Computer aided verification

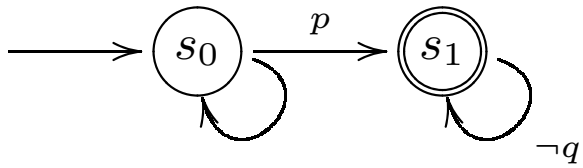
Lecture 3:

LTL model-checking by translation to ω-automata

Sławomir Lasota
University of Warsaw

Example:

$\phi = \neg G(p \implies \mathsf{X}\, Fq) \quad \mapsto \quad A_\phi =$



LTL $\subseteq$ ω-automata

Plan

- ω-automata
- LTL $\mapsto$ ω-automata
- exponential blow-up
- LTL $\mapsto$ alternating ω-automata

ω-automata

ω-automata (BA)

Def.: ω-automaton (**Büchi** automaton) $\mathcal{A} = \langle \Sigma, S, S_{\text{init}}, \sigma, F \rangle$

- Σ finite input alphabet
- S finite set of states
- $S_{\text{init}} \subseteq S$ nonempty subset of initial states
- $\sigma \subseteq S \times \Sigma \times S$ transition relation
- $F \subseteq S$ nonempty subset of accepting states

ω-automata (BA)

Def.: ω-automaton (**Büchi** automaton) $\mathcal{A} = \langle \Sigma, S, S_{\text{init}}, \sigma, F \rangle$

- Σ finite input alphabet
- S finite set of states
- $S_{\text{init}} \subseteq S$ nonempty subset of initial states
- $\sigma \subseteq S \times \Sigma \times S$ transition relation
- $F \subseteq S$ nonempty subset of accepting states

$\mathcal{A}$ is deterministic when $|S_{\text{init}}| = 1$ and $\forall s, a.\ |\sigma(s, a)| \leq 1$.

ω-automata (BA)

Def.: ω-automaton (**Büchi** automaton) $\mathcal{A} = \langle \Sigma, S, S_{\text{init}}, \sigma, F \rangle$

- Σ finite input alphabet
- S finite set of states
- $S_{\text{init}} \subseteq S$ nonempty subset of initial states
- $\sigma \subseteq S \times \Sigma \times S$ transition relation
- $F \subseteq S$ nonempty subset of accepting states

$\mathcal{A}$ is deterministic when $|S_{\text{init}}| = 1$ and $\forall s, a.\ |\sigma(s, a)| \leq 1$.

ω-words: $w = a_0\ a_1\ a_2\ \ldots$

ω-automata (BA)

Def.: For $w = a_0\ a_1\ a_2\ \ldots$, a run of an automaton $\mathcal{A}$ is

$r = s_0\ s_1\ s_2\ \ldots$ such that $\forall i.\ (s_i, a_i, s_{i+1}) \in \sigma$.

ω-automata (BA)

Def.: For $w = a_0\ a_1\ a_2\ \ldots$, a run of an automaton $\mathcal{A}$ is

$r = s_0\ s_1\ s_2\ \ldots$ such that $\forall i.\ (s_i, a_i, s_{i+1}) \in \sigma$.

A run is accepting when $s_i \in F$ for infinitely many i.

ω-automata (BA)

Def.: For $w = a_0\ a_1\ a_2\ \ldots$, a run of an automaton $\mathcal{A}$ is

$r = s_0\ s_1\ s_2\ \ldots$ such that $\forall i.\ (s_i, a_i, s_{i+1}) \in \sigma$.

A run is accepting when $s_i \in F$ for infinitely many i.

Let $\inf(r) = \{s \in S : s = s_i$ for infinitely many $i\}$.
A run is accepting when $\inf(r) \cap F \neq \emptyset$.

ω-automata (BA)

Def.: For $w = a_0\ a_1\ a_2\ \ldots$, a run of an automaton $\mathcal{A}$ is

$r = s_0\ s_1\ s_2\ \ldots$ such that $\forall i.\ (s_i, a_i, s_{i+1}) \in \sigma$.

A run is accepting when $s_i \in F$ for infinitely many i.

Let $\inf(r) = \{s \in S : s = s_i$ for infinitely many $i\}$.
A run is accepting when $\inf(r) \cap F \neq \emptyset$.

$L_\omega(\mathcal{A}) := \{w \in \Sigma^\omega : \mathcal{A}$ has an accepting run for $w\}$.

ω-automata (BA)

Def.: For $w = a_0\ a_1\ a_2\ \ldots$, a run of an automaton $\mathcal{A}$ is

$r = s_0\ s_1\ s_2\ \ldots$ such that $\forall i.\ (s_i, a_i, s_{i+1}) \in \sigma$.

A run is accepting when $s_i \in F$ for infinitely many i.

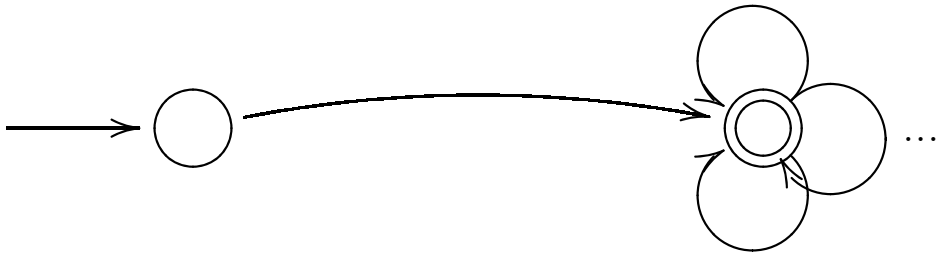
Let $\inf(r) = \{s \in S : s = s_i$ for infinitely many $i\}$.
A run is accepting when $\inf(r) \cap F \neq \emptyset$.

$L_\omega(\mathcal{A}) := \{w \in \Sigma^\omega : \mathcal{A}$ has an accepting run for $w\}$.

Def.: A language is $L \subseteq \Sigma^\omega$ is ω-regular if $L = L_\omega(\mathcal{A})$ for some $\mathcal{A}$.

ω-automata (BA)

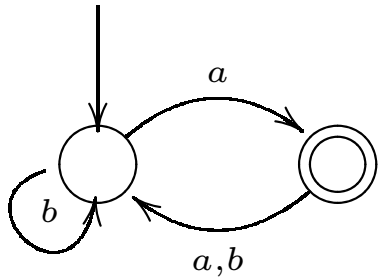
An accepting run looks like:



Examples

$\Sigma = \{a, b\}$

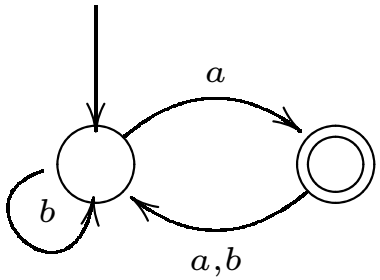
infinitely often a $\quad (b^*\ a)^\omega$



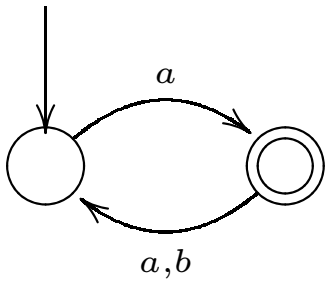
Examples

$\Sigma = \{a, b\}$

infinitely often a $\quad (b^*\ a)^\omega$



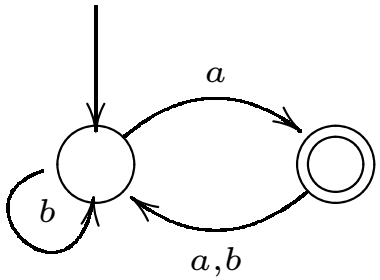
odd(a) $\quad (a\ (a + b))^\omega$



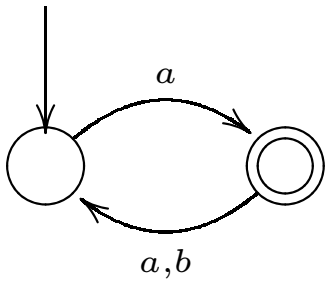
Examples

$\Sigma = \{a, b\}$

infinitely often a $\quad (b^*\ a)^\omega$



odd(a) $\quad (a\ (a + b))^\omega$



$LTL \subsetneq \omega$-automata

Exercise

– infinitely often a's and b's

– between any two consecutive a's
an even number of b's

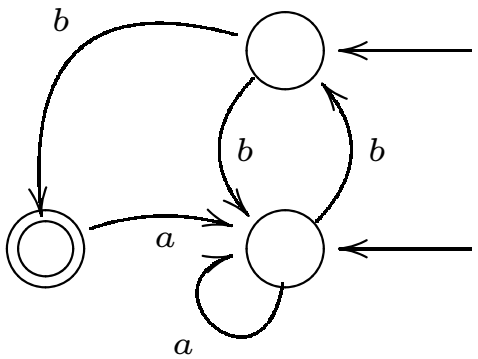
$$b^* \ (aa^* \ bb(bb)^*)^\omega$$

Exercise

– infinitely often a's and b's

$$b^* \ (aa^* \ bb(bb)^*)^\omega$$

– between any two consecutive a's
an even number of b's

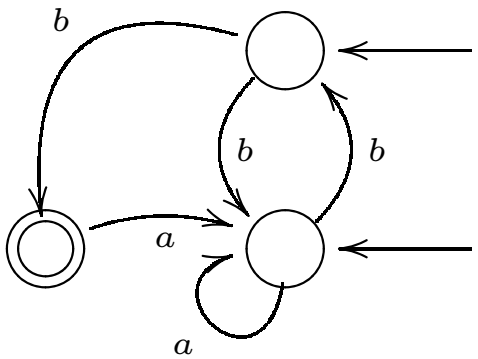


Exercise

– infinitely often a's and b's

$b^*\ (aa^*\ bb(bb)^*)^\omega$

– between any two consecutive a's
an even number of b's



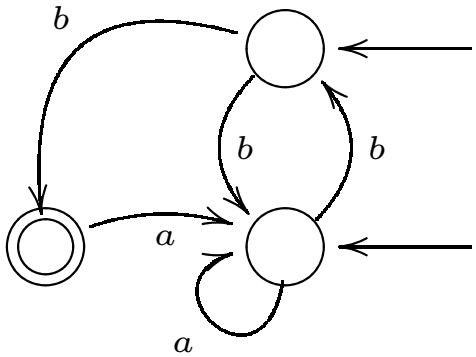
and what about deterministic ?

