Deterministic Automata for the (F,G)-fragment of LTL

Jan *Křetínský*, Javier Esparza

报告人：谢淼

Fakultät *für* Informatik, Technische *UniversitätMünchen*, Germany
Faculty of Informatics, Masaryk University, Brno, Czech Republic

2013-5-25

Outline

Outline

Motivation

Problem LTL $\Rightarrow$ deterministic $\omega - automata$

Background
1. Synthesis of reactive modules for LTL specifications[PR88].
2. Model checking Markov decision processes[BK08].

Previous approach
1. LTL $\Rightarrow$ non-deterministic *Büchi* automaton(NBW) and then NBW $\Rightarrow$ deterministic Rabin automata by Safra's construction[Saf88]

disadvantage Safra's construction is difficult to handle algorithmically due to its "messy" state space

Outline

Related Works

- How to overcome this difficulty?
  1. Heuristics
     - ltl2dstar Tool[KB06,KB07,Kle].
  2. new algorithm
     - Directly generate deterministic automaton from LTL fragments [AT04] for reactivity(1) formulas and ANZU tools[PPS06,JGWB07].
     - Construct a symbolic description of a deterministic parity automaton[MS08] from LTL formulae.

Related Works

- Is symbolic approach wonderful?
- What about probabilistic model checking?
  - Requires Linear arithmetic:
  - Can not use sophisticated symbolic representations.
  - Can not use Tree automata.
- So current Prism use:
  - ltl2destar explicitly constructs reduced DRW.

Outline

Outline

LTL Syntax

Definition 1 (LTL Syntax). *The formulae of the* (**F**,**G**)*-fragment of linear temporal logic are given by the following syntax:*

$$\varphi ::= a \mid \neg a \mid \varphi \wedge \varphi \mid \varphi \vee \varphi \mid \mathbf{F}\varphi \mid \mathbf{G}\varphi$$

where a ranges over a finite fixed set Ap of atomic propositions.

We use the standard abbreviations $\mathbf{tt} := a \vee \neg a$, $\mathbf{ff}; = a \wedge \neg a$. We only have negations of atomic propositions, as negations can be pushed inside due to the equivalence of $\mathbf{F}\varphi$ and $\neg\mathbf{G}\neg\varphi$.

Outline

One-step unfolding definition of LTL

- one-step unfolding $\mho()$
  - $\mho(a) = a$
  - $\mho(\neg a) = \neg a$
  - $\mho(\varphi \wedge \psi) = \mho(\varphi) \wedge \mho(\psi)$
  - $\mho(\varphi \vee \psi) = \mho(\varphi) \vee \mho(\psi)$
  - $\mho(F\varphi) = \mho(\varphi) \vee XF\psi$
  - $\mho(G\varphi) = \mho(\varphi) \wedge XG\psi$

One-step unfolding definition of LTL

- Example $\varphi = Fa \wedge GFb$
  - $\mho(\varphi) = (a \vee XFa) \wedge (\mho(Fb) \wedge XGFb)$
  - $\mho(\varphi) = (a \vee XFa) \wedge ((\mho(b) \vee XFb) \wedge XGFb)$
  - $\mho(\varphi) = (a \vee XFa) \wedge (b \vee XFb) \wedge XGFb$

Outline

Construction of state space

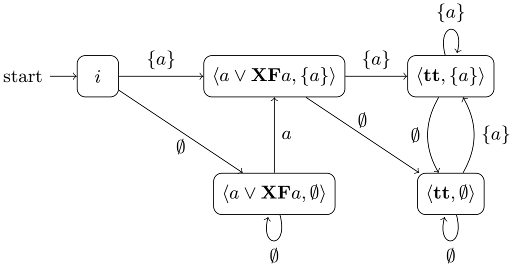
- Given a LTL φ, output a deterministic automation
- clue: $\mho()$
  - closure$(\varphi) = C(\varphi) := Ap \cup \{\neg a | a \in Ap\} \cup X\mathbb{T}$.
  - $\mathbb{F}$ and $\mathbb{G}$ is the set of all subformulae of the form $F\varphi$ and $G\varphi$
  - $\mathbb{T} := \mathbb{F} \cup \mathbb{G}$
  - $X\Psi := \{X\psi | \psi \in \Psi\}$
- $states(\varphi)$ is the set of $2^{2^{|\varphi|}}$.

