Reasoning about Liveness Properties in Event-B

Thai Son Hoang[1] and Jean-Raymond Abrial[2]

[1]Institute of Information Security, Department of Computer Science
Swiss Federal Institute of Technology Zürich (ETH Zürich)

and

[2]Marseille, France

ICFEM 2011, Durham, U.K.
26th October 2011

(part of the work is supported by the DEPLOY project)

ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Motivation

- Event-B Models
  - Discrete transition systems
- Safety properties
  - Something (bad) never happens.
  - e.g. invariance properties
  - part of Event-B models
- Liveness properties
  - Something (good) will happen
  - e.g. termination, eventually, progress, persistence
  - How to reason about them practically?

Event-B Models – Discrete Transition Systems

machine M
variables v
invariants $I(v)$
initialisation $K(c, v')$

events
evt$_\mathrm{i}$ $\widehat{=}$ **any** t_i **where** $G_i(t_i, v)$ **then** $S(t_i, v, v')$ **end**

- v denotes the vector of variables $v_1, \ldots, v_n$.
- $K(c, v')$ is the initialisation.
- t_i is the parameters of event evt$_\mathrm{i}$.
- $G_i(t_i, v)$ is the guard of event evt$_\mathrm{i}$.
- evt$_\mathrm{i}$ is said to be enabled in some state s if $\exists t_i \cdot G_i(t_i, v)$ holds in s.
- $S(t_i, v, v')$ is the action (before-after predicate) of event evt$_\mathrm{i}$.

Executions and Traces (of States)

Executions $\alpha = s_0 \xrightarrow{e_0} s_1 \xrightarrow{e_1} s_2 \xrightarrow{e_2} s_3 \xrightarrow{e_3} \ldots$

Traces $\sigma = s_0, s_1, s_2, s_3, \ldots$

- Initialisation: $s_0 = \langle v' \rangle$ (as defined by init)
- Sequencing: For all s_k, s_{k+1}, there exists evt_i s.t. $s_k \xrightarrow{evt_i} s_{k+1}$
- Maximality: The sequence is either infinite or ends in a state s_k where all events are disabled

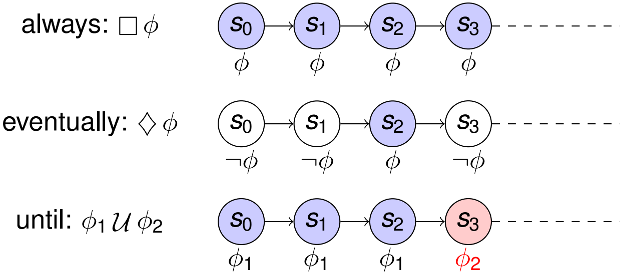
Example

machine *Counter*	**events**
variables $c \in \mathbb{Z}$	inc $\hat{=}$ **when** $c \neq 5$ **then** $c := c + 1$ **end**
initialisation $c := 0$	dec $\hat{=}$ **when** $c > 3$ **then** $c := c - 1$ **end**

e.g. $\sigma_{Counter}$: $\langle 0 \rangle, \langle 1 \rangle, \langle 2 \rangle, \langle 3 \rangle, \langle 4 \rangle, \langle 5 \rangle, \langle 4 \rangle, \langle 3 \rangle, \langle 4 \rangle, \langle 5 \rangle, \ldots$

The Language of Temporal Logic

- A (basic) state formula P is any first-order logic formula,
- The basic formulas can be extended by combining the Boolean operators ($\neg, \wedge, \vee, \Rightarrow$) with temporal operators:



- A machine M satisfying property ϕ if all its traces satisfy ϕ.
- $\mathrm{M} \vdash \phi$ states that $\mathrm{M} \vDash \phi$ is provable.

