Probabilistic Automata for Safety LTL Specifications

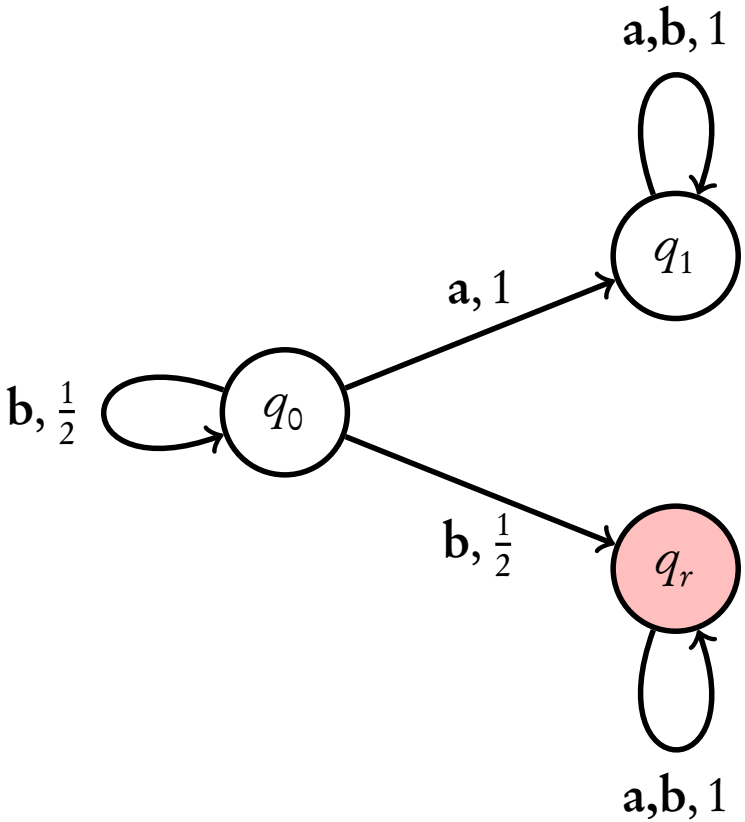
Dileep Kini

joint work with Mahesh Viswanathan

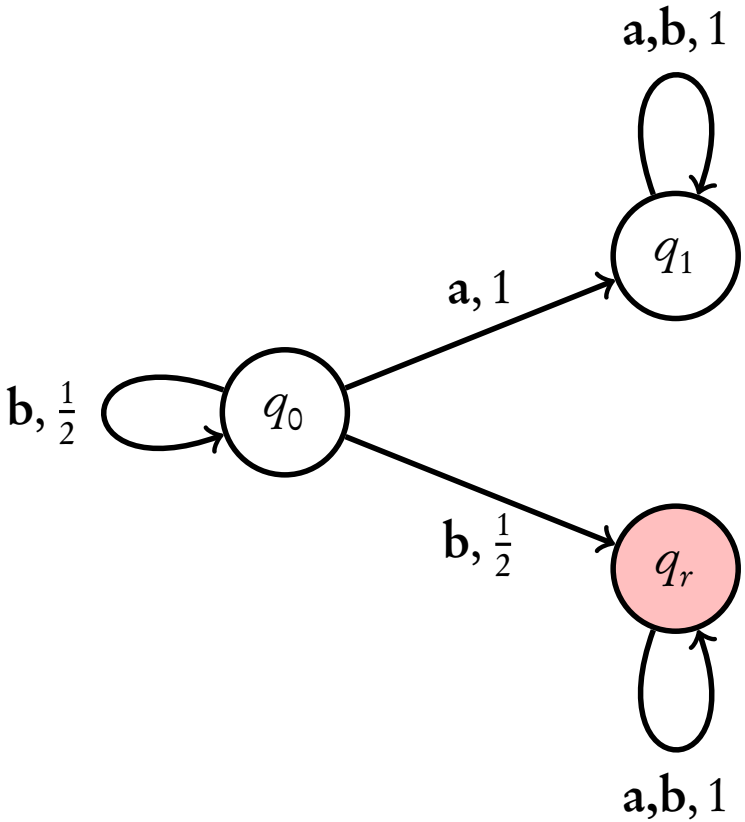
University of Illinois at Urbana Champaign

