LTL to Buchi

Ralf Huuck

The imagination driving Australia's ICT future. NATIONAL ICT AUSTRALIA

Overview

- Buchi
- Model Checking LTL
- Translating LTL into Buchi

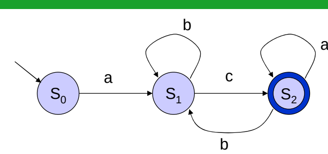
The imagination driving Australia's ICT future. NATIONAL ICT AUSTRALIA

Buchi Automata

- Automaton which accepts infinite traces δ
- A Buchi automaton is 5-tuple $\langle \Sigma, Q, Q_0, \delta, F \rangle$
  - Σ is a finite alphabet
  - Q is a finite set of states
  - $Q_0 \subseteq Q$ is a subset of initial states
  - $\delta: Q \times \Sigma \to \mathcal{P}(Q)$ is a transition relation
  - $F \subseteq Q$ is a subset of accepting states
- An infinite sequence of states is accepted iff it contains accepting states infinitely often

The imagination driving Australia's ICT future. NATIONAL ICT AUSTRALIA

Example



$\sigma_1 = S_0 S_1 S_2 S_2 S_2 S_2 \ldots$ ACCEPTED

$\sigma_2 = S_0 S_1 S_2 S_1 S_2 S_1 \ldots$ ACCEPTED

$\sigma_3 = S_0 S_1 S_2 S_1 S_1 S_1 \ldots$ REJECTED

Model Checking LTL

Basic idea:

A_{sys} automaton describing system
ϕ LTL specification
A_{ϕ} automaton representing ϕ exactly

check

$L(A_{sys}) \subseteq L(A_{\phi})$

Model Checking LTL

Basic idea:

A_{sys} automaton describing system
ϕ LTL specification
A_{ϕ} automaton representing ϕ exactly

check

$L(A_{sys}) \cap L(A_{\neg\phi}) = \emptyset$

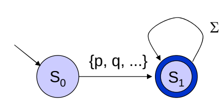
negation

Key Problem

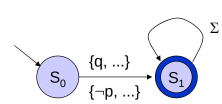
How translate LTL formula into Buchi automaton?

Easy for Non-Temporal

$p \wedge q$



$p \Rightarrow q$



How to do it for temporal formulas?

The imagination driving Australia's ICT future.

Different Approaches

e.g.:

- tableau construction
  - Kersten, Manna, McGuire, Pnueli
  - Gerth, Peled, Vardi, Wolper
- local/eventuality automaton
  - Vardi, Wolper
- automata theoretic
  - Vardi

different ways to tackle, all are not simple and straightforward ☹

The imagination driving Australia's ICT future.

Construction via Local/Eventuality Automaton

The imagination driving Australia's ICT future.

Idea

1. reducing number of temporal LTL operators to U, and X for any LTL formula ϕ
2. construct local automaton for ϕ
   - describes all possible behaviors that do not violate ϕ
   - does not guarantee "termination" of U
3. construct eventuality automaton for ϕ
   - accepts exactly terminating U
4. intersect both automata

The imagination driving Australia's ICT future.

LTL Syntax

LTL formula are inductively defined by:

$$\phi ::= p \mid \neg \phi \mid \phi_1 \vee \phi_2 \mid X\phi \mid F\phi \mid G\phi \mid \phi_1 U \phi_2$$

p denotes atomic proposition

X denotes next-state operator

F denotes eventually/finally

G denotes always/globally

U denotes until

LTL semantics

- LTL formula ϕ interpreted over infinite paths of states $\pi = s_0 s_1 s_2 \ldots$
- we define LTL wrt Kripke structure M
- $M,\pi \vDash \phi$ denotes ϕ holds in a path π of Kripke structure M.
- $M \vDash \phi$ iff all paths of M satisfy ϕ, i.e., for all π in M we have $M,\pi \vDash \phi$

Semantics of LTL Operators

let π^k denote suffix $s_k s_{k+1} s_{k+2} \ldots$ ($k \geq 0$)

