# Foundations of Privacy 2014

## Recitation on Logic

Blackboard Issues?

# Propositional ("0$^{th}$ order") Logic

# Propositional ("0th order") Logic

A model for a simple **subset**
of mathematical reasoning

| | |
|---|---|
| Not | $\neg$ |
| And | $\wedge$ |
| Or | $\vee$ |
| Implies | $\rightarrow$ |
| If And Only If | $\leftrightarrow$ |

# Propositional ("0th order") Logic

| An English statement that can be true or false | Propositional variable: a symbol (letter) representing it |
| --- | --- |
| "Potassium is observed." | k |
| "Hydrogen is observed." | h |
| "Pixel 29 is black." | $p_{29}$ |
| "It's raining." | r |

| Compound sentence | Propositional formula |
| --- | --- |
| Potassium is not observed. | $\neg k$ |
| At least one of hydrogen and potassium is observed. | $(h \vee k)$ |
| If potassium is observed then hydrogen is also observed. | $(k \rightarrow h)$ |
| If I'm not playing tennis then I'm watching tennis, and if I'm not watching tennis then I'm reading about tennis. | p,w,r<br>$((\neg p \rightarrow w) \wedge (\neg w \rightarrow r))$ |

Formally, formulas are strings made up of:

| | |
|---|---|
| ( | (punctuation) |
| ) | (punctuation) |
| $\neg$ | (not) |
| $\wedge$ | (and) |
| $\vee$ | (or) |
| $\rightarrow$ | (implies) |
| $\leftrightarrow$ | (if and only if) |
| $x_1, x_2, x_3, \ldots$ | (variable symbols) |

# Well-formed formula (WFF)

= A string which is syntactically “legitimate”.

| WFF | not a WFF |
| --- | --- |
| $x_1$ | $x_1 \wedge$ |
| $((x_1 \wedge (x_3 \rightarrow \neg x_2)) \vee x_1)$ | $))x_2 \rightarrow \rightarrow$ |
| $\neg((x_{10} \leftrightarrow x_{11}) \wedge (x_2 \rightarrow x_5))$ | $((x_1 \wedge (x_3 \rightarrow \neg x_2)) \neg x_1)$ |

# Well-formed formula (WFF)

Formally, WFFs have an inductive definition:

Base case: Single variables are WFFs.

Inductive rules:

- If A is a WFF, so is ¬A .
- If A, B are WFFs, so are
  (A∧B) ,
  (A∨B) ,
  (A→B) ,
  (A↔B) .

Let’s talk about **TRUTH (SEMANTICS)**.

"If potassium is observed then carbon and hydrogen are also observed."

$$(k \rightarrow (c \wedge h))$$

Q: Is this statement true?

A: The question does not make sense.

"If potassium is observed then carbon and hydrogen are also observed."

$(k \rightarrow (c \wedge h))$

Whether this statement/formula is true/false depends on whether the variables are true/false ("state of the world").

If k is **T**, c is **T**, h is **F**…

… the formula is **False**.

If k is **F**, c is **F**, h is **T**…

… the formula is **True**.

Truth assignment **V** :

assigns **T** or **F** to each variable

Extends to give a truth value **V**[S]
for any formula S by applying these rules:

| A | B | ¬A | (A∧B) | (A∨B) | (A→B) | (A↔B) | *¬A∨B* |
|---|---|---|---|---|---|---|---|
| F | F | T | F | F | T | T | *T* |
| F | T | T | F | T | T | F | *T* |
| T | F | F | F | T | F | F | *F* |
| T | T | F | T | T | T | T | *T* |

# Truth assignment example

$$S = (x_1 \rightarrow (x_2 \wedge x_3))$$

$$\mathbf{V}: \quad \begin{array}{l} x_1 = \mathbf{T} \\ x_2 = \mathbf{T} \\ x_3 = \mathbf{F} \end{array}$$

$$\mathbf{V}[S] = (\mathbf{T} \rightarrow (\mathbf{T} \wedge \mathbf{F}))$$

$$\mathbf{V}[S] = (\mathbf{T} \rightarrow \mathbf{F})$$

$$\mathbf{V}[S] = \mathbf{F}$$

# Satisfiability

V **satisfies** S:

**V** [S] = **T**

S is **satisfiable**:

there exists **V** such that **V** [S] = **T**

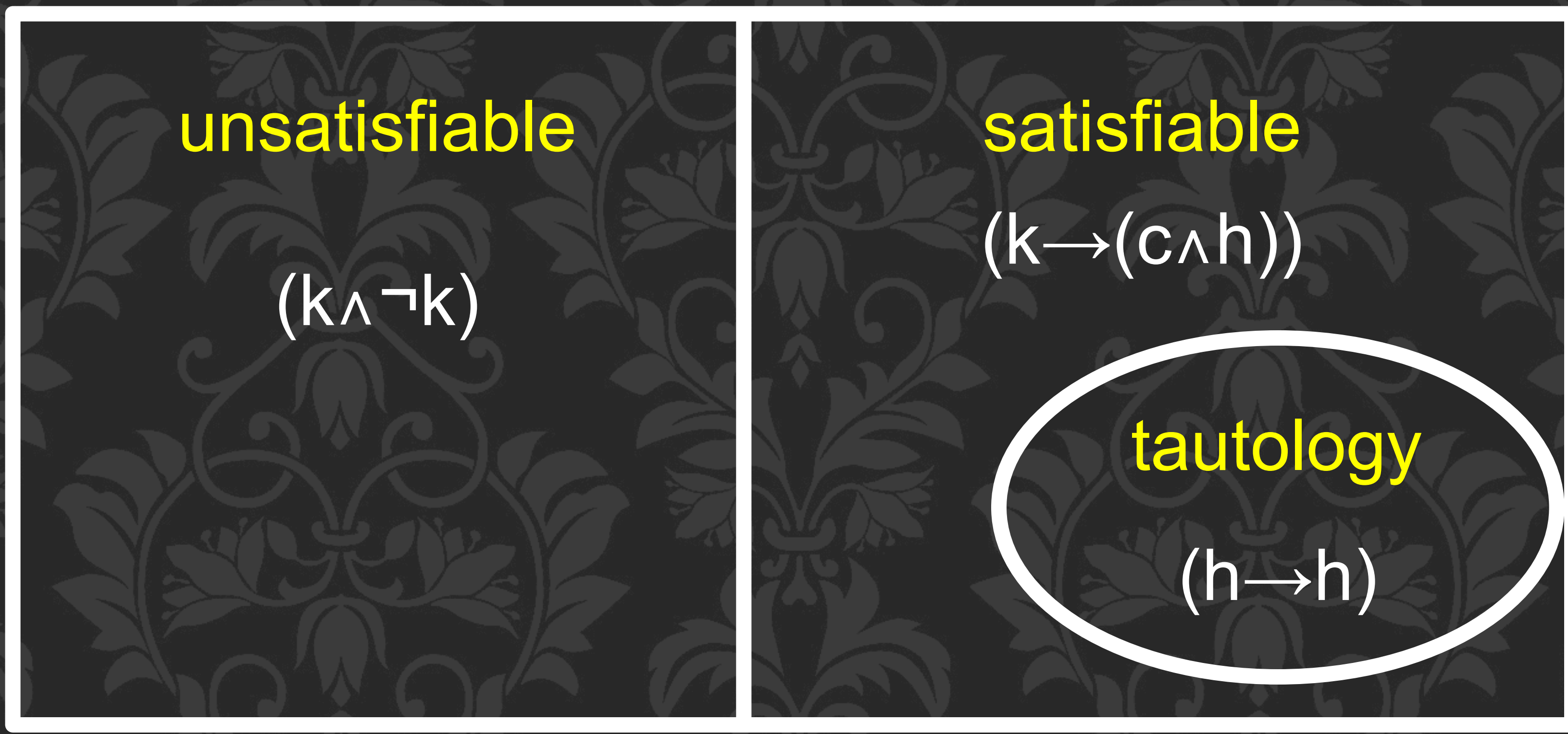
S is **unsatisfiable**:

**V** [S] = **F** for all **V**

S is a **tautology**:

**V** [S] = **T** for all **V**

# All well-formed formulas




"Potassium is observed and potassium is not observed."