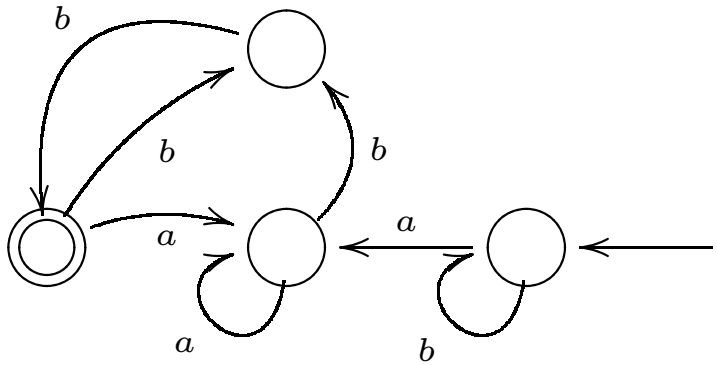
Exercise

– infinitely often a's and b's

$b^*\ (aa^*\ bb(bb)^*)^\omega$

– between any two consecutive a's
an even number of b's





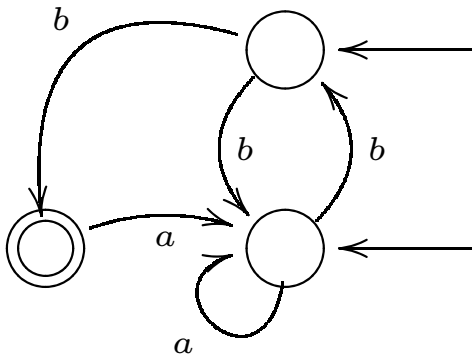
and what about deterministic ?

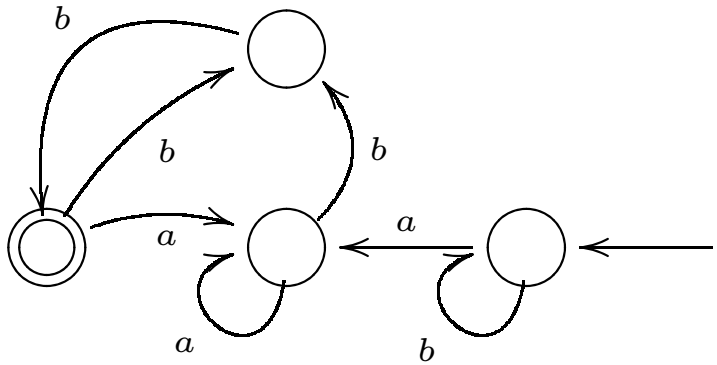
Exercise

– infinitely often a's and b's

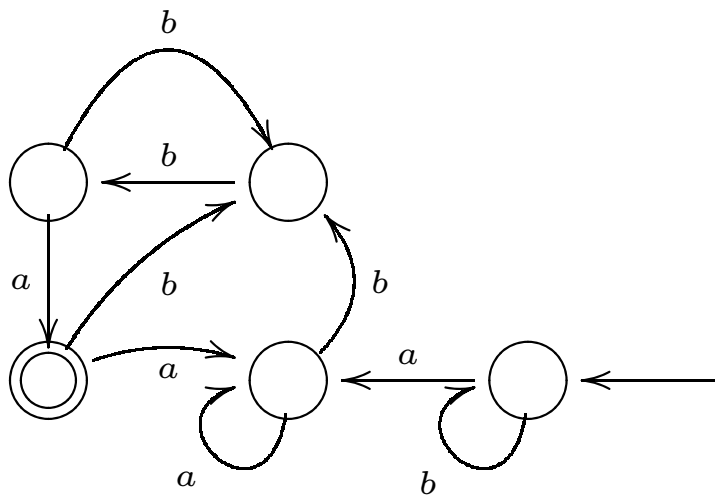
$b^*\ (aa^*\ bb(bb)^*)^\omega$

– between any two consecutive a's
an even number of b's





and what about deterministic ?



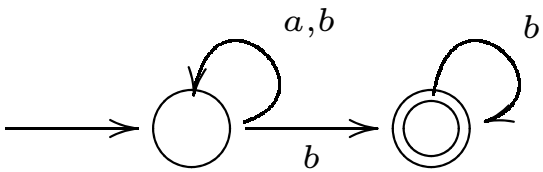
Exercise

finitely often a $(b + a)^* b^\omega$

Exercise

finitely often a

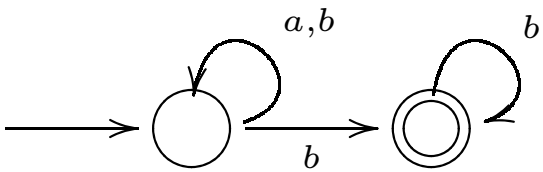
$(b + a)^* b^\omega$



Exercise

finitely often a

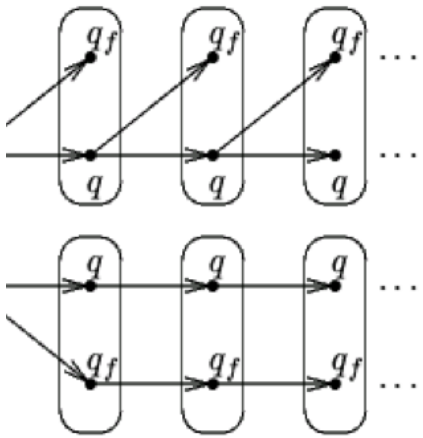
$(b + a)^* b^\omega$



and what about deterministic ?

Determinisation?

– powerset construction does not work



No determinization!

Thm: $(a+b)^*b^\omega$ is not accepted by a deterministic automaton.

No determinization!

Thm: $(a+b)^*b^\omega$ is not accepted by a deterministic automaton.

Proof: Assume $L_\omega(\mathcal{A}) = (a+b)^*b^\omega$, $\mathcal{A}$ deterministic.

No determinization!

Thm: $(a+b)^*b^\omega$ is not accepted by a deterministic automaton.

Proof: Assume $L_\omega(\mathcal{A}) = (a+b)^*b^\omega$, $\mathcal{A}$ deterministic.

$w_0 = b^\omega$. For some k_0, $\sigma(s_0, b^{k_0}) \in F$.

No determinization!

Thm: $(a+b)^*b^\omega$ is not accepted by a deterministic automaton.

Proof: Assume $L_\omega(\mathcal{A}) = (a+b)^*b^\omega$, $\mathcal{A}$ deterministic.

$w_0 = b^\omega$. For some k_0, $\sigma(s_0, b^{k_0}) \in F$.
$w_1 = b^{k_0}ab^\omega$. For some k_1, $\sigma(s_0, b^{k_0}ab^{k_1}) \in F$.
...

No determinization!

Thm: $(a+b)^*b^\omega$ is not accepted by a deterministic automaton.

Proof: Assume $L_\omega(\mathcal{A}) = (a+b)^*b^\omega$, $\mathcal{A}$ deterministic.

$w_0 = b^\omega$. For some k_0, $\sigma(s_0, b^{k_0}) \in F$.
$w_1 = b^{k_0}ab^\omega$. For some k_1, $\sigma(s_0, b^{k_0}ab^{k_1}) \in F$.
...

$\exists i < j$ such that $\sigma(s_0, b^{k_0}ab^{k_1} \ldots ab^{k_i}) = \sigma(s_0, b^{k_0}ab^{k_1} \ldots ab^{k_j})$

No determinization!

Thm: $(a+b)^*b^\omega$ is not accepted by a deterministic automaton.

Proof: Assume $L_\omega(\mathcal{A}) = (a+b)^*b^\omega$, $\mathcal{A}$ deterministic.

$w_0 = b^\omega$. For some k_0, $\sigma(s_0, b^{k_0}) \in F$.
$w_1 = b^{k_0}ab^\omega$. For some k_1, $\sigma(s_0, b^{k_0}ab^{k_1}) \in F$.
...

$\exists i < j$ such that $\sigma(s_0, b^{k_0}ab^{k_1} \ldots ab^{k_i}) = \sigma(s_0, b^{k_0}ab^{k_1} \ldots ab^{k_j})$

Thus $\mathcal{A}$ accepts $b^{k_0}ab^{k_1} \ldots ab^{k_i}(a \ldots ab^{k_j})^\omega$

contradiction!

Operations

Thm: ω-regular languages are closed under $\cup$, $\cap$ and complementation.

$\vee$, $\wedge$ and $\neg$

$\mathcal{A}_1, \mathcal{A}_2 \mapsto \mathcal{A}$

(1) $L_\omega(\mathcal{A}) = L_\omega(\mathcal{A}_1) \cup L_\omega(\mathcal{A}_2)$

(2) $L_\omega(\mathcal{A}) = L_\omega(\mathcal{A}_1) \cap L_\omega(\mathcal{A}_2)$

$\mathcal{A} \mapsto \bar{\mathcal{A}}$

(3) $L_\omega(\bar{\mathcal{A}}) = \Sigma^\omega \setminus L_\omega(\mathcal{A})$

Intersection

(2) $\mathcal{A}_1, \mathcal{A}_2 \mapsto \mathcal{A}$ $\qquad L_\omega(\mathcal{A}) = L_\omega(\mathcal{A}_1) \cap L_\omega(\mathcal{A}_2)$

?

