Linear and Branching Temporal Logics[1]

Frits Vaandrager

Institute for Computing and Information Sciences
Radboud University Nijmegen
fvaan@cs.ru.nl

June 25, 2015

[1] Based on slides Julien Schmaltz

Agenda coming lectures ...

- Part I: Linear time temporal logic (LTL)
- Part II: Model checking LTL
- Part III: Branching time temporal logic (CTL)
- Part IV: Expressiveness of CTL vs LTL
- Part V: Model checking CTL
- Part VI: Binary decision diagrams and symbolic model checking
- Part VII: Partial order reduction

Agenda for today

- Course intro
- Linear time temporal logic

Part I

Linear Time Logic

Principles: next time or until ...

- Temporal logic = logic about time
- Abstract notion of (discrete) time = sequence of events
- Two principal operators
  - next A: at the next "time" A holds
  - A until B: A holds until B holds
- Application to software/hardware specification
  - At the next clock cycle, the request signal must be high
  - The request signal must be high until the acknowledge is high
  - Eventually the request signal must become low again
  - The arbiter always grants at most one request
  - The elevator should never travel when the doors are open

Syntax

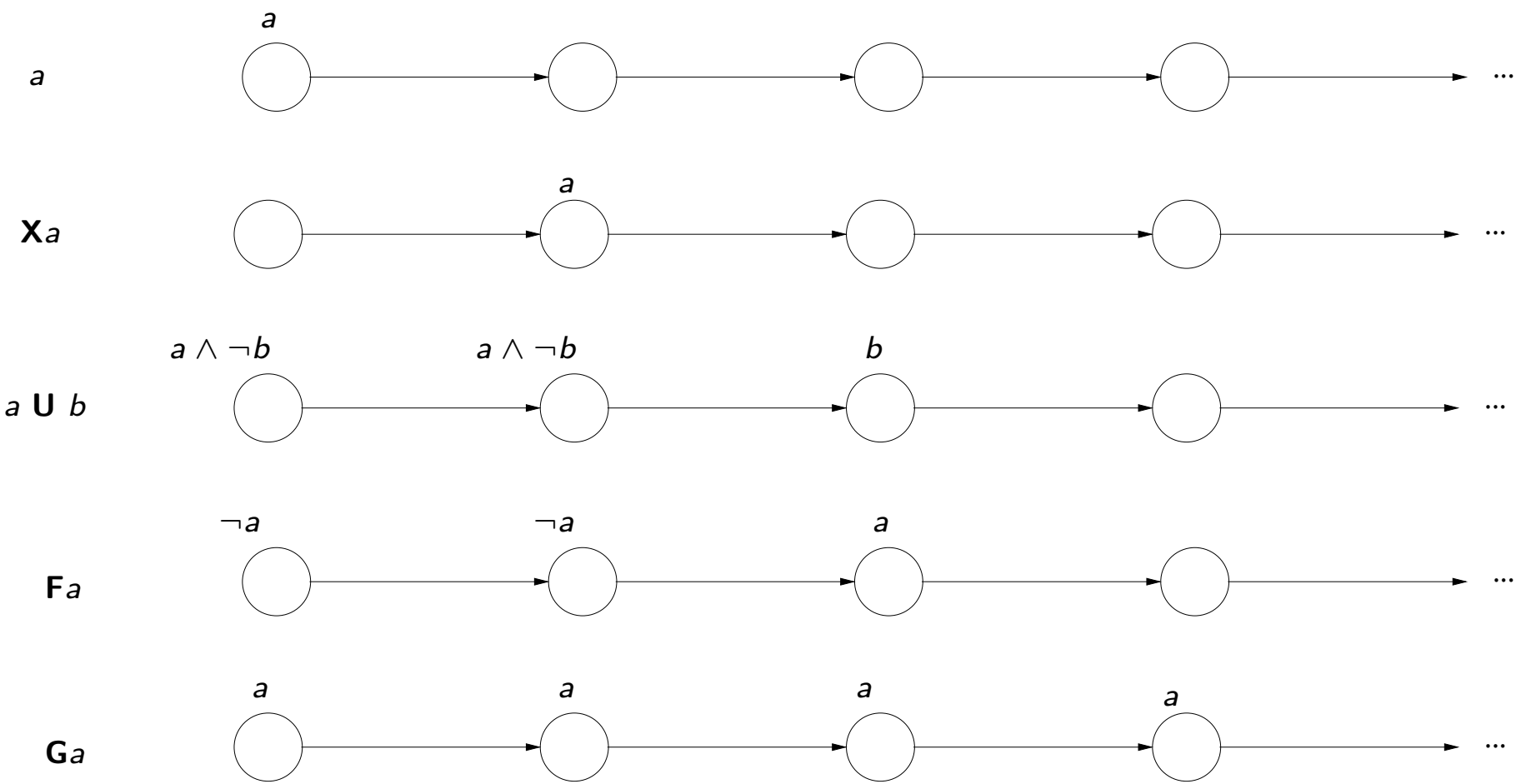
modal logic over infinite sequences [Pnueli 1977]

