Program Analysis and Verification

0368-4479

http://www.cs.tau.ac.il/~maon/teaching/2013-2014/paav/paav1314b.html

Noam Rinetzky

Lecture 8: Axiomatic Semantics – Rely/Guarantee

(Take II*)

Slides credit: Roman Manevich, Mooly Sagiv, Eran Yahav

We begin …

- Mobiles

- Scribe

Programming Language

- Syntax: … $S_1 \parallel \ldots \parallel S_n$ | ⟨c⟩ | ⟨await b then c⟩
  - In our case: ⟨c⟩ = `case | x:=a`

- Operational Semantics:
  - States $s \in \Sigma$
  - Commands
    $$\frac{\langle S_1, s\rangle \Rightarrow \langle S'_1, s'\rangle}{\langle S_1 \parallel S_2, s\rangle \Rightarrow \langle S'_1 \parallel S_2, s\rangle} \quad [\text{Par}_1]$$
  - Traces $\langle S_0, s_0\rangle \overset{\langle c_0\rangle}{\Rightarrow} \langle S_1, s_1\rangle \overset{\langle c_1\rangle}{\Rightarrow} \ldots \overset{\langle c_k\rangle}{\Rightarrow} s_k$

Programming Language

- Syntax: … $S_1 \parallel \ldots \parallel S_n$ | ⟨c⟩ | ⟨await b then c⟩
  - In our case: ⟨c⟩ = `case | x:=a`

- Operational Semantics:
  - States $s \in \Sigma$
  - Commands
$$\frac{\langle S_1, s\rangle \Rightarrow \langle S'_1, s'\rangle}{\langle S_1 \parallel S_2, s\rangle \Rightarrow \langle S'_1 \parallel S_2, s\rangle} \quad [Par_1]$$
  - Traces $\langle S_0, s_0\rangle \overset{\langle c_0\rangle}{\Rightarrow} \langle S_1, s_1\rangle \overset{\langle c_1\rangle}{\Rightarrow} \ldots \overset{\langle c_k\rangle}{\Rightarrow} \ldots$

Axiomatic Semantics (Hoare Logic)

- Disjoint parallelism

- Global invariant

- Owicky – Gries [PhD. '76]

$$\frac{\ldots}{\{ P \}\ S_1 \parallel S_2\ \{ Q \}} \quad \ldots$$

Rely / Guarantee

- Aka Assume/Guarantee
- Cliff Jones [IFIP '83]
- Main idea: Modular capture of interference
  - Compositional proofs

Meaning of (atomic) Commands

- A relation between pre-states and post-states

- $[\![\langle c \rangle]\!] \subseteq \Sigma \times \Sigma$

$$s_0 \overset{\langle c_0 \rangle}{\Rightarrow} s_1 \overset{\langle c_1 \rangle}{\Rightarrow} \ldots \overset{\langle c_k \rangle}{\Rightarrow} s_{k+1}$$

Meaning of (atomic) Commands

- A relation between pre-states and post-states

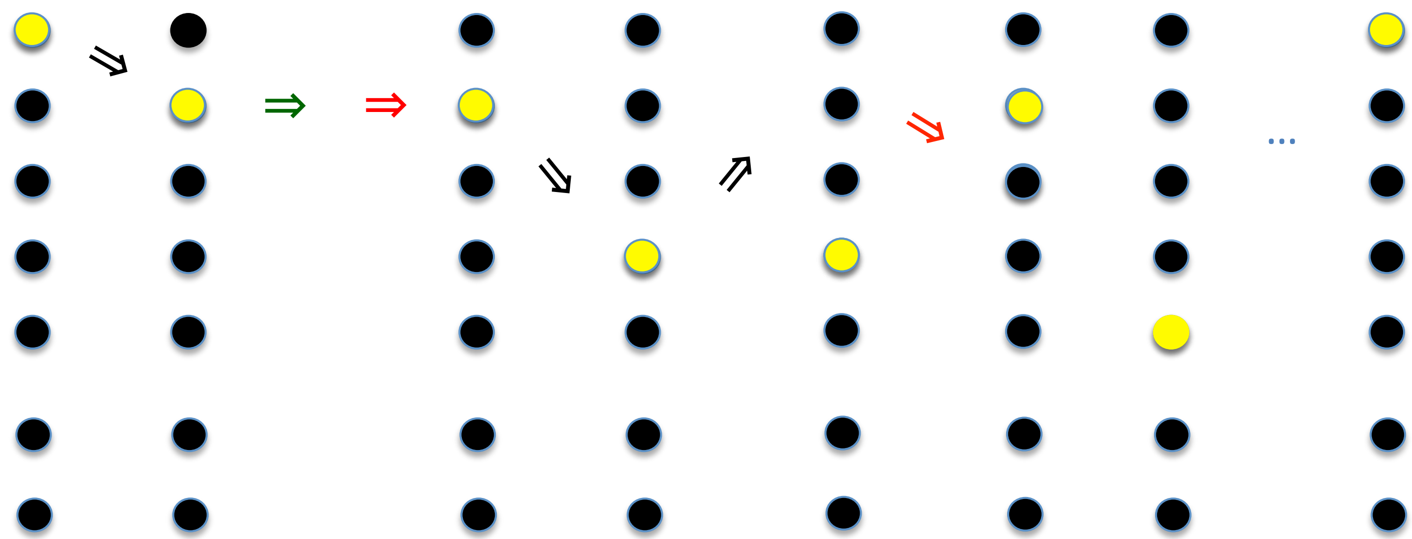
- $[\![\langle c \rangle]\!] \subseteq \Sigma \times \Sigma$

