Temporal Logic

[Syntax and Semantics]

Michael Fisher
Department of Computer Science, University of Liverpool, UK

[MFisher@liverpool.ac.uk]

An Introduction to Practical Formal Methods Using Temporal Logic

PTL Syntax

Formulae in PTL are constructed from the following.

- A finite set of propositional symbols, PROP, such as p, q, r, *trigger*, *terminate_condition2*, *lunch*, ...
- Propositional connectives: **true**, **false**, $\neg$, $\vee$, $\wedge$, $\Rightarrow$.
- Temporal connectives: $\bigcirc$, $\lozenge$, $\square$, **start**, U, and W.
- Parentheses, '(' and ')', used to avoid ambiguity.

The set of well-formed formulae of PTL, denoted by WFF, is now inductively defined as follows.

- PROP $\subseteq$ WFF, and **true**, **false** and **start** are in WFF.
- If φ and ψ are in WFF, then so are

$$\neg\varphi \quad \varphi \vee \psi \quad \varphi \wedge \psi \quad \varphi \Rightarrow \psi \quad (\varphi)$$
$$\lozenge\varphi \quad \square\varphi \quad \varphi U \psi \quad \varphi W \psi \quad \bigcirc\varphi.$$

Examples of Syntax

The following are all legal WFF of PTL

$$p\,\mathcal{U}(q \wedge \Diamond r) \qquad a \Rightarrow \Box \bigcirc (b\,\mathcal{W} c) \qquad (f \wedge \bigcirc g)\,\mathcal{U} \Diamond \Box \neg h$$

But the following are ***not***

$$p \Diamond q \qquad (\mathcal{U} r) \qquad a \Rightarrow \Box b \bigcirc c$$

Semantic Structures (1)

Models of PTL are formally

$$Model \;=\; \langle S, R, \pi \rangle$$

where

- S is the set of *moments* in time (accessible worlds),
- R is the *temporal accessibility relation* (linear, discrete, finite past), and
- $\pi : S \mapsto \mathbb{P}PROP$, a *propositional valuation*, mapping each moment/world to a set of propositions (i.e. those that are true in that moment/world).

Semantic Structures (2)

A linear, discrete relation, such as R, is isomorphic to $\mathbb{N}$. So, this is often reduced to

$$\mathit{Model} \;=\; \langle \mathbb{N}, \pi \rangle$$

where

- $\pi : \mathbb{N} \mapsto \mathbb{P}\mathit{PROP}$ maps each moment in time to a set of propositions .

And, still further to

$$\mathit{Model} \;=\; s_0, s_1, s_2, s_3, \ldots$$

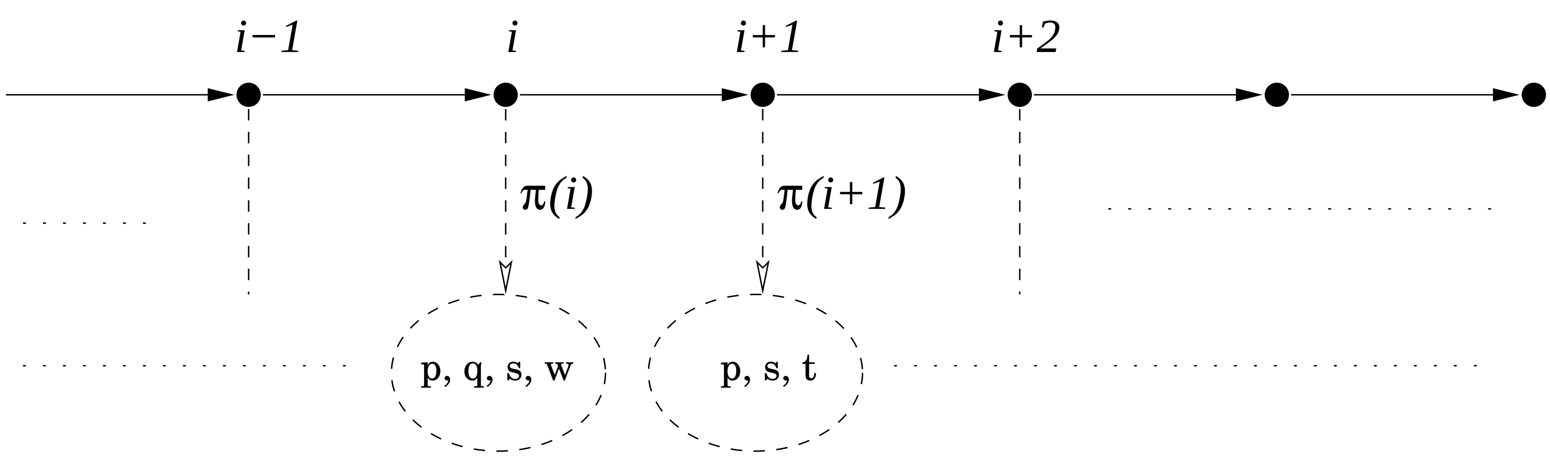
where each s_i is a set of propositions.