Construction of state space

- $A(\varphi) = (Q, i, \delta)$ to be a deterministic finite automaton over $\Sigma = 2^{Ap}$ given by
  - the set of states $Q = \{i\} \cup (states(\varphi) \times 2^{Ap})$
  - the initial state i
  - the transition function
    - $\delta = \{(i, \alpha, <\mho(\varphi), \alpha>) | \alpha \in \Sigma\} \cup \{(<\psi, \alpha>, \beta, < succ(\psi, \alpha), \beta >) | <\psi, \alpha> \in Q, \beta \in \Sigma\}$
    - $succ(\psi, \alpha) = \mho(next(\psi[\alpha \mapsto tt, Ap \setminus \alpha \mapsto ff]))$
    - $next(\psi)$ removes X's from φ
- $states(\varphi)$ is the set of $2^{2^{|\varphi|}}$.
- Key point: store one-step history.

Construction of state space

Example $\varphi = Fa$



Construction of state space

- Is one-step history very important?
- Example $\varphi = GF(a \wedge Fb)$
  - $\mho(\varphi) = XGF(a \wedge Fb) \wedge (XF(a \wedge Fb) \vee (a \wedge (b \vee XFb)))$
  - after reading a
  - $GF(a \wedge Fb) \wedge (F(a \wedge Fb) \vee Fb)$
  - after reading b and $\emptyset$
  - $GF(a \wedge Fb) \wedge (F(a \wedge Fb))$
  - infinitely required $(GF(a \wedge Fb))$
  - thus, $(\{a\}\{b\})^\omega$ and $(\{a\}\emptyset)^\omega$ are equal.
- Solution:
  - one-step history.

Outline

Outline

Method

- Muller Accepting Condition
  - The set of all states visited infinitely often must be an element of the acceptance set

Method

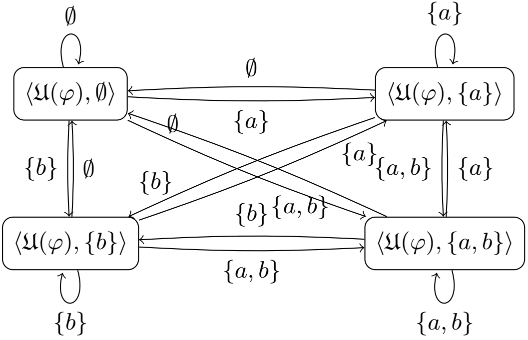
- Until now, we have a formula φ and its corresponding automaton $A(\varphi) = (Q, i, \delta)$
- Consider a formula χ as a Boolean Function over elements of $C(\varphi)$.
- For sets $T, F \subseteq C(\varphi)$, let $[T \mapsto tt, F \mapsto ff]$ denote the formula where tt is substituted for elements of T, and ff for F.
- $I \models_\alpha \chi$: $\chi[\alpha \cup I \mapsto tt, Ap \backslash \alpha \mapsto ff]$ is equivalent to tt, where $I \subseteq \mathbb{T}$

Method

- Muller acceptance
- A set $M \subseteq Q$ is Muller accepting for a set $I \subseteq \mathbb{T}$ if the following is satisfied:
  1. for each $(\chi, \alpha) \in M$, we have $XI \models_\alpha \chi$,
  2. for each $F\psi \in I$ there is $(\chi, \alpha) \in M$ with $I \models_\alpha \psi$,
  3. for each $G\psi \in I$ and for each $(\chi, \alpha) \in M$ we have $I \models_\alpha \psi$.
- A set $F \subseteq Q$ is Muller accepting (for φ) if it is Muller accepting for some $I \subseteq \mathbb{T}$.

Method

Example $\varphi = F(Ga \vee Gb)$



Outline

Correctness of sound and complete

- Theorem
- Let φ be a formula and w a word. Then w is accepted by the deterministic automaton $A(\varphi)$ with the Muller condition $M(\varphi)$ if and only if $w \models \varphi$.

