

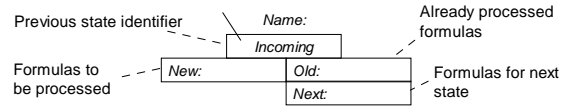


Translating LTL to Automata

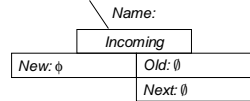
Literature: Peled ch. 6.8 – end of 6

Mads Dam

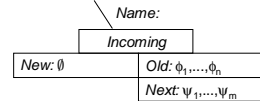
Automaton State



Initial nodes:



Final nodes = automaton states:



Positive Form

Positive form: Negation only on primitive state assertions:

$$\phi ::= \eta \mid \neg\eta \mid \phi \wedge \psi \mid \phi \vee \psi \mid \phi \cup \psi \mid \phi \vee \psi \mid O\phi$$

Rewriting procedure:

$$\begin{aligned} \neg\neg\phi &\Rightarrow \phi & \neg(\phi \vee \psi) &\Rightarrow (\neg\phi) \cup (\neg\psi) \\ \neg(\phi \wedge \psi) &\Rightarrow \neg\phi \vee \neg\psi & \neg(O\phi) &\Rightarrow O\neg\phi \\ \neg(\phi \vee \psi) &\Rightarrow \neg\phi \wedge \neg\psi & \langle \rangle\phi &\Rightarrow \text{true} \cup \phi \\ \neg(\phi \cup \psi) &\Rightarrow (\neg\phi) \vee (\neg\psi) & []\phi &\Rightarrow \text{false} \vee \phi \end{aligned}$$

Context C[]:

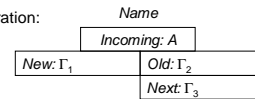
Formula (term) with a "hole" []

Rule of substitutivity:

$$\frac{\phi \Rightarrow \psi}{C[\phi] \Rightarrow C[\psi]}$$

Base Step

Current configuration:



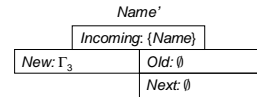
Condition: $\Gamma_1 = \emptyset$ (all formulas have been processed)

Is there node *Name'* with identical *Old*, *Next*?

- Then discard *Name* and add *Name'.Incoming* to *Name'.Incoming*

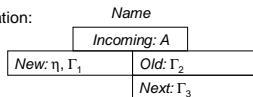
Otherwise:

- *Name* is a new state
- Create new name and node:



Case: Proposition Symbol

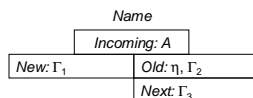
Current configuration:



Is $\neg\eta \in \Gamma_2$?

Yes: Discard the node

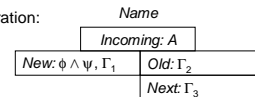
No: Next configuration:



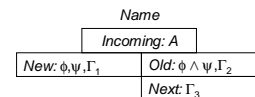
Case for $\neg\eta$ in *New* is similar

Case: Conjunction

Current configuration:

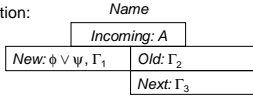


Next configuration:

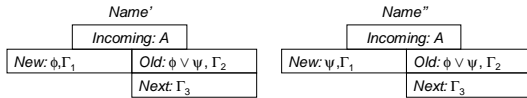


Case: Disjunction

Current configuration:



Configuration split into two:



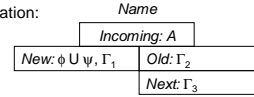
2005 Mads Dam IMIT, KTH

7

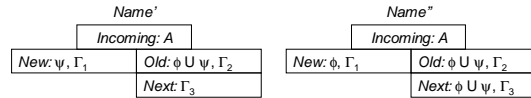
2G1516 Formal Methods

Case: Until

Current configuration:



Configuration split into two:



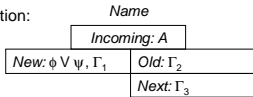
2005 Mads Dam IMIT, KTH

8

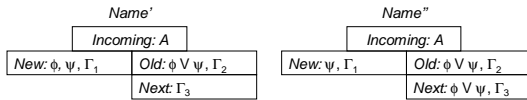
2G1516 Formal Methods

Case: Release

Current configuration:



Configuration split into two:



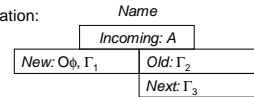
2005 Mads Dam IMIT, KTH

9

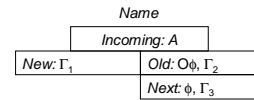
2G1516 Formal Methods

Case: Next

Current configuration:



Next configuration:



2005 Mads Dam IMIT, KTH

10

2G1516 Formal Methods

Constructing the Automaton

Automaton: $(Q, \Sigma, \Delta, I, F)$

- Σ = truth assignments of propositional symbols in ϕ
Ex: $\{a, b, \neg c, \neg d\} \in \Sigma$
- Q = {final nodes} = $\{q \mid q.New = \emptyset\}$
- $\Delta = \{(q, \alpha, q') \mid q.Name \in q'.Incoming \text{ and } \{\eta \mid \eta \in q'.Old\} \subseteq \alpha \text{ and } \{\neg\eta \mid \neg\eta \in q'.Old\} \subseteq \alpha\}$
- $I = \{q\}$, q special initial node to kick off construction
- Generalized Buchi automaton acceptance set $F = \{f_1, \dots, f_n\}$:
Each f_i determined by subformula of shape $\phi_i \cup \psi_i$
 $f_i = \{q \mid \text{either } \psi_i \in q.Old \text{ or } \phi_i \cup \psi_i \notin q.Old\}$

2005 Mads Dam IMIT, KTH

11

2G1516 Formal Methods

Complexity

Let ϕ be given LTL formula

Size of state is $O(|\phi|)$
Size of automaton is $O(2^{|\phi|})$

- Alternative construction can be given such that
1. States can be recognized in poly time and space
 2. Transitions can be recognised in poly time and space

- Then complexity of deciding satisfaction is
- Polynomial for Buchi automata
 - (use a binary search procedure)
 - PSPACE complete for LTL
 - NONELEMENTARY for monadic 2nd order logic

But keep in mind the state space explosion problem!

2005 Mads Dam IMIT, KTH

12

2G1516 Formal Methods

State Space Explosion

[Global state space]: exponential in number of component processes

Strategies: BDD's:

- Symbolic representation of states, as DAG's

Partial order reduction:

- Recognise states reached by different interleavings



- Symmetry reductions

2005 Mads Dam MIT, KTH

13

2G1516 Formal Methods