But: We will generally use the $\mathit{Model} \;=\; \langle \mathbb{N}, \pi \rangle$ variety.

We will use the

$$\mathcal{M} = \langle \mathbb{N}, \pi \rangle$$

semantic basis, which can be viewed as



The semantics of a temporal formula is provided by an interpretation relation

$$\models : (\mathit{Model} \times \mathbb{N}) \to \mathbb{B}$$

For a model, M, temporal index, i, and formula, φ, then

$$\langle M, i \rangle \models \varphi$$

is true if φ is satisfied at moment i within model M.

The way the interpretation relation is defined provides the semantics for the logic.

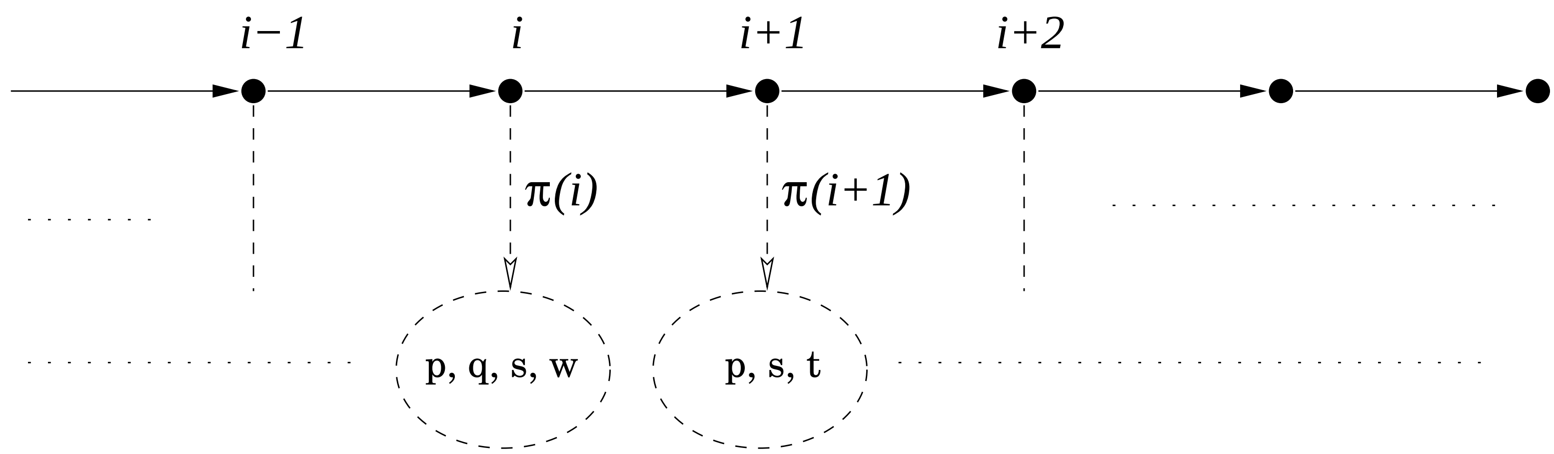
Semantics of Propositions

We begin with the semantics of basic propositions:

$$\langle M, i\rangle \models p \quad \text{iff} \quad p \in \pi(i) \qquad (\text{for } p \in \text{PROP})$$

i.e. look up the proposition in the model provided to see whether it is satisfied or not.

