Class Notes for CS 819A3 - Spring 2003

4. Procedures

John C. Reynolds
Department of Computer Science
Carnegie Mellon University

Revised February 25

Inference for Simple Nonrecursive Procedures

A simple procedure definition has the form

$$h(x_1, \cdots, x_m; y_1, \cdots, y_n) = c,$$

where $y_1, \cdots, y_n$ are the distinct free variables assigned by the command c, and $x_1, \cdots, x_m$ are the distinct free variables not assigned by c.

If one can prove the specification $\{p\}\ c\ \{q\}$, then one can assume the specification $\{p\}\ h(x_1, \cdots, x_m; y_1, \cdots, y_n)\ \{q\}$ in proving a specification of commands (other than c) that contains calls of h:

Simple Nonrecursive Procedures (SNPROC)

When $h(x_1, \cdots, x_m; y_1, \cdots, y_n) = c$,

$$\frac{\{p\}\ c\ \{q\}}{\{p\}\ h(x_1, \cdots, x_m; y_1, \cdots, y_n)\ \{q\}.}$$

From the conclusion of this rule, one can reason about other calls by using the rule for free variable substitution (SUB), and

$$\mathrm{FA}(h(x_1, \cdots, x_m; y_1, \cdots, y_n)) = \{y_1, \cdots, y_n\}$$
$$\mathrm{FV}(h(x_1, \cdots, x_m; y_1, \cdots, y_n)) = \{x_1, \cdots, x_m, y_1, \cdots, y_n\}$$

This rule is the same for total correctness.

Encapsulating Maximum-Finding as a Procedure

In the last section we proved the following specification of a command for finding the maximum of an array:

$$
\begin{array}{l}
[\mathsf{a} \leq \mathsf{b} \wedge \mathsf{a}\ \mathbf{to}\ \mathsf{b} \in \mathbf{dom}\ \mathsf{X}] \\
\mathbf{newvar}\ \mathsf{k}\ \mathbf{in}\ \big(\mathsf{j} := \mathsf{a}\ ;\ \mathsf{k} := \mathsf{a}\ ; \\
\quad \mathbf{while}\ \mathsf{k} < \mathsf{b}\ \mathbf{do} \\
\qquad (\mathsf{k} := \mathsf{k} + 1\ ;\ \mathbf{if}\ \mathsf{X}(\mathsf{k}) > \mathsf{X}(\mathsf{j})\ \mathbf{then}\ \mathsf{j} := \mathsf{k}\ \mathbf{else\ skip})\big) \\
[\mathsf{a}\ \mathbf{to}\ \mathsf{b} \in \mathbf{dom}\ \mathsf{X} \wedge \mathsf{a} \leq \mathsf{j} \leq \mathsf{b} \wedge \{\mathsf{X}]\mathsf{a}\ \mathbf{to}\ \mathsf{b}\} \leq^* \mathsf{X}(\mathsf{j})]
\end{array}
$$

Thus, we may define the procedure

$$
\begin{array}{l}
\mathsf{max}(\mathsf{a}, \mathsf{b}, \mathsf{X}; \mathsf{j}) = \\
\quad \mathbf{newvar}\ \mathsf{k}\ \mathbf{in}\ \big(\mathsf{j} := \mathsf{a}\ ;\ \mathsf{k} := \mathsf{a}\ ; \\
\qquad \mathbf{while}\ \mathsf{k} < \mathsf{b}\ \mathbf{do} \\
\qquad\quad (\mathsf{k} := \mathsf{k} + 1\ ;\ \mathbf{if}\ \mathsf{X}(\mathsf{k}) > \mathsf{X}(\mathsf{j})\ \mathbf{then}\ \mathsf{j} := \mathsf{k}\ \mathbf{else\ skip})\big)
\end{array}
$$

and then use the specification

$$
\begin{array}{l}
[\mathsf{a} \leq \mathsf{b} \wedge \mathsf{a}\ \mathbf{to}\ \mathsf{b} \in \mathbf{dom}\ \mathsf{X}] \\
\mathsf{max}(\mathsf{a}, \mathsf{b}, \mathsf{X}; \mathsf{j}) \\
[\mathsf{a}\ \mathbf{to}\ \mathsf{b} \in \mathbf{dom}\ \mathsf{X} \wedge \mathsf{a} \leq \mathsf{j} \leq \mathsf{b} \wedge \{\mathsf{X}]\mathsf{a}\ \mathbf{to}\ \mathsf{b}\} \leq^* \mathsf{X}(\mathsf{j})]
\end{array}
$$

to reason about calls of max.