Contribution

Proof rules for some class of liveness properties

- Eventually: $\Box \Diamond P$
- Until: $\Box(P_1 \Rightarrow (P_1 \mathcal{U} P_2))$
- Progress: $\Box(P_1 \Rightarrow \Diamond P_2)$
- Persistence: $\Diamond \Box P$

Proof Obligations (1/4)

Machine leads from P_1 to P_2

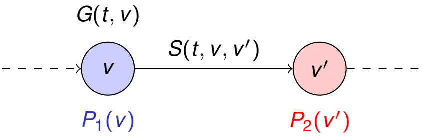
A machine M leads from P_1 to P_2 if
every event evt in M leads from P_1 to P_2

When M leads from P_1 to P_2 is provable, we write

$\vdash$ M leads from P_1 to P_2

- Given M with $\text{evt}_i \;\widehat{=}\;$ **any** t_i **where** $G_i(t_i, v)$ **then** $S_i(t_i, v, v')$ **end**
- Event evt_i leads from P_1 to P_2 if

$$P_1(v) \land G_i(t_i, v) \land S_i(t_i, v, v') \;\Rightarrow\; P_2(v')$$



Proof Obligations (2/4)

Machine is convergent in P

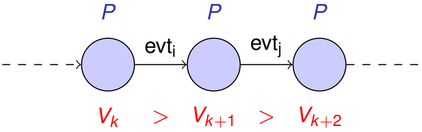
A macine M is said to be convergent in P if for any trace of M, it does not end with an infinite sequence of states satisfying P

$\vdash$ M is convergent in P

- Given M with $evt_i \;\widehat{=}\;$ **any** t_i **where** $G_i(t_i, v)$ **then** $S_i(t_i, v, v')$ **end**
- Give a integer variant $V(v)$
- M converges in P if for all events evt_i of M, we have

$$P(v) \wedge G_i(t_i, v) \Rightarrow V(v) \in \mathbb{N}$$

$$P(v) \wedge G_i(t_i, v) \wedge S_i(t_i, v, v') \;\Rightarrow\; V(v') < V(v)$$



Proof Obligations (3/4)

Machine is deadlock-free in P

- Machine M is deadlock-free in P if
  there exists an enabled event of M when P holds.
- When the above fact is provable, we denote it as
  $$\vdash \text{M is deadlock-free in } P$$

Deadlock-freeness in P is guaranteed by proving the following

$$P(v) \;\Rightarrow\; (\exists t_1 \cdot G_1(t_1, v)) \lor \ldots \lor (\exists t_n \cdot G_n(t_n, v))$$

Proof Obligations (4/4)

Machine is divergent in P

- M is said to be divergent in P if for every infinite trace of M it ends with an infinite sequences of states satisfying P.
- When the above fact is provable, we denote it as

$$\vdash \text{M is divergent in } P$$

- Given M with $\text{evt}_i \;\widehat{=}\;$ **any** t_i **where** $G_i(t_i, v)$ **then** $S_i(t_i, v, v')$ **end**
- Give a integer variant $V(v)$
- M diverges when P holds if for all events evt_i of M

$$\neg P(v) \land G_i(t_i, v) \Rightarrow V(v) \in \mathbb{N}$$

$$\neg P(v) \land G_i(t_i, v) \land S_i(t_i, v, v') \;\Rightarrow\; V(v') < V(v)$$

$$P(v) \land G_i(t_i, v) \land S_i(t_i, v, v') \land V(v') \in \mathbb{N} \Rightarrow\; V(v') \leq V(v)$$

Proof Obligations (4/4)

Machine is divergent in P

- M is said to be divergent in P if for every infinite trace of M it ends with an infinite sequences of states satisfying P.
- When the above fact is provable, we denote it as

$$\vdash \text{M is divergent in } P$$

- Given M with $\text{evt}_i \;\widehat{=}\;$ **any** t_i **where** $G_i(t_i, v)$ **then** $S_i(t_i, v, v')$ **end**
- Give a integer variant $V(v)$
- M diverges when P holds if for all events evt_i of M

$$\neg P(v) \land G_i(t_i, v) \Rightarrow V(v) \in \mathbb{N}$$

$$\neg P(v) \land G_i(t_i, v) \land S_i(t_i, v, v') \;\Rightarrow\; V(v') < V(v)$$

$$P(v) \land G_i(t_i, v) \land S_i(t_i, v, v') \land V(v') \in \mathbb{N} \;\Rightarrow\; V(v') \leq V(v)$$

$$\frac{\vdash \text{M is convergent in } \neg P \qquad \vdash \text{M is deadlock-free in } \neg P}{\text{M} \vdash \Box\Diamond P} \quad \textbf{LIVE}_{\Box\Diamond}$$