- Propositional logic
  - Atomic propositions: $a \in AP$
  - Boolean connectives: $\neg a$ and $\varphi \wedge \psi$
- Temporal operators
  - "Next" noted X φ or $\bigcirc \varphi$
  - "Until" noted φ U ψ or $\varphi \cup \psi$

Derived operators

- $\varphi \vee \psi \equiv \neg(\neg\varphi \wedge \neg\psi)$
- $\varphi \Rightarrow \psi \equiv \neg\varphi \vee \psi$
- $\varphi \Leftrightarrow \psi \equiv (\varphi \Rightarrow \psi) \wedge (\psi \Rightarrow \varphi)$
- True (or $\top$) $\equiv \varphi \vee \neg\varphi$
- False (or $\bot$) $\equiv \neg\top$
- $\mathbf{F}\varphi$ (also noted $\Diamond\varphi$) $\equiv \top$ **U** φ "eventually φ"
- $\mathbf{G}\varphi$ (also noted $\Box\varphi$) $\equiv \neg\mathbf{F}\neg\varphi$ "globally φ"

Intuitive semantics



Example: traffic lights

- Whenever the light is red, it cannot become green immediately

$$\mathbf{G}(red \Rightarrow \neg \mathbf{X} green)$$

- The traffic light eventually becomes green

$$\mathbf{F} green$$

- Once red, the light eventually becomes green

$$\mathbf{G}(red \Rightarrow \mathbf{F} green)$$

- After being red, the light goes yellow and then eventually becomes green

$$\mathbf{G}(red \Rightarrow \mathbf{X}(red \mathbf{U}(yellow \wedge \mathbf{X}(yellow \mathbf{U} green))))$$

Classification of LTL Properties

- Reachability
  - negated reachability: $\mathbf{F}\neg\psi$
  - conditional reachability: $\varphi\mathbf{U}\psi$
  - reachability from any state: not expressible
- Safety
  - simple safety: $\mathbf{G}\neg\psi$
  - conditional safety (weak until): $(\varphi\mathbf{U}\psi) \vee \mathbf{G}\varphi$
- Liveness: $\mathbf{G}(\varphi \Rightarrow \mathbf{F}\psi)$ and others
- Fairness: $\mathbf{GF}\psi$ and others

Semantics over words

A word σ is an infinite sequence of sets of atomic propositions.
LTL property ϕ defines set of words for which the property is true.
$\text{Words}(\varphi) = \{\sigma \in (2^{AP})^\omega \mid \sigma \models \varphi\}$

$$
\begin{array}{lcll}
\sigma & \models & a & \text{iff } a \in A_0 \text{ (or } A_0 \models a) \\
\sigma & \models & \varphi \wedge \psi & \text{iff } \sigma \models \varphi \text{ and } \sigma \models \psi \\
\sigma & \models & \neg\varphi & \text{iff } \sigma \not\models \varphi \\
\sigma & \models & \mathbf{X}\varphi & \text{iff } \sigma[1..] = A_1A_2A_3\ldots \models \varphi \\
\sigma & \models & \varphi\mathbf{U}\psi & \text{iff } \exists j \geq 0 : \sigma[j..] \models \psi \text{ and } \sigma[i..] \models \varphi, 0 \leq i < j
\end{array}
$$

for $\sigma = A_0A_1A_2\ldots$, $\sigma[i..] = A_iA_{i+1}A_{i+2}\ldots$ is suffix of σ from index i

