Program Analysis and Verification

0368-4479

Noam Rinetzky

Lecture 4: Axiomatic Semantics - Concurrency

Slides credit: Roman Manevich, Mooly Sagiv, Eran Yahav

Axiomatic Semantics (Hoare Logic)

- Programming Language
  - Syntax (`skip` | $S_1 ; S_2$ | …)
  - Semantics (e.g., states Σ + Stmts $\langle C, s\rangle \rightarrow s$)
- Assertions
  - Syntax ($x = 3$ | $x < y + a$ | …)
  - Semantics ($[\![P]\!] \subseteq \Sigma$ alt. $s \models_p P$)
- Judgments
  - $\{P\}\ C\ \{Q\}$, $[P]\ C\ [Q]$
  - $\models_p \{P\}\ C\ \{Q\} : \forall s, s' \in \Sigma. (s \models_p P \wedge \langle C, s\rangle \rightarrow s') \Rightarrow s' \models_p Q)$
- Inference rules
- Proofs

Axiomatic semantics for **While**

Axiom for every primitive statement

[ass_p] $\{ P[a/\mathtt{x}] \}\ \mathtt{x} := a\ \{ P \}$

[skip_p] $\{ P \}\ \mathtt{skip}\ \{ P \}$

[comp_p] $$\frac{\{ P \}\ S_1\ \{ Q \}, \quad \{ Q \}\ S_2\ \{ R \}}{\{ P \}\ S_1; S_2\ \{ R \}}$$

[if_p] $$\frac{\{ b \wedge P \}\ S_1\ \{ Q \}, \quad \{ \neg b \wedge P \}\ S_2\ \{ Q \}}{\{ P \}\ \mathtt{if}\ b\ \mathtt{then}\ S_1\ \mathtt{else}\ S_2\ \{ Q \}}$$

Inference rule for every composed statement

[while_p] $$\frac{\{ b \wedge P \}\ S\ \{ P \}}{\{ P \}\ \mathtt{while}\ b\ \mathtt{do}\ S\ \{ \neg b \wedge P \}}$$

[cons_p] $$\frac{\{ P' \}\ S\ \{ Q' \}}{\{ P \}\ S\ \{ Q \}}$$ if $P \Rightarrow P'$ and $Q' \Rightarrow Q$

Factorial proof

Goal: { x=n } **`y:=1; while (x≠1) do (y:=y*x; x:=x-1)`** { **y**=$n! \land n>0$ }

W = **`while (x≠1) do (y:=y*x; x:=x-1)`**

INV = $x > 0 \Rightarrow (y \cdot x! = n! \land n \geq x)$

{ INV[x-1/x][y*x/y] } **`y:=y*x`** { INV[x-1/x] } { INV[x-1/x] } **`x:=x-1`** {INV}

[comp] ————————————————————————————

{ INV[x-1/x][y*x/y] } **`y:=y*x; x:=x-1`** {INV}

[cons] ————————————————————————————

{**x≠1** $\land$ INV } **`y:=y*x; x:=x-1`** { INV }

[while] ————————————————————————————

{ INV } W {x=1 $\land$ INV }

{ INV[1/y] } **`y:=1`** { INV }

[cons] ———————————— [cons] ————————————————————————————

{ x=n } **`y:=1`** { INV } { INV } W { **y**=$n! \land n>0$ }

[comp] ——

{ x=n } **`while (x≠1) do (y:=y*x; x:=x-1)`** { **y**=$n! \land n>0$ }

Soundness

- The inference system is sound:
  - $\vdash_p \{ P \} C \{ Q \}$ implies $\models_p \{ P \} C \{ Q \}$

Soundness and completeness

- The inference system is sound:
  - $\vdash_p \{ P \}\, C \,\{ Q \}$ implies $\models_p \{ P \}\, C \,\{ Q \}$
- The inference system is relatively complete:
  - $\models_p \{ P \}\, C \,\{ Q \}$ implies $\vdash_p \{ P \}\, C \,\{ Q \}$
    - $\forall$ A,B. A$\Rightarrow$B
    - Assertion language is expressive enough

