5. Linear Temporal Logic

Computer-Aided Verification

Dave Parker

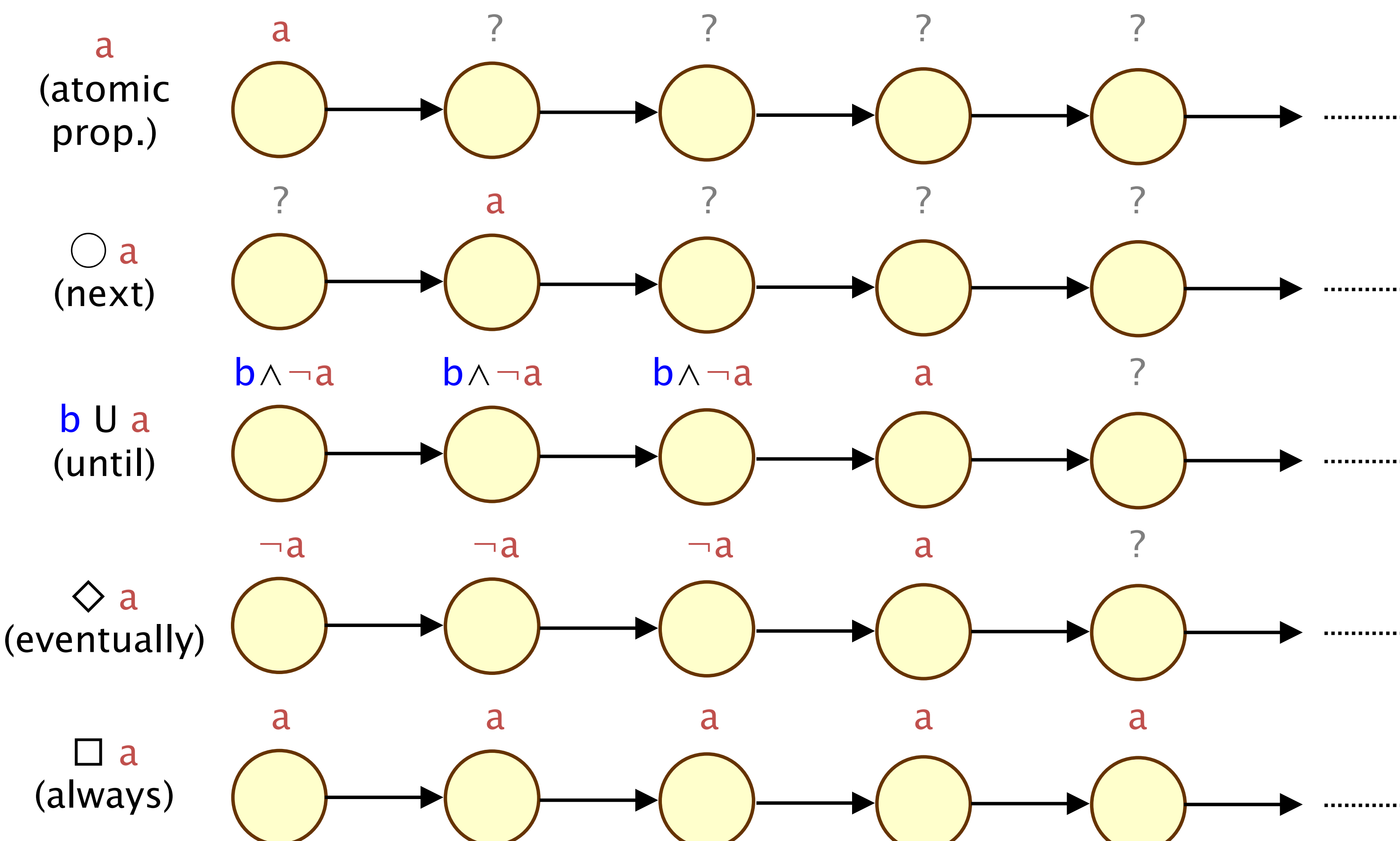
University of Birmingham

2016/17

Linear temporal logic (LTL)