Intersection

(2) $\mathcal{A}_1, \mathcal{A}_2 \mapsto \mathcal{A}$ $\qquad L_\omega(\mathcal{A}) = L_\omega(\mathcal{A}_1) \cap L_\omega(\mathcal{A}_2)$

$$S = S_1 \times S_2 \times \{1, 2\}$$

$$S_{\text{init}} = S_{1,\text{init}} \times S_{2,\text{init}} \times \{1\}$$

$$F = F_1 \times S_2 \times \{1\}$$

$$((s,t,i), a, (s',t',j)) \in \sigma \iff (s,a,s') \in \sigma_1,\ (t,a,t') \in \sigma_2,$$

$$j = \begin{cases} 2 & \text{if } i = 1,\ s \in F_1 \\ 1 & \text{if } i = 2,\ t \in F_2 \\ i & \text{otherwise} \end{cases}$$

Complementation?

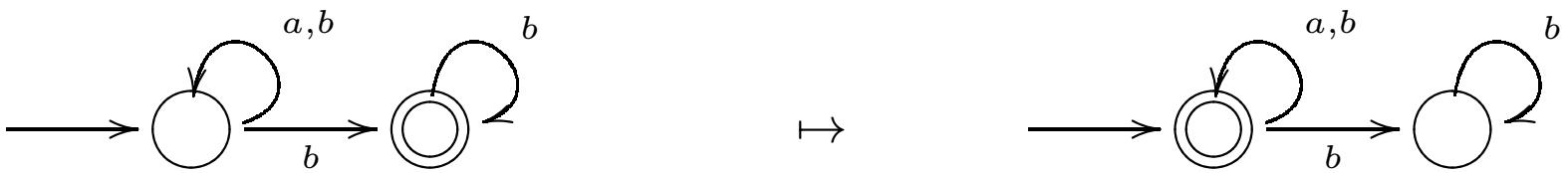
(3) $\mathcal{A} \mapsto \bar{\mathcal{A}}$ $\qquad L_\omega(\bar{\mathcal{A}}) = \Sigma^\omega \setminus L_\omega(\mathcal{A})$

– no determinization

Complementation?

(3) $\mathcal{A} \mapsto \bar{\mathcal{A}}$ $\qquad L_\omega(\bar{\mathcal{A}}) = \Sigma^\omega \setminus L_\omega(\mathcal{A})$

- no determinization
- naive approach is not correct



Complementation

(3) $\mathcal{A} \mapsto \bar{\mathcal{A}}$ $\qquad L_\omega(\bar{\mathcal{A}}) = \Sigma^\omega \setminus L_\omega(\mathcal{A})$

– no determinization

Complementation

(3) $\mathcal{A} \mapsto \bar{\mathcal{A}}$ $\qquad L_\omega(\bar{\mathcal{A}}) = \Sigma^\omega \setminus L_\omega(\mathcal{A})$

- no determinization
- a complex construction

Complementation

(3) $\mathcal{A} \mapsto \bar{\mathcal{A}}$ $\qquad L_\omega(\bar{\mathcal{A}}) = \Sigma^\omega \setminus L_\omega(\mathcal{A})$

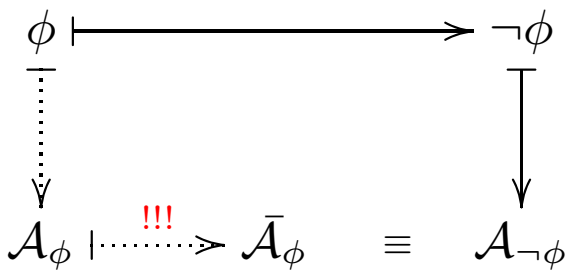
- no determinization
- a complex construction
- $|\bar{\mathcal{A}}| = 2^{\mathcal{O}(n \cdot \log n)}$, where $n = |\mathcal{A}|$

Complementation

(3) $\mathcal{A} \mapsto \bar{\mathcal{A}}$ $\qquad L_\omega(\bar{\mathcal{A}}) = \Sigma^\omega \setminus L_\omega(\mathcal{A})$

- no determinization
- a complex construction
- $|\bar{\mathcal{A}}| = 2^{\mathcal{O}(n \cdot \log n)}$, where $n = |\mathcal{A}|$

Moral: Better to avoid complementation



Complementation

Question: How complementation is done if $\mathcal{A}$ is deterministic?

Complementation

Question: How complementation is done if $\mathcal{A}$ is deterministic?

$$\mathcal{A} \mapsto \bar{\mathcal{A}}$$

$$F \mapsto \bar{F} = Q \setminus F$$

$L_\omega(\bar{\mathcal{A}}) = \Sigma^\omega \setminus L_\omega(\mathcal{A})$?

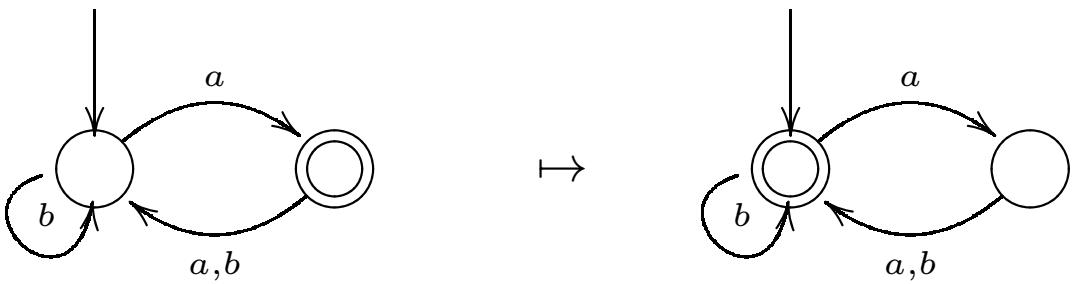
Complementation

Question: How complementation is done if $\mathcal{A}$ is deterministic?

$$\mathcal{A} \mapsto \bar{\mathcal{A}}$$

$$F \mapsto \bar{F} = Q \setminus F$$

$L_\omega(\bar{\mathcal{A}}) = \Sigma^\omega \setminus L_\omega(\mathcal{A})$? **NO!**



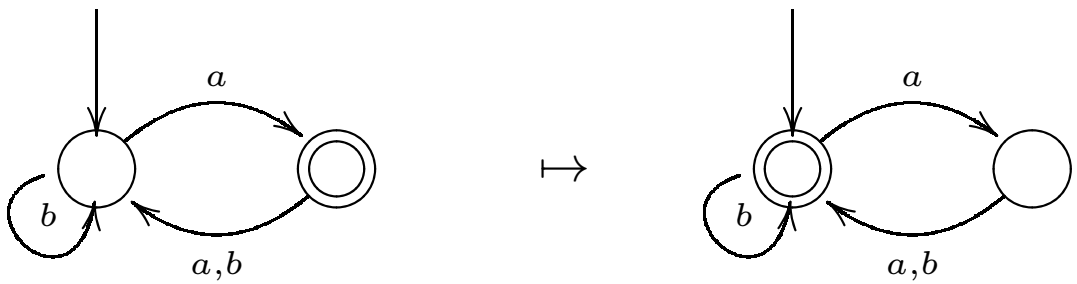
Complementation

Question: How complementation is done if $\mathcal{A}$ is deterministic?

$$\mathcal{A} \mapsto \bar{\mathcal{A}}$$

$$F \mapsto \bar{F} = Q \setminus F$$

$L_\omega(\bar{\mathcal{A}}) = \Sigma^\omega \setminus L_\omega(\mathcal{A})$? **NO!**



co-Büchi: a run $r = s_0\ s_1\ s_2\ \ldots$ is accepting when $s_i \in \bar{F}$ for almost all i ($\inf(r) \subseteq \bar{F}$).

Decision problems

problem for finite automata	problem for ω-automata	complexity	cost of algorithm
$L(A) \neq \emptyset$	$L_\omega(A) \neq \emptyset$	NLOGSPACE	$\mathcal{O}(n)$
$L(A) = \Sigma^*$	$L_\omega(A) = \Sigma^\omega$	PSPACE	$2^{\mathcal{O}(n \cdot \log n)}$
$L(A) \subseteq L(B)$	$L_\omega(A) \subseteq L_\omega(B)$	PSPACE	$2^{\mathcal{O}(n \cdot \log n)}$

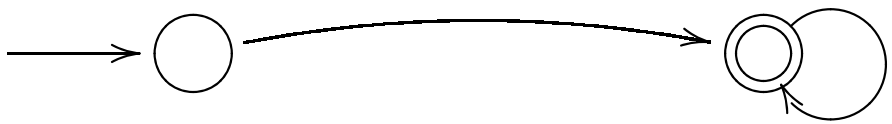
$L(\mathcal{A}_M) \subseteq L(\mathcal{A}_\phi)?$ vs $L(\mathcal{A}_M) \cap L(\mathcal{A}_{\neg\phi}) = \emptyset?$

Decision problems

problem for finite automata	problem for ω-automata	complexity	cost of algorithm
$L(A) \neq \emptyset$	$L_\omega(A) \neq \emptyset$	NLOGSPACE	$\mathcal{O}(n)$
$L(A) = \Sigma^*$	$L_\omega(A) = \Sigma^\omega$	PSPACE	$2^{\mathcal{O}(n \cdot \log n)}$
$L(A) \subseteq L(B)$	$L_\omega(A) \subseteq L_\omega(B)$	PSPACE	$2^{\mathcal{O}(n \cdot \log n)}$

$L(\mathcal{A}_M) \subseteq L(\mathcal{A}_\phi)?$ vs $L(\mathcal{A}_M) \cap L(\mathcal{A}_{\neg\phi}) = \emptyset?$

Lasso

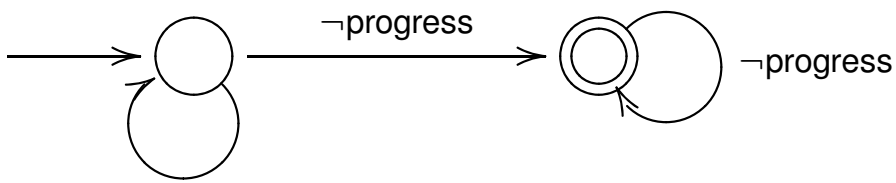


Thm: $L_\omega(A) \neq \emptyset$ iff $\mathcal{A}$ has a lasso.