$$s_0 \overset{\langle c_0 \rangle}{\Rightarrow} s_1 \overset{\langle c_1 \rangle}{\Rightarrow} \ldots \overset{\langle c_k \rangle}{\Rightarrow} s_{k+1}$$

Meaning of (atomic) Commands

- A relation between pre-states and post-states

$$s_0 \overset{\langle c_0 \rangle}{\Rightarrow} s_1 \overset{\langle c_1 \rangle}{\Rightarrow} \ldots \overset{\langle c_k \rangle}{\Rightarrow} s_{k+1} \overset{\langle c_{k+1} \rangle}{\Rightarrow} s_{k+2} \overset{\langle c_{k+2} \rangle}{\Rightarrow} s_{k+3} \overset{\langle c_{k+3} \rangle}{\Rightarrow} s_{k+3} \overset{\langle c_{k+3} \rangle}{\Rightarrow} s_{k+4} \ldots \overset{\langle c_n \rangle}{\Rightarrow} s_{n+1}$$

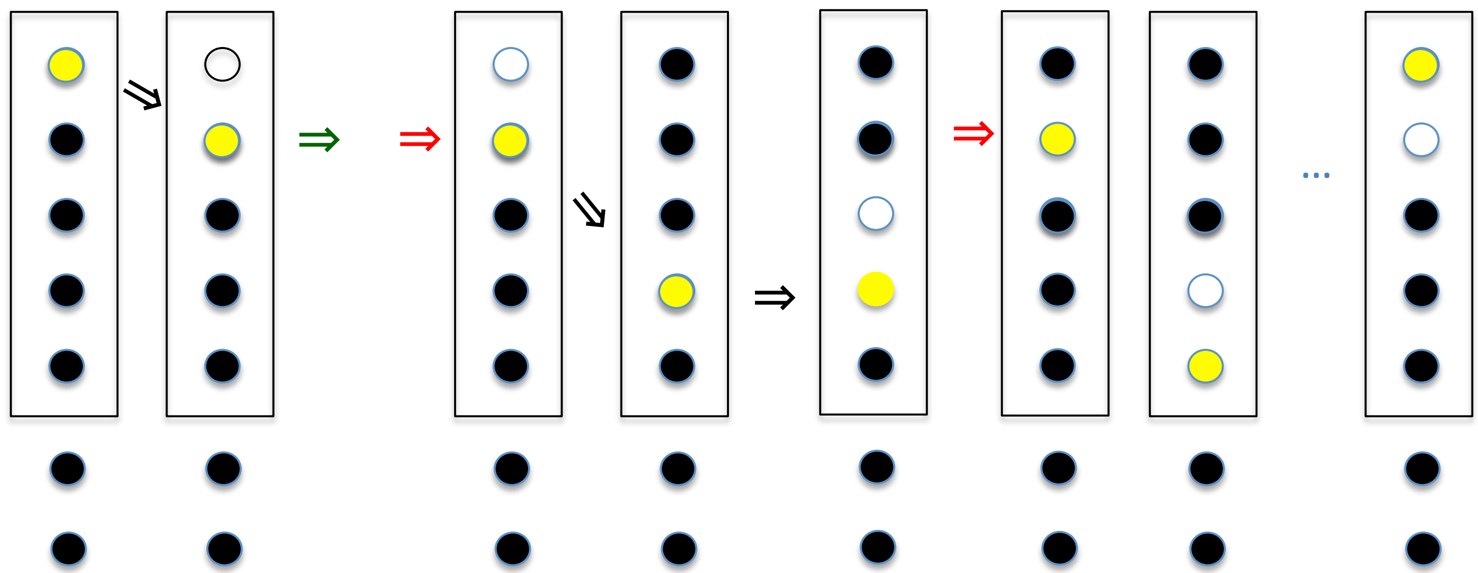


Intuition: Global Invariant

- Every (intermediate) state satisfies invariant I

$$s_0 \overset{\langle c_0\rangle}{\Rightarrow} s_1 \overset{\langle c_1\rangle}{\Rightarrow} \dots \overset{\langle c_k\rangle}{\Rightarrow} s_{k+1} \overset{\langle c_{k+1}\rangle}{\Rightarrow} s_{k+2} \overset{\langle c_{k+2}\rangle}{\Rightarrow} s_{k+3} \overset{\langle c_{k+3}\rangle}{\Rightarrow} s_{k+3} \overset{\langle c_{k+3}\rangle}{\Rightarrow} s_{k+4} \dots \overset{\langle c_n\rangle}{\Rightarrow} s_{n+1}$$

