From LTL to rLTL Monitoring

Maximilian Schwenger

Joint Work With Corto Mascle, Daniel Neider, Paulo Tabuada, Alexander Weinert, Martin Zimmermann

OSARES

CPEC
CENTER FOR PERSPICUOUS COMPUTING

Why rLTL rather than LTL?

Assumption	$\Longrightarrow$	Guarantee
View Always Unobstructed	$\Longrightarrow$	Always Stay on Lane

$$G(\text{unobs. view}) \Longrightarrow G(\text{on lane})$$

WHY rLTL RATHER THAN LTL?

Assumption $\implies$ Guarantee

View Always Unobstructed $\implies$ Always Stay on Lane

G(unobs. view) $\implies$ G(on lane)

Problem 1: One Frame Camera Glitch $\implies$ Do Whatever You Want

Why rLTL rather than LTL?

Assumption ⟹ Guarantee

View Always Unobstructed ⟹ Always Stay on Lane

G(unobs. view) ⟹ G(on lane)

Problem 1: One Frame Camera Glitch ⟹ Do Whatever You Want

Problem 2: Crash Immediately ⟺ Drive Perfectly

WHY rLTL RATHER THAN LTL?

Assumption ⟹ Guarantee

View Always Unobstructed ⟹ Always Stay on Lane

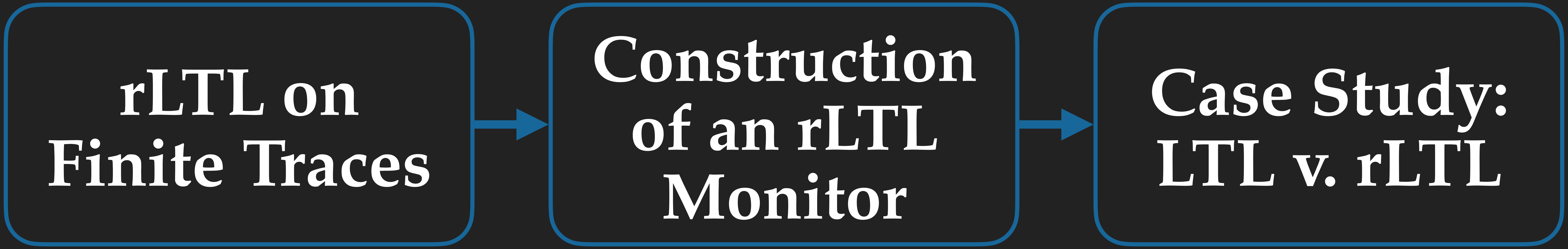
G(unobs. view) ⟹ G(on lane)

LTL to rLTL:
More Robustness
More Information

Problem 1: One Frame Camera Glitch ⟹ Do Whatever You Want

Problem 2: Crash Immediately ⟺ Drive Perfectly

Lift Monitoring from LTL to rLTL

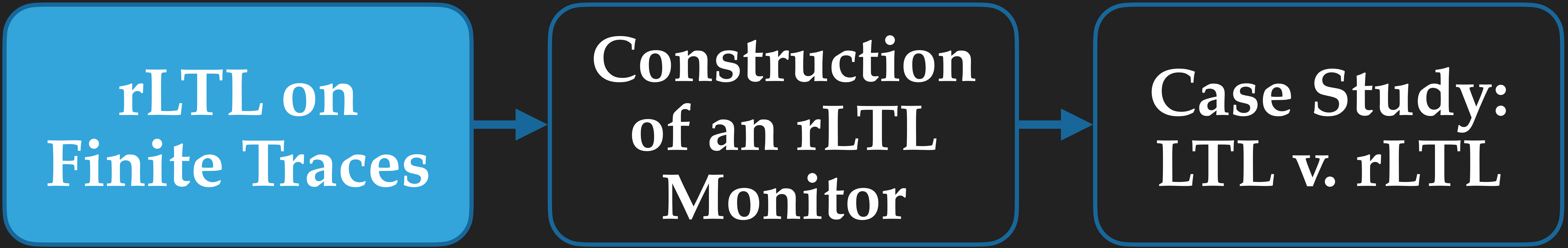


rLTL on Finite Traces

Construction of an rLTL Monitor

Case Study: LTL v. rLTL

Lift Monitoring from LTL to rLTL



rLTL on Finite Traces

Construction of an rLTL Monitor

Case Study: LTL v. rLTL

What you need to know about (r)LTL semantics

LTL

$a \in \Sigma, \quad \text{AP} = 2^{\Sigma}, \quad \text{trace } \pi \in \text{AP}^{\omega}$

Example

$\varphi \equiv a$

$\pi = \{a\} \; * \; * \; *$

Manna, Pnueli. "*Temporal verification of reactive systems*". 1995.

What you need to know about (r)LTL semantics

LTL

$a \in \Sigma, \quad \mathsf{AP} = 2^{\Sigma}, \quad \text{trace } \pi \in \mathsf{AP}^{\omega}$

Example

$$\varphi \equiv a \qquad \pi = \{a\} \; * \; * \; *$$

$$\varphi \equiv \mathbf{G}a \qquad \pi = \{a\}\{a\}\{a\}\{a\}$$

Manna, Pnueli. "*Temporal verification of reactive systems*". 1995.

What you need to know about (r)LTL semantics

LTL

$a \in \Sigma, \quad \text{AP} = 2^{\Sigma}, \quad \text{trace } \pi \in \text{AP}^{\omega}$

Example

$\varphi \equiv a$ $\qquad \pi = \{a\} * * *$

$\varphi \equiv \mathbf{G} a$ $\qquad \pi = \{a\}\{a\}\{a\}\{a\}$

$\varphi \equiv \mathbf{F} a$ $\qquad \pi = \{\}\{\}\{a\} *$

Manna, Pnueli. “*Temporal verification of reactive systems*”. 1995.

What you need to know about (r)LTL semantics

LTL

$a \in \Sigma, \quad \text{AP} = 2^{\Sigma}, \quad \text{trace } \pi \in \text{AP}^{\omega}$

	Example
$\varphi \equiv a$	$\pi = \{a\} \ * \ * \ *$
$\varphi \equiv \mathbf{G} a$	$\pi = \{a\}\{a\}\{a\}\{a\}$
$\varphi \equiv \mathbf{F} a$	$\pi = \{\}\ \{\}\ \{a\} \ *$

Output: 1/0

Manna, Pnueli. "*Temporal verification of reactive systems*". 1995.

What you need to know about (r)LTL semantics

rLTL

$a \in \Sigma, \quad \mathsf{AP} = 2^{\Sigma}, \quad \text{trace } \pi \in \mathsf{AP}^{\omega}$

Example

$$\varphi \equiv \mathbf{G}a \qquad \pi = \{a\}\{a\}\{a\}\{a\}$$

Tabuada, Neider. "*Robust linear temporal logic*". CSL 2016

What you need to know about (r)LTL semantics

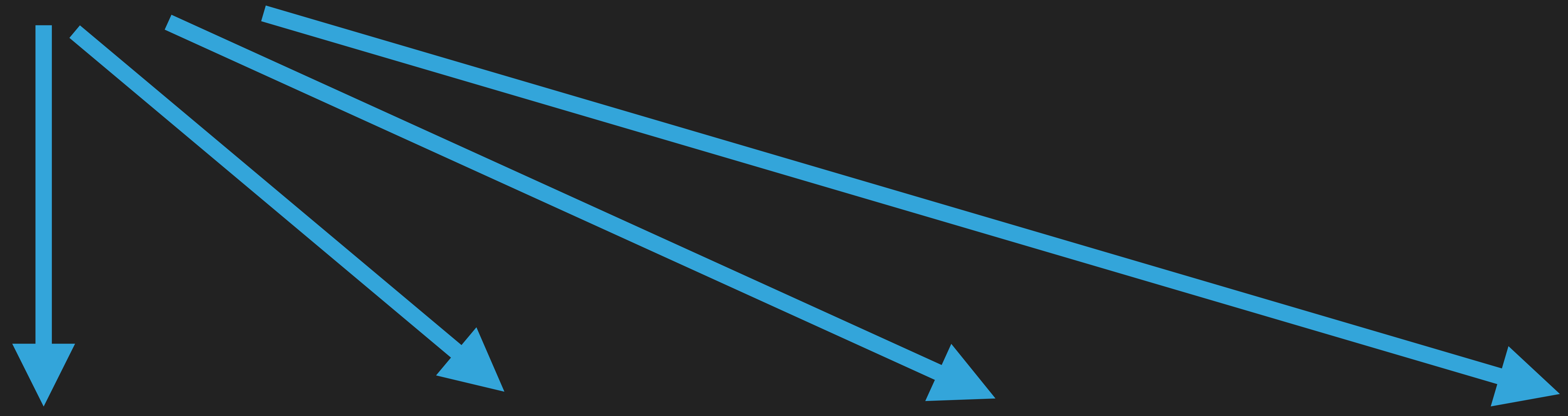
rLTL

$a \in \Sigma, \quad \mathsf{AP} = 2^{\Sigma}, \quad \text{trace } \pi \in \mathsf{AP}^{\omega}$

Example

$$\varphi \equiv \mathrm{G}a$$

$$\pi = \{a\}\{a\}\{a\}\{a\}$$



“Ga” “FGa” “GFa” “Fa”

Tabuada, Neider. "*Robust linear temporal logic*". CSL 2016

What you need to know about (r)LTL semantics

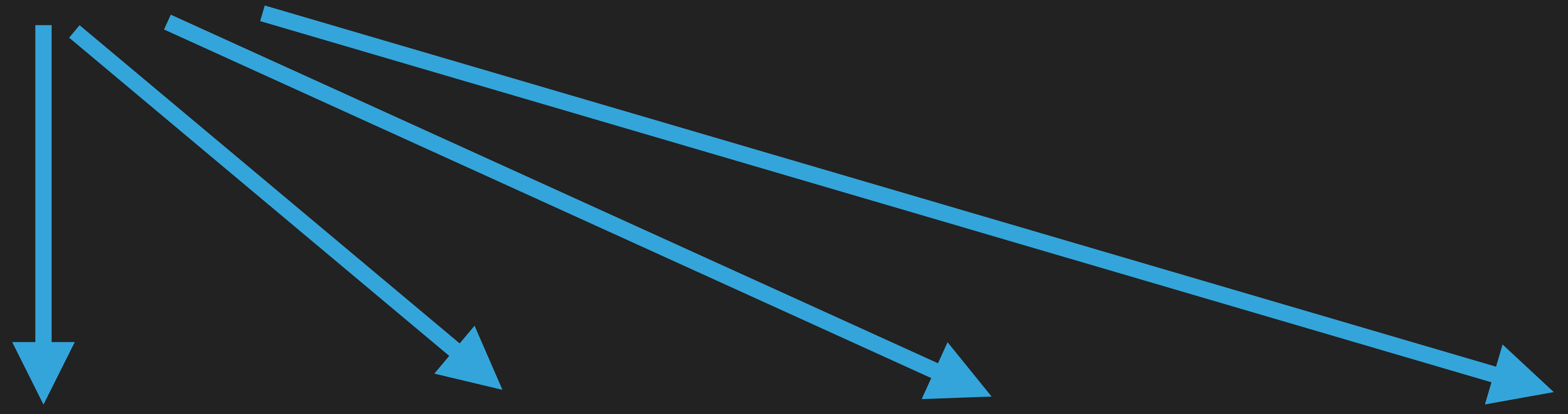
rLTL

$a \in \Sigma, \quad \mathrm{AP} = 2^{\Sigma}, \quad \text{trace } \pi \in \mathrm{AP}^{\omega}$

