CS 228 : Logic in Computer Science

Krishna. S

Recap and now

- LTL modelchecking
- Complexity of LTL modelchecking : later
- Satisfiability of LTL : start today

GNBA

- Generalized NBA, a variant of NBA
- Only difference is in acceptance condition
- Acceptance condition in GNBA is a set $\mathcal{F} = \{F_1, \ldots, F_k\}$, each $F_i \subseteq Q$
- An infinite run ρ is accepting in a GNBA iff

$$\forall F_i \in \mathcal{F}, \mathit{Inf}(\rho) \cap F_i \neq \emptyset$$

- Note that when $\mathcal{F} = \emptyset$, all infinite runs are accepting
- GNBA and NBA are equivalent in expressive power.

LTL to GNBA

- Given φ, consider all possible subformulae of φ, their negations

LTL to GNBA

- Given φ, consider all possible subformulae of φ, their negations
- Each state *s* of the automaton constructed gives some guarantees about the truth of some subformulae

LTL to GNBA

- Given φ, consider all possible subformulae of φ, their negations
- Each state *s* of the automaton constructed gives some guarantees about the truth of some subformulae
- The initial states give guarantees about the truth of φ

LTL to GNBA

- Given φ, consider all possible subformulae of φ, their negations
- Each state *s* of the automaton constructed gives some guarantees about the truth of some subformulae
- The initial states give guarantees about the truth of φ
  - Identify states of A_φ with various sets of subformulae of φ
  - Think of this as some labelling of the states
  - If B is a label for state s, and if $B = \{\varphi_1, \psi_1, \neg a\}$, then every infinite accepted string w starting at state s is such that $w \models \varphi_1, \psi_1, \neg a$.
  - The initial state(s) of A_φ must be such that all accepting paths beginning from them satisfy φ

LTL to GNBA

- Let $\varphi = \bigcirc a$.
- Subformulae of φ : $\{a, \bigcirc a\}$. Let $B = \{a, \bigcirc a, \neg a, \neg \bigcirc a\}$.
- Possibilities at each state : some consistent subset of B holds
  - $\{a, \bigcirc a\}$
  - $\{\neg a, \bigcirc a\}$
  - $\{a, \neg \bigcirc a\}$
  - $\{\neg a, \neg \bigcirc a\}$
- Our initial state(s) must guarantee truth of $\bigcirc a$. Thus, initial states: $\{a, \bigcirc a\}$ and $\{\neg a, \bigcirc a\}$

LTL to GNBA

$\{a, \bigcirc a\}$

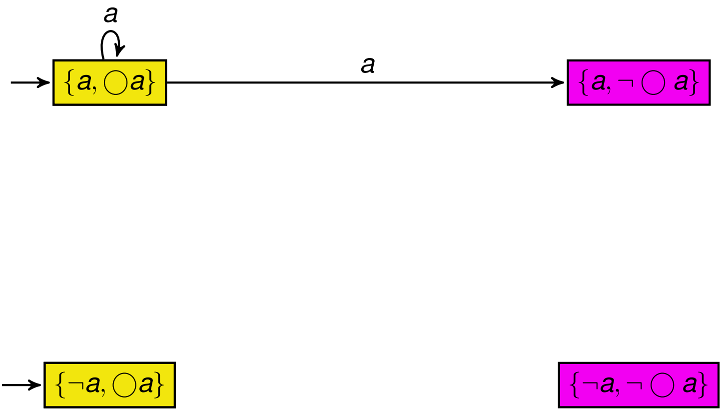
$\{a, \neg \bigcirc a\}$

$\{\neg a, \bigcirc a\}$

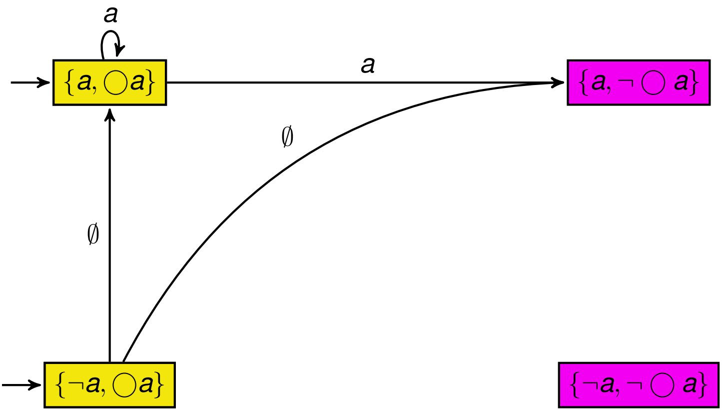
$\{\neg a, \neg \bigcirc a\}$

LTL to GNBA

LTL to GNBA

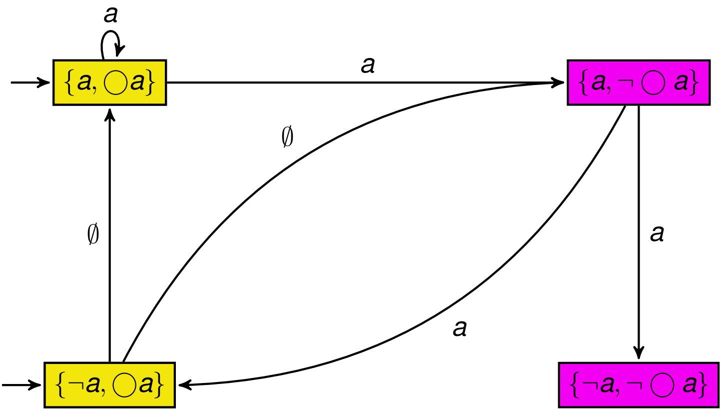

$\{a, \bigcirc a\}$
a
a
$\{a, \neg \bigcirc a\}$
$\{\neg a, \bigcirc a\}$
$\{\neg a, \neg \bigcirc a\}$

