Lecture 3: Linear-Time Temporal Logic

Lecturer: Dr. Jie Fu

Department of Electrical and Computer Engineering

University of Florida

Fall, 2023

Reading

- Principle of model checking. Chapter 5.1.1, 5.1.2. Mainly focus on the syntax and semantics.
- Other related reading:
  - https://cgi.csc.liv.ac.uk/~michael/TLBook/tl3.pdf [many interesting examples.] or the book: https://cgi.csc.liv.ac.uk/~michael/TLBook/ section slides 1.

What are formal specifications?

- Motivating applications:
  - Human-robot interaction: The robot needs to understand human's intention and task requirements.
  - Autonomous driving: The autonomous vehicle needs to follow traffic rules.

Photo: https://www.nature.com/articles/d41586-022-00072-z

Photo: spectrum.ieee.org

Formal specifications use **mathematical notations** to describe in a **precise** way the **properties/objectives** which an **intelligent** system should have/achieve.

A motivating example

"Please fetch a clean cup for me from the kitchen, "

"If you cannot find the cup in the kitchen, check the dinner table."

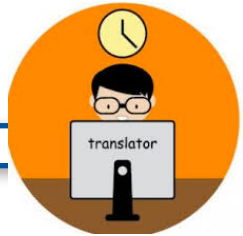
@%#%@%#^@Q^$^@

I don't understand…

A motivating example

"Please fetch a clean cup for me from the kitchen, "

"If you cannot find the cup in the kitchen, check the dinner table."



$\Diamond$(HasCup $\wedge$ Inkitchen $\wedge$ IsCupClean $\rightarrow$ $\Diamond$InLivingRoom)

$\neg$HasCup $\wedge$ InKitchen $\rightarrow$ $\Diamond$InDinningRoom

Understanding specifications

The first step:

Designing a (semi)-autonomous robot is to specify the **intended** behavior of the robot in a **compact** and **rigorous** manner.

- **Compact**: Minimal number of memory.
- **Rigorous**: No ambiguous interpretation.

What is logic?

A mathematical language that can describe non-mathematical and mathematical facts in mathematical "propositions".

- Propositional Logic
- First-order Logic
- Linear Temporal Logic (LTL) (*)
- OTHERS: Signal Temporal Logic, Metric Temporal Logic, Computational Tree Logic (will be introduced later if time allows)

Let's start with propositions

- Propositions: A statement that can be either true or false, but not both.
  - Which ones are propositions?
    - "The traffic light is red."
    - "The cup is clean."
    - "The robot is in dining room."
    - "Is the cup in the kitchen?"

Propositional logic

- Propositional logic formulas are constructed from atomic propositions by logical connectives.
- The truth value of a propositional logic formulas can be computed from the truth values of the atomic propositions it contains.

Formal Name	Symbol	Read	Symbolic Form
Negation	$\sim$	"Not"	$\sim p$
Conjunction	$\wedge$	"And"	$p \wedge q$
Disjunction	$\vee$	"Or"	$p \vee q$
Conditional	$\rightarrow$	"If-then"	$p \rightarrow q$
Biconditional	$\leftrightarrow$	"If and only if"	$p \leftrightarrow q$

Temporal Logic: What it is about?

- Limited expressiveness of propositional logic:
  - Describes **a current state**
    - E.g. “The robot is at its destination.”
- **Temporal logic to reason** with temporal sequences of states/event
  - Describe a future state
    - E.g. “The robot shall eventually reach its destination.”
    - E.g. “The robot should first go to the kitchen, then pick up the cup, and last return to the lady with the cup.”

Temporal Logic: What it is about?

- Specifications for autonomous systems are given as **temporal sequence of events.**
  - Examples:
    - The robot should check the kitchen first, and if the cup is not there, then the robot should check the dinning room.
    - The autonomous vehicle must always stop at a STOP sign before proceeding if it is OK to pass.
    - The vehicle should reach NEB first and then the commuter Parkin lot.
    - A patrolling robot must visit check points A, B, C, D infinitely often and avoid running into dynamic or static obstacles. Every check point must be revisited within 10 time steps after the last check.

Linear temporal logic

"Temporal" here refers to the **relative order of events**, but not specific time point/ duration of events.

"Linear Temporal logic" refers to the linear order of events evolving over time.

Example of properties in LTL:

"The car will stop **after** the driver steps on the brake."

Example of properties NOT in LTL:

"There is **a delay no smaller than 1 s** between braking and the car fully stops given the current speed limit."

Linear temporal logic

Linear Temporal Logic (LTL) is an infinite sequence of states where each point in time has a unique successor, based on the **linear** time perspective.

- Propositional logic + Temporal Operators:
  - X (Next)
  - U (Until)

Linear temporal logic

- Inductively defined as:

$$\varphi := p \mid \neg\varphi \mid \varphi \wedge \varphi \mid X\varphi \mid \varphi U \varphi \mid F\varphi \mid G\varphi$$

- Intuitive semantics:
  - Proposition p: holds at the current time.
  - $X\varphi$: φ is true at the next time instant.
  - $\phi U \psi$: ϕ is true until ψ becomes true.
  - $F\varphi$: At some future time, φ holds true. $F\varphi := \text{true} U \varphi$
  - $G\varphi$: At all time, φ holds true. $G\varphi := \neg(\text{true} U \neg\varphi)$