LTL $\mapsto$ ω-automata

SPIN – examples

F G ¬progress



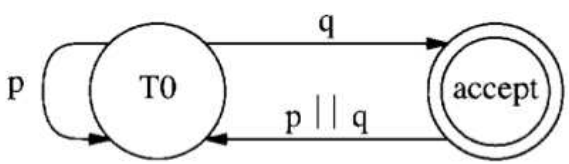

```
never { /* non-progress: ◇□¬progress */
    do
    :: skip
    :: !progress -> break
    od;
accept: do
    :: !progress
    od
}
```

[Holzmann,Peled,Yannakakis 1996]

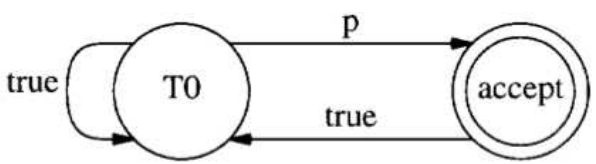
(co-Büchi $\subseteq$ Büchi)

SPIN – examples (cont.)

```
$ spin -f "[](p U q)"
never {
T0:
        if
        :: (p) -> goto T0
        :: (q) -> goto accept
        fi;
accept:
        if
        :: ((p) || (q)) -> goto T0
        fi
}
```




```
$ spin -f "[]<>p"
never {
T0:
        if
        :: (true) -> goto T0
        :: (p) -> goto accept
        fi;
accept:
        if
        :: (true) -> goto T0
        fi
}
```



SPIN's doc

Generalized ω-automata (GBA)

- $\{F_1, \ldots, F_n\}$ instead of F
- a run r is accepting when $\forall i.\ \inf(r) \cap F_i \neq \emptyset$

Question: Are generalized automata more expressive?

Generalized ω-automata (GBA)

- $\{F_1, \ldots, F_n\}$ instead of F
- a run r is accepting when $\forall i.\ \inf(r) \cap F_i \neq \emptyset$

Question: Are generalized automata more expressive?

$$\mathcal{A}_{F_1 \ldots F_n} \ \mapsto \ \mathcal{A}_F$$

$$L_\omega(\mathcal{A}_{F_1 \ldots F_n}) \ = \ L_\omega(\mathcal{A}_F)$$

Generalized ω-automata (GBA)

- $\{F_1, \ldots, F_n\}$ instead of F
- a run r is accepting when $\forall i.\ \inf(r) \cap F_i \neq \emptyset$

Question: Are generalized automata more expressive?

$$\mathcal{A}_{F_1 \ldots F_n} \ \mapsto \ \mathcal{A}_F$$

$$L_\omega(\mathcal{A}_{F_1 \ldots F_n}) \ = \ L_\omega(\mathcal{A}_F)$$

$$|\mathcal{A}_F| = \mathcal{O}(|\mathcal{A}_{F_1,\ldots,F_n}| \cdot n)$$

$$L_\omega(\mathcal{A}_F) \ \subseteq \ L_\omega(\mathcal{A}_{F_1}) \cap \ldots \cap L_\omega(\mathcal{A}_{F_n})$$

LTL $\mapsto$ BA

- **SPIN:** LTL $\mapsto$ GBA $\mapsto$ BA
- **LTL2BA:** LTL $\mapsto$ ABA $\mapsto$ GBA' $\mapsto$ BA

- On-the-fly verification

LTL $\mapsto$ GBA (1)

LTL$^+$:

$$\phi \;:=\; p \mid \neg p \mid \phi_1 \wedge \phi_2 \mid \phi_1 \vee \phi_2 \mid \mathsf{X}\,\phi \mid \phi_1 \,\mathsf{U}\, \phi_2 \mid \phi_1 \,\mathsf{R}\, \phi_2 \mid \texttt{true} \mid \texttt{false}$$

Intuition: $\phi \;\equiv\; \mathsf{now}(\phi) \stackrel{\wedge}{\vee} \mathsf{later}(\phi)$

$$\phi \,\mathsf{U}\, \psi \;\equiv\; \psi \;\vee\; (\phi \wedge \mathsf{X}\,(\phi \,\mathsf{U}\, \psi))$$

$$\phi \,\mathsf{R}\, \psi \;\equiv\; \psi \;\wedge\; (\phi \vee \mathsf{X}\,(\phi \,\mathsf{R}\, \psi))$$

(fixed points)

LTL $\mapsto$ GBA (2)

. . . do not think about tomorrow! :)

$$\bar{P} = \{\neg p : p \in P\}$$

$\alpha \mapsto \mathsf{today}(\alpha)$ – positive boolean formula over facts $P \cup \bar{P} \cup \{\mathsf{X}\,\phi : \phi \ldots\}$

today facts $P \cup \bar{P}$
tomorrow facts $\{\mathsf{X}\,\phi : \phi \ldots\}$

$$
\begin{array}{lcl}
\mathsf{today}(\alpha) & = & \alpha, \quad \text{when} \quad \alpha = p, \neg p, \mathsf{X}\,\beta, \texttt{true}, \texttt{false} \\
\mathsf{today}(\alpha \vee \beta) & = & \mathsf{today}(\alpha) \vee \mathsf{today}(\beta) \\
\mathsf{today}(\alpha \wedge \beta) & = & \mathsf{today}(\alpha) \wedge \mathsf{today}(\beta) \\
\mathsf{today}(\alpha\,\mathsf{U}\,\beta) & = & \mathsf{today}(\beta) \vee (\mathsf{today}(\alpha) \wedge \mathsf{X}\,(\alpha\,\mathsf{U}\,\beta)) \\
\mathsf{today}(\alpha\,\mathsf{R}\,\beta) & = & \mathsf{today}(\beta) \wedge (\mathsf{today}(\alpha) \vee \mathsf{X}\,(\alpha\,\mathsf{R}\,\beta))
\end{array}
$$

LTL $\mapsto$ GBA (3)

$$\alpha \;\mapsto\; \mathsf{today}(\alpha) \;\mapsto\; \mathsf{dnf}(\alpha) \;\subseteq\; \mathcal{P}(P \cup \bar{P} \cup \{\mathsf{X}\,\phi : \phi \ldots\})$$

$$\mathsf{today}(\alpha) \;\equiv\; \mathsf{dnf}(\alpha) \;\equiv\; \vee_{X \in \mathsf{dnf}(\alpha)} \left(\wedge X\right)$$

For example:

$\mathsf{dnf}(\alpha) = \{\{\alpha\}\}$, when $\alpha = p, \neg p, \mathsf{X}\,\beta$

$\mathsf{dnf}(\alpha \vee \beta) = \mathsf{dnf}(\alpha) \cup \mathsf{dnf}(\beta)$

$\mathsf{dnf}(\alpha \wedge \beta) = \{X \cup Y \;:\; X \in \mathsf{dnf}(\alpha),\; Y \in \mathsf{dnf}(\beta)\}$

$\mathsf{dnf}(\alpha\,\mathsf{U}\,\beta) = \mathsf{dnf}(\beta) \cup \mathsf{dnf}(\alpha \wedge \mathsf{X}\,(\alpha\,\mathsf{U}\,\beta)))$

$\mathsf{dnf}(\texttt{true}) = \{\emptyset\}$ $\quad \wedge\emptyset \equiv \texttt{true}$

$\mathsf{dnf}(\texttt{false}) = \emptyset$ $\quad \vee\emptyset \equiv \texttt{false}$

LTL $\mapsto$ GBA (4)

GBA $\mathcal{A}_\phi = \langle \Sigma, S, S_{\text{init}}, \sigma, F \rangle$:

- $\Sigma = \mathcal{P}(P)$
- $S = \mathcal{P}(P \cup \bar{P} \cup \{ \mathsf{X}\,\phi : \phi \ldots \})$
- $S_{\text{init}} = \mathsf{dnf}(\phi)$
- $X \xrightarrow{A} Y$ iff
  - $X \cap P \subseteq A$ — X and A non-contradictory today
  - $(X \cap \bar{P}) \cap A = \emptyset$
  - $Y \in \mathsf{dnf}(\wedge \{\alpha \mid \mathsf{X}\,\alpha \in X\})$ — possible tomorrow
- $F = ?$

LTL $\mapsto$ GBA (example 1)

$\phi = \neg a \,\mathsf{U}\, b$

$\phi \equiv b \vee (\neg a \wedge \mathsf{X}\,\phi)$

$S = \mathcal{P}(a,\ \neg a,\ b,\ \neg b,\ \mathsf{X}\,(\neg a \,\mathsf{U}\, b))$

$\Sigma = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}$

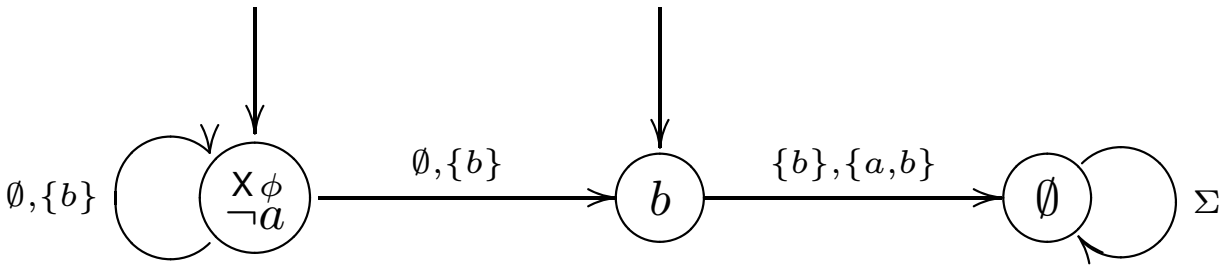
LTL $\mapsto$ GBA (example 1)