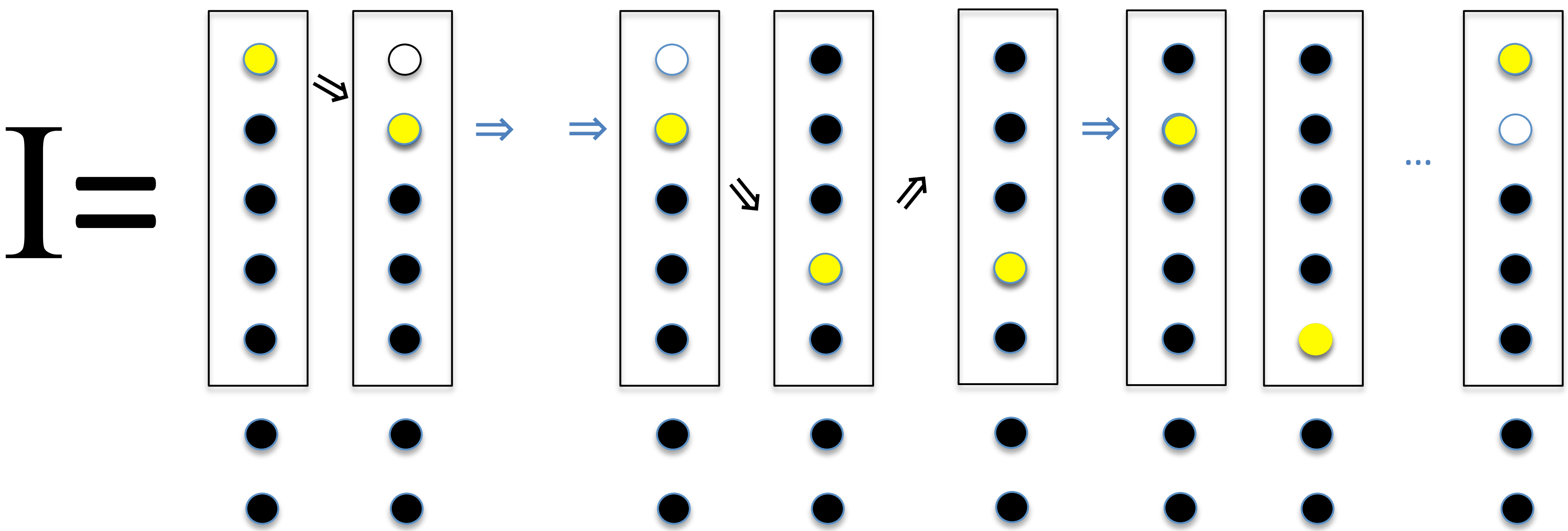
$I =$



Intuition: Global Invariant

- Thread-view

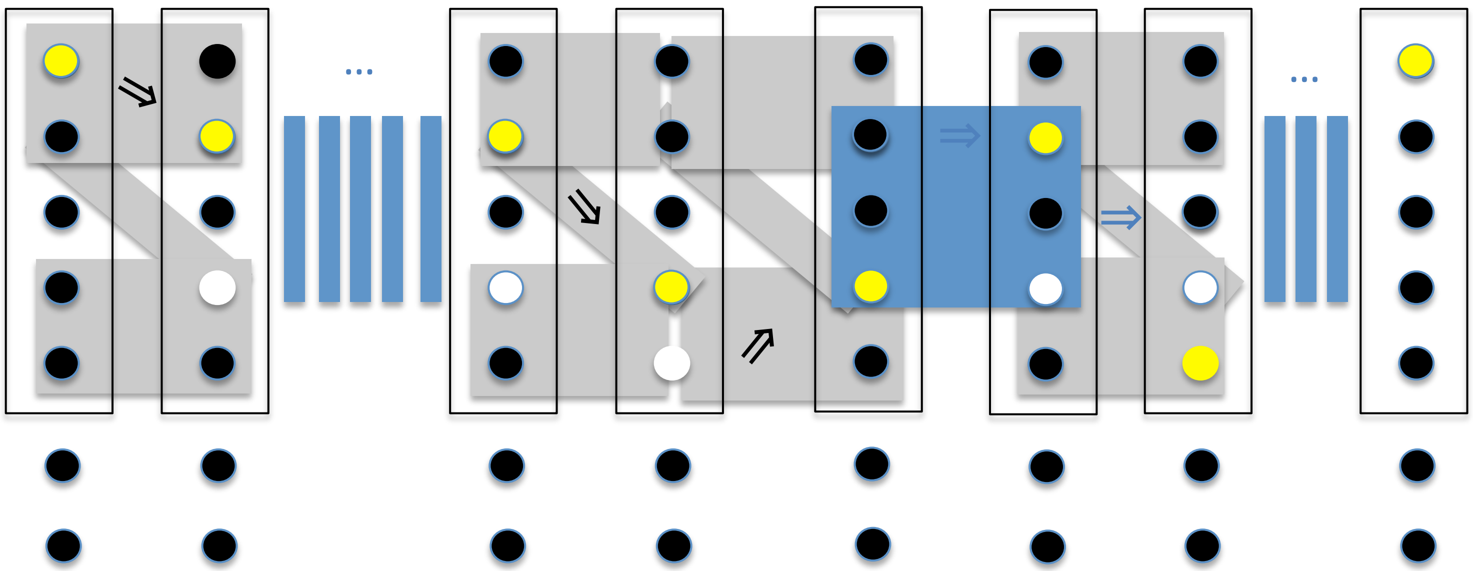
$$s_0 \overset{\langle c_0 \rangle}{\Rightarrow} s_1 \overset{\langle c_1 \rangle}{\Rightarrow} \ldots \overset{\langle c_k \rangle}{\Rightarrow} s_{k+1} \overset{\langle c_{k+1} \rangle}{\Rightarrow} s_{k+2} \overset{\langle c_{k+2} \rangle}{\Rightarrow} s_{k+3} \overset{\langle c_{k+3} \rangle}{\Rightarrow} s_{k+3} \overset{\langle c_{k+3} \rangle}{\Rightarrow} s_{k+4} \ldots \overset{\langle c_n \rangle}{\Rightarrow} s_{n+1}$$