G not hit people

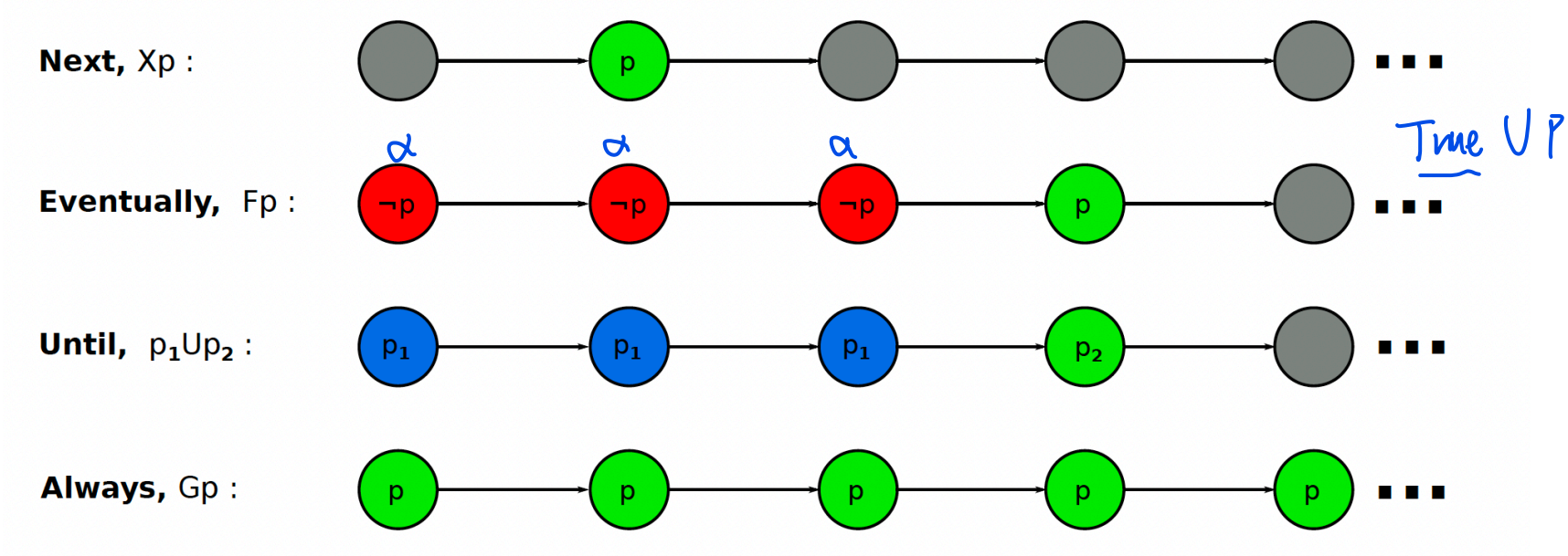
¬ (F hit people)

¬ (True U hit people)

¬ (True U ¬φ)

Linear temporal logic

- Intuitive semantics:



Linear temporal logic

- Inductively defined as:

$$\varphi := p \mid \neg\varphi \mid \varphi \wedge \varphi \mid X\varphi \mid \varphi U\varphi \mid F\varphi \mid G\varphi$$

- What does "inductive definition" mean?
  - If φ and ψ are LTL formulas, so is $\varphi \wedge \psi, X\varphi, \varphi U\psi, F\varphi, G\varphi,$
  - And so is $\varphi U(\psi U\varphi_1), FG\varphi, GF\varphi, \ldots$
  - But not $U\varphi, G\varphi X\psi$

Semantics

$w = w_0 w_1 w_2 \cdots$

↑ symbol → "Event"

- The semantics of a temporal logic formula is given by an interpretation relation:

  $\models: M \times \mathbb{N} \rightarrow \{0,1\}$

  M: a model (in our context, a word w over 2^{AP})

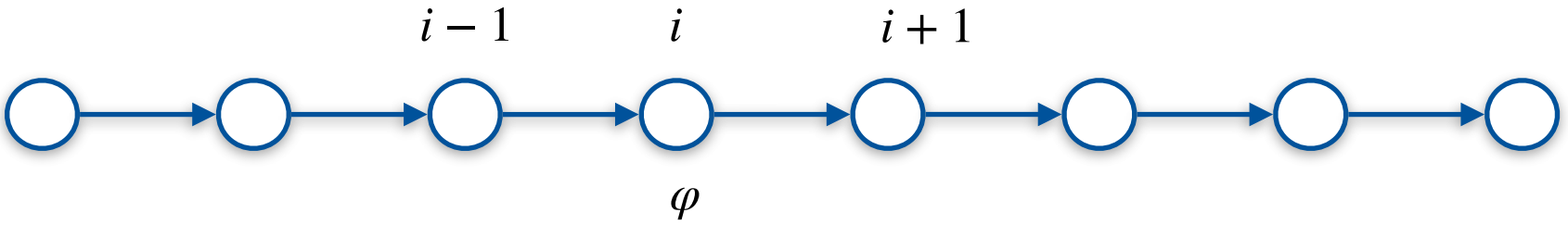
  i: a time index (starting point)

  $< w, i > \models \varphi$ if starting from the i-th point in the word, the formula φ is satisfied.

Semantics

$< w, i > \models \varphi$ if starting from the i-th point in the model, the formula φ is satisfied.

