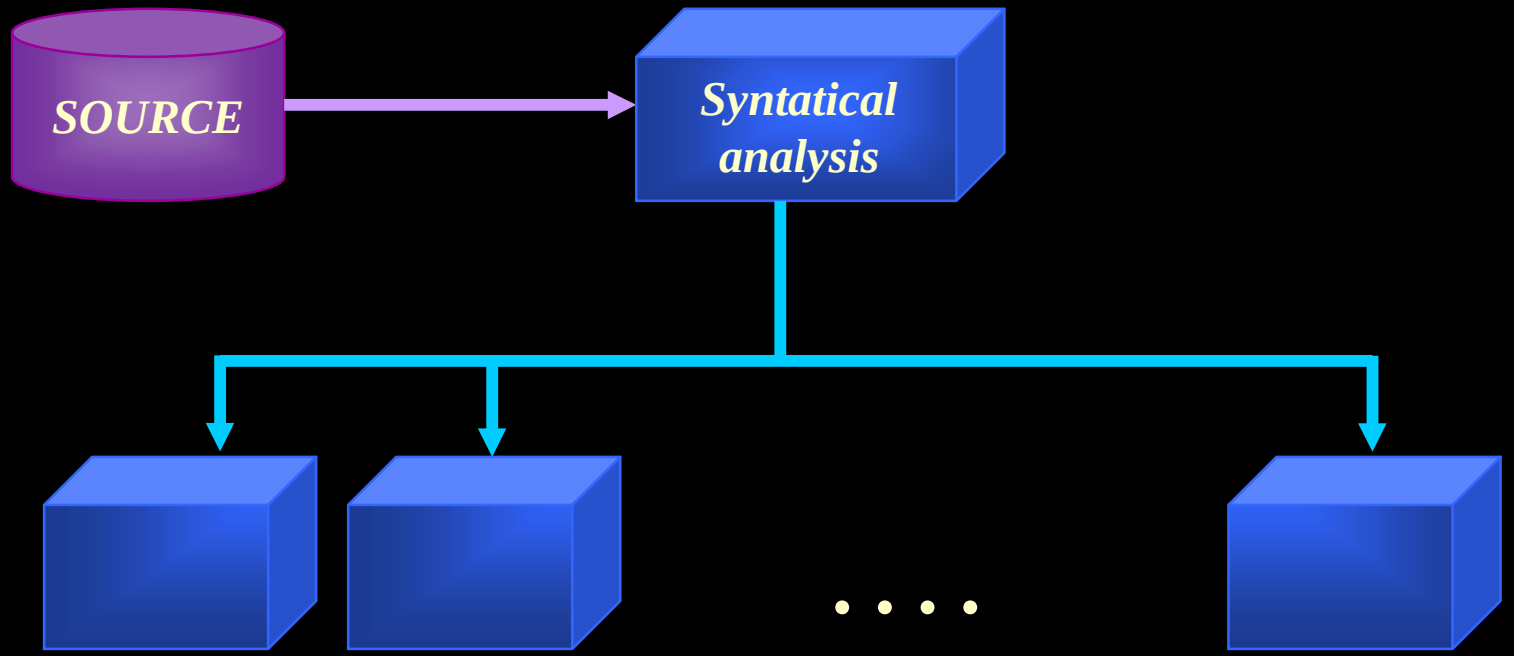
AGATHA

Differences between STATECHARTS and other classical automata



AGATHA

STATECHARTS ANALYSIS