While + Concurrency

Abstract syntax:

$$a ::= n \mid x \mid a_1 + a_2 \mid a_1 \star a_2 \mid a_1 - a_2$$

$$b ::= \mathbf{true} \mid \mathbf{false}$$

$$\mid a_1 = a_2 \mid a_1 \leq a_2 \mid \neg b \mid b_1 \wedge b_2$$

$$S ::= x := a \mid \mathbf{skip} \mid S_1; S_2$$

$$\mid \mathbf{if}\ b\ \mathbf{then}\ S_1\ \mathbf{else}\ S_2$$

$$\mid \mathbf{while}\ b\ \mathbf{do}\ S$$

$$\mid \mathbf{cobegin}\ \ S_1 \parallel \ldots \parallel S_n\ \mathbf{coend}$$

Proofs

$$\frac{\dfrac{\dots}{\{\,P_1\,\}\ S_1\,\{\,Q_2\,\}} \qquad \dfrac{\dots}{\{\,P_2\,\}\ S_2\,\{\,Q_2\,\}} \qquad \dots}{\{P_1 \wedge P_1\,\}\ S_1 \parallel S_2\,\{\,Q_2 \wedge Q_2\,\}}$$

Challenge: Interference

Axiomatic Semantics (Hoare Logic)

- Disjoint parallelism
- Global invariant
- Owicky – Gries [PhD. '76]
- Rely/Guarantee [Jones.]

$$\frac{\dots}{\{\,P\,\}\ S_1 \parallel S_2\ \{\,Q\,\}} \quad \dots$$

Disjoint Parallelism

$$\frac{\{\, P_1 \,\}\; S_1 \,\{\, Q_2 \,\} \qquad \{\, P_2 \,\}\; S_2 \,\{\, Q_2 \,\}}{\{P_1 \land P_1 \,\}\; S_1 \parallel S_2 \,\{\, Q_2 \land Q_2 \,\}}$$

$$FV(P_1,S_1,Q_1) \cap FV(P_2,S_2,Q_2) = \emptyset$$

Global Invariant

$$\frac{I \vdash \{ P_1 \}\ S_1 \{ Q_2 \} \qquad I \vdash \{ P_2 \}\ S_2 \{ Q_2 \}}{I \vdash \{P_1 \wedge P_1 \}\ S_1 \parallel S_2 \{ Q_2 \wedge Q_2 \}}$$

