Verification – Lecture 7
Precedence Properties, Part II

Bernd Finkbeiner – Sven Schewe
Rayna Dimitrova – Lars Kuhtz – Anne Proetzsch

Wintersemester 2007/2008

Precedence Properties

Review

are of the form

$$p \;\Rightarrow\; q_m \;\mathcal{W}\; (q_{m-1} \;\cdots\; (q_1 \;\mathcal{W}\; q_0)\ldots)$$

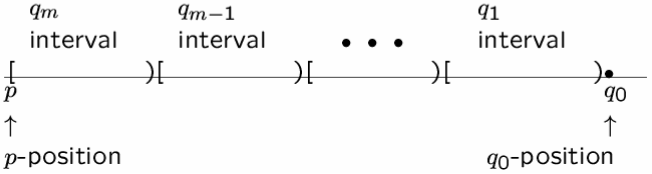
also written

$$\boxed{p \;\Rightarrow\; q_m \;\mathcal{W}\; q_{m-1} \;\cdots\; q_1 \;\mathcal{W}\; q_0}$$

for assertions $p, q_0, q_1, \ldots, q_m$.

Each interval may be empty, may extend to infinity.

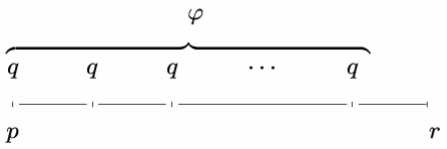
Models that satisfy these formulas



General Waiting-For

Review

$$p \Rightarrow q \,\mathcal{W}\, r$$



Rule WAIT (general waiting-for)

For assertions p, q, r, φ

W1. $p \rightarrow \varphi \vee r$

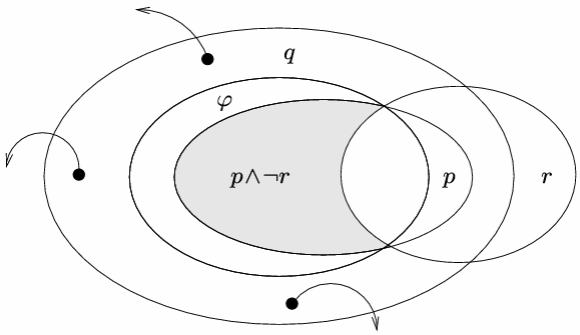
W2. $\varphi \rightarrow q$

W3. $\{\varphi\}\mathcal{T}\{\varphi \vee r\}$

$p \Rightarrow q \,\mathcal{W}\, r$

Strengthening & Weakening

Review



$\varphi \rightarrow q$	"φ strengthens q"
$p \rightarrow \varphi \vee r$, i.e., $p \wedge \neg r \rightarrow \varphi$	"φ weakens $p \wedge \neg r$"

Forward Propagation

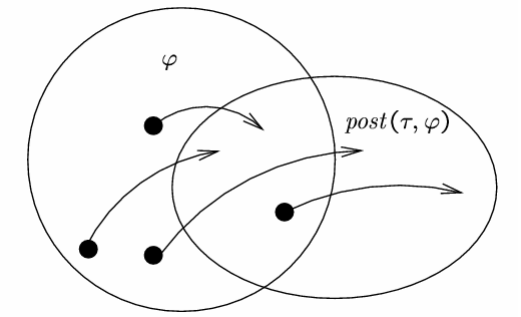
Review

characterizes all states that can be reached from a $(p \wedge \neg r)$-state without taking an escape transition.

Based on postcondition:

$post(\tau, \varphi)$: $\exists V^0 \,.\, \varphi(V^0) \wedge \rho_\tau(V^0, V)$

$post(\tau, \varphi)$ characterizes all states that are τ-successors of a φ-state.