- $M,\pi \vDash p$ iff $s_0 \vDash p$, i.e., $p \in \mu(s_0)$
- $M,\pi \vDash \neg\phi$ iff not $M,\pi \vDash \phi$
- $M,\pi \vDash \phi_1 \vee \phi_2$ iff $M,\pi \vDash \phi_1$ or $M,\pi \vDash \phi_2$
- $M,\pi \vDash X\phi$ iff $M,\pi^1 \vDash \phi$, i.e., $s_1 s_2 s_3 \ldots$ satisfies ϕ
- $M,\pi \vDash F\phi$ iff $\exists\, k \geq 0$ s.t. $M,\pi^k \vDash \phi$
- $M,\pi \vDash G\phi$ iff $\forall k \geq 0$ $M,\pi^k \vDash \phi$
- $M,\pi \vDash \phi_1 U \phi_2$ iff $\exists k \geq 0$ s.t. $M,\pi^k \vDash \phi_2$ and $\forall 0 \leq j < k$ we have $M,\pi^j \vDash \phi_1$

Reducing Number of Operators

- $F\phi$ can be expressed by true U ϕ
- $G\phi$ can be expressed by $\neg F \neg \phi$

Exercise: PROOF

Preliminaries (1)

closure $cl(\phi)$ of a LTL formula ϕ

- $\phi \in cl(\phi)$
- $\psi_1 \wedge \psi_2 \in cl(\phi)$, then $\psi_1, \psi_2 \in cl(\phi)$
- $\neg\, \psi \in cl(\phi)$, then $\psi \in cl(\phi)$
- $X\psi \in cl(\phi)$, then $\psi \in cl(\phi)$
- ψ_1 U $\psi_2 \in cl(\phi)$, then $\psi_1, \psi_2 \in cl(\phi)$

i.e., set of all sub-formulas and their negation

Example Closure

$cl(\psi_1 U\ \psi_2)$ =

$\{\quad \psi_1 U\ \psi_2,$

$\neg(\psi_1 U\ \psi_2),$

$\psi_1, \neg\psi_1,$

$\psi_2, \neg\psi_2$

$\}$

other examples?

The imagination driving Australia's ICT future. NATIONAL ICT AUSTRALIA

Preliminaries (2)

$Sub(\phi)$ is the set of all maximal subsets of $cl(\phi)$, that have no propositional inconsistency.

- $\psi \in Sub(\phi)$ iff $\neg\psi \notin Sub(\phi)$
- $\psi_1 \wedge \psi_2 \in Sub(\phi)$, then $\psi_1 \in Sub(\phi)$ and $\psi_2 \in Sub(\phi)$