"If potassium is observed then
carbon and hydrogen are observed."

"If hydrogen is observed then hydrogen is observed."

Tautology: automatically true,
for ‘purely logical’ reasons

Unsatisfiable: automatically false,
for purely logical reasons

Satisfiable (but not a tautology):

truth value depends
on the state of the world

$S = ((x \rightarrow (y \rightarrow z)) \leftrightarrow ((x \wedge y) \rightarrow z))$

# Truth table

| x | y | z | $((x \rightarrow (y \rightarrow z)) \leftrightarrow ((x \wedge y) \rightarrow z))$ |
|---|---|---|---|
| F | F | F | |
| F | F | T | |
| F | T | F | |
| F | T | T | |
| T | F | F | |
| T | F | T | |
| T | T | F | |
| T | T | T | |

$S = ((x \rightarrow (y \rightarrow z)) \leftrightarrow ((x \wedge y) \rightarrow z))$

# Truth table

| x | y | z | $((x \rightarrow (y \rightarrow z)) \leftrightarrow ((x \wedge y) \rightarrow z))$ |
|---|---|---|---|
| F | F | F | T |
| F | F | T | |
| F | T | F | |
| F | T | T | |
| T | F | F | |
| T | F | T | |
| T | T | F | |
| T | T | T | |

S is **satisfiable!**

$S = ((x \rightarrow (y \rightarrow z)) \leftrightarrow ((x \wedge y) \rightarrow z))$

# Truth table

| x | y | z | $((x \rightarrow (y \rightarrow z)) \leftrightarrow ((x \wedge y) \rightarrow z))$ |
|---|---|---|---|
| F | F | F | T |
| F | F | T | T |
| F | T | F | T |
| F | T | T | T |
| T | F | F | T |
| T | F | T | T |
| T | T | F | T |
| T | T | T | T |

S is a **tautology**!

**Problem:** Show $(((x \to y) \land x) \to y)$ is a tautology.

Truth-table method: quite long, not intuitive

Can we build up a proof systematically?

Inference rules:

¬ introduction

$$\frac{A \to \neg B \quad A \to B}{\neg A}$$

∧ introduction

$$\frac{A \quad B}{A \land B}$$

∨ introduction

$$\frac{A}{A \lor B}$$

…

→introduction

$$\frac{\begin{array}{c} A \\ \vdots \\ B \end{array}}{A \to B}$$

¬ elimination

$$\frac{\neg A}{A \to B}$$

∧ elimination

$$\frac{A \land B}{A}$$

∧ elimination

$$\frac{A \land B}{B}$$

…

→elimination

$$\frac{A \to B \quad A}{B}$$

$$\dfrac{\dfrac{\dfrac{(x\to y)\wedge x}{(x\to y)}\;\wedge\text{ elimination} \qquad \dfrac{(x\to y)\wedge x}{x}\;\wedge\text{ elimination}}{y}\;\to\text{ elimination}}{(((x\to y)\wedge x)\to y}\;\to\text{introduction}$$

**What is a proof?**

A sequence of statements,
each of which
is an axiom,
or a hypothesis,
or follows from previous statements
using an inference rule

**Problem:** Show $(((x \rightarrow y) \wedge x) \rightarrow y)$ is a tautology.

**Solution 1**: Truth-table method (semantic proof)

**Solution 2**: Use proof system: (syntactic proof)

Are all theorems (whatever can be proved) tautology?

Yes…for propositional logic

This property is called soundness of propositional logic

Are all tautology theorems?

Yes…for propositional logic

This property is called completeness of propositional logic

# Semantic entailment

**Definition:**

Formulas $A_1, \ldots, A_m$ **entail** formula S,

written $A_1, \ldots, A_m \models S$,

if every interpretation **I** which makes

$A_1, \ldots, A_m$ equal **T** also makes S equal **T**.