LTL to GNBA



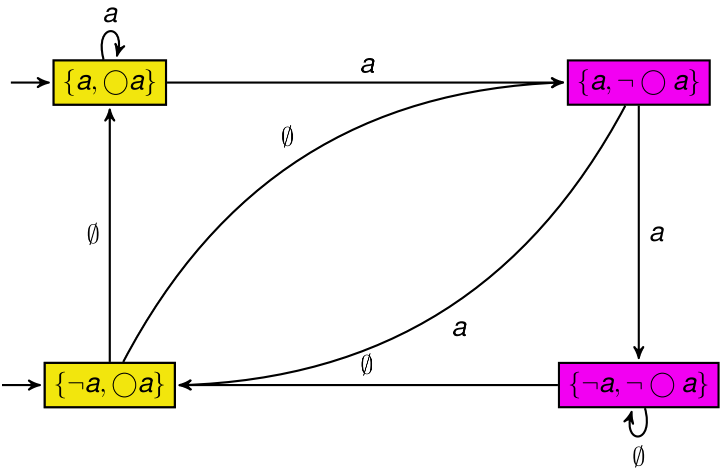
a
a
$\{a, \bigcirc a\}$
$\{a, \neg \bigcirc a\}$
$\emptyset$
$\emptyset$
$\{\neg a, \bigcirc a\}$
$\{\neg a, \neg \bigcirc a\}$

LTL to GNBA



a
$\{a, \bigcirc a\}$
a
$\{a, \neg \bigcirc a\}$
$\emptyset$
$\emptyset$
a
a
$\{\neg a, \bigcirc a\}$
$\{\neg a, \neg \bigcirc a\}$

LTL to GNBA



a
$\{a, \bigcirc a\}$
a
$\{a, \neg \bigcirc a\}$
$\emptyset$
$\emptyset$
a
a
$\emptyset$
$\{\neg a, \bigcirc a\}$
$\{\neg a, \neg \bigcirc a\}$
$\emptyset$

LTL to GNBA

- Claim : Runs from a state labelled set B indeed satisfy B
- No good states. All strings accepted.

LTL to GNBA

- Let $\varphi = a \,\mathsf{U} b$.
- Subformulae of φ : $\{a, b, a \,\mathsf{U} b\}$. Let $B = \{a, \neg a, b, \neg b, a \,\mathsf{U} b, \neg(a \,\mathsf{U} b)\}$.
- Possibilities at each state : some consistent subset of B holds
  - $\{a, \neg b, a \,\mathsf{U} b\}$
  - $\{\neg a, b, a \,\mathsf{U} b\}$
  - $\{a, b, a \,\mathsf{U} b\}$
  - $\{a, \neg b, \neg(a \,\mathsf{U} b)\}$
  - $\{\neg a, \neg b, \neg(a \,\mathsf{U} b)\}$
- Our initial state(s) must guarantee truth of $a \,\mathsf{U} b$. Thus, initial states: $\{a, b, a \,\mathsf{U} b\}$ and $\{\neg a, b, a \,\mathsf{U} b\}$ and $\{a, \neg b, a \,\mathsf{U} b\}$.

LTL to GNBA

$\{a, b, a \,\mathsf{U}\, b\}$

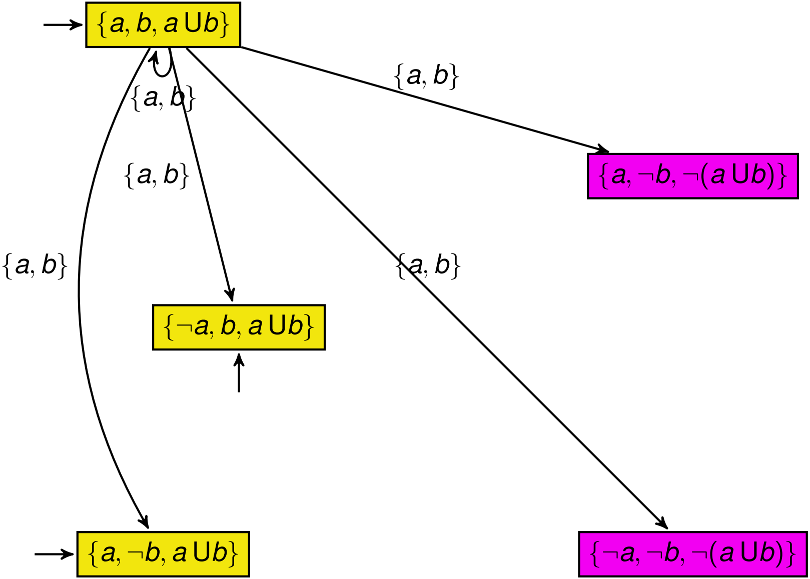
$\{a, \neg b, \neg(a \,\mathsf{U}\, b)\}$

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

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

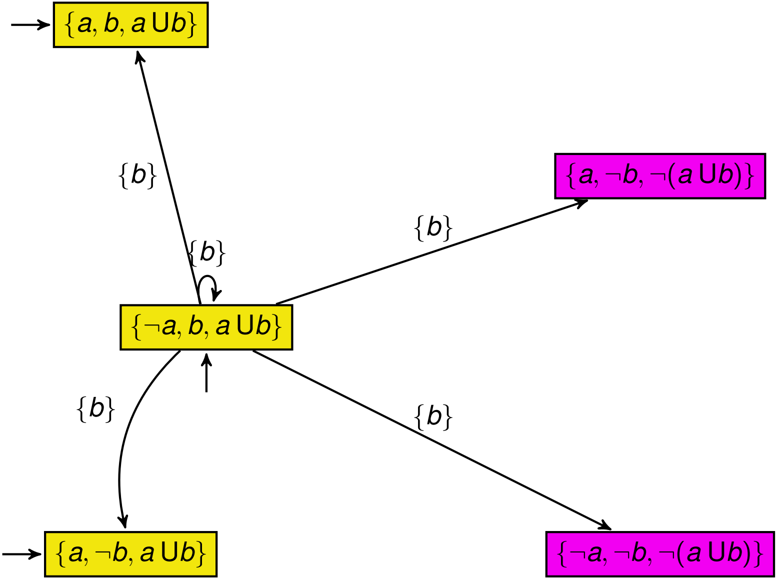
$\{\neg a, \neg b, \neg(a \,\mathsf{U}\, b)\}$

