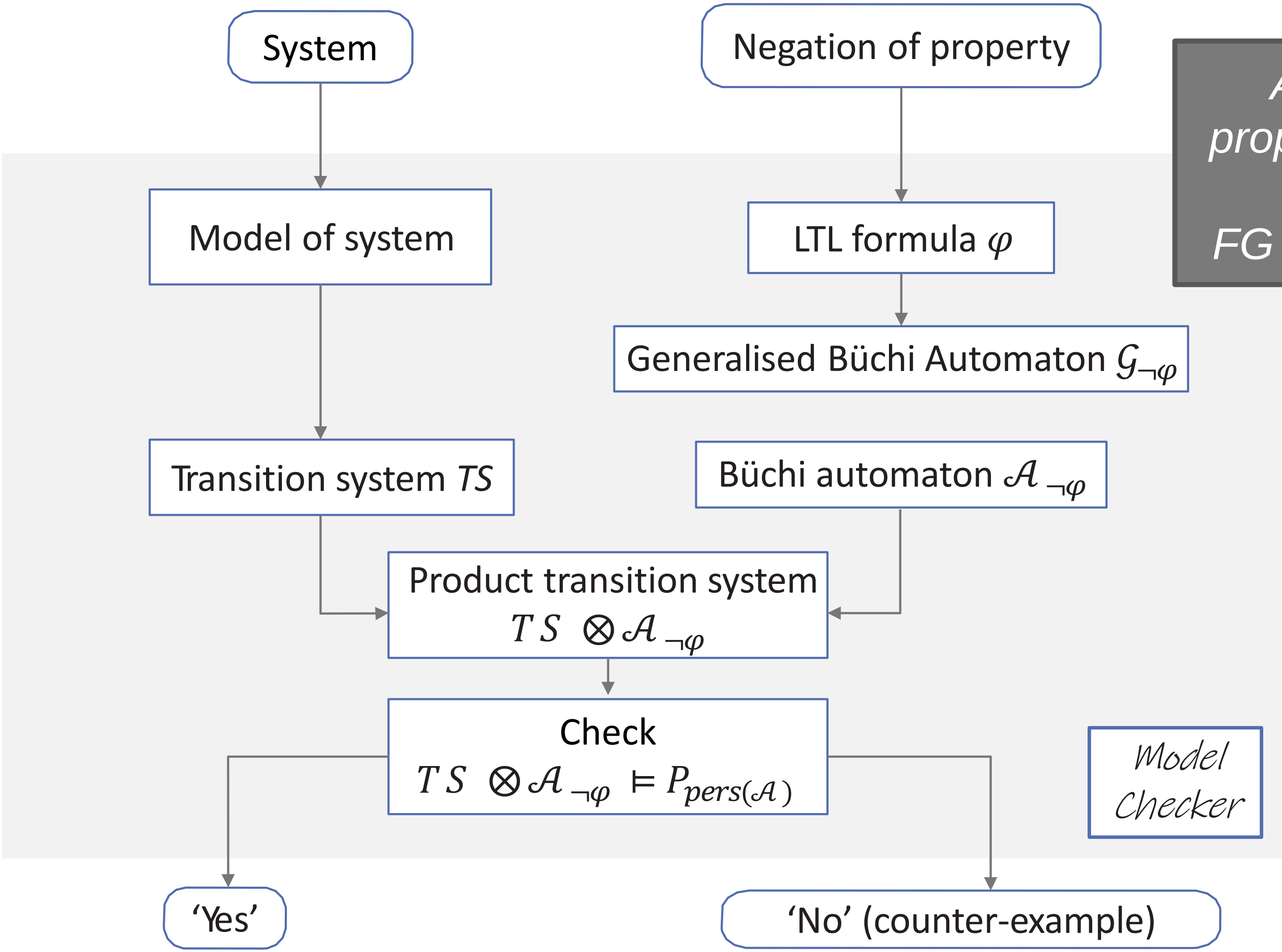
LTL Model Checking

FORMAL SYSTEMS (CS60030)

Pallab Dasgupta
Professor,
Dept. of Computer Sc & Engg

LTL Model Checking – An Overview



A persistence property for an NBA $\mathcal{A}$ is FG ("no final state")

Taking the Product : $\boxed{TS \otimes \mathcal{A}_\varphi}$

For a transitions system TS = (S, Act, →, I, AP, L), without terminal states, and a non-blocking NBA $\mathcal{A}$ =(Q, Σ, δ, Q_0, F) where $\Sigma = 2^{AP}$, let:

TS $\otimes \mathcal{A}$ = (S', Act, →', I', AP', L') where,

- S' = S X Q, AP' = Q, and L'(<s,q>) = {q}
- →' is the smallest relation defined by : $\dfrac{s \xrightarrow{\alpha} t \wedge q \xrightarrow{L(t)} p}{<s, q> \xrightarrow{\alpha}{}' <t, p>}$
- I' = $\{<s_0, q> \mid s_0 \in I \wedge \exists q_0 \in Q_0 . q_0 \xrightarrow{L(s_0)} q\}$

q is a state that is reached via a transition from some $q_0 \in \boldsymbol{Q_0}$ labeled with $L(s_0)$

From LTL to GNBAs

- For LTL property φ (for a transition system over AP), construct GNBA $\mathcal{G}_\varphi$ over 2^{AP} with $\mathcal{L}_\omega(\mathcal{G}_\varphi) = \boldsymbol{Words}(\varphi)$.
  - Assume φ contains operators $\wedge, \neg, \mathrm{O}, \mathrm{U}$.
  - States of the GNBA: *Elementary sets of sub-formulas in φ*
  - Transitions between states of the GNBA: *derived from the* O *and* U *operator expansion laws.*
  - Accept states guarantee that: $\hat{\sigma}$ is an accepting run in $\mathcal{G}_\varphi$ iff $\sigma \models \varphi$

over states of the GNBA (elementary sets)

over 2^{AP} for TS

Elementary Sets (the states of the GNBA) for φ

- For $\sigma = A_0 A_1 A_2 \ldots \in Words(\varphi)$, each $A_i \subseteq AP$.
- For each A_i we construct B_i (a set of sub-formula of φ), to obtain word $\hat{\sigma} = B_0 B_1 B_2 \ldots$ such that:
  - $\psi \in B_i$ "if and only if" $\sigma^i = A_i A_{i+1} A_{i+2} \ldots \vDash \psi$
    - What should the initial state of the GNBA contain in its elementary sets?
  - $\hat{\sigma}$ should be a run of the GNBA $\mathcal{G}_\varphi$ for a word σ.

Elementary Sets for φ : Computing Closure of φ

Closure.

- For an LTL-property φ, the set closure(φ) consists of:
  - All sub-formulas ψ of φ and their negation $\neg\psi$.
  - EXAMPLE: a U ($\neg$a $\wedge$ b)

Can we take B_i to be any subset of the closure(φ)?

NO!

They must be *"elementary" – consistent (logically and locally) & maximal.*

"Elementary" Sets for φ

The set B $\subseteq$ closure(φ) is elementary if:

1. B is logically consistent - if for all $\varphi_1 \wedge \varphi_2$, $\psi \in$ closure(φ):
   - $\varphi_1 \wedge \varphi_2 \in B \iff \varphi_1 \in B$ and $\varphi_2 \in B$
   - $\psi \in B \implies \neg\psi \notin B$
   - true $\in$ closure(φ) $\implies$ true $\in B$

2. B is locally consistent – if for all φ_1 U $\varphi_2 \in$ closure(φ):
   - $\varphi_2 \in B \implies \varphi_1 \text{ U } \varphi_2 \in B$
   - $\varphi_1 \text{ U } \varphi_2 \in B$ and $\varphi_2 \notin B \implies \varphi_1 \in B$