<u>Recall:</u>



Semantics of Classical Operators

Next we consider the standard classical operators.

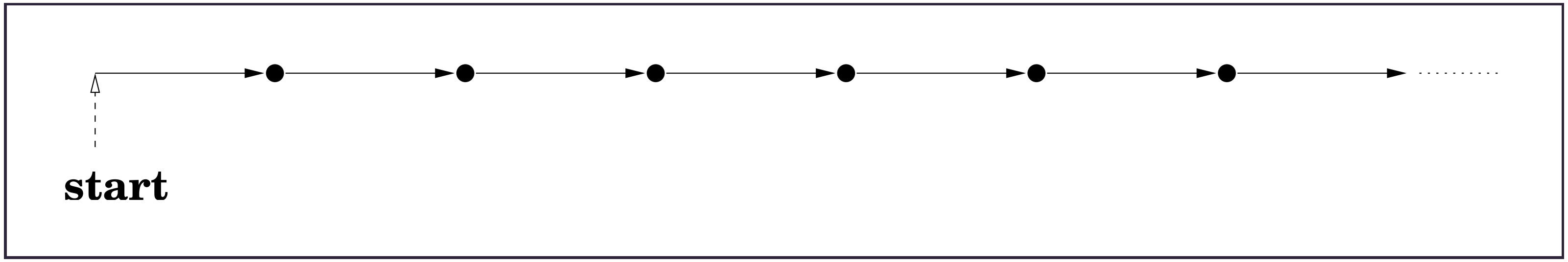
$\langle M, i \rangle \models \neg\varphi$	iff	it is not the case that $\langle M, i \rangle \models \varphi$
$\langle M, i \rangle \models \varphi \wedge \psi$	iff	$\langle M, i \rangle \models \varphi$ and $\langle M, i \rangle \models \psi$
$\langle M, i \rangle \models \varphi \vee \psi$	iff	$\langle M, i \rangle \models \varphi$ or $\langle M, i \rangle \models \psi$

And so on....

Temporal Operators: Start

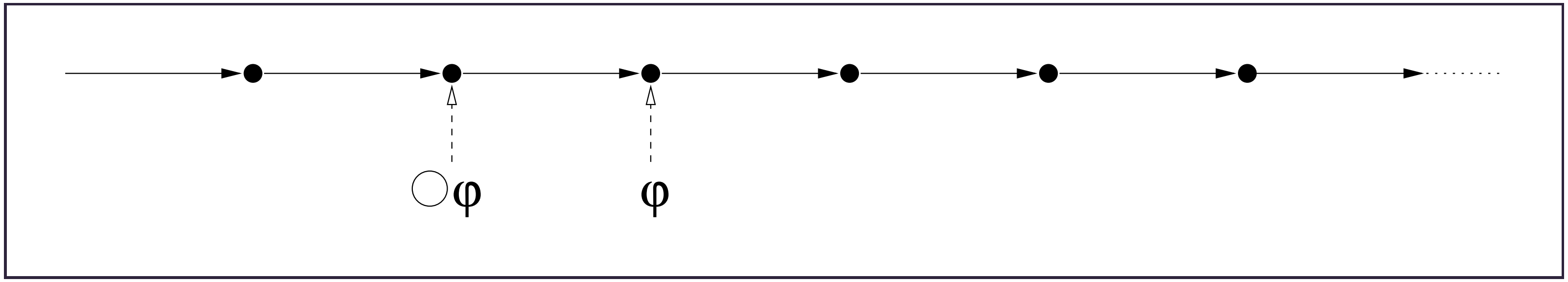
$$\langle M, i \rangle \models \textbf{start} \quad \text{iff} \quad (i = 0)$$

Only ever satisfied at the "beginning of time".



