Program Analysis and Verification

0368-4479

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

Noam Rinetzky

Lecture 7: Axiomatic Semantics - Concurrency

Slides credit: Roman Manevich, Mooly Sagiv, Eran Yahav

Good manners

- Mobiles

Home Work Assignment #1 & #2

- #1 due today
  - Modulo justified extensions
- #2 Wednesday
  - Due lesson 10

Axiomatic Semantics (Hoare Logic)

- Programming Language
  - Syntax (`skip` | $S_1 ; S_2$ | …)
  - Semantics (e.g., states $\sum$ + Stmts $\langle C, s \rangle \rightarrow s$)
- Assertions
  - Syntax (x = 3 | x < y + a | …)
  - Semantics ($[\![P]\!] \subseteq \sum$ 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

$[\text{ass}_p]$ $\{ P[a/\mathtt{x}] \}\ \mathtt{x} := a \{ P \}$

$[\text{skip}_p]$ $\{ P \}\ \mathtt{skip} \{ P \}$

$[\text{comp}_p]$ $\dfrac{\{ P \} S_1 \{ Q \}, \quad \{ Q \} S_2 \{ R \}}{\{ P \} S_1; S_2 \{ R \}}$

$[\text{if}_p]$ $\dfrac{\{ b \wedge P \} S_1 \{ Q \}, \quad \{ \neg b \wedge P \} S_2 \{ Q \}}{\{ P \}\ \mathtt{if}\ b\ \mathtt{then}\ S_1\ \mathtt{else}\ S_2 \{ Q \}}$

Inference rule for every composed statement

$[\text{while}_p]$ $\dfrac{\{ b \wedge P \} S \{ P \}}{\{ P \}\ \mathtt{while}\ b\ \mathtt{do}\ S \{ \neg b \wedge P \}}$

$[\text{cons}_p]$ $\dfrac{\{ P' \} S \{ Q' \}}{\{ P \} S \{ Q \}}$ if $P \Rightarrow P'$ and $Q' \Rightarrow Q$

Factorial proof

Goal: $\{ x=n \}\ \mathbf{y:=1;\ while\ (x\neq 1)\ do\ (y:=y*x;\ x:=x-1)}\ \{ \mathbf{y}=n! \wedge n>0 \}$

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

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

$$\dfrac{\dfrac{\dfrac{\{ \mathrm{INV}[1/y] \}\ \mathbf{y:=1}\ \{ \mathrm{INV} \}}{\{ x=n \}\ \mathbf{y:=1}\ \{ \mathrm{INV} \}}\ [\mathrm{cons}] \qquad \dfrac{\dfrac{\dfrac{\{ \mathrm{INV}[x-1/x][y*x/y] \}\ \mathbf{y:=y*x}\ \{ \mathrm{INV}[x-1/x] \} \quad \{ \mathrm{INV}[x-1/x] \}\ \mathbf{x:=x-1}\ \{\mathrm{INV}\}}{\{ \mathrm{INV}[x-1/x][y*x/y] \}\ \mathbf{y:=y*x;\ x:=x-1}\ \{\mathrm{INV}\}}\ [\mathrm{comp]}}{\{ \mathbf{x\neq 1} \wedge \mathrm{INV} \}\ \mathbf{y:=y*x;\ x:=x-1}\ \{ \mathrm{INV} \}}\ [\mathrm{cons}]}{\{ \mathrm{INV} \}\ W\ \{ x=1 \wedge \mathrm{INV} \}}\ [\mathrm{while}]}{\{ \mathrm{INV} \}\ W\ \{ \mathbf{y}=n! \wedge n>0 \}}\ [\mathrm{cons}]}{\{ x=n \}\ \mathbf{while\ (x\neq 1)\ do\ (y:=y*x;\ x:=x-1)}\ \{ \mathbf{y}=n! \wedge n>0 \}}\ [\mathrm{comp}]$$

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:

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

$$b ::= \texttt{true} \mid \texttt{false}$$
$$\mid a_1 = a_2 \mid a_1 \leq a_2 \mid \neg b \mid b_1 \wedge b_2$$

$$S ::= x := a \mid \texttt{skip} \mid S_1 ; S_2$$
$$\mid \texttt{if } b \texttt{ then } S_1 \texttt{ else } S_2$$
$$\mid \texttt{while } b \texttt{ do } S$$
$$\mid \texttt{cobegin } S_1 \parallel \ldots \parallel S_n \texttt{ coend}$$