Example

$\varphi \equiv \mathbf{G} a$

$\pi = \{a\}\{a\}\{a\}\{a\}$



“Ga” “FGa” “GFa” “Fa”

Output: 1/0 1/0 1/0 1/0

Tabuada, Neider. "*Robust linear temporal logic*". CSL 2016

Finite Semantics: Ternary Output

`1` – Already Satisfied

`0` – Already Falsified

`?` – Don’t Know

Bauer, Leucker, Schallhart. “*Runtime verification for LTL and TLTL*”. ACM Trans. Softw. Eng. Methodol. 2011

Finite Semantics: Ternary Output

1 – Already Satisfied 0 – Already Falsified ? – Don't Know

Formula	Prefix	LTL	rLTL (**G**, **FG**, **GF**, **F**)
Ga	ε	?	????
	{a}	?	???1
	{a}{ }	0	0??1

Bauer, Leucker, Schallhart. "*Runtime verification for LTL and TLTL*". ACM Trans. Softw. Eng. Methodol. 2011

Finite Semantics: Ternary Output

1 – Already Satisfied 0 – Already Falsified ? – Don’t Know

Formula	Prefix	LTL	rLTL $(\mathbf{G}, \mathbf{FG}, \mathbf{GF}, \mathbf{F})$
Ga	ε	?	????
	{a}	?	???1
	{a}{ }	0	0??1

Questions: What truth values might occur?

Bauer, Leucker, Schallhart. “*Runtime verification for LTL and TLTL*”. ACM Trans. Softw. Eng. Methodol. 2011

Finite Semantics: Realizable Verdicts

Value	*Prefix*	*Formula*	*Value*	*Prefix*	*Formula*
0000	ε	$a \wedge \neg a$	0?11	$\emptyset\{a\}$	$\boxdot a \vee \boxdot \neg a$
000?	ε	$\diamondcdot \boxdot a \wedge \diamondcdot \neg \diamondcdot a$	0111	$\emptyset\{a\}$	$a \mathbin{\mathbf{R}} a$
0001	unrealizable		????	ε	$\boxdot a$
00??	ε	$\boxdot a \wedge \boxdot \neg a$	???1	$\{a\}$	$\boxdot a$
00?1	$\emptyset\{a\}$	$\boxdot a \wedge \boxdot \neg a$	??11	ε	$\boxdot a \vee \diamondcdot \neg \diamondcdot a$
0011	unrealizable		?111	ε	$\boxdot a \vee \neg \diamondcdot \neg \diamondcdot \neg a$
0???	$\emptyset$	$\boxdot a$	1111	ε	$a \vee \neg a$
0??1	$\emptyset\{a\}$	$\boxdot a$			

Finite Semantics: Realizable Verdicts

Value	*Prefix*	*Formula*
0000	ε	$a \land \lnot a$
000?	ε	$⟐\boxdot a \land ⟐\lnot ⟐ a$
0001	unrealizable	
00??	ε	$\boxdot a \land \boxdot \lnot a$
00?1	$\emptyset\{a\}$	$\boxdot a \land \boxdot \lnot a$
0011	unrealizable	
0???	$\emptyset$	$\boxdot a$
0??1	$\emptyset\{a\}$	$\boxdot a$
0?11	$\emptyset\{a\}$	$\boxdot a \lor \boxdot \lnot a$
0111	$\emptyset\{a\}$	$a \mathbf{R} a$
????	ε	$\boxdot a$
???1	$\{a\}$	$\boxdot a$
??11	ε	$\boxdot a \lor ⟐\lnot ⟐ a$
?111	ε	$\boxdot a \lor \lnot ⟐\lnot ⟐\lnot a$
1111	ε	$a \lor \lnot a$

Theorem: An rLTL Monitor cannot yield 0001 nor 0011.

Finite Semantics: Ternary Output

1 – Already Satisfied   0 – Already Falsified   ? – Undetermined

Formula	Prefix	LTL	rLTL $(\mathbf{G}, \mathbf{FG}, \mathbf{GF}, \mathbf{F})$
Ga	ε	?	????
	{a}	?	???1
	{a}{ }	0	0??1

Finite Semantics: Ternary Output

1 – Already Satisfied   0 – Already Falsified   ? – Undetermined

Formula	Prefix	LTL	rLTL (**G**, **FG**, **GF**, **F**)
Ga	ε	?	????
	{a}	?	???1
	{a}{ }	0	0??1

Questions: How do values "evolve"?

Finite Semantics: Ternary Output

1 – Already Satisfied   0 – Already Falsified   ? – Undetermined

Formula	Prefix	LTL	rLTL $(\mathbf{G}, \mathbf{FG}, \mathbf{GF}, \mathbf{F})$
Ga	ε	?	????
	{a}	?	???1
	{a}{ }	0	0??1

Questions: How do values “evolve”?

Theorem: Up to four refinements are possible.

Monitorability

rLTL-Ugly Prefix: Every continuation yields ?**???**

rLTL-Monitorable: There are no **r**LTL-Ugly Prefixes

	LTL Monitorable	**Not LTL Monitorable**
rLTL Monitorable	$\mathbf{Ga}$	$\mathbf{GFa}$
Not rLTL Monitorable	$(Ga \wedge G\neg a) \Longrightarrow (FGa \wedge FG\neg a)$	$(p \wedge \varphi_{LTL}) \vee (\neg p \wedge \varphi_{rLTL})$

Monitorability

rLTL-Ugly Prefix: Every continuation yields ????

rLTL-Monitorable: There are no rLTL-Ugly Prefixes

	LTL Monitorable	Not LTL Monitorable
rLTL Monitorable	rLTL: “Adding { } will always yield 0***” **Ga** LTL: “Adding { } will always yield 0”	**GFa**
Not rLTL Monitorable	$(\mathbf{G}a \wedge \mathbf{G}\neg a) \Longrightarrow (\mathbf{FG}a \wedge \mathbf{FG}\neg a)$	$(p \wedge \varphi_{LTL}) \vee (\neg p \wedge \varphi_{rLTL})$

Monitorability

rLTL-Ugly Prefix: Every continuation yields ?**???**

rLTL-Monitorable: There are no **r**LTL-Ugly Prefixes

	LTL Monitorable	**Not LTL Monitorable**
rLTL Monitorable	rLTL: “Adding { } will always yield 0***” **Ga** LTL: “Adding { } will always yield 0”	rLTL: “Adding {a} will yield 1 in last bit” **GFa** LTL: “Depends on infinite behavior.”
Not rLTL Monitorable	$(\mathbf{G}a \wedge \mathbf{G}\neg a) \Longrightarrow (\mathbf{FG}a \wedge \mathbf{FG}\neg a)$	$(p \wedge \varphi_{LTL}) \vee (\neg p \wedge \varphi_{rLTL})$

LTL-Mon does not imply rLTL-Mon

rLTL-Ugly Prefix: Every continuation yields ?**???**

rLTL-Monitorable: There are no **r**LTL-Ugly Prefixes

$$\boxed{(\mathbf{Ga} \wedge \mathbf{G}\neg\mathbf{a}) \implies (\mathbf{FGa} \wedge \mathbf{F}\underline{\mathbf{G}}\neg\mathbf{a})}$$

LTL-mon

$(Ga \wedge G\neg a)$: Contradiction

$(Ga \wedge G\neg a) \implies (FGa \wedge F\underline{G}\neg a)$: Tautology

Not rLTL-mon

Ugly Prefix { }{a}

$\forall\rho$: { }{a}ρ{ }$^\omega$ yields 1111

{ }{a}ρ{a}$^\omega$ yields 0000

Monitorability

rLTL-Ugly Prefix: Every continuation yields ????

rLTL-Monitorable: There are no **r**LTL-Ugly Prefixes

	LTL Monitorable	**Not LTL Monitorable**
rLTL Monitorable	rLTL: “Adding { } will always yield 0***” $\mathbf{Ga}$ LTL: “Adding { } will always yield 0”	rLTL: “Adding {a} will yield 1 in last bit” $\mathbf{GFa}$ LTL: “Depends on infinite behavior.”
Not rLTL Monitorable	$(\mathbf{G}a \wedge \mathbf{G}\neg a) \implies (\mathbf{FG}a \wedge \mathbf{FG}\neg a)$	$(p \wedge \varphi_{LTL}) \vee (\neg p \wedge \varphi_{rLTL})$

