15–819A3 — Class Notes 4
Reasoning about Low-Level Programming Languages

John C. Reynolds
Department of Computer Science
Carnegie Mellon University

March 5, 2001 (revised)

Type Assertions

Let

$$\Gamma \quad \text{be} \quad x_1 : \tau_1, \ldots, x_n : \tau_n$$

$$\mathcal{C} \quad \text{be as in Walker's notes}$$

$$P \quad \text{be} \quad \mathcal{C} \,;\, \Gamma$$

with

$$x_1 : \tau_1, \ldots, x_n : \tau_n \vdash x_1 : \tau'_1, \ldots, x_m : \tau'_m$$
$$\text{when } 0 \leq m \leq n \text{ and } \tau_1 \leq \tau'_1 \text{ and } \ldots \text{ and } \tau_m \leq \tau'_m$$

$\mathcal{C} \vdash \mathcal{C}'$ as in Walker's notes, plus a rule for junk:

$$\frac{}{\rho \mapsto \ldots, \tau, \ldots \vdash \rho \mapsto \ldots, -, \ldots}$$

$\mathcal{C} \,;\, \Gamma \vdash \mathcal{C} \,;\, \Gamma'$ when $\mathcal{C} \vdash \mathcal{C}'$ and $\Gamma \vdash \Gamma'$

$\mathcal{C} \,;\, \Gamma \vdash E : \tau$ when $\Gamma \vdash E : \tau$

Rules of Inference

$$\frac{}{\{P\}\ \mathbf{skip}\ \{P\}}$$

$$\frac{\{P\}\ C\ \{P'\} \qquad \{P'\}\ C'\ \{P''\}}{\{P\}\ C\ ;\ C'\ \{P''\}}$$

$$\frac{P \vdash P' \qquad \{P'\}\ C\ \{P''\}}{\{P\}\ C\ \{P''\}}$$

$$\frac{\{P\}\ C\ \{P'\} \qquad P' \vdash P''}{\{P\}\ C\ \{P''\}}$$

$$\frac{P \vdash E : \mathbf{bool} \qquad \{P\}\ C_1\ \{P'\} \qquad \{P\}\ C_2\ \{P'\}}{\{P\}\ \mathbf{if}\ E\ \mathbf{then}\ C_1\ \mathbf{else}\ C_2\ \{P'\}}$$

$$\frac{P \vdash E : \mathbf{bool} \qquad \{P\}\ C\ \{P\}}{\{P\}\ \mathbf{while}\ E\ \mathbf{do}\ C\ \{P\}}$$

More Rules of Inference

$$\frac{\Gamma \vdash E : \tau}{\{\mathcal{C} \,;\, \Gamma\}\; x := E\; \{\mathcal{C} \,;\, [\,\Gamma \mid x{:}\, \tau\,]\}}$$

$$\frac{\Gamma \vdash E : \rho}{\{\mathcal{C} \wedge ((\rho \mapsto -, \ldots, \tau_i, \ldots, -) \; * \; \mathbf{true}) \,;\, \Gamma\}\; x := E.i\; \{\mathcal{C} \,;\, [\,\Gamma \mid x{:}\, \tau_i\,]\}}$$

$$\frac{}{\{\mathcal{C} \,;\, \Gamma\}\; x := \mathbf{new}\; i\; \{\mathcal{C} \; * \; (\rho \mapsto -, \ldots, -) \,;\, [\,\Gamma \mid x{:}\, \rho\,]\}}$$

where ρ is not free in $\mathcal{C}$ or Γ.

$$\frac{\Gamma \vdash E : \rho \qquad \Gamma \vdash E' : \tau}{\begin{array}{l}\{\mathcal{C} \; * \; (\rho \mapsto \tau_1, \ldots, \tau_i, \ldots, \tau_n) \,;\, \Gamma\} \\ E.i := E' \\ \{\mathcal{C} \; * \; (\rho \mapsto \tau_1, \ldots, \tau, \ldots, \tau_n) \,;\, \Gamma\}\end{array}}$$

$$\frac{\Gamma \vdash E : \rho}{\{\mathcal{C} \; * \; (\rho \mapsto -, \ldots, -) \,;\, \Gamma\}\; \mathbf{dispose}\; E\; \{\mathcal{C} \,;\, \Gamma\}}$$

