Robust Linear Temporal Logic

Paulo Tabuada [1] **Daniel Neider** [1,2]

[1]University of California, Los Angeles

[2]RWTH Aachen University

25th EACSL Annual Conference on Computer Science Logic

Marseille, France

29 September 2016

Logic and Theory of Discrete Systems

RWTH AACHEN UNIVERSITY

Motivation

$$\underbrace{\varphi}_{\text{Environment assumption}} \Rightarrow \underbrace{\psi}_{\text{System guarantee}}$$

$$\underbrace{\varphi}_{\text{Environment assumption}} \Rightarrow \underbrace{\psi}_{\text{System guarantee}}$$

Desired Notion of Robustness (from Wikipedia on fault tolerance)

"[...] If its operating quality decreases at all, the decrease is proportional to the severity of the failure, as compared to a naively designed system in which even a small failure can cause total breakdown. [...]"

$$\underbrace{\varphi}_{\text{Environment assumption}} \Rightarrow \underbrace{\psi}_{\text{System guarantee}}$$

Goal

Develop a semantics for LTL capturing "robustness"

- Here: only the fragment LTL($\Box, \Diamond$); full LTL on arXiv

$$\underbrace{\varphi}_{\text{Environment assumption}} \Rightarrow \underbrace{\psi}_{\text{System guarantee}}$$

Goal

Develop a semantics for LTL capturing "robustness"

- Here: only the fragment LTL($\Box, \Diamond$); full LTL on arXiv

Design Goals

1. Robustness should be internal to the logic
2. Familiarity with LTL should be the only prerequisite

Syntax of LTL($\Box, \Diamond$)

Let $\mathcal{P}$ be a (finite, nonempty) set of atomic propositions

- Each $p \in \mathcal{P}$ is an LTL($\Box, \Diamond$) formula; and
- if φ, ψ are LTL($\Box, \Diamond$) formulas, so are $\neg\varphi$, $\varphi \vee \psi$, $\Box\varphi$, and $\Diamond\varphi$

Syntax of LTL($\Box, \Diamond$)

Let $\mathcal{P}$ be a (finite, nonempty) set of atomic propositions

- Each $p \in \mathcal{P}$ is an LTL($\Box, \Diamond$) formula; and
- if φ, ψ are LTL($\Box, \Diamond$) formulas, so are $\neg\varphi$, $\varphi \vee \psi$, $\Box\varphi$, and $\Diamond\varphi$

Semantics of LTL($\Box, \Diamond$) ...

... is a function $W : \Phi_{\mathrm{LTL}(\Box,\Diamond)} \times (2^{\mathcal{P}})^{\omega} \to \mathbb{B}$ inductively defined by

Syntax of LTL($\Box, \Diamond$)

Let $\mathcal{P}$ be a (finite, nonempty) set of atomic propositions

- Each $p \in \mathcal{P}$ is an LTL($\Box, \Diamond$) formula; and
- if φ, ψ are LTL($\Box, \Diamond$) formulas, so are $\neg\varphi$, $\varphi \vee \psi$, $\Box\varphi$, and $\Diamond\varphi$

Semantics of LTL($\Box, \Diamond$) ...

... is a function $W \colon \Phi_{\mathrm{LTL}(\Box,\Diamond)} \times (2^{\mathcal{P}})^{\omega} \to \mathbb{B}$ inductively defined by

$$W(p, \sigma) = \begin{cases} 1 & \text{if } p \in \sigma(0) \\ 0 & \text{if } p \notin \sigma(0) \end{cases}$$

Syntax of LTL($\Box, \Diamond$)

Let $\mathcal{P}$ be a (finite, nonempty) set of atomic propositions

- Each $p \in \mathcal{P}$ is an LTL($\Box, \Diamond$) formula; and
- if φ, ψ are LTL($\Box, \Diamond$) formulas, so are $\neg\varphi$, $\varphi \vee \psi$, $\Box\varphi$, and $\Diamond\varphi$

Semantics of LTL($\Box, \Diamond$) ...

... is a function $W \colon \Phi_{\mathrm{LTL}(\Box,\Diamond)} \times (2^{\mathcal{P}})^{\omega} \to \mathbb{B}$ inductively defined by

$$W(p, \sigma) = \begin{cases} 1 & \text{if } p \in \sigma(0) \\ 0 & \text{if } p \notin \sigma(0) \end{cases}$$

$$W(\neg\varphi, \sigma) = 1 - W(\varphi, \sigma)$$

Syntax of LTL($\Box, \Diamond$)

Let $\mathcal{P}$ be a (finite, nonempty) set of atomic propositions

- Each $p \in \mathcal{P}$ is an LTL($\Box, \Diamond$) formula; and
- if φ, ψ are LTL($\Box, \Diamond$) formulas, so are $\neg\varphi$, $\varphi \vee \psi$, $\Box\varphi$, and $\Diamond\varphi$

Semantics of LTL($\Box, \Diamond$) ...

... is a function $W \colon \Phi_{\mathrm{LTL}(\Box,\Diamond)} \times (2^{\mathcal{P}})^{\omega} \to \mathbb{B}$ inductively defined by

$$W(p, \sigma) = \begin{cases} 1 & \text{if } p \in \sigma(0) \\ 0 & \text{if } p \notin \sigma(0) \end{cases}$$

$$W(\neg\varphi, \sigma) = 1 - W(\varphi, \sigma)$$

$$W(\varphi \vee \psi, \sigma) = \max\{W(\varphi, \sigma), W(\psi, \sigma)\}$$

Syntax of LTL($\Box, \Diamond$)

Let $\mathcal{P}$ be a (finite, nonempty) set of atomic propositions

- Each $p \in \mathcal{P}$ is an LTL($\Box, \Diamond$) formula; and

a	b	$a \vee b$	$\max\{a, b\}$	$a \wedge b$	$\min\{a, b\}$
0	0	0	0	0	0
0	1	1	1	0	0
1	0	1	1	0	0
1	1	1	1	1	1

$$W(\neg\varphi, \sigma) = 1 - W(\varphi, \sigma)$$

$$W(\varphi \vee \psi, \sigma) = \max\{W(\varphi, \sigma), W(\psi, \sigma)\}$$

Syntax of LTL($\Box, \Diamond$)

Let $\mathcal{P}$ be a (finite, nonempty) set of atomic propositions

- Each $p \in \mathcal{P}$ is an LTL($\Box, \Diamond$) formula; and
- if φ, ψ are LTL($\Box, \Diamond$) formulas, so are $\neg\varphi$, $\varphi \vee \psi$, $\Box\varphi$, and $\Diamond\varphi$

Semantics of LTL($\Box, \Diamond$) ...