VMCAI 2014

Finite state Probabilistic Monitor [CSV09]

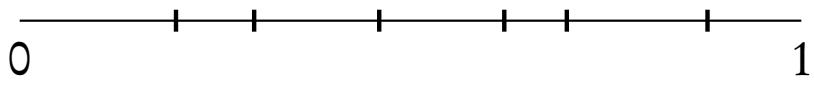


Finite state Probabilistic Monitor [CSV09]

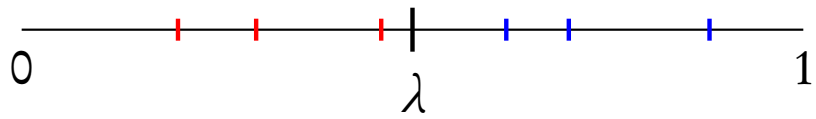


Rejection Probability: Probability of reaching the reject state after having consumed the word.

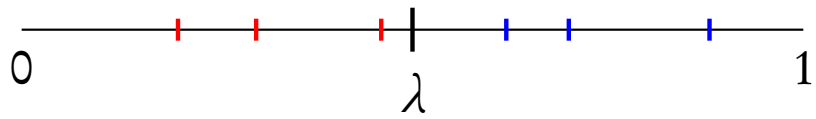
Monitorable languages



Monitorable languages



Monitorable languages



Given a cutpoint $\lambda \in [0, 1]$, words with acceptence probability at least (more than) λ is denoted by $L_{\geq\lambda}(\mathcal{M})$ (resp. $L_{>\lambda}(\mathcal{M})$).

Monitorable languages

Language L is monitorable/recognizable

Monitorable languages

Language L is monitorable/recognizable

- **strongly** if there is an $\mathcal{M}$ such that $L_{\geq 1}(\mathcal{M}) = L$.

Monitorable languages

Language L is monitorable/recognizable

- **strongly** if there is an $\mathcal{M}$ such that $L_{\geq 1}(\mathcal{M}) = L$.
- **weakly** if there is an $\mathcal{M}$ such that $L_{>0}(\mathcal{M}) = L$.

Monitorable languages

Language L is monitorable/recognizable

- **strongly** if there is an $\mathcal{M}$ such that $L_{\geq 1}(\mathcal{M}) = L$.
- **weakly** if there is an $\mathcal{M}$ such that $L_{>0}(\mathcal{M}) = L$.
- **robustly** if there is an $\mathcal{M}$ and λ such that $L_{>\lambda}(\mathcal{M}) = L$ and $\mathcal{M}$ is *isolated* at λ.

Monitorable languages

Language L is monitorable/recognizable

- **strongly** if there is an $\mathcal{M}$ such that $L_{\geq 1}(\mathcal{M}) = L$.
- **weakly** if there is an $\mathcal{M}$ such that $L_{>0}(\mathcal{M}) = L$.
- **robustly** if there is an $\mathcal{M}$ and λ such that $L_{>\lambda}(\mathcal{M}) = L$ and $\mathcal{M}$ is *isolated* at λ.

isolated: $\exists\, \epsilon$ such that no word is accepted with probability $(\lambda - \epsilon, \lambda + \epsilon)$.

The problem we are interested in . . .

Given any safety property in LTL, how large is the smallest FPM that recognizes it?

The problem we are interested in . . .

Given any safety property in LTL, how large is the smallest FPM that recognizes it?

Motivation

Deterministic Automata for LTL can be 2-EXP large [KR10]

The problem we are interested in ...

Given any safety property in LTL, how large is the smallest FPM that recognizes it?

Motivation

Deterministic Automata for LTL can be 2-EXP large [KR10]

Applications

- Optimal FPMs yield efficient monitoring algorithms
- Qualitative verification of Markov Chains [BG05]

Overview

We consider logics Safe-LTL and LTL(G), and investigate bounds on the size of equivalent FPMs

	DBA	NBA	Strong Monitors	Weak Monitors	Robust Monitors
Safe-LTL	2-EXP	EXP	?	?	?
LTL(G)	2-EXP	EXP	?	?	?