Counter $\vdash \Box\Diamond c \geq 2$

inc $\widehat{=}$ **when** $c \neq 5$ **then** $c := c + 1$ **end**

dec $\widehat{=}$ **when** $c > 3$ **then** $c := c - 1$ **end**

- Convergence: Using variant $V \widehat{=} 5 - c$.
  - $5 - c \in \mathbb{N}$ (using invariant $c \in 0 \,..\, 5$)
  - inc: $\neg c \geq 2 \wedge c \neq 5 \Rightarrow 5 - (c + 1) < 5 - c$
  - dec: $\neg c \geq 2 \wedge c > 3 \Rightarrow 5 - (c - 1) < 5 - c$
- Deadlock-free: $\neg c \geq 2 \Rightarrow c \neq 5 \vee c > 3$

Proof Rules (1/4)

Always Eventually

$$\frac{\vdash \text{M is convergent in } \neg P \qquad \vdash \text{M is deadlock-free in } \neg P}{\text{M} \vdash \Box\Diamond P} \quad \textbf{LIVE}_{\Box\Diamond}$$

Counter $\vdash \Box\Diamond c \geq 2$

inc $\widehat{=}$ **when** $c \neq 5$ **then** $c := c + 1$ **end**

dec $\widehat{=}$ **when** $c > 3$ **then** $c := c - 1$ **end**

- Convergence: Using variant $V \widehat{=} 5 - c$.
  - $5 - c \in \mathbb{N}$ (using invariant $c \in 0\,..\,5$)
  - inc: $\neg c \geq 2 \wedge c \neq 5 \Rightarrow 5 - (c + 1) < 5 - c$
  - dec: $\neg c \geq 2 \wedge c > 3 \Rightarrow 5 - (c - 1) < 5 - c$
- Deadlock-free: $\neg c \geq 2 \Rightarrow c \neq 5 \vee c > 3$

Proof Rules (1/4)
Always Eventually

$$\frac{\vdash \text{M is convergent in } \neg P \qquad \vdash \text{M is deadlock-free in } \neg P}{\text{M} \vdash \Box\Diamond P} \quad \textbf{LIVE}_{\Box\Diamond}$$

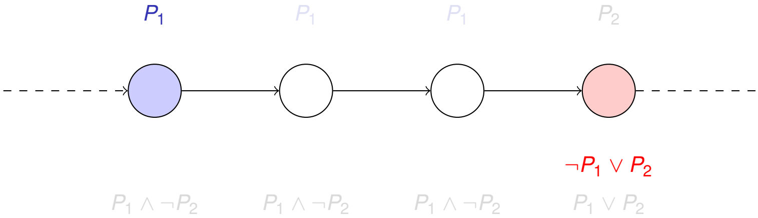
Counter $\vdash \Box\Diamond c \geq 2$

inc $\hat{=}$ **when** $c \neq 5$ **then** $c := c + 1$ **end**

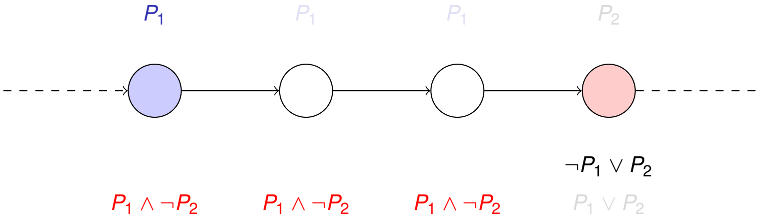
dec $\hat{=}$ **when** $c > 3$ **then** $c := c - 1$ **end**

- Convergence: Using variant $V \hat{=} 5 - c$.
  - $5 - c \in \mathbb{N}$ (using invariant $c \in 0\,..\,5$)
  - inc: $\neg c \geq 2 \land c \neq 5 \;\Rightarrow\; 5 - (c + 1) < 5 - c$
  - dec: $\neg c \geq 2 \land c > 3 \;\Rightarrow\; 5 - (c - 1) < 5 - c$
- Deadlock-free: $\neg c \geq 2 \;\Rightarrow\; c \neq 5 \lor c > 3$