... is a function $W \colon \Phi_{\mathrm{LTL}(\Box,\Diamond)} \times (2^{\mathcal{P}})^{\omega} \to \mathbb{B}$ inductively defined by

$$W(p, \sigma) = \begin{cases} 1 & \text{if } p \in \sigma(0) \\ 0 & \text{if } p \notin \sigma(0) \end{cases}$$

$$W(\neg\varphi, \sigma) = 1 - W(\varphi, \sigma)$$

$$W(\varphi \vee \psi, \sigma) = \max\{W(\varphi, \sigma), W(\psi, \sigma)\}$$

$$W(\Box\varphi, \sigma) = \inf_{i \geq 0}\{W(\varphi, \sigma_{i..})\}$$

Syntax of LTL($\Box, \Diamond$)

Let $\mathcal{P}$ be a (finite, nonempty) set of atomic propositions

- Each $p \in \mathcal{P}$ is an LTL($\Box, \Diamond$) formula; and
- if φ, ψ are LTL($\Box, \Diamond$) formulas, so are $\neg\varphi$, $\varphi \vee \psi$, $\Box\varphi$, and $\Diamond\varphi$

Semantics of LTL($\Box, \Diamond$) ...

... is a function $W \colon \Phi_{\mathrm{LTL}(\Box,\Diamond)} \times (2^{\mathcal{P}})^{\omega} \to \mathbb{B}$ inductively defined by

$$W(p, \sigma) = \begin{cases} 1 & \text{if } p \in \sigma(0) \\ 0 & \text{if } p \notin \sigma(0) \end{cases}$$

$$W(\neg\varphi, \sigma) = 1 - W(\varphi, \sigma)$$

$$W(\varphi \vee \psi, \sigma) = \max\{W(\varphi, \sigma), W(\psi, \sigma)\}$$

$$W(\Box\varphi, \sigma) = \inf_{i \geq 0}\{W(\varphi, \sigma_{i..})\}$$

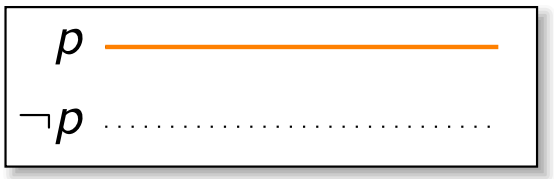
$$W(\Diamond\varphi, \sigma) = \sup_{i \geq 0}\{W(\varphi, \sigma_{i..})\}$$

Different Shades of False

Consider the specification $\Box p \Rightarrow \Box q$. How can $\Box p$ be violated?

Different Shades of False

Consider the specification $\Box p \Rightarrow \Box q$. How can $\Box p$ be violated?

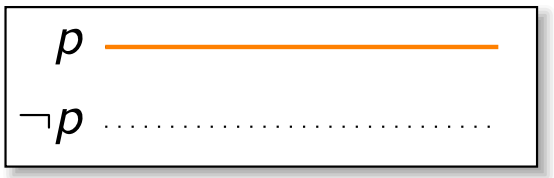


$\Box p$

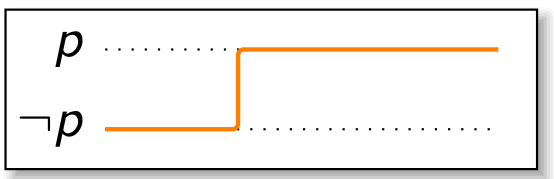
Weakening

Different Shades of False

Consider the specification $\Box p \Rightarrow \Box q$. How can $\Box p$ be violated?



$\Box p$

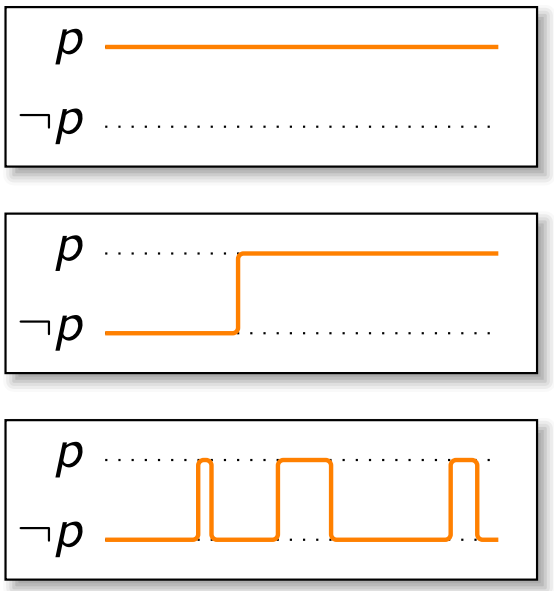


$\Diamond \Box p$

Weakening

Different Shades of False

Consider the specification $\Box p \Rightarrow \Box q$. How can $\Box p$ be violated?



$\Box p$

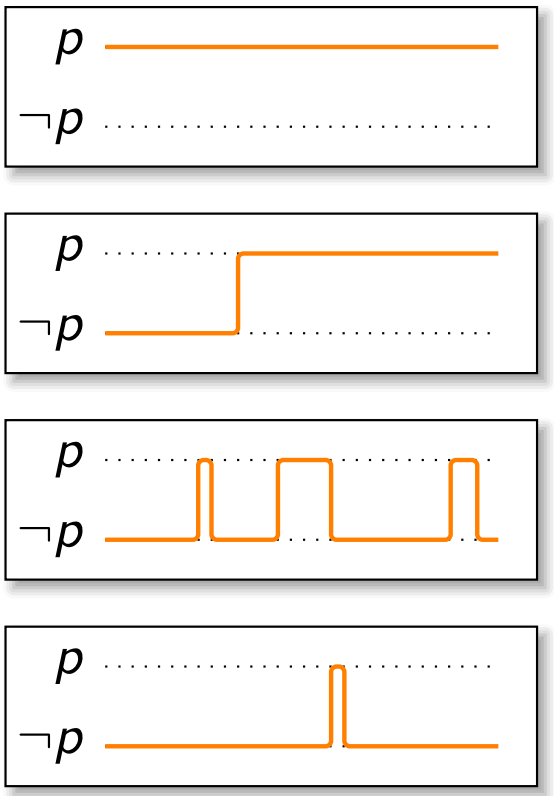
$\Diamond \Box p$

$\Box \Diamond p$

Weakening

Different Shades of False

Consider the specification $\Box p \Rightarrow \Box q$. How can $\Box p$ be violated?