Backward Propagation

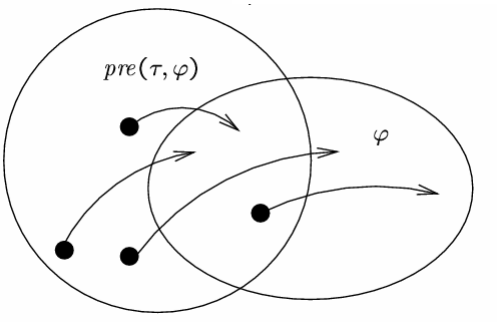
Review

characterizes all states that can reach a q-state without taking an escape transition

Based on precondition:

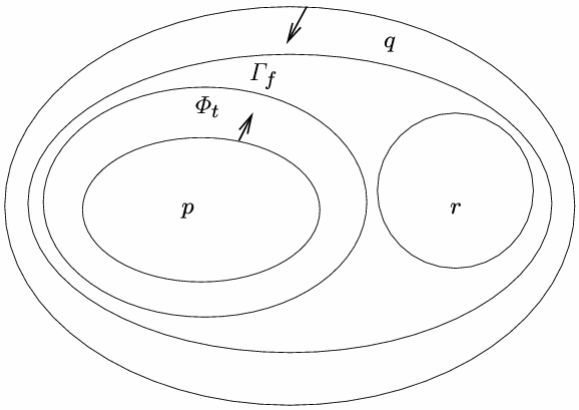
$pre(\tau, \varphi)$: $\forall V' \,.\, \rho_\tau(V, V') \rightarrow \varphi(V')$

$pre(\tau, \varphi)$ characterizes all states of which all τ-successors satisfy φ.



Forward vs. Backward

Review



General Rule

Review

Rule NWAIT (nested waiting-for)

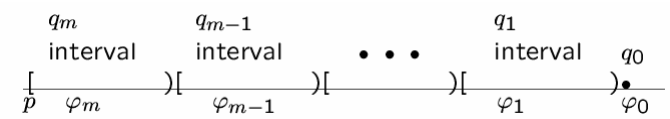
For assertions p, $q_0, q_1, \ldots, q_m$ and $\varphi_0, \varphi_1, \ldots, \varphi_m$

N1. $p \rightarrow \bigvee_{j=0}^{m} \varphi_j$

N2. $\varphi_i \rightarrow q_i$ for $i = 0, 1, \ldots, m$

N3. $\{\varphi_i\} \mathcal{T} \left\{ \bigvee_{j \leq i} \varphi_j \right\}$ for $i = 1, \ldots, m$

$p \Rightarrow q_m \mathcal{W} q_{m-1} \cdots q_1 \mathcal{W} q_0$



Completeness

Review

If the formula

$$p \Rightarrow q_m \mathcal{W} (q_{m-1} \cdots (q_1 \mathcal{W} q_0) \ldots)$$

is P-valid, then there exist assertions $\varphi_0, \varphi_1, \ldots, \varphi_m$, such that the premises of rule NWAIT are provable from state-validities.

Segments

Review

- Let $\sigma = s_0, s_1, \ldots$ be a *P*-computation.
- A *P*-segment is a finite sequence of states $[s_a, \ldots, s_b]$ such that $b \geq a$ and for every i, $a \leq i \leq b-1$, s_{i+1} is a τ-successor of s_i for some $\tau \in T$.
- We say that the segment $[s_a, \ldots, s_b]$ originates in s_a.

Segments Satisfying Waiting-For Formulas

Review

- Consider $\psi_j = q_j \, W \, q_{j-1} \; \ldots \; q_1 \, W \, q_0$
- A segment $[s_a,\ldots,s_b]$ satisfies ψ_j if there exist indices $a=i_j \leq i_{j-1} \leq \ldots \leq i_0 \leq b+1$ such that
  for every $r=1, \ldots, j$, $\sigma[i_r,i_{r-1})$ is a q_r-interval
  and if $i_0 < b+1$ then q_0 is satisfied by s_{i_0}.
- Notation:
  $\sigma[a,b] = [s_a,\ldots,s_b]$
  $\sigma[a,b) = [s_a,\ldots,s_{b-1}]$

Properties

Review

- Property P0:
  If the formula $\psi_j = q_j \, W \, q_{j-1} \; \ldots \; q_1 \, W \, q_0$
  holds at position $a \geq 0$ of a computation $\sigma=s_0,s_1,\ldots$
  then, for every $b \geq a$, the segment $\sigma[a,b]$ satisfies ψ_j.
- Property P1:
  If $\sigma[a,b]$, with $a < b$, satisfies $\psi_j = q_j \, W \, q_{j-1} \; \ldots \; q_1 \, W \, q_0$
  and s_a does not satisfy q_0
  then $\sigma[a+1, b]$, satisfies ψ_j.