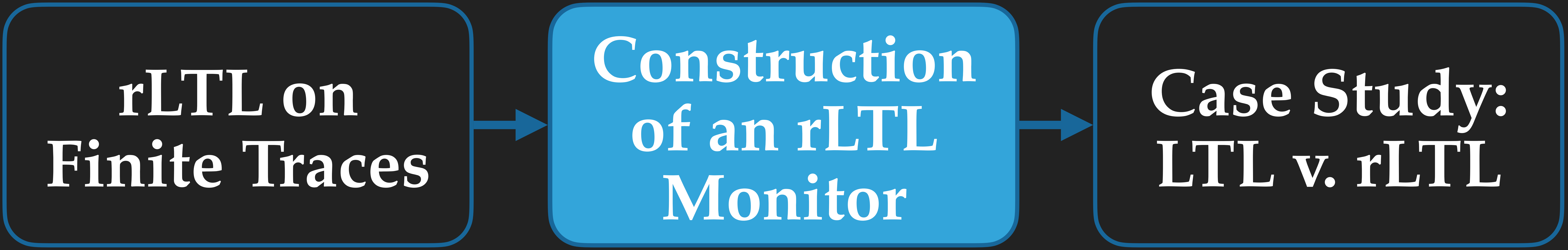
Lift Monitoring from LTL to rLTL

rLTL on Finite Traces

Construction of an rLTL Monitor

Case Study: LTL v. rLTL

Lift Monitoring from LTL to rLTL



rLTL on Finite Traces

Construction of an rLTL Monitor

Case Study: LTL v. rLTL

Constructing an rLTL Monitor

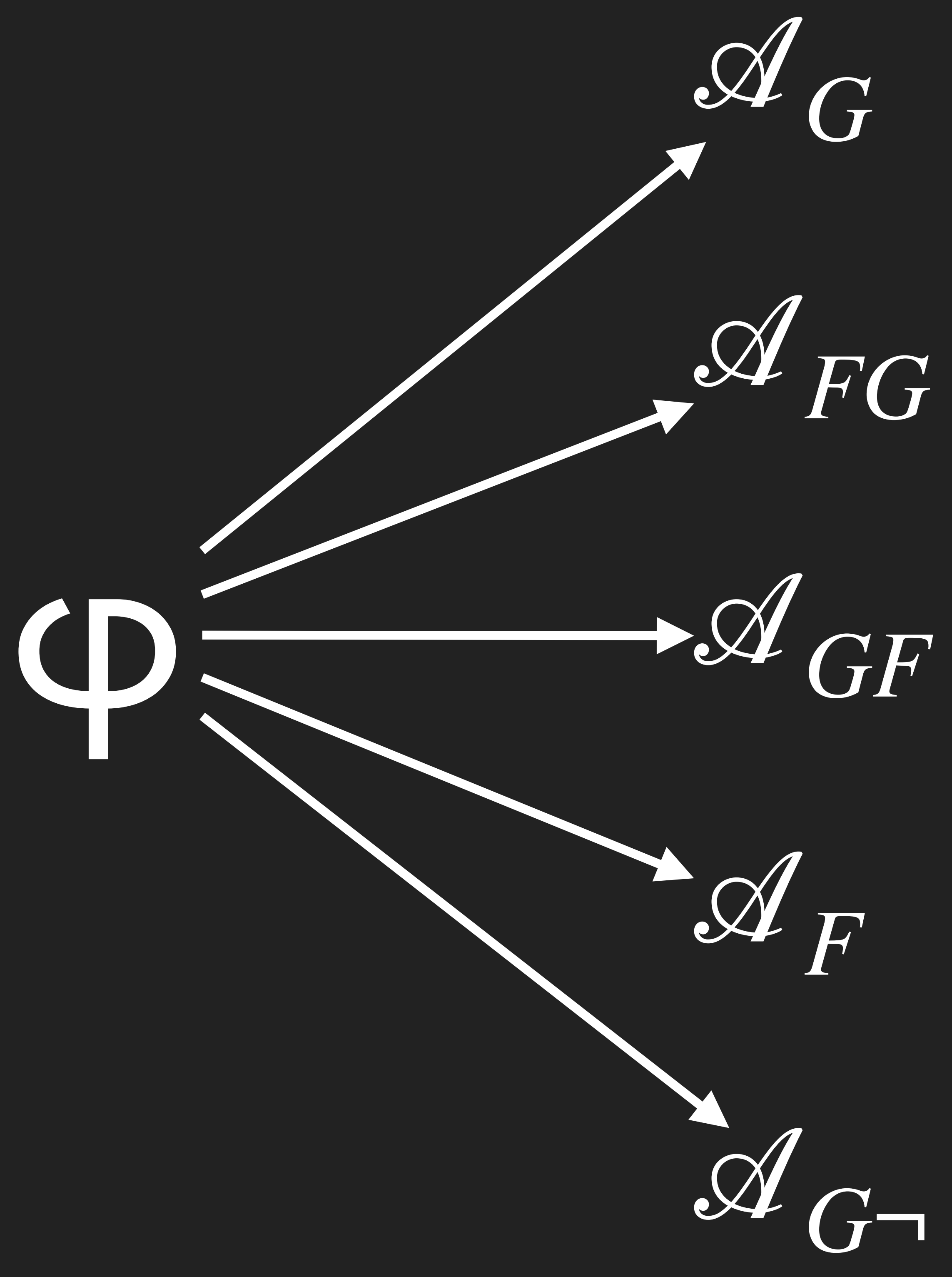
rLTL

φ

Constructing an rLTL Monitor

rLTL

Büchi



Constructing an rLTL Monitor

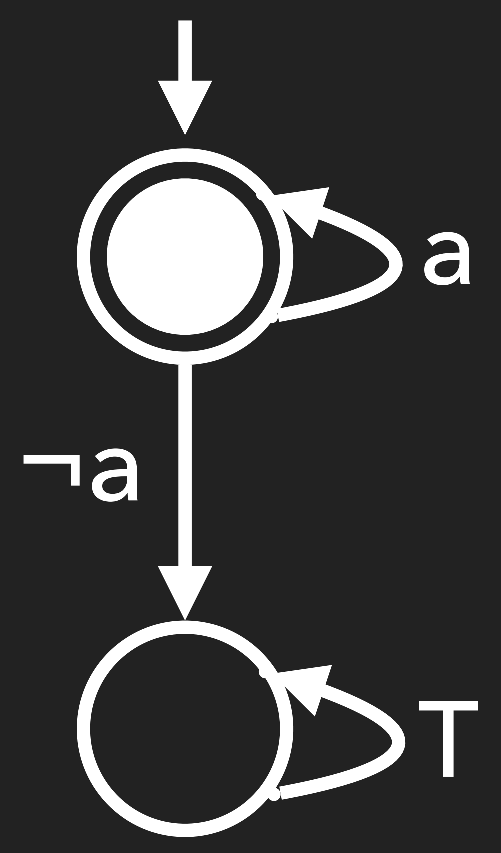
rLTL Büchi

$$\begin{tikzcd}
 & \mathscr{A}_{G} \\
 & \mathscr{A}_{FG} \\
\varphi \arrow[ruu] \arrow[ru] \arrow[r] \arrow[rd] \arrow[rdd] & \mathscr{A}_{GF} \\
 & \mathscr{A}_{F} \\
 & \mathscr{A}_{G\neg}
\end{tikzcd}$$