Safety LTL

Syntax

Formulae in Safe-LTL are given by:

$$\varphi ::= p \mid \neg p \mid \varphi \wedge \varphi \mid \varphi \vee \varphi \mid X\varphi \mid \varphi R \varphi$$

- where p ranges over propositions P.

- Interpreted over $\alpha = \sigma_0\sigma_1\ldots$ where $\sigma_i \in 2^P$
- $[\![\varphi]\!] = \{\alpha \in (2^P)^\omega \mid \alpha \vDash \varphi\}$

Safety LTL

Strong Monitors

Safety LTL

Strong Monitors

Theorem

For every formula φ in Safe-LTL there is a FPM $\mathcal{M}_\varphi$ of size $O(2^{|\varphi|})$ such that $\mathcal{M}_\varphi$ strongly monitors $[\![\varphi]\!]$, i.e. $L_{\geq 1}(\mathcal{M}_\varphi) = [\![\varphi]\!]$.

	DBA	NBA	Strong Monitors	Weak Monitors	Robust Monitors
Safe-LTL	2-EXP	EXP	EXP	?	?
LTL(G)	2-EXP	EXP	EXP	?	?

Safety LTL

Strong Monitors

Theorem

For every formula φ in Safe-LTL there is a FPM $\mathcal{M}_\varphi$ of size $O(2^{|\varphi|})$ such that $\mathcal{M}_\varphi$ strongly monitors $[\![\varphi]\!]$, i.e. $L_{\geq 1}(\mathcal{M}_\varphi) = [\![\varphi]\!]$.

NBA constructed from the alternating automata [Var96] for $\neg\phi$, has a single absorbing accept state.

	DBA	NBA	Strong Monitors	Weak Monitors	Robust Monitors
Safe-LTL	2-EXP	EXP	EXP	?	?
LTL(G)	2-EXP	EXP	EXP	?	?

Communication Complexity

Communication Complexity

- Alice has input $x \in X$, Bob has input $y \in Y$

Communication Complexity

- Alice has input $x \in X$, Bob has input $y \in Y$
- Given $f : X, Y \to \{0, 1\}$, collaboratively compute $f(x, y)$

Communication Complexity

- Alice has input $x \in X$, Bob has input $y \in Y$
- Given $f : X, Y \to \{0, 1\}$, collaboratively compute $f(x, y)$
- We will be interested in **randmoized one-round** protocols

Communication Complexity

- Alice has input $x \in X$, Bob has input $y \in Y$
- Given $f : X, Y \to \{0, 1\}$, collaboratively compute $f(x, y)$
- We will be interested in **randmoized one-round** protocols
- $R_{\epsilon}^{A \to B}(f)$ is the min number of bits that need to be exchanged by a protocol that implements f with error atmost ϵ.

Communication Complexity

- Alice has input $x \in X$, Bob has input $y \in Y$
- Given $f : X, Y \to \{0, 1\}$, collaboratively compute $f(x, y)$
- We will be interested in **randmoized one-round** protocols
- $R_\epsilon^{A \to B}(f)$ is the min number of bits that need to be exchanged by a protocol that implements f with error atmost ϵ.

Complexity of the disjointness function $R_\epsilon^{A \to B}(g_n) = \Omega(2^n)$ [KNR95].

Safety LTL
Weak Monitors

Theorem

There is a family of Safe-LTL formulas $\{\varphi_n\}_{n\in\mathbb{N}}$ where φ_n is of size $O(n^2)$, such that any family of FPMs $\{\mathcal{M}_n\}_{n\in\mathbb{N}}$ that weakly monitors it, $L_{>0}(\mathcal{M}_n) = [\![\varphi_n]\!]$, has size 2^{2^n}.

	DBA	NBA	Strong Monitors	Weak Monitors	Robust Monitors
Safe-LTL	2-EXP	EXP	EXP	2-EXP	?
LTL(G)	2-EXP	EXP	EXP	?	?

