# CADP Construction and Analysis of Distributed Processes

#### **ETAPS Test-of-time Tool Award 2023**

Hubert GARAVEL Frédéric LANG Radu MATEESCU Wendelin SERWE







#### **CADP Objectives**

- Formal analysis of concurrent systems: design-error detection: safety, security, correctness
- Message-passing communication
- Wide usage in various (3<sup>rd</sup> party) research work:
   > 200 case studies
   > 100 research tools



#### **CADP in Practice**

- Comprehensive software package:
   59 tools, 18 libraries, 630 pages of documentation
- Continuously improved since 1987
- Rolling release schedule (one per month)
- 6 supported 32/64-bit architectures (Linux, macOS, Solaris, Windows)
- Worldwide distribution
- https://cadp.inria.fr



# **Principal Modelling Language: LNT**

- Features
  - Uniform usual imperative syntax
  - Heavy use of static analysis (semantics & warnings)
  - Strong typing
- Concepts: expressions, instructions, behaviours
- Convenient translation target
- Development language of most compilers in CADP

```
process FILTER [GET: option_channel,
        PUT: nat_channel] (b: Nat) is
var opt: Option in
        loop
        GET (?opt) ;
        case opt var x: Nat in
        none -> null
        | some(x) where x > b -> PUT (x)
        end case
        end loop
        end var
end process
```

Positive feedback from academia and industry

# **Other Modelling Languages**

LOTOS (ISO standard 8807)

- Supported since the beginning of CADP
- Current target of the LNT tool chain
- **FSP** (Finite State Processes)

Language of the LTSA tool

EXP (networks of communicating automata)

Synchronization vectors as generic composition means

- Common features
  - Labelled Transition Systems semantics
  - Parallel composition, interleaving, rendezvous

# **Visual Checking / Simulation**

- Manipulation of explicit LTS
  - Compact storage (BCG format)
  - ► Visualization
- Step-by-step simulation
  - ▶ Backtracking
  - Save & load simulations
- Random simulation





# **Equivalence Checking**

- LTS comparison and reduction/minimization
- Various relations and preorders, including
  - strong bisimulation
  - (divergence-preserving) branching bisimulation
  - (weak) trace equivalence
  - probabilistic/stochastic variants

#### Basis for compositional techniques



# **Model Checking**

- XTL (on LTS in the BCG format): functional language for graph traversals
- MCL (on-the-fly)
  - regular alternation free μ-calculus
  - macro libraries for CTL, ACTL, …
  - infinite looping operator
  - regular expressions on action sequences
  - action predicates with data-handling constructs
  - probabilistic extensions



```
NEVER (
    (not { PUT ?any })* .
    { PUT ?m<sub>1</sub>:Nat } .
    (not { GET ?any })* .
    { GET ?m<sub>2</sub>:Nat
        where m<sub>1</sub> <> m<sub>2</sub> }
}
```

# **Distributed Tools**

Distributed state space generation

- Use memory of up to hundreds of computers
- Good speed-up
- Manipulation of distributed state spaces
- Distributed solving of Boolean equation systems

(distributed model- and equivalence checking)



<u>Overview</u>	Labels	Progress	s <u>S</u> tatistics <u></u>	Resources		
	Hosts		Explored States	Remaining States	Transitions	Variatio
chinqchint-9.lille.grid5000.fr		165428	1698	1043000		
chinqchint-25.lille.grid5000.fr		170529	9475	1063000		
econome-3.nantes.grid5000.fr			163321	10454	1051000	
econome-5.nantes.grid5000.fr			169938	4467	1070000	
genepi-27.grenoble.grid5000.fr			169763	11149	1072000	
genepi-29.grenoble.grid5000.fr			171719	27670	1101000	
griffon-8.nancy.grid5000.fr			171460	50449	1094000	
griffon-85.nancy.grid5000.fr		153841	67795	1002000		
sol-8.sophia.grid5000.fr		172277	3435	1118000		
sol-9.sophia.grid5000.fr		160818	13689	1055000		
stremi-5.reims.grid5000.fr		154833	48895	1002000		
stremi-7.reims.grid5000.fr		171505	54835	1104000		
stremi-9.reims.grid5000.fr		172909	69826	1089000		
stremi-35.reims.grid5000.fr			153477	43638	978000	
suno-12.sophia.grid5000.fr			169408	4115	1079000	
suno-13.sophia.grid5000.fr			170017		1046000	
taurus-2.lyon.grid5000.fr			173015	8186	1065000	
taurus-9.lyon.grid5000.fr			167511	4358	1059000	