Tautology: $\phi \models S$

# Syntactic entailment

**Definition:**

Formulas $A_1, \ldots, A_m$ **entail** formula S,

written $A_1, \ldots, A_m \vdash S$,

if assuming $A_1, \ldots, A_m$ yields a proof of S

Theorem: $\phi \vdash S$

# Soundness and Completeness

**Soundness:**

$\Gamma \vdash S$ implies $\Gamma \vDash S$

**Completeness:**

$\Gamma \vDash S$ implies $\Gamma \vdash S$

# First order logic (FOL)

# A model for **pretty much all** mathematical reasoning

Not, And, Or, Implies, If And Only If

Plus: For All (∀), There Exists (∃), Equals (=)

“constants”, “predicates”, “functions”

Variables like x now represent **objects**, not truth-values.

"Alex is smarter than everyone":

$\forall x\ \mathrm{IsSmarter}(\mathbf{a}, x)$

**variable**:
stands for an object (person)

**constant name**:
stands for a particular object

**predicate name**:
stands for a mapping, object(s) $\mapsto$ **T/F**

"Alex is smarter than everyone":

$\forall x\ IsSmarter(\mathbf{a},x)$

"Alex is smarter than everyone else":

$\forall x\ (\neg(x=\mathbf{a}) \rightarrow IsSmarter(\mathbf{a},x))$

**propositional logic**, as usual

**equality** (of objects)

“Alex is smarter than everyone”:

$\forall x\ IsSmarter(\mathbf{a},x)$

“Alex is smarter than everyone else”:

$\forall x\ (\neg(x=\mathbf{a})\rightarrow IsSmarter(\mathbf{a},x))$

“Alex’s father is smarter than everyone else’s father”:

$\forall x\ (\neg(x=\mathbf{a})\rightarrow IsSmarter(Father(\mathbf{a}),Father(x)))$

**function name**:
stands for a mapping,
object(s) $\mapsto$ object

Vocabulary: A collection of constant-names,
function-names,
predicate-names.

Vocabulary from the previous slide:

one constant-name: **a**

one function-name: Father(·)

one predicate-name: IsSmarter(·, ·)

Vocabulary: A collection of constant-names,
function-names,
predicate-names.

Another example of a vocabulary:

one constant-name: **a**

two function-names: Next(·), Combine(·, ·)

one predicate-name: IsPrior(·, ·)

Example (well-formed) “sentences”:

$$\exists x\,(\mathrm{Next}(x)=\mathbf{a})$$

$$\forall x\,\forall y\,(\mathrm{IsPrior}(x,\mathrm{Combine}(\mathbf{a},y))) \rightarrow (\mathrm{Next}(x)=y))$$

$$(\forall x\,\mathrm{IsPrior}(x,\mathrm{Next}(x))) \rightarrow (\mathrm{Next}(\mathbf{a})=\mathrm{Next}(\mathbf{a}))$$

# Sorts/Type and Scope

Domain can be partitioned into sorts - a:boy b:girl

**Sorted Logic -** $\forall x$:boy P($x$)
Unsorted logic - $\forall x$: $x \in$ Boy $\rightarrow$ P($x$)

**Scope:**

$$\forall x.\ \overbrace{\exists\, y,z.\ \underbrace{x^2 = y^2 + z^2}}$$

Let’s talk about **TRUTH**.

# $\exists x\,(\text{Next}(x)=\text{Combine}(\mathbf{a},\mathbf{a}))$

Q: Is this sentence true?

A: The question does not make sense.

Whether or not this sentence is true depends on the interpretation of the vocabulary.

---

**Interpretation:**

Informally, says what objects are and what the vocabulary means.

# $\exists x\,(\text{Next}(x)=\text{Combine}(\mathbf{a},\mathbf{a}))$

Q: Is this sentence true?

A: The question does not make sense.

Whether or not this sentence is true depends on the interpretation of the vocabulary.

---

**Interpretation:**

Specifies a nonempty set ("universe") of objects.

Maps each constant-name to a specific object.

Maps each predicate-name to an actual predicate.

Maps each function-name to an actual function.