An Example

$\{\rho_1 \mapsto \mathbf{int}, \rho_2 \ * \ \rho_2 \mapsto \mathbf{int}, \mathbf{nil} \,; \mathsf{x}\colon \rho_1\}$

$\mathsf{y} := \mathbf{new}\ 2 \,;$

$\{\rho_1 \mapsto \mathbf{int}, \rho_2 \ * \ \rho_2 \mapsto \mathbf{int}, \mathbf{nil} \ * \ \rho_1' \mapsto -, - \,; \mathsf{x}\colon \rho_1, \mathsf{y}\colon \rho_1'\}$

$\mathsf{y}.1 := 1 \,;$

$\{\rho_1 \mapsto \mathbf{int}, \rho_2 \ * \ \rho_2 \mapsto \mathbf{int}, \mathbf{nil} \ * \ \rho_1' \mapsto \mathbf{int}, - \,; \mathsf{x}\colon \rho_1, \mathsf{y}\colon \rho_1'\}$

$\{(\rho_1 \mapsto \mathbf{int}, \rho_2 \ * \ \rho_2 \mapsto \mathbf{int}, \mathbf{nil} \ * \ \rho_1' \mapsto \mathbf{int}, -) \wedge$
$\quad (\rho_1 \mapsto -, \rho_2 \ * \ \mathbf{true}) \,; \mathsf{x}\colon \rho_1, \mathsf{y}\colon \rho_1'\}$

$\mathsf{z} := \mathsf{x}.2 \,;$

$\{\rho_1 \mapsto \mathbf{int}, \rho_2 \ * \ \rho_2 \mapsto \mathbf{int}, \mathbf{nil} \ * \ \rho_1' \mapsto \mathbf{int}, - \,;$
$\quad \mathsf{x}\colon \rho_1, \mathsf{y}\colon \rho_1', \mathsf{z}\colon \rho_2\}$

$\mathsf{y}.2 := \mathsf{z} \,;$

$\{\rho_1 \mapsto \mathbf{int}, \rho_2 \ * \ \rho_2 \mapsto \mathbf{int}, \mathbf{nil} \ * \ \rho_1' \mapsto \mathbf{int}, \rho_2 \,;$
$\quad \mathsf{x}\colon \rho_1, \mathsf{y}\colon \rho_1', \mathsf{z}\colon \rho_2\}$

$\{\rho_1 \mapsto \mathbf{int}, \rho_2 \ * \ \rho_2 \mapsto \mathbf{int}, \mathbf{nil} \ * \ \rho_1' \mapsto \mathbf{int}, \rho_2 \,; \mathsf{x}\colon \rho_1, \mathsf{y}\colon \rho_1'\}$

$\mathbf{dispose}\ \mathsf{x} \,;$

$\{\rho_2 \mapsto \mathbf{int}, \mathbf{nil} \ * \ \rho_1' \mapsto \mathbf{int}, \rho_2 \,; \mathsf{x}\colon \rho_1, \mathsf{y}\colon \rho_1'\}$

$\mathsf{x} := \mathsf{y}$

$\{\rho_2 \mapsto \mathbf{int}, \mathbf{nil} \ * \ \rho_1' \mapsto \mathbf{int}, \rho_2 \,; \mathsf{x}\colon \rho_1', \mathsf{y}\colon \rho_1'\}$

$\{\rho_1' \mapsto \mathbf{int}, \rho_2 \ * \ \rho_2 \mapsto \mathbf{int}, \mathbf{nil} \,; \mathsf{x}\colon \rho_1'\}$

The Missing Link

$$P/\sigma \vdash P$$

where σ is a substitution of location variables for location variables.