Ranks

Review

- For a formula $\psi_m = q_m \, W \, q_{m-1} \; \ldots \; q_1 \, W \, q_0$

  we say that a state s <u>has rank</u> j, $0 \leq j \leq m$,
  if all segments originating at s satisfy
  $\psi_j = q_j \, W \, q_{j-1} \; \ldots \; q_1 \, W \, q_0$.

- If j is the smallest nonnegative integer s.t. s has rank j then s <u>has minimal rank</u> j.

Example

- $V = \{y : \text{integer}\}$
- $\Theta = y < 0$
- $T = \{\tau_I, \tau_<, \tau_2, \tau_{11}\}$
- $\rho_I : y' = y$
- $\rho_< : y < 0 \wedge y' \leq 20$
- $\rho_2 : y' = y-2$
- $\rho_{11} : y' = y-11$

- Consider: $\text{even}(y) \; W \; \text{odd}(y) \; W \; \text{even}(y) \; W \; y<0$

The completeness proof was done on the blackboard.

For details, see

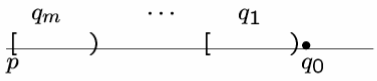
Temporal Verification of Reactive Systems – Safety
by Zohar Manna and Amir Pnueli, Springer Verlag,

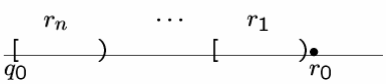
Section 3.5 (pages 288-296).

Concatenation of Waiting-For Formulas

Rule CONC-W

$$\frac{p \Rightarrow q_m \mathcal{W} \cdots q_1 \mathcal{W} q_0 \qquad q_0 \Rightarrow r_n \mathcal{W} \cdots \mathcal{W} r_0}{p \Rightarrow q_m \mathcal{W} \cdots \mathcal{W} q_1 \mathcal{W} r_n \mathcal{W} \cdots \mathcal{W} r_0}$$





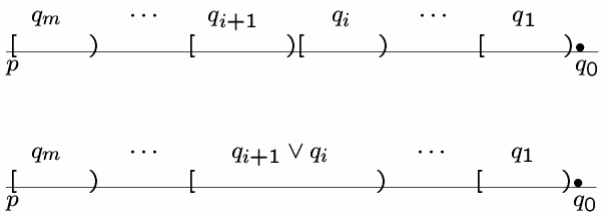
Collapsing of Waiting-For Formulas

Rule COLL-W

For $i > 0$

$$p \;\Rightarrow\; q_m \;\mathcal{W}\; \cdots \;\mathcal{W}\; q_{i+1} \;\mathcal{W}\; q_i \;\mathcal{W}\; \cdots \;\mathcal{W}\; q_0$$

$$p \;\Rightarrow\; q_m \;\mathcal{W}\; \cdots \;\mathcal{W}\; (q_{i+1} \vee q_i) \;\mathcal{W}\; \cdots \;\mathcal{W}\; q_0$$



Example: Another version of Peterson

local y_1, y_2: boolean where $y_1 = \text{F}, y_2 = \text{F}$
s : integer where $s = 1$

P_1 ::
ℓ_0 : loop forever do
- ℓ_1 : noncritical
- ℓ_2 : $y_1 := \text{T}$
- ℓ_3 : $s := 1$
- ℓ_4 : await $(\neg y_2) \vee (s = 2)$
- ℓ_5 : critical
- ℓ_6 : $y_1 := \text{F}$

||

P_2 ::
m_0 : loop forever do
- m_1 : noncritical
- m_2 : $y_2 := \text{T}$
- m_3 : $s := 2$
- m_4 : await $(\neg y_1) \vee (s = 1)$
- m_5 : critical
- m_6 : $y_2 := \text{F}$