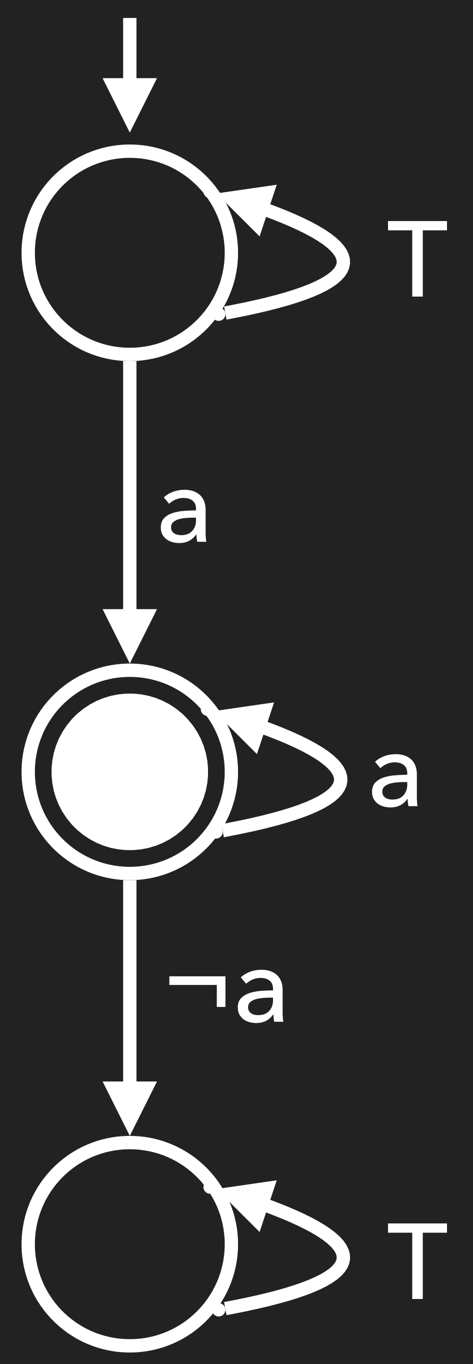
$2^{O(|\varphi|)}$

Constructing an rLTL Monitor

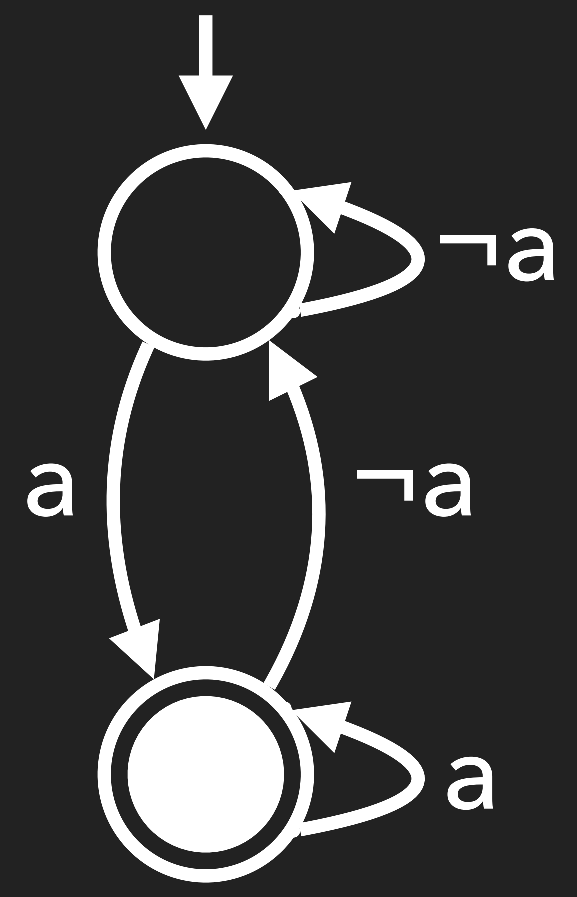
Ga



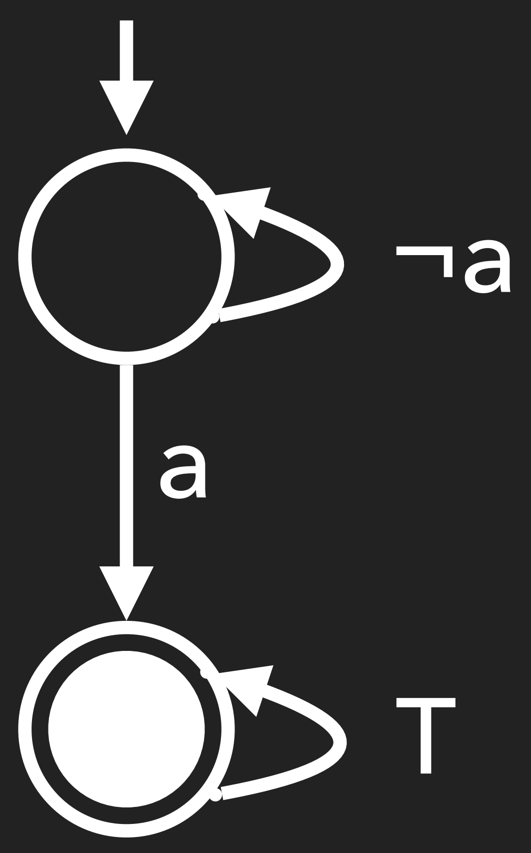
FGa



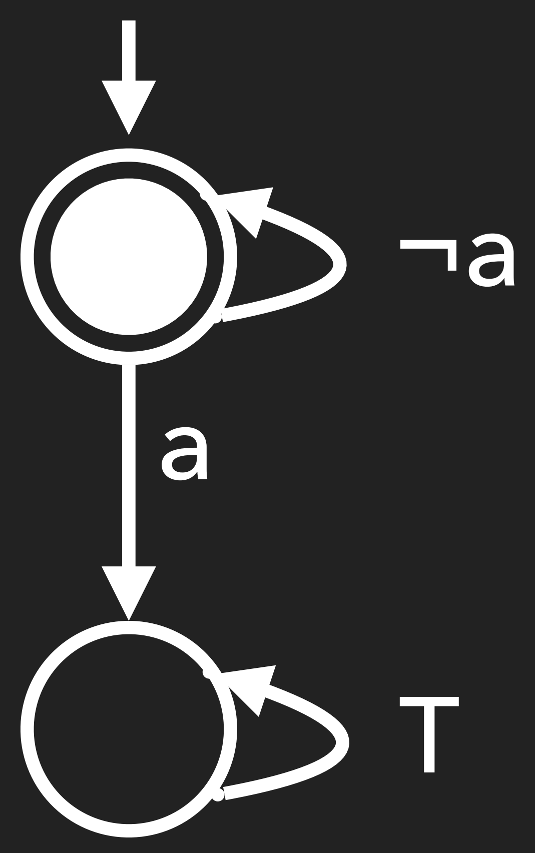
GFa



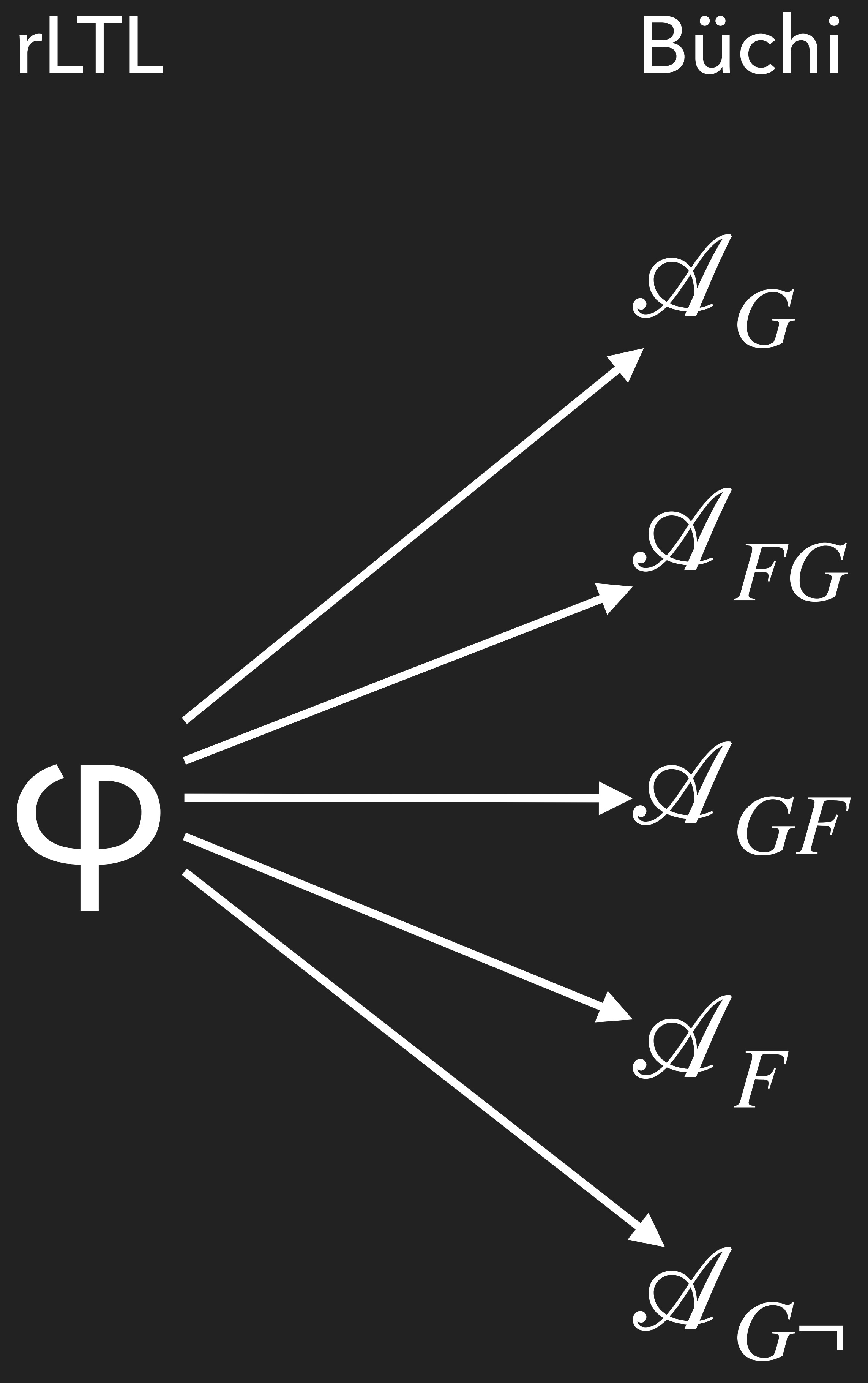
Fa



G¬a



Constructing an rLTL Monitor



rLTL

Büchi

φ

$\mathscr{A}_G$

$\mathscr{A}_{FG}$

$\mathscr{A}_{GF}$

$\mathscr{A}_F$

$\mathscr{A}_{G\neg}$

$2^{O(|\varphi|)}$

Constructing an rLTL Monitor

rLTL Büchi NFA

$$\begin{tikzcd}
 & \mathscr{A}_{G} \arrow[r] & \mathscr{B}_{G} \\
 & \mathscr{A}_{FG} \arrow[r] & \mathscr{B}_{FG} \\
\varphi \arrow[uur] \arrow[ur] \arrow[r] \arrow[dr] \arrow[ddr] & \mathscr{A}_{GF} \arrow[r] & \mathscr{B}_{GF} \\
 & \mathscr{A}_{F} \arrow[r] & \mathscr{B}_{F} \\
 & \mathscr{A}_{G\neg} \arrow[r] & \mathscr{B}_{G\neg}
\end{tikzcd}$$

$2^{O(|\varphi|)}$

Constructing an rLTL Monitor

rLTL Büchi NFA

$$\begin{tikzcd}
 & \mathscr{A}_{G} \arrow[r] & \mathscr{B}_{G} \\
 & \mathscr{A}_{FG} \arrow[r] & \mathscr{B}_{FG} \\
\varphi \arrow[uur] \arrow[ur] \arrow[r] \arrow[dr] \arrow[ddr] & \mathscr{A}_{GF} \arrow[r] & \mathscr{B}_{GF} \\
 & \mathscr{A}_{F} \arrow[r] & \mathscr{B}_{F} \\
 & \mathscr{A}_{G\neg} \arrow[r] & \mathscr{B}_{G\neg}
\end{tikzcd}$$

$2^{O(|\varphi|)}$ $O(|\mathscr{A}|^3)$

Constructing an rLTL Monitor

rLTL Büchi NFA Det. Moore

$$\begin{tikzcd}
 & \mathscr{A}_{G} \arrow[r] & \mathscr{B}_{G} \arrow[r] & \mathscr{C}_{G} \\
 & \mathscr{A}_{FG} \arrow[r] & \mathscr{B}_{FG} \arrow[r] & \mathscr{C}_{FG} \\
\varphi \arrow[uur] \arrow[ur] \arrow[r] \arrow[dr] \arrow[ddr] & \mathscr{A}_{GF} \arrow[r] & \mathscr{B}_{GF} \arrow[r] & \mathscr{C}_{GF} \\
 & \mathscr{A}_{F} \arrow[r] & \mathscr{B}_{F} \arrow[r] & \mathscr{C}_{F} \\
 & \mathscr{A}_{G\neg} \arrow[r] & \mathscr{B}_{G\neg} \arrow[r] & \mathscr{C}_{G\neg}
\end{tikzcd}$$