More semantics ...

$$\sigma \models \mathbf{F}\psi \quad \text{iff}$$

More semantics ...

$$\sigma \models \mathbf{F}\psi \quad \text{iff} \quad \exists j \geq 0 : \sigma[j..] \models \psi$$

More semantics ...

$$\sigma \models \mathbf{F}\psi \quad \text{iff} \quad \exists j \geq 0 : \sigma[j..] \models \psi$$
$$\sigma \models \mathbf{G}\psi \quad \text{iff}$$

More semantics ...

$$\sigma \models \mathbf{F}\psi \quad \text{iff} \quad \exists j \geq 0 : \sigma[j..] \models \psi$$
$$\sigma \models \mathbf{G}\psi \quad \text{iff} \quad \forall j \geq 0 : \sigma[j..] \models \psi$$

More semantics ...

$$
\begin{array}{lcll}
\sigma & \models & \mathbf{F}\psi & \text{iff} \quad \exists j \geq 0 : \sigma[j..] \models \psi \\
\sigma & \models & \mathbf{G}\psi & \text{iff} \quad \forall j \geq 0 : \sigma[j..] \models \psi \\
\sigma & \models & \mathbf{GF}\psi & \text{iff}
\end{array}
$$

More semantics ...

$$
\begin{array}{lcll}
\sigma & \models & \mathbf{F}\psi & \text{iff} \quad \exists j \geq 0 : \sigma[j..] \models \psi \\
\sigma & \models & \mathbf{G}\psi & \text{iff} \quad \forall j \geq 0 : \sigma[j..] \models \psi \\
\sigma & \models & \mathbf{GF}\psi & \text{iff} \quad \forall j \geq 0, \exists i \geq j : \sigma[i..] \models \psi
\end{array}
$$

More semantics ...

$$
\begin{array}{lcll}
\sigma & \models & \mathbf{F}\psi & \text{iff} \quad \exists j \geq 0 : \sigma[j..] \models \psi \\
\sigma & \models & \mathbf{G}\psi & \text{iff} \quad \forall j \geq 0 : \sigma[j..] \models \psi \\
\sigma & \models & \mathbf{GF}\psi & \text{iff} \quad \forall j \geq 0, \exists i \geq j : \sigma[i..] \models \psi \\
\sigma & \models & \mathbf{FG}\psi & \text{iff}
\end{array}
$$

More semantics ...

$$
\begin{array}{lcll}
\sigma & \models & \mathbf{F}\psi & \text{iff} \quad \exists j \geq 0 : \sigma[j..] \models \psi \\
\sigma & \models & \mathbf{G}\psi & \text{iff} \quad \forall j \geq 0 : \sigma[j..] \models \psi \\
\sigma & \models & \mathbf{GF}\psi & \text{iff} \quad \forall j \geq 0, \exists i \geq j : \sigma[i..] \models \psi \\
\sigma & \models & \mathbf{FG}\psi & \text{iff} \quad \exists j \geq 0, \forall i \geq j : \sigma[i..] \models \psi
\end{array}
$$

Duality

From the semantics, we have $\neg \mathbf{F} \neg \varphi = \mathbf{G} \varphi$.

Proof.

$$\sigma \models \neg \mathbf{F} \neg \varphi$$

Duality

From the semantics, we have $\neg \mathbf{F} \neg \varphi = \mathbf{G} \varphi$.

Proof.

$$\sigma \models \neg \mathbf{F} \neg \varphi$$
$$\sigma \models \neg \exists j \geq 0 : \sigma[j..] \models \neg \varphi \quad \text{(Def. of } \mathbf{F}\text{)}$$

Duality

From the semantics, we have $\neg \mathbf{F} \neg \varphi = \mathbf{G} \varphi$.

Proof.

$$
\begin{aligned}
&\sigma \models \neg \mathbf{F} \neg \varphi \\
&\sigma \models \neg \exists j \geq 0 : \sigma[j..] \models \neg \varphi && \text{(Def. of } \mathbf{F}\text{)} \\
&\sigma \models \forall j \geq 0 : \sigma[j..] \models \varphi && \text{(Def. of } \neg\text{)}
\end{aligned}
$$

Duality

From the semantics, we have $\neg \mathbf{F} \neg \varphi = \mathbf{G} \varphi$.