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

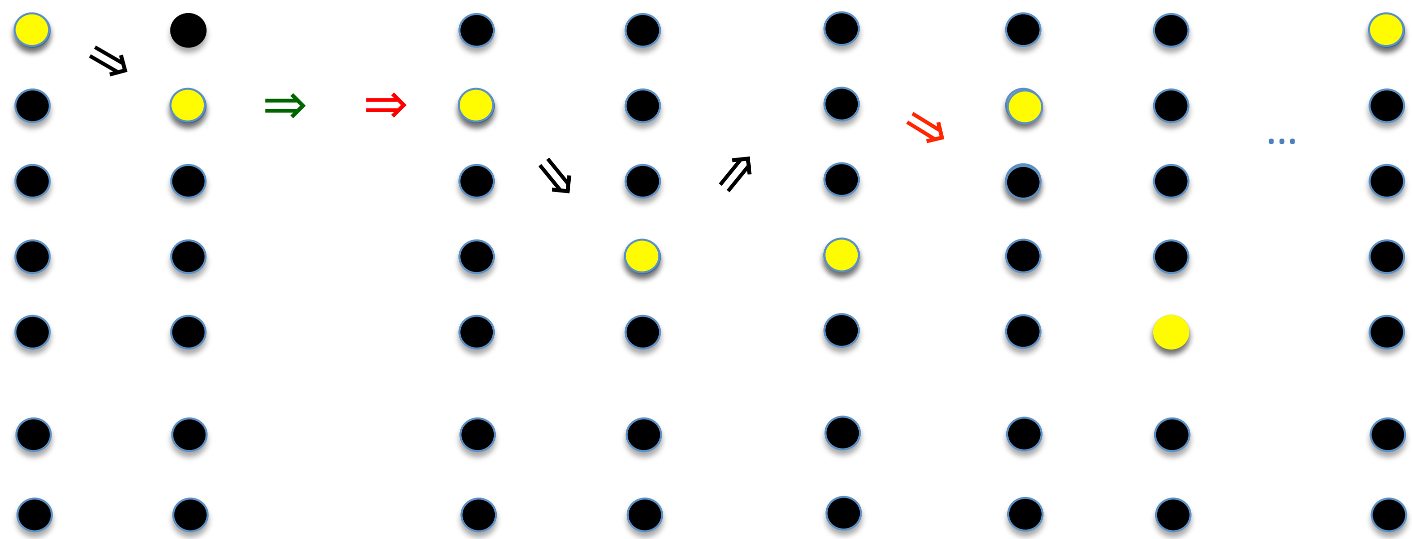
- $[\![\langle c \rangle]\!] \subseteq \Sigma \times \Sigma$

