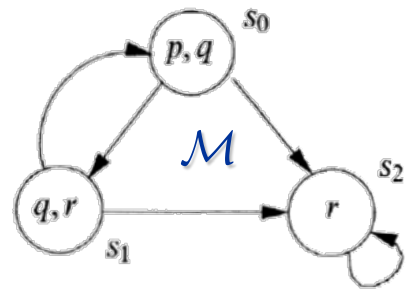
# Temporal Logic (2/2)

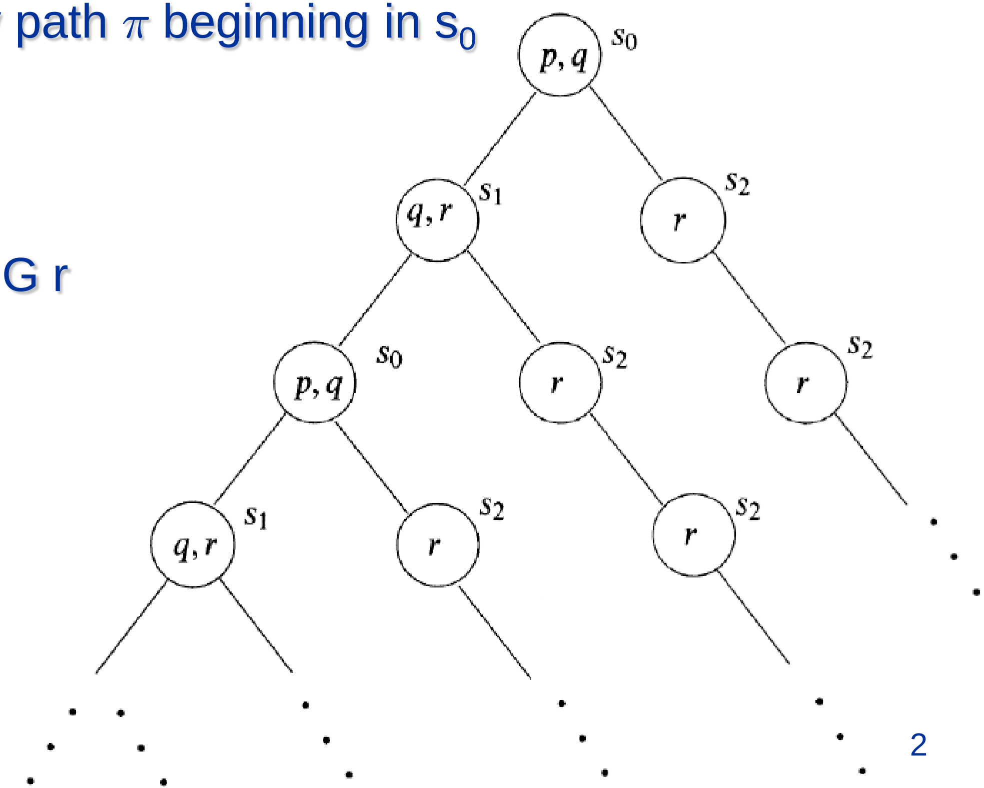
Moonzoo Kim
CS Division of EECS Dept.
KAIST

# Semantics of LTL (3/3)

- Def 3.8 Suppose $\mathcal{M}$ = (S, $\rightarrow$, L) is a model, s $\in$ S, and $\phi$ an LTL formula. We write $\mathcal{M}$,s $\vDash \phi$ if for every execution path $\pi$ of $\mathcal{M}$ starting at s, we have $\pi \vDash \phi$
  - If $\mathcal{M}$ is clear from the context, we write s $\vDash \phi$




- Example
  - $s_0 \vDash p \wedge q$ since $\pi \vDash p \wedge q$ for every path $\pi$ beginning in $s_0$
  - $s_0 \vDash \neg r$, $s_0 \vDash \top$
  - $s_0 \vDash X\, r$, $s_0 \nvDash X\,(q \wedge r)$
  - $s_0 \vDash G\, \neg(p \wedge r)$, $s_2 \vDash G\, r$
  - For any s of $\mathcal{M}$, s $\vDash F(\neg q \wedge r) \rightarrow F\, G\, r$
    - Note that $s_2$ satisfies $\neg q \wedge r$
  - $s_0 \nvDash G\, F\, p$
    - $s_0 \rightarrow s_1 \rightarrow s_0 \rightarrow s_1 \ldots \vDash G\, F\, p$
    - $s_0 \rightarrow s_2 \rightarrow s_2 \rightarrow s_2 \ldots \nvDash G\, F\, p$
  - $s_0 \vDash G\, F\, p \rightarrow G\, F\, r$
  - $s_0 \nvDash G\, F\, r \rightarrow G\, F\, p$



# Practical patterns of specification

- For any state, if a request occurs, then it will eventually be acknowledge
  - $G(\text{requested} \rightarrow F\ \text{acknowledged})$
- A certain process is enabled infinitely often on every computation path
  - $G\ F\ \text{enabled}$
- Whatever happens, a certain process will eventually be permanently deadlocked
  - $F\ G\ \text{deadlock}$
- If the process is enabled infinitely often, then it runs infinitely often
  - $G\ F\ \text{enabled} \rightarrow G\ F\ \text{running}$
- An upwards traveling lift at the second floor does not change its direction when it has passengers wishing to go to the fifth floor
  - $G\ (\text{fllor2} \wedge \text{directionup} \wedge \text{ButtonPressed5} \rightarrow (\text{directionup}\ U\ \text{floor5}))$
- It is impossible to get to a state where a system has started but is not ready
  - $\phi = G\ \neg(\text{started} \wedge \neg\text{ready})$
  - What is the meaning of (intuitive) negation of $\phi$ ?
    - It is possible to get to such a state ($\text{started} \wedge \neg\text{ready}$).
    - There exists a such path that gets to such a state.
      - we cannot express this meaning directly
- LTL has limited expressive power
  - For example, LTL cannot express statements which assert the existence of a path
    - From any state s, there exists a path $\pi$ starting from s to get to a restart state
    - The lift can remain idle on the third floor with its doors closed
  - Computation Tree Logic (CTL) has operators for quantifying over paths and can express these properties