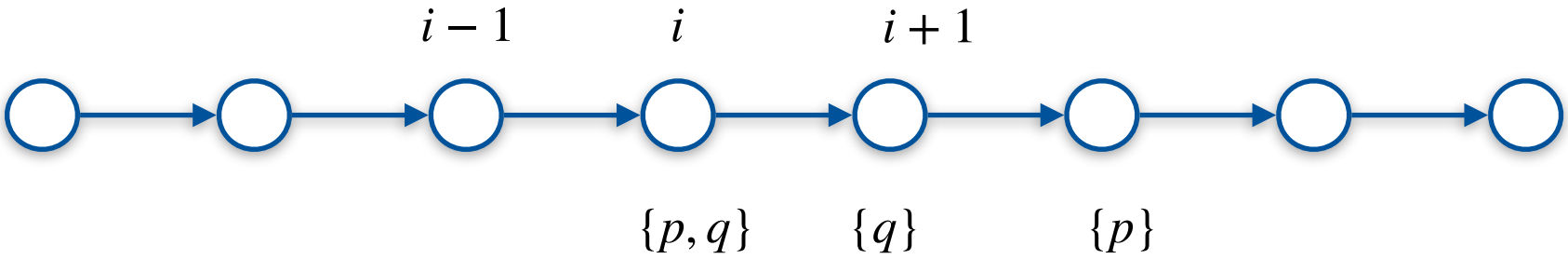
Pictorially:



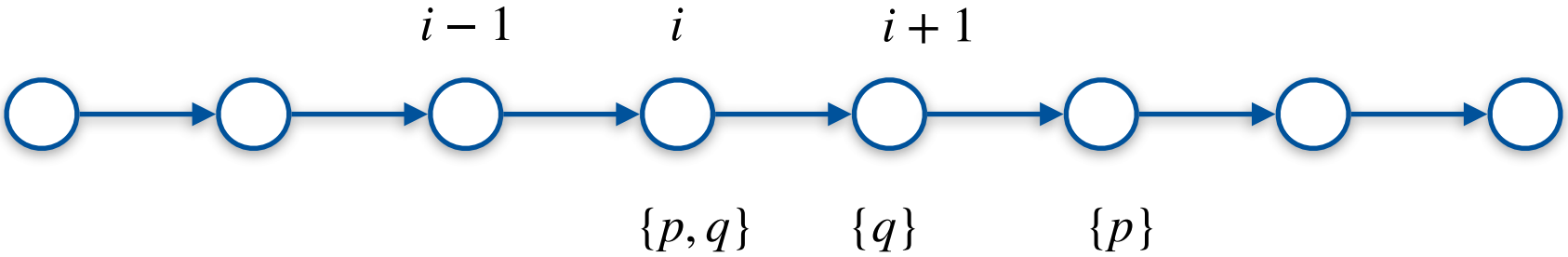
Semantics

$< w, i > \models p$ if starting from the i-th point in the model, the proposition p is satisfied.

Pictorially:



Semantics: Example



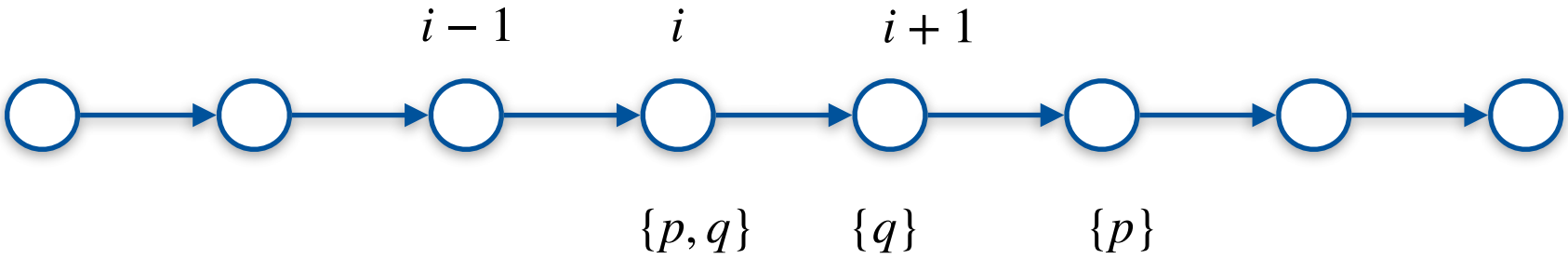
Quiz: what statements are true?

1. $< w, i > \models p$
2. $< w, i > \models q$
3. $< w, i > \models p \wedge q$
4. $< w, i > \models p \vee q$
5. $< w, i+1 > \models p$
6. $< w, i+2 > \models p \vee q$

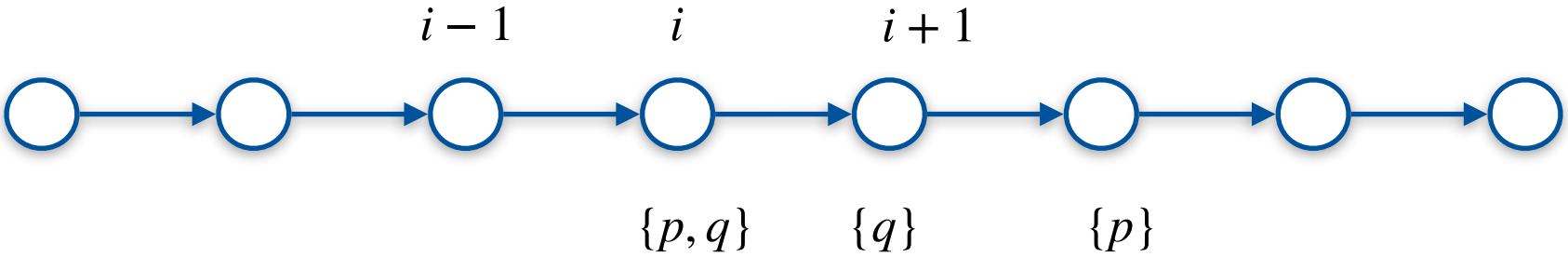
Semantics

$< w, i > \models X\varphi$ **iff** $< w, i+1 > \models \varphi$

$< w, i > \models Xp?$ $< w, i > \models Xq?$



Semantics



Quiz: what statements are true?