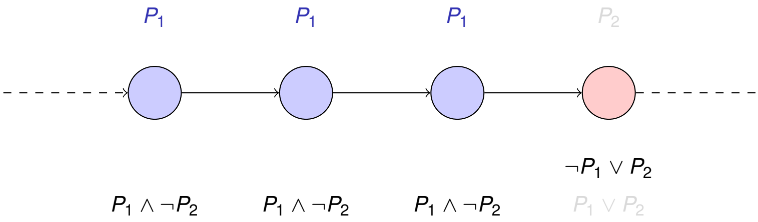
$$\frac{\vdash \text{M leads from } (P_1 \land \neg P_2) \text{ to } (P_1 \lor P_2) \qquad M \vdash \Box\Diamond(\neg P_1 \lor P_2)}{M \vdash \Box(P_1 \Rightarrow (P_1 \,\mathcal{U}\, P_2))} \quad \textbf{Until}$$



$$\frac{\vdash \text{M leads from } (P_1 \land \neg P_2) \text{ to } (P_1 \lor P_2) \qquad \text{M} \vdash \Box\Diamond(\neg P_1 \lor P_2)}{\text{M} \vdash \Box(P_1 \Rightarrow (P_1 \,\mathcal{U}\, P_2))} \quad \textbf{Until}$$



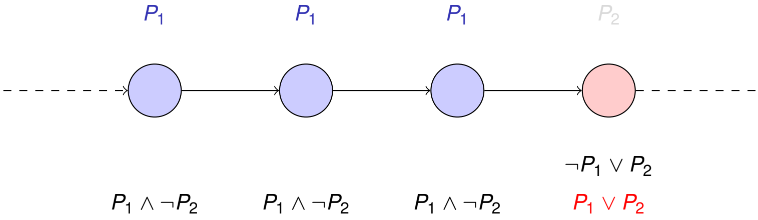
$$\frac{\vdash \text{M leads from } (P_1 \land \neg P_2) \text{ to } (P_1 \lor P_2) \qquad \text{M} \vdash \Box\Diamond(\neg P_1 \lor P_2)}{\text{M} \vdash \Box(P_1 \Rightarrow (P_1 \,\mathcal{U}\, P_2))}\ \textbf{Until}$$



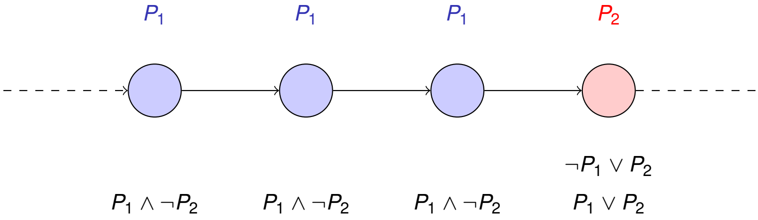
Proof Rules (2/4)

Until (1/2)

$$\frac{\vdash \text{M leads from } (P_1 \wedge \neg P_2) \text{ to } (P_1 \vee P_2) \qquad \text{M} \vdash \Box\Diamond(\neg P_1 \vee P_2)}{\text{M} \vdash \Box(P_1 \Rightarrow (P_1 \,\mathcal{U}\, P_2))} \quad \textbf{Until}$$



$$\dfrac{\begin{array}{c}\vdash \text{M leads from } (P_1 \land \neg P_2) \text{ to } (P_1 \lor P_2) \\ \text{M} \vdash \Box\Diamond(\neg P_1 \lor P_2)\end{array}}{\text{M} \vdash \Box(P_1 \Rightarrow (P_1\,\mathcal{U}\,P_2))} \quad \textbf{Until}$$



Proof Rules (2/4)

Until (2/2)

$$\frac{\vdash \text{M leads from } (P_1 \land \neg P_2) \text{ to } (P_1 \lor P_2) \qquad \text{M} \vdash \Box\Diamond(\neg P_1 \lor P_2)}{\text{M} \vdash \Box(P_1 \Rightarrow (P_1 \,\mathcal{U}\, P_2))} \quad \textbf{Until}$$