Suppose we have
1-bounded overtaking from ℓ_3

$$\psi_1\text{: } at\_\ell_3 \;\Rightarrow\; (\neg at\_m_5)\;\mathcal{W}\; at\_m_5\;\mathcal{W}\;(\neg at\_m_5)\;\mathcal{W}\; at\_\ell_4$$

1-bounded overtaking from ℓ_3

$$\psi_2\text{: } at\_\ell_3 \;\Rightarrow\; (\neg at\_m_4)\;\mathcal{W}\; at\_m_4\;\mathcal{W}\;(\neg at\_m_4)\;\mathcal{W}\; at\_\ell_4$$

By Rule CONC-W

$$at\_\ell_2 \;\Rightarrow\; (\neg at\_m_4)\;\mathcal{W}\; at\_m_4\;\mathcal{W}\;(\neg at\_m_4)\;\mathcal{W}\; (\neg at\_m_4)\;\mathcal{W}\; at\_m_4\;\mathcal{W}\;(\neg at\_m_4)\;\mathcal{W}\; at\_\ell_4$$

By Rule COLL-W

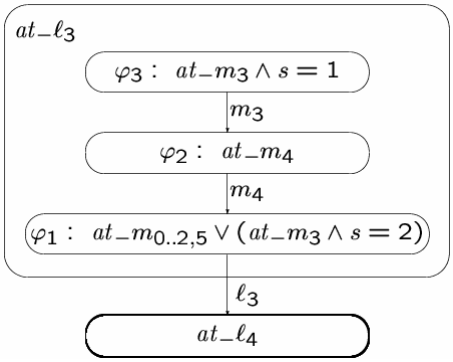
$$\psi\text{: } at\_\ell_2 \;\Rightarrow\; (\neg at\_m_4)\;\mathcal{W}\; at\_m_4\;\mathcal{W}\;(\neg at\_m_4)\;\mathcal{W}\; at\_m_4\;\mathcal{W}\;(\neg at\_m_4)\;\mathcal{W}\; at\_\ell_4$$

Therefore, 2-bounded overtaking from ℓ_2

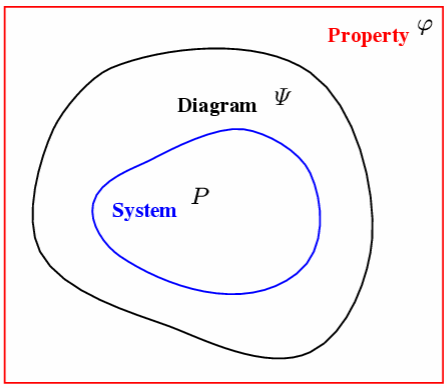
Verification Diagrams

Verification diagrams allow a graphical representation of a proof of a temporal property.

Example:



Idea



$\mathcal{L}(P) \subseteq \mathcal{L}(\Psi)$ proved by verification conditions.

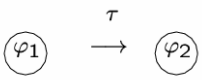
$\mathcal{L}(\Psi) \subseteq \mathcal{L}(\varphi)$ follows from well-formedness of diagram

P-Valid Verification Diagrams

Directed labeled graph with

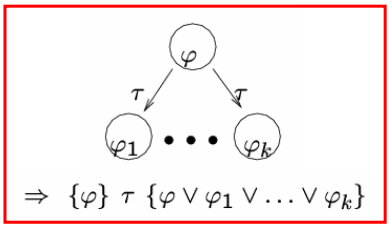
Nodes – labeled by assertions

Edges – labeled by names of transitions



Terminal Node ("goal") – no edges depart from it

Verification conditions

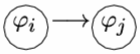


Definition: VD is P-valid iff all VCs associated with nodes in the diagram are P-state valid

Wait Diagrams

VDs with nodes $\varphi_m, \ldots, \varphi_0$ such that:

- weakly acyclic, i.e.,

  if 

  then $i \geq j$

- φ_0 is a terminal node

Proofs with Wait Diagrams

A P-valid WAIT diagram establishes that

$$\bigvee_{j=0}^{m} \varphi_j \;\Rightarrow\; \varphi_m \;\mathcal{W}\; \varphi_{m-1} \;\cdots\; \varphi_1 \;\mathcal{W}\; \varphi_0$$

is P-valid.