1. $< w, i > \models XXp$ ⇒ $(w, i+1) \models Xp$ ⇒ $(w, i+2) \models p$
2. $< w, i > \models Xq$
3. $< w, i > \models Xp \vee q$
4. $< w, i > \models X(p \vee q)$

Semantics

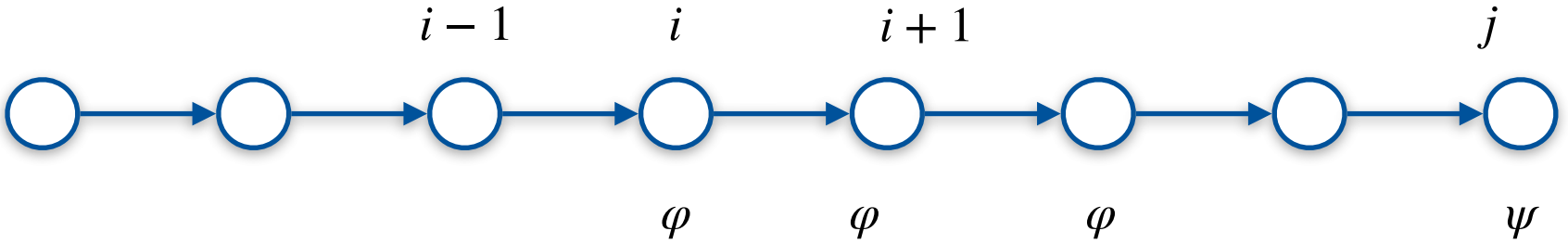
hold plate φ U deliever ψ

$< w, i > \models \varphi U \psi$ **(reads property φ holds until property ψ holds.)**

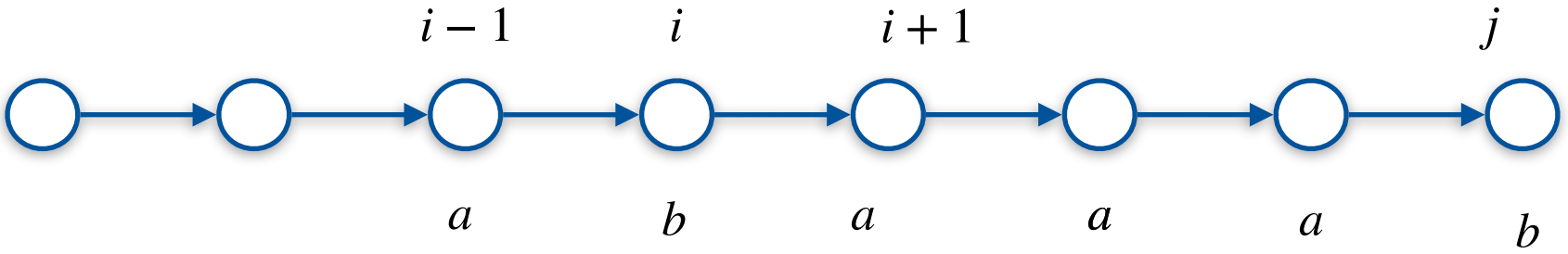
if and only if

- there exists some j, $< w, j > \models \psi$, and

- for all $j > k \geq i$, $< w, k > \models \varphi$



Semantics: Example



- Quiz: what statements are true?

1. $< w, i > \models aUb$ ✓
2. $< w, i+1 > \models aUb$ ✓ $\Leftrightarrow \langle w, i \rangle \models X(a \vee b)$
3. $< w, i-1 > \models aUb$
4. $< w, i > \models bUa$
5. $< w, j > \models aUb$

Semantics

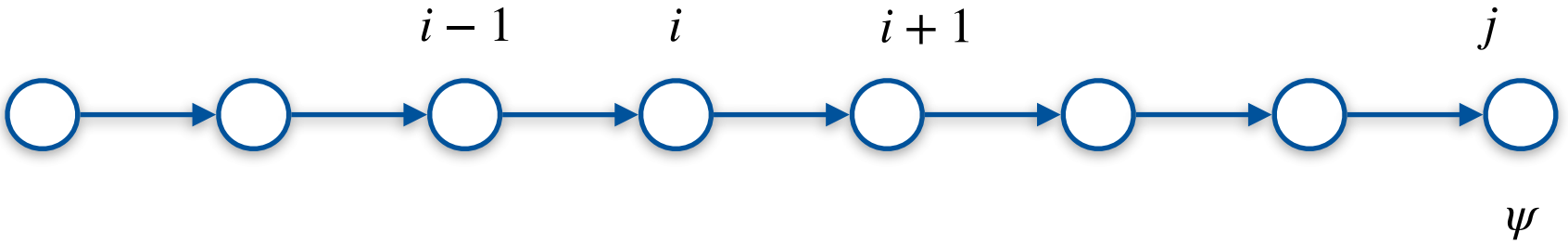
$F\psi$

$< w, i > \models$ **true** $U\psi$ **(universally true until property** ψ **holds.)**

true : Logic symbol for tautology for universally true.