The imagination driving Australia's ICT future. NATIONAL ICT AUSTRALIA

Example Sub

$cl(\psi_1 U\ \psi_2)$ =

$\{\quad \psi_1 U\ \psi_2,$

$\neg(\psi_1 U\ \psi_2),$

$\psi_1, \neg\psi_1,$

$\psi_2, \neg\psi_2$

$\}$

$Sub(\psi_1 U\ \psi_2)$ =

$\{\ \{\psi_1 U\ \psi_2,\quad \psi_1,\quad \psi_2\},$

$\{\psi_1 U\ \psi_2,\quad \neg\psi_1,\quad \psi_2\},$

$\{\neg(\psi_1 U\ \psi_2), \neg\psi_1, \neg\psi_2\},$

$\{\psi_1 U\ \psi_2,\quad \psi_1, \neg\psi_2\},$

$\{\neg(\psi_1 U\ \psi_2),\quad \psi_1, \neg\psi_2\}$

$\}$

The imagination driving Australia's ICT future. NATIONAL ICT AUSTRALIA

Local Automaton

$A^L_\phi = (2^{cl(\phi)}, Sub(\phi), \delta^L_\phi, Sub(\phi), Sub(\phi))$

alphabet — states — transition relation — initial states — accepting states

$Sub^\phi(\phi)$, all sets of $Sub(\phi)$, where ϕ holds

Example States

$\psi_1 U \psi_2, \psi_1, \psi_2$

$\psi_1 U\ \psi_2, \neg\psi_1, \psi_2$

$\psi_1 U \psi_2, \psi_1, \neg\psi_2$

$\neg(\psi_1 U \psi_2), \psi_1, \neg\psi_2$

$\neg\ (\psi_1 U\ \psi_2), \neg\psi_1, \neg\psi_2$

initial/accepting states

The imagination driving Australia's ICT future. NATIONAL ICT AUSTRALIA

Transition Relation δ^L_ϕ

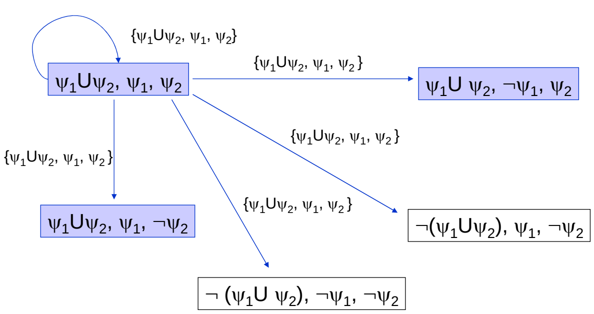
$v \in \delta^L_\phi$ (u,a) iff a=u and

$u,v \in Sub(\phi)$

- $X\psi \in u$ iff $\psi \in v$
- $\psi_1 U \psi_2 \in u$ iff $\psi_2 \in u$ or, $\psi_1 \in u$ and $\psi_1 U \psi_2 \in v$

The imagination driving Australia's ICT future. NATIONAL ICT AUSTRALIA

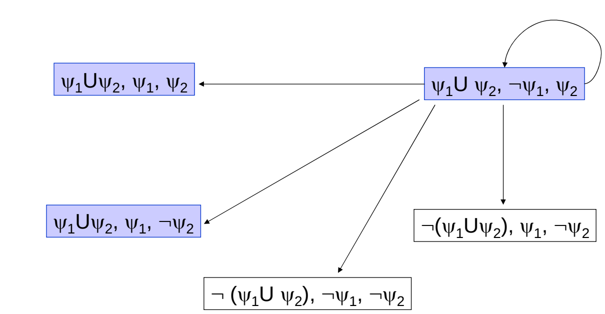
Example Transitions (1)



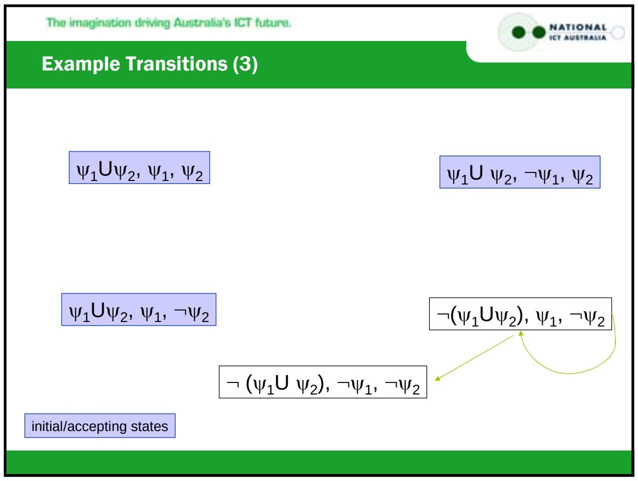
initial/accepting states

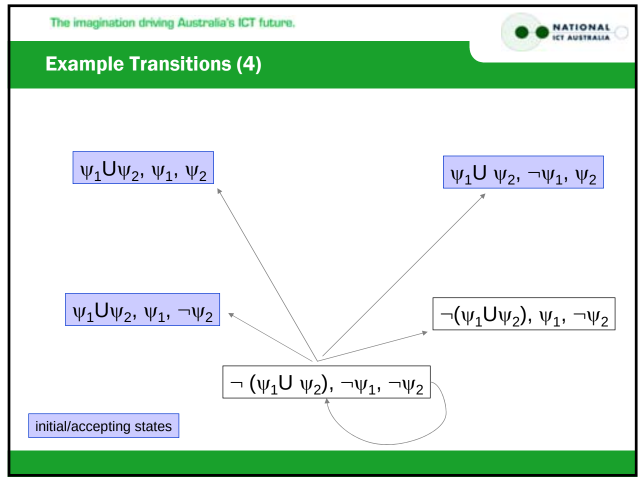
The imagination driving Australia's ICT future. NATIONAL ICT AUSTRALIA