Correctness of sound and complete

- Proposition Local finitary correctness
- Let w be a word and $A(\varphi)(w) = i(\chi_0, \alpha_0)(\chi_1, \alpha_1)\ldots$ the corresponding run. Then for all $n \in \mathbb{N}$, we have $w \models \varphi$ if and only if $w_n \models \chi_n$
- Proof:The one-step unfold produces a temporally equivalent (w.r.t. LTL satisfaction) formula.The unfold is a Boolean function over atomic propositions and elements of $X\mathbb{T}$. Therefore, this unfold is satisfied if and only if the next state satisfied next(φ) where φ is the result of partial application of the Boolean function to the currently read letter of the word. We conclude by induction.Comments: each occurrence of satisfaction of F must happen in limit time.

Correctness of sound and complete

- Completeness
- If$w \models \varphi$ then $Inf(A(\varphi)(w))$ is a Muller accepting set.
- Proof:
  1. Let us show that $M := inf(A(\varphi)(w))$ is a Muller accepting for $I := \{\psi \in \mathbb{F} | w \models G\psi\} \cup \{\psi \in \mathbb{G} | w \models F\psi\}$
  2. Condition 1. Let $(\chi, \beta) \in M$. Since $w \models \varphi$ by Proposition Local finitary correctness $w_i \models \chi$ whenever we enter (χ, α) after reading w^i, which happens for infinitely many $i \in \mathbb{N}$. Hence we have a recurring set $I_{\chi,\alpha}$ modelling χ Since $I_{\chi,\alpha} \models_\alpha \chi$ we get also $I \models_\alpha \chi$ by $I_{\chi,\alpha} \subseteq I$.

Correctness of sound and complete

Condition 2. Let $\mathbf{F}\psi \in I$, then $w \models \mathbf{GF}\psi$. Since there are finitely many states, there is $(\chi, \alpha) \in M$ for which after infinitely many entrances by w^i it holds $w_i \models \psi$ by Proposition 9, hence we have a recurring set $I_{\chi,\alpha}$ modelling ψ and conclude as above.

Condition 3. Let $\mathbf{G}\psi \in I$, then $w \models \mathbf{FG}\psi$. Hence for every $(\chi, \alpha) \in M$ infinitely many w^i leading to (χ, α) satisfy $w_i \models \psi$ by Proposition 9, hence we have a recurring set $I_{\chi,\alpha}$ modelling ψ and conclude as above. □

Correctness of sound and complete

Lemma 11. *Let ρ be a run. If* $\mathrm{Inf}(\rho)$ *is Muller accepting for I then $Ap(\rho) \models \mathbf{G}\psi$ for each $\psi \in I \cap \mathbb{F}$ and $Ap(\rho) \models \mathbf{F}\psi$ for each $\psi \in I \cap \mathbb{G}$.*

Proof. Denote $w = Ap(\rho)$. Let us first assume $\psi \in I \cap \mathbb{F}$ and $w_j \not\models \psi$ for all $j \geq i \in \mathbb{N}$. Since $\psi \in I \cap \mathbb{F}$, for infinitely many j, ρ passes through some $(\chi, \alpha) \in \mathrm{Inf}(\rho)$ for which $I \models_\alpha \psi$. Hence, there is $\psi_1 \in I$ which is a subformula of ψ such that for infinitely many i, $w_i \not\models \psi_1$. If $\psi_1 \in \mathbb{F}$, we proceed as above; similarly for $\psi_1 \in \mathbb{G}$. Since we always get a smaller subformula, at some point we obtain either $\psi_n = \mathbf{F}\beta$ or $\psi_n = \mathbf{G}\beta$ with β a Boolean combination over Ap and we get a contradiction with the second or the third point of Definition 7, respectively. □

In other words, if we have a Muller accepting set for I then all elements of I hold true in w_i for almost all i.

Correctness of sound and complete

Proposition 12 (Soundness). *If* $\mathrm{Inf}(\mathcal{A}(\varphi)(w))$ *is a Muller accepting set then* $w \models \varphi$.