- there exists some j, $< w, j > \models \psi$, **and**

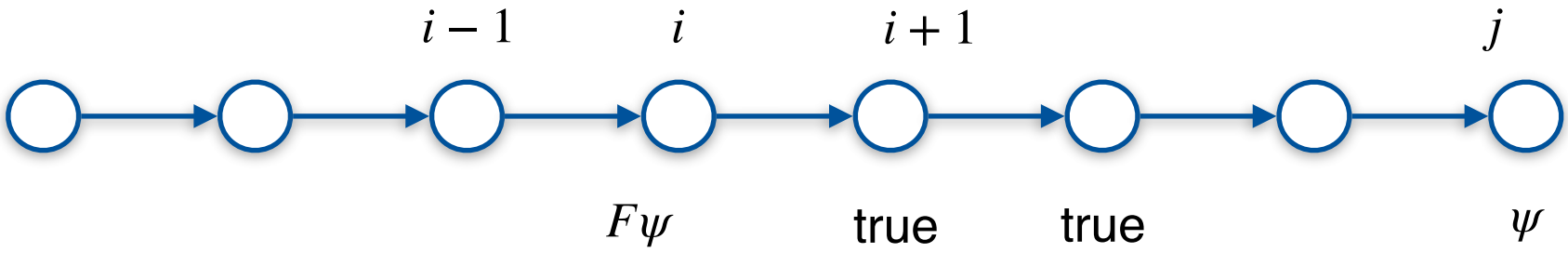
- for all $j > k \geq i$, $< w, k > \models$ **True**



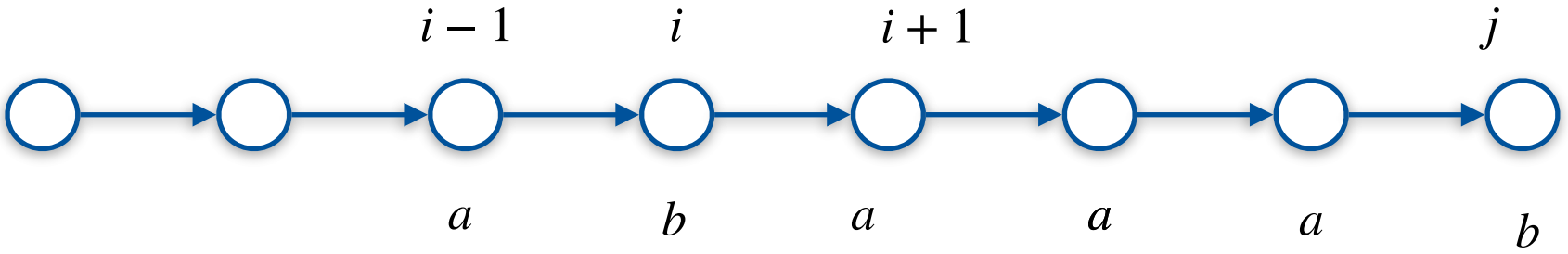
Semantics

$< w, i > \models \textbf{True}\ U\psi$ is equivalently expressed as $< w, i > \models F\psi$

F also written as $\Diamond$: "Eventually …"



Semantics: Example



- Quiz: what statements are true?

1. $< w, i > \models Fa$ ✓
2. $< w, i+1 > \models Fa$ ✓
3. $< w, i-1 > \models Fb$ ✓
4. $< w, j > \models Fb$ ✓

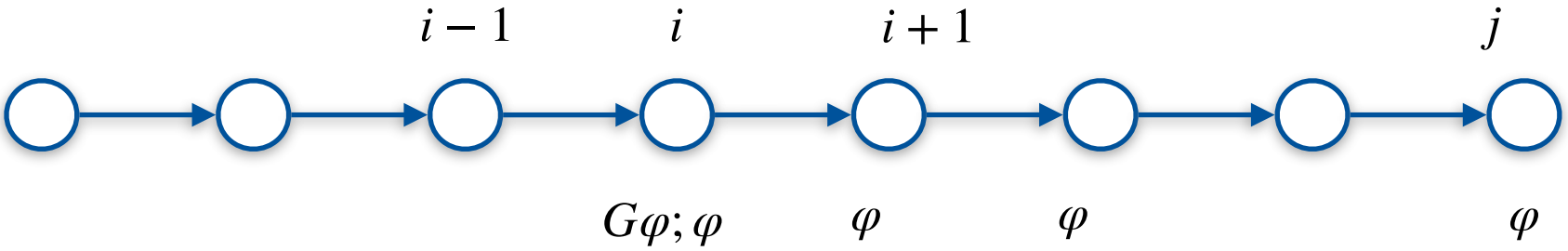
Semantics

$< w, i > \models G\phi$

G also written as $\Box$: reads Globally or Always .

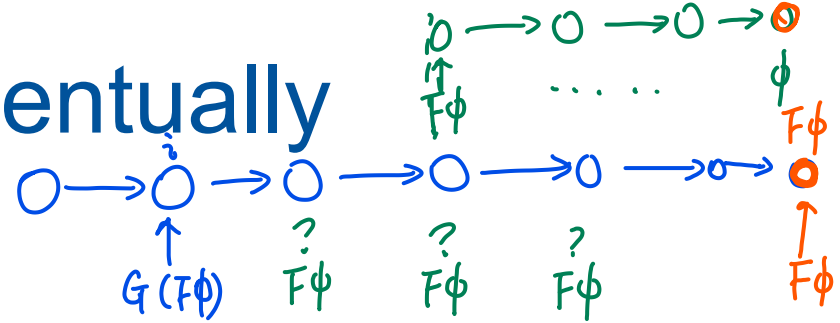
if and only if

- for all $j \geq i, < w, j > \models \varphi$



Semantics: Always Eventually

$< w, i > \models GF\phi \Rightarrow$ G(Fϕ)