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

Meaning of (atomic) Commands

- A relation between pre-states and post-states

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

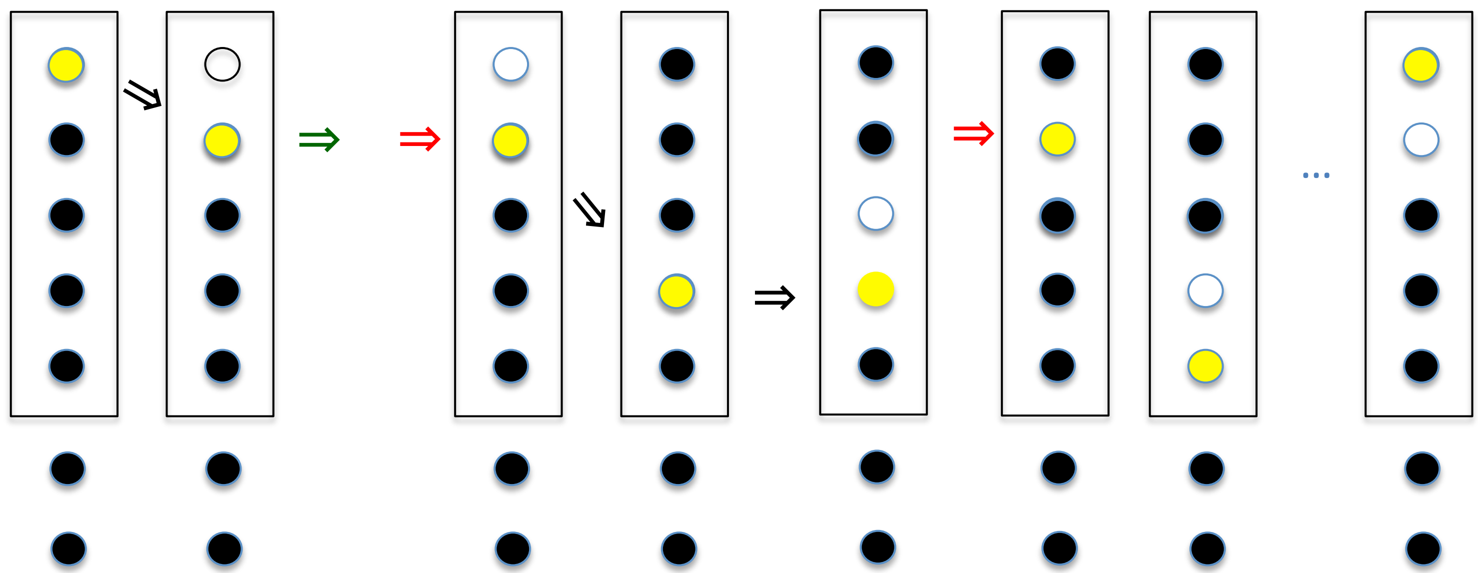


Intuition: Global Invariant

- Every (intermediate) state satisfies invariant I

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

$\mathrm{I} =$

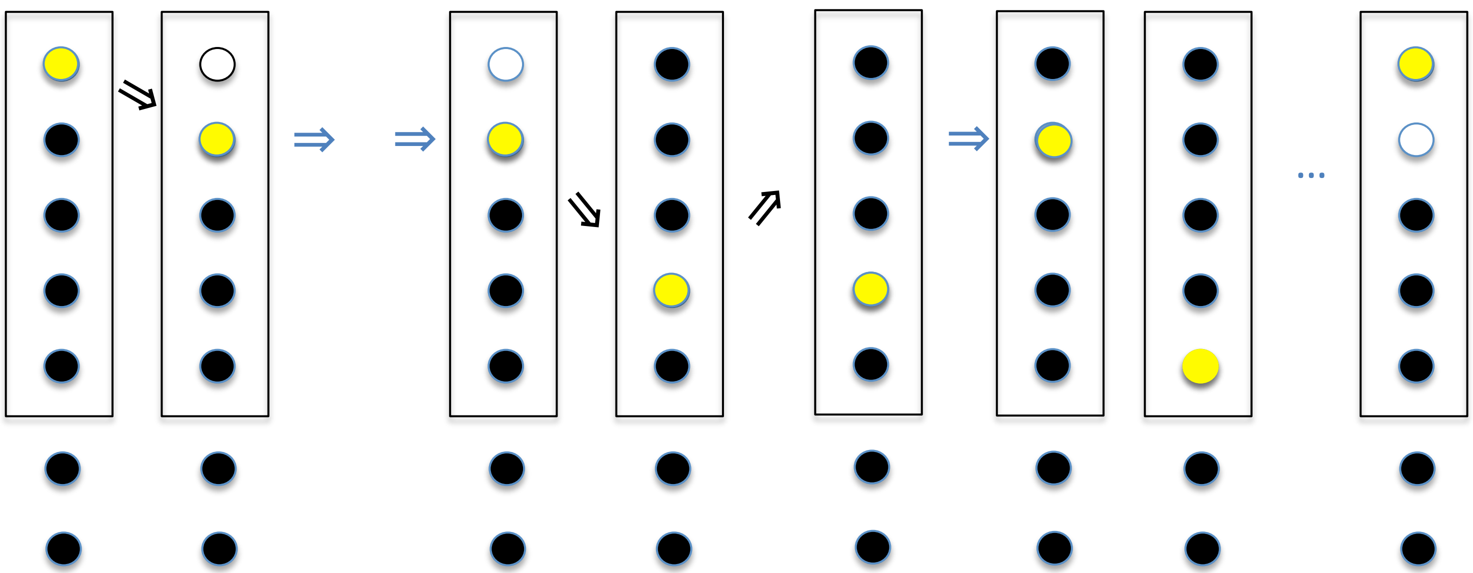


Intuition: Global Invariant

- Thread-view

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

$I =$



Global Invariant

$$\frac{I \vdash \{P\}\, S_1 \,\{Q\} \qquad I \vdash \{Q\}\, S_2 \,\{R\}}{I \vdash \{P\}\, S_1; S_2 \,\{R\}}$$

$$\frac{I \vdash \{P_1\}\ S_1 \{Q_2\} \qquad I \vdash \{P_2\}\ S_2 \{Q_2\}}{I \vdash \{P_1 \wedge P_1\}\ S_1 \parallel S_2 \{Q_2 \wedge Q_2\}}$$