$\Box p$

$\Diamond \Box p$

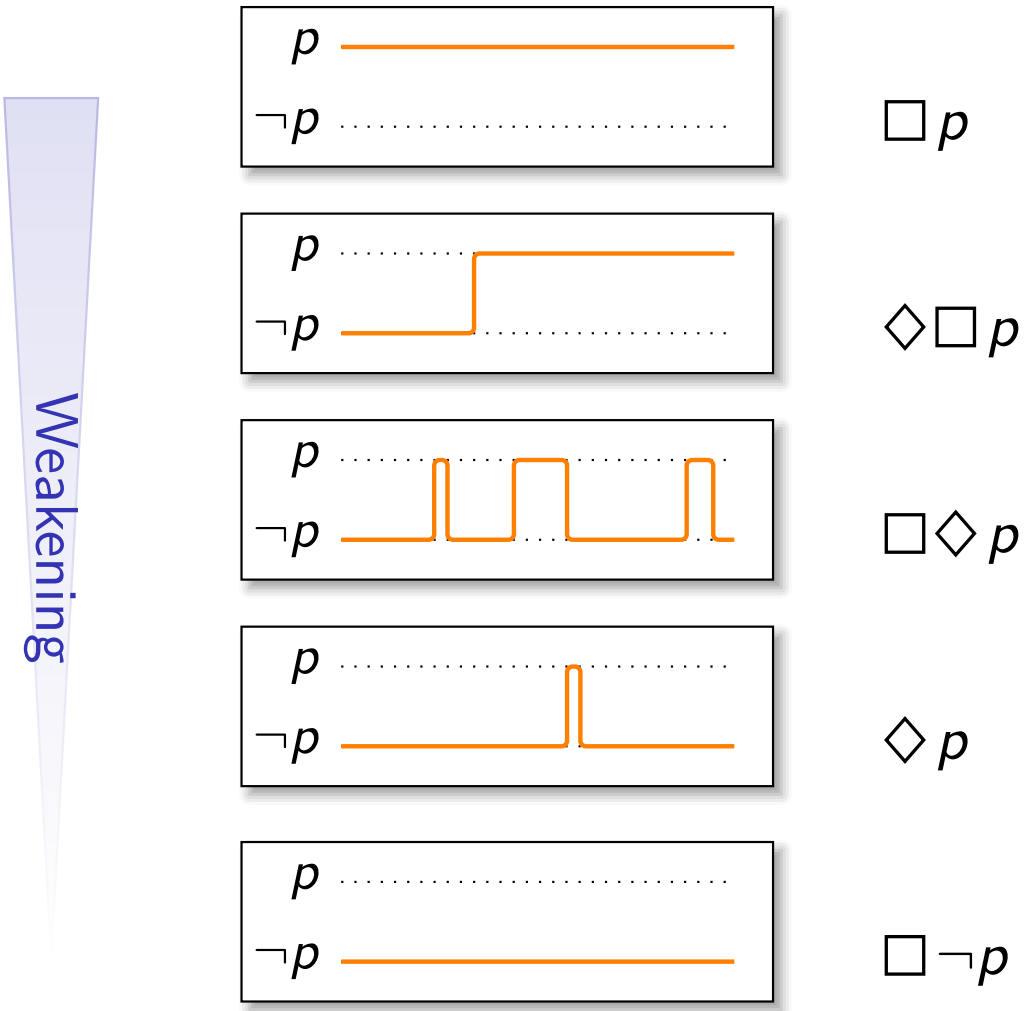
$\Box \Diamond p$

$\Diamond p$

Weakening

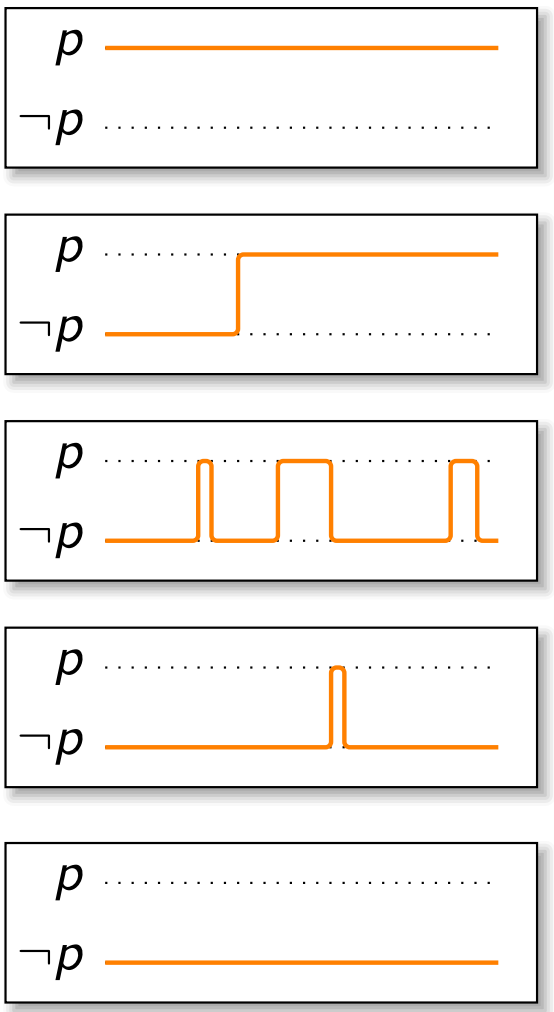
Different Shades of False

Consider the specification $\Box p \Rightarrow \Box q$. How can $\Box p$ be violated?



Different Shades of False

Consider the specification $\Box p \Rightarrow \Box q$. How can $\Box p$ be violated?



Weakening

$\Box p$

$\Diamond \Box p$

$\Box \Diamond p$

$\Diamond p$

$\Box \neg p$

true

$(1,1,1,1)$

$(0,1,1,1)$

$(0,0,1,1)$

$(0,0,0,1)$

$(0,0,0,0)$

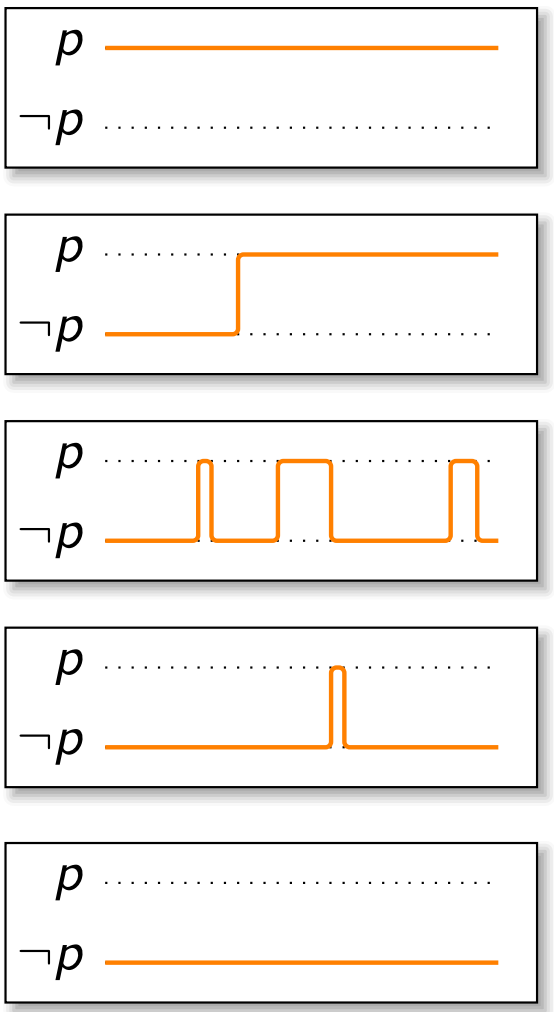
false

shades of false

Different Shades of False

Consider the specification $\Box p \Rightarrow \Box q$. How can $\Box p$ be violated?

