Symbolic Model Checking of Labelled Transition Systems: a case study

MoVES FUNDP-UCL Presentation Meeting

25 May 2007

José Vander Meulen, UC Louvain

Introduction

- "NuSMV with Actions" was never applied to process algebras
- Turntable system for drilling products
  - "real life" example
  - easy to scale
  - baseline from Mateescu (CADP)
- Objectives of this case study
  - Evaluation of "NuSMV with Actions"
  - From process algebra to NuSMV
  - Also familiarization with model-checking techniques and with "NuSMV with Actions" source code.

Turntable system for drilling products

- Case study from CADP (Verimag INRIA)

- From Lotos to “NuSMV with Actions”
- Difficulty to model synchronization in NuSMV.
  - Lotos has an operator of parallel composition, and a concept of process synchronization by rendez-vous

  - NuSMV has no concept of rendez-vous synchronization
    - synchronous or asynchronous processes
    - synchronization have to be explicitly encoded using shared variables

Turntable system for drilling products

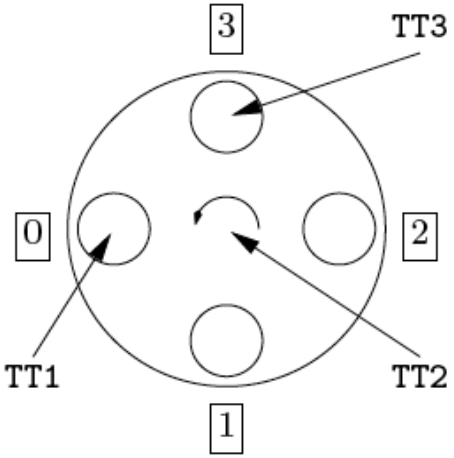
- From regular alternation-free mu-calculus formulas to Action Restricted CTL

- A safety property:

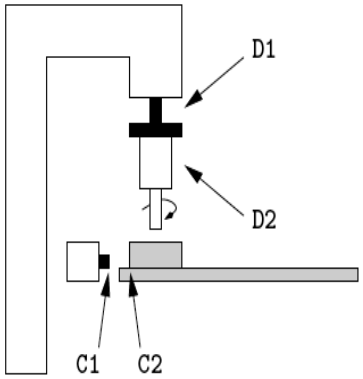
```
[ true* . "INF !DRILLED" .
(not 'INF !UNLOCKED')* ."CMD !TURN"] false

!E[TRUE U
 (EAX(action = INF_Drilled)
   (EA(action != INF_Unlocked)
      [TRUE  U
          (EAX(action = CMD_Turn)( TRUE ))
      ]
))]
```