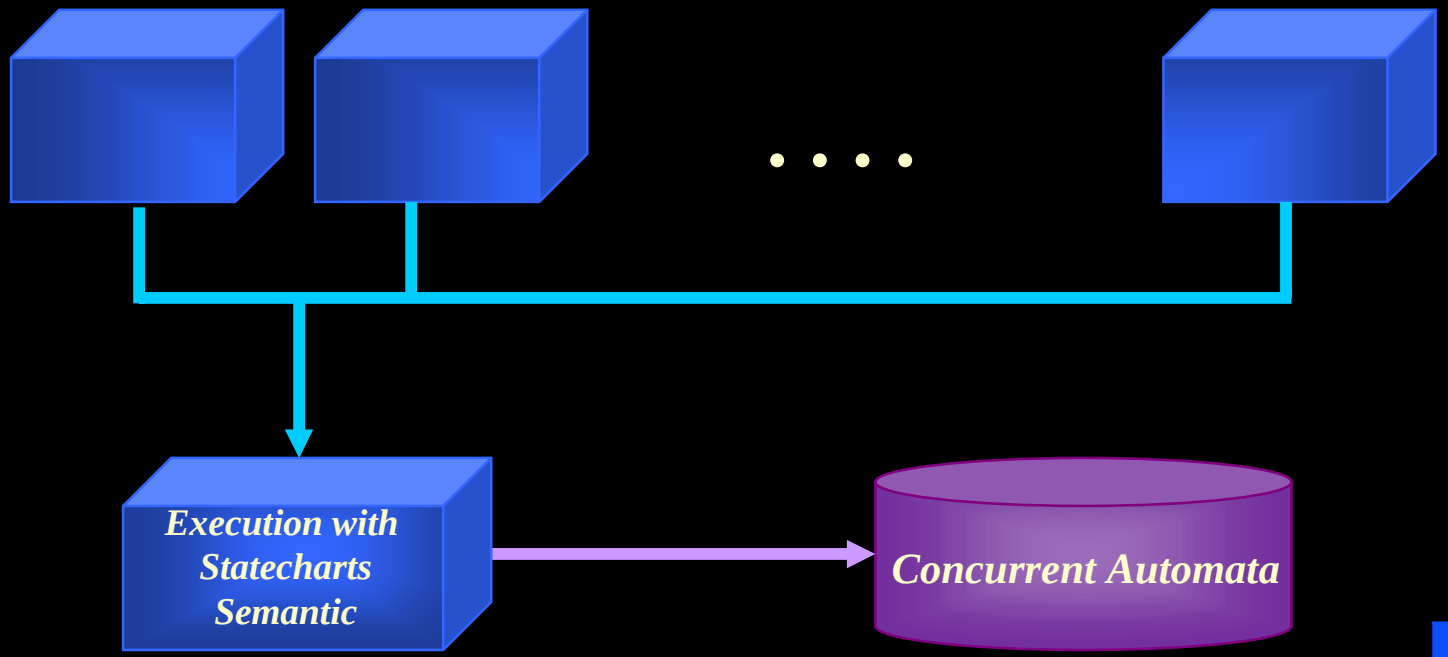


N Hierarchical Automata

AGATHA

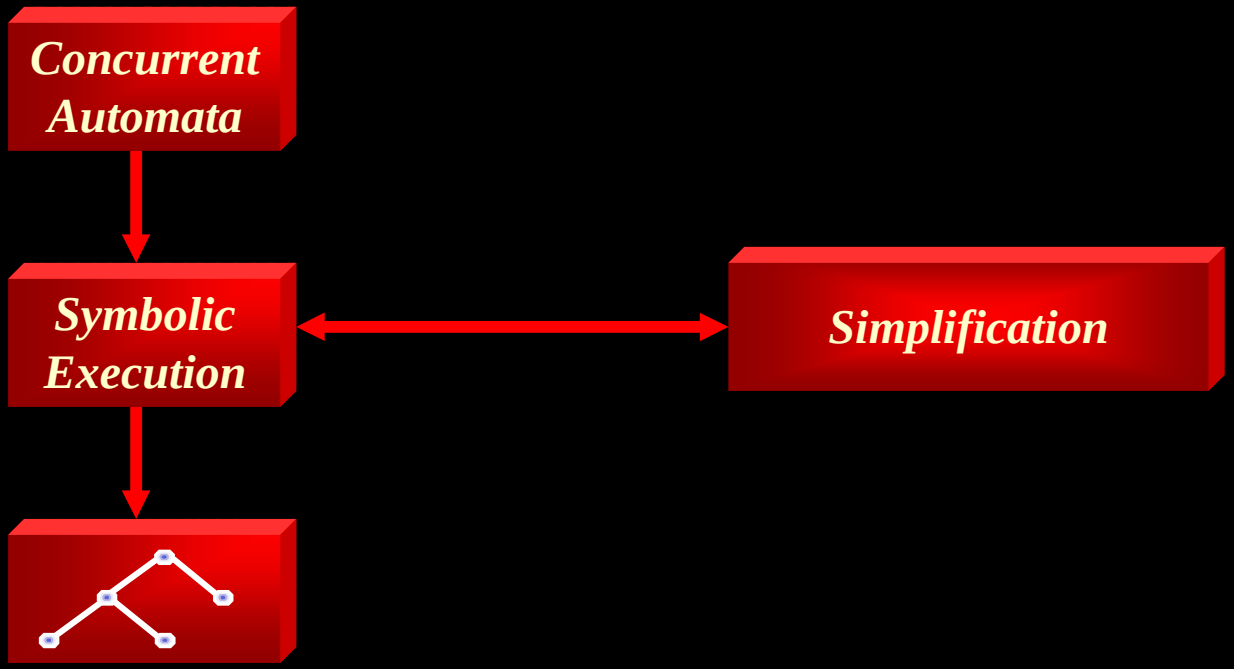
Calculus with statecharts without data