A Procedure for Exchanging Array Elements

$$
\begin{array}{l}
\textbf{coninv}\ \mathsf{j}, \mathsf{m} \in \textbf{dom}\ \mathsf{X}\ \textbf{in} \\
\quad [[\,\mathsf{X} \mid \mathsf{j}{:}\, \mathsf{X}(\mathsf{m}) \mid \mathsf{m}{:}\, \mathsf{X}(\mathsf{j})\,] = \mathsf{X}_1] \\
\quad \textbf{newvar}\ \mathsf{t}\ \textbf{in} \\
\qquad \big(\mathsf{t} := \mathsf{X}(\mathsf{j})\ ; \\
\qquad [[\,\mathsf{X} \mid \mathsf{j}{:}\, \mathsf{X}(\mathsf{m}) \mid \mathsf{m}{:}\, \mathsf{t}\,] = \mathsf{X}_1] \\
\qquad \mathsf{X}(\mathsf{j}) := \mathsf{X}(\mathsf{m})\ ; \\
\qquad [[\,\mathsf{X} \mid \mathsf{m}{:}\, \mathsf{t}\,] = \mathsf{X}_1] \\
\qquad \mathsf{X}(\mathsf{m}) := \mathsf{t}\big) \\
\quad [\mathsf{X} = \mathsf{X}_1].
\end{array}
$$

Thus we may define the procedure

$$
\begin{array}{l}
\mathsf{exchange}(\mathsf{j}, \mathsf{m}; \mathsf{X}) = \\
\quad \textbf{newvar}\ \mathsf{t}\ \textbf{in}\ (\mathsf{t} := \mathsf{X}(\mathsf{j})\ ; \mathsf{X}(\mathsf{j}) := \mathsf{X}(\mathsf{m})\ ; \mathsf{X}(\mathsf{m}) := \mathsf{t})
\end{array}
$$

and then use the specification

$$
\begin{array}{l}
[\mathsf{j}, \mathsf{m} \in \textbf{dom}\ \mathsf{X} \wedge [\,\mathsf{X} \mid \mathsf{j}{:}\, \mathsf{X}(\mathsf{m}) \mid \mathsf{m}{:}\, \mathsf{X}(\mathsf{j})\,] = \mathsf{X}_1] \\
\mathsf{exchange}(\mathsf{j}, \mathsf{m}; \mathsf{X}) \\
[\mathsf{j}, \mathsf{m} \in \textbf{dom}\ \mathsf{X} \wedge \mathsf{X} = \mathsf{X}_1]
\end{array}
$$

to reason about calls of $\mathsf{exchange}$.

A Procedure for Exchanging Elements (continued)

From

$$[\mathsf{j}, \mathsf{m} \in \mathbf{dom}\, \mathsf{X} \wedge [\, \mathsf{X} \mid \mathsf{j}\colon \mathsf{X}(\mathsf{m}) \mid \mathsf{m}\colon \mathsf{X}(\mathsf{j})\,] = \mathsf{X}_1]$$
$$\mathsf{exchange}(\mathsf{j}, \mathsf{m}; \mathsf{X})$$
$$[\mathsf{j}, \mathsf{m} \in \mathbf{dom}\, \mathsf{X} \wedge \mathsf{X} = \mathsf{X}_1],$$

the rule of constancy (CONST) gives, for any assertion p,

$$[\mathsf{j}, \mathsf{m} \in \mathbf{dom}\, \mathsf{X} \wedge [\, \mathsf{X} \mid \mathsf{j}\colon \mathsf{X}(\mathsf{m}) \mid \mathsf{m}\colon \mathsf{X}(\mathsf{j})\,] = \mathsf{X}_1 \wedge (p/\mathsf{X} \to \mathsf{X}_1)]$$
$$\mathsf{exchange}(\mathsf{j}, \mathsf{m}; \mathsf{X})$$
$$[\mathsf{j}, \mathsf{m} \in \mathbf{dom}\, \mathsf{X} \wedge \mathsf{X} = \mathsf{X}_1 \wedge (p/\mathsf{X} \to \mathsf{X}_1)],$$

since the only variable assigned by $\mathsf{exchange}(\mathsf{j}, \mathsf{m}; \mathsf{X})$ is X, which does not occur free in $p/\mathsf{X} \to \mathsf{X}_1$.

Then existential quantification (EQ) gives

$$[\exists \mathsf{X}_1.\ \mathsf{j}, \mathsf{m} \in \mathbf{dom}\, \mathsf{X} \wedge [\, \mathsf{X} \mid \mathsf{j}\colon \mathsf{X}(\mathsf{m}) \mid \mathsf{m}\colon \mathsf{X}(\mathsf{j})\,] = \mathsf{X}_1 \wedge (p/\mathsf{X} \to \mathsf{X}_1)]$$
$$\mathsf{exchange}(\mathsf{j}, \mathsf{m}; \mathsf{X})$$
$$[\exists \mathsf{X}_1.\ \mathsf{j}, \mathsf{m} \in \mathbf{dom}\, \mathsf{X} \wedge \mathsf{X} = \mathsf{X}_1 \wedge (p/\mathsf{X} \to \mathsf{X}_1)],$$

which simplifies to

$$[\mathsf{j}, \mathsf{m} \in \mathbf{dom}\, \mathsf{X} \wedge (p/\mathsf{X} \to [\, \mathsf{X} \mid \mathsf{j}\colon \mathsf{X}(\mathsf{m}) \mid \mathsf{m}\colon \mathsf{X}(\mathsf{j})\,])]$$
$$\mathsf{exchange}(\mathsf{j}, \mathsf{m}; \mathsf{X})$$
$$[\mathsf{j}, \mathsf{m} \in \mathbf{dom}\, \mathsf{X} \wedge p],$$

providing X_1 does not occur free in p.