$\exists x\ (\text{Next}(x)=\text{Combine}(\mathbf{a},\mathbf{a}))$

Interpretation #1:

- Universe = all strings of 0’s and 1’s
- **a** = 1001
- Next(x) = x0
- Combine(x,y) = xy
- IsPrior(x,y) = **True** iff x is a prefix of y

For this interpretation,
the sentence is… **…False**

$\exists x\ (\text{Next}(x)=\text{Combine}(\mathbf{a},\mathbf{a}))$

Interpretation #2:

- Universe = integers
- **a** = 0
- Next(x) = x+1
- Combine(x,y) = x+y
- IsPrior(x,y) = **True** iff x < y

For this interpretation, the sentence is… **…True**

(x = −1)

# $\exists x\ (Next(x)=Combine(\mathbf{a},\mathbf{a}))$

## Interpretation #2:

- Universe = positive integers
- **a** = 0
- Next(x) = x+1
- Combine(x,y) = x+y
- IsPrior(x,y) = **True** iff x < y

For this interpretation,
the sentence is… **…False**

# Satisfiability / Tautology

Interpretation **I** satisfies sentence S:

**I** [S] = **T**

S is satisfiable:

there exists **I** such that **I** [S] = **T**

S is unsatisfiable:

**I** [S] = **F** for all **I**

S is a tautology:

**I** [S] = **T** for all **I**

# All sentences in a given vocabulary

unsatisfiable

$\exists x\ \neg(\mathrm{Next}(x)=\mathrm{Next}(x))$

satisfiable

$\exists x\ (\mathrm{Next}(x)=\mathrm{Combine}(\mathbf{a},\mathbf{a}))$

tautology

$(\forall x(x=\mathbf{a}))\rightarrow(\mathrm{Next}(\mathbf{a})=\mathbf{a})$

Tautology: automatically true,
for ‘purely logical’ reasons

Unsatisfiable: automatically false,
for purely logical reasons

Satisfiable (but not a tautology):

truth value depends
on the interpretation
of the vocabulary

$(\exists y\ \forall x\ (x=\text{Next}(y))) \rightarrow (\forall w\ \forall z\ (w=z))$

**Problem 1:** Show this is satisfiable.

Let's pick this interpretation:

Universe = integers, Next(y) = y+1.

Now $(\exists y\ \forall x\ (x=\text{Next}(y)))$ means

"there's an integer y such that every integer = y+1".

That's **False**!

So the whole sentence becomes **True**.

Hence the sentence **is satisfiable.**

$(\exists y\ \forall x\ (x{=}Next(y))) \rightarrow (\forall w\ \forall z\ (w{=}z))$

**Problem 2:** Is it a tautology?

There is no “truth table method”.

You can’t enumerate all possible interpretations!

It **seems like** you have to use some cleverness…

$(\exists y\ \forall x\ (x=Next(y))) \rightarrow (\forall w\ \forall z\ (w=z))$

**Problem 2:** Is it a tautology?

**Solution:** Yes, it is a tautology!

**Proof:** Let **I** be any interpretation.

If **I** $[\exists y\ \forall x\ (x=Next(y))]$ = **F**,

then the sentence is **True**.

If **I** $[\exists y\ \forall x\ (x=Next(y))]$ = **T**,

then every object equals Next(y).

In that case, **I** $[\forall w\ \forall z\ (w=z)]$ = **T**.

So no matter what, **I** [the sentence] = **T**.

$$(\exists y\ \forall x\ (x=\mathrm{Next}(y))) \rightarrow (\forall w\ \forall z\ (w=z))$$

**Problem 2:** Is it a tautology?

Hmm… It’s really a shame
that there’s no truth table method.

Is there **any** “mechanical method”??