Proofs

$$\frac{\dots \qquad \dots}{\{P_1\}\ S_1\ \{Q_2\} \qquad \{P_2\}\ S_2\ \{Q_2\}}\ \dots$$

$$\{P_1 \wedge P_1\}\ S_1 \parallel S_2\ \{Q_2 \wedge Q_2\}$$

Challenge: Interference

Disjoint Parallelism

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

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

Global Invariant

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

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

- 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 $\forall\ x := a$ "$\in$" 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

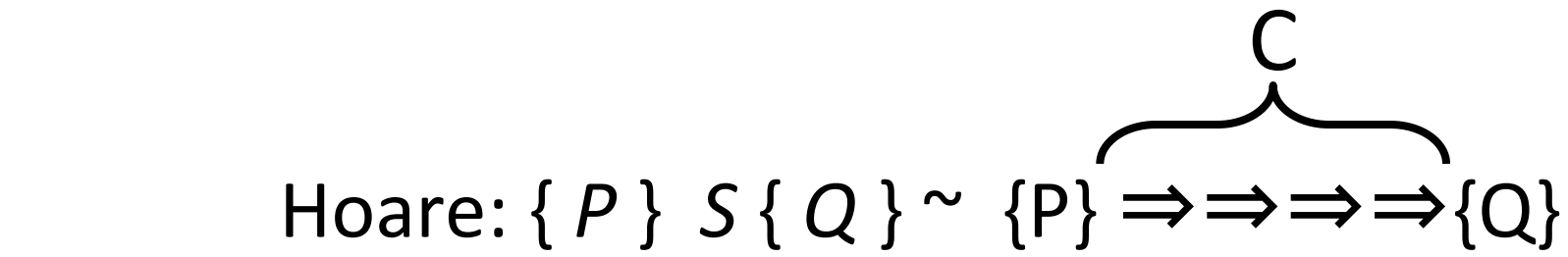
Rely / Guarantee

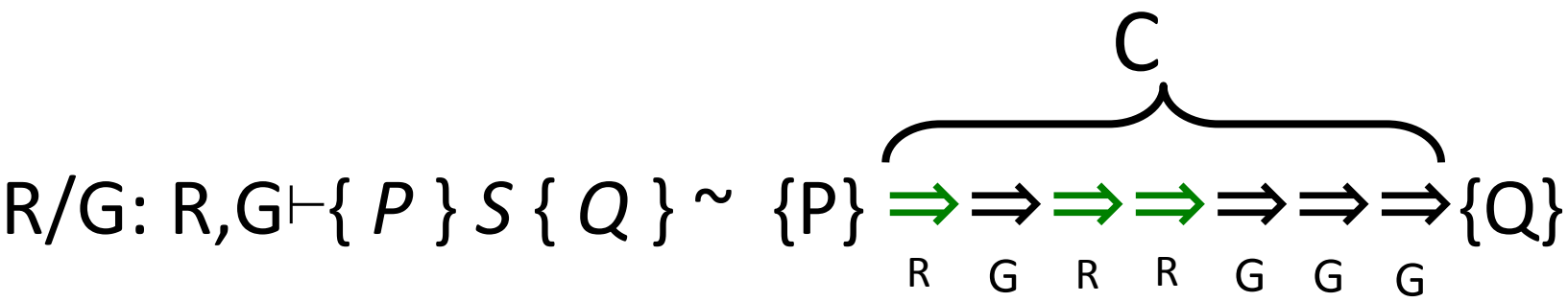
- Aka assume Guarantee
- Cliff Jones
- Main idea: Modular capture of interference
  - Compositional proofs

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





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

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

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

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

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

Conditional Critical Section

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

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

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

Loops

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

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

$$\frac{\begin{array}{c} c_1 \vdash (p_1, R_1, G_1, Q_1) \\ c_2 \vdash (p_2, R_2, G_2, Q_2) \\ G_1 \Rightarrow R_2 \\ G_2 \Rightarrow R_1 \end{array}}{c_1 \,||\, c_2 \vdash (p_1 \wedge p_1, (R_1 \wedge R2), (G_1 \vee G_2), Q)} \quad \text{(PAR)}$$

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