$\phi = \neg a \,\mathsf{U}\, b$

$S = \mathcal{P}(a,\ \neg a,\ b,\ \neg b,\ \mathsf{X}(\neg a \,\mathsf{U}\, b))$

$\Sigma = \{\emptyset, \{a\}, \{b\}, \{a,b\}\}$

$\phi \equiv b \vee (\neg a \wedge \mathsf{X}\,\phi)$



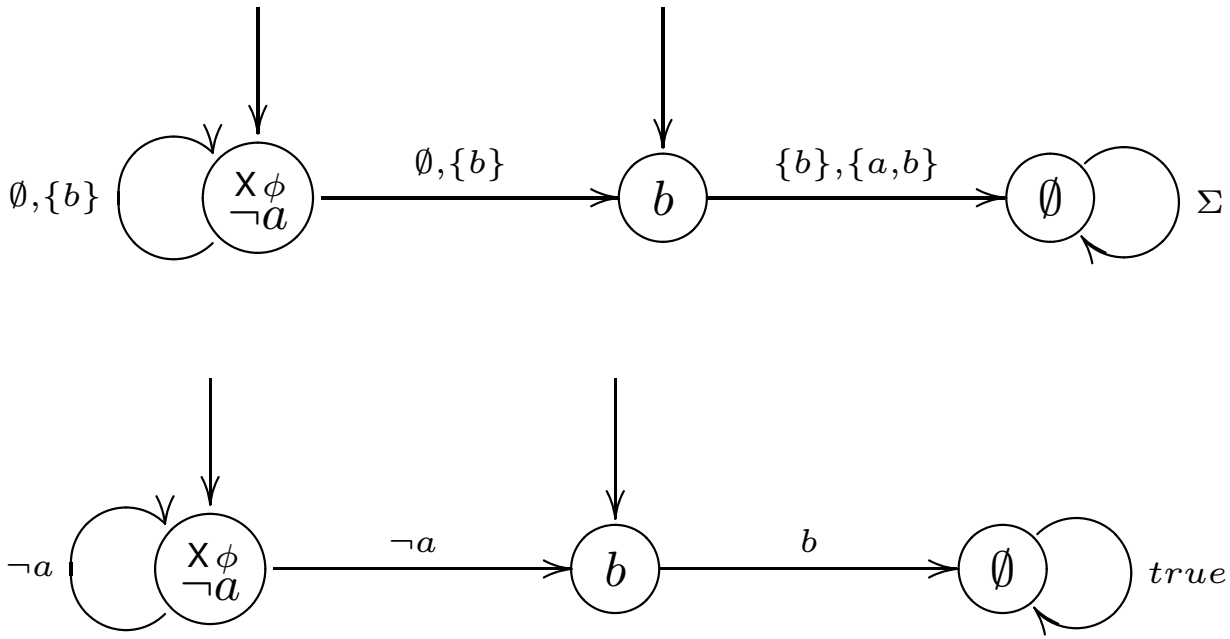
LTL $\mapsto$ GBA (example 1)

$\phi = \neg a \,\mathsf{U}\, b$

$S = \mathcal{P}(a,\ \neg a,\ b,\ \neg b,\ \mathsf{X}(\neg a \,\mathsf{U}\, b))$

$\Sigma = \{\emptyset, \{a\}, \{b\}, \{a,b\}\}$

$\phi \equiv b \vee (\neg a \wedge \mathsf{X}\,\phi)$



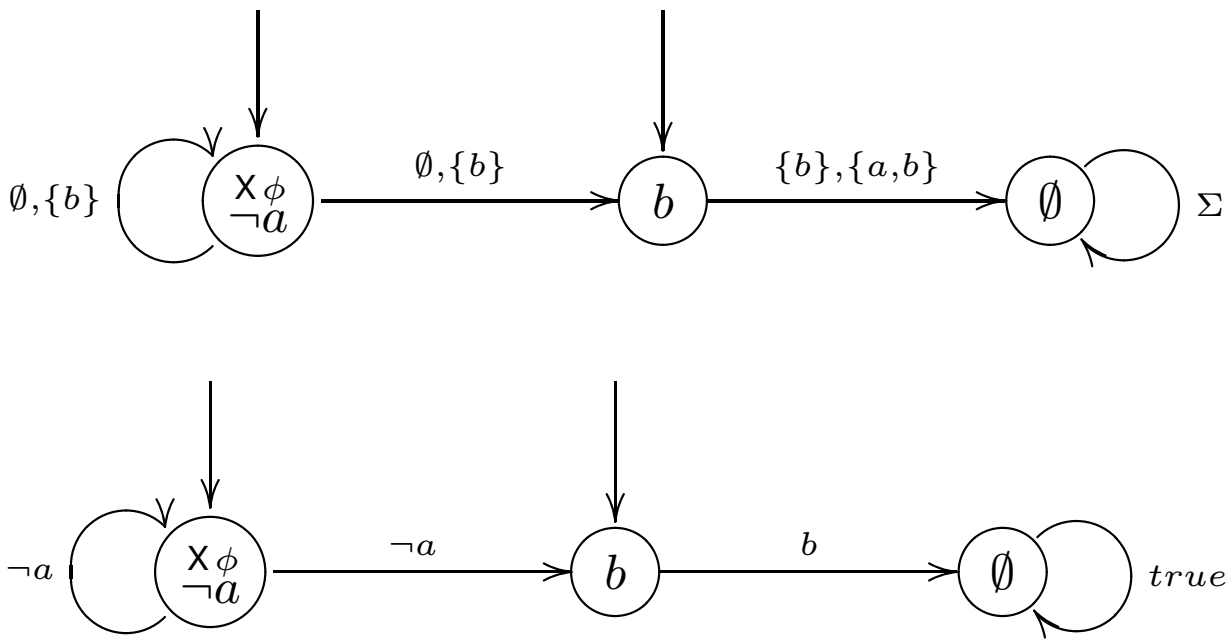
LTL $\mapsto$ GBA (example 1)

$\phi = \neg a \,\mathsf{U}\, b$

$S = \mathcal{P}(a,\ \neg a,\ b,\ \neg b,\ \mathsf{X}(\neg a \,\mathsf{U}\, b))$

$\Sigma = \{\emptyset, \{a\}, \{b\}, \{a,b\}\}$

$\phi \equiv b \vee (\neg a \wedge \mathsf{X}\,\phi)$



$F = ?$

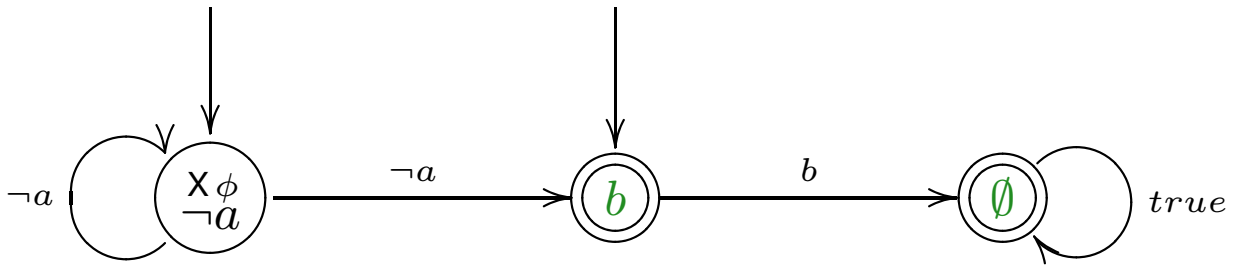
LTL $\mapsto$ GBA (example 1)

$\phi = \neg a \,\mathsf{U}\, b$

$S = \mathcal{P}(a,\ \neg a,\ b,\ \neg b,\ \mathsf{X}(\neg a \,\mathsf{U}\, b))$

$\Sigma = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}$

$\phi \equiv b \vee (\neg a \wedge \mathsf{X}\,\phi)$



$F = \{\emptyset, \{b\}\}$

LTL $\mapsto$ GBA (F)

– $\{\alpha_i \,\mathsf{U}\, \beta_i \mid i = 1, \ldots, n\} \subseteq \mathsf{subformulas}(\phi)$

LTL $\mapsto$ GBA (F)

- $\{\alpha_i \,\mathsf{U}\, \beta_i \mid i = 1, \ldots, n\} \subseteq \mathsf{subformulas}(\phi)$
- $S \setminus F_i \;=\; \{X \in S \;\mid\; \alpha_i \,\mathsf{U}\, \beta_i \in X \;\wedge\; \beta_i \notin X\}, \quad i = 1, \ldots, n$

LTL $\mapsto$ GBA (F)

- $\{\alpha_i \,\mathsf{U}\, \beta_i \mid i = 1, \ldots, n\} \subseteq \mathsf{subformulas}(\phi)$
- $S \setminus F_i \;=\; \{X \in S \;\mid\; \alpha_i \,\mathsf{U}\, \beta_i \in X \;\wedge\; \beta_i \notin X\}, \quad i = 1, \ldots, n$
- $S \setminus F_i \;=\; \{X \in S \;\mid\; \alpha_i \,\mathsf{U}\, \beta_i \in \mathsf{cons}(X) \;\wedge\; \beta_i \notin \mathsf{cons}(X)\}$

LTL $\mapsto$ GBA (F)