Proof.

$$
\begin{aligned}
&\sigma \models \neg \mathbf{F} \neg \varphi \\
&\sigma \models \neg \exists j \geq 0 : \sigma[j..] \models \neg \varphi && \text{(Def. of } \mathbf{F}\text{)} \\
&\sigma \models \forall j \geq 0 : \sigma[j..] \models \varphi && \text{(Def. of } \neg\text{)} \\
&\sigma \models \mathbf{G} \varphi && \text{(Def. of } \mathbf{G}\text{)}
\end{aligned}
$$

Semantics over paths, states, and transition systems

Let $TS = (S, \Sigma, T, I, AP, L)$ be a transition system and let φ be an LTL formula over AP.

- An infinite path π of TS satisfies φ iff the trace of π satisfies φ:

$$\pi \models \varphi \qquad \text{iff} \qquad trace(\pi) \models \varphi$$

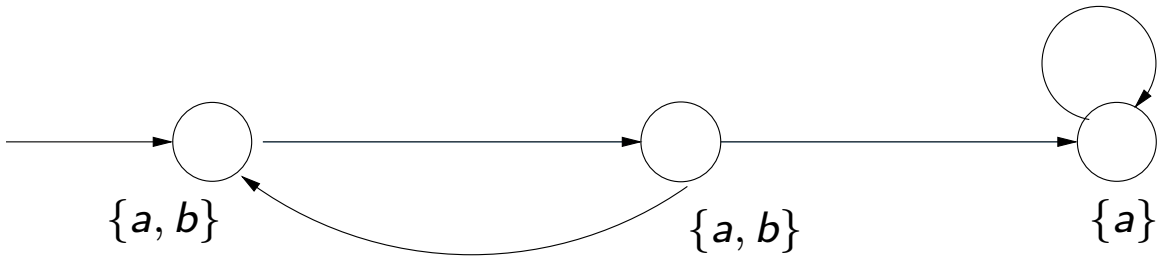
- A state $s \in S$ satisfies φ iff all paths from s satisfy φ:

$$s \models \varphi \qquad \text{iff} \qquad \forall \pi \in Paths(s) : \pi \models \varphi$$

- A transition system satisfies φ iff φ holds from all initial states:

$$TS \models \varphi \text{ iff } Traces(TS) \subseteq Words(\varphi) \text{ iff } \forall s_0 \in I : s_0 \models \varphi$$

Example



$TS \models \mathbf{G}a$

$TS \models \mathbf{X}(a \wedge b)$

$TS \models \mathbf{G}(\neg b \Rightarrow \mathbf{G}(a \wedge \neg b))$

$TS \not\models b\mathbf{U}(a \wedge \neg b)$

Semantics of negation

For paths, it holds $\pi \models \varphi$ iff $\pi \not\models \neg\varphi$ since:

$$Words(\neg\varphi) = (2^{AP})^{\omega} \setminus Words(\varphi)$$

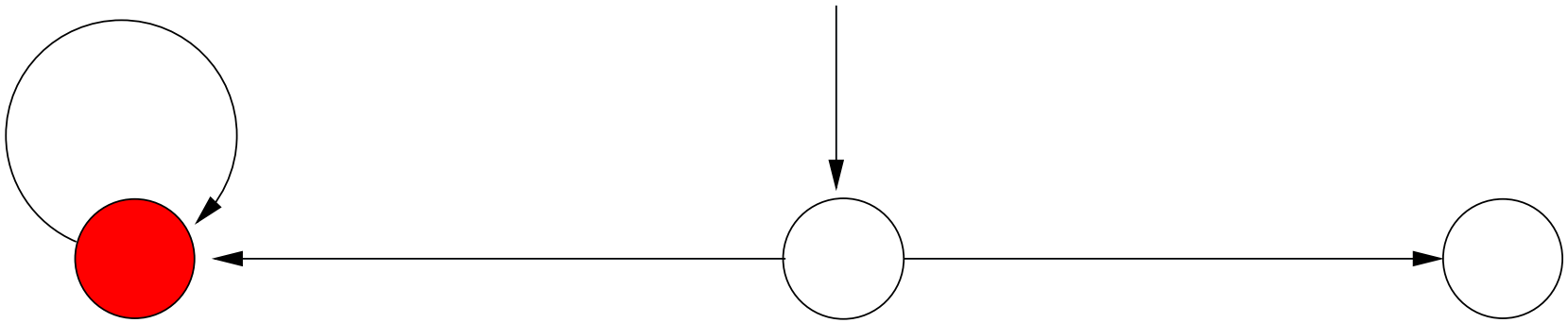
But: $TS \not\models \varphi$ and $TS \models \neg\varphi$ are not equivalent in general