Proof. Let $M := \mathrm{Inf}(\mathcal{A}(\varphi)(w))$ be a Muller accepting set for some I. There is $i \in \mathbb{N}$ such that after reading w^i we come to (χ, α) and stay in $\mathrm{Inf}(\mathcal{A}(\varphi)(w))$ from now on and, moreover, $w_i \models \psi$ for all $\psi \in I$ by Lemma 11. For a contradiction, let $w \not\models \varphi$. By Proposition 9 we thus get $w_i \not\models \chi$. By the first condition of Definition 7, we get $I \models_\alpha \chi$. Therefore, there is $\psi \in I$ such that $w_i \not\models \psi$, a contradiction. □

Outline

Rabin accepting condition

Definition 14 (Generalized Rabin Automaton). *A* generalized Rabin automaton *is a (deterministic) ω-automaton $\mathcal{A} = (Q, i, \delta)$ over some alphabet Σ, where Q is a set of states, i is the initial state, $\delta : Q \times \Sigma \to Q$ is a transition function, together with a* generalized Rabin condition $\mathcal{GR} \in \mathcal{B}^+(2^Q \times 2^Q)$. *A run ρ of $\mathcal{A}$ is accepting if* $\mathrm{Inf}(\rho) \models \mathcal{GR}$, *which is defined inductively as follows:*

$$
\begin{aligned}
\mathrm{Inf}(\rho) \models \varphi \wedge \psi &\iff \mathrm{Inf}(\rho) \models \varphi \textit{ and } \mathrm{Inf}(\rho) \models \psi \\
\mathrm{Inf}(\rho) \models \varphi \vee \psi &\iff \mathrm{Inf}(\rho) \models \varphi \textit{ or } \mathrm{Inf}(\rho) \models \psi \\
\mathrm{Inf}(\rho) \models (F, I) &\iff F \cap \mathrm{Inf}(\rho) = \emptyset \textit{ and } I \cap \mathrm{Inf}(\rho) \neq \emptyset
\end{aligned}
$$

Rabin accepting condition

- How to use Rabin Condition by an example
- $\varphi = FGa \vee GFb$
- $\mho(\varphi) = XFGa \vee (XGa \wedge a) \vee (XGFb \wedge (XFb \vee b))$
- sub-element: Ga, FGa, GFb, Fb
- require: visit states with $\neg a$ only finitely often, visit b infinitely often.
- Rabin condition: $(\{q|q \models \neg a, Q\} \vee (\emptyset, \{q|q \models b\}))$

Rabin accepting condition

Definition 15 (Generalized Rabin Acceptance). *Let φ be a formula. The* generalized Rabin condition $\mathcal{GR}(\varphi)$ *is*

$$\bigvee_{I \subseteq \mathbb{T}} \left(\left(\{(\chi, \alpha) \mid I \not\models_\alpha \chi \wedge \bigwedge_{\mathbf{G}\psi \in I} \psi\}, Q \right) \wedge \bigwedge_{\mathbf{F}\omega \in I} \left(\emptyset, \{(\chi, \alpha) \mid I \models_\alpha \omega\} \right) \right)$$

By the argumentation above, we get the equivalence of the Muller and the generalized Rabin conditions for φ and thus the following.

Proposition 16. *Let φ be a formula and w a word. Then w is accepted by the deterministic automaton $\mathcal{A}(\varphi)$ with the generalized Rabin condition $\mathcal{GR}(\varphi)$ if and only if $w \models \varphi$.*

Rabin accepting condition

- How to obtain a Rabin automaton from $A(\varphi)$ and the generalized Rabin condition $\mathcal{G}R(\varphi)$
- For a fixed I, the whole conjunction of Definition 15 corresponds to the intersection of automata with different Rabin conditions.
- $(G, Q) \wedge \bigwedge_{f \in F := I \subseteq \mathbb{F}} (\emptyset, F_f)$
    - "counting construction approach" that $Q' = Q \times (1, ..., n)$
    - $(G \times F, F_{\bar{f}} \times \{\bar{f}\})$ for an arbitrary fixed $\bar{f} \in F$