- $\{\alpha_i \,\mathsf{U}\, \beta_i \mid i = 1, \ldots, n\} \subseteq \mathsf{subformulas}(\phi)$
- $S \setminus F_i = \{X \in S \mid \alpha_i \,\mathsf{U}\, \beta_i \in X \wedge \beta_i \notin X\}, \quad i = 1, \ldots, n$
- $S \setminus F_i = \{X \in S \mid \alpha_i \,\mathsf{U}\, \beta_i \in \mathsf{cons}(X) \wedge \beta_i \notin \mathsf{cons}(X)\}$

$X \subseteq \mathsf{cons}(X)$

$\alpha \vee \beta \in \mathsf{cons}(X)$	if	$\alpha \in \mathsf{cons}(X)$
$\alpha \vee \beta \in \mathsf{cons}(X)$	if	$\beta \in \mathsf{cons}(X)$
$\alpha \wedge \beta \in \mathsf{cons}(X)$	if	$\alpha \in \mathsf{cons}(X)$ and $\beta \in \mathsf{cons}(X)$
$\alpha \,\mathsf{U}\, \beta \in \mathsf{cons}(X)$	if	$\beta \vee (\alpha \wedge \mathsf{X}(\alpha \,\mathsf{U}\, \beta)) \in \mathsf{cons}(X)$
$\alpha \,\mathsf{R}\, \beta \in \mathsf{cons}(X)$	if	$\beta \wedge (\alpha \vee \mathsf{X}(\alpha \,\mathsf{R}\, \beta)) \in \mathsf{cons}(X)$
$\texttt{true} \in \mathsf{cons}(X)$		

$\alpha \,\mathsf{U}\, \beta \in \mathsf{cons}(X)$ if $\beta \in \mathsf{cons}(X)$
or
$\alpha \in \mathsf{cons}(X)$ and $\mathsf{X}(\alpha \,\mathsf{U}\, \beta)) \in X$

LTL $\mapsto$ GBA (F)

- $\{\alpha_i \,\mathsf{U}\, \beta_i \mid i = 1, \ldots, n\} \subseteq \mathsf{subformulas}(\phi)$
- $S \setminus F_i \;=\; \{X \in S \;\mid\; \alpha_i \,\mathsf{U}\, \beta_i \in X \;\wedge\; \beta_i \notin X\}, \quad i = 1, \ldots, n$
- $S \setminus F_i \;=\; \{X \in S \;\mid\; \alpha_i \,\mathsf{U}\, \beta_i \in \mathsf{cons}(X) \;\wedge\; \beta_i \notin \mathsf{cons}(X)\}$

$X \subseteq \mathsf{cons}(X)$

$\alpha \vee \beta \in \mathsf{cons}(X)$ if $\alpha \in \mathsf{cons}(X)$

$\alpha \vee \beta \in \mathsf{cons}(X)$ if $\beta \in \mathsf{cons}(X)$

$\alpha \wedge \beta \in \mathsf{cons}(X)$ if $\alpha \in \mathsf{cons}(X)$ and $\beta \in \mathsf{cons}(X)$

$\alpha \,\mathsf{U}\, \beta \in \mathsf{cons}(X)$ if $\beta \;\vee\; (\alpha \wedge \mathsf{X}\,(\alpha \,\mathsf{U}\, \beta)) \in \mathsf{cons}(X)$

$\alpha \,\mathsf{R}\, \beta \in \mathsf{cons}(X)$ if $\beta \;\wedge\; (\alpha \vee \mathsf{X}\,(\alpha \,\mathsf{R}\, \beta)) \in \mathsf{cons}(X)$

$\texttt{true} \in \mathsf{cons}(X)$

$\alpha \,\mathsf{U}\, \beta \in \mathsf{cons}(X)$ if $\beta \in \mathsf{cons}(X)$
or
$\alpha \in \mathsf{cons}(X)$ and $\mathsf{X}\,(\alpha \,\mathsf{U}\, \beta)) \in X$

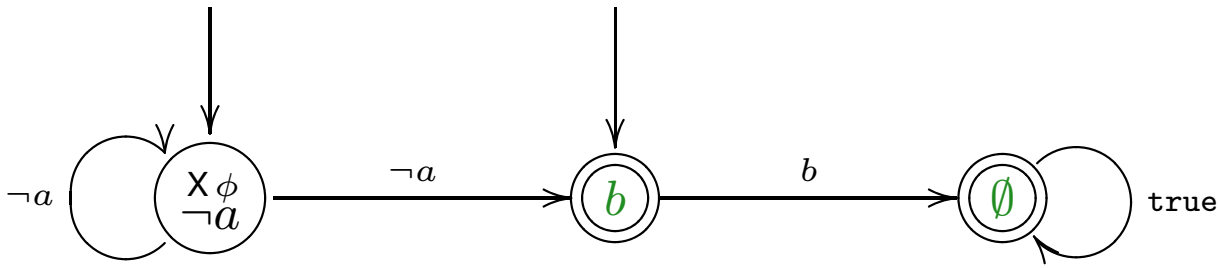
- $S \setminus F_i \;=\; \{X \in S \;\mid\; \alpha_i \in \mathsf{cons}(X) \;\wedge\; \mathsf{X}\,(\alpha_i \,\mathsf{U}\, \beta_i) \in X \;\wedge\; \beta_i \notin \mathsf{cons}(X)\}$

LTL $\mapsto$ GBA (example 1 cont.)

$\phi = \neg a \,\mathsf{U}\, b$

$S = \mathcal{P}(a,\ \neg a,\ b,\ \neg b,\ \mathsf{X}(\neg a \,\mathsf{U}\, b))$

$\Sigma = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}$



$S \setminus F = \{X \in S \mid \neg a \in X \ \wedge\ \mathsf{X}\phi \in X \ \wedge\ b \notin X\}$

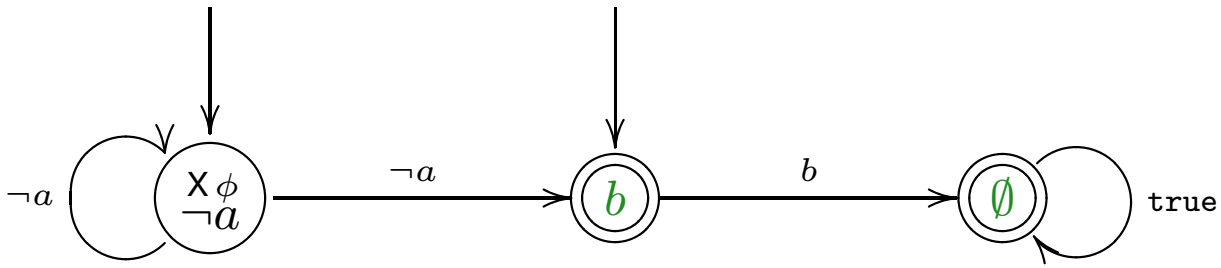
Can automaton $\mathcal{A}_\phi$ be smaller?

LTL $\mapsto$ GBA (example 1 cont.)

$\phi = \neg a \,\mathsf{U}\, b$

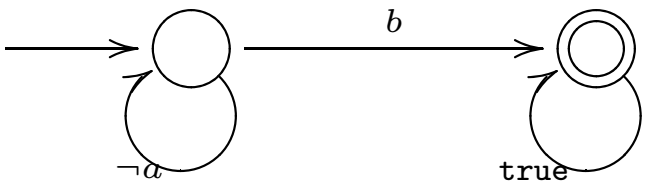
$S = \mathcal{P}(a,\ \neg a,\ b,\ \neg b,\ \mathsf{X}(\neg a \,\mathsf{U}\, b))$

$\Sigma = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}$



$S \setminus F = \{X \in S \mid \neg a \in X \ \wedge\ \mathsf{X}\phi \in X \ \wedge\ b \notin X\}$

Can automaton $\mathcal{A}_\phi$ be smaller? **YES!**



exponential blow-up

LTL $\mapsto$ GBA (example 2)

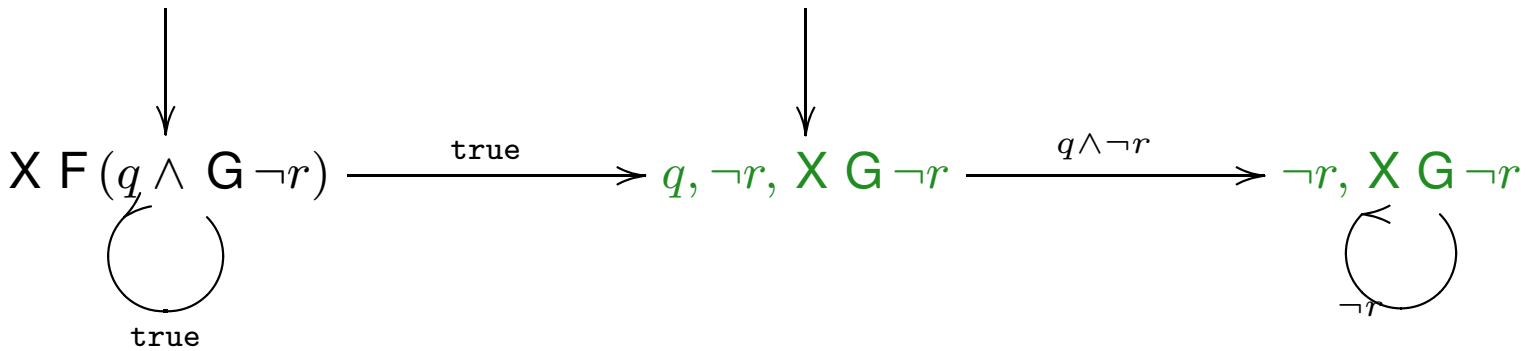
$\theta = \neg \mathsf{G}(q \implies \mathsf{F}\, r) \equiv \mathsf{F}(q \wedge \mathsf{G} \neg r)$

$S = \mathcal{P}(q,\ \neg q,\ r,\ \neg r,\ \mathsf{X}(\mathsf{F}(q \wedge \mathsf{G} \neg r)),\ \mathsf{X}\, \mathsf{G} \neg r)$ $\qquad F = ?$