Weakening



$\Box p$ $(1,1,1,1)$

$\Diamond \Box p$ $(0,1,1,1)$

$\Box \Diamond p$ $(0,0,1,1)$

$\Diamond p$ $(0,0,0,1)$

$\Box \neg p$ $(0,0,0,0)$

$\mathbb{B}_4$

A Da Costa Algebra over $\mathbb{B}_4$

Elements of $\mathbb{B}_4$ are ordered:

$$(0,0,0,0) < (0,0,0,1) < (0,0,1,1) < (0,1,1,1) < (1,1,1,1)$$

We introduce the following four operations:

A Da Costa Algebra over $\mathbb{B}_4$

Elements of $\mathbb{B}_4$ are ordered:

$$(0,0,0,0) < (0,0,0,1) < (0,0,1,1) < (0,1,1,1) < (1,1,1,1)$$

We introduce the following four operations:

- $a \sqcap b = \min\{a, b\}$
- $a \sqcup b = \max\{a, b\}$

A Da Costa Algebra over $\mathbb{B}_4$

Elements of $\mathbb{B}_4$ are ordered:

W

		Negation
	$(1,1,1,1)$	$(0,0,0,0)$
	$(0,1,1,1)$	$(1,1,1,1)$
	$(0,0,1,1)$	$(1,1,1,1)$
	$(0,0,0,1)$	$(1,1,1,1)$
	$(0,0,0,0)$	$(1,1,1,1)$

A Da Costa Algebra over $\mathbb{B}_4$

Elements of $\mathbb{B}_4$ are ordered:

$$(0,0,0,0) < (0,0,0,1) < (0,0,1,1) < (0,1,1,1) < (1,1,1,1)$$

We introduce the following four operations:

- $a \sqcap b = \min\{a, b\}$
- $a \sqcup b = \max\{a, b\}$
- $\overline{a} = \begin{cases} (0,0,0,0) & \text{if } a = (1,1,1,1) \\ (1,1,1,1) & \text{otherwise} \end{cases}$

A Da Costa Algebra over $\mathbb{B}_4$

Elements of $\mathbb{B}_4$ are ordered:

$$(0,0,0,0) < (0,0,0,1) < (0,0,1,1) < (0,1,1,1) < (1,1,1,1)$$

We introduce the following four operations:

- $a \sqcap b = \min\{a, b\}$
- $a \sqcup b = \max\{a, b\}$
- $\overline{a} = \begin{cases} (0,0,0,0) & \text{if } a = (1,1,1,1) \\ (1,1,1,1) & \text{otherwise} \end{cases}$
- $a \to b = \begin{cases} (1,1,1,1) & \text{if } a \leq b \\ b & \text{otherwise} \end{cases}$

A Da Costa Algebra over $\mathbb{B}_4$

Elements of $\mathbb{B}_4$ are ordered:

$$(0,0,0,0) < (0,0,0,1) < (0,0,1,1) < (0,1,1,1) < (1,1,1,1)$$

We introduce the following four operations:

- $a \sqcap b = \min\{a, b\}$
- $a \sqcup b = \max\{a, b\}$
- $\overline{a} = \begin{cases} (0,0,0,0) & \text{if } a = (1,1,1,1) \\ (1,1,1,1) & \text{otherwise} \end{cases}$
- $a \to b = \begin{cases} (1,1,1,1) & \text{if } a \leq b \\ b & \text{otherwise} \end{cases}$

The structure $(\mathbb{B}_4, <, \sqcap, \sqcup, \overline{\cdot}, \to)$ is a so-called da Costa algebra

Robust Semantics

We use new symbols $\boxdot$, $\diamondsuit$ and call this "logic" rLTL

The semantics of rLTL($\boxdot, \diamondsuit$) is a function
$V : \Phi_{\text{rLTL}(\boxdot,\diamondsuit)} \times (2^{\mathcal{P}})^{\omega} \to \mathbb{B}_4$ inductively defined by

Robust Semantics

We use new symbols $\boxdot$, $\diamondsuit$ and call this "logic" rLTL

The semantics of rLTL($\boxdot, \diamondsuit$) is a function
$V : \Phi_{\text{rLTL}(\boxdot,\diamondsuit)} \times (2^{\mathcal{P}})^{\omega} \to \mathbb{B}_4$ inductively defined by

- $V(p, \sigma) = \begin{cases} (1,1,1,1) & \text{if } p \in \sigma(0) \\ (0,0,0,0) & \text{otherwise} \end{cases}$

We use new symbols $\boxdot$, $\diamondsuit$ and call this "logic" rLTL

The semantics of rLTL($\boxdot, \diamondsuit$) is a function
$V : \Phi_{\text{rLTL}(\boxdot,\diamondsuit)} \times (2^{\mathcal{P}})^{\omega} \to \mathbb{B}_4$ inductively defined by

- $V(p, \sigma) = \begin{cases} (1,1,1,1) & \text{if } p \in \sigma(0) \\ (0,0,0,0) & \text{otherwise} \end{cases}$
- $V(\varphi \wedge \psi, \sigma) = V(\varphi, \sigma) \sqcap V(\psi, \sigma)$
- $V(\varphi \vee \psi, \sigma) = V(\varphi, \sigma) \sqcup V(\psi, \sigma)$
- $V(\neg\varphi, \sigma) = \overline{V(\varphi, \sigma)}$
- $V(\varphi \Rightarrow \psi, \sigma) = V(\varphi, \sigma) \to V(\psi, \sigma)$

We use new symbols $\boxdot$, $\diamondsuit$ and call this "logic" rLTL

The semantics of rLTL($\boxdot, \diamondsuit$) is a function
$V : \Phi_{\text{rLTL}(\boxdot,\diamondsuit)} \times (2^{\mathcal{P}})^{\omega} \to \mathbb{B}_4$ inductively defined by