Global Invariant

$$\frac{I \vdash \{P\}\, S_1 \{R\} \qquad I \vdash \{R\}\, S_2 \{Q\}}{I \vdash \{P\}\, S_1; S_2 \{Q\}} \qquad \frac{\{P \wedge I\}\, S \{Q \wedge I\}}{I \vdash \{P\}\, S \{Q\}}$$

$$\frac{I \vdash \{P_1\}\ S_1 \{Q_2\} \qquad I \vdash \{P_2\}\ S_2 \{Q_2\}}{I \vdash \{P_1 \wedge P_1\}\ S_1 \parallel S_2 \{Q_2 \wedge Q_2\}}$$

Owicky-Gries: Interference in Proofs

- A command **C** with a precondition ***pre(C)*** does not interfere with the proof of **{P} S {Q}** if:
  - **{Q ∧ pre(C) } C {Q}**
  - For any **S'** "∈" **S**: **{pre(S') ∧ pre(C) } C {pre(S')}**

- $\{P_1\}\ C_1\ \{Q_1\} \ldots \{P_k\}\ C_k\ \{Q_k\}$ are interference free if

  $\forall\ i \neq j$ and $\forall\ x := a$ "∈" C_i ,

  $x := a$ does not interfere with $\{P_j\}\ C_j\ \{Q_j\}$

Parallel Composition Rule

$$\frac{I \vdash \{\, P_1 \,\}\ S_1 \,\{\, Q_2 \,\} \qquad I \vdash \{\, P_2 \,\}\ S_2 \,\{\, Q_2 \,\}}{I \vdash \{P_1 \wedge P_1 \,\}\ S_1 \parallel S_2 \,\{\, Q_2 \wedge Q_2 \,\}}$$

$\{P_1\}\ C_1\ \{Q_1\}\ \ldots\ \{P_k\}\ C_k\ \{Q_k\}$ are interference free

Owicky-Gries: Limiations

- Checking interference can be hard
  - Non-compositionality
    - Until you finished the local proofs cannot check interference
    - Proofs need to be “saved”
      - Hard to handle libraries and missing code

- A non-standard meaning of Hoare triples
  - Depends on the interference of other threads with the proof
  - Soundness is non-trivial

- Completeness depends on auxiliary variables

Rely / Guarantee

- Aka assume Guarantee
- Cliff Jones
- Main idea: Modular capture of interference
  - Compositional proofs