Counter $\vdash \Box(c < 2 \Rightarrow (c < 2 \,\mathcal{U}\, c = 2))$

inc $\widehat{=}$ **when** $c \neq 5$ **then** $c := c + 1$ **end**

dec $\widehat{=}$ **when** $c > 3$ **then** $c := c - 1$ **end**

- *Counter* leads from $c < 2 \land \neg c = 2$ to $c < 2 \lor c = 2$, equivalently *Counter* leads from $c < 2$ to $c \leq 2$
  - inc: $c < 2 \land c \neq 5 \Rightarrow c + 1 \leq 2$
  - dec: $c < 2 \land c > 3 \Rightarrow c - 1 \leq 2$
- Eventually: $\Box\Diamond(\neg c < 2 \lor c = 2)$, equivalent to $\Box\Diamond c \geq 2$

Proof Rules (2/4)

Until (2/2)

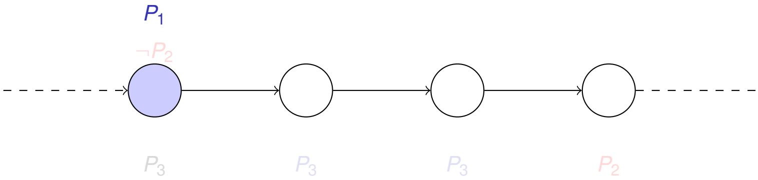
$$\frac{\vdash \text{M leads from } (P_1 \land \neg P_2) \text{ to } (P_1 \lor P_2) \qquad \text{M} \vdash \square \lozenge (\neg P_1 \lor P_2)}{\text{M} \vdash \square (P_1 \Rightarrow (P_1 \,\mathcal{U}\, P_2))} \quad \textbf{Until}$$

Counter $\vdash \square(c < 2 \;\Rightarrow\; (c < 2 \;\mathcal{U}\; c = 2))$

$$\text{inc} \;\widehat{=}\; \textbf{when } c \neq 5 \textbf{ then } c := c + 1 \textbf{ end}$$
$$\text{dec} \;\widehat{=}\; \textbf{when } c > 3 \textbf{ then } c := c - 1 \textbf{ end}$$

- *Counter* leads from $c < 2 \land \neg c = 2$ to $c < 2 \lor c = 2$, equivalently *Counter* leads from $c < 2$ to $c \leq 2$
  - inc: $c < 2 \land c \neq 5 \;\Rightarrow\; c + 1 \leq 2$
  - dec: $c < 2 \land c > 3 \;\Rightarrow\; c - 1 \leq 2$
- Eventually: $\square \lozenge (\neg c < 2 \lor c = 2)$, equivalent to $\square \lozenge c \geq 2$

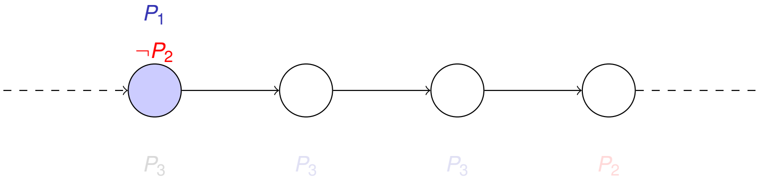
$$\frac{\begin{array}{c} \mathrm{M} \vdash \square(P_1 \land \neg P_2 \Rightarrow P_3) \\ \mathrm{M} \vdash \square(P_3 \Rightarrow (P_3 \,\mathcal{U}\, P_2)) \end{array}}{\mathrm{M} \vdash \square(P_1 \Rightarrow \lozenge P_2)} \quad \textbf{LIVE}_{\textbf{progress}}$$



Proof Rules (3/4)

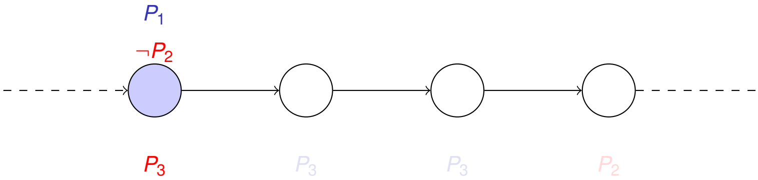
Progress (1/2)

$$\frac{\begin{array}{c} M \vdash \Box(P_1 \land \neg P_2 \Rightarrow P_3) \\ M \vdash \Box(P_3 \Rightarrow (P_3 \,\mathcal{U}\, P_2)) \end{array}}{M \vdash \Box(P_1 \Rightarrow \Diamond P_2)} \quad \textbf{LIVE}_{\textbf{progress}}$$