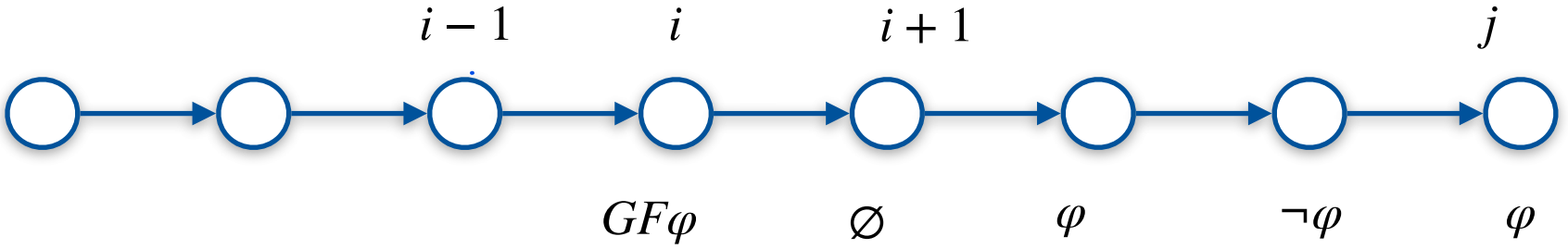


GF also written as $\square\Diamond$: reads Always, Eventually ... .

if and only if

- **for all** $j \geq i$, $< w, j > \models F\varphi$ —"always (at all time points,) eventually event ϕ occurs"

Or "Event ϕ occurs infinitely often"



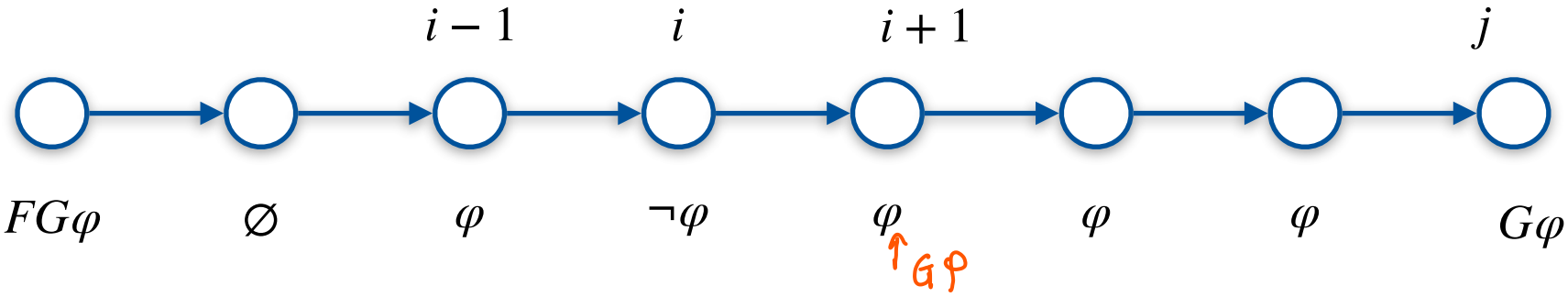
Semantics: Eventually Always

$< w, i > \models FG\phi$ $\Rightarrow$ $F(G\phi)$

FG also written as $\Diamond\Box$: reads Eventually Always... .

if and only if

- there is a time $j \geq i, < w, j > \models G\varphi$ —"eventually (at all time points,) event ϕ occurs and holds for all future time."



Semantics

- Propositions: AP = {a,b,c,d} (such as waypoints for the robot)
- Model: The labeling of the path, given as a word over 2^{AP}.
- e.g. $w = \{a\}\varnothing\{a,b\}\varnothing\{b\}$
- Correct or wrong:
  - $< w,0 > \models a?$ $< w,0 > \models b?$
  - $< w,0 > \models Xa?$ $< w,1 > \models Xa?$ $< w,0 > \models XXa?$
  - $< w,2 > \models a \wedge b?$
  - $< w,0 > \models F(b \wedge \neg a)?$

Correct or wrong

0 1 2 3 4

- $w = \{a\}\varnothing\{a,b\}\varnothing\{b\}(\{c\}\{a\})^{\omega}$ → omega-regular

  empty set

  $\{c\}\{a\}\{c\}\{a\}\ldots$

  - $< w,0 > \models Ga$
  - ✗ $< w,0 > \models FGa$ $FG(a \vee c)$
  - $< w,0 > \models G\neg d$
  - $< w,4 > \models bUc$

Example

AP = { A, B, C, D, Blue, white, Black }

G (Blue ∧ ¬ Black)

- Always stay in the blue region and not enter the black cell.
- Stay in the blue region until a black cell is reached. Blue U Black
- Eventually reach region A. F A
- Eventually reach region A or region B. F(A ∨ B)

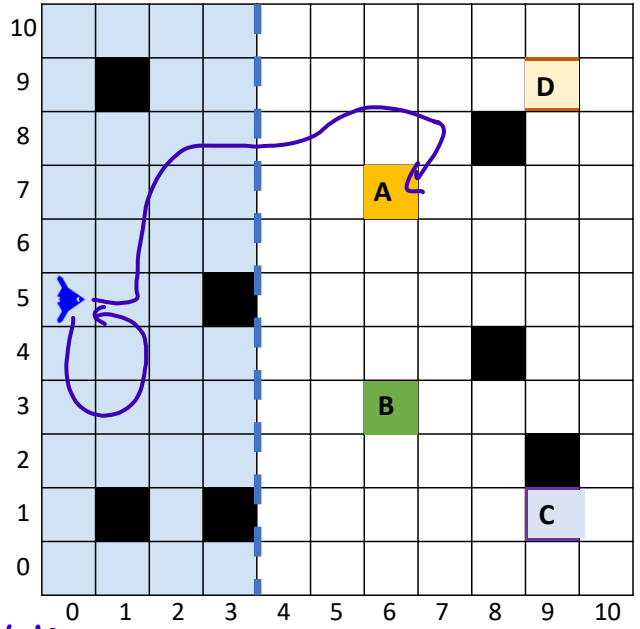
F A ∨ B ✗

- Always, Eventually reach region A or region B.