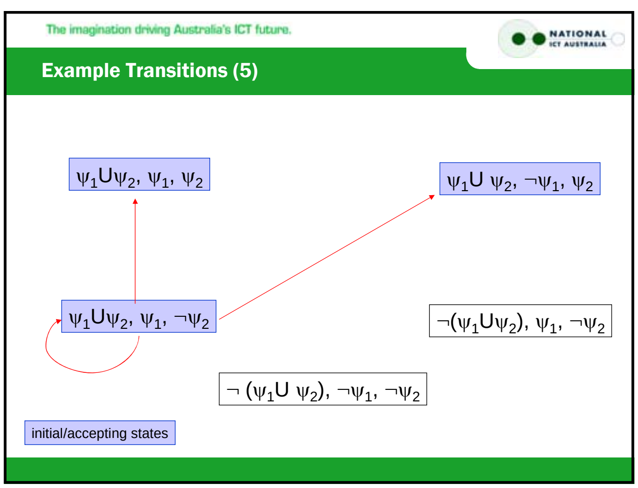
Example Transitions (2)

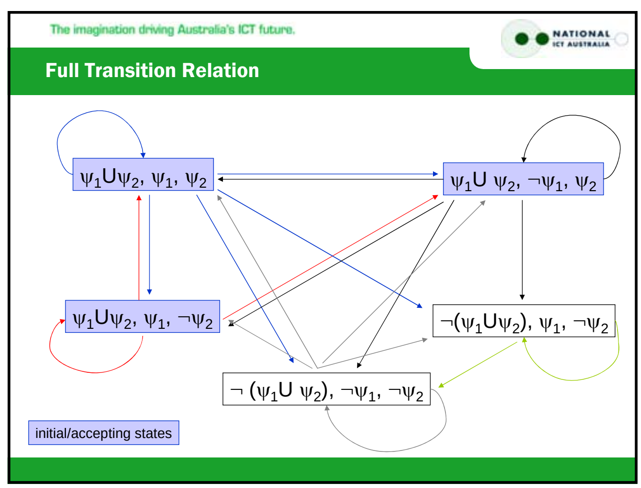


initial/accepting states

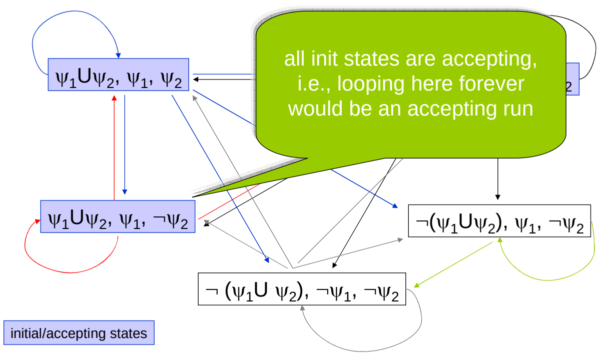

The imagination driving Australia's ICT future.
NATIONAL ICT AUSTRALIA
Example Transitions (3)
$\psi_1 U \psi_2, \psi_1, \psi_2$
$\psi_1 U \psi_2, \neg\psi_1, \psi_2$
$\psi_1 U \psi_2, \psi_1, \neg\psi_2$
$\neg(\psi_1 U \psi_2), \psi_1, \neg\psi_2$
$\neg(\psi_1 U \psi_2), \neg\psi_1, \neg\psi_2$
initial/accepting states


The imagination driving Australia's ICT future.
NATIONAL ICT AUSTRALIA
Example Transitions (4)
$\psi_1 U \psi_2, \psi_1, \psi_2$
$\psi_1 U \psi_2, \neg\psi_1, \psi_2$
$\psi_1 U \psi_2, \psi_1, \neg\psi_2$
$\neg(\psi_1 U \psi_2), \psi_1, \neg\psi_2$
$\neg(\psi_1 U \psi_2), \neg\psi_1, \neg\psi_2$
initial/accepting states


The imagination driving Australia's ICT future.
NATIONAL ICT AUSTRALIA
Example Transitions (5)
$\psi_1 U \psi_2, \psi_1, \psi_2$
$\psi_1 U \psi_2, \neg\psi_1, \psi_2$
$\psi_1 U \psi_2, \psi_1, \neg\psi_2$
$\neg(\psi_1 U \psi_2), \psi_1, \neg\psi_2$
$\neg(\psi_1 U \psi_2), \neg\psi_1, \neg\psi_2$
initial/accepting states


The imagination driving Australia's ICT future.
NATIONAL ICT AUSTRALIA
Full Transition Relation
$\psi_1 U \psi_2, \psi_1, \psi_2$
$\psi_1 U \psi_2, \neg\psi_1, \psi_2$
$\psi_1 U \psi_2, \psi_1, \neg\psi_2$
$\neg(\psi_1 U \psi_2), \psi_1, \neg\psi_2$
$\neg(\psi_1 U \psi_2), \neg\psi_1, \neg\psi_2$
initial/accepting states

Almost ...