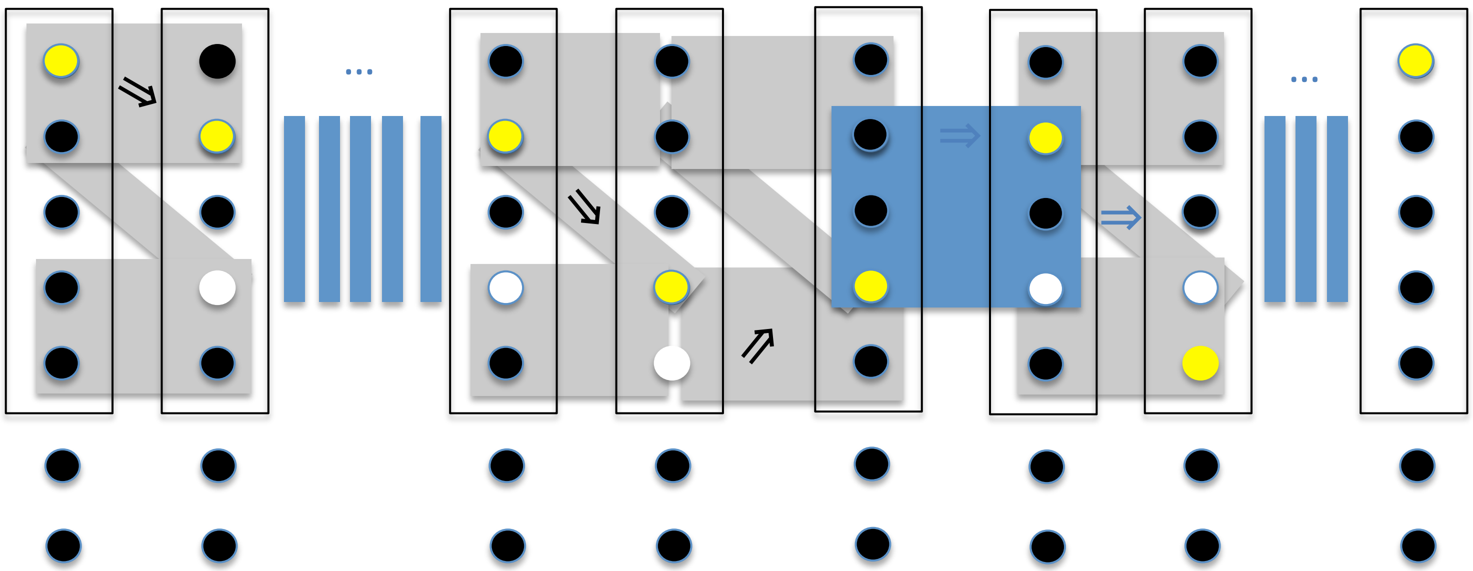
Commands as relations

- It is convenient to view the meaning of commands as relations between pre-states and post-states
- In {P} C {Q}
  - P is a one state predicate
  - Q is a two-state predicate
    - Recall auxiliary variables
- Example
  - {true} x := x + 1 {x= $\underline{x}$ + 1}