If, in addition,

(N1) $\quad p \;\rightarrow\; \bigvee_{j=0}^{m} \varphi_j$

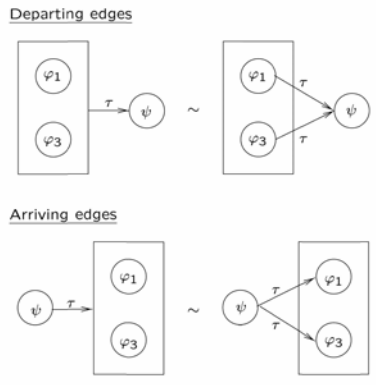
(N2) $\quad \varphi_i \;\rightarrow\; q_i \quad$ for $\quad i = 0, 1, \ldots, m$

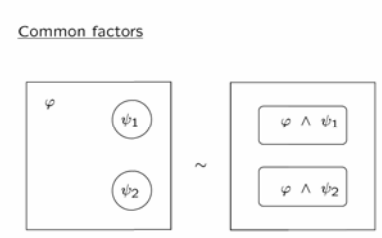
are P-state valid, then

$$p \;\Rightarrow\; q_m \;\mathcal{W}\; q_{m-1} \;\cdots\; q_1 \;\mathcal{W}\; q_0$$

is P-valid.

Compound Nodes (Statecharts Conventions)





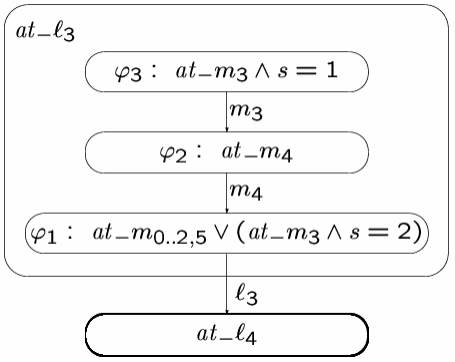
Example

local y_1, y_2: boolean where $y_1 = \text{F}, y_2 = \text{F}$
s : integer where $s = 1$

P_1 ::
ℓ_0 : loop forever do
- ℓ_1 : noncritical
- ℓ_2 : $(y_1, s) := (\text{T}, 1)$
- ℓ_3 : await $(\neg y_2) \vee (s = 2)$
- ℓ_4 : critical
- ℓ_5 : $y_1 := \text{F}$

||

P_2 ::
m_0 : loop forever do
- m_1 : noncritical
- m_2 : $(y_2, s) := (\text{T}, 2)$
- m_3 : await $(\neg y_1) \vee (s = 1)$
- m_4 : critical
- m_5 : $y_2 := \text{F}$



Associated VCs

- From φ_3
  $\{\varphi_3\}\ m_3\ \{\varphi_3 \vee \varphi_2\}$ $\{\varphi_3\}\ \overline{m_3}\ \{\varphi_3\}$
- From φ_2
  $\{\varphi_2\}\ m_4\ \{\varphi_2 \vee \varphi_1\}$ $\{\varphi_2\}\ \overline{m_4}\ \{\varphi_2\}$

Example (cont'd)

- From φ_3
  $\{\varphi_3\}\ m_3\ \{\varphi_3 \vee \varphi_2\}$ $\{\varphi_3\}\ \overline{m_3}\ \{\varphi_3\}$ P-state valid
- From φ_2
  $\{\varphi_2\}\ m_4\ \{\varphi_2 \vee \varphi_1\}$ $\{\varphi_2\}\ \overline{m_4}\ \{\varphi_2\}$ P-state valid
- $\underbrace{at\_\ell_3}_{p} \rightarrow \bigvee_{j=0}^{3} \varphi_j$