G F(A ∨ B)

- Eventually, Always reach region A.

F G A



state

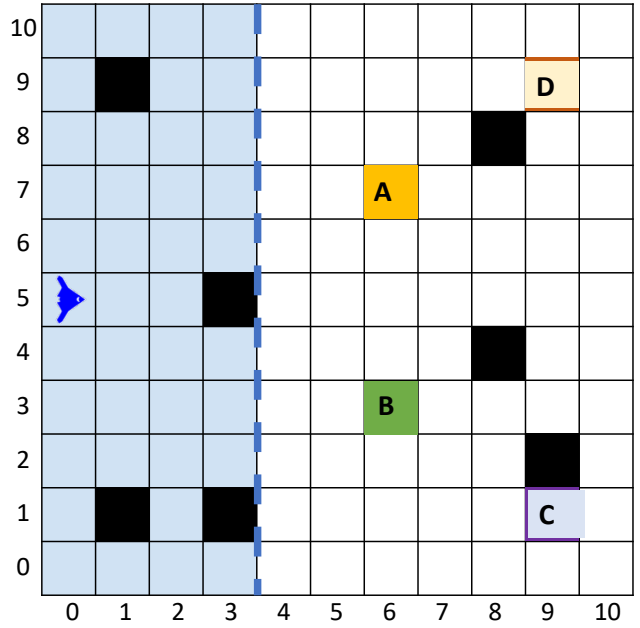
0 → 0 → 0 → 0 →

(0,5) (1,5) (1,6) (1,7) (2,7) (2,8) .

{Blue} {Blue}

Example

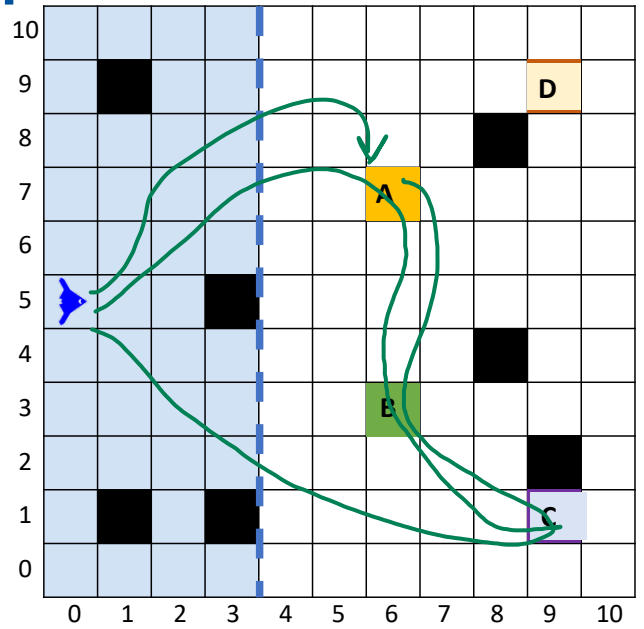
- Goal reaching task:
  - Eventually reach region A.
  - Eventually reach region A or region B.
- Safe until reach task:
  - Always avoid obstacles (black) until one of the goals is reached.



$G(\neg \text{Black} \; U \; (A \vee B \vee C \vee D))$

Examples: Robotic mission

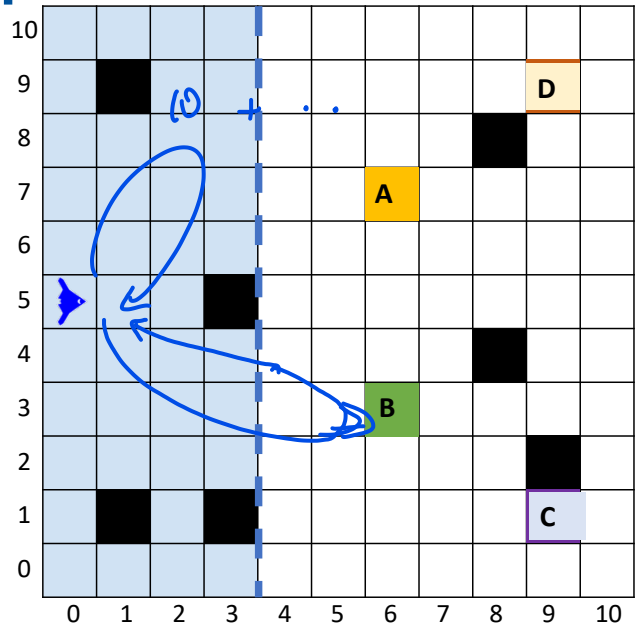
- Sequential subgoals:
  - visiting A, B, and C in any order.
  - Visiting A first, B second, ~~and C last.~~
  - Visiting A first, B second, and visiting C.