LTL to GNBA

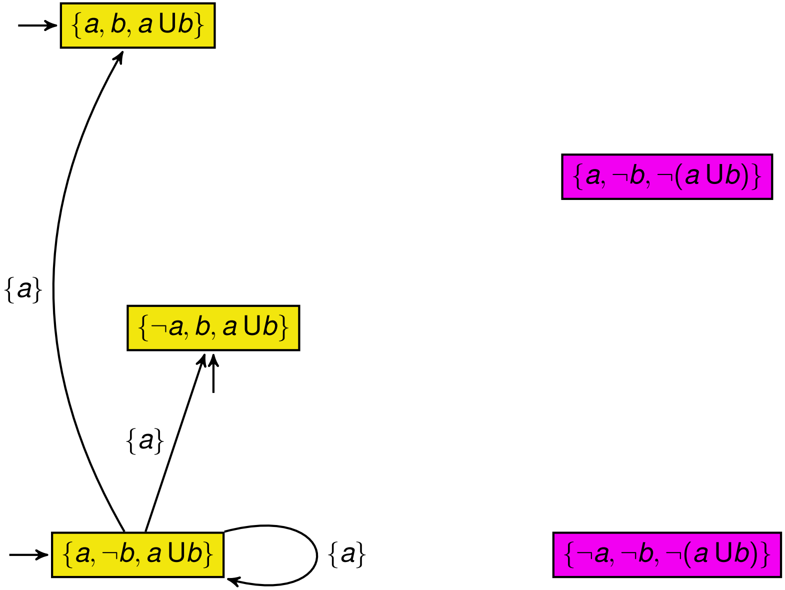


$\{a, b, a \,\mathsf{U}\, b\}$
$\{a, b\}$
$\{a, b\}$
$\{a, b\}$
$\{a, \neg b, \neg(a \,\mathsf{U}\, b)\}$
$\{a, b\}$
$\{a, b\}$
$\{\neg a, b, a \,\mathsf{U}\, b\}$
$\{a, \neg b, a \,\mathsf{U}\, b\}$
$\{\neg a, \neg b, \neg(a \,\mathsf{U}\, b)\}$

LTL to GNBA

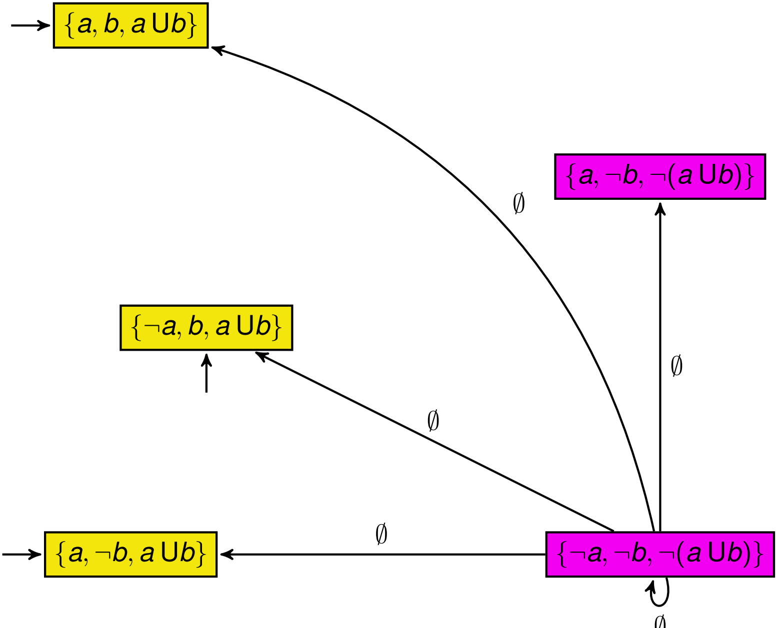

$\{a, b, a \mathsf{U} b\}$
$\{b\}$
$\{a, \neg b, \neg(a \mathsf{U} b)\}$
$\{b\}$
$\{b\}$
$\{\neg a, b, a \mathsf{U} b\}$
$\{b\}$
$\{b\}$
$\{a, \neg b, a \mathsf{U} b\}$
$\{\neg a, \neg b, \neg(a \mathsf{U} b)\}$

LTL to GNBA



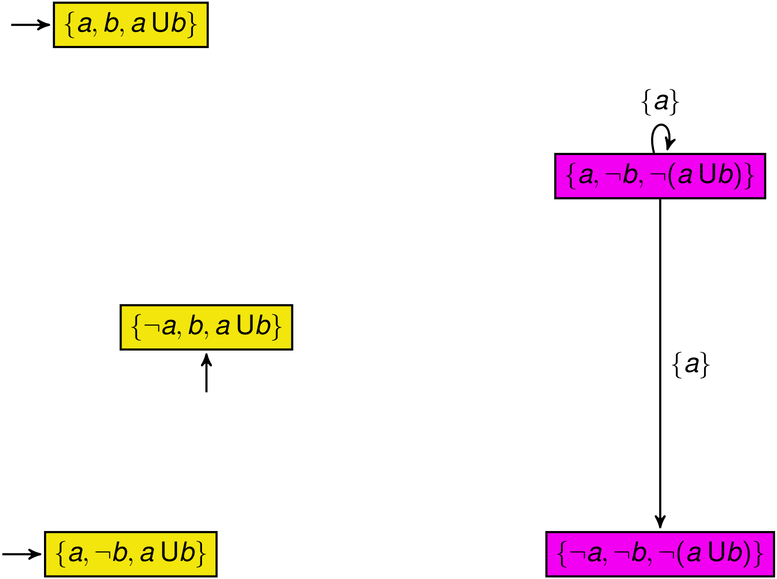
$\{a, b, a\,\mathsf{U}\,b\}$
$\{a, \neg b, \neg(a\,\mathsf{U}\,b)\}$
$\{a\}$
$\{\neg a, b, a\,\mathsf{U}\,b\}$
$\{a\}$
$\{a, \neg b, a\,\mathsf{U}\,b\}$
$\{a\}$
$\{\neg a, \neg b, \neg(a\,\mathsf{U}\,b)\}$