Safety LTL
Weak Monitors

Theorem

There is a family of Safe-LTL formulas $\{\varphi_n\}_{n\in\mathbb{N}}$ where φ_n is of size $O(n^2)$, such that any family of FPMs $\{\mathcal{M}_n\}_{n\in\mathbb{N}}$ that weakly monitors it, $L_{>0}(\mathcal{M}_n) = [\![\varphi_n]\!]$, has size 2^{2^n}.

- Consider $\varphi_n \in$ Safe-LTL of size $O(n^2)$ which specifies L_n

Safety LTL
Weak Monitors

Theorem

There is a family of Safe-LTL formulas $\{\varphi_n\}_{n\in\mathbb{N}}$ where φ_n is of size $O(n^2)$, such that any family of FPMs $\{\mathcal{M}_n\}_{n\in\mathbb{N}}$ that weakly monitors it, $L_{>0}(\mathcal{M}_n) = [\![\varphi_n]\!]$, has size 2^{2^n}.

- Consider $\varphi_n \in$ Safe-LTL of size $O(n^2)$ which specifies L_n
- $\mathcal{M}$ that weakly monitors L_n can be used to construct a protocol for g_n which costs $\log_2(|\mathcal{M}|)$ bits.

Safety LTL
Weak Monitors

Theorem

There is a family of Safe-LTL formulas $\{\varphi_n\}_{n\in\mathbb{N}}$ where φ_n is of size $O(n^2)$, such that any family of FPMs $\{\mathcal{M}_n\}_{n\in\mathbb{N}}$ that weakly monitors it, $L_{>0}(\mathcal{M}_n) = [\![\varphi_n]\!]$, has size 2^{2^n}.

- Consider $\varphi_n \in$ Safe-LTL of size $O(n^2)$ which specifies L_n
- $\mathcal{M}$ that weakly monitors L_n can be used to construct a protocol for g_n which costs $\log_2(|\mathcal{M}|)$ bits.
- $|\mathcal{M}| = 2^{\Omega(2^n)}$ from $R_\epsilon^{A\to B}(g_n) = \Omega(2^n)$

LTL(G)

LTL(G)

Syntax and Semantics

Formulae in LTL(G) are given by:

$$\varphi ::= p \mid \neg p \mid \varphi \wedge \varphi \mid \varphi \vee \varphi \mid X\varphi \mid G\varphi$$

- $G\varphi$ is $\mathit{false}\, R\, \varphi$, holds when φ is true for all suffixes.