# More Inference Rules

∀ introduction

$$\frac{\overline{a\ \text{var}} \\ \vdots \\ P(a)\ \text{true}}{\forall x.\ P(x)\ \text{true}}$$

∃ introduction

$$\frac{a\ \text{var} \qquad P(a)\ \text{true}}{\exists x.\ P(x)\ \text{true}}$$

∃ elimination

$$\frac{\exists x.\ P(x)\ \text{true} \qquad \begin{array}{c}\overline{a\ \text{var}} \quad \overline{P(a)\ \text{true}} \\ \vdots \\ C\ \text{true}\end{array}}{C\ \text{true}}$$

∀ elimination

$$\frac{a\ \text{var} \qquad \forall x.\ P(x)\ \text{true}}{P(a)\ \text{true}}$$

# Prove $\forall x.\, \exists y.\, y>x$ over natural number

$$\dfrac{x \text{ var}}{x+1 \text{ var}} \qquad \dfrac{\vdots}{\forall x.\, x+1>x \text{ true}}$$

$$\dfrac{\dfrac{\dfrac{\dfrac{}{a \text{ var}}}{a+1 \text{ var}} \qquad \dfrac{\dfrac{}{a \text{ var}} \quad \dfrac{\vdots}{\forall x.\, x+1>x \text{ true}}}{a+1>a \text{ true}}\ \forall \text{ elimination}}{\exists y.\, y>a}\ \exists \text{ introduction}}{\forall x.\, \exists y.\, y>x}\ \forall \text{ introduction}$$

# Checking tautologies

**Consequence:**

There is a purely mechanical (algorithmic) way to verify that a given S is a tautology.

Just brute-force search for the shortest proof in Deductive Calculus!

# Logical entailment

"Is S a tautology of $1^{st}$ order logic?"

moderately interesting

"Assuming 'axioms' $A_1, \ldots, A_m$,
is S a logical consequence ('theorem')?"

more typical kind of
thing to be interested in

# Temporal logic

## Propositional/FO logics have just one static state where formulae are evaluated

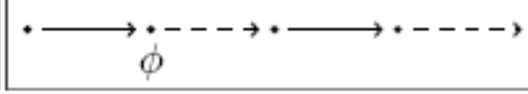
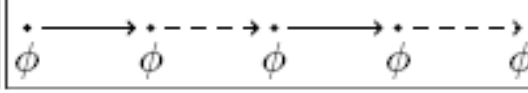
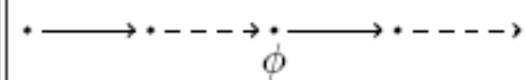
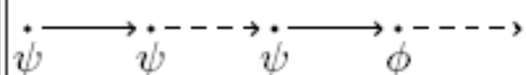
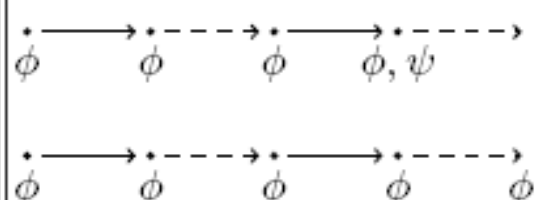
E.g.:
k stands for "it is snowing"
Is k true? No, but, only for today.

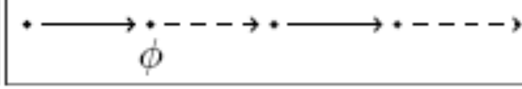
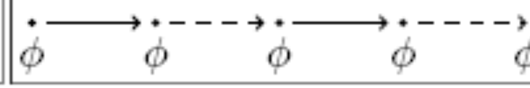
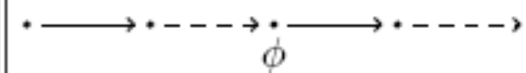
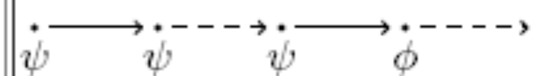
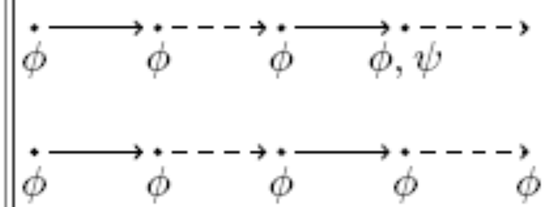
How to say:
It will snow someday in future.
It will snow everyday in future

Actually, it is possible to say the above in FOL, but, there is a much more elegant logic, which is also computationally easier to reason about