- LTL formulae ψ are defined by the grammar:
  - $\psi ::= \text{true} \mid a \mid \psi \wedge \psi \mid \neg\psi \mid \bigcirc \psi \mid \psi \,\mathsf{U}\, \psi$
  - where $a \in AP$ is an atomic proposition
- Temporal operators: "next" ($\bigcirc$) and "until" (U)
  - $\bigcirc\, \psi$ means "ψ is true in the next state"
  - $\psi_1 \,\mathsf{U}\, \psi_2$ means "ψ_2 is true eventually and ψ_1 is true until then"
- Equivalences (in addition to false, $\vee$, $\rightarrow$, $\leftrightarrow$, $\oplus$)
  - "eventually ψ": $\Diamond\, \psi \equiv \text{true} \,\mathsf{U}\, \psi$
  - "always ψ": $\Box\, \psi \equiv \neg\Diamond(\neg\psi)$

LTL – Intuitive semantics



LTL

- Some simple examples:
- $\Box \neg(\text{critical}_1 \wedge \text{critical}_2)$
  - "the processes never enter the critical section simultaneously"
- $\Diamond$ end
  - "the program eventually terminates"
- $\neg$error U end
  - "the program terminates without any errors occurring"

- Alternative styles of syntax
  - $\bigcirc$ a $\equiv$ X a ("next")
  - $\Diamond$ a $\equiv$ F a ("future", "finally")
  - $\Box$ a $\equiv$ G a ("globally")

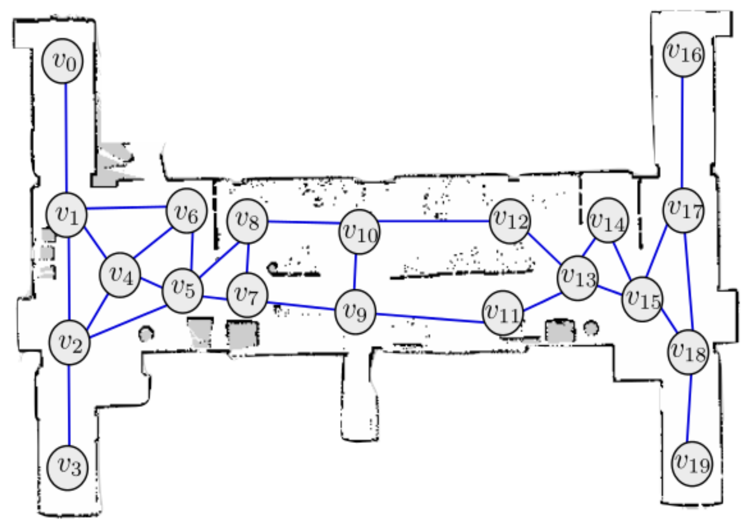
LTL – More properties

- LTL syntax:
  - ψ ::= true | a | $\psi \wedge \psi$ | $\neg\psi$ | $\bigcirc\, \psi$ | $\psi\ \mathsf{U}\ \psi$ | $\Diamond\, \psi$ | $\Box\, \psi$
  - many more properties formed by combining temporal operators
  - simple example: $\bigcirc \bigcirc a$

- $\Box(a \rightarrow \Diamond b)$
  - "b always follows a"
- $\Box(a \rightarrow \bigcirc b)$
  - "b always immediately follows a"
- $\Box \Diamond a$
  - "a is true infinitely often"
- $\Diamond \Box a$
  - "a becomes true and remains true forever"

Other uses of LTL

- Example: robot task specifications
  - $\neg zone_3 \; \mathrm{U} \; (zone_1 \wedge (\Diamond \; zone_4))$
    - visit zone 1 (without passing through zone 3), and then go to zone 4
  - $(\Box \neg zone_3) \wedge (\Box \; \Diamond \; zone_5)$
    - avoid zone 3 and patrol $zone_5$ infinitely often



LTL semantics

- Recall: we define properties in terms of:
  - infinite words $\sigma = A_0 A_1 A_2 A_3 \ldots$ over 2^{AP}
- Some notation:
  - $\sigma[j]$ is the (j+1)th symbol, i.e. A_j
  - $\sigma[j\ldots]$ is the suffix starting in $\sigma[j]$, i.e. $A_j A_{j+1} A_{j+2} \ldots$