Sorting by Maximum Finding

$$
\begin{array}{l}
\textbf{coninv}\ \mathsf{a} - 1 \le \mathsf{b} \wedge \mathsf{a}\ \textbf{to}\ \mathsf{b} \subseteq \textbf{dom}\ \mathsf{X}\ \textbf{in} \\
\quad [\textbf{true}] \\
\quad \textbf{newvar}\ \mathsf{m}\ \textbf{in} \\
\qquad \big(\mathsf{m} := \mathsf{b}\ ; \\
\qquad [\mathsf{a} - 1 \le \mathsf{m} \le \mathsf{b} \wedge \textbf{ord}_{\le}\ (\mathsf{X}\rceil \mathsf{m} + 1\ \textbf{to}\ \mathsf{b}) \wedge \\
\qquad\quad \{\mathsf{X}\rceil \mathsf{a}\ \textbf{to}\ \mathsf{m}\} \le^{*} \{\mathsf{X}\rceil \mathsf{m} + 1\ \textbf{to}\ \mathsf{b}\}] \\
\qquad \textbf{while}\ [\textbf{vrnt}\ \mathsf{m} - \mathsf{a} + 1]\ \mathsf{a} \le \mathsf{m}\ \textbf{do}\ \textbf{newvar}\ \mathsf{j}\ \textbf{in} \\
\qquad\quad \big([\mathsf{a} \le \mathsf{m} \le \mathsf{b} \wedge \textbf{ord}_{\le}\ (\mathsf{X}\rceil \mathsf{m} + 1\ \textbf{to}\ \mathsf{b}) \wedge \\
\qquad\qquad \{\mathsf{X}\rceil \mathsf{a}\ \textbf{to}\ \mathsf{m}\} \le^{*} \{\mathsf{X}\rceil \mathsf{m} + 1\ \textbf{to}\ \mathsf{b}\} \wedge \mathsf{a}\ \textbf{to}\ \mathsf{m} \in \textbf{dom}\ \mathsf{X}] \\
\qquad\quad \mathsf{max}(\mathsf{a}, \mathsf{m}, \mathsf{X}; \mathsf{j})\ ; \\
\qquad\quad [\mathsf{a} \le \mathsf{j} \le \mathsf{m} \le \mathsf{b} \wedge \textbf{ord}_{\le}\ (\mathsf{X}\rceil \mathsf{m} + 1\ \textbf{to}\ \mathsf{b}) \wedge \\
\qquad\qquad \{\mathsf{X}\rceil \mathsf{a}\ \textbf{to}\ \mathsf{m}\} \le^{*} \{\mathsf{X}\rceil \mathsf{m} + 1\ \textbf{to}\ \mathsf{b}\} \wedge \{\mathsf{X}\rceil \mathsf{a}\ \textbf{to}\ \mathsf{m}\} \le^{*} \mathsf{X}(\mathsf{j})] \\
\qquad\qquad\ \vdots \\
\qquad\quad \mathsf{exchange}(\mathsf{j}, \mathsf{m}; \mathsf{X})\ ; \\
\qquad\quad [\mathsf{a} \le \mathsf{j} \le \mathsf{m} \le \mathsf{b} \wedge \textbf{ord}_{\le}\ (\mathsf{X}\rceil \mathsf{m} + 1\ \textbf{to}\ \mathsf{b}) \wedge \\
\qquad\qquad \{\mathsf{X}\rceil \mathsf{a}\ \textbf{to}\ \mathsf{m}\} \le^{*} \{\mathsf{X}\rceil \mathsf{m} + 1\ \textbf{to}\ \mathsf{b}\} \wedge \{\mathsf{X}\rceil \mathsf{a}\ \textbf{to}\ \mathsf{m}\} \le^{*} \mathsf{X}(\mathsf{m})] \\
\qquad\quad [\mathsf{a} - 1 \le \mathsf{m} - 1 \le \mathsf{b} \wedge \textbf{ord}_{\le}\ (\mathsf{X}\rceil \mathsf{m}\ \textbf{to}\ \mathsf{b}) \wedge \\
\qquad\qquad \{\mathsf{X}\rceil \mathsf{a}\ \textbf{to}\ \mathsf{m} - 1\} \le^{*} \{\mathsf{X}\rceil \mathsf{m}\ \textbf{to}\ \mathsf{b}\}] \\
\qquad\quad \mathsf{m} := \mathsf{m} - 1\big)\big) \\
\quad [\textbf{ord}_{\le}\ \mathsf{X}\rceil \mathsf{a}\ \textbf{to}\ \mathsf{b}]
\end{array}
$$