$\varphi_0 \rightarrow \underbrace{at\_\ell_4}_{q_0}$ $\varphi_1 \rightarrow \underbrace{\neg at\_m_4}_{q_1}$

$\varphi_2 \rightarrow \underbrace{at\_m_4}_{q_2}$ $\varphi_3 \rightarrow \underbrace{\neg at\_m_4}_{q_3}$

are state-valid.

Therefore,

ψ: $\underbrace{at\_\ell_3}_{p} \Rightarrow$

$\underbrace{(\neg at\_m_4)}_{q_3}\ \mathcal{W}\ \underbrace{at\_m_4}_{q_2}\ \mathcal{W}\ \underbrace{(\neg at\_m_4)}_{q_1}\ \mathcal{W}\ \underbrace{at\_\ell_4}_{q_0}$

Invariance Diagrams

VDs with no terminal nodes (cycles OK)

Claim (invariance diagram):

A P-valid INVARIANCE diagram establishes that

$$\bigvee_{j=1}^{m} \varphi_j \;\Rightarrow\; \Box(\bigvee_{j=1}^{m} \varphi_j)$$

is P-valid.

If, in addition,

(I1) $\bigvee_{j=1}^{m} \varphi_j \rightarrow q$

(I2) $\Theta \rightarrow \bigvee_{j=1}^{m} \varphi_j$

are P-state valid, then

$\Box q$ is P-valid

Example

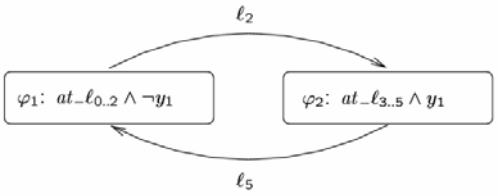
local y_1, y_2: boolean where $y_1 = \text{F}, y_2 = \text{F}$
s : integer where $s = 1$

P_1 ::
ℓ_0 : loop forever do
- ℓ_1 : noncritical
- ℓ_2 : $(y_1, s) := (\text{T}, 1)$
- ℓ_3 : await $(\neg y_2) \vee (s = 2)$
- ℓ_4 : critical
- ℓ_5 : $y_1 := \text{F}$

||

P_2 ::
m_0 : loop forever do
- m_1 : noncritical
- m_2 : $(y_2, s) := (\text{T}, 2)$
- m_3 : await $(\neg y_1) \vee (s = 1)$
- m_4 : critical
- m_5 : $y_2 := \text{F}$

- INVARIANCE diagram valid for program MUX-PET1



- Also,

(I2) $\underbrace{at\_\ell_0 \wedge \neg y_1 \wedge \cdots}_{\Theta} \rightarrow \underbrace{at\_\ell_{0..2} \wedge \neg y_1}_{\varphi_1} \vee \underbrace{\cdots}_{\varphi_2}$

(I1) $\underbrace{at\_\ell_{0..2} \wedge \neg y_1}_{\varphi_1} \rightarrow \underbrace{y_1 \leftrightarrow at\_\ell_{3..5}}_{q}$

$\underbrace{at\_\ell_{3..5} \wedge y_1}_{\varphi_2} \rightarrow \underbrace{y_1 \leftrightarrow at\_\ell_{3..6}}_{q}$