Intuition: Rely Guarantee

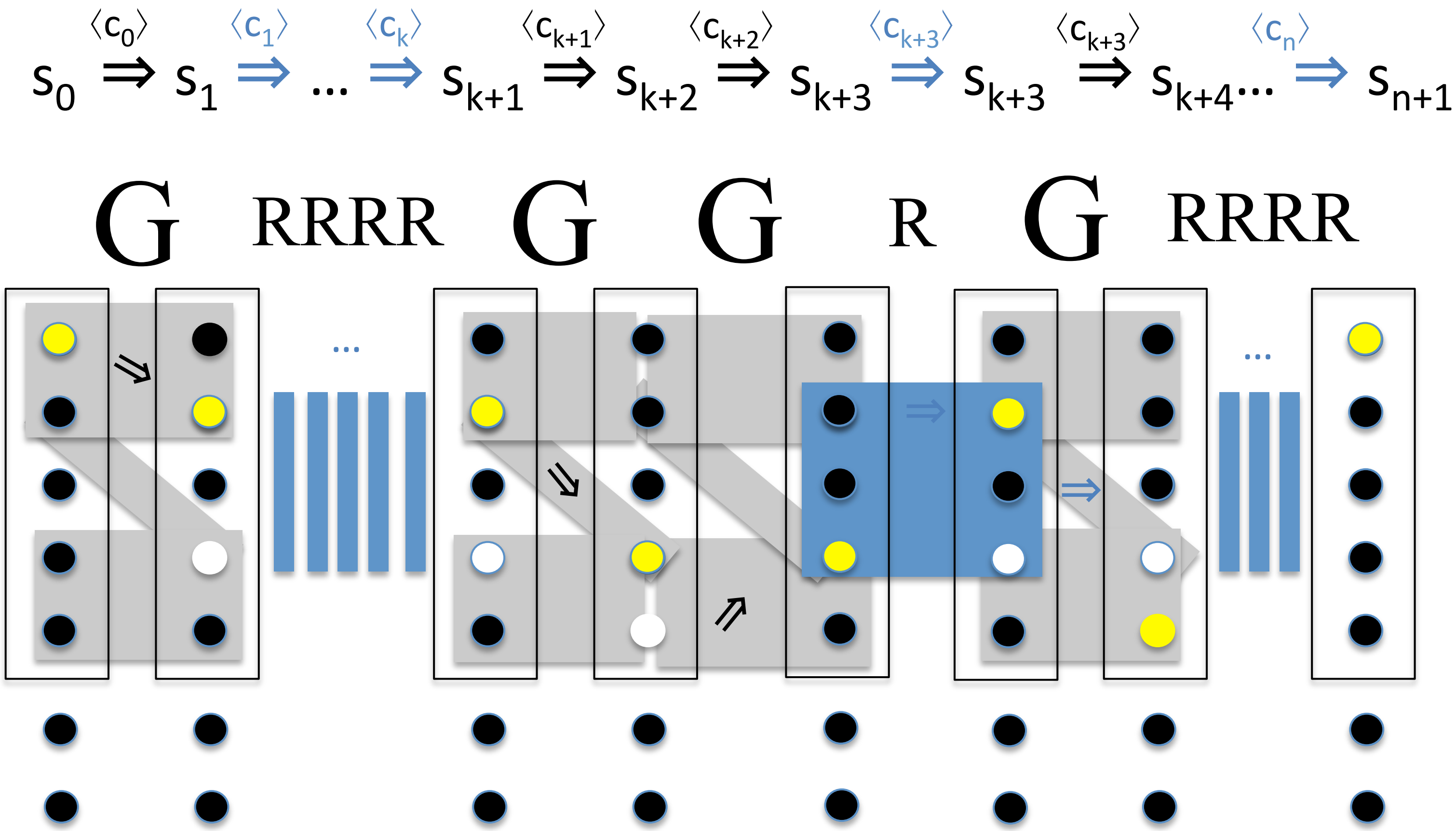
- Thread-view

$$s_0 \overset{\langle c_0\rangle}{\Rightarrow} s_1 \overset{\langle c_1\rangle}{\Rightarrow} \dots \overset{\langle c_k\rangle}{\Rightarrow} s_{k+1} \overset{\langle c_{k+1}\rangle}{\Rightarrow} s_{k+2} \overset{\langle c_{k+2}\rangle}{\Rightarrow} s_{k+3} \overset{\langle c_{k+3}\rangle}{\Rightarrow} s_{k+3} \overset{\langle c_{k+3}\rangle}{\Rightarrow} s_{k+4} \dots \overset{\langle c_n\rangle}{\Rightarrow} s_{n+1}$$