N hierarchical Automata



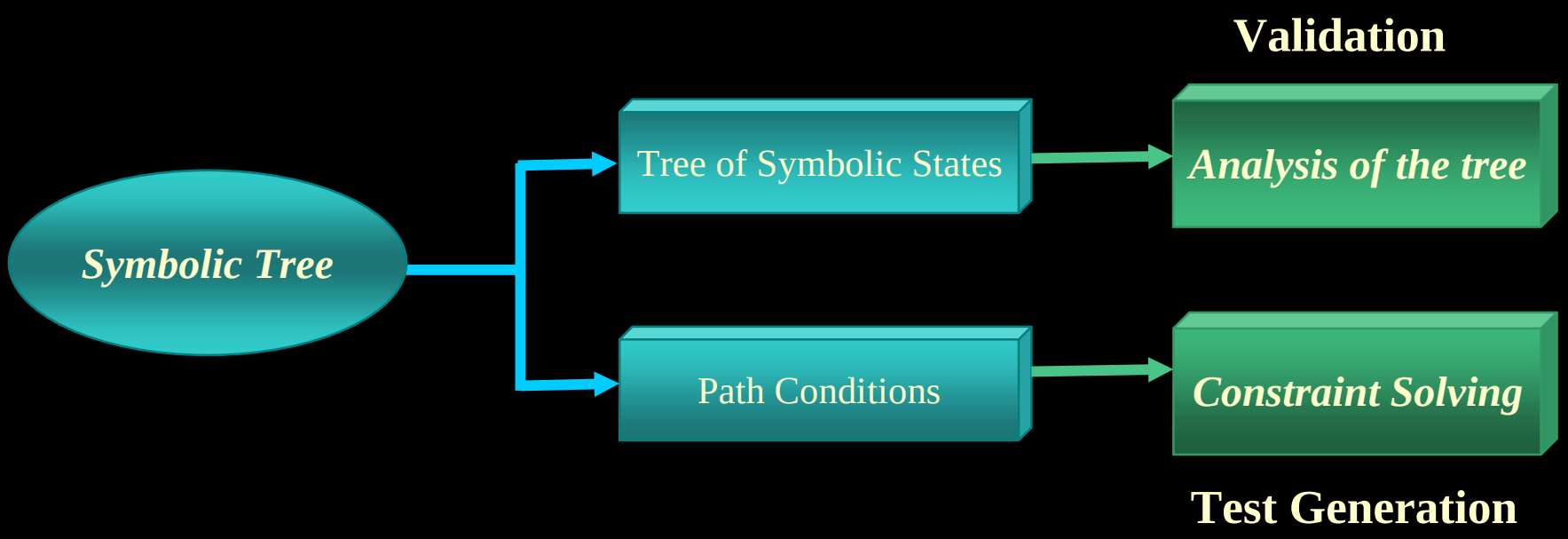
AGATHA

Calculus with data : re-execute the model with data