- LTL semantics ($\sigma \vDash \psi$, for infinite word σ and LTL formula ψ)
  - $\sigma \vDash \mathit{true}$ always
  - $\sigma \vDash a \quad \Leftrightarrow \quad a \in \sigma[0]$
  - $\sigma \vDash \psi_1 \wedge \psi_2 \quad \Leftrightarrow \quad \sigma \vDash \psi_1$ and $\sigma \vDash \psi_2$
  - $\sigma \vDash \neg\psi \quad \Leftrightarrow \quad \sigma \nvDash \psi$
  - $\sigma \vDash \bigcirc \psi \quad \Leftrightarrow \quad \sigma[1\ldots] \vDash \psi$
  - $\sigma \vDash \psi_1 \,\mathsf{U}\, \psi_2 \quad \Leftrightarrow \quad \exists k \geq 0$ s.t. $\sigma[k\ldots] \vDash \psi_2$ and $\forall i<k \; \sigma[i\ldots] \vDash \psi_1$

LTL semantics

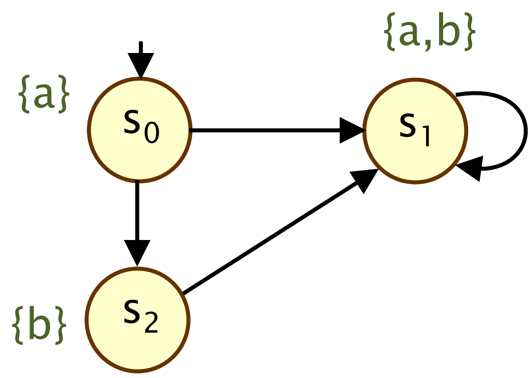
- When does an LTS M satisfy an LTL formula ψ?
  - intuitively, if all paths of M satisfy ψ
- More precisely:
  - if all traces of all paths of M satisfy ψ:
  - $M \models \psi \iff \sigma \models \psi$ for every $\sigma \in \mathrm{Traces}(M)$

    $\iff \mathrm{trace}(\pi) \models \psi$ for every $\pi \in \mathrm{Paths}(M)$
- Alternatively (using a linear-time property):
  - $\mathrm{Words}(\psi) = \{ \sigma \in (2^{AP})^\omega \mid \sigma \models \psi \}$
  - $M \models \psi \iff \mathrm{Traces}(M) \subseteq \mathrm{Words}(\psi)$

Examples

- $M \models \Box\,(a \vee b)$?
- $M \models b$?
- $M \models \bigcirc\, b$?
- $M \models \Box \bigcirc\, b$?
- $M \models \Box \Diamond \neg a$?
- $M \models \Box((a \wedge \neg b) \rightarrow \Diamond \neg b)$?

M:



What can we express in LTL?

- Invariants?
  - yes: $\Box\Phi$, for some propositional formula Φ
- Safety properties?
  - yes: e.g. $\Box(\text{receive} \rightarrow \bigcirc \text{ack})$
    - "ack always immediately follows receive"
- Liveness properties?
  - yes: e.g. $\Diamond\text{terminates}$
    - "the program eventually terminates"
  - yes: e.g. $\Box\Diamond\text{ready}$
    - "the server always gets back into a ready state"

Equivalence

- LTL formulae ψ_1 and ψ_2 are equivalent, written $\psi_1 \equiv \psi_2$ if:
  - they are satisfied by exactly the same traces
  - $\sigma \models \psi_1 \Leftrightarrow \sigma \models \psi_2$ (for any trace σ)
  - i.e. $\mathrm{Words}(\psi_1) = \mathrm{Words}(\psi_2)$

With respect to some set AP of propositions

- Or, equivalently:
  - if they are satisfied by exactly the same models
  - $M \models \psi_1 \Leftrightarrow M \models \psi_2$ (for any LTS M)

- This gives us a notion of expressiveness of LTL
  - "expressiveness" = "expressivity" = '"expressive power"
  - i.e. which models can LTL distinguish between?

LTL equivalences

- Equivalences
  - shorthand for common formulae, e.g.: $\Diamond\ \psi \equiv \text{true}\ U\ \psi$
  - simplifications, e.g.: $\neg\neg p \equiv p$
  - syntax vs. semantics

Does not add expressive power to LTL

- Equivalences for: propositional logic + temporal operators

- Temporal operator equivalences:
  - $\Box\psi \equiv \neg\Diamond\neg\psi$ (duality)
  - $\Box\Box\psi \equiv \Box\psi$ (idempotency)
  - $\Diamond\psi \equiv \psi \vee \bigcirc\Diamond\psi$ (expansion law)
  - $\Box(\psi_1 \wedge \psi_2) \equiv \Box\psi_1 \wedge \Box\psi_2$ (distributive law)