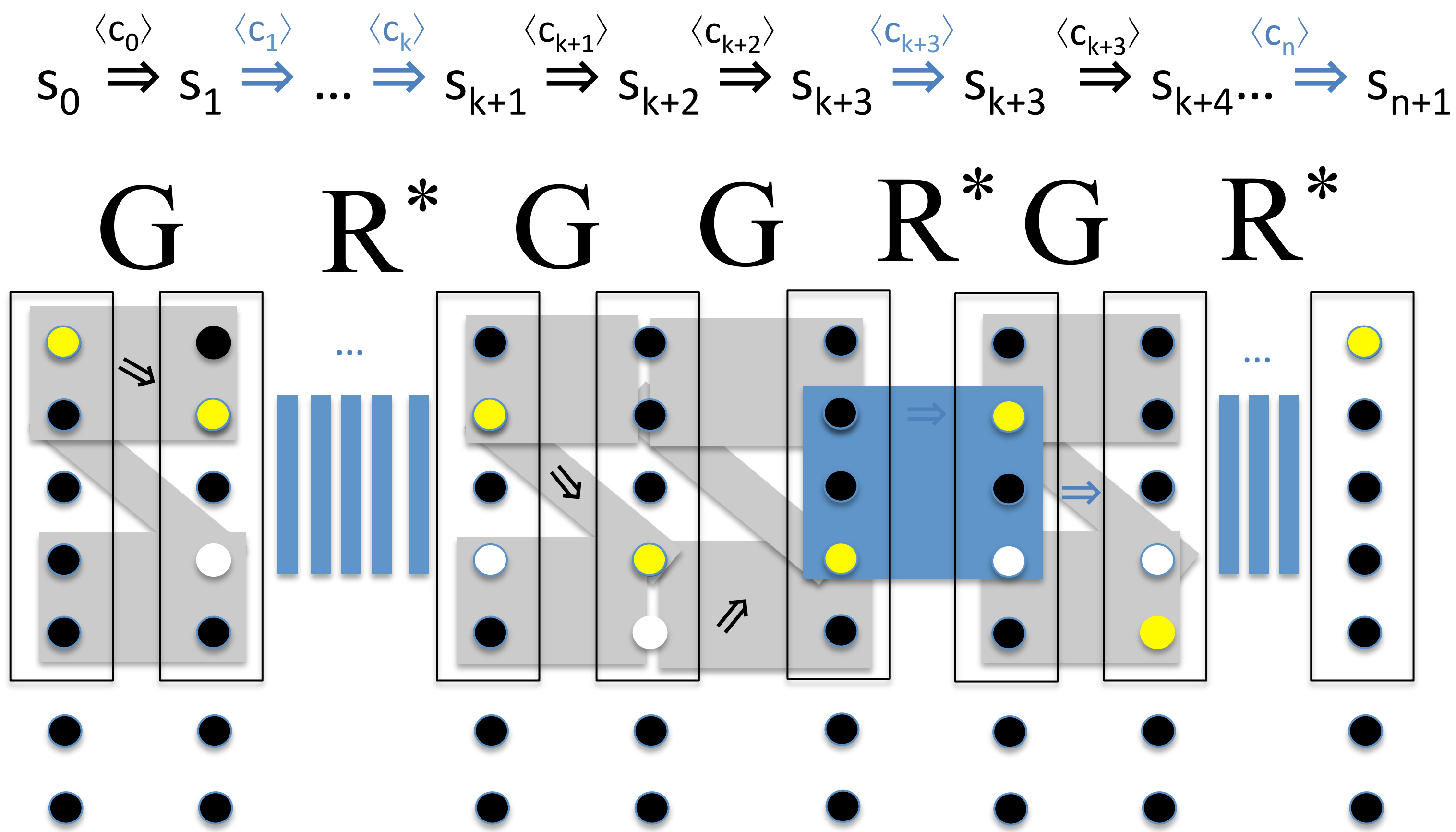
Intuition: Rely Guarantee

- Thread-view



Intuition: Rely Guarantee

- Thread-view



Relational Post-Conditions

- meaning of commands a relations between pre-states and post-states

- Option I: {P} C {Q}
  - P is a one state predicate
  - Q is a two-state predicate

- Example
  - {true} x := x + 1 {x= $\underline{x}$ + 1}

Relational Post-Conditions

- meaning of commands a relations between pre-states and post-states

- Option II: {P} C {Q}
  - P is a one state predicate
  - P is a one-state predicate
    - Use logical variables to record pre-state

- Example
  - $\{x = \underline{X}\}\ x := x + 1\ \{x = \underline{X} + 1\}$

Intuition (again)

Hoare: $\{\ P\ \}\ S\ \{\ Q\ \} \sim\ \{P\} \overbrace{\Rightarrow\Rightarrow\Rightarrow\Rightarrow}^{C} \{Q\}$

R/G: $R,G \vdash \{\ P\ \}\ S\ \{\ Q\ \} \sim\ \{P\} \overbrace{\underset{R}{\Rightarrow}\underset{G}{\Rightarrow}\underset{R}{\Rightarrow}\underset{R}{\Rightarrow}\underset{G}{\Rightarrow}\underset{G}{\Rightarrow}\underset{G}{\Rightarrow}}^{C} \{Q\}$

Goal: Parallel Composition

$$\frac{\begin{array}{c} R \vee G_2,\ G_1 \vdash \{\,P\,\}\ S_1 \parallel S_2\ \{\,Q\,\} \\ R \vee G_1,\ G_2 \vdash \{\,P\,\}\ S_1 \parallel S_2\ \{\,Q\,\} \end{array}}{R,\ G_1 \vee G_2 \vdash \{\,P\,\}\ S_1 \parallel S_2\ \{\,Q\,\}} \quad \text{(PAR)}$$

Relational Post-Conditions

- meaning of commands a relations between pre-states and post-states

- Option I: {P} C {Q}