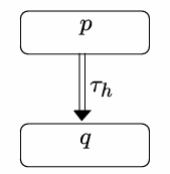
Therefore

$\Box(y_1 \leftrightarrow at\_\ell_{3..5})$

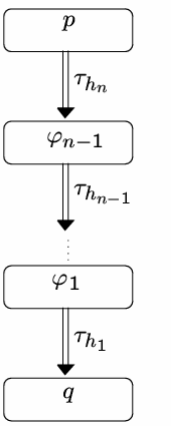
Proving Response under Justice

$$p \Rightarrow \Diamond q$$

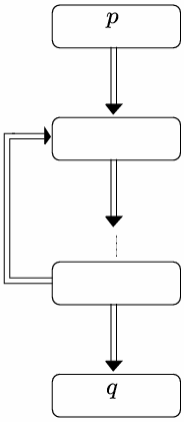
Overview: 3 Rules



1. Rule RESP-J
   (single-step response under justice)

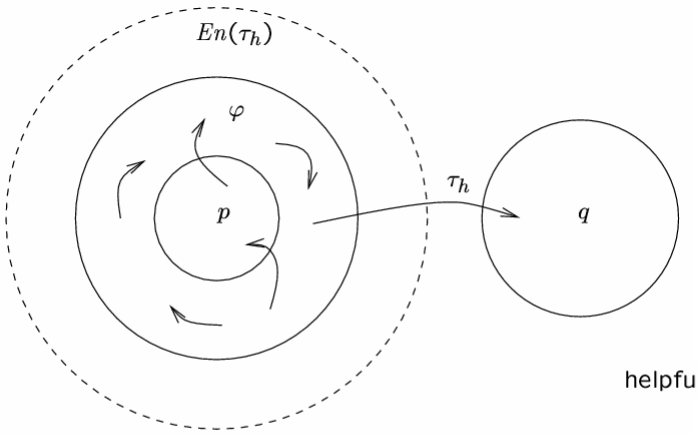


2. Rule CHAIN-J
   (chain rule under justice)



3. Rule WELL-J
   (well-founded response under justice)

Single-Step Rule (Motivation)



helpful transition τ_h

Justice requirement: it is not the case that a just transition is continuously enabled but never taken.

Single-Step Rule

For assertions p, q, φ, and transition $\tau_h \in \mathcal{J}$,

$$\begin{array}{ll} \text{J1.} & p \rightarrow q \vee \varphi \\ \text{J2.} & \{\varphi\}\ \mathcal{T}\ \{q \vee \varphi\} \\ \text{J3.} & \{\varphi\}\ \tau_h\ \{q\} \\ \text{J4.} & \varphi \rightarrow En(\tau_h) \\ \hline & p \Rightarrow \Diamond q \end{array}$$

Useful Rules

- Monotonicity:

$$\frac{p \Rightarrow q \qquad q \Rightarrow \Diamond r \qquad r \Rightarrow t}{p \Rightarrow \Diamond t}$$

- Reflexivity:

$$p \Rightarrow \Diamond p$$

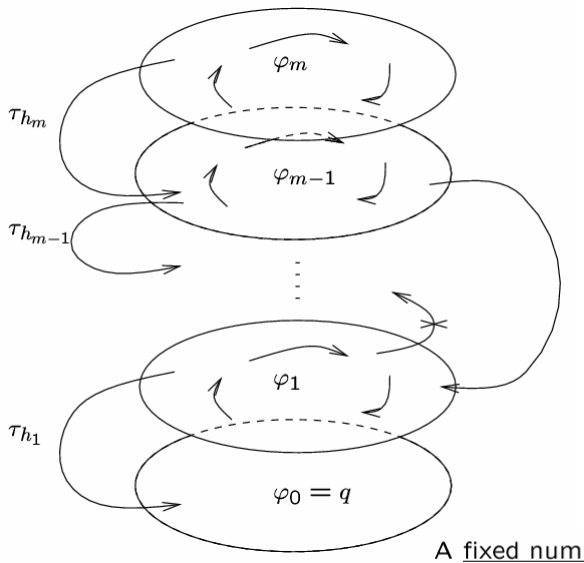
- Transitivity:

$$\frac{p \Rightarrow \Diamond q \qquad q \Rightarrow \Diamond r}{p \Rightarrow \Diamond r}$$

- Case analysis:

$$\frac{p \Rightarrow \Diamond r \qquad q \Rightarrow \Diamond r}{(p \vee q) \Rightarrow \Diamond r}$$

Chain Rule (Motivation)