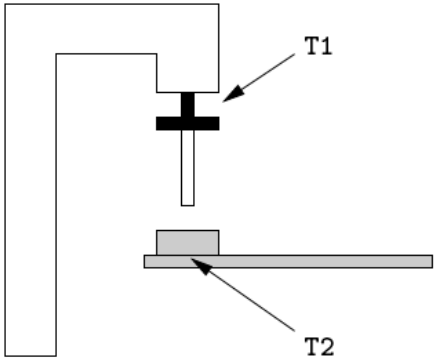
Turntable system for drilling products



Turn Table



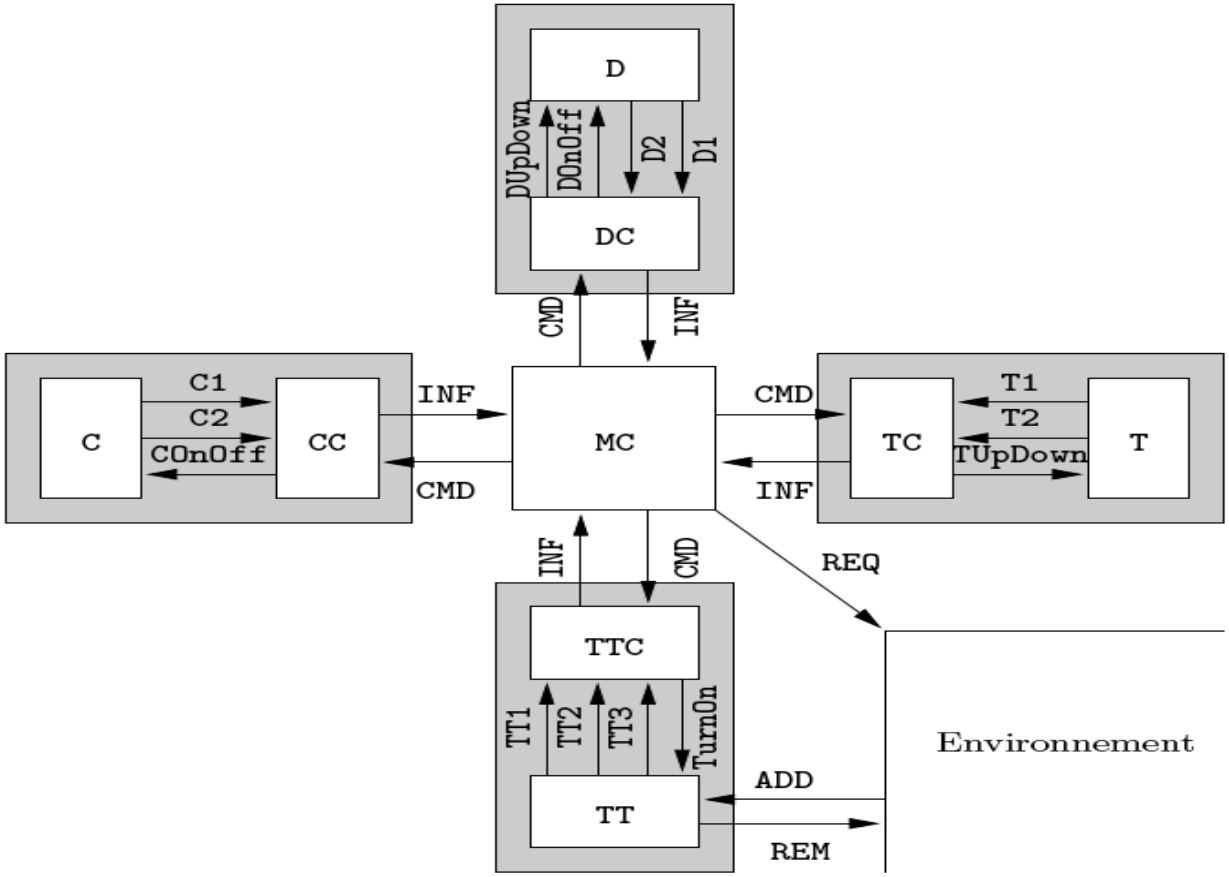
Drill



Tester

Modélisation et analyse de systèmes asynchrones avec CADP, Radu Mateescu, 2006

Turntable system for drilling products (II)



Architecture

Modélisation et analyse de systèmes asynchrones avec CADP, Radu Mateescu, 2006

Number of States

- Number of states from the NuSMV model.
  - cadp gives similar results

	1 drill	2 drills	3 drills	4 drills
states	≈ 10^4	≈ $1.7*10^5$	≈ $2*10^6$	≈ $4.4*10^7$
BDD variables	123	165	207	250

Evaluation

- **14 properties were checked**
  - **7 liveness properties**
  - **7 safety properties**

	1 drill		2 drills		3 drills	
	CADP	NuSVM	CADP	NuSVM	CADP	NuSVM
1	3s	2 s.	7s	42s.	2,5 m.	14m
2	3s	2 s.	5s	43s.	1 m	14m
4	3s	2 s.	7s	42s.	2 m	14m
9	4s	4s	8s	46s.	3 m	15m
14	4s	7s	13s	2,5 m.	3,5 m	41m

How to reduce the checking time?

- **Within BDD model checking**
  - **Variable ordering strongly impacts the size of the model**
  - **Explore the minimization of the model modulo weak equivalence**
  - **Explore the Partial Order Reduction in Symbolic Model Checking**
- **Use Sat-based bounded model checking**

Perspectives

- Encode process algebras into BDD
- Encode action-based temporal logics such as PDL, ACTL into BDD-based model checking
- Consolidate and distribute “NuSMV with Actions”
- Generalize to game-theoretic logics such as ATL