  - P is a one state predicate
  - Q is a two-state predicate

- Example
  - {true} x := x + 1 {x= $\underline{x}$ + 1}

Meaning of (atomic) Commands

- meaning of atomic commands is relations between pre-states and post-states

- ⟦ C ⟧{Q}
  - P is a one state predicate
  - Q is a two-state predicate

- Example
  - {true} x := x + 1 {x= $\underline{x}$ + 1}

Meaning of (atomic) Commands

- meaning of atomic commands is relations between pre-states and post-states

- ⟦ C ⟧{Q}
  - P is a one state predicate
  - Q is a two-state predicate

- Example
  - {true} x := x + 1 {x= $\underline{x}$ + 1}

From one- to two-state relations

- $p(\underline{\sigma}, \sigma) = p(\sigma)$
- $\underline{p}(\underline{\sigma}, \sigma) = p(\underline{\sigma})$
- A single state predicate p is **preserved** by a two-state relation R if
  - $\underline{p} \wedge R \Rightarrow p$
  - $\forall \underline{\sigma}, \sigma \colon p(\underline{\sigma}) \wedge R(\underline{\boldsymbol{\sigma}}, \sigma) \Rightarrow p(\sigma)$
  - P is **stable** under R

Operations on Relations

- $(P;Q)(\underline{\sigma}, \sigma)=\exists\tau:P(\underline{\sigma}, \tau) \wedge Q(\tau, \sigma)$
- $ID(\underline{\sigma}, \sigma)= (\underline{\sigma}=\sigma)$
- $R^{*}= ID \vee R \vee (R;R) \vee (R;R;R) \vee \ldots \vee$
  - Reflexive transitive closure of R

Formulas

- ID(x) = ($\underline{x}$ = x)
- ID(p) =($\underline{p} \Leftrightarrow$p)
- Preserve (p)= $\underline{p} \Rightarrow$p