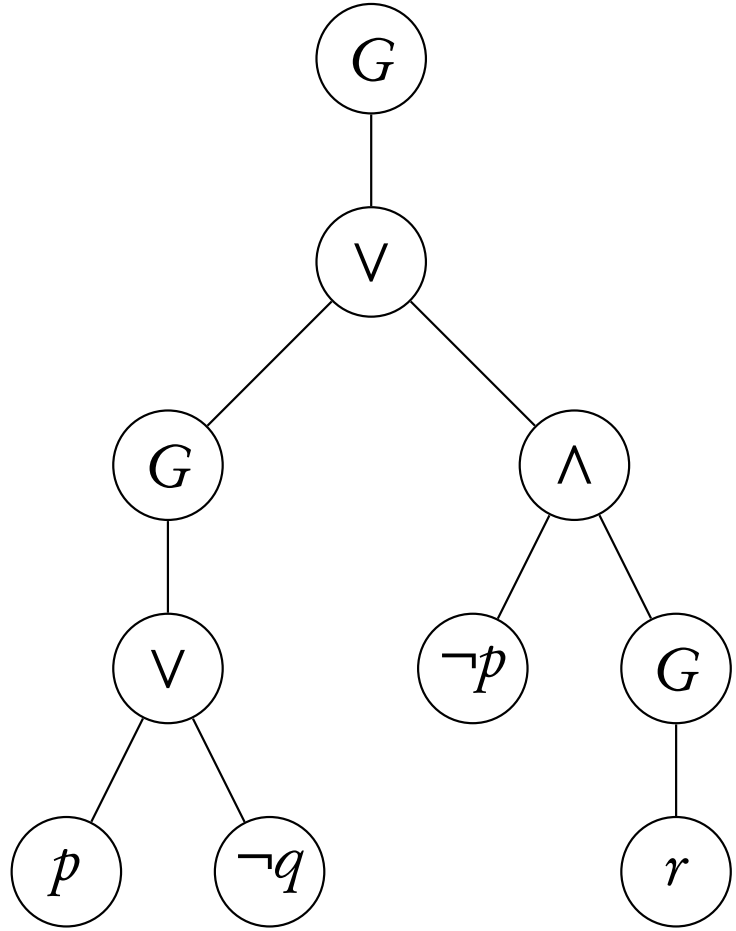
LTL(G)
Weak Monitors

Theorem

For every formula φ in LTL(G) there is a FPM $\mathcal{M}_\varphi$ of size $O(2^{|\varphi|})$ such that $\mathcal{M}_\varphi$ weakly monitors $[\![\varphi]\!]$ i.e. $L_{>0}(\mathcal{M}_\varphi) = [\![\varphi]\!]$.

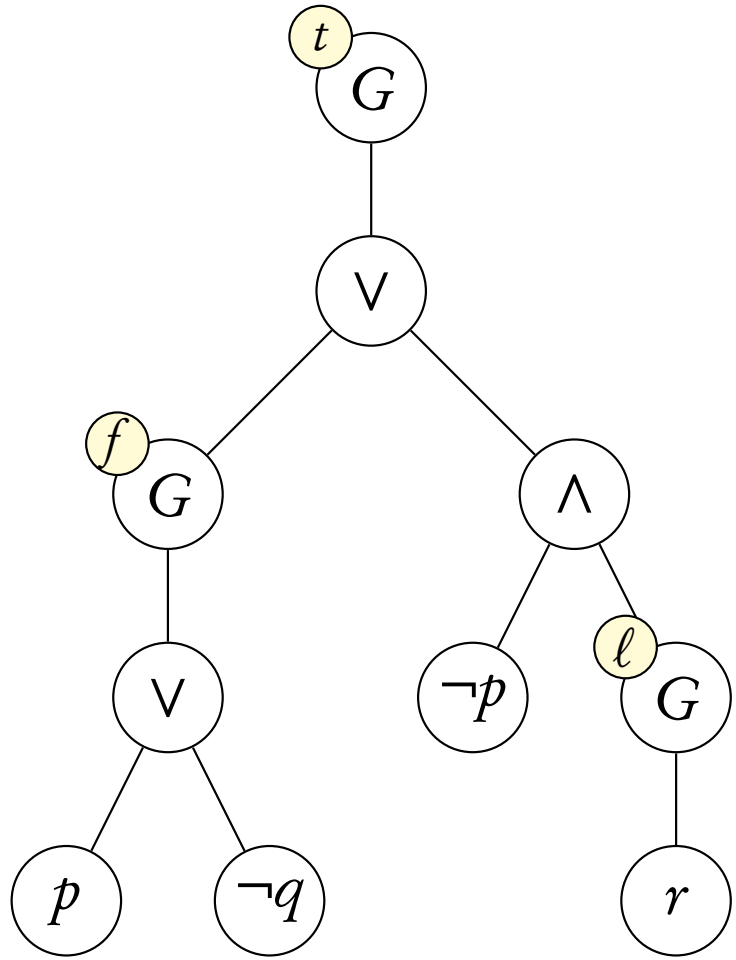
	DBA	NBA	Strong Monitors	Weak Monitors	Robust Monitors
Safe-LTL	2-EXP	EXP	EXP	2-EXP	?
LTL(G)	2-EXP	EXP	EXP	EXP	?