Rabin accepting condition

- State Space
- $\varphi = (FGa \vee GFb) \wedge (FGc \vee GFd) \wedge (FGe \vee GFf)$
- FG or GF proposition
- state space of A is $\{i\} \cup 2^{\{abcdef\}}$, the size is $1 + 2^6$
- $((\neg a, Q) \vee (\emptyset, b)) \wedge ((\neg c, Q) \vee (\emptyset, d)) \wedge ((\neg e, Q) \vee (\emptyset, f))$
- right of the pairs: $tt, b, d, f, b \wedge d, b \wedge f, d \wedge f, b \wedge d \wedge f$
- $2 * 2 * 2 * 3 = 24$
- state space is of the size of $24 * 1 * (1 + 2^6) = 1560$

Outline

Complexity

- Safra's complexity is $2^{n * \bigcirc(2_n)} = 2^{\bigcirc(2^n + logn)}$
- Our Muller automaton size is $\bigcirc(2^{2^{|\mathbb{T}|}} * 2^{|Ap|}) = \bigcirc(2^{2^n+1}) \subseteq 2^{\bigcirc(2^n)}$
- the number of Rabin pairs is $\bigcirc(m) = \bigcirc(2^n)$

Outline

Outline

Experimental Results

- Aim: Compare the size of produced automaton by our method with the Rabin automaton produced by ltl2dstar.
- Method: Ltl2dstar firstly calls an external translator from LTL to non-deterministic *Büchi* automata by LTL2BA. Then it performs Safra's determinization.
- Ltl2dstar implements several optimizations of Safra's construction.
- our implementation does not perform any ad hoc optimization, since we want to evaluate whether the basic idea of the Safraless construction is already competitive.

Experimental Results

- Database: BEEM (BEnchmarks for Explicit Model checkers)[Pel07] and formulae from [SB00] which tests Ltl2dstar.
- Record attributes:
  1. $|states(\varphi)|$, the number of the first component.
  2. $Muller/GR$, the number of states of the Muller or generalized Rabin automata follows.
  3. $\mathcal{G}$R-factor, the complexity of generalized Rabin condition.
  4. Rabin, the number of copies of the state space that are created to obtain an equivalent Rabin automaton
  5. ltl2dstar, the size of the state space of the Rabin automaton generated by ltl2dstar using LTL2BA.

Experimental Results

Table 1. Experimental comparison to ltl2dstar on formulae of [Pel07], [SB00], fairness constraints and some other examples of formulae of the “infinitary” fragment

Formula	states	Muller/GR	$\mathcal{GR}$-factor	Rabin	ltl2dstar
$\mathbf{G}(a \vee \mathbf{F}b)$	2	5	1	5	4
$\mathbf{FG}a \vee \mathbf{FG}b \vee \mathbf{GF}c$	1	9	1	9	36
$\mathbf{F}(a \vee b)$	2	4	1	4	2
$\mathbf{GF}(a \vee b)$	1	3	1	3	4
$\mathbf{G}(a \vee b \vee c)$	2	4	1	4	3
$\mathbf{G}(a \vee \mathbf{F}b)$	2	5	1	5	4
$\mathbf{G}(a \vee \mathbf{F}(b \vee c))$	2	5	1	5	4
$\mathbf{F}a \vee \mathbf{G}b$	3	7	1	7	5
$\mathbf{G}(a \vee \mathbf{F}(b \wedge c))$	2	5	1	5	4
$(\mathbf{FG}a \vee \mathbf{GF}b)$	1	5	1	5	12
$\mathbf{GF}(a \vee b) \wedge \mathbf{GF}(b \vee c)$	1	5	2	10	12