$\mathsf{dnf}(\mathsf{F}\, \alpha) = \mathsf{dnf}(\alpha) \vee \mathsf{X}\, \mathsf{F}\, \alpha$ $\qquad \mathsf{F}\, \alpha \equiv \alpha \vee \mathsf{X}\, \mathsf{F}\, \alpha$

$\mathsf{dnf}(\mathsf{G}\, \alpha) = \mathsf{dnf}(\alpha \wedge \mathsf{X}\, \mathsf{G}\, \alpha)$ $\qquad \mathsf{G}\, \alpha \equiv \alpha \wedge \mathsf{X}\, \mathsf{G}\, \alpha$

$\mathsf{dnf}(\mathsf{F}(q \wedge \mathsf{G} \neg r)) = \mathsf{X}\, \mathsf{F}(q \wedge \mathsf{G} \neg r) \vee q \wedge \neg r \wedge \mathsf{X}\, \mathsf{G} \neg r$



LTL $\mapsto$ GBA (example 2)

$$\theta = \neg(\mathsf{G}\,\mathsf{F}\,p \implies \mathsf{G}\,(q \implies \mathsf{F}\,r)) \equiv \mathsf{G}\,\mathsf{F}\,p \wedge \mathsf{F}\,(q \wedge \mathsf{G}\,\neg r)$$

$\mathsf{dnf}(\mathsf{F}\,\alpha) = \mathsf{dnf}(\alpha) \vee \mathsf{X}\,\mathsf{F}\,\alpha$ $\qquad$ $\mathsf{F}\,\alpha \equiv \alpha \vee \mathsf{X}\,\mathsf{F}\,\alpha$

$\mathsf{dnf}(\mathsf{G}\,\alpha) = \mathsf{dnf}(\alpha \wedge \mathsf{X}\,\mathsf{G}\,\alpha)$ $\qquad$ $\mathsf{G}\,\alpha \equiv \alpha \wedge \mathsf{X}\,\mathsf{G}\,\alpha$

$\mathsf{dnf}(\mathsf{F}\,(q \wedge \mathsf{G}\,\neg r)) = \mathsf{X}\,\mathsf{F}\,(q \wedge \mathsf{G}\,\neg r) \vee (q \wedge \neg r \wedge \mathsf{X}\,\mathsf{G}\,\neg r)$

$\mathsf{dnf}(\mathsf{G}\,\mathsf{F}\,p) = \mathsf{dnf}((p \vee \mathsf{X}\,\mathsf{F}\,p) \wedge \mathsf{X}\,\mathsf{G}\,\mathsf{F}\,p) =$

$(p \wedge \mathsf{X}\,\mathsf{G}\,\mathsf{F}\,p) \vee (\mathsf{X}\,\mathsf{F}\,p \wedge \mathsf{X}\,\mathsf{G}\,\mathsf{F}\,p)$

$\mathsf{dnf}(\mathsf{G}\,\mathsf{F}\,p \wedge \mathsf{F}\,(q \wedge \mathsf{G}\,\neg r)) = \ldots \vee \ldots \vee \ldots \vee \ldots$

$\mathsf{X}\,\mathsf{F}\,(q \wedge \mathsf{G}\,\neg r), p, \mathsf{X}\,\mathsf{G}\,\mathsf{F}\,p$ $\qquad$ $q, \neg r, \mathsf{X}\,\mathsf{G}\,\neg r, p, \mathsf{X}\,\mathsf{G}\,\mathsf{F}\,p$

$\mathsf{X}\,\mathsf{F}\,(q \wedge \mathsf{G}\,\neg r), \mathsf{X}\,\mathsf{F}\,p, \mathsf{X}\,\mathsf{G}\,\mathsf{F}\,p$ $\qquad$ $q, \neg r, \mathsf{X}\,\mathsf{G}\,\neg r, \mathsf{X}\,\mathsf{F}\,p, \mathsf{X}\,\mathsf{G}\,\mathsf{F}\,p$

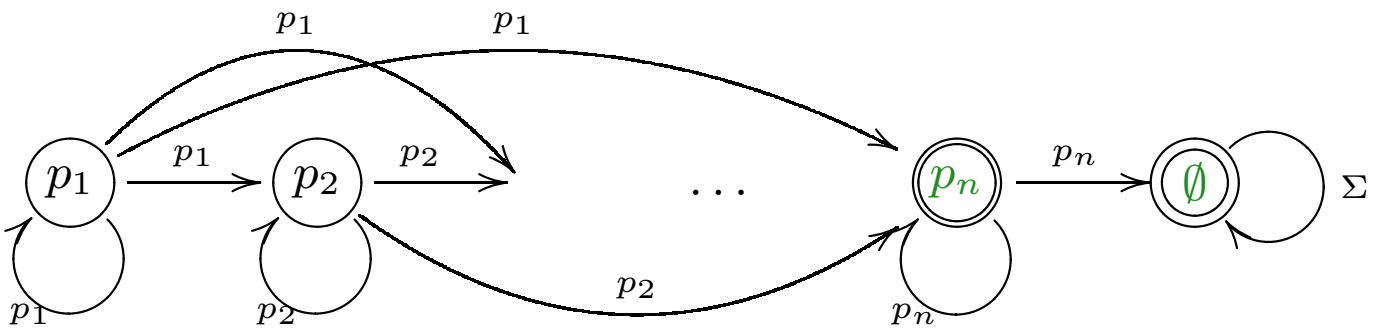
LTL $\mapsto$ GBA (example 2)

$$\theta_n = \neg((\mathsf{G}\,\mathsf{F}\,p_1 \wedge \ldots \wedge \mathsf{G}\,\mathsf{F}\,p_n) \Longrightarrow \mathsf{G}\,(q \Longrightarrow \mathsf{F}\,r)) \equiv$$

$$\mathsf{G}\,\mathsf{F}\,p_1 \wedge \ldots \wedge \mathsf{G}\,\mathsf{F}\,p_n \wedge \mathsf{F}\,(q \wedge \mathsf{G}\,\neg r)$$

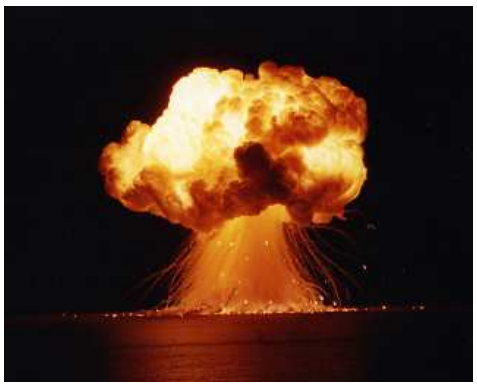
LTL $\mapsto$ GBA (example 3)

$$\phi_n \;=\; p_1 \,\mathsf{U}\, (p_2 \,\mathsf{U}\, (\ldots \,\mathsf{U}\, p_n) \ldots)$$



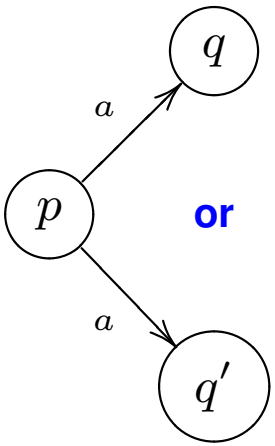
$$\theta_n \;=\; \neg\big(p_1 \,\mathsf{U}\, (p_2 \,\mathsf{U}\, (\ldots \,\mathsf{U}\, p_n) \ldots)\big) \;\equiv\; \big(\neg p_1 \,\mathsf{R}\, (\neg p_2 \,\mathsf{R}\, (\ldots \,\mathsf{R}\, \neg p_n) \ldots)\big)$$

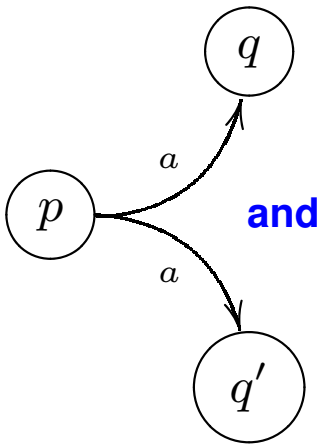
$$\phi \,\mathsf{R}\, \psi \;\equiv\; \psi \wedge (\phi \vee \mathsf{X}\,(\phi \,\mathsf{R}\, \psi))$$



LTL $\mapsto$ ABA

Alternation (ABA)





$\sigma(p, a) = q \vee q'$

$(p, a, q), (p, a, q') \in \sigma$

$\sigma(p, a) = q \wedge q'$

—

Example transition: $\sigma(p, a) = p_1 \vee p_2 \wedge p_3$ (think of positive DNF)

run = tree (dag) labeled with states

LTL $\mapsto$ ABA (1)

ABA $\mathcal{A}_\phi = \langle \Sigma, S, S_{\text{init}}, \sigma, F \rangle$:

- S = modal subformulas ($\mathsf{X}\,\alpha,\ \alpha\,\mathsf{U}\,\beta,\ \alpha\,\mathsf{R}\,\beta$), literals ($p,\ \neg p$), `true`, `false`
- $S_{\text{init}} = \phi$!!!
- $\sigma : S \times \Sigma \to \text{Bool}^+(S)$