Eventuality Automaton (1)

- task is to prevent looping of $\psi_1 U \psi_2$ without ever satisfying ψ_2
- eventually ψ_2 has to hold

Eventuality Automaton (2)

$A^E_\phi = (2^{cl(\phi)}, 2^{e(\phi)}, \delta^E_\phi, \{\emptyset\}, \{\emptyset\})$

alphabet, states, transition relation, initial states, accepting states

$e(\phi)$, subset of $cl(\phi)$ which exactly contains all untils

Example Eventuality Automaton

initial state + accepting state

Transition Relation δ^E_ϕ

$v \in \delta^E_\phi(u,a)$ iff

$u,v \in 2^{e(\phi)}$
$a \in 2^{cl(\phi)}$

- $u=\emptyset$ and for all $\psi_1 U \psi_2 \in a$,
  either $\psi_2 \in a$ or $\psi_1 U \psi_2 \in v$
- $u \neq \emptyset$ and for all $\psi_1 U \psi_2 \in u$,
  either $\psi_2 \in a$ or $\psi_1 U \psi_2 \in v$

The imagination driving Australia's ICT future.

Transition Relation δ^E_ϕ

$v \in \delta^E_\phi(u,a)$ iff

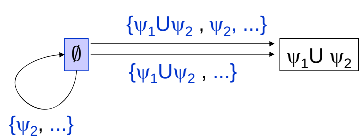
$u,v \in 2^{e(\phi)}$
$a \in 2^{cl(\phi)}$

- $u=\emptyset$ and for all $\psi_1 U \psi_2 \in a$,
  either $\psi_2 \in a$ or $\psi_1 U \psi_2 \in v$

starting in initial/accepting state and
we see $\psi_1 U \psi_2$, we also have to see either ψ_2 or $\psi_1 U \psi_2$ has
to be in the target

The imagination driving Australia's ICT future.

Example Eventuality Automaton



initial state + accepting state

The imagination driving Australia's ICT future.

Transition Relation δ^E_ϕ

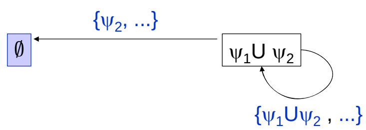
$v \in \delta^E_\phi(u,a)$ iff

$u,v \in 2^{e(\phi)}$
$a \in 2^{cl(\phi)}$

- $u \neq \emptyset$ and for all $\psi_1 U \psi_2 \in u$,
  either $\psi_2 \in a$ or $\psi_1 U \psi_2 \in v$

in an $\psi_1 U \psi_2$ state, we see either ψ_2
or in the target $\psi_1 U \psi_2$

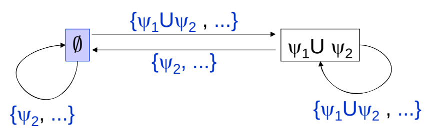
Example Eventuality Automaton



initial state + accepting state

The imagination driving Australia's ICT future.

Example Eventuality Automaton



initial state + accepting state

The imagination driving Australia's ICT future.

Intersection of Both Automata

- does what it is supposed to do ☺
- EXERCISE

The imagination driving Australia's ICT future.

Complexity

- each node in local automaton is maximal, i.e., contains each subformula either negated or non-negated: number of nodes exponential in size of formula.
- eventuality automaton has states consisting of sets of until formulas: exponential in number of until formulas
- then product, then reduction to reachable states
- heaps of overhead here, other methods are smarter…

The imagination driving Australia's ICT future.

NATIONAL ICT AUSTRALIA

Lessons learnt

- Model checking by checking inclusion
- requires LTL to Buchi transformation
- can be constructed through locality/eventuality automaton

The imagination driving Australia's ICT future.

NATIONAL ICT AUSTRALIA

THE END