A fixed number of helpful transitions

Chain Rule

For assertions p and $q = \varphi_0, \varphi_1, \ldots, \varphi_m$
and transitions $\tau_{h_1}, \ldots, \tau_{h_m} \in \mathcal{J}$

J1. $p \rightarrow \bigvee_{j=0}^{m} \varphi_j$

J2. $\{\varphi_i\}\mathcal{T}\left\{\bigvee_{j \leq i} \varphi_j\right\}$

J3. $\{\varphi_i\}\tau_{h_i}\left\{\bigvee_{j < i} \varphi_j\right\}$

J4. $\varphi_i \rightarrow En(\tau_{h_i})$

} for $i = 1, \ldots, m$

$p \Rightarrow \diamondsuit q$

Chain Diagrams

Edges: labeled by transitions

single-lined ———— (represents a regular transition)

double-lined ═══ (represents a helpful transition)

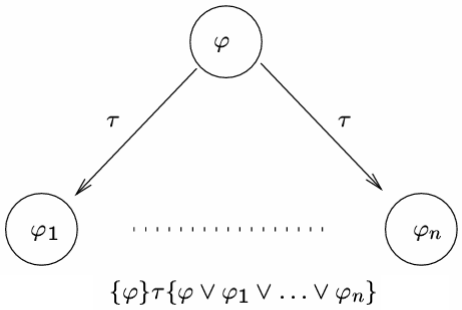
Nodes: labeled by assertions (φ_i)

Terminal node (φ_0)

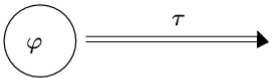
well-formedness conditions:

- weakly acyclic in $\longrightarrow$:
  if $(\varphi_i) \longrightarrow (\varphi_j)$ then $i \geq j$
- acyclic in $\Longrightarrow$:
  if $(\varphi_i) \Longrightarrow (\varphi_j)$ then $i > j$
- every nonterminal node has a double edge departing from it.

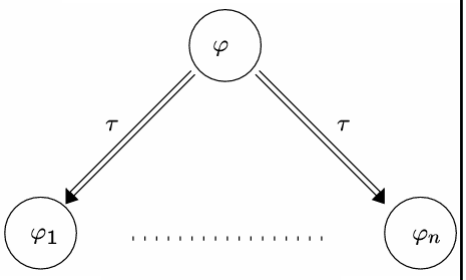
Verification Conditions



$\{\varphi\}\tau\{\varphi \vee \varphi_1 \vee \ldots \vee \varphi_n\}$



$\varphi \rightarrow En(\tau)$



$\{\varphi\}\tau\{\varphi_1 \vee \ldots \vee \varphi_n\}$

Chain Diagram Validity

A chain diagram is P-valid
if all the verification conditions associated with the diagram are P-valid.

Claim: A P-valid chain diagram establishes that

$$\bigvee_{j=0}^{m} \varphi_j \Rightarrow \Diamond \varphi_0$$

is P-valid.

With $p \rightarrow \bigvee_{j=0}^{m} \varphi_j$ and $\varphi_0 \rightarrow q$,
we can conclude the P-validity of

$$\boxed{p \Rightarrow \Diamond q}$$

Example

$at\_\ell_3 \Rightarrow \Diamond\, at\_\ell_4$

local y_1, y_2: boolean where $y_1 = \text{F}, y_2 = \text{F}$
s : integer where $s = 1$

P_1 ::
ℓ_0 : loop forever do
- ℓ_1 : noncritical
- ℓ_2 : $(y_1, s) := (\text{T}, 1)$
- ℓ_3 : await $(\neg y_2) \vee (s = 2)$
- ℓ_4 : critical
- ℓ_5 : $y_1 := \text{F}$

||

P_2 ::
m_0 : loop forever do
- m_1 : noncritical
- m_2 : $(y_2, s) := (\text{T}, 2)$
- m_3 : await $(\neg y_1) \vee (s = 1)$
- m_4 : critical
- m_5 : $y_2 := \text{F}$