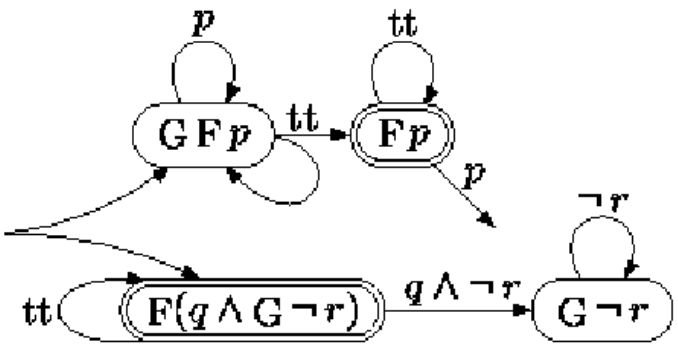
$$
\begin{array}{lcl}
\sigma(p, A) & = & \text{accepts, if } p \in A \text{ (otherwise rejects)} \\
\sigma(\neg p, A) & = & \text{accepts, if } p \notin A \text{ (otherwise rejects)} \\
\sigma(\texttt{true}, A) & = & \text{accepts} \\
\sigma(\texttt{false}, A) & = & \text{rejects} \\
\sigma(\mathsf{X}\,\alpha, A) & = & \alpha \qquad \text{!!!} \\
\sigma(\alpha\,\mathsf{U}\,\beta, A) & = & \sigma(\beta, A) \ \vee \ (\sigma(\alpha, A) \ \wedge \ \alpha\,\mathsf{U}\,\beta) \\
\sigma(\alpha\,\mathsf{R}\,\beta, A) & = & \sigma(\beta, A) \ \wedge \ (\sigma(\alpha, A) \ \vee \ \alpha\,\mathsf{R}\,\beta)
\end{array}
$$

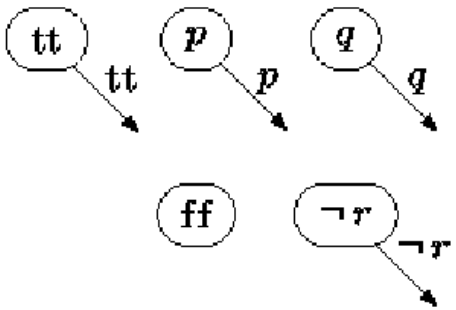
$$
\begin{array}{l}
\sigma(\mathsf{F}\,\alpha, A) = \sigma(\alpha, A) \ \vee \ \mathsf{F}\,\alpha \\
\sigma(\mathsf{G}\,\alpha, A) = \sigma(\alpha, A) \ \wedge \ \mathsf{G}\,\alpha
\end{array}
$$

LTL $\mapsto$ ABA (example)

$$\phi = \neg(\mathsf{G}\,\mathsf{F}\,p \implies \mathsf{G}\,(q \implies \mathsf{F}\,r)) \equiv \mathsf{G}\,\mathsf{F}\,p \wedge \mathsf{F}\,(q \wedge \mathsf{G}\,\neg r)$$

$\sigma(p, A)$	=	accepts, if $p \in A$ (otherwise rejects)
$\sigma(\neg p, A)$	=	accepts, if $p \notin A$ (otherwise rejects)
$\sigma(\mathtt{true}, A)$	=	accepts
$\sigma(\mathtt{false}, A)$	=	rejects
$\sigma(\mathsf{F}\,\alpha, A)$	=	$\sigma(\alpha, A) \vee \mathsf{F}\,\alpha$
$\sigma(\mathsf{G}\,\alpha, A)$	=	$\sigma(\alpha, A) \wedge \mathsf{G}\,\alpha$
$\sigma(\mathsf{GF}\,\alpha, A)$	=	$(\sigma(\alpha, A) \vee \mathsf{F}\,\alpha) \wedge \mathsf{GF}\,\alpha$

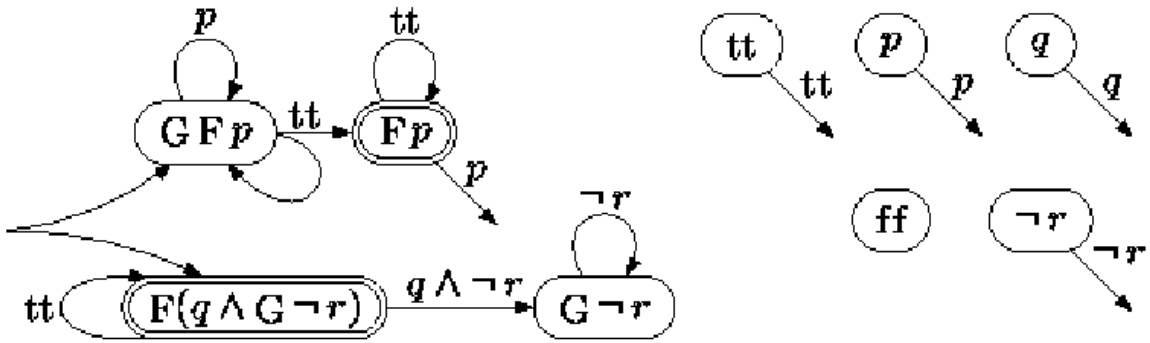


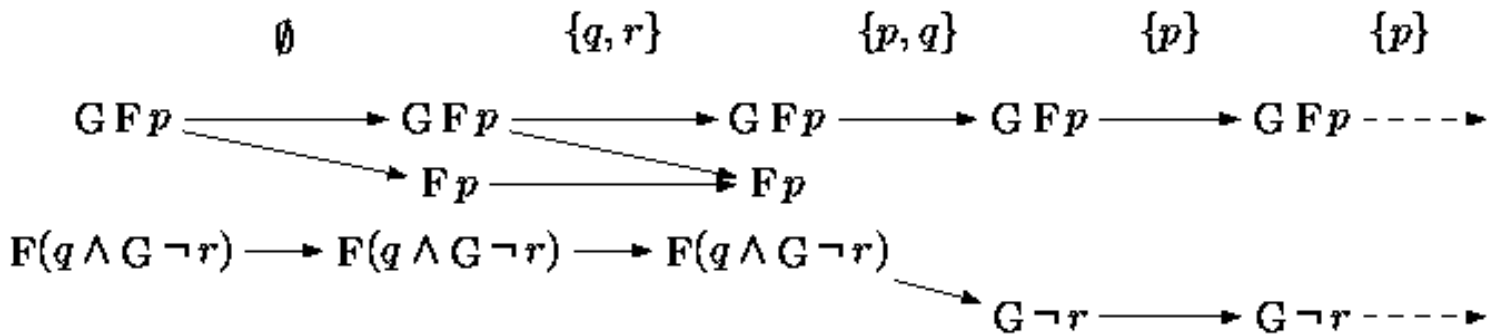


[Gastin,Oddoux 2001]

LTL $\mapsto$ ABA (example)

$$\phi = \neg(\mathsf{G}\,\mathsf{F}\,p \implies \mathsf{G}(q \implies \mathsf{F}\,r)) \equiv \mathsf{G}\,\mathsf{F}\,p \wedge \mathsf{F}(q \wedge \mathsf{G}\,\neg r)$$





[Gastin,Oddoux 2001]

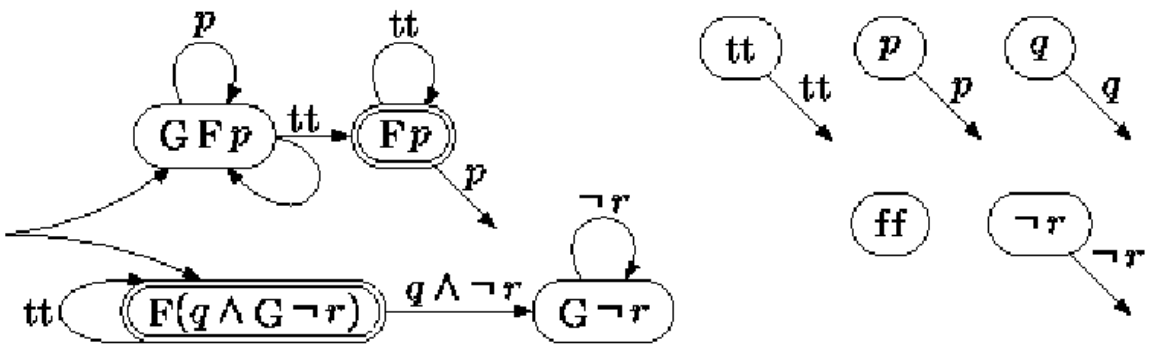
LTL $\mapsto$ ABA (2)

ABA $\mathcal{A}_\phi = \langle \Sigma, S, S_{\text{init}}, \sigma, F \rangle$:

- S = modal subformulas ($\mathsf{X}\,\alpha,\ \alpha\,\mathsf{U}\,\beta,\ \alpha\,\mathsf{R}\,\beta$), literals ($p,\ \neg p$), `true`, `false`
- $S_{\text{init}} = \phi$
- $\sigma : S \times \Sigma \to \text{Bool}^+(S)$

  ...

- $F = \{\alpha\,\mathsf{R}\,\beta\}$



LTL $\mapsto$ GBA vs LTL $\mapsto$ ABA

$$\theta_n = \neg((\mathsf{G}\,\mathsf{F}\,p_1 \wedge \ldots \wedge \mathsf{G}\,\mathsf{F}\,p_n) \Longrightarrow \mathsf{G}(q \Longrightarrow \mathsf{F}\,r))$$

	Spin		Wring		EQLTL	LTL2BA–		LTL2BA	
	time	space	time	space	time	time	space	time	space
θ_1	0.18	460	0.56	4,100	16	0.01	9	0.01	9
θ_2	4.6	4,200	2.6	4,100	16	0.01	19	0.01	11
θ_3	170	52,000	16	4,200	18	0.01	86	0.01	19
θ_4	9,600	970,000	110	4,700	25	0.07	336	0.06	38
θ_5			1,000	6,500	135	0.70	1,600	0.37	48
θ_6			8,400	13,000	N/A	12	8,300	4.0	88
θ_7			72,000†	43,000†		220	44,000	32	175
θ_8						4,200	260,000	360	250
θ_9						97,000	1,600,000	3,000	490
θ_{10}								36,000	970

[Gastin,Oddoux 2001]

LTL and ω-automata