LTL to GNBA



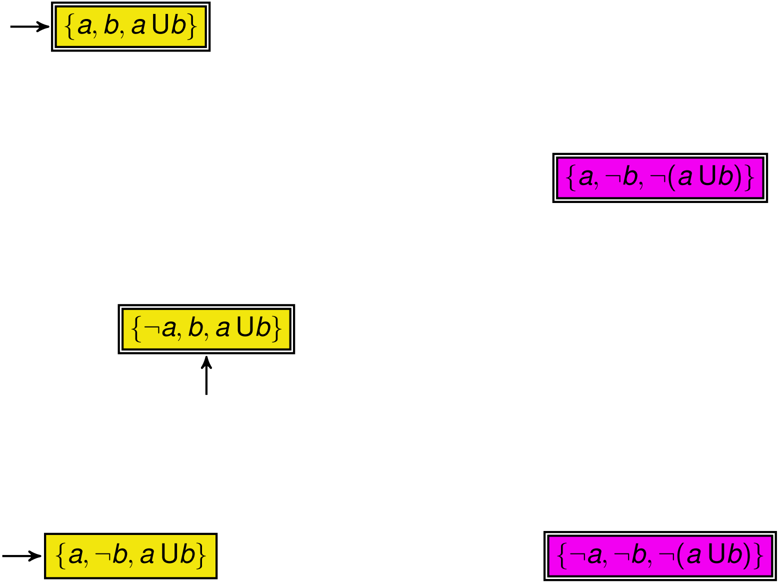
$\{a, b, a \,\mathsf{U}\, b\}$
$\{a, \neg b, \neg(a \,\mathsf{U}\, b)\}$
$\{\neg a, b, a \,\mathsf{U}\, b\}$
$\{a, \neg b, a \,\mathsf{U}\, b\}$
$\{\neg a, \neg b, \neg(a \,\mathsf{U}\, b)\}$
$\emptyset$
$\emptyset$
$\emptyset$
$\emptyset$
$\emptyset$

LTL to GNBA



$\{a, b, a\,\mathsf{U}\,b\}$
$\{a\}$
$\{a, \neg b, \neg(a\,\mathsf{U}\,b)\}$
$\{\neg a, b, a\,\mathsf{U}\,b\}$
$\{a\}$
$\{a, \neg b, a\,\mathsf{U}\,b\}$
$\{\neg a, \neg b, \neg(a\,\mathsf{U}\,b)\}$

LTL to GNBA : Accepting States



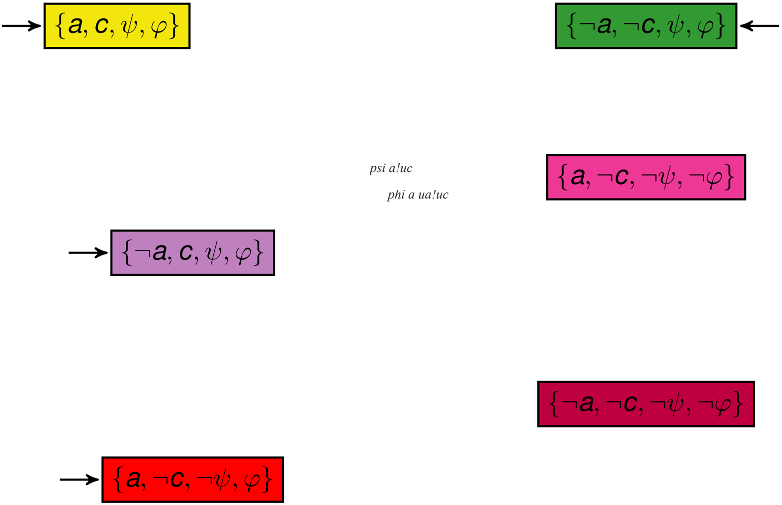
Do It Yourself

- Construct GNBA for $\neg(a \,\mathsf{U} b)$.
- Construct GNBA for $\bigcirc a \,\mathsf{U} b$
- Construct GNBA for $\bigcirc(a \,\mathsf{U} \bigcirc b)$
- Construct GNBA for $\bigcirc(\bigcirc\neg a \,\mathsf{U} \bigcirc (\neg \bigcirc b))$

LTL to GNBA

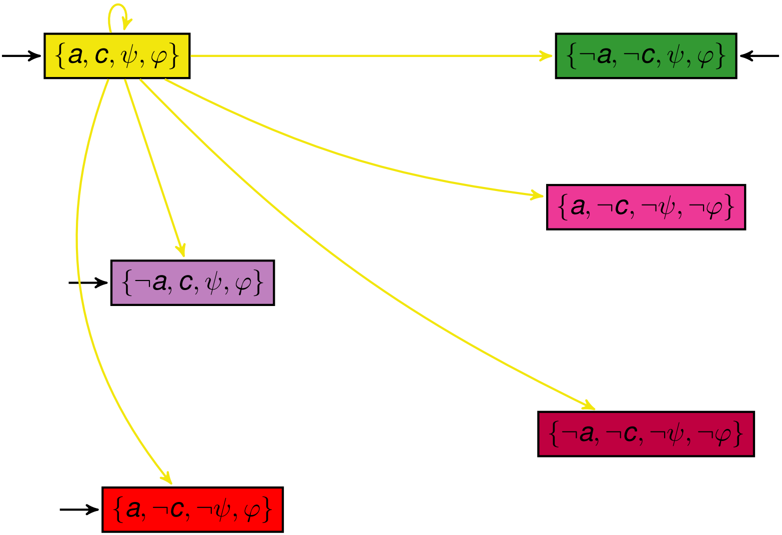
- Let $\varphi = a\,\mathsf{U}(\neg a\,\mathsf{U}c)$. Let $\psi = \neg a\,\mathsf{U}c$
- Subformulae of φ : $\{a, \neg a, c, \psi, \varphi\}$. Let $B = \{a, \neg a, c, \neg c, \psi, \neg\psi, \varphi, \neg\varphi\}$.
- Possibilities at each state : some consistent subset of B holds
  - $\{a, c, \psi, \varphi\}$
  - $\{\neg a, c, \psi, \varphi\}$
  - $\{a, \neg c, \neg\psi, \varphi\}$
  - $\{a, \neg c, \neg\psi, \neg\varphi\}$
  - $\{\neg a, \neg c, \psi, \varphi\}$
  - $\{\neg a, \neg c, \neg\psi, \neg\varphi\}$