Provides a constraint on the *next* moment in time.

$$\langle M, i \rangle \models \bigcirc \varphi \quad \text{iff} \quad \langle M, i+1 \rangle \models \varphi$$



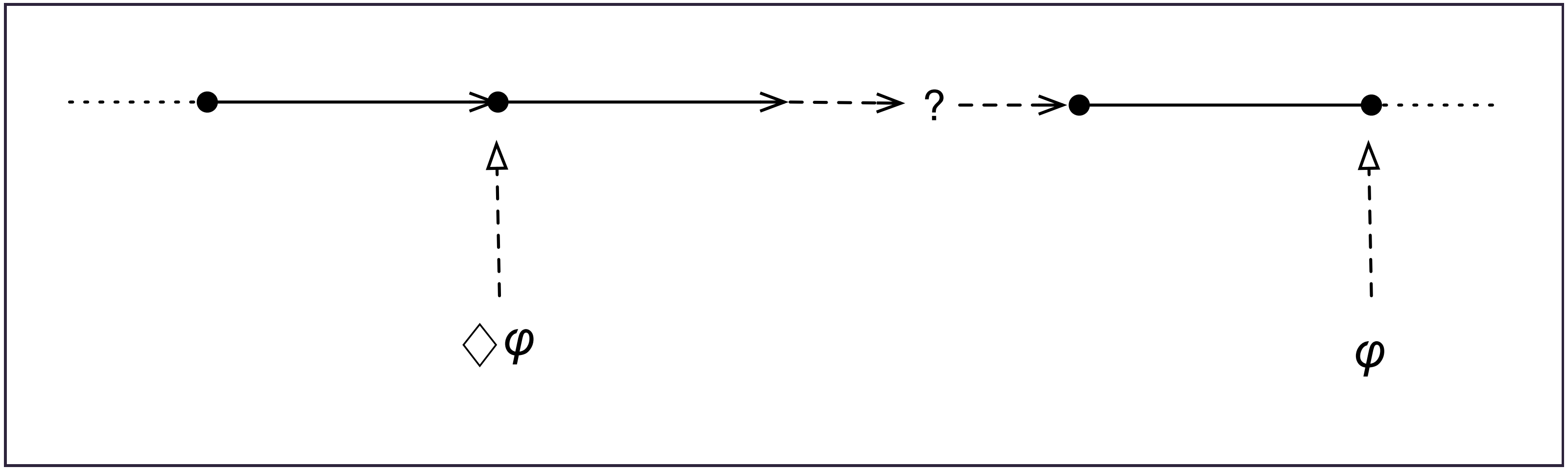
Examples

- $(sad \wedge \neg rich) \Rightarrow \bigcirc sad$
- $hop \wedge \bigcirc skip \wedge \bigcirc\bigcirc jump$
- $(x\_equals\_1 \wedge added\_3) \Rightarrow \bigcirc(x\_equals\_4)$

Temporal Operators: Sometime

Provides a constraint on the future — we can not be sure *when* φ will be true, only that it *will* eventually occur.

$$\langle M, i \rangle \models \Diamond\varphi \quad \text{iff} \quad \text{there exists } j \geq i \text{ such that } \langle M, j \rangle \models \varphi$$



Temporal Operators: Sometime^{+}

There is a choice in the semantics of 'sometime' about whether to take $j \geq i$ or $j > i$; an alternative operator can be defined as follows:

$$\langle M, i \rangle \models \lozenge^{+}\varphi \quad \text{iff} \quad \text{there exists } j > i \text{ such that } \langle M, j \rangle \models \varphi$$

Clearly: $\quad \lozenge\varphi \Leftrightarrow (\varphi \vee \lozenge^{+}\varphi)$

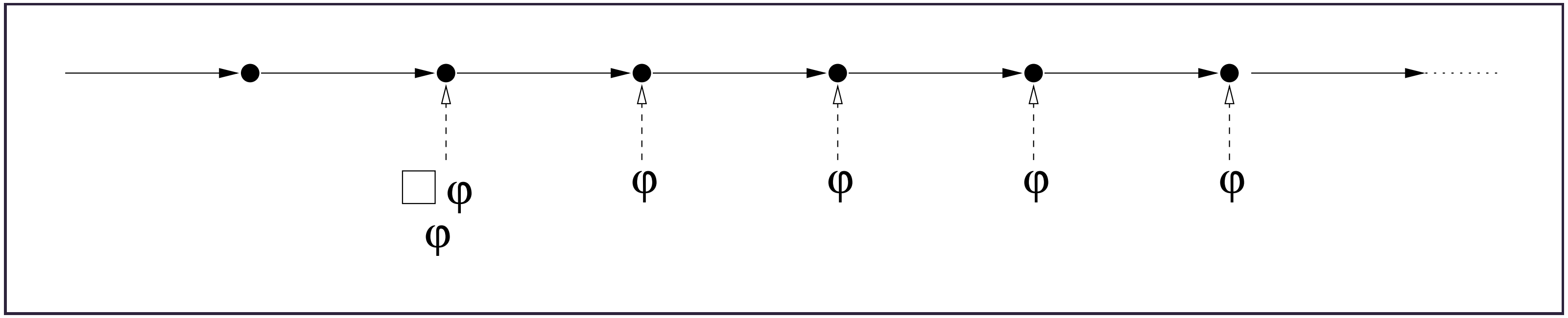
Examples:

- $(\neg \mathit{resigned} \wedge \mathit{sad}) \Rightarrow \lozenge \mathit{famous}$
- $(\lozenge \mathit{accident}) \Rightarrow (\bigcirc \mathit{buy\_insurance})$
- $\mathit{sad} \Rightarrow \lozenge \mathit{happy}$
- $\mathit{is\_monday} \Rightarrow \lozenge^{+} \mathit{is\_friday}$

Temporal Operators: Always

Provides *invariant* properties (c.f. safety properties).

$$\langle M, i \rangle \models \Box\varphi \quad \text{iff} \quad \text{for all } j.\ \text{if } (j \geq i) \text{ then } \langle M, j \rangle \models \varphi$$



Examples:

- $lottery\_win \Rightarrow \Box rich$
- $born \Rightarrow \bigcirc\Box(age > 0)$
- $\Box(stop\_msg \Rightarrow \bigcirc\Box\neg executing)$

Example

Why do we term $\square \lozenge p$, "infinitely often P"?

Let us take the semantics of $\square \lozenge p$ at a particular moment i in model M:

$$\langle M, i \rangle \models \square \lozenge p \quad \text{iff} \quad \text{for all } j.\ \text{if } (j \geq i) \text{ then } \langle M, j \rangle \models \lozenge p$$

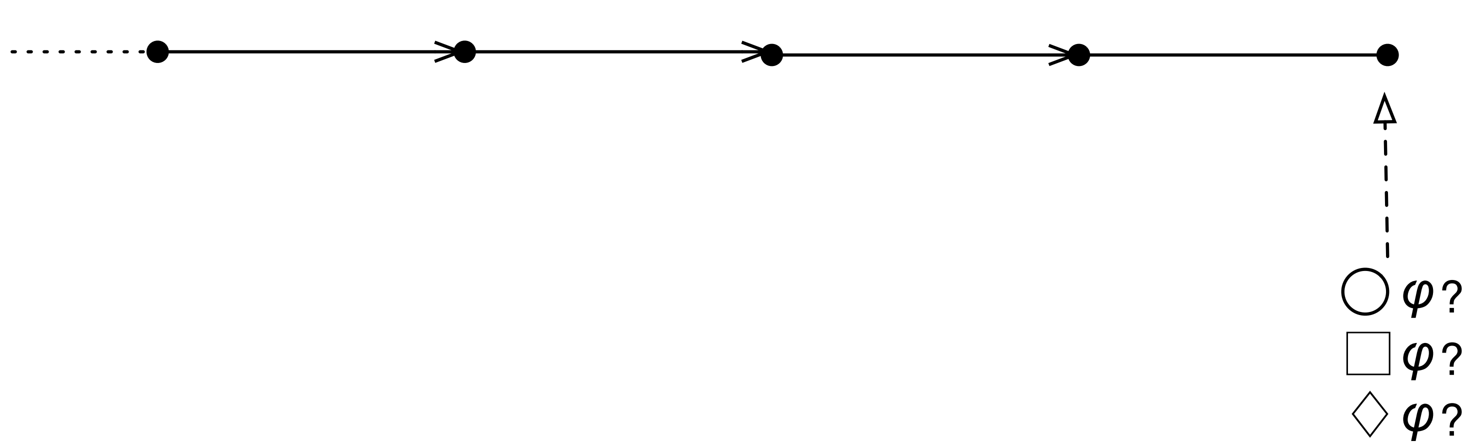
$$\text{iff} \quad \text{for all } j.\ \text{if } (j \geq i) \text{ then there exists } k.\ (k \geq j) \wedge \langle M, k \rangle \models \varphi$$

Now, choose a j, and a $k \geq j$ where $\langle M, k \rangle \models \varphi$

As we quantify over all j's, then we can now choose another j, such that $j > k$, which requires us to satisfy φ again in the future, and so on....