Experimental Results

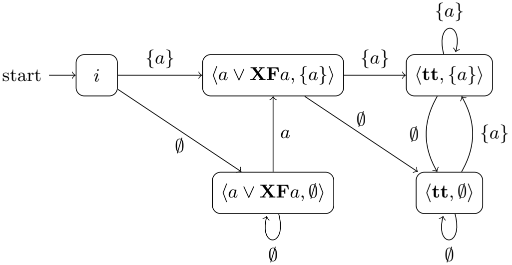
$(\mathbf{FF}a \wedge \mathbf{G}\neg a) \vee (\mathbf{GG}\neg a \wedge \mathbf{F}a)$	2	4	1	4	1
$(\mathbf{GF}a) \wedge \mathbf{FG}b$	1	5	1	5	7
$(\mathbf{GF}a \wedge \mathbf{FG}b) \vee (\mathbf{FG}\neg a \wedge \neg b)$	1	5	1	5	14
$\mathbf{FG}a \wedge \mathbf{GF}a$	1	3	1	3	3
$\mathbf{G}(\mathbf{F}a \wedge \mathbf{F}b)$	1	5	2	10	5
$\mathbf{F}a \wedge \mathbf{F}b$	4	8	1	8	4
$(\mathbf{G}(b \vee \mathbf{GF}a) \wedge \mathbf{G}(c \vee \mathbf{GF}\neg a)) \vee \mathbf{G}b \vee \mathbf{G}c$	4	18	2	36	26
$(\mathbf{G}(b \vee \mathbf{FG}a) \wedge \mathbf{G}(c \vee \mathbf{FG}\neg a)) \vee \mathbf{G}b \vee \mathbf{G}c$	4	18	1	18	29
$(\mathbf{F}(b \wedge \mathbf{FG}a) \vee \mathbf{F}(c \wedge \mathbf{FG}\neg a)) \wedge \mathbf{F}b \wedge \mathbf{F}c$	4	18	1	18	8
$(\mathbf{F}(b \wedge \mathbf{GF}a) \vee \mathbf{F}(c \wedge \mathbf{GF}\neg a)) \wedge \mathbf{F}b \wedge \mathbf{F}c$	4	18	1	18	45
$(\mathbf{FG}a \vee \mathbf{GF}b)$	1	5	1	5	12
$(\mathbf{FG}a \vee \mathbf{GF}b) \wedge (\mathbf{FG}c \vee \mathbf{GF}d)$	1	17	2	34	17527
$\bigwedge_{i=1}^{3}(\mathbf{GF}a_i \rightarrow \mathbf{GF}b_i)$	1	65	24	1 560	1 304 706
$(\bigwedge_{i=1}^{5} \mathbf{GF}a_i) \rightarrow \mathbf{GF}b$	1	65	1	65	972
$\mathbf{GF}(\mathbf{F}a\mathbf{GF}b\mathbf{FG}(a \vee b))$	1	5	1	5	159
$\mathbf{FG}(\mathbf{F}a \vee \mathbf{GF}b \vee \mathbf{FG}(a \vee b))$	1	5	1	5	2918
$\mathbf{FG}(\mathbf{F}a \vee \mathbf{GF}b \vee \mathbf{FG}(a \vee b) \vee \mathbf{FG}b)$	1	5	1	5	4516

Experimental Results

- Advantage: for "infinitary" fragment, fairness constraints, Drawback: for "finitary" behavior.
- Reason: The problem is that some states such as $< a \vee XFa, \{a\} >$ are only "passed through" and are equivalent to some of their successors, here $< tt, \{a\} >$.
- Overcome: perform the following collapse:
- For two states, $(\chi, \alpha), (\chi', \alpha)$ satisfy that $\chi[\alpha \mapsto tt, Ap \backslash \alpha \mapsto ff]$ is propositionally equivalent to $\chi'[\alpha \mapsto tt, Ap \setminus \alpha \mapsto ff]$, collapse.
- result: the size as the one produced by ltl2dstar. $(Fa \wedge Fb)$

Experimental Results

Example $\varphi = Fa$



Outline

Conclusion and Future Works

- Conclusion
  1. show a direct translation of the LTL fragment with operators F and G to deterministic automata.
  2. First of all, in our opinion it is a lot simpler than the determinization and its various non-trivial optimizations.
  3. the state space has a clear logical structure.
  4. the state space is not much bigger even when compared to already optimized determinization. Very often it is considerably smaller, especially for the "infinitary" formulae; in particular, for fairness conditions.
  5. given a very compact deterministic w-automaton with a small and in our opinion reasonably simple generalized Rabin acceptance condition.

Conclusion and Future Works

- Future works
  1. Extend to the (X,F,G)-fragment and even to the whole LTL.(may have a n-step look-ahead, for instance, $GF(a \wedge Xb)$)
  2. There is space for further performance improvements in this new approach by optimizations