Reasoning about the Call of max

From

$$[\mathsf{a} \leq \mathsf{b} \wedge \mathsf{a}\ \mathbf{to}\ \mathsf{b} \in \mathbf{dom}\ \mathsf{X}]$$
$$\mathsf{max}(\mathsf{a}, \mathsf{b}, \mathsf{X}; \mathsf{j})$$
$$[\mathsf{a}\ \mathbf{to}\ \mathsf{b} \in \mathbf{dom}\ \mathsf{X} \wedge \mathsf{a} \leq \mathsf{j} \leq \mathsf{b} \wedge \{\mathsf{X}\rceil \mathsf{a}\ \mathbf{to}\ \mathsf{b}\} \leq^* \mathsf{X}(\mathsf{j})],$$

the substitution rule (SUB) and weakening consequent (WC) give

$$[\mathsf{a} \leq \mathsf{m} \wedge \mathsf{a}\ \mathbf{to}\ \mathsf{m} \in \mathbf{dom}\ \mathsf{X}]$$
$$\mathsf{max}(\mathsf{a}, \mathsf{m}, \mathsf{X}; \mathsf{j})\ ;$$
$$[\mathsf{a}\ \mathbf{to}\ \mathsf{m} \in \mathbf{dom}\ \mathsf{X} \wedge \mathsf{a} \leq \mathsf{j} \leq \mathsf{m} \wedge \{\mathsf{X}\rceil \mathsf{a}\ \mathbf{to}\ \mathsf{m}\} \leq^* \mathsf{X}(\mathsf{j})]$$
$$[\mathsf{a} \leq \mathsf{j} \leq \mathsf{m} \wedge \{\mathsf{X}\rceil \mathsf{a}\ \mathbf{to}\ \mathsf{m}\} \leq^* \mathsf{X}(\mathsf{j})].$$

Then the rule of constancy (CONST) gives

$$[\mathsf{a} \leq \mathsf{m} \leq \mathsf{b} \wedge \mathbf{ord}_{\leq}\ (\mathsf{X}\rceil \mathsf{m}+1\ \mathbf{to}\ \mathsf{b}) \wedge$$
$$\quad \{\mathsf{X}\rceil \mathsf{a}\ \mathbf{to}\ \mathsf{m}\} \leq^* \{\mathsf{X}\rceil \mathsf{m}+1\ \mathbf{to}\ \mathsf{b}\} \wedge \mathsf{a}\ \mathbf{to}\ \mathsf{m} \in \mathbf{dom}\ \mathsf{X}]$$
$$\mathsf{max}(\mathsf{a}, \mathsf{m}, \mathsf{X}; \mathsf{j})\ ;$$
$$[\mathsf{a} \leq \mathsf{j} \leq \mathsf{m} \leq \mathsf{b} \wedge \mathbf{ord}_{\leq}\ (\mathsf{X}\rceil \mathsf{m}+1\ \mathbf{to}\ \mathsf{b}) \wedge$$
$$\quad \{\mathsf{X}\rceil \mathsf{a}\ \mathbf{to}\ \mathsf{m}\} \leq^* \{\mathsf{X}\rceil \mathsf{m}+1\ \mathbf{to}\ \mathsf{b}\} \wedge \{\mathsf{X}\rceil \mathsf{a}\ \mathbf{to}\ \mathsf{m}\} \leq^* \mathsf{X}(\mathsf{j})].$$

Reasoning about the Call of exchange

From

$$[\mathsf{j}, \mathsf{m} \in \mathbf{dom}\ \mathsf{X} \wedge (p/\mathsf{X} \to [\,\mathsf{X} \mid \mathsf{j}\colon \mathsf{X}(\mathsf{m}) \mid \mathsf{m}\colon \mathsf{X}(\mathsf{j})\,])]$$
$$\mathsf{exchange}(\mathsf{j}, \mathsf{m}; \mathsf{X})$$
$$[\mathsf{j}, \mathsf{m} \in \mathbf{dom}\ \mathsf{X} \wedge p],$$