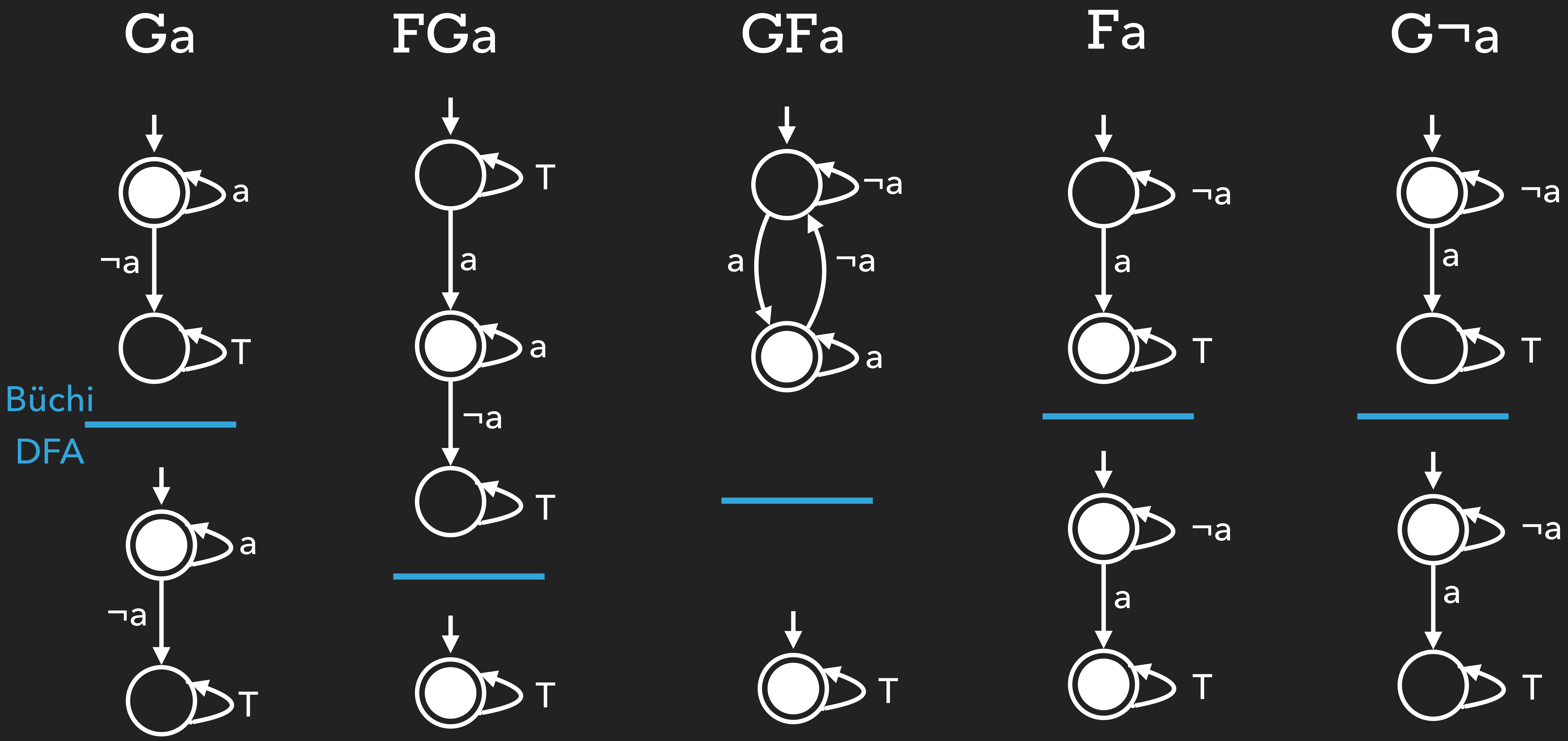
$2^{O(|\varphi|)}$ $O(|\mathscr{A}|^3)$

Constructing an rLTL Monitor

$$\begin{tikzcd}
\text{rLTL} & \text{Büchi} & \text{NFA} & \text{Det. Moore} \\
 & \mathscr{A}_G \arrow[r] & \mathscr{B}_G \arrow[r] & \mathscr{C}_G \\
 & \mathscr{A}_{FG} \arrow[r] & \mathscr{B}_{FG} \arrow[r] & \mathscr{C}_{FG} \\
\varphi \arrow[uur] \arrow[ur] \arrow[r] \arrow[dr] \arrow[ddr] & \mathscr{A}_{GF} \arrow[r] & \mathscr{B}_{GF} \arrow[r] & \mathscr{C}_{GF} \\
 & \mathscr{A}_F \arrow[r] & \mathscr{B}_F \arrow[r] & \mathscr{C}_F \\
 & \mathscr{A}_{G\neg} \arrow[r] & \mathscr{B}_{G\neg} \arrow[r] & \mathscr{C}_{G\neg}
\end{tikzcd}$$

$2^{O(|\varphi|)}$ $O(|\mathscr{A}|^3)$ $2^{O(|\mathscr{B}|)}$

Constructing an rLTL Monitor



Constructing an rLTL Monitor

rLTL Büchi NFA Det. Moore

$$\begin{tikzcd}
 & \mathscr{A}_{G} \arrow[r] & \mathscr{B}_{G} \arrow[r] & \mathscr{C}_{G} \\
 & \mathscr{A}_{FG} \arrow[r] & \mathscr{B}_{FG} \arrow[r] & \mathscr{C}_{FG} \\
\varphi \arrow[uur] \arrow[ur] \arrow[r] \arrow[dr] \arrow[ddr] & \mathscr{A}_{GF} \arrow[r] & \mathscr{B}_{GF} \arrow[r] & \mathscr{C}_{GF} \\
 & \mathscr{A}_{F} \arrow[r] & \mathscr{B}_{F} \arrow[r] & \mathscr{C}_{F} \\
 & \mathscr{A}_{G\neg} \arrow[r] & \mathscr{B}_{G\neg} \arrow[r] & \mathscr{C}_{G\neg}
\end{tikzcd}$$

$2^{O(|\varphi|)}$ $O(|\mathscr{A}|^3)$ $2^{O(|\mathscr{B}|)}$

Constructing an rLTL Monitor

$$\begin{tikzcd}
\text{rLTL} & \text{Büchi} & \text{NFA} & \text{Det. Moore} & \text{Det. Moore} \\
 & \mathscr{A}_{G} \arrow[r] & \mathscr{B}_{G} \arrow[r] & \mathscr{C}_{G} \arrow[ddr] & \\
 & \mathscr{A}_{FG} \arrow[r] & \mathscr{B}_{FG} \arrow[r] & \mathscr{C}_{FG} \arrow[dr] & \\
\varphi \arrow[uur] \arrow[ur] \arrow[r] \arrow[dr] \arrow[ddr] & \mathscr{A}_{GF} \arrow[r] & \mathscr{B}_{GF} \arrow[r] & \mathscr{C}_{GF} \arrow[r] & \mathscr{M}_{\varphi} \\
 & \mathscr{A}_{F} \arrow[r] & \mathscr{B}_{F} \arrow[r] & \mathscr{C}_{F} \arrow[ur] & \\
 & \mathscr{A}_{G\neg} \arrow[r] & \mathscr{B}_{G\neg} \arrow[r] & \mathscr{C}_{G\neg} \arrow[uur] &
\end{tikzcd}$$

$2^{O(|\varphi|)}$ $O(|\mathscr{A}|^{3})$ $2^{O(|\mathscr{B}|)}$

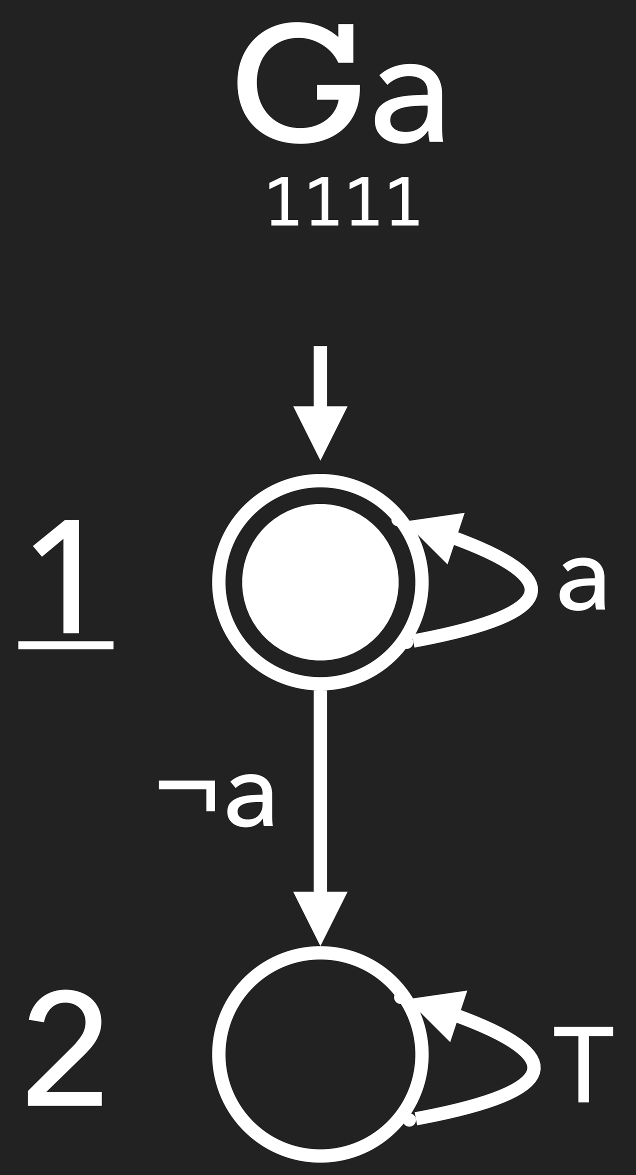
Constructing an rLTL Monitor

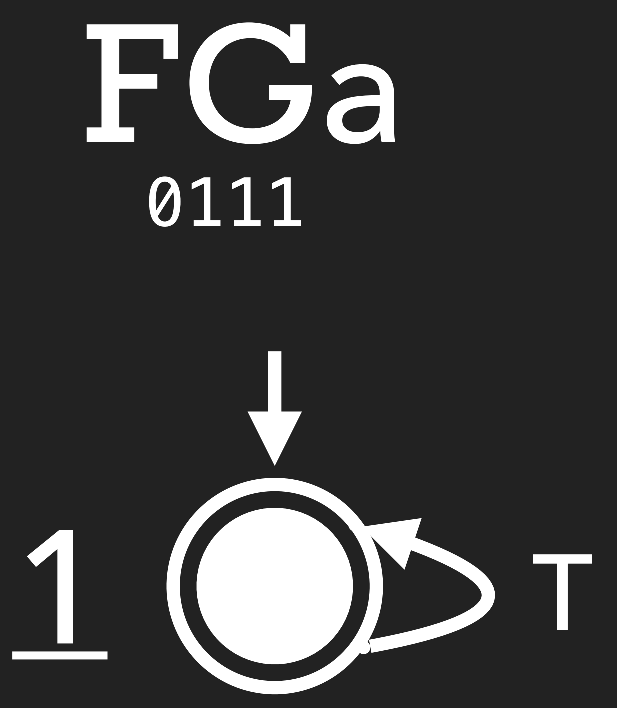
rLTL Büchi NFA Det. Moore Det. Moore

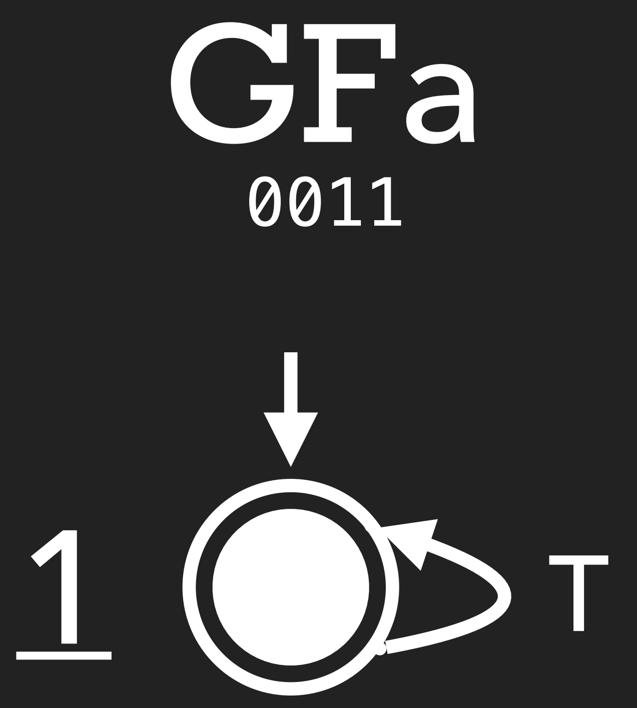
$$\begin{tikzcd}
 & \mathscr{A}_{G} \arrow[r] & \mathscr{B}_{G} \arrow[r] & \mathscr{C}_{G} \arrow[ddr] & \\
 & \mathscr{A}_{FG} \arrow[r] & \mathscr{B}_{FG} \arrow[r] & \mathscr{C}_{FG} \arrow[dr] & \\
\varphi \arrow[uur] \arrow[ur] \arrow[r] \arrow[dr] \arrow[ddr] & \mathscr{A}_{GF} \arrow[r] & \mathscr{B}_{GF} \arrow[r] & \mathscr{C}_{GF} \arrow[r] & \mathscr{M}_{\varphi} \\
 & \mathscr{A}_{F} \arrow[r] & \mathscr{B}_{F} \arrow[r] & \mathscr{C}_{F} \arrow[ur] & \\
 & \mathscr{A}_{G\neg} \arrow[r] & \mathscr{B}_{G\neg} \arrow[r] & \mathscr{C}_{G\neg} \arrow[uur] &
\end{tikzcd}$$