# Temporal Logic Operators

## Temporal operators:

| Textual | Symbolic† | Explanation | Diagram |
|---|---|---|---|
| Unary operators: | | | |
| X $\phi$ | $\bigcirc\phi$ | neXt: $\phi$ has to hold at the next state. |  |
| G $\phi$ | $\Box\phi$ | Globally: $\phi$ has to hold on the entire subsequent path. |  |
| F $\phi$ | $\Diamond\phi$ | Finally: $\phi$ eventually has to hold (somewhere on the subsequent path). |  |
| Binary operators: | | | |
| $\psi$ U $\phi$ | $\psi\mathcal{U}\phi$ | Until: $\psi$ has to hold *at least* until $\phi$, which holds at the current or a future position. |  |
| $\psi$ R $\phi$ | $\psi\mathcal{R}\phi$ | Release: $\phi$ has to be true until and including the point where $\psi$ first becomes true; if $\psi$ never becomes true, $\phi$ must remain true forever. |  |

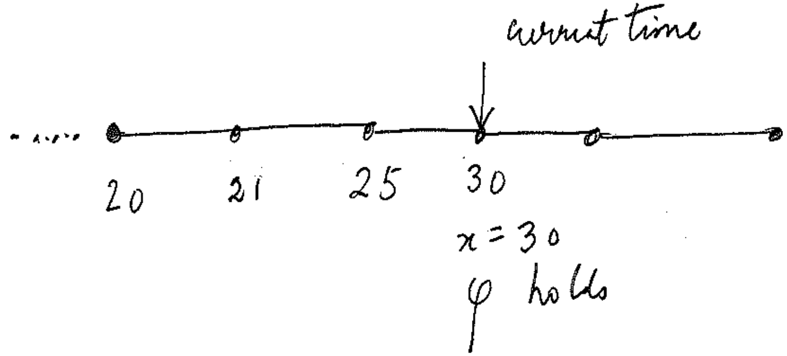
| Textual | Symbolic† | Explanation | Diagram |
|---|---|---|---|
| Unary operators: | | | |
| X $\phi$ | $\bigcirc\phi$ | **neXt**: $\phi$ has to hold at the next state. |  |
| G $\phi$ | $\Box\phi$ | **Globally**: $\phi$ has to hold on the entire subsequent path. |  |
| F $\phi$ | $\Diamond\phi$ | **Finally**: $\phi$ eventually has to hold (somewhere on the subsequent path). |  |
| Binary operators: | | | |
| $\psi$ U $\phi$ | $\psi\mathcal{U}\phi$ | **Until**: $\psi$ has to hold *at least* until $\phi$, which holds at the current or a future position. |  |
| $\psi$ R $\phi$ | $\psi\mathcal{R}\phi$ | **Release**: $\phi$ has to be true until and including the point where $\psi$ first becomes true; if $\psi$ never becomes true, $\phi$ must remain true forever. |  |

$FG\,\phi$, $GF\,\phi$

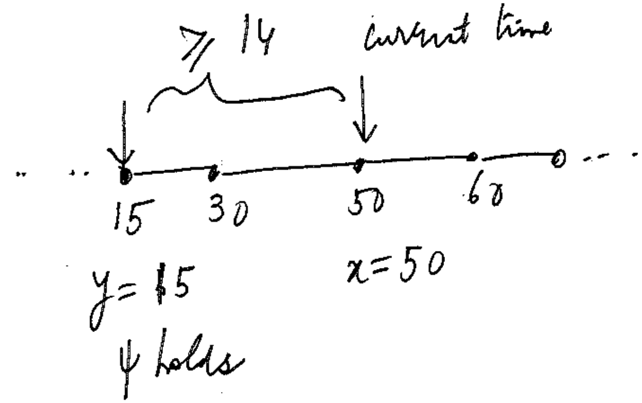
**Is $G\,\phi$ equivalent to $\neg F \neg \phi$**

$\downarrow x.\, \varphi$

At the current time $\varphi$ holds




$\downarrow x.\, (\diamondminus \downarrow y.\, ((x-y) \geq 14 \wedge \psi))$




Freeze Quantifier

**Acknowledgement: Slides are from last year's recitation**

**Acknowledgement[2]: Many Slides are from 15251**