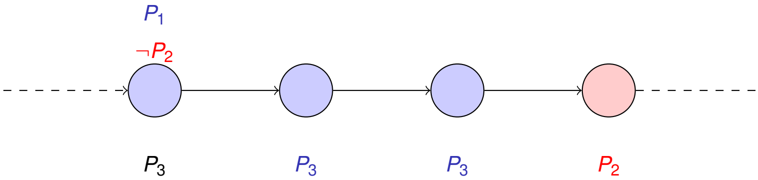


Proof Rules (3/4)
Progress (1/2)

$$\frac{\mathrm{M} \vdash \square(P_1 \land \neg P_2 \Rightarrow P_3) \qquad \mathrm{M} \vdash \square(P_3 \Rightarrow (P_3 \,\mathcal{U}\, P_2))}{\mathrm{M} \vdash \square(P_1 \Rightarrow \Diamond P_2)} \quad \textbf{LIVE}_{\textbf{progress}}$$



$$\frac{\begin{array}{l} \mathrm{M} \vdash \Box(P_1 \land \neg P_2 \Rightarrow P_3) \\ \mathrm{M} \vdash \Box(P_3 \Rightarrow (P_3 \,\mathcal{U}\, P_2)) \end{array}}{\mathrm{M} \vdash \Box(P_1 \Rightarrow \Diamond P_2)} \quad \textbf{LIVE}_{\textbf{progress}}$$



Proof Rules (3/4)

Progress (2/2)

$$\frac{\begin{array}{c} M \vdash \Box(P_1 \land \neg P_2 \Rightarrow P_3) \\ M \vdash \Box(P_3 \Rightarrow (P_3 \,\mathcal{U}\, P_2)) \end{array}}{M \vdash \Box(P_1 \Rightarrow \Diamond P_2)} \quad \textbf{LIVE}_{\textbf{progress}}$$

$Counter \vdash \Box(c = 0 \Rightarrow \Diamond c = 2)$

$$\begin{array}{l} \text{inc} \mathrel{\widehat{=}} \textbf{when } c \neq 5 \textbf{ then } c := c + 1 \textbf{ end} \\ \text{dec} \mathrel{\widehat{=}} \textbf{when } c > 3 \textbf{ then } c := c - 1 \textbf{ end} \end{array}$$

Choose $P_3 \mathrel{\widehat{=}} c < 2$

- $\Box(c = 0 \land \neg c = 2 \Rightarrow c < 2)$
- $\Box(c < 2 \Rightarrow (c < 2 \,\mathcal{U}\, c = 2))$

Proof Rules (3/4)
Progress (2/2)

$$\frac{\begin{array}{c} M \vdash \Box(P_1 \land \neg P_2 \Rightarrow P_3) \\ M \vdash \Box(P_3 \Rightarrow (P_3 \,\mathcal{U}\, P_2)) \end{array}}{M \vdash \Box(P_1 \Rightarrow \Diamond P_2)} \quad \textbf{LIVE}_{\textbf{progress}}$$

Counter $\vdash \Box(c = 0 \Rightarrow \Diamond c = 2)$

inc $\hat{=}$ **when** $c \neq 5$ **then** $c := c + 1$ **end**

dec $\hat{=}$ **when** $c > 3$ **then** $c := c - 1$ **end**

Choose $P_3 \hat{=} c < 2$

- $\Box(c = 0 \land \neg c = 2 \Rightarrow c < 2)$
- $\Box(c < 2 \Rightarrow (c < 2 \,\mathcal{U}\, c = 2))$

Proof Rules (4/4)

Persistence

$$\frac{\vdash \text{M is divergent in } P \qquad \vdash \text{M is deadlock-free in } \neg P}{\text{M} \vdash \Diamond\Box P} \quad \textbf{LIVE}_{\Diamond\Box}$$