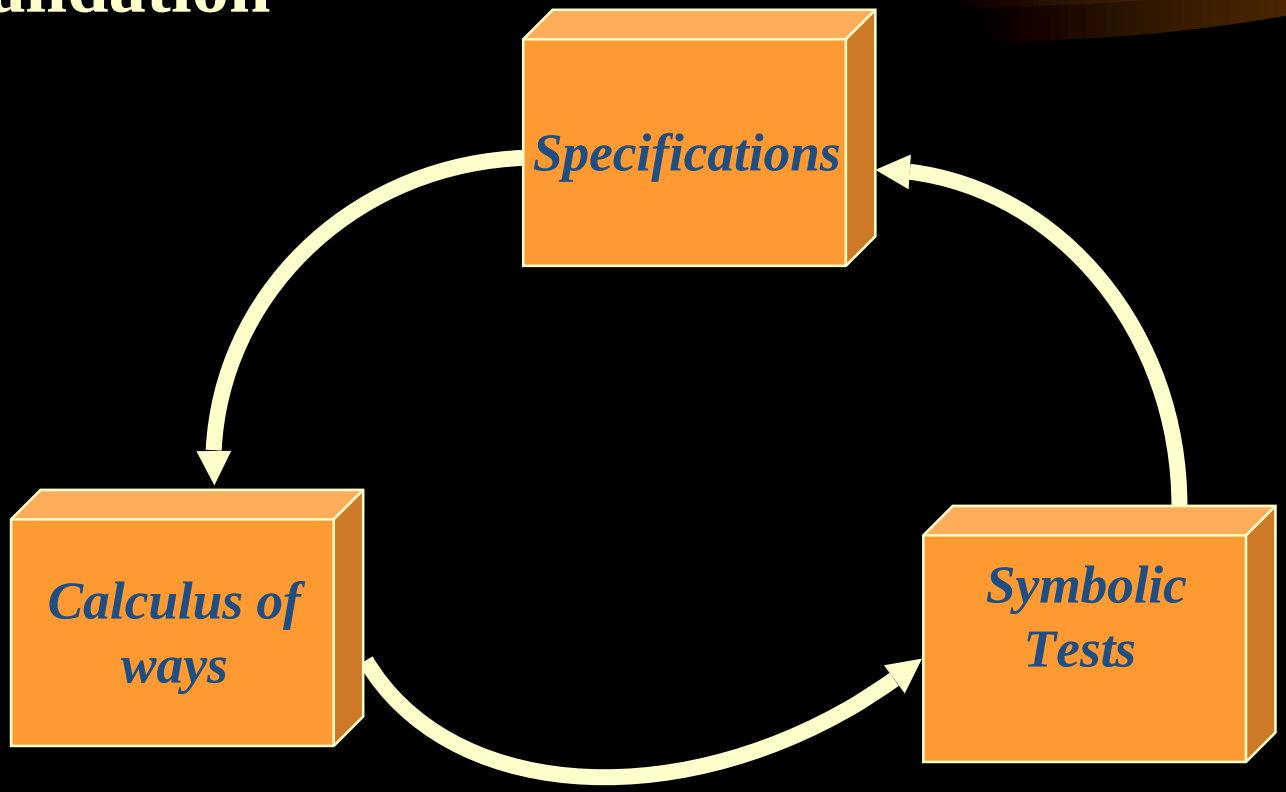
AGATHA

Final Result



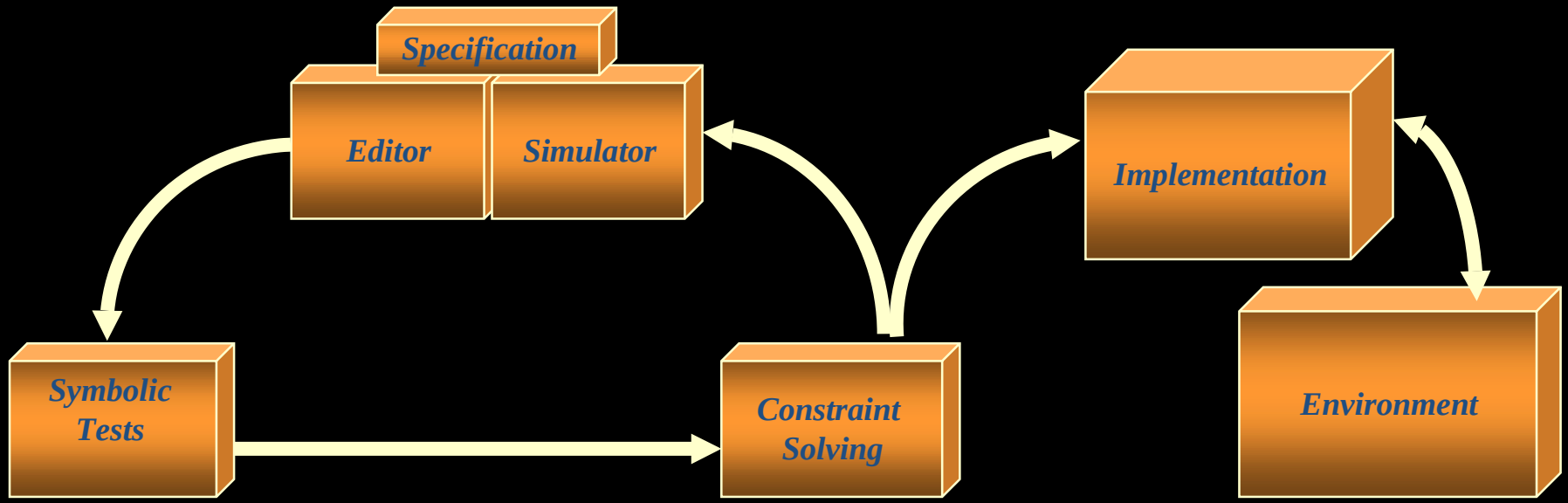
AGATHA

Validation



AGATHA

Test Generation



FIN