Judgements

- $c \models (p, R, G, Q)$

Informal Semantics

- $c \models (p, R, G, Q)$
  - For every state $\underline{\sigma}$ such that $\underline{\sigma} \models p$:
    - Every execution of c on state $\underline{\sigma}$ with (potential) interventions which satisfy R results in a state σ such that $(\underline{\sigma}, \sigma) \models Q$
    - The execution of every atomic sub-command of c on any possible intermediate state satisfies G

Informal Semantics

- $c \models (p, R, G, Q)$
  - For every state $\underline{\sigma}$ such that $\underline{\sigma} \models p$:
    - Every execution of c on state $\underline{\sigma}$ with (potential) interventions which satisfy R results in a state σ such that $(\underline{\sigma}, \sigma) \models Q$
    - The execution of every atomic sub-command of c on any possible intermediate state satisfies G
- $c \models [p, R, G, Q]$
  - For every state $\underline{\sigma}$ such that $\underline{\sigma} \models p$:
    - Every execution of c on state $\underline{\sigma}$ with (potential) interventions which satisfy R must terminate in a state σ such that $(\underline{\sigma}, \sigma) \models Q$
    - The execution of every atomic sub-command of c on any possible intermediate state satisfies G

A Formal Semantics

- Let $[\![C]\!]^R$ denotes the set of quadruples $<\sigma_1, \sigma_2, \sigma_3, \sigma_4>$ s.t. that when c executes on σ_1 with potential interferences by R it yields an intermediate state σ_2 followed by an intermediate state σ_3 and a final state σ_4
  - $\sigma_4 = \perp$ when c does not terminate

- $[\![C]\!]^R = \{<\sigma_1, \sigma_2, \sigma_3, \sigma_4> :$

  $\exists\, \sigma: <\sigma_1, \sigma> \models R \wedge$

  $(<C, \sigma> \Rightarrow^* \sigma_2 \wedge \sigma_2 = \sigma_3 = \sigma_4 \vee$

  $\exists\, \sigma', C' : <C, \sigma> \Rightarrow^* <C', \sigma'>$

  $\wedge\ (\quad (\sigma_2 = \sigma_1 \vee \sigma_2 = \sigma) \wedge (\sigma_3 = \sigma \vee \sigma_3 = \sigma') \wedge \sigma_4 = \perp)$

  $\vee \quad <\sigma', \sigma_2, \sigma_3, \sigma_4> \in [\![C']\!]^R)$

- $c \models (p, R, G, Q)$
  - For every $<\sigma_1, \sigma_2, \sigma_3, \sigma_4> \in [\![C]\!]^R$ such that $\sigma_1 \models p$
    - $< \sigma_2, \sigma_3> \models G$
    - If $\sigma 4 \neq \perp$: $<\sigma 1, \sigma 4> \models Q$

A Formal Semantics

- Let $[\![C]\!]^R$ denotes the set of quadruples $<\sigma_1, \sigma_2, \sigma_3, \sigma_4>$ s.t. that when c executes on σ_1 with potential interferences by R it yields an intermediate state σ_2 followed by an intermediate state σ_3 and a final state σ_4
  - $\sigma_4 = \perp$ when c does not terminate

- $[\![C]\!]^R = \{<\sigma_1, \sigma_2, \sigma_3, \sigma_4> :$

  $\exists\, \sigma: <\sigma_1, \sigma> \models R \;\wedge$

  $(<C, \sigma> \Rightarrow^* \sigma_2 \wedge \sigma_2 = \sigma_3 = \sigma_4) \vee$

  $(\exists\, \sigma', C' : <C, \sigma> \Rightarrow^* <C', \sigma'> \wedge$

  $(\quad (\sigma_2 = \sigma_1 \vee \sigma_2 = \sigma) \wedge (\sigma_3 = \sigma \vee \sigma_3 = \sigma') \wedge$

  $(\sigma_4 = \perp \;\vee\; <\sigma', \sigma_2, \sigma_3, \sigma_4> \in [\![C']\!]^R) \quad)$

- $c \models (p, R, G, Q)$
  - For every $<\sigma_1, \sigma_2, \sigma_3, \sigma_4> \in [\![C]\!]^R$ such that $\sigma_1 \models p$
    - $<\sigma_2, \sigma_3> \models G$
    - If $\sigma 4 \neq \perp$: $<\sigma 1, \sigma 4> \models Q$

A Formal Semantics

- Let $[\![C]\!]^R$ denotes the set of quadruples $<\sigma_1, \sigma_2, \sigma_3, \sigma_4>$ s.t. that when c executes on σ_1 with potential interferences by R it yields an intermediate state σ_2 followed by an intermediate state σ_3 and a final state σ_4
  - $\sigma_4 = \perp$ when c does not terminate