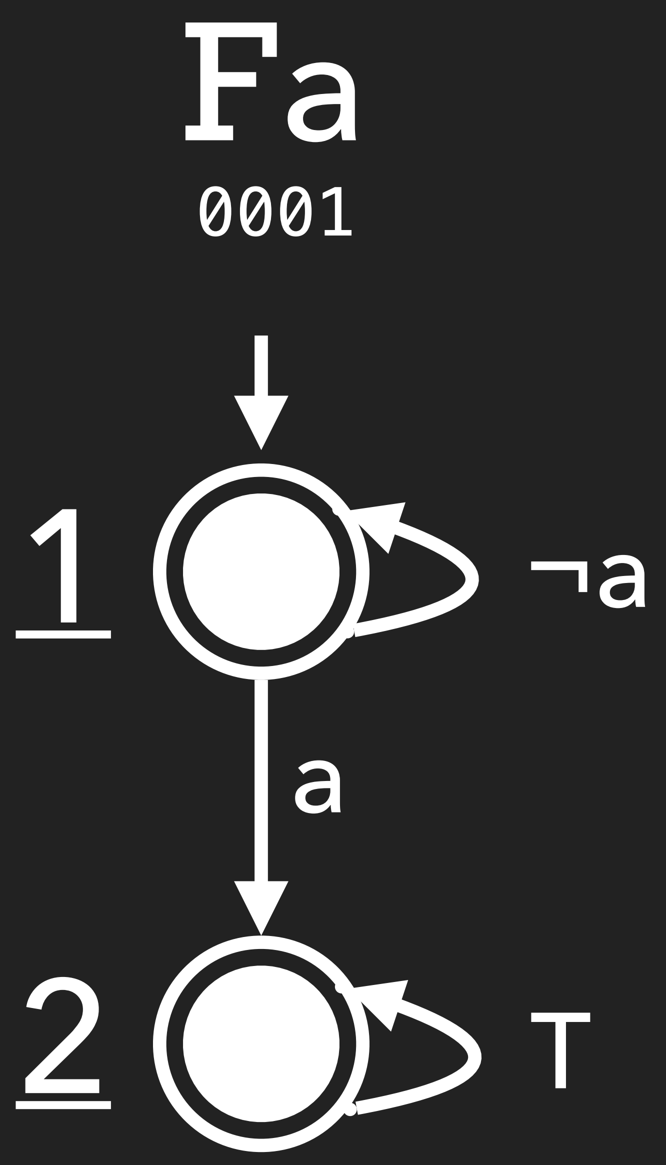
$2^{O(|\varphi|)}$ $O(|\mathscr{A}|^3)$ $2^{O(|\mathscr{B}|)}$ $O(|\mathscr{C}|)$

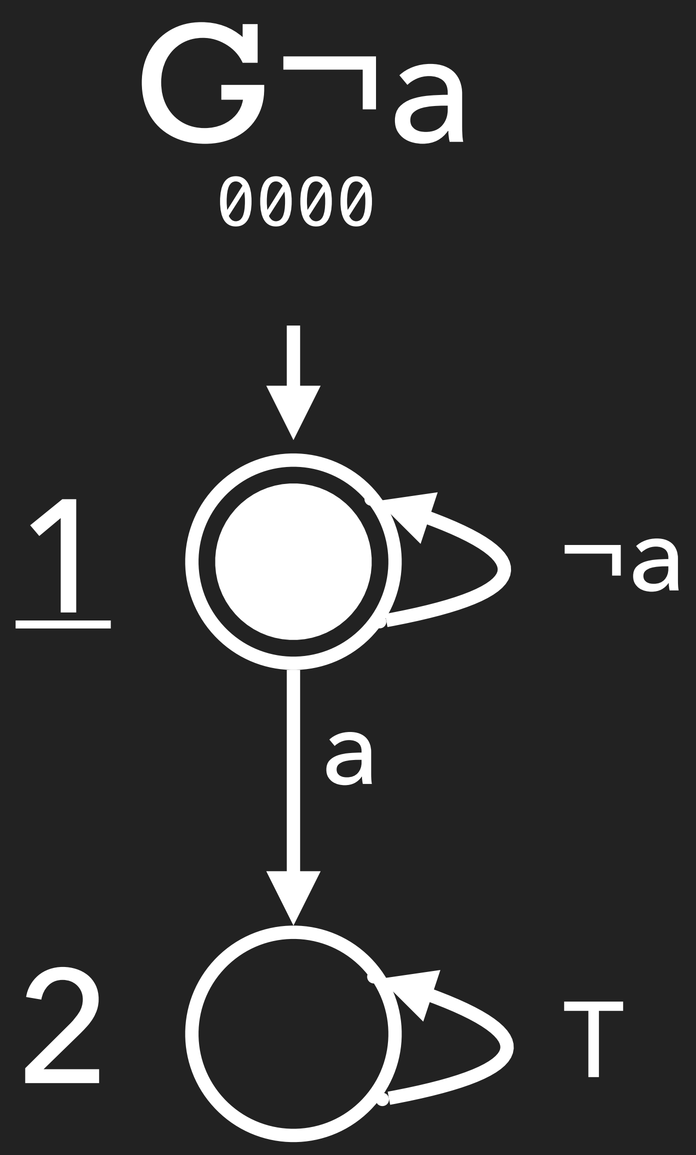
Constructing an rLTL Monitor

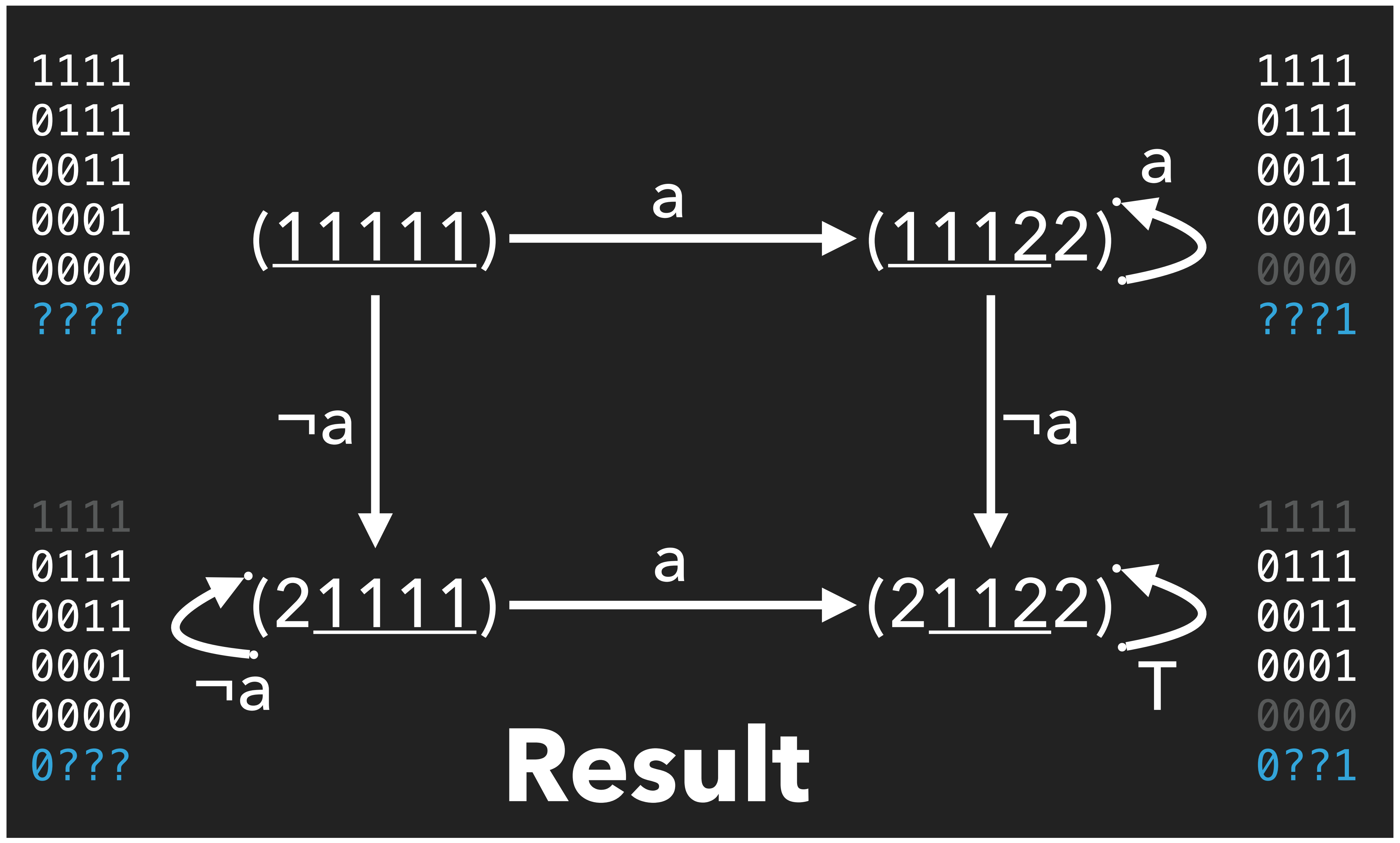












Result

Constructing an rLTL Monitor

rLTL Büchi NFA Det. Moore Det. Moore

$$\begin{tikzcd}
 & \mathscr{A}_{G} \arrow[r] & \mathscr{B}_{G} \arrow[r] & \mathscr{C}_{G} \arrow[ddr] & \\
 & \mathscr{A}_{FG} \arrow[r] & \mathscr{B}_{FG} \arrow[r] & \mathscr{C}_{FG} \arrow[dr] & \\
\varphi \arrow[uur] \arrow[ur] \arrow[r] \arrow[dr] \arrow[ddr] & \mathscr{A}_{GF} \arrow[r] & \mathscr{B}_{GF} \arrow[r] & \mathscr{C}_{GF} \arrow[r] & \mathscr{M}_{\varphi} \\
 & \mathscr{A}_{F} \arrow[r] & \mathscr{B}_{F} \arrow[r] & \mathscr{C}_{F} \arrow[ur] & \\
 & \mathscr{A}_{G\neg} \arrow[r] & \mathscr{B}_{G\neg} \arrow[r] & \mathscr{C}_{G\neg} \arrow[uur] &
\end{tikzcd}$$