We have: $TS \models \neg\varphi$ implies $TS \not\models \varphi$.

TS neither satisfies φ or $\neg\varphi$ if there are paths π_1 and π_2 such that $\pi_1 \models \varphi$ and $\pi_2 \models \neg\varphi$.

Example

A transition system for which $TS \not\models \mathbf{F}a$ and $TS \not\models \neg\mathbf{F}a$.



More dualities and idempotent laws

- Duality

$$\begin{aligned} \neg \mathbf{G}\varphi &\equiv \mathbf{F}\neg\varphi \\ \neg \mathbf{F}\varphi &\equiv \mathbf{G}\neg\varphi \\ \neg \mathbf{X}\varphi &\equiv \mathbf{X}\neg\varphi \end{aligned}$$

- Idempotency

$$\begin{aligned} \mathbf{GG}\varphi &\equiv \mathbf{G}\varphi \\ \mathbf{FF}\varphi &\equiv \mathbf{F}\varphi \\ \varphi\mathbf{U}(\varphi\mathbf{U}\psi) &\equiv \varphi\mathbf{U}\psi \\ (\varphi\mathbf{U}\psi)\mathbf{U}\psi &\equiv \varphi\mathbf{U}\psi \end{aligned}$$

Absorption and distributive laws

- Absorption

$$\begin{aligned} \mathbf{FGF}\varphi &\equiv \mathbf{GF}\varphi \\ \mathbf{GFG}\varphi &\equiv \mathbf{FG}\varphi \end{aligned}$$

- Distribution

$$\begin{aligned} \mathbf{X}(\varphi \mathbf{U} \psi) &\equiv (\mathbf{X}\varphi)\mathbf{U}(\mathbf{X}\psi) \\ \mathbf{F}(\varphi \vee \psi) &\equiv \mathbf{F}\varphi \vee \mathbf{F}\psi \\ \mathbf{G}(\varphi \wedge \psi) &\equiv \mathbf{G}\varphi \wedge \mathbf{G}\psi \end{aligned}$$

- But we have:

$$\begin{aligned} \mathbf{F}(\varphi \wedge \psi) &\not\equiv \mathbf{F}\varphi \wedge \mathbf{F}\psi \\ \mathbf{G}(\varphi \vee \psi) &\not\equiv \mathbf{G}\varphi \vee \mathbf{G}\psi \end{aligned}$$

Absorption Laws(1)

$\mathbf{FGF}\varphi \equiv \mathbf{GF}\varphi$

More formally: $\mathbf{GF}\varphi$ means $\forall i \geq 0, \exists j \geq i : \sigma[j..] \models \varphi$

$\mathbf{FGF}\varphi$ means $\exists k \geq 0, \forall i \geq k, \exists j \geq i : \sigma[j..] \models \varphi$

Absorption Laws(2)

$\mathbf{GFG}\varphi \equiv \mathbf{FG}\varphi$

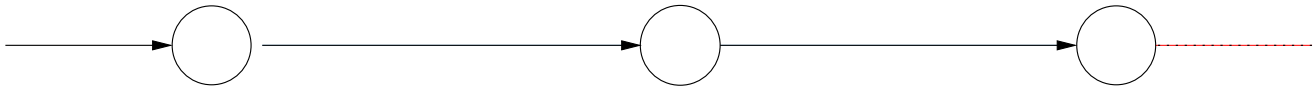
More formally: $\mathbf{FG}\varphi$ means $\exists i \geq 0, \forall j \geq i : \sigma[j..] \models \varphi$

$\mathbf{GFG}\varphi$ means $\forall k \geq 0, \exists i \geq k, \forall j \geq i : \sigma[j..] \models \varphi$