and weakening consequent (WC), we get the final step in

$$
\begin{array}{l}
\mathbf{coninv}\ \mathsf{a} - 1 \le \mathsf{b} \wedge \mathsf{a}\ \mathbf{to}\ \mathsf{b} \subseteq \mathbf{dom}\ \mathsf{X}\ \mathbf{in} \\
\quad [\mathsf{a} \le \mathsf{j} \le \mathsf{m} \le \mathsf{b} \wedge \mathbf{ord}_{\le}\ (\mathsf{X}\rceil \mathsf{m}+1\ \mathbf{to}\ \mathsf{b}) \wedge \\
\quad\quad \{\mathsf{X}\rceil \mathsf{a}\ \mathbf{to}\ \mathsf{m}\} \le^{*} \{\mathsf{X}\rceil \mathsf{m}+1\ \mathbf{to}\ \mathsf{b}\} \wedge \{\mathsf{X}\rceil \mathsf{a}\ \mathbf{to}\ \mathsf{m}\} \le^{*} \mathsf{X}(\mathsf{j})] \\
\quad [\mathsf{a} \le \mathsf{j} \le \mathsf{m} \le \mathsf{b} \wedge \mathbf{ord}_{\le}\ ([\,\mathsf{X} \mid \mathsf{j}\colon \mathsf{X}(\mathsf{m}) \mid \mathsf{m}\colon \mathsf{X}(\mathsf{j})\,]\rceil \mathsf{m}+1\ \mathbf{to}\ \mathsf{b}) \wedge \\
\quad\quad \{[\,\mathsf{X} \mid \mathsf{j}\colon \mathsf{X}(\mathsf{m}) \mid \mathsf{m}\colon \mathsf{X}(\mathsf{j})\,]\rceil \mathsf{a}\ \mathbf{to}\ \mathsf{m}\} \le^{*} \\
\quad\quad\quad \{[\,\mathsf{X} \mid \mathsf{j}\colon \mathsf{X}(\mathsf{m}) \mid \mathsf{m}\colon \mathsf{X}(\mathsf{j})\,]\rceil \mathsf{m}+1\ \mathbf{to}\ \mathsf{b}\} \wedge \\
\quad\quad \{[\,\mathsf{X} \mid \mathsf{j}\colon \mathsf{X}(\mathsf{m}) \mid \mathsf{m}\colon \mathsf{X}(\mathsf{j})\,]\rceil \mathsf{a}\ \mathbf{to}\ \mathsf{m}\} \le^{*} [\,\mathsf{X} \mid \mathsf{j}\colon \mathsf{X}(\mathsf{m}) \mid \mathsf{m}\colon \mathsf{X}(\mathsf{j})\,](\mathsf{m}) \wedge \\
\quad\quad \mathsf{j}, \mathsf{m} \in \mathbf{dom}\ \mathsf{X}] \\
\quad \mathsf{exchange}(\mathsf{j}, \mathsf{m}; \mathsf{X})\ ; \\
\quad [\mathsf{a} \le \mathsf{j} \le \mathsf{m} \le \mathsf{b} \wedge \mathbf{ord}_{\le}\ (\mathsf{X}\rceil \mathsf{m}+1\ \mathbf{to}\ \mathsf{b}) \wedge \\
\quad\quad \{\mathsf{X}\rceil \mathsf{a}\ \mathbf{to}\ \mathsf{m}\} \le^{*} \{\mathsf{X}\rceil \mathsf{m}+1\ \mathbf{to}\ \mathsf{b}\} \wedge \{\mathsf{X}\rceil \mathsf{a}\ \mathbf{to}\ \mathsf{m}\} \le^{*} \mathsf{X}(\mathsf{m})].
\end{array}
$$

The first step is justified since $\mathsf{a} \le \mathsf{j} \le \mathsf{m} \le \mathsf{b} \wedge \mathsf{a}\ \mathbf{to}\ \mathsf{b} \subseteq \mathbf{dom}\ \mathsf{X}$ implies

$$
\begin{array}{rl}
[\,\mathsf{X} \mid \mathsf{j}\colon \mathsf{X}(\mathsf{m}) \mid \mathsf{m}\colon \mathsf{X}(\mathsf{j})\,]\rceil \mathsf{m}+1\ \mathbf{to}\ \mathsf{b} & = \mathsf{X}\rceil \mathsf{m}+1\ \mathbf{to}\ \mathsf{b} \\
\{[\,\mathsf{X} \mid \mathsf{j}\colon \mathsf{X}(\mathsf{m}) \mid \mathsf{m}\colon \mathsf{X}(\mathsf{j})\,]\rceil \mathsf{a}\ \mathbf{to}\ \mathsf{m}\} & = \{[\,\mathsf{X}\rceil \mathsf{a}\ \mathbf{to}\ \mathsf{m} \mid \mathsf{j}\colon \mathsf{X}(\mathsf{m}) \mid \mathsf{m}\colon \mathsf{X}(\mathsf{j})\,]\} \\
& = \{\mathsf{X}\rceil \mathsf{a}\ \mathbf{to}\ \mathsf{m}\} \\
\mathsf{j}, \mathsf{m} & \in \mathbf{dom}\ \mathsf{X}.
\end{array}
$$

The Final Implication

Assume $\mathsf{a}\ \mathbf{to}\ \mathsf{b} \subseteq \mathbf{dom}\ \mathsf{X}$ and

$$\mathsf{a} \le \mathsf{j} \le \mathsf{m} \le \mathsf{b} \wedge \mathbf{ord}_{\le}\ (\mathsf{X}\rceil \mathsf{m}+1\ \mathbf{to}\ \mathsf{b}) \wedge \\ \{\mathsf{X}\rceil \mathsf{a}\ \mathbf{to}\ \mathsf{m}\} \le^* \{\mathsf{X}\rceil \mathsf{m}+1\ \mathbf{to}\ \mathsf{b}\} \wedge \{\mathsf{X}\rceil \mathsf{a}\ \mathbf{to}\ \mathsf{m}\} \le^* \mathsf{X}(\mathsf{m}).$$

Since $\mathsf{a} \le \mathsf{m} \le \mathsf{b}$ and $\mathsf{a}\ \mathbf{to}\ \mathsf{b} \subseteq \mathbf{dom}\ \mathsf{X}$,

$$(\mathsf{a}\ \mathbf{to}\ \mathsf{m}-1) \cup (\mathsf{m}\ \mathbf{to}\ \mathsf{m}) = (\mathsf{a}\ \mathbf{to}\ \mathsf{m}) \subseteq (\mathsf{a}\ \mathbf{to}\ \mathsf{b}) \subseteq \mathbf{dom}\ \mathsf{X}$$
$$(\mathsf{m}\ \mathbf{to}\ \mathsf{m}) \cup (\mathsf{m}+1\ \mathbf{to}\ \mathsf{b}) = (\mathsf{m}\ \mathbf{to}\ \mathsf{b}) \subseteq (\mathsf{a}\ \mathbf{to}\ \mathsf{b}) \subseteq \mathbf{dom}\ \mathsf{X},$$

and thus

$$\{\mathsf{X}\rceil \mathsf{a}\ \mathbf{to}\ \mathsf{m}-1\} \cup \{\mathsf{X}\rceil \mathsf{m}\ \mathbf{to}\ \mathsf{m}\} = \{\mathsf{X}\rceil \mathsf{a}\ \mathbf{to}\ \mathsf{m}\} \subseteq \{\mathsf{X}\rceil \mathsf{a}\ \mathbf{to}\ \mathsf{b}\}$$
$$\{\mathsf{X}\rceil \mathsf{m}\ \mathbf{to}\ \mathsf{m}\} \cup \{\mathsf{X}\rceil \mathsf{m}+1\ \mathbf{to}\ \mathsf{b}\} = \{\mathsf{X}\rceil \mathsf{m}\ \mathbf{to}\ \mathsf{b}\} \subseteq \{\mathsf{X}\rceil \mathsf{a}\ \mathbf{to}\ \mathsf{b}\}.$$

Since $\{\mathsf{X}\rceil \mathsf{a}\ \mathbf{to}\ \mathsf{m}\} \le^* \{\mathsf{X}\rceil \mathsf{m}+1\ \mathbf{to}\ \mathsf{b}\}$ and $(\mathsf{a}\ \mathbf{to}\ \mathsf{m}-1) \cup (\mathsf{m}\ \mathbf{to}\ \mathsf{m}) = (\mathsf{a}\ \mathbf{to}\ \mathsf{m})$,

$$\{\mathsf{X}\rceil \mathsf{a}\ \mathbf{to}\ \mathsf{m}-1\} \le^* \{\mathsf{X}\rceil \mathsf{m}+1\ \mathbf{to}\ \mathsf{b}\}$$
$$\{\mathsf{X}\rceil \mathsf{m}\ \mathbf{to}\ \mathsf{m}\} \le^* \{\mathsf{X}\rceil \mathsf{m}+1\ \mathbf{to}\ \mathsf{b}\}.$$

Since $\#(\mathsf{m}\ \mathbf{to}\ \mathsf{m}) = 1$,

$$\mathbf{ord}_{\le}\ (\mathsf{X}\rceil \mathsf{m}\ \mathbf{to}\ \mathsf{m}).$$

Then since $\mathbf{dom}(\mathsf{X}\rceil \mathsf{m}\ \mathbf{to}\ \mathsf{b}) = \mathsf{m}\ \mathbf{to}\ \mathsf{b}$ and $\mathsf{m} \le \mathsf{m} \le \mathsf{b}$ and

$$\mathbf{ord}_{\le}\ (\mathsf{X}\rceil \mathsf{m}\ \mathbf{to}\ \mathsf{m})$$
$$\mathbf{ord}_{\le}\ (\mathsf{X}\rceil \mathsf{m}+1\ \mathbf{to}\ \mathsf{b})$$
$$\{\mathsf{X}\rceil \mathsf{m}\ \mathbf{to}\ \mathsf{m}\} \le^* \{\mathsf{X}\rceil \mathsf{m}+1\ \mathbf{to}\ \mathsf{b}\},$$

we have

$$\mathbf{ord}_{\le}\ (\mathsf{X}\rceil \mathsf{m}\ \mathbf{to}\ \mathsf{b}).$$

The Final Implication (continued)

Next, since $\{\mathsf{X}\rceil \mathsf{a}\ \mathbf{to}\ \mathsf{m}\} \le^* \mathsf{X}(\mathsf{m})$, which abbreviates $\{\mathsf{X}\rceil \mathsf{a}\ \mathbf{to}\ \mathsf{m}\} \le^* \mathsf{X}(\mathsf{m})\ \mathbf{to}\ \mathsf{X}(\mathsf{m})$, and

$$\{\mathsf{X}\rceil \mathsf{a}\ \mathbf{to}\ \mathsf{m}-1\} \subseteq \{\mathsf{X}\rceil \mathsf{a}\ \mathbf{to}\ \mathsf{m}\}$$
$$\mathsf{X}(\mathsf{m})\ \mathbf{to}\ \mathsf{X}(\mathsf{m}) = \{X\rceil \mathsf{m}\ \mathbf{to}\ \mathsf{m}\},$$

we have

$$\{\mathsf{X}\rceil \mathsf{a}\ \mathbf{to}\ \mathsf{m}-1\} \le^* \{X\rceil \mathsf{m}\ \mathbf{to}\ \mathsf{m}\}.$$

In conjunction with

$$\{\mathsf{X}\rceil \mathsf{m}\ \mathbf{to}\ \mathsf{m}\} \cup \{\mathsf{X}\rceil \mathsf{m}+1\ \mathbf{to}\ \mathsf{b}\} = \{\mathsf{X}\rceil \mathsf{m}\ \mathbf{to}\ \mathsf{b}\}$$
$$\{\mathsf{X}\rceil \mathsf{a}\ \mathbf{to}\ \mathsf{m}-1\} \le^* \{\mathsf{X}\rceil \mathsf{m}+1\ \mathbf{to}\ \mathsf{b}\},$$

this gives

$$\{\mathsf{X}\rceil \mathsf{a}\ \mathbf{to}\ \mathsf{m}-1\} \le^* \{X\rceil \mathsf{m}\ \mathbf{to}\ \mathsf{b}\}.$$

Finally, $\mathsf{a} \le \mathsf{m} \le \mathsf{b}$ implies $\mathsf{a}-1 \le \mathsf{m}-1 \le \mathsf{b}$.

More about Functions

If **dom** $F = S$ and $\{F\} \subseteq T$, we write $F : S \rightarrow T$ and say that F is a function from S to T.

Composition and Identity

If $F\colon S \rightarrow T$ and $G\colon T \rightarrow U$, then $(F\,;G)\colon S \rightarrow U$ is the function such that $(F\,;G)(i) = G(F(i))$ for all $i \in S$. Also, $I_S\colon S \rightarrow S$, called the *identity function* on S, is the function such that $I_S(i) = i$ for all $i \in S$.

If $F\colon S \rightarrow T$, $G\colon T \rightarrow U$, and $H\colon U \rightarrow V$, then

$$(F\,;G)\,;H = F\,;(G\,;H)$$

$$I_S\,;F = F$$

$$F\,;I_T = F.$$

Also, if $F\colon S \rightarrow T$, $G\colon T \rightarrow U$, $S' \subseteq S$, $i \in S$, and $j \in T$, then

$$(F\,;G)\rceil S' = (F\rceil S')\,;G$$

$$\{F\,;G\} = \{G\rceil\{F\}\}$$

$$I_S\rceil S' = I_{S'}$$

$$\{I_S\} = S$$

$$[\,F \mid i\colon j\,]\,;G = [\,F\,;G \mid i\colon G(j)\,],$$

and if, also, $<$ is defined on S and T, and ρ is defined on U,

$$\mathbf{ord}_< F \wedge \mathbf{ord}_\rho G \Rightarrow \mathbf{ord}_\rho (F\,;G)$$

$$\mathbf{ord}_< I_S.$$

More about Functions (continued)

A function F is *injective* when

$$\forall i, j \in \mathbf{dom}\ F.\ i \neq j \Rightarrow F(i) \neq F(j).$$

If $\mathbf{dom}\ F$ is totally ordered, then F is injective iff $\mathbf{ord}_{\neq}\ F$.

A function $F\colon S \to T$ is *surjective from S to T* when

$$\{F\} = T.$$

When F is injective, and surjective from S to T, it is called a *bijection from S to T*. Thus, whenever F is injective, it is a bijection from S to T just when $S = \mathbf{dom}\ F$ and $T = \{F\}$, and is often simply called a *bijection*.

If $F\colon S \to T$ and $F^{-1}\colon T \to S$ satisfy

$$F \,;\, F^{-1} = I_S \qquad \text{and} \qquad F^{-1} \,;\, F = I_T,$$

then F^{-1} is called *the inverse* of F. (No function has more than one inverse.)

A function F possesses an inverse iff it is a bijection.

If its domain and image are totally ordered, then F is said to be *monotone* when

$$\forall i, j \in \mathbf{dom}\ F.\ i \leq j \Rightarrow F(i) \leq F(j).$$

Then

$\mathbf{ord}_{\leq}\ F$ iff F is monotone

$\mathbf{ord}_{<}\ F$ iff F is monotone and injective.

More about Bijections

If B is a (monotone) bijection from S to T and C is a (monotone) bijection from T to U, then $B\,;C$ is a (monotone) bijection from S to U, with $(B\,;C)^{-1} = C^{-1}\,;B^{-1}$.

I_S is a (monotone) bijection from S to S, with $(I_S)^{-1} = I_S$.

If B is a (monotone) bijection from S to T, then B^{-1} is a (monotone) bijection for T to S, with $(B^{-1})^{-1} = B$.

If $i \in S$ and $j \in S$, then $[\,I_S \mid i{:}\,j \mid j{:}\,i\,]$ is a bijection from S to S that is its own inverse.

The function B from $(i\ \textbf{to}\ i)$ to $(j\ \textbf{to}\ j)$ such that $B(i) = j$ is a monotone bijection with an inverse such that $B^{-1}(j) = i$.

Rearrangement and Realignment

- F is a *rearrangement* of G, written $F \sim G$ iff there is a bijection $B\colon \mathbf{dom}\ F \to \mathbf{dom}\ G$ such that $F = B \,;\, G$.
- F is a *realignment* of G, written $F \simeq G$ iff there is a monotone bijection $B\colon \mathbf{dom}\ F \to \mathbf{dom}\ G$ such that $F = B \,;\, G$.

Rearrangement and realignment are both equivalence relations:

Transitivity: $F \sim G \wedge G \sim H \Rightarrow F \sim H$

$F \simeq G \wedge G \simeq H \Rightarrow F \simeq H$

Reflexivity: $F \sim F$

$F \simeq F$

Symmetry: $F \sim G \Rightarrow G \sim F$

$F \simeq G \Rightarrow G \simeq F$

Also,

$$F \simeq G \Rightarrow F \sim G$$

$$i, j \in \mathbf{dom}\ F \Rightarrow [\, F \mid i\colon F(j) \mid j\colon F(i) \,] \sim F$$

$$\mathbf{dom}\ F = i\ \mathbf{to}\ i \wedge \mathbf{dom}\ G = j\ \mathbf{to}\ j \wedge F(i) = G(j) \Rightarrow F \simeq G$$

$$F \sim G \Rightarrow \{F\} = \{G\}$$

$$F \simeq G \wedge \mathbf{ord}_\rho\ F \Rightarrow \mathbf{ord}_\rho\ G$$

$$F \sim G \Rightarrow F \,;\, H \sim G \,;\, H$$

$$F \simeq G \Rightarrow F \,;\, H \simeq G \,;\, H$$

Reasoning about the Call of exchange (revisited)

Let

$$RR \stackrel{\text{def}}{=} \mathsf{X}\rceil \mathsf{a}\ \mathbf{to}\ \mathsf{b} \sim \mathsf{X}_0\rceil \mathsf{a}\ \mathbf{to}\ \mathsf{b}\ \wedge$$
$$\mathsf{X}\rceil(\mathbf{dom}\ \mathsf{X} - \mathsf{a}\ \mathbf{to}\ \mathsf{b}) = \mathsf{X}_0\rceil(\mathbf{dom}\ \mathsf{X} - \mathsf{a}\ \mathbf{to}\ \mathsf{b}).$$

From

$$[\mathsf{j}, \mathsf{m} \in \mathbf{dom}\ \mathsf{X} \wedge (p/\mathsf{X} \rightarrow [\,\mathsf{X} \mid \mathsf{j}{:}\, \mathsf{X}(\mathsf{m}) \mid \mathsf{m}{:}\, \mathsf{X}(\mathsf{j})\,])]$$
$$\mathsf{exchange}(\mathsf{j}, \mathsf{m}; \mathsf{X})$$
$$[\mathsf{j}, \mathsf{m} \in \mathbf{dom}\ \mathsf{X} \wedge p],$$

and weakening consequent (WC), we get the final step in

$$\mathbf{coninv}\ \mathsf{a} - 1 \le \mathsf{b} \wedge \mathsf{a}\ \mathbf{to}\ \mathsf{b} \subseteq \mathbf{dom}\ \mathsf{X}\ \mathbf{in}$$
$$[\mathsf{a} \le \mathsf{j} \le \mathsf{m} \le \mathsf{b} \wedge \cdots \wedge RR]$$
$$[\mathsf{a} \le \mathsf{j} \le \mathsf{m} \le \mathsf{b} \wedge \cdots \wedge [\,\mathsf{X} \mid \mathsf{j}{:}\, \mathsf{X}(\mathsf{m}) \mid \mathsf{m}{:}\, \mathsf{X}(\mathsf{j})\,]\rceil \mathsf{a}\ \mathbf{to}\ \mathsf{b} \sim \mathsf{X}_0\rceil \mathsf{a}\ \mathbf{to}\ \mathsf{b}\ \wedge$$
$$[\,\mathsf{X} \mid \mathsf{j}{:}\, \mathsf{X}(\mathsf{m}) \mid \mathsf{m}{:}\, \mathsf{X}(\mathsf{j})\,]\rceil(\mathbf{dom}\ \mathsf{X} - \mathsf{a}\ \mathbf{to}\ \mathsf{b}) = \mathsf{X}_0\rceil(\mathbf{dom}\ \mathsf{X} - \mathsf{a}\ \mathbf{to}\ \mathsf{b})]$$
$$\mathsf{exchange}(\mathsf{j}, \mathsf{m}; \mathsf{X})\ ;$$
$$[\mathsf{a} \le \mathsf{j} \le \mathsf{m} \le \mathsf{b} \wedge \cdots \wedge RR].$$

The first step is justified since $\mathsf{a} \le \mathsf{j} \le \mathsf{m} \le \mathsf{b} \wedge \mathsf{a}\ \mathbf{to}\ \mathsf{b} \subseteq \mathbf{dom}\ \mathsf{X}$ implies

$$[\,\mathsf{X} \mid \mathsf{j}{:}\, \mathsf{X}(\mathsf{m}) \mid \mathsf{m}{:}\, \mathsf{X}(\mathsf{j})\,]\rceil \mathsf{a}\ \mathbf{to}\ \mathsf{b} = [\,\mathsf{X}\rceil \mathsf{a}\ \mathbf{to}\ \mathsf{b} \mid \mathsf{j}{:}\, \mathsf{X}(\mathsf{m}) \mid \mathsf{m}{:}\, \mathsf{X}(\mathsf{j})\,]$$
$$\sim \mathsf{X}\rceil \mathsf{a}\ \mathbf{to}\ \mathsf{b}$$

$$[\,\mathsf{X} \mid \mathsf{j}{:}\, \mathsf{X}(\mathsf{m}) \mid \mathsf{m}{:}\, \mathsf{X}(\mathsf{j})\,]\rceil(\mathbf{dom}\ \mathsf{X} - \mathsf{a}\ \mathbf{to}\ \mathsf{b}) =$$
$$\mathsf{X}\rceil(\mathbf{dom}\ \mathsf{X} - \mathsf{a}\ \mathbf{to}\ \mathsf{b}).$$