LTL(G)
Weak Monitors



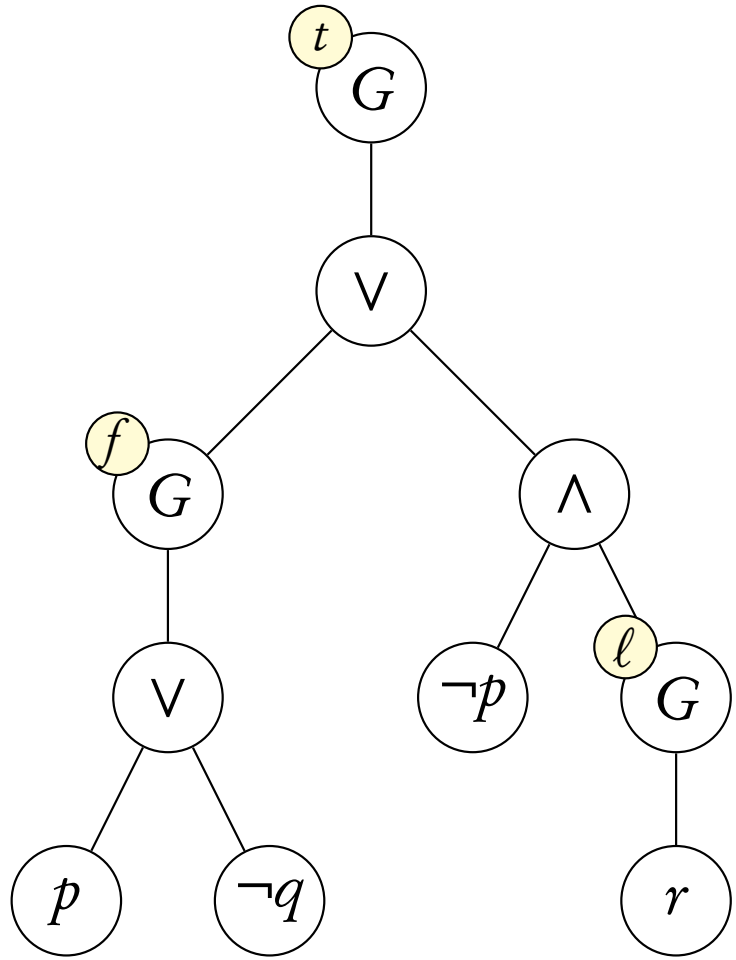
LTL(G)
Weak Monitors

- Annotation: $a : G\psi \to \{t, f, \ell\}$



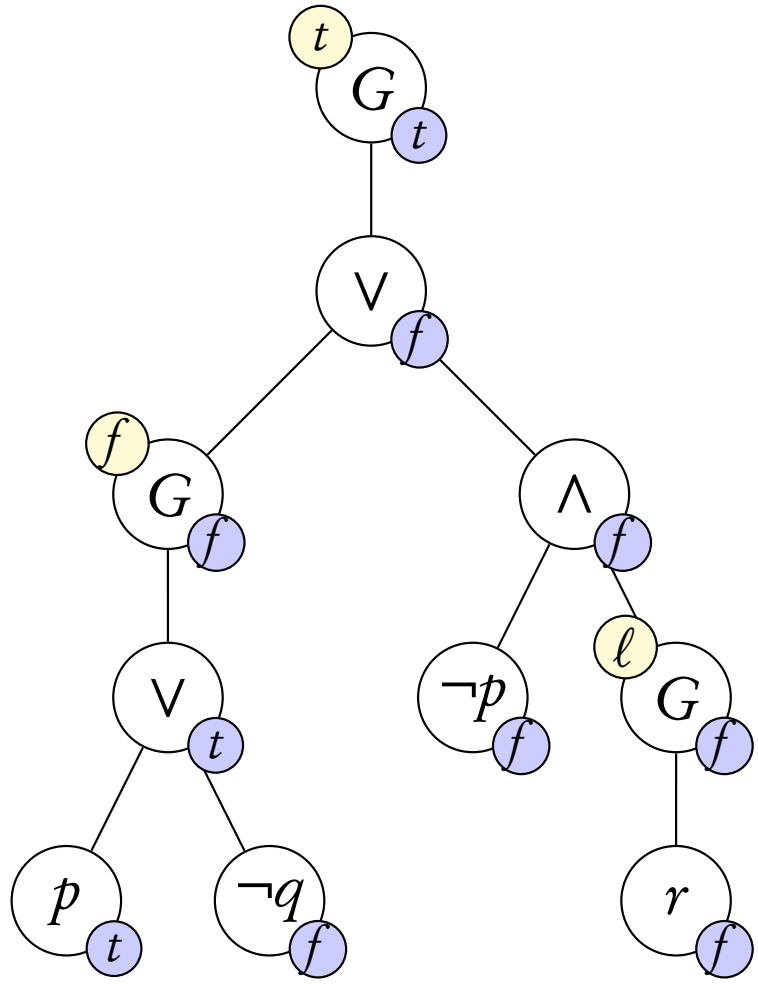
LTL(G)
Weak Monitors

- Annotation: $a : G\psi \to \{t, f, \ell\}$
- Assignment: $\sigma \in 2^P$. eg: $\sigma = \{p, q\}$



LTL(G)
Weak Monitors

- Annotation: $a : G\psi \to \{t, f, \ell\}$
- Assignment: $\sigma \in 2^P$. eg: $\sigma = \{p, q\}$
- Evaluation: $e_a^\sigma : \psi \to \{t, f\}$