- $V(p, \sigma) = \begin{cases} (1,1,1,1) & \text{if } p \in \sigma(0) \\ (0,0,0,0) & \text{otherwise} \end{cases}$
- $V(\varphi \wedge \psi, \sigma) = V(\varphi, \sigma) \sqcap V(\psi, \sigma)$
- $V(\varphi \vee \psi, \sigma) = V(\varphi, \sigma) \sqcup V(\psi, \sigma)$
- $V(\neg\varphi, \sigma) = \overline{V(\varphi, \sigma)}$
- $V(\varphi \Rightarrow \psi, \sigma) = V(\varphi, \sigma) \to V(\psi, \sigma)$
- $V(\boxdot p, \sigma) = (\Box p,\ \diamondsuit\Box p,\ \Box\diamondsuit p,\ \diamondsuit p)$

Robust Semantics

We use new symbols $\boxdot$, $\diamondsuit$ and call this "logic" rLTL

σ	$\sigma(0)$	$\sigma(1)$	$\sigma(2)$	
$V(\varphi, \sigma_{i..})$	$(0,1,1,1)$	$(0,0,1,1)$	$(0,0,1,1)$	$\cdots$

- $V(\boxdot p, \sigma) = (\Box p,\ \diamondsuit\Box p,\ \Box\diamondsuit p,\ \diamondsuit p)$

We use new symbols $\boxdot$, $\diamondsuit$ and call this "logic" rLTL

σ	$\sigma(0)$	$\sigma(1)$	$\sigma(2)$	
$V(\varphi, \sigma_{i..})$	$(0,1,1,1)$	$(0,0,1,1)$	$(0,0,1,1)$	$\cdots$

φ_1: $000\ldots$

φ_2: $100\ldots$

φ_3: $111\ldots$

φ_4: $111\ldots$

- $V(\boxdot p, \sigma) = (\Box p,\ \diamondsuit\Box p,\ \Box\diamondsuit p,\ \diamondsuit p)$

Robust Semantics

We use new symbols $\boxdot$, $\diamondsuit$ and call this "logic" rLTL

σ	$\sigma(0)$	$\sigma(1)$	$\sigma(2)$	
$V(\varphi, \sigma_{i..})$	$(0,1,1,1)$	$(0,0,1,1)$	$(0,0,1,1)$	$\cdots$

φ_1: $000\ldots$

φ_2: $100\ldots$

φ_3: $111\ldots$

φ_4: $111\ldots$

- $V(\boxdot p, \sigma) = (\Box p,\ \diamondsuit\Box p,\ \Box\diamondsuit p,\ \diamondsuit p)$

We use new symbols $\boxdot$, $\diamondsuit$ and call this "logic" rLTL

The semantics of rLTL($\boxdot, \diamondsuit$) is a function
$V : \Phi_{\text{rLTL}(\boxdot,\diamondsuit)} \times (2^{\mathcal{P}})^{\omega} \to \mathbb{B}_4$ inductively defined by

- $V(p, \sigma) = \begin{cases} (1,1,1,1) & \text{if } p \in \sigma(0) \\ (0,0,0,0) & \text{otherwise} \end{cases}$
- $V(\varphi \wedge \psi, \sigma) = V(\varphi, \sigma) \sqcap V(\psi, \sigma)$
- $V(\varphi \vee \psi, \sigma) = V(\varphi, \sigma) \sqcup V(\psi, \sigma)$
- $V(\neg\varphi, \sigma) = \overline{V(\varphi, \sigma)}$
- $V(\varphi \Rightarrow \psi, \sigma) = V(\varphi, \sigma) \to V(\psi, \sigma)$
- $V(\boxdot\varphi, \sigma) = (\Box\varphi_1,\ \diamondsuit\Box\varphi_2,\ \Box\diamondsuit\varphi_3,\ \diamondsuit\varphi_4)$

We use new symbols $\boxdot$, $\diamondsuit$ and call this "logic" rLTL

The semantics of rLTL($\boxdot, \diamondsuit$) is a function
$V : \Phi_{\text{rLTL}(\boxdot,\diamondsuit)} \times (2^{\mathcal{P}})^{\omega} \to \mathbb{B}_4$ inductively defined by

- $V(p, \sigma) = \begin{cases} (1,1,1,1) & \text{if } p \in \sigma(0) \\ (0,0,0,0) & \text{otherwise} \end{cases}$
- $V(\varphi \wedge \psi, \sigma) = V(\varphi, \sigma) \sqcap V(\psi, \sigma)$
- $V(\varphi \vee \psi, \sigma) = V(\varphi, \sigma) \sqcup V(\psi, \sigma)$
- $V(\neg\varphi, \sigma) = \overline{V(\varphi, \sigma)}$
- $V(\varphi \Rightarrow \psi, \sigma) = V(\varphi, \sigma) \to V(\psi, \sigma)$
- $V(\boxdot\varphi, \sigma) = (\Box\varphi_1,\ \diamondsuit\Box\varphi_2,\ \Box\diamondsuit\varphi_3,\ \diamondsuit\varphi_4)$
- $V(\diamondsuit\varphi, \sigma) = (\diamondsuit\varphi_1,\ \diamondsuit\varphi_2,\ \diamondsuit\varphi_3,\ \diamondsuit\varphi_4)$

Example

Consider $\boxdot p \Rightarrow \boxdot q$, and assume $V(\boxdot p \Rightarrow \boxdot q, \sigma) = (1,1,1,1)$

Recall: $$a \to b = \begin{cases} (1,1,1,1) & \text{if } a \leq b \\ b & \text{otherwise} \end{cases}$$

Example

Consider $\boxdot p \Rightarrow \boxdot q$, and assume $V(\boxdot p \Rightarrow \boxdot q, \sigma) = (1,1,1,1)$

- If $\Box p$ holds, then $\boxdot p$ evaluates to $(1,1,1,1)$. Hence, $\boxdot q$ has to evaluate to $(1,1,1,1)$, which means that $\Box q$ holds

Recall: $$a \to b = \begin{cases} (1,1,1,1) & \text{if } a \leq b \\ b & \text{otherwise} \end{cases}$$

Example

Consider $\boxdot p \Rightarrow \boxdot q$, and assume $V(\boxdot p \Rightarrow \boxdot q, \sigma) = (1,1,1,1)$

- If $\Box p$ holds, then $\boxdot p$ evaluates to $(1,1,1,1)$. Hence, $\boxdot q$ has to evaluate to $(1,1,1,1)$, which means that $\Box q$ holds
- If $\Diamond\Box p$ holds (and $\Box p$ does not), then $\boxdot p$ evaluates to $(0,1,1,1)$. Hence, $\boxdot q$ has to evaluate to $(0,1,1,1)$ or higher, which implies that $\Diamond\Box q$ holds