Intuition: Rely Guarantee

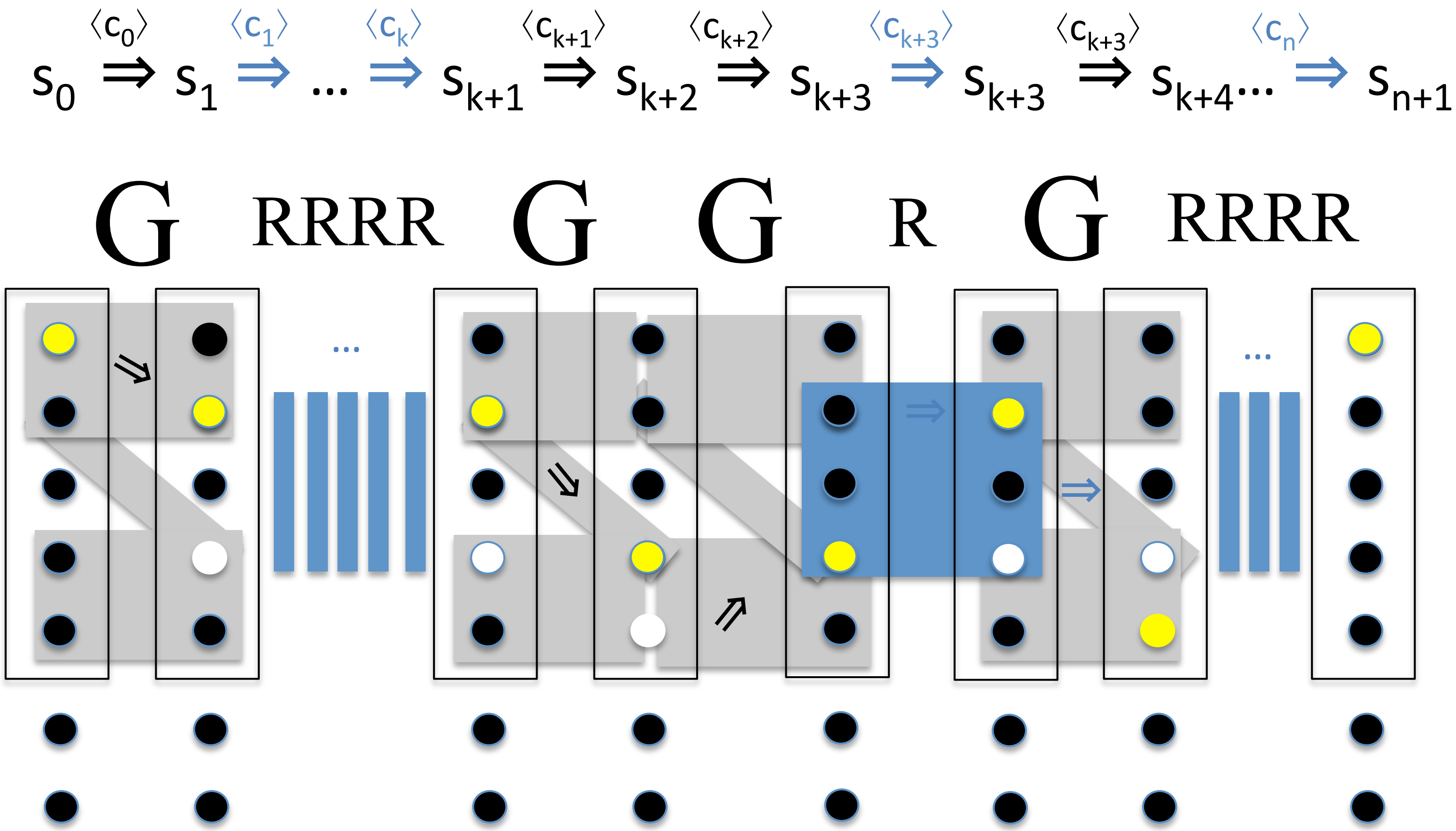
- Thread-view

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



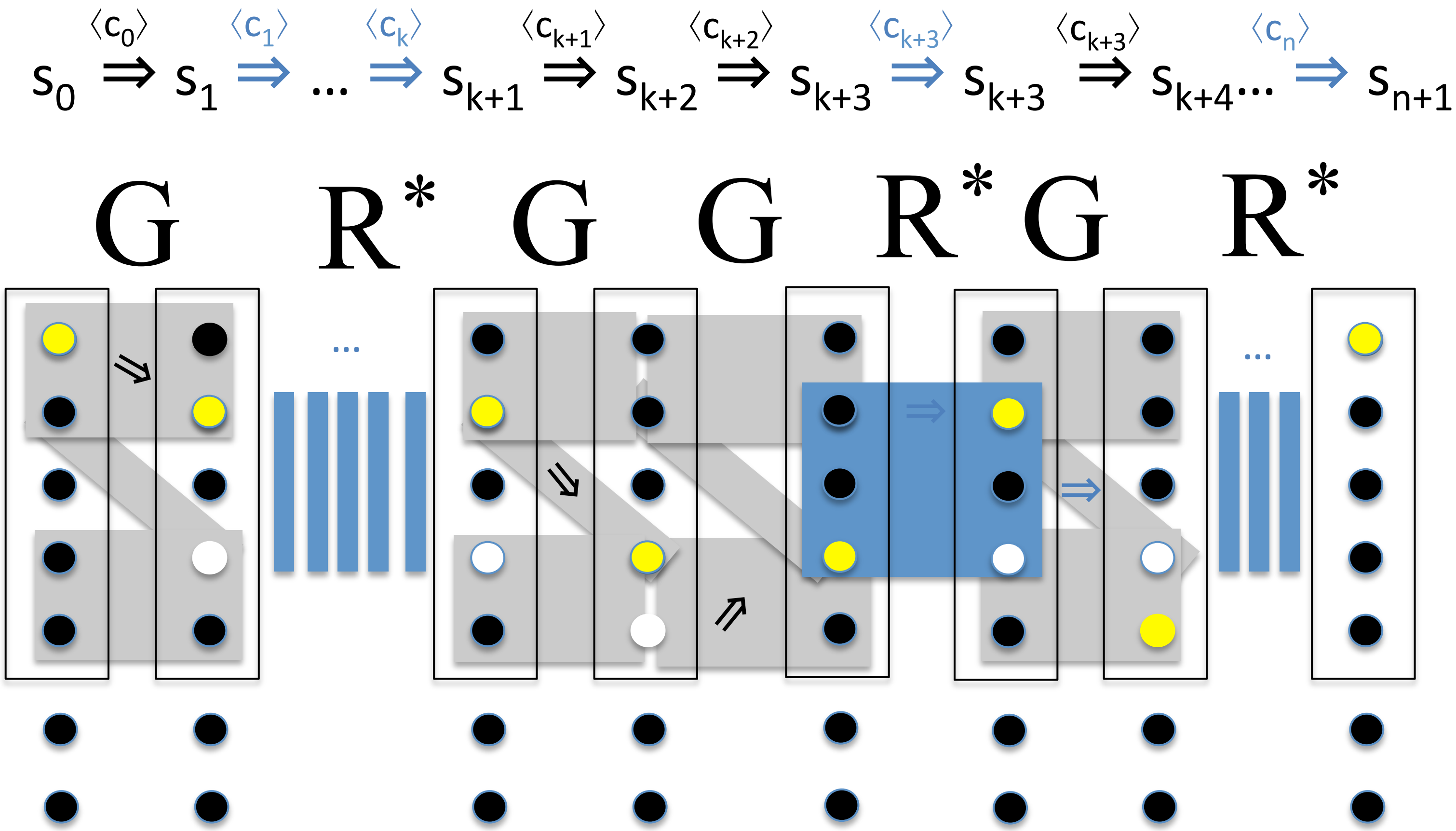
Intuition: Rely Guarantee

- Thread-view



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

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

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}

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
  - $\underline{p} \wedge R \Rightarrow p$
  - $\forall \underline{\sigma}, \sigma: p(\underline{\sigma}) \wedge R(\underline{\boldsymbol{\sigma}}, \sigma) \Rightarrow p(\sigma)$

Operations on Relations

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

Formulas

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

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
  - as usual $\sigma_4=\perp$ when c does not terminate

- $[\![C]\!]^R = \{<\sigma_1, \sigma_2, \sigma_3, \sigma_4> : \exists \sigma: <\sigma 1, \sigma> \models R \land$
  $(<C, \sigma> \Rightarrow^* \sigma_2 \land \sigma_2 = \sigma_3 = \sigma_4 \lor$
  $\exists \sigma', C' : <C, \sigma> \Rightarrow^* <C', \sigma'>$
  $\land ((\sigma_2 = \sigma_1 \lor \sigma_2 = \sigma) \land (\sigma_3 = \sigma \lor \sigma_3 = \sigma') \land \sigma_4 = \perp)$
  $\lor <\sigma', \sigma_2, \sigma_3, \sigma_4> \in [\![C']\!]^R)$

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

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

Conditional Critical Section

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

Sequential Composition

$$\frac{c_1 \vdash (p_1, R, G, Q_1) \quad c_2 \vdash (p_2, R, G, Q_2) \quad Q_1 \Rightarrow p_2}{c_1 \,;\, c_2 \vdash (p_1, R, G, (Q_1; R^*; Q_2))} \text{(SEQ)}$$

Conditionals

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

Loops

$$\frac{c \vdash (j \wedge b_1, R, G, j) \quad j \wedge b \wedge R^* \Rightarrow b_1 \qquad R \Rightarrow Preserve(j)}{\text{while atomic } \{b\} \text{ do } c \vdash (j, R, G, \neg b \wedge j)} \; (\text{WHILE})$$

Refinement

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

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