- $[\![C]\!]^R = \{<\sigma_1, \sigma_2, \sigma_3, \sigma_4> :$

  $\exists\, \sigma: <\sigma_1, \sigma> \models R \;\wedge$

  $(<C, \sigma> \Rightarrow^* \sigma_2 \wedge \sigma_2 = \sigma_3 = \sigma_4) \vee$

  $(\exists\, \sigma', C' : <C, \sigma> \Rightarrow^* <C', \sigma'> \wedge$

  $(\quad (\sigma_2 = \sigma_1 \vee \sigma_2 = \sigma) \wedge (\sigma_3 = \sigma \vee \sigma_3 = \sigma') \wedge \sigma_4 = \perp)$

  $\vee \quad <\sigma', \sigma_2, \sigma_3, \sigma_4> \in [\![C']\!]^R))$

- $c \models (p, R, G, Q)$
  - For every $<\sigma_1, \sigma_2, \sigma_3, \sigma_4> \in [\![C]\!]^R$ such that $\sigma_1 \models p$
    - $< \sigma_2, \sigma_3> \models G$
    - If $\sigma 4 \neq \perp$: $<\sigma 1, \sigma 4> \models Q$

Simple Examples

- $X := X + 1 \models (\text{true}, X=\underline{X}, X=\underline{X}+1 \vee X=\underline{X}, X=\underline{X}+1)$
- $X := X + 1 \models (X \geq 0, X \geq \underline{X}, X>0 \vee X=\underline{X}, X>0)$
- $X := X + 1 ; Y := Y + 1 \models (X \geq 0 \wedge Y \geq 0, X \geq \underline{X} \wedge Y \geq \underline{Y}, G, X>0 \wedge Y>0)$

Inference Rules

- Define $c \vdash (p, R, G, Q)$ by structural induction on c
- Soundness
  - If $c \vdash (p, R, G, Q)$ then $c \models (p, R, G, Q)$

Atomic Command

$$\frac{\{p\}\ c\ \{Q\}}{\langle c \rangle \vdash (p,\ preserve(p),\ Q \vee ID,\ Q)} \quad \text{(Atomic)}$$

Conditional Critical Section

$$\frac{\{p \wedge b\}\ c\ \{Q\}}{\text{await } b \text{ then } c \vdash (p,\ \text{preserve}(p),\ Q \vee ID,\ Q)} \quad \text{(Critical)}$$

Sequential Composition

$$c_1 \vdash (p_1, R, G, Q_1)$$

$$c_2 \vdash (p_2, R, G, Q_2)$$

$$Q_1 \Rightarrow p_2$$

(SEQ)

$$c_1 \; ; c_2 \vdash (p_1, R, G, (Q_1; R^*; Q_2))$$

Conditionals

$$\frac{c_1 \vdash (b_1, R, G, Q) \quad \underline{p} \wedge b \wedge R^* \Rightarrow b_1 \qquad c_2 \vdash (b_2, R, G, Q) \quad \underline{p} \wedge \neg b \wedge R^* \Rightarrow b_2}{\text{if atomic } \{b\} \text{ then } c_1 \text{ else } c_2 \vdash (p, R, G, Q)} \quad \text{(IF)}$$

Loops

$$c \vdash (j \wedge b_1, R, G, j) \qquad j \wedge b \wedge R^* \Rightarrow b_1$$

$$R \Rightarrow \mathrm{Preserve}(j)$$

$$\frac{\qquad\qquad\qquad}{\text{while atomic } \{b\} \text{ do } c \vdash (j, R, G, \neg b \wedge j)} \quad \text{(WHILE)}$$

Refinement

$$\frac{c \vdash (p, R, G, Q) \qquad p' \Rightarrow p \qquad Q \Rightarrow Q' \qquad R' \Rightarrow R \qquad G \Rightarrow G'}{c \vdash (p', R', G', Q')} \quad \text{(REFINE)}$$

Parallel Composition

$$c_1 \vdash (p_1, R_1, G_1, Q_1)$$

$$c_2 \vdash (p_2, R_2, G_2, Q_2)$$

$$G_1 \Rightarrow R_2$$

$$G_2 \Rightarrow R_1$$

(PAR)

$$c_1 \,||\, c_2 \vdash (p_1 \wedge p_1, (R_1 \wedge R2), (G_1 \vee G_2), Q)$$

where $Q = (Q_1 ; (R_1 \wedge R_2)^*; Q_2) \vee (Q_2 ; (R_1 \wedge R_2)^*; Q_1)$

Issues in R/G

- Total correctness is trickier
- Restrict the structure of the proofs
  - Sometimes global proofs are preferable
- Many design choices
  - Transitivity and Reflexivity of Rely/Guarantee
  - No standard set of rules
- Suitable for designs