$2^{O(|\varphi|)}$ $O(|\mathscr{A}|^3)$ $2^{O(|\mathscr{B}|)}$ $O(|\mathscr{C}|)$

Constructing an rLTL Monitor

rLTL Büchi NFA Det. Moore Det. Moore Det. Moore

$$\begin{tikzcd}
 & \mathscr{A}_{G} \arrow[r] & \mathscr{B}_{G} \arrow[r] & \mathscr{C}_{G} \arrow[ddr] & & \\
 & \mathscr{A}_{FG} \arrow[r] & \mathscr{B}_{FG} \arrow[r] & \mathscr{C}_{FG} \arrow[dr] & & \\
\varphi \arrow[uur] \arrow[ur] \arrow[r] \arrow[dr] \arrow[ddr] & \mathscr{A}_{GF} \arrow[r] & \mathscr{B}_{GF} \arrow[r] & \mathscr{C}_{GF} \arrow[r] & \mathscr{M}_{\varphi} \arrow[r] & \mathscr{M}'_{\varphi} \\
 & \mathscr{A}_{F} \arrow[r] & \mathscr{B}_{F} \arrow[r] & \mathscr{C}_{F} \arrow[ur] & & \\
 & \mathscr{A}_{G\neg} \arrow[r] & \mathscr{B}_{G\neg} \arrow[r] & \mathscr{C}_{G\neg} \arrow[uur] & &
\end{tikzcd}$$

$2^{O(|\varphi|)}$ $O(|\mathscr{A}|^3)$ $2^{O(|\mathscr{B}|)}$ $O(|\mathscr{C}|)$

Constructing an rLTL Monitor

$$\begin{tikzcd}
\text{rLTL} & \text{Büchi} & \text{NFA} & \text{Det. Moore} & \text{Det. Moore} & \text{Det. Moore} \\
 & \mathscr{A}_{G} \arrow[r] & \mathscr{B}_{G} \arrow[r] & \mathscr{C}_{G} \arrow[ddr] & & \\
 & \mathscr{A}_{FG} \arrow[r] & \mathscr{B}_{FG} \arrow[r] & \mathscr{C}_{FG} \arrow[dr] & & \\
\varphi \arrow[uur] \arrow[ur] \arrow[r] \arrow[dr] \arrow[ddr] & \mathscr{A}_{GF} \arrow[r] & \mathscr{B}_{GF} \arrow[r] & \mathscr{C}_{GF} \arrow[r] & \mathscr{M}_{\varphi} \arrow[r] & \mathscr{M}'_{\varphi} \\
 & \mathscr{A}_{F} \arrow[r] & \mathscr{B}_{F} \arrow[r] & \mathscr{C}_{F} \arrow[ur] & & \\
 & \mathscr{A}_{G\neg} \arrow[r] & \mathscr{B}_{G\neg} \arrow[r] & \mathscr{C}_{G\neg} \arrow[uur] & &
\end{tikzcd}$$

$2^{O(|\varphi|)}$ $\quad O(|\mathscr{A}|^3)$ $\quad 2^{O(|\mathscr{B}|)}$ $\quad O(|\mathscr{C}|)$ $\quad O(|\mathscr{M}|\log(|\mathscr{M}|))$

Constructing an rLTL Monitor

$$\begin{tikzcd}
\text{rLTL} & \text{Büchi} & \text{NFA} & \text{Det. Moore} & \text{Det. Moore} & \text{Det. Moore} \\
 & \mathscr{A}_{G} \arrow[r] & \mathscr{B}_{G} \arrow[r] & \mathscr{C}_{G} \arrow[rdd] & & \\
 & \mathscr{A}_{FG} \arrow[r] & \mathscr{B}_{FG} \arrow[r] & \mathscr{C}_{FG} \arrow[rd] & & \\
\varphi \arrow[ruu] \arrow[ru] \arrow[r] \arrow[rd] \arrow[rdd] & \mathscr{A}_{GF} \arrow[r] & \mathscr{B}_{GF} \arrow[r] & \mathscr{C}_{GF} \arrow[r] & \mathscr{M}_{\varphi} \arrow[r] & \mathscr{M}'_{\varphi} \\
 & \mathscr{A}_{F} \arrow[r] & \mathscr{B}_{F} \arrow[r] & \mathscr{C}_{F} \arrow[ru] & & \\
 & \mathscr{A}_{G\neg} \arrow[r] & \mathscr{B}_{G\neg} \arrow[r] & \mathscr{C}_{G\neg} \arrow[ruu] & &
\end{tikzcd}$$

Total: $2^{2^{O(|\varphi|)}}$

$2^{O(|\varphi|)}$ $O(|\mathscr{A}|^3)$ $2^{O(|\mathscr{B}|)}$ $O(|\mathscr{C}|)$ $O(|\mathscr{M}|\log(|\mathscr{M}|))$

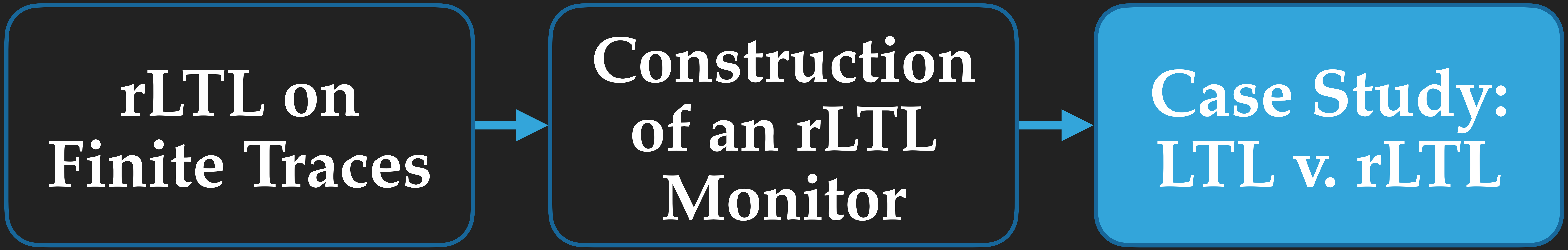
Lift Monitoring from LTL to rLTL

rLTL on Finite Traces

Construction of an rLTL Monitor

Case Study: LTL v. rLTL

Lift Monitoring from LTL to rLTL



rLTL on Finite Traces

Construction of an rLTL Monitor

Case Study: LTL v. rLTL

Benchmark

Dwyer et al [1]:

97 LTL formulas

frequent specification patterns

[1] Dwyer, Avrunin, Corbett. "*Patterns in property specifications for finite-state verification*". ICSE 1999

Benchmark

Dwyer et al [1]:

97 LTL formulas

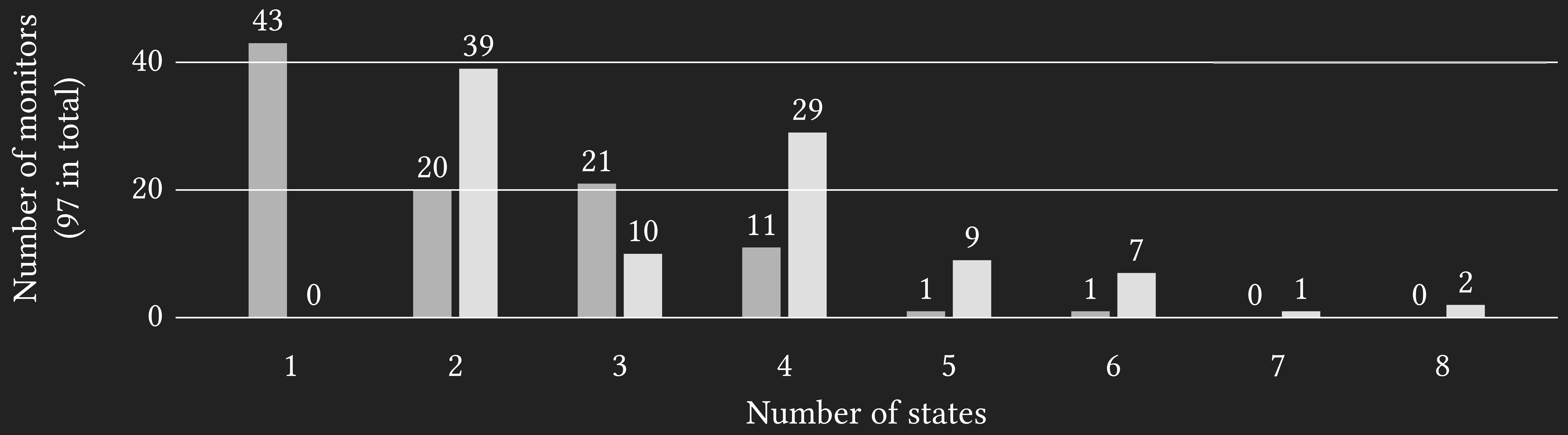
frequent specification patterns

55.7% LTL-monitorable [2] versus **100% rLTL**-monitorable

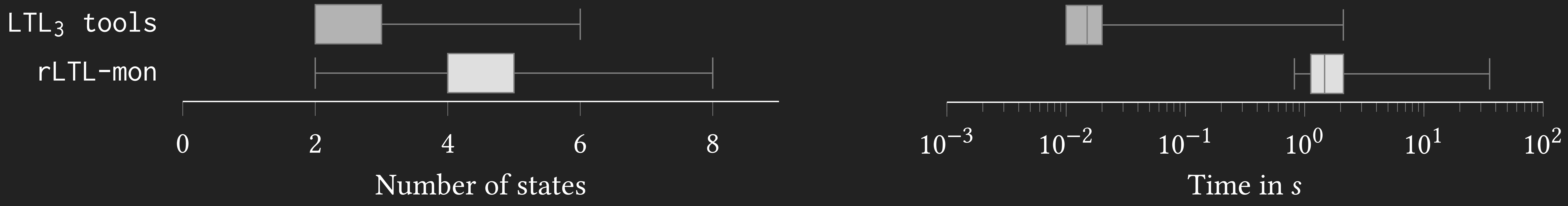
[1] Dwyer, Avrunin, Corbett. "*Patterns in property specifications for finite-state verification*". ICSE 1999