Recall: $$a \to b = \begin{cases} (1,1,1,1) & \text{if } a \leq b \\ b & \text{otherwise} \end{cases}$$

Example

Consider $\boxdot p \Rightarrow \boxdot q$, and assume $V(\boxdot p \Rightarrow \boxdot q, \sigma) = (1,1,1,1)$

- If $\Box p$ holds, then $\boxdot p$ evaluates to $(1,1,1,1)$. Hence, $\boxdot q$ has to evaluate to $(1,1,1,1)$, which means that $\Box q$ holds
- If $\Diamond\Box p$ holds (and $\Box p$ does not), then $\boxdot p$ evaluates to $(0,1,1,1)$. Hence, $\boxdot q$ has to evaluate to $(0,1,1,1)$ or higher, which implies that $\Diamond\Box q$ holds
- Similarly, $\Box\Diamond p$ implies $\Box\Diamond q$ and $\Diamond p$ implies $\Diamond q$

Recall: $$a \rightarrow b = \begin{cases} (1,1,1,1) & \text{if } a \leq b \\ b & \text{otherwise} \end{cases}$$

Example

Consider $\boxdot p \Rightarrow \boxdot q$, and assume $V(\boxdot p \Rightarrow \boxdot q, \sigma) < (1,1,1,1)$

Recall: $a \to b = \begin{cases} (1,1,1,1) & \text{if } a \leq b \\ b & \text{otherwise} \end{cases}$

Example

Consider $\boxdot p \Rightarrow \boxdot q$, and assume $V(\boxdot p \Rightarrow \boxdot q, \sigma) < (1,1,1,1)$

- If $V(\boxdot p \Rightarrow \boxdot q, \sigma) = b < (1,1,1,1)$, then

$$V(\boxdot q, \sigma) = b \quad \text{and} \quad V(\boxdot p, \sigma) > b$$

Recall: $$a \to b = \begin{cases} (1,1,1,1) & \text{if } a \leq b \\ b & \text{otherwise} \end{cases}$$

Example

Consider $\boxdot p \Rightarrow \boxdot q$, and assume $V(\boxdot p \Rightarrow \boxdot q, \sigma) < (1,1,1,1)$

- If $V(\boxdot p \Rightarrow \boxdot q, \sigma) = b < (1,1,1,1)$, then

$$V(\boxdot q, \sigma) = b \quad \text{and} \quad V(\boxdot p, \sigma) > b$$

- Thus, value $V(\boxdot p \Rightarrow \boxdot q, \sigma)$ describes which weakened guarantee follows from the environment assumption whenever the intended system guarantee does not follow

Recall: $$a \to b = \begin{cases} (1,1,1,1) & \text{if } a \leq b \\ b & \text{otherwise} \end{cases}$$

Theorem

LTL($\Box, \Diamond$) and rLTL($\boxdot, \diamondsuit$) are *equally expressive*:

Theorem

LTL($\Box, \Diamond$) and rLTL($\boxdot, \diamondsuit$) are *equally expressive*:

- Given an LTL($\Box, \Diamond$) formula ψ, one can construct an rLTL($\boxdot, \diamondsuit$) formula φ such that for $\sigma \in (2^{\mathcal{P}})^{\omega}$

$$V(\varphi, \sigma) = (1, 1, 1, 1) \text{ if and only if } W(\psi, \sigma) = 1$$

Theorem

LTL($\Box, \Diamond$) and rLTL($\boxdot, \diamondsuit$) are *equally expressive*:

- Given an LTL($\Box, \Diamond$) formula ψ, one can construct an rLTL($\boxdot, \diamondsuit$) formula φ such that for $\sigma \in (2^{\mathcal{P}})^{\omega}$

$$V(\varphi, \sigma) = (1, 1, 1, 1) \text{ if and only if } W(\psi, \sigma) = 1$$

- Given an rLTL($\boxdot, \diamondsuit$) formula φ and $b \in \mathbb{B}_4$, one can construct an LTL($\Box, \Diamond$) formula ψ such that for $\sigma \in (2^{\mathcal{P}})^{\omega}$

$$V(\varphi, \sigma) = b \text{ if and only if } W(\psi, \sigma) = 1$$

Theorem

LTL($\Box, \Diamond$) and rLTL($\boxdot, \diamondsuit$) are *equally expressive*:

- Given an LTL($\Box, \Diamond$) formula ψ, one can construct an rLTL($\boxdot, \diamondsuit$) formula φ such that for $\sigma \in (2^{\mathcal{P}})^{\omega}$

$$V(\varphi, \sigma) = (1, 1, 1, 1) \text{ if and only if } W(\psi, \sigma) = 1$$

- Given an rLTL($\boxdot, \diamondsuit$) formula φ and $b \in \mathbb{B}_4$, one can construct an LTL($\Box, \Diamond$) formula ψ such that for $\sigma \in (2^{\mathcal{P}})^{\omega}$

$$V(\varphi, \sigma) = b \text{ if and only if } W(\psi, \sigma) = 1$$

However, $|\psi| \in \mathcal{O}(c^{|\varphi|})$ for a suitable $c \geq 4$

Theorem

Given an rLTL($\boxdot, \diamondsuit$) formula φ and a set $B \subseteq \mathbb{B}_4$, one can construct a generalized Büchi Automaton $\mathcal{A}_\varphi^B$ such that for all $\sigma \in (2^{\mathcal{P}})^\omega$

$$V(\varphi, \sigma) \in B \text{ if and only if } \sigma \in L(\mathcal{A}_\varphi^B).$$

$\mathcal{A}_\varphi^B$ comprises $\mathcal{O}(5^{|\varphi|})$ states and at most $4 \cdot |\varphi|$ acceptance sets.

Theorem

Given an rLTL($\boxdot, \diamondsuit$) formula φ and a set $B \subseteq \mathbb{B}_4$, one can construct a generalized Büchi Automaton $\mathcal{A}_\varphi^B$ such that for all $\sigma \in (2^{\mathcal{P}})^\omega$

$$V(\varphi, \sigma) \in B \text{ if and only if } \sigma \in L(\mathcal{A}_\varphi^B).$$

$\mathcal{A}_\varphi^B$ comprises $\mathcal{O}(5^{|\varphi|})$ states and at most $4 \cdot |\varphi|$ acceptance sets.