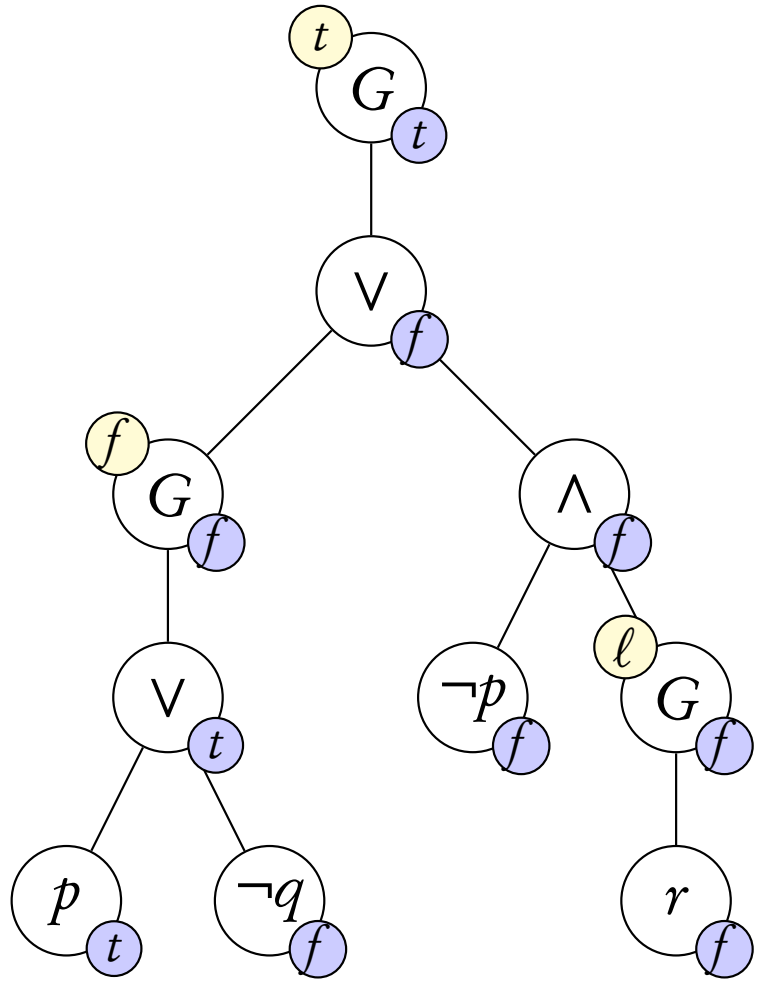


LTL(G)
Weak Monitors

- Annotation: $a : G\psi \to \{t, f, \ell\}$
- Assignment: $\sigma \in 2^P$. eg: $\sigma = \{p, q\}$
- Evaluation: $e^\sigma_a : \psi \to \{t, f\}$

$$a \xrightarrow{\sigma} b$$

- truth of $G\psi$ be preserved from a to b
- if $G\psi$ is true then so should $e^\sigma_a(\psi)$



LTL(G)
Robust Monitors

LTL(G)

Robust Monitors

Gap of $\mathcal{M}$ wrt λ is the smallest difference between the acceptance probability of any word and λ.