3. B is maximal – for all $\psi \in$ closure(φ):
   - $\psi \notin B \implies \neg\psi \in B$

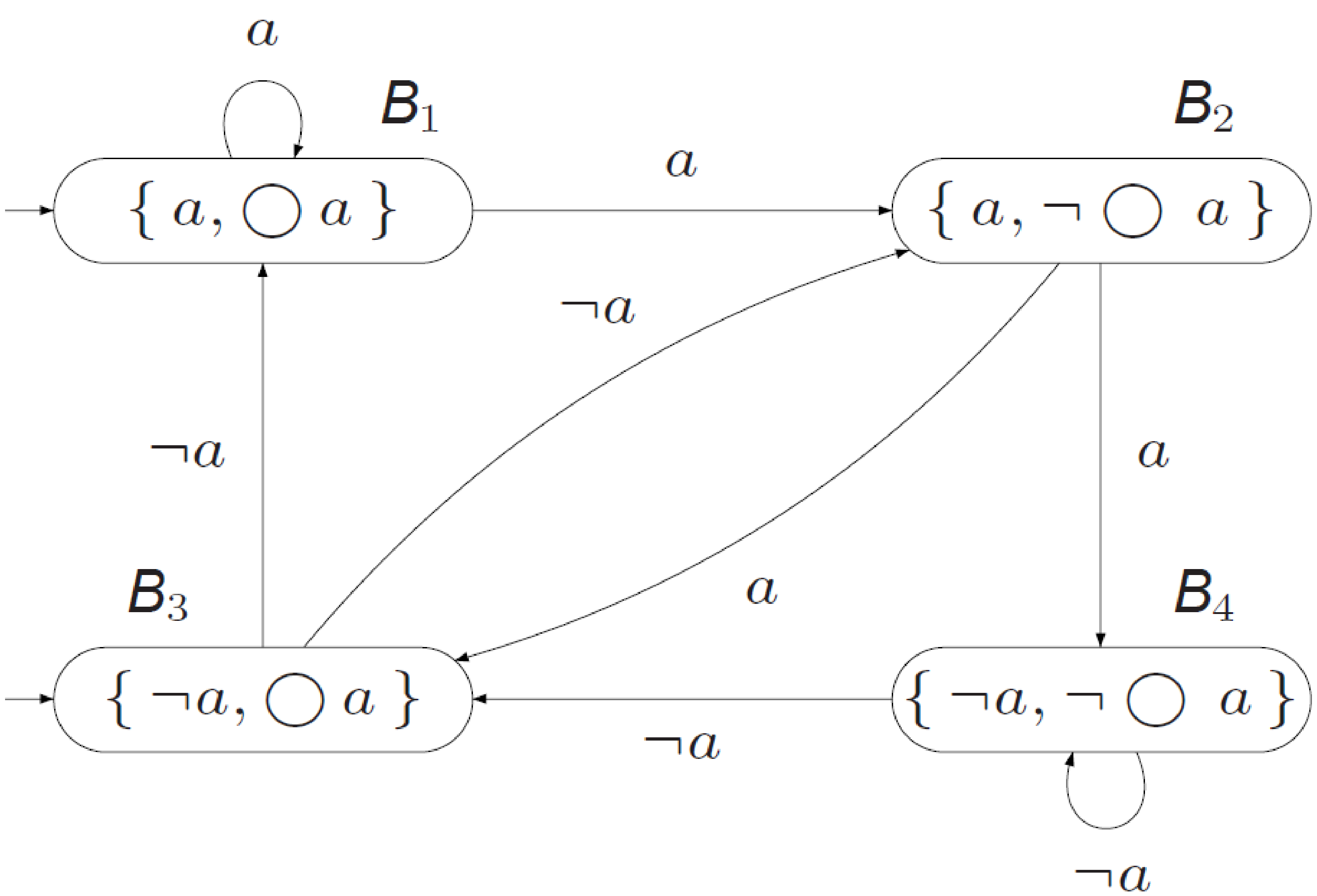
Examples:

The GNBA for the LTL-property φ

For the LTL-property φ, let $\mathcal{G}_\varphi$ = (Q, 2^{AP}, δ, Q_0, $\mathcal{F}$), where

- Q is the set of elementary sets of formulas B $\subseteq$ closure(φ).
  - $Q_0 = \{ B \in Q \mid \varphi \in B \}$
- $\mathcal{F} = \{ \{ B \in Q \mid \varphi_1 \, U \, \varphi_2 \notin B \text{ or } \varphi_2 \in B \} \mid \varphi_1 \, U \, \varphi_2 \in \text{closure}(\varphi) \}$
- The transition relation δ: Q x $2^{AP} \longrightarrow$ Q is given by:
  - $\delta(B, B \cap AP)$ is the set of all elementary sets of formulas B' satisfying:
    - For every $O\psi \in$ closure(φ) :
      $O\psi \in B \Leftrightarrow \psi \in B'$
      AND
    - For every $\varphi_1 \, U \, \varphi_2 \in$ closure(φ):
      $\varphi_1 \, U \, \varphi_2 \in B \Leftrightarrow (\varphi_2 \in B \vee (\varphi_1 \in B \wedge \varphi_1 \, U \, \varphi_2 \in B'))$

GNBA for $\varphi = \bigcirc a$



GNBA for φ = a U b