	Time complexity	
	rLTL($\boxdot, \diamondsuit$)	LTL
Model checking	$5^{\lvert\varphi\rvert}$	$2^{\lvert\varphi\rvert}$
Synthesis	$2^{5^{\lvert\varphi\rvert}}$	$2^{2^{\lvert\varphi\rvert}}$

Consider the formula $\Diamond p \Rightarrow \Diamond q$

We prefer

$$\Box\neg q \prec \Diamond q \prec \Box\Diamond q \prec \Diamond\Box q \prec \Box q$$

Consider the formula $\Diamond p \Rightarrow \Diamond q$

We prefer

$$\Box\neg q \prec \Diamond q \prec \Box\Diamond q \prec \Diamond\Box q \prec \Box q$$

$$\underbrace{(0,0,0,0)}_{\text{False}} < \underbrace{(0,0,0,1) < (0,0,1,1) < (0,1,1,1) < (1,1,1,1)}_{\text{Shades of true}}$$

Consider the formula $\Diamond p \Rightarrow \Diamond q$

We prefer

$$\Box\neg q \prec \Diamond q \prec \Box\Diamond q \prec \Diamond\Box q \prec \Box q$$

$$\underbrace{(0,0,0,0)}_{\text{False}} < \underbrace{(0,0,0,1) < (0,0,1,1) < (0,1,1,1) < (1,1,1,1)}_{\text{Shades of true}}$$

$$\overline{a} = \begin{cases} (1,1,1,1) & \text{if } a = (0,0,0,0) \\ (0,0,0,0) & \text{otherwise} \end{cases}$$

An algebra with this negation is called Heyting algebra

Summary

- We introduced a semantics for LTL capturing robustness
- We demonstrated how to leverage the existing wealth of techniques for LTL

Get the full paper from arXiv!

Future Work

- Address the "problem" of operators that work differently from classical logics (e.g., "$\neg\neg\varphi \neq \varphi$")
- Can we improve on the size of $\mathcal{A}_\varphi^B$?
- Do (complexity) results for LTL fragments carry over (e.g., GR(1))?

Construct for an rLTL($\boxdot, \diamondsuit$) (sub-)formula φ four LTL($\Box, \Diamond$) formulas $\psi_\varphi^1, \psi_\varphi^2, \psi_\varphi^3, \psi_\varphi^4$ such that for $\sigma \in (2^{\mathcal{P}})^\omega$ and $j \in \{1, \ldots, 4\}$

$$V_j(\varphi, \sigma) = 1 \text{ if and only if } \sigma \models \psi_\varphi^j$$

1. If $\varphi = p$, then $\psi_\varphi^j := p$
2. If $\varphi = \varphi_1 \wedge \varphi_2$, then $\psi_\varphi^j := \psi_{\varphi_1}^j \wedge \psi_{\varphi_2}^j$
3. If $\varphi = \varphi_1 \vee \varphi_2$, then $\psi_\varphi^j := \psi_{\varphi_1}^j \vee \psi_{\varphi_2}^j$
4. If $\varphi = \diamondsuit \varphi'$, then $\psi_\varphi^j := \Diamond \psi_{\varphi'}^j$
5. If $\varphi = \boxdot \varphi'$, then $\psi_\varphi^1 := \Box \psi_{\varphi'}^1$, $\psi_\varphi^2 := \Diamond \Box \psi_{\varphi'}^2$, ...
6. If $\varphi = \neg \varphi'$, then $\psi_\varphi^j := \neg(\psi_{\varphi'}^1 \wedge \psi_{\varphi'}^2 \wedge \psi_{\varphi'}^3 \wedge \psi_{\varphi'}^4)$
7. If $\varphi = \varphi_1 \Rightarrow \varphi_2$, then $\psi_\varphi^j := (\bigvee_{k=1,\ldots,4} \psi_{\varphi_1}^k \wedge \neg \psi_{\varphi_1}^k) \Rightarrow \psi_{\varphi_2}^j$

Note: $|\psi_\varphi^j| \in \mathcal{O}(c^{|\varphi|})$ for a suitable $c \geq 4$

From rLTL($\boxdot, \diamondsuit$) to Generalized Büchi Automata

σ	$\{p\}$	$\{q\}$	$\emptyset$	$\{q\}$	$\emptyset$	$\ldots$

From rLTL($\boxdot, \diamondsuit$) to Generalized Büchi Automata

	σ	$\{p\}$	$\{q\}$	$\emptyset$	$\{q\}$	$\emptyset$	$\ldots$
LTL	p	1	0	0	0	0	
	q	0	1	0	1	0	$\ldots$
	$p \vee q$	1	1	0	1	0	
	$\Box(p \vee q)$	0	0	0	0	0	

- States: valuations of subformulas
- Transitions: defined according to expansion rules
- Acceptance conditions: assert that an infinite run respects the temporal operators

From rLTL($\boxdot, \diamondsuit$) to Generalized Büchi Automata

	σ	$\{p\}$	$\{q\}$	$\emptyset$	$\{q\}$	$\emptyset$	$\ldots$
LTL	p	1	0	0	0	0	
	q	0	1	0	1	0	
	$p \vee q$	1	1	0	1	0	$\ldots$
	$\Box(p \vee q)$	0	0	0	0	0	
rLTL	p	1111	0000	0000	0000	0000	
	q	0000	1111	0000	1111	0000	
	$p \vee q$	1111	1111	0000	1111	0000	$\ldots$
	$\boxdot(p \vee q)$	0011	0011	0011	0011	0011	

- States: valuations of subformulas
- Transitions: defined according to expansion rules
- Acceptance conditions: assert that an infinite run respects the temporal operators

Expansion Rule for $\boxdot$

Recall: $\boxdot\varphi = (\Box\varphi_1, \Diamond\Box\varphi_2, \Box\Diamond\varphi_3, \Diamond\varphi_4)$

$$\Box\varphi_1 = \varphi_1 \wedge \bigcirc\Box\varphi_1$$

$$\Diamond\Box\varphi_2 = \Box\varphi_2 \vee \bigcirc\Diamond\Box\varphi_2$$

$$\Box\Diamond\varphi_3 = \Diamond\varphi_3 \wedge \bigcirc\Box\Diamond\varphi_3$$

$$\Diamond\varphi_4 = \varphi_4 \vee \bigcirc\Diamond\varphi_4$$

Expansion Rule for $\boxdot$

Recall: $\boxdot\varphi = (\Box\varphi_1, \Diamond\Box\varphi_2, \Box\Diamond\varphi_3, \Diamond\varphi_4)$