LTL to GNBA



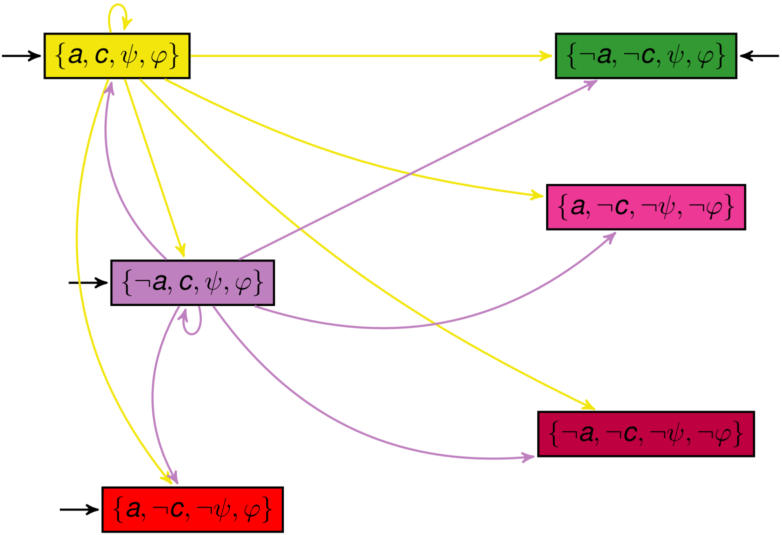
$\{a, c, \psi, \varphi\}$
$\{\neg a, \neg c, \psi, \varphi\}$
psi a!uc
phi a ua!uc
$\{a, \neg c, \neg\psi, \neg\varphi\}$
$\{\neg a, c, \psi, \varphi\}$
$\{\neg a, \neg c, \neg\psi, \neg\varphi\}$
$\{a, \neg c, \neg\psi, \varphi\}$

LTL to GNBA

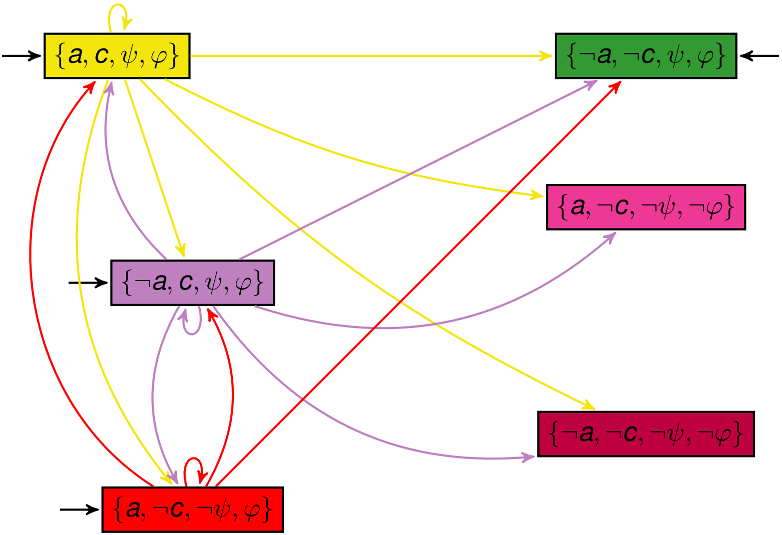


$\{a, c, \psi, \varphi\}$
$\{\neg a, \neg c, \psi, \varphi\}$
$\{a, \neg c, \neg\psi, \neg\varphi\}$
$\{\neg a, c, \psi, \varphi\}$
$\{\neg a, \neg c, \neg\psi, \neg\varphi\}$
$\{a, \neg c, \neg\psi, \varphi\}$

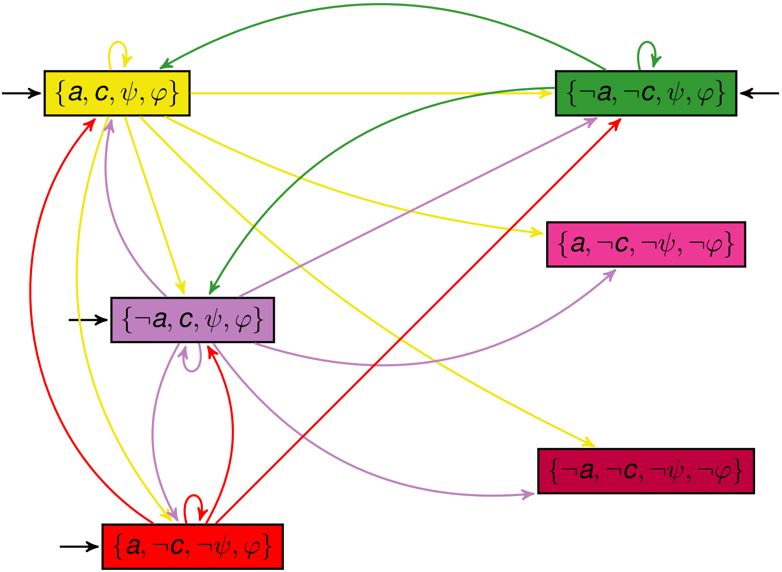
LTL to GNBA


$\{a, c, \psi, \varphi\}$
$\{\neg a, \neg c, \psi, \varphi\}$
$\{a, \neg c, \neg\psi, \neg\varphi\}$
$\{\neg a, c, \psi, \varphi\}$
$\{\neg a, \neg c, \neg\psi, \neg\varphi\}$
$\{a, \neg c, \neg\psi, \varphi\}$