[2] Bauer, Leucker, Schallhart. "*Runtime verification for LTL and TLTL*". ACM Trans. Softw. Eng. Methodol. 2011

Results



Histogram of the number of monitors with respect to their size



Analysis of the monitor construction for the 54 formulas that are both LTL-monitorable and rLTL-monitorable

Summary

rLTL | Büchi | NFA | Det. Moore | Det. Moore | Det. Moore

$$\begin{tikzcd}
 & \mathscr{A}_G \arrow[r] & \mathscr{B}_G \arrow[r] & \mathscr{C}_G \arrow[ddr] & & \\
 & \mathscr{A}_{FG} \arrow[r] & \mathscr{B}_{FG} \arrow[r] & \mathscr{C}_{FG} \arrow[dr] & & \\
\varphi \arrow[uur] \arrow[ur] \arrow[r] \arrow[dr] \arrow[ddr] & \mathscr{A}_{GF} \arrow[r] & \mathscr{B}_{GF} \arrow[r] & \mathscr{C}_{GF} \arrow[r] & \mathscr{M}_\varphi \arrow[r] & \mathscr{M}'_\varphi \\
 & \mathscr{A}_F \arrow[r] & \mathscr{B}_F \arrow[r] & \mathscr{C}_F \arrow[ur] & & \\
 & \mathscr{A}_{G\neg} \arrow[r] & \mathscr{B}_{G\neg} \arrow[r] & \mathscr{C}_{G\neg} \arrow[uur] & &
\end{tikzcd}$$

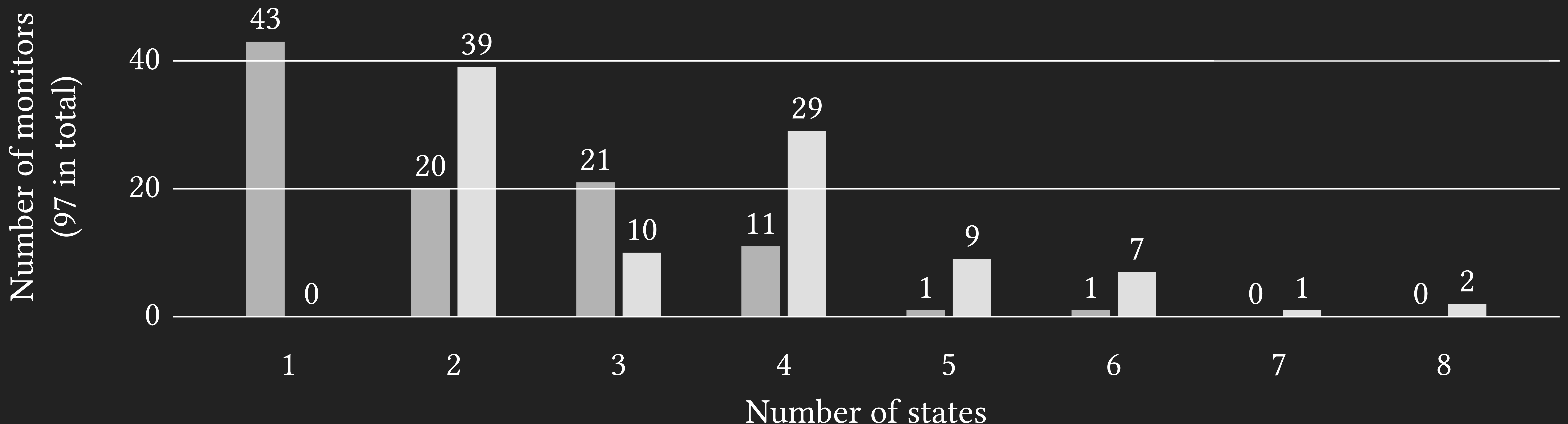
Total: $2^{2^{O(|\varphi|)}}$

$2^{O(|\varphi|)}$ $O(|\mathscr{A}|^3)$ $2^{O(|\mathscr{B}|)}$ $O(|\mathscr{C}|)$ $O(|\mathscr{M}|\log(|\mathscr{M}|))$

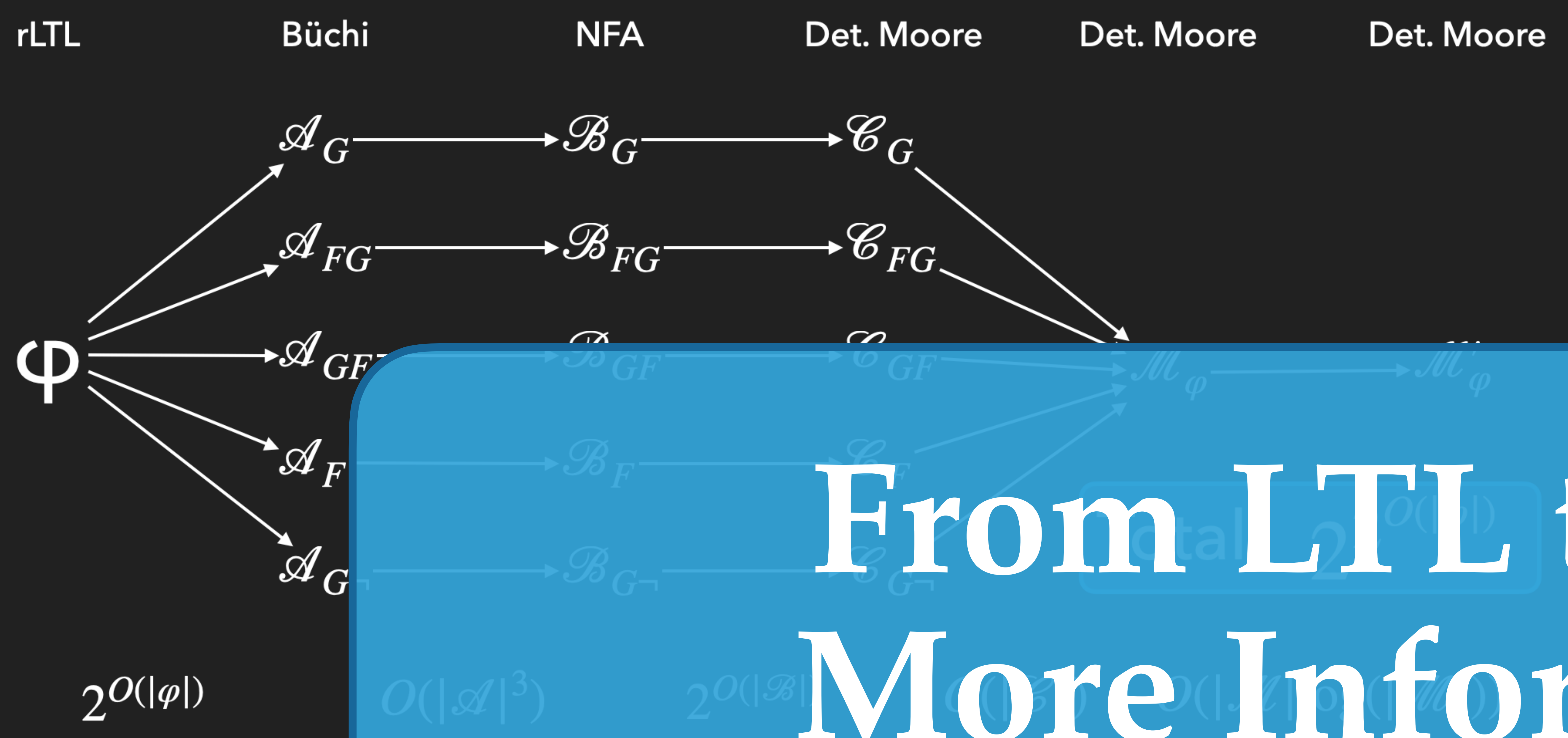
55.7% LTL-monitorable

versus

100% rLTL-monitorable



Summary

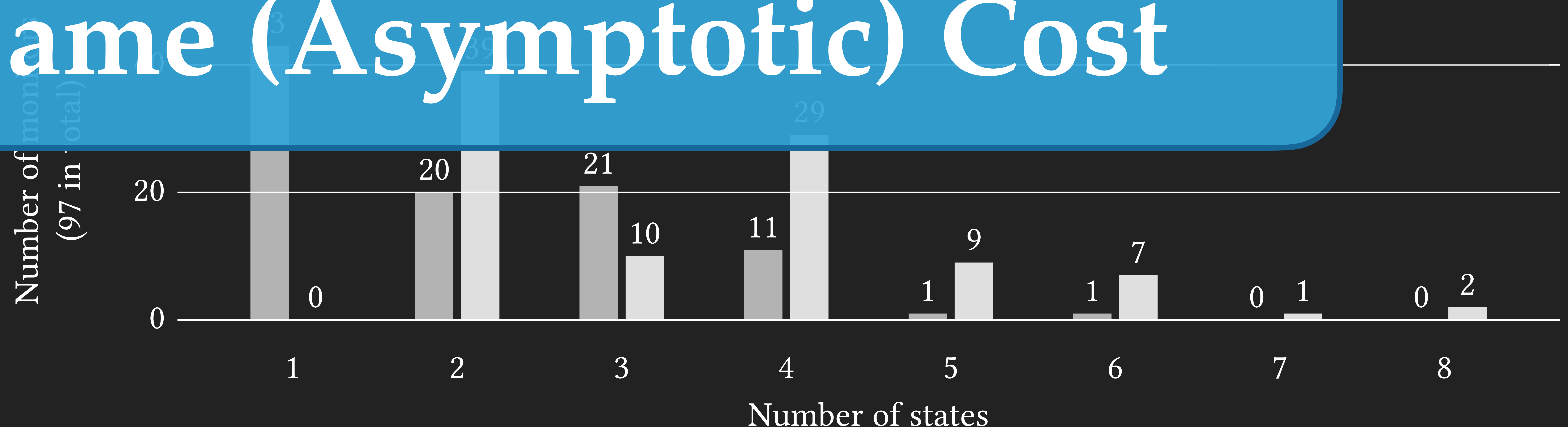


55.7% LTL-monitorable

versus

100% rLTL-monitorable

From LTL to rLTL: More Information; Same (Asymptotic) Cost


Number of monitors
(97 in total)
Number of states