Examples: Robotic mission

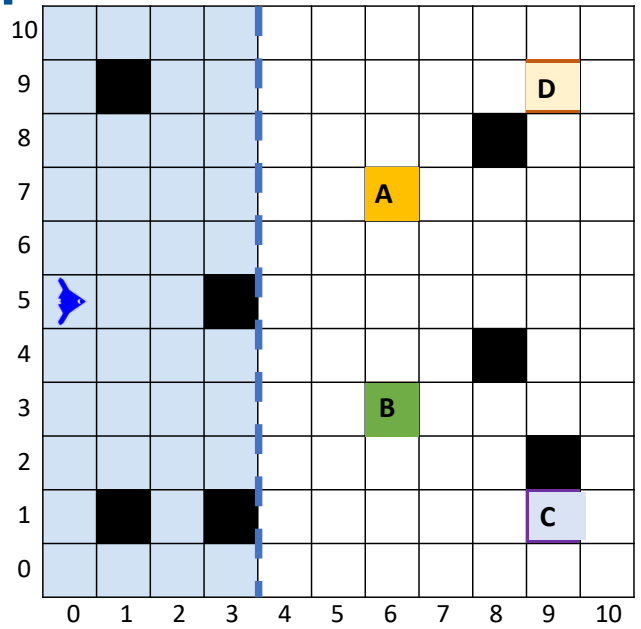
- ~~Always eventually visiting region A or region B.~~

- Always Eventually reach blue region after visiting one of the goals in the white region.



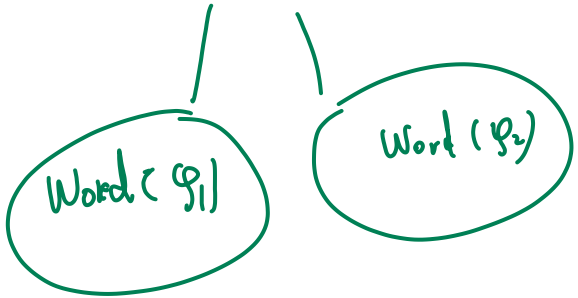
Examples: Robotic mission

- (Conditional) safety:
  - If collision occurs, return to repair station at A.
  - If the alarm is sound in region B, reach region B eventually.



LTL equivalence

- An LTL formula φ is equivalent to a set of (infinite) words satisfying φ, denoted Word(φ).
- Two formulas φ_1, φ_2 are equivalent if and only if $\text{Word}(\varphi_1) = \text{Word}(\varphi_2)$.



LTL equivalence (duality)

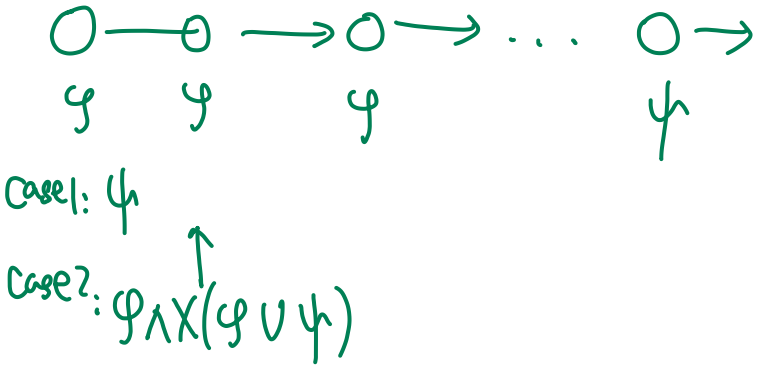
- $\neg X\varphi = X\neg\varphi$ ``self-duality of the next''
- $\neg F\varphi = G\neg\varphi$
- $\neg G\varphi = F\neg\varphi$

LTL equivalence (absorption)

- $FGF\varphi = GF\varphi$ "from some point, φ holds infinitely often " is equivalent to "infinitely often φ. "
- $GFG\varphi = FG\varphi$ "at every time point, eventually φ holds always" is equivalent to "eventually φ holds always."

LTL equivalence (expansion law)

- $\varphi U \psi = \psi \vee (\varphi \wedge X(\varphi U \psi))$
- $F\varphi = \varphi \vee XF\varphi$
- $G\varphi = \varphi \wedge XG\varphi$



LTL equivalence (distributive law)

- $F\varphi_1 \vee F\varphi_2 = F(\varphi_1 \vee \varphi_2)$

φ_1: A φ_2: B $F\varphi_1 \vee F\varphi_2 = F(\varphi_1 \vee \varphi_2)$

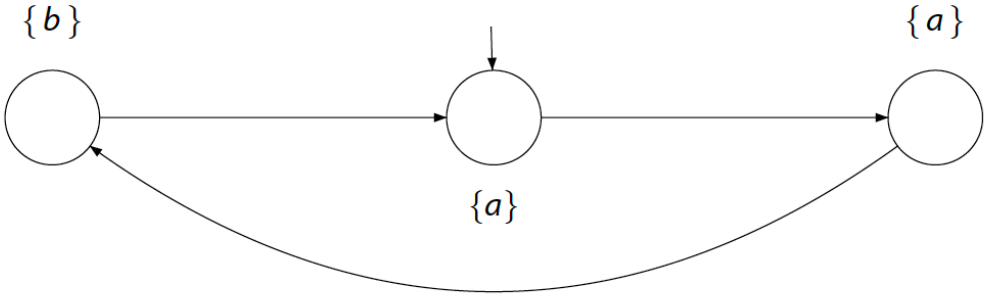
Right or wrong? (distributive law)

- $F\varphi_1 \wedge F\varphi_2 = F(\varphi_1 \wedge \varphi_2)$?
- $G\varphi_1 \wedge G\varphi_2 = G(\varphi_1 \wedge \varphi_2)$? ✓
- $G\varphi_1 \vee G\varphi_2 = G(\varphi_1 \vee \varphi_2)$?

AB AB ...

Right or wrong (distribution law)

- $Fa \wedge Fb = F(a \wedge b)$?
- $Ga \vee Gb = G(a \vee b)$?



Expressive completeness

- First-order logic + linear order: First order logic with 0 and $<$, unary symbols, and interpreted over words.
- Theorem [Kamp'68]: Every language that can be defined by first order logic + linear order, then the language can be defined by linear temporal logic.