LTL to GNBA

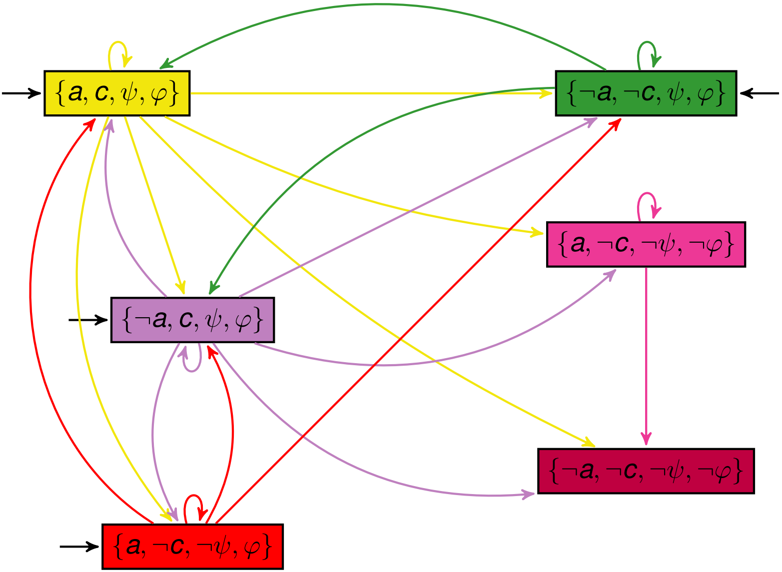

$\{a, c, \psi, \varphi\}$
$\{\neg a, \neg c, \psi, \varphi\}$
$\{a, \neg c, \neg\psi, \neg\varphi\}$
$\{\neg a, c, \psi, \varphi\}$
$\{\neg a, \neg c, \neg\psi, \neg\varphi\}$
$\{a, \neg c, \neg\psi, \varphi\}$

LTL to GNBA



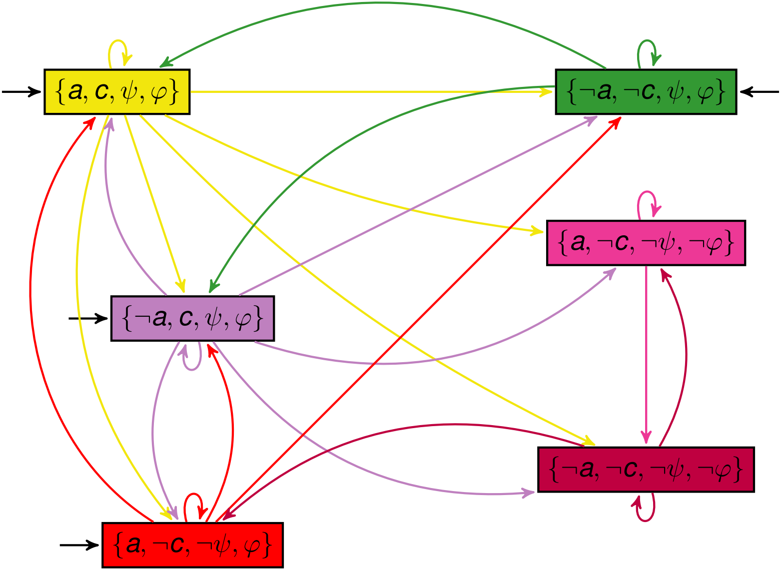
$\{a, c, \psi, \varphi\}$
$\{\neg a, \neg c, \psi, \varphi\}$
$\{a, \neg c, \neg\psi, \neg\varphi\}$
$\{\neg a, c, \psi, \varphi\}$
$\{\neg a, \neg c, \neg\psi, \neg\varphi\}$
$\{a, \neg c, \neg\psi, \varphi\}$

LTL to GNBA



$\{a, c, \psi, \varphi\}$
$\{\neg a, \neg c, \psi, \varphi\}$
$\{a, \neg c, \neg\psi, \neg\varphi\}$
$\{\neg a, c, \psi, \varphi\}$
$\{\neg a, \neg c, \neg\psi, \neg\varphi\}$
$\{a, \neg c, \neg\psi, \varphi\}$

LTL to GNBA



$\{a, c, \psi, \varphi\}$
$\{\neg a, \neg c, \psi, \varphi\}$
$\{a, \neg c, \neg\psi, \neg\varphi\}$
$\{\neg a, c, \psi, \varphi\}$
$\{\neg a, \neg c, \neg\psi, \neg\varphi\}$
$\{a, \neg c, \neg\psi, \varphi\}$

GNBA Acceptance Condition

- $\psi = \neg a \, \mathsf{U} c$
- $\varphi = a \, \mathsf{U} \psi$
- $F_1 = \{B \mid \psi \in B \to c \in B\}$
- $F_2 = \{B \mid \varphi \in B \to \psi \in B\}$
- $\mathcal{F} = \{F_1, F_2\}$

Final States

$\rightarrow$ $\{a, c, \psi, \varphi\} \in F_1, F_2$

$\{\neg a, \neg c, \psi, \varphi\} \in F_1$ $\leftarrow$

$\{a, \neg c, \neg\psi, \neg\varphi\} \in F_1, F_2$

$\rightarrow$ $\{\neg a, c, \psi, \varphi\} \in F_1, F_2$

$\{\neg a, \neg c, \neg\psi, \neg\varphi\} \in F_1, F_2$

$\rightarrow$ $\{a, \neg c, \neg\psi, \varphi\} \in F_2$

Putting Together

- Given φ, build $Cl(\varphi)$, the set of all subformulae of φ and their negations