Hosts	Visited States	Number
hinqchint-9.lille.grid5000.fr		175057
inqchint-25.lille.grid5000.fr		198325
onome-3.nantes.grid5000.fi	·	199651
onome-5.nantes.grid5000.fi	·	201996
nepi-27.grenoble.grid5000.fi	r	203272
nepi-29.grenoble.grid5000.fi		186483
riffon-8.nancy.grid5000.fr		183960
iffon-85.nancy.grid5000.fr		204958
sol-8.sophia.grid5000.fr		194509
sol-9.sophia.grid5000.fr		193091
tremi-5.reims.grid5000.fr		195624
aremi-7.reims.grid5000.fr		182463
tremi-9.reims.grid5000.fr		194007
tremi-35.reims.grid5000.fr		193484
uno-12.sophia.grid5000.fr		178893
uno-13.sophia.grid5000.fr		196150
aurus-2.lyon.grid5000.fr		177846
taurus-9.lyon.grid5000.fr		193113

# **Compositional Verification**

- Divide and conquer principle: generate, reduce, and compose components hierarchically
- Heuristics to select composition order
- Semi-composition using interfaces
- Property-dependent reductions
- Success stories
  - [ASYNC18] 146 LNT processes, 660 concurrent units, semicomposition, intermediate LTSs below 116 Mstates
  - [RERS2019] up to 70 automata (each with up to 153 states), new sharp bisimulation, property dependent reduction



# **Conformance Testing**

- Model-based testing: model as *test oracle*
- ioco conformance relation
- Test purpose to guide on-the-fly test case generation
- Coverage guarantees
- EXEC/CÆSAR framework simultaneous execution of the model and an implementation



### **Software Libraries**

- Manipulation of binary LTS format
- Auxiliary data structures: hash table, bitmap, cache, stack, hiding/renaming, ...
- Common algorithms: BES solving
- Extensive documentation
- Example: components of a test generation tool



## **User Interfaces**

- Convenient access to tools
- Eucalyptus GUI
  - Contextual menus
  - Well-chosen default values
- SVL (Script Verification Language)

EME	EUGA	EVPTUS Taaliset	L5 B
File View Detione	Eucalyptus	s Toolset (Version 2.3)	Heb Help
Leventional Equivalence     Series     Series	entre formation and and and and and and and and and an	Ranits limits         Rill         Error           [concerted polyage 5 (p. Arge/pase_241.2005, Long         Images in the second polyage for the second polyage in th	<ol> <li>С Азанти/зитритии/</li> <li>С Азанти/зитритии/</li> <li>0.001.100/01/*</li> <li>1.001.1000/*</li> <li>1.001.1000/*</li> <li>1.000/*</li> <li>1.000/*</li> <li>1.000/*</li> <li>1.000/*</li> <li>1.000/*</li> <li>1.000/*</li> <li>1.000/*</li> <li>1.000/*</li> </ol>
ding File (optional)	Brouns	"IM_BUS_OP INLIFUGHICO" "PROBE_TRANSFER INLIFUGHICO"	00-
wawing File (optional)	Irons	"FREE_ING ING ING TRUGHT NO "FREE_UNIT ING TRUGHT NO "BUG TRANS INL INRITE FLUSH NA"	
Reduce using Fc2tools		"PRIDET TRANSFER INLING INCLAM INCLOLE TIMUTO" "PRIDET TRANSFER INLING INCLAM ING INETRESP_NIL IDUTION IN "BUG_TRANS ING IRAUTH INC"	o
Reduction Relation Strong Equivalence Branching Equivalence Medi Equivalence	5	"UBLIGET HIM IDITIO IAO IAO HOC.SH IFLAG (FALSE, TRUE) HO "ALDAG EMPORY" Cohedlook?	X-00L (0010"
Decision Hethod Standard V Bina	ry lectrics liegram		
_DKCo	ncel		

- Integration of verification, properties, and shell commands
- Automatic advanced verification heuristics
- Support for compositional techniques



# **Quality Control and Support**

- Code review before integration
- Nightly test of demo examples
- Large collections of models and properties
  - CONTRIBUTOR tool for automatic gathering of examples
  - Example provider for benchmarks and model repositories (<u>VLTS</u>, <u>VLSAT</u>, <u>MARS</u>)
  - Benchmark provider for tool competitions (MCC, SAT competition, SMT-COMP, Model Counting)
- Support tools
  - INSTALLATOR: graphical installer
  - **TST**: diagnostics of installation problems
  - UPC: upgrade specifications following language changes



## **Conclusion: Salient CADP Features**

- Sophisticated rich modelling languages with explicit parallelism and general data types
- Action-based branching-time logics
- Model checking and equivalence checking
  - ► On-the-fly algorithms
  - Distributed tools
  - Compositional approaches
- Smooth combination of all techniques

"Concurrency theory in practically usable tools"

# **More Information about CADP**

- Website: <u>https://cadp.inria.fr</u> demo examples, documentation, current status, ...
- User forum: <u>https://cadp.forumotion.com</u>
- Overview [Garavel-Lang-Mateescu-Serwe-13]
- Awards
  - ▶9 gold medals at RERS competitions (2019 & 2020)
  - Innovation award (French Académie des sciences, 2021)
  - ETAPS Test-of-time Tool (2023)
- To obtain a free academic license <u>https://cadp.inria.fr/registration</u>