LTL(G)
Robust Monitors

Gap of $\mathcal{M}$ wrt λ is the smallest difference between the acceptance probability of any word and λ.

Theorem

For every formula $\varphi \in \text{LTL(G)}$ there is a $\mathcal{M}, \lambda$ with $2^{O(|\varphi|)}$ states and $\frac{1}{2^{|\varphi|}}$ gap such that $\mathcal{M}$ with cutpoint λ recognizes φ.

	DBA	NBA	Strong Monitors	Weak Monitors	Robust Monitors
Safe-LTL	2-EXP	EXP	EXP	2-EXP	?
LTL(G)	2-EXP	EXP	EXP	EXP	with gap $\frac{1}{2^n}$: EXP

LTL(G)
Robust Monitors

Key idea: Syntactic Transformation

- Consider $\mathrm{LTL}_{\vee}(\mathrm{G})$ and show every formula has an equivalent *guarded* formula of the same size.
- Every guarded formula has deterministic automata of EXP size
- Convert φ in LTL(G) into a conjunct of $\mathrm{LTL}_{\vee}(\mathrm{G})$ formula by pulling out conjunction.
- Take disjoint union of deterministic monitor for each conjunct and start in any of them with equal probability.

Guarded: every subformula $G(\psi)$ of φ is of the form $G(\alpha \vee \beta)$ where α is disjunction of literals and β is a disjunction of formulae of the form $G\gamma$

LTL(G)

Robust Monitors with Large Gap

LTL(G)

Robust Monitors with Large Gap

Theorem

There is a family of LTL(G) formulae $\{\varphi_n\}_{n\in\mathbb{N}}$ of size $O(n)$ s.t any family of robust FPM with gap $\frac{1}{2^{o(n)}}$ that recognizes it has size $2^{2^{\Omega(n)}}$.

LTL(G)

Robust Monitors with Large Gap

Theorem

There is a family of LTL(G) formulae $\{\varphi_n\}_{n\in\mathbb{N}}$ of size $O(n)$ s.t any family of robust FPM with gap $\frac{1}{2^{o(n)}}$ that recognizes it has size $2^{2^{\Omega(n)}}$.

Idea: Use communication complexity as before to prove lower bound on constant gap and then use chernoff bounds.

Summary

	DBA	NBA	Strong Monitors	Weak Monitors	Robust Monitors
Safe-LTL	2-EXP	EXP	EXP	2-EXP	with gap $\frac{1}{2^{o(n)}}$: 2-EXP
LTL(G)	2-EXP	EXP	EXP	EXP	with gap $\frac{1}{2^{o(n)}}$: 2-EXP with gap $\frac{1}{2^n}$: EXP

It still remains open whether there are EXP sized robust monitors with small gap for Safe-LTL.

Thank You!

Questions?

Bibliography

C. Baier and M. Größer.

Recognizing ω-regular languages with probabilistic automata.
In *Proceedings of the IEEE Symposium on Logic in Computer Science*, pages 137–146, 2005.

Rohit Chadha, A. Prasad Sistla, and Mahesh Viswanathan.

On the expressiveness and complexity of randomization in finite state monitors.
Journal of ACM, 56(5):26:1–26:44, 2009.

I. Kremer, N. Nisan, and D. Ron.

On randomized one-round communication complexity.
Symposium on Theory of Computing, June 1995.

Orna Kupferman and Adin Rosenberg.

The blow-up in translating ltl to deterministic automata.
In *Proceedings of the 6th International Conference on Model Checking and Artificial Intelligence*, MoChArt'10, pages 85–94, Berlin, Heidelberg, 2010. Springer-Verlag.

Moshe Y. Vardi.

An automata-theoretic approach to linear temporal logic.
In *Logics for Concurrency: Structure versus Automata, volume 1043 of Lecture Notes in Computer Science*, pages 238–266. Springer-Verlag, 1996.