Putting Together

- Given φ, build $Cl(\varphi)$, the set of all subformulae of φ and their negations
- Consider those $B \subseteq Cl(\varphi)$ which are consistent
  - $\varphi_1 \wedge \varphi_2 \in B \leftrightarrow \varphi_1 \in B$ and $\varphi_2 \in B$

Putting Together

- Given φ, build $Cl(\varphi)$, the set of all subformulae of φ and their negations
- Consider those $B \subseteq Cl(\varphi)$ which are consistent
  - $\varphi_1 \wedge \varphi_2 \in B \leftrightarrow \varphi_1 \in B$ and $\varphi_2 \in B$
  - $\psi \in B \rightarrow \neg\psi \notin B$ and $\psi \notin B \rightarrow \neg\psi \in B$

Putting Together

- Given φ, build $Cl(\varphi)$, the set of all subformulae of φ and their negations
- Consider those $B \subseteq Cl(\varphi)$ which are consistent
  - $\varphi_1 \wedge \varphi_2 \in B \leftrightarrow \varphi_1 \in B$ and $\varphi_2 \in B$
  - $\psi \in B \to \neg\psi \notin B$ and $\psi \notin B \to \neg\psi \in B$
  - Whenever $\psi_1 \, \mathsf{U} \psi_2 \in Cl(\varphi)$,
    - $\psi_2 \in B \to \psi_1 \, \mathsf{U} \psi_2 \in B$
    - $\psi_1 \, \mathsf{U} \psi_2 \in B$ and $\psi_2 \notin B \to \psi_1 \in B$

Putting Together

Given φ over AP, construct $A_\varphi = (Q, 2^{AP}, \delta, Q_0, \mathcal{F})$,

- $Q = \{B \mid B \subseteq Cl(\varphi)$ is consistent $\}$
- $Q_0 = \{B \mid \varphi \in B\}$
- $\delta : Q \times 2^{AP} \rightarrow 2^Q$ is such that

Putting Together

Given φ over AP, construct $A_\varphi = (Q, 2^{AP}, \delta, Q_0, \mathcal{F})$,

- $Q = \{B \mid B \subseteq Cl(\varphi)$ is consistent $\}$
- $Q_0 = \{B \mid \varphi \in B\}$
- $\delta : Q \times 2^{AP} \to 2^Q$ is such that
  - For $C = B \cap AP$, $\delta(B, C)$ is enabled and is defined as :
  - If $\bigcirc\psi \in Cl(\varphi)$, $\bigcirc\psi \in B$ iff $\psi \in \delta(B, C)$
  - If $\varphi_1 \mathsf{U} \varphi_2 \in Cl(\varphi)$,
    $\varphi_1 \mathsf{U} \varphi_2 \in B$ iff $(\varphi_2 \in B \vee (\varphi_1 \in B \wedge \varphi_1 \mathsf{U} \varphi_2 \in \delta(B, C)))$

Putting Together

Given φ over AP, construct $A_\varphi = (Q, 2^{AP}, \delta, Q_0, \mathcal{F})$,

- $Q = \{B \mid B \subseteq Cl(\varphi) \text{ is consistent } \}$
- $Q_0 = \{B \mid \varphi \in B\}$
- $\delta : Q \times 2^{AP} \rightarrow 2^Q$ is such that
  - For $C = B \cap AP$, $\delta(B, C)$ is enabled and is defined as :
  - If $\bigcirc\psi \in Cl(\varphi)$, $\bigcirc\psi \in B$ iff $\psi \in \delta(B, C)$
  - If $\varphi_1 \mathsf{U} \varphi_2 \in Cl(\varphi)$,
    $\varphi_1 \mathsf{U} \varphi_2 \in B$ iff $(\varphi_2 \in B \vee (\varphi_1 \in B \wedge \varphi_1 \mathsf{U} \varphi_2 \in \delta(B, C)))$
- $\mathcal{F} = \{F_{\varphi_1 \mathsf{U} \varphi_2} \mid \varphi_1 \mathsf{U} \varphi_2 \in Cl(\varphi)\}$, with
  $F_{\varphi_1 \mathsf{U} \varphi_2} = \{B \in Q \mid \varphi_1 \mathsf{U} \varphi_2 \in B \rightarrow \varphi_2 \in B\}$

Putting Together

Given φ over AP, construct $A_\varphi = (Q, 2^{AP}, \delta, Q_0, \mathcal{F})$,

- $Q = \{B \mid B \subseteq Cl(\varphi)$ is consistent $\}$
- $Q_0 = \{B \mid \varphi \in B\}$
- $\delta : Q \times 2^{AP} \rightarrow 2^Q$ is such that
  - For $C = B \cap AP$, $\delta(B, C)$ is enabled and is defined as :
  - If $\bigcirc\psi \in Cl(\varphi)$, $\bigcirc\psi \in B$ iff $\psi \in \delta(B, C)$
  - If $\varphi_1 \mathsf{U} \varphi_2 \in Cl(\varphi)$,
    $\varphi_1 \mathsf{U} \varphi_2 \in B$ iff $(\varphi_2 \in B \vee (\varphi_1 \in B \wedge \varphi_1 \mathsf{U} \varphi_2 \in \delta(B, C)))$
- $\mathcal{F} = \{F_{\varphi_1 \mathsf{U} \varphi_2} \mid \varphi_1 \mathsf{U} \varphi_2 \in Cl(\varphi)\}$, with
  $F_{\varphi_1 \mathsf{U} \varphi_2} = \{B \in Q \mid \varphi_1 \mathsf{U} \varphi_2 \in B \rightarrow \varphi_2 \in B\}$
- Prove that $L(\varphi) = L(A_\varphi)$