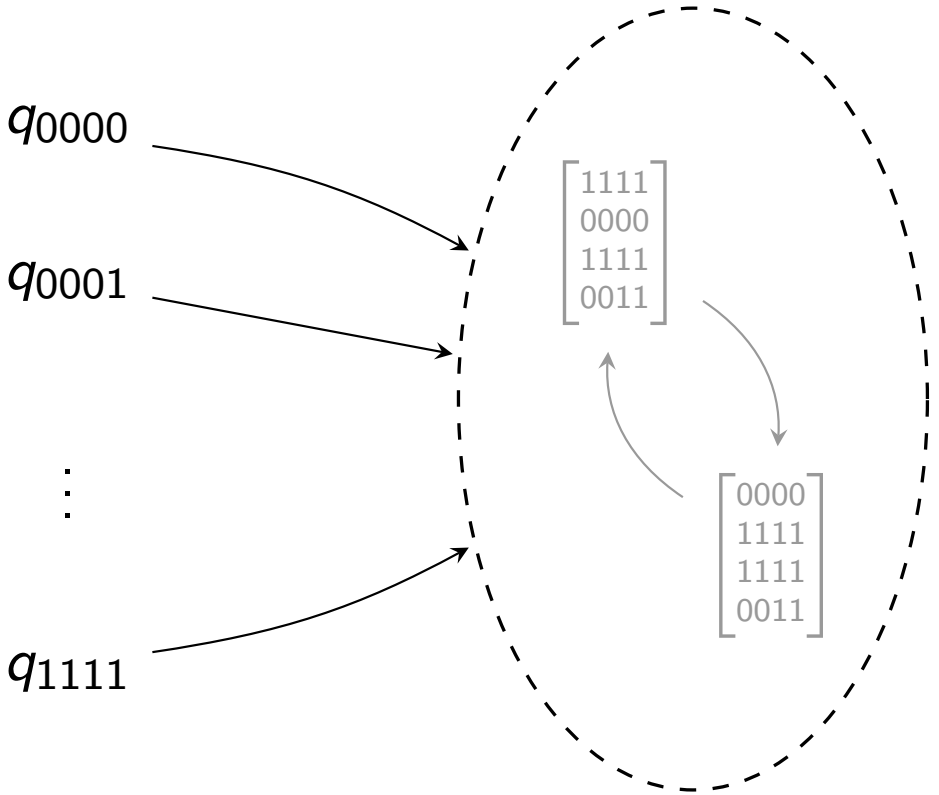
$$\Box\varphi_1 = \varphi_1 \wedge \bigcirc\Box\varphi_1$$

$$\Diamond\Box\varphi_2 = \Box\varphi_1 \vee \bigcirc\Diamond\Box\varphi_2$$

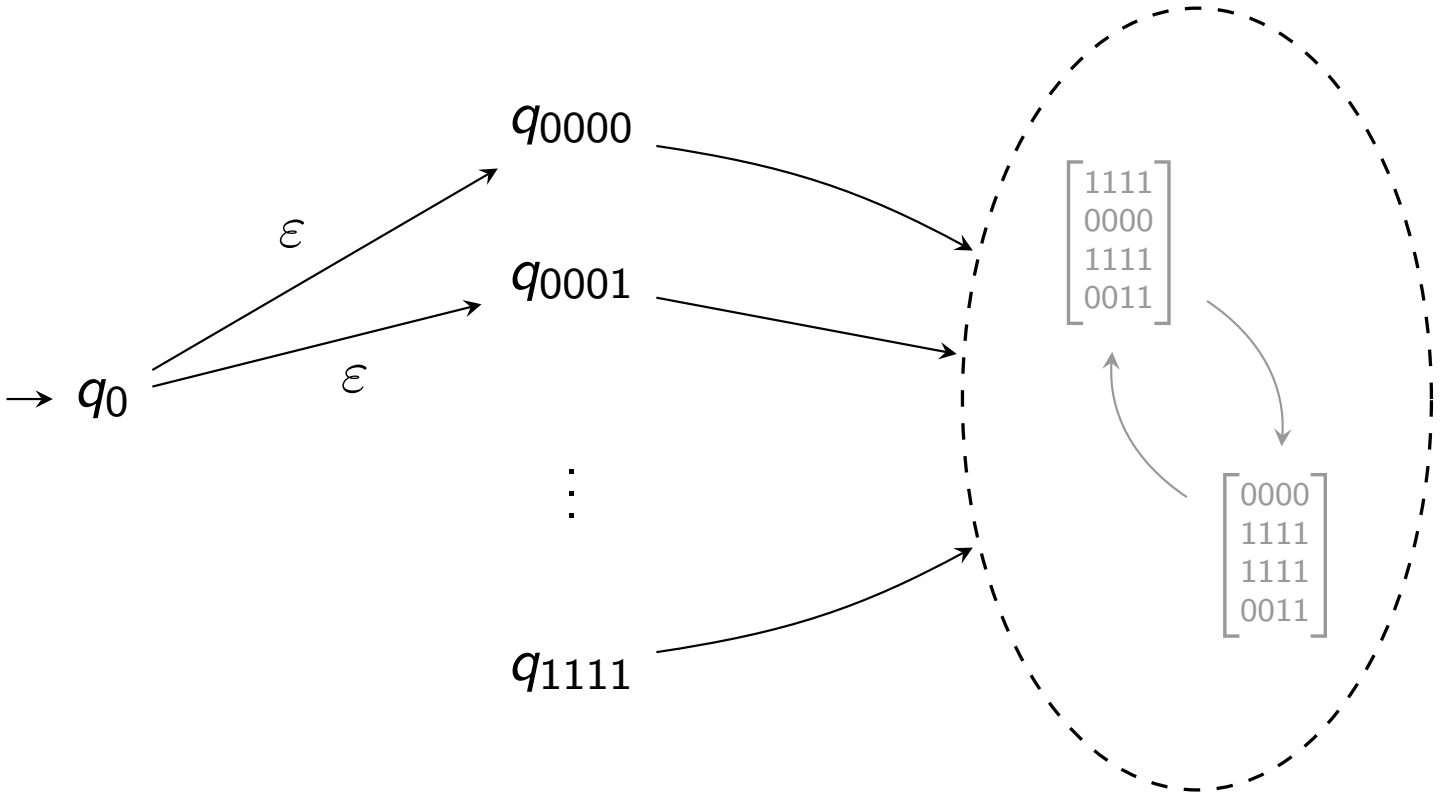
$$\Box\Diamond\varphi_3 = \Diamond\varphi_4 \wedge \bigcirc\Box\Diamond\varphi_3$$

$$\Diamond\varphi_4 = \varphi_4 \vee \bigcirc\Diamond\varphi_4$$

The automaton $\mathcal{A}_\varphi^B$



The automaton $\mathcal{A}_\varphi^B$



Note: $\mathcal{A}_\varphi^B$ has $5^{|\varphi|} + 6$ states