Aside: No Future

Rather than using $\mathbb{N}$ as our underlying model of time, what if we use a linear, discrete sequence, but with a *finite* length:



Semantics of the temporal operators must be modified.

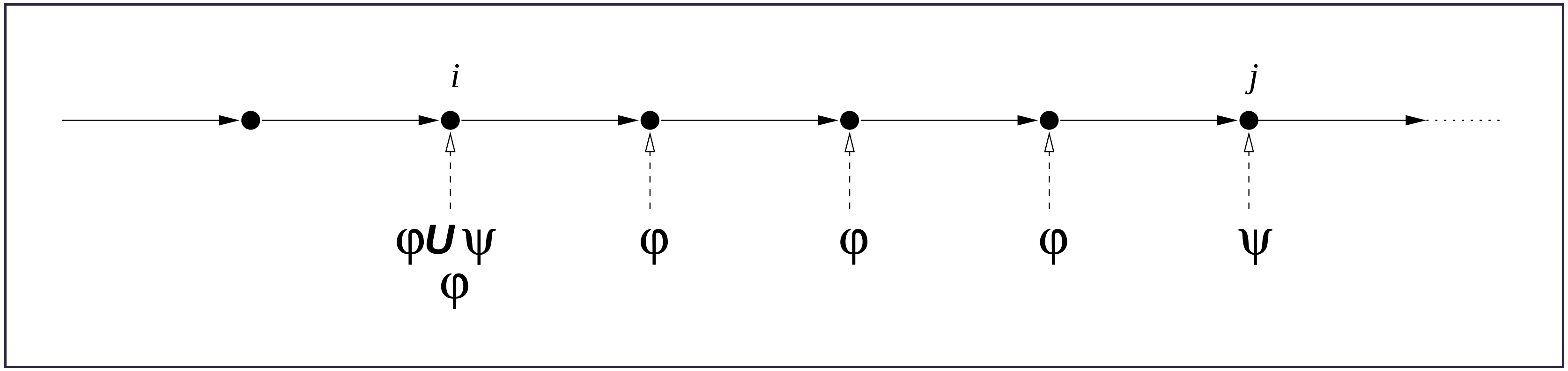
For example, the '$\bigcirc$' operator typically defaults to **true** if there is no 'next' moment. So, '$\bigcirc$**false**' is actually only satisfied at the last state in a finite sequence!

See also: bounded approximations and related techniques.

Temporal Operators: Until

A property persists until a point occurs (which is guaranteed to occur) where another property becomes true.

$\langle M, i\rangle \models \varphi U \psi$ iff there exists j. $(j \geq i)$ and $\langle M, j\rangle \models \psi$ and for all k. if $(j > k \geq i)$ then $\langle M, k\rangle \models \varphi$



Examples:

- $start\_lecture \Rightarrow talk\, U\, end\_lecture$
- $born \Rightarrow living\, U\, dead$

Temporal Operators: Unless (1)

Unless: as until, except that the 'ψ' point is not *guaranteed* potentially to occur and so the persistent property can persist forever.

$$\langle M, i \rangle \models \varphi \mathcal{W} \psi \quad \textbf{iff} \quad \langle M, i \rangle \models \varphi \mathcal{U} \psi \textbf{ or } \langle M, i \rangle \models \square \varphi$$

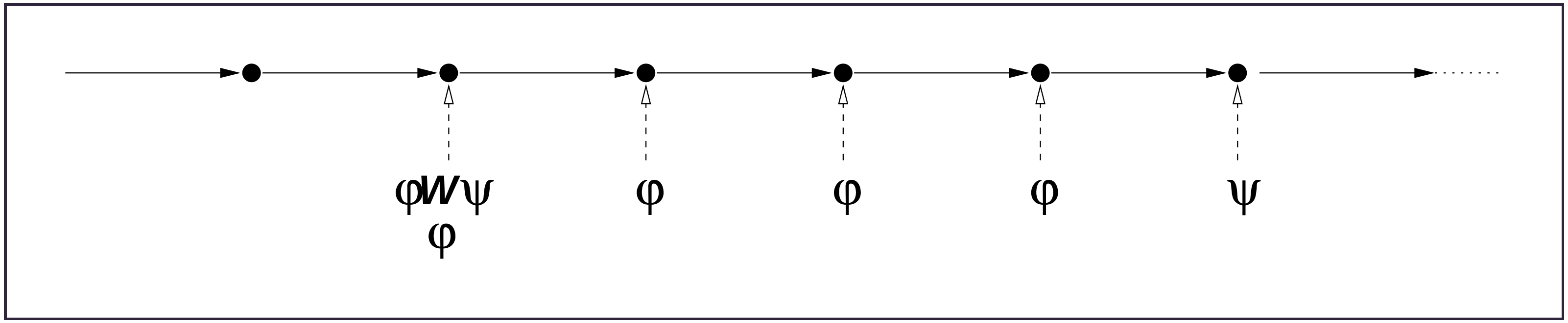
Examples:

$$stay\_in\_room \, \mathcal{W} fire\_alarm$$

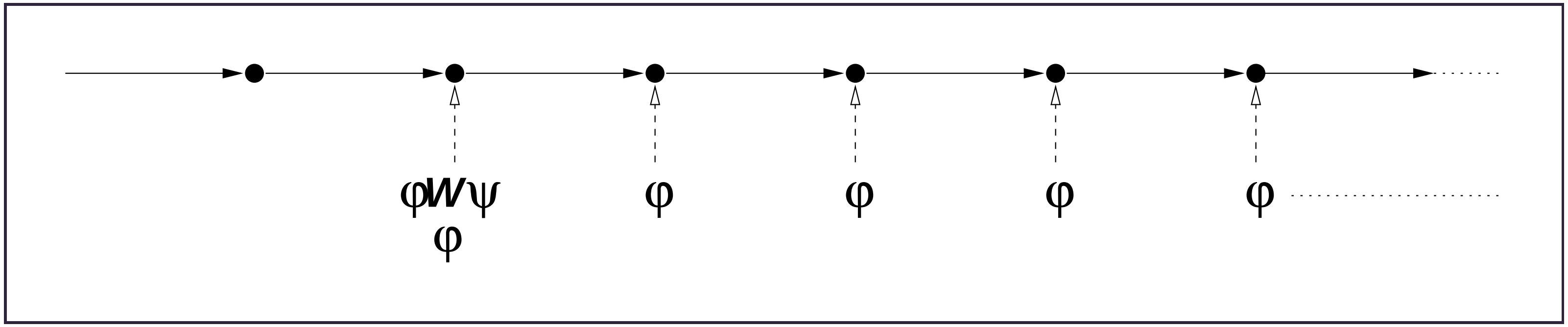
$$commence \Rightarrow (executing \, \mathcal{W} stop\_msg)$$

Temporal Operators: Unless (2)

Either:



or:



Useful Interactions

By their semantic definitions:

$$a\,\mathcal{U}\,b \;\Leftrightarrow\; ((a\,\mathcal{W}\,b) \wedge \Diamond b)$$
$$c\,\mathcal{W}\,d \;\Leftrightarrow\; ((c\,\mathcal{U}\,d) \vee \Box c)$$

Of course:

$$\neg \Box r \;\Leftrightarrow\; \Diamond \neg r$$

Less obviously:

$$\neg(e\,\mathcal{U}\,f) \;\Leftrightarrow\; (\neg f)\,\mathcal{W}\,(\neg f \wedge \neg e)$$
$$\neg(p\,\mathcal{W}\,q) \;\Leftrightarrow\; (\neg q)\,\mathcal{U}\,(\neg p \wedge \neg q)$$

But, happily, at least in infinite and linear models,

$$\neg \bigcirc w \;\Leftrightarrow\; \bigcirc \neg w$$