Counter $\vdash \Diamond\Box c \geq 3$

- Divergence: Using variant $V \mathrel{\hat=} 2 - c$
  - $\neg c \geq 3 \Rightarrow 2 - c \in \mathbb{N}$
  - inc: $\neg c \geq 3 \land c \neq 5 \Rightarrow 2 - (c + 1) < 2 - c$
  - dec: $\neg c \geq 3 \land c > 3 \Rightarrow 2 - (c - 1) < 2 - c$
  - inc: $c \geq 3 \land c \neq 5 \land 2 - (c + 1) \in \mathbb{N} \Rightarrow 2 - (c + 1) \leq 2 - c$
  - dec: $c \geq 3 \land c > 3 \land 2 - (c - 1) \in \mathbb{N} \Rightarrow 2 - (c - 1) \leq 2 - c$
- Deadlock-free: $\neg c \geq 3 \;\Rightarrow\; c \neq 5 \lor c > 3$

Proof Rules (4/4)

Persistence

$$\frac{\vdash \text{M is divergent in } P \qquad \vdash \text{M is deadlock-free in } \neg P}{\text{M} \vdash \Diamond \Box P} \quad \textbf{LIVE}_{\Diamond\Box}$$

Counter $\vdash \Diamond \Box c \geq 3$

- Divergence: Using variant $V \mathrel{\widehat{=}} 2 - c$
  - $\neg c \geq 3 \Rightarrow 2 - c \in \mathbb{N}$
  - inc: $\neg c \geq 3 \land c \neq 5 \Rightarrow 2 - (c + 1) < 2 - c$
  - dec: $\neg c \geq 3 \land c > 3 \Rightarrow 2 - (c - 1) < 2 - c$
  - inc: $c \geq 3 \land c \neq 5 \land 2 - (c + 1) \in \mathbb{N} \Rightarrow 2 - (c + 1) \leq 2 - c$
  - dec: $c \geq 3 \land c > 3 \land 2 - (c - 1) \in \mathbb{N} \Rightarrow 2 - (c - 1) \leq 2 - c$
- Deadlock-free: $\neg c \geq 3 \;\Rightarrow\; c \neq 5 \lor c > 3$

Proof Rules (4/4)

Persistence

$$\frac{\vdash \text{M is divergent in } P \qquad \vdash \text{M is deadlock-free in } \neg P}{\text{M} \vdash \Diamond\Box P} \quad \textbf{LIVE}_{\Diamond\Box}$$

Counter $\vdash \Diamond\Box c \geq 3$

- Divergence: Using variant $V \mathrel{\hat=} 2 - c$
  - $\neg c \geq 3 \Rightarrow 2 - c \in \mathbb{N}$
  - inc: $\neg c \geq 3 \land c \neq 5 \Rightarrow 2 - (c + 1) < 2 - c$
  - dec: $\neg c \geq 3 \land c > 3 \Rightarrow 2 - (c - 1) < 2 - c$
  - inc: $c \geq 3 \land c \neq 5 \land 2 - (c + 1) \in \mathbb{N} \Rightarrow 2 - (c + 1) \leq 2 - c$
  - dec: $c \geq 3 \land c > 3 \land 2 - (c - 1) \in \mathbb{N} \Rightarrow 2 - (c - 1) \leq 2 - c$
- Deadlock-free: $\neg c \geq 3 \;\Rightarrow\; c \neq 5 \lor c > 3$

Summary

- Proof rules for certain classes of liveness properties.
  - eventually
  - until
  - progress
  - persistence
- The proof rules based on the reasoning about:
  - the machine leads from P_1 to P_2
  - the machine is convergent when P holds
  - the machine is deadlock-free when P holds.
  - the machine is divergent when P holds

Further Directions

- Proofs become tedious when the system becomes large.
- Refinement helps to reduce the complexity.
- Concurrent systems: fairness assumptions.

For Further Reading I

- Zohar Manna and Amir Pnueli.
  Adequate Proof Principles
  for Invariance and Liveness Properties of Concurrent Programs.
  Science of Computer Programming 4:259-289, 1984.
- Zohar Manna and Amir Pnueli.
  Completing the Temporal Picture.
  Theoretical Computer Science 81(1):97-130, 1991.