# Summary of practical patterns

| | | |
|---|---|---|
| G p | always p | invariance |
| F p | eventually p | guarantee |
| $p \rightarrow (F\ q)$ | p implies eventually q | response |
| $p \rightarrow (q\ U\ r)$ | p implies q until r | precedence |
| G F p | always, eventually p | recurrence (progress) |
| F G p | eventually, always p | stability (non-progress) |
| $F\ p \rightarrow F\ q$ | eventually p implies eventually q | correlation |

# Equivalences between LTL formulas

- Def 3.9 $\phi \equiv \psi$ if for all models $\mathcal{M}$ and all paths $\pi$ in $\mathcal{M}$: $\pi \vDash \phi$ iff $\pi \vDash \psi$
- $\neg G\ \phi \equiv F\ \neg\phi$, $\neg F\ \phi \equiv G\ \neg\phi$, $\neg X\ \phi \equiv X\ \neg\phi$
- $\neg\ (\phi\ U\ \psi) \equiv \neg\phi\ R\ \neg\psi$, $\neg(\phi\ R\ \psi) \equiv \neg\phi\ U\ \neg\psi$
- $F\ (\phi \lor \psi) \equiv F\ \phi \lor F\ \psi$
- $G\ (\phi \land \psi) \equiv G\ \phi \land G\ \psi$
- $F\ \phi \equiv T\ U\ \phi$, $G\ \phi \equiv \bot\ R\ \phi$
- $\phi\ U\ \psi \equiv \phi\ W\ \psi \land F\ \psi$
- $\phi\ W\ \psi \equiv \phi\ U\ \psi \lor G\ \phi$
- $\phi\ W\ \psi \equiv \psi\ R\ (\phi \lor \psi)$
- $\phi\ R\ \psi \equiv \psi\ W\ (\phi \land \psi)$

# Adequate sets of connectives for LTL (1/2)

- X is completely orthogonal to the other connectives
  - X does not help in defining any of the other connectives.
  - The other way is neither possible
- Each of the sets {U,X}, {R,x}, {W,X} is adequate
  - {U,X}
    - $\phi$ R $\psi \equiv \neg(\neg \phi$ U $\neg \psi)$
    - $\phi$ W $\psi \equiv \psi$ R $(\phi \vee \psi) \equiv \neg(\neg\psi$ U $\neg(\phi \vee \psi))$
  - {R,X}
    - $\phi$ U $\psi \equiv \neg(\neg\phi$ R $\neg\psi)$
    - $\phi$ W $\psi \equiv \psi$ R $(\phi \vee \psi)$
  - {W,X}
    - $\phi$ U $\psi \equiv \neg(\neg \phi$ R $\neg \psi)$
    - $\phi$ R $\psi \equiv \psi$ W $(\phi \wedge \psi)$

# Adequate sets of connectives for LTL (2/2)

- Thm 4.10 $\phi \text{ U } \psi \equiv \neg(\neg\psi \text{ U } (\neg\phi \wedge \neg\psi)) \wedge \text{F } \psi$
- Proof: take any path $s_0 \to s_1 \to s_2 \to \ldots$ in any model
  - Suppose $s_0 \vDash \phi \text{ U } \psi$
    - Let n be the smallest number s.t. $s_n \vDash \psi$
      - We know that such n exists from $\phi \text{ U } \psi$. Thus, $s_0 \vDash \text{F } \psi$
      - For each k < n, $s_k \vDash \phi$ since $\phi \text{ U } \psi$
    - We need to show $s_0 \vDash \neg(\neg\psi \text{ U } (\neg\phi \wedge \neg\psi))$
      - case 1: for all i, $s_i \nvDash \neg\phi \wedge \neg\psi$. Then, $s_0 \vDash \neg(\neg\psi \text{ U } (\neg\phi \wedge \neg\psi))$
      - case 2: for some i, $s_i \vDash \neg\phi \wedge \neg\psi$. Then, we need to show
        - (*)for each i >0, if $s_i \vDash \neg\phi \wedge \neg\psi$, then there is some j < i with $s_j \nvDash \neg\psi$ (i.e. $s_j \vDash \psi$)
        - Take any i >0 with $s_i \vDash \neg\phi \wedge \neg\psi$. We know that i > n since $s_0 \vDash \phi \text{ U } \psi$. So we can take j=n and have $s_j \vDash \psi$
  - Conversely, suppose $s_0 \vDash \neg(\neg\psi \text{ U } (\neg\phi \wedge \neg\psi)) \wedge \text{F } \psi$
    - Since $s_0 \vDash \text{F } \psi$, we have a minimal n as before s.t. $s_n \vDash \psi$
      - case 1: for all i, $s_i \nvDash \neg\phi \wedge \neg\psi$ (i.e. $s_i \vDash \phi \vee \psi$). Then $s_0 \vDash \phi \text{ U } \psi$
      - case 2: for some i, $s_i \vDash \neg\phi \wedge \neg\psi$. We need to prove for any i <n, $s_i \vDash \phi$
        - Suppose $s_i \nvDash \phi$ (i.e., $s_i \vDash \neg\phi$ ). Since n is minimal, we know $s_i \vDash \neg\psi$. So by (*) there is some j <i<n with $s_j \vDash \psi$, contradicting the minimality of n. Contradiction