GNBA Size

- States of A_φ are subsets of $Cl(\varphi)$

GNBA Size

- States of A_φ are subsets of $Cl(\varphi)$
- Maximum number of states $\leqslant 2^{|\varphi|}$

GNBA Size

- States of A_φ are subsets of $Cl(\varphi)$
- Maximum number of states $\leqslant 2^{|\varphi|}$
- Number of sets in $\mathcal{F} = |\varphi|$

GNBA Size

- States of A_φ are subsets of $Cl(\varphi)$
- Maximum number of states $\leqslant 2^{|\varphi|}$
- Number of sets in $\mathcal{F} = |\varphi|$
- LTL $\varphi \rightsquigarrow$ NBA A_φ : Number of states in $A_\varphi \leqslant |\varphi|.2^{|\varphi|}$
- Lower Bound : Find a family of LTL formulae φ_n such that the state space of $A_{\varphi_n} \geqslant |\varphi|.2^{|\varphi|}$

Complexity of LTL model checking

The hamiltonian path problem is polynomially reducible to the complement of the LTL modelchecking problem.

- Given graph $G = (V, E)$ synthesize in polynomial time a TS and an LTL formula φ
- Show that G has a HP iff $TS \not\models \varphi$.
- G does not have a HP iff $TS \models \varphi$.
- co-NP hardness of the model-checking problem.
  - Class co-NP=complement of NP.
  - Example: φ in DNF is valid iff $\neg\varphi$ in CNF is unsat.
  - Since CNF SAT is NP-complete, DNF valid is co-NP complete

Complexity of LTL model checking

- *TS* is the graph itself, with one new node added, say b s.t. all vertices of G have an edge to b, and b has a self loop. Let the label of a node in the TS be the name of the vertex.
- Write an LTL formula to capture absence of a HP in G. Assume $V = \{v_1, \ldots, v_n\}$.
- The formula $\varphi = \neg\psi$ where ψ is

$$(\Diamond v_1 \wedge \Box(v_1 \rightarrow \bigcirc\Box\neg v_1)) \wedge \ldots (\Diamond v_n \wedge \Box(v_n \rightarrow \bigcirc\Box\neg v_n))$$

- Show that G has a HP iff $TS \not\models \varphi$.

A Weak Lower Bound

Assume *TS* $\not\models \neg\psi$. Then there is a path witnessing ψ.

- Let π be the path in *TS* such that $\pi \models \psi$.

A Weak Lower Bound

Assume $TS \not\models \neg\psi$. Then there is a path witnessing ψ.

- Let π be the path in TS such that $\pi \models \psi$.
- As $\pi \models \bigwedge_{v \in V}(\Diamond v \wedge \Box(v \rightarrow \bigcirc\Box\neg v))$, π witnesses all vertices of V, and does not repeat any vertex.

A Weak Lower Bound

Assume $TS \not\models \neg\psi$. Then there is a path witnessing ψ.

- Let π be the path in TS such that $\pi \models \psi$.
- As $\pi \models \bigwedge_{v \in V}(\Diamond v \wedge \Box(v \to \bigcirc\Box\neg v))$, π witnesses all vertices of V, and does not repeat any vertex.
- π has the form $v_{i_1} v_{i_2} \ldots v_{i_n} b^\omega$, $i_1, \ldots, i_n \in \{1, 2, \ldots, n\}$, $i_j \neq i_k$.

A Weak Lower Bound

Assume $TS \not\models \neg\psi$. Then there is a path witnessing ψ.

- Let π be the path in TS such that $\pi \models \psi$.
- As $\pi \models \bigwedge_{v \in V}(\Diamond v \wedge \Box(v \rightarrow \bigcirc\Box\neg v))$, π witnesses all vertices of V, and does not repeat any vertex.
- π has the form $v_{i_1} v_{i_2} \dots v_{i_n} b^{\omega}$, $i_1, \dots, i_n \in \{1, 2, \dots, n\}$, $i_j \neq i_k$.
- So G has the HP $v_{i_1} v_{i_2} \dots v_{i_n}$.

A Weak Lower Bound

Assume $TS \not\models \neg\psi$. Then there is a path witnessing ψ.

- Let π be the path in TS such that $\pi \models \psi$.
- As $\pi \models \bigwedge_{v \in V}(\Diamond v \wedge \Box(v \to \bigcirc\Box\neg v))$, π witnesses all vertices of V, and does not repeat any vertex.
- π has the form $v_{i_1} v_{i_2} \ldots v_{i_n} b^\omega$, $i_1, \ldots, i_n \in \{1, 2, \ldots, n\}$, $i_j \neq i_k$.
- So G has the HP $v_{i_1} v_{i_2} \ldots v_{i_n}$.
- The converse is similar : a HP in G extends to a path $\pi = v_{i_1} v_{i_2} \ldots v_{i_n} b^\omega$ in TS. Clearly, $\pi \models \psi$.

A Weak Lower Bound

Assume $TS \not\models \neg\psi$. Then there is a path witnessing ψ.

- Let π be the path in TS such that $\pi \models \psi$.
- As $\pi \models \bigwedge_{v \in V}(\Diamond v \wedge \Box(v \rightarrow \bigcirc\Box\neg v))$, π witnesses all vertices of V, and does not repeat any vertex.
- π has the form $v_{i_1} v_{i_2} \dots v_{i_n} b^\omega$, $i_1, \dots, i_n \in \{1, 2, \dots, n\}$, $i_j \neq i_k$.
- So G has the HP $v_{i_1} v_{i_2} \dots v_{i_n}$.
- The converse is similar : a HP in G extends to a path $\pi = v_{i_1} v_{i_2} \dots v_{i_n} b^\omega$ in TS. Clearly, $\pi \models \psi$.
- So LTL model checking is co-NP hard as HP is NP-complete.
- Actual complexity of LTL model checking : PSPACE-complete. For this, show that given a LBTM M and a word w, construct in poly time a TS and an LTL formula φ such that M accepts w iff $TS \models \varphi$.