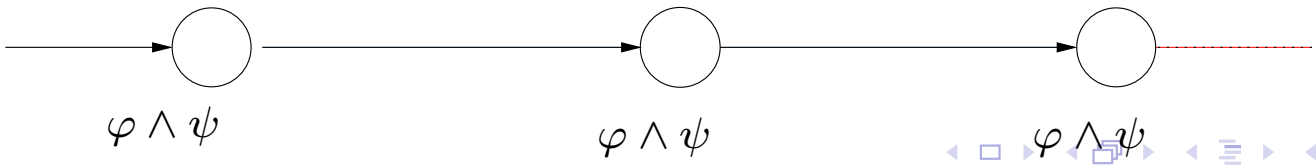
Distributive Laws (1)

$$\mathbf{X}(\varphi \mathbf{U} \psi) \equiv (\mathbf{X}\varphi)\mathbf{U}(\mathbf{X}\psi)$$

$$\mathbf{F}(\varphi \vee \psi) \equiv \mathbf{F}\varphi \vee \mathbf{F}\psi$$

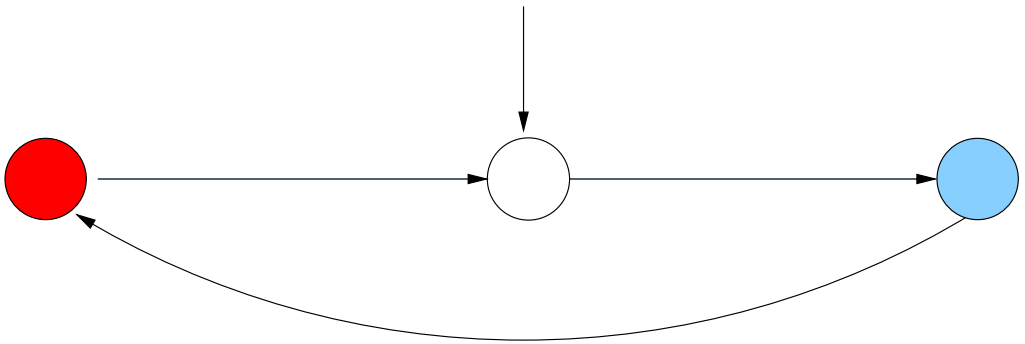


$$\mathbf{G}(\varphi \wedge \psi) \equiv \mathbf{G}\varphi \wedge \mathbf{G}\psi$$



Distributive Laws (2)

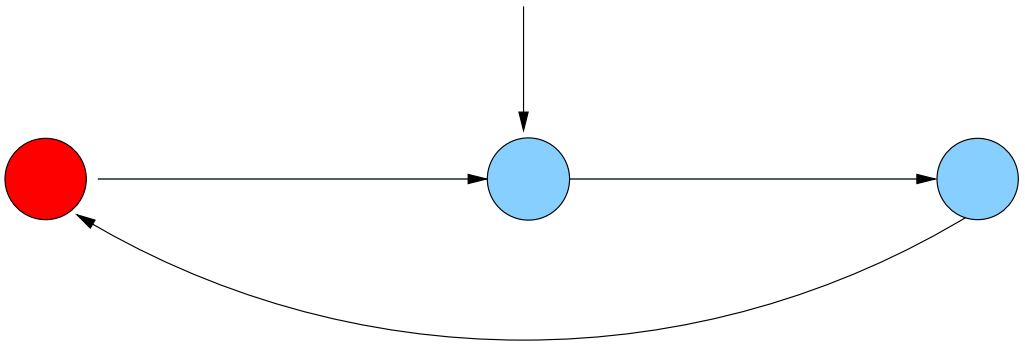
$$\mathbf{F}(a \wedge b) \not\equiv \mathbf{F}a \wedge \mathbf{F}b$$



$$TS \not\models \mathbf{F}(a \wedge b) \text{ and } TS \models \mathbf{F}a \wedge \mathbf{F}b$$

Distributive Laws (3)

$\mathbf{G}(a \vee b) \not\equiv \mathbf{G}a \vee \mathbf{G}b$



$TS \models \mathbf{G}(a \vee b)$ and $TS \not\models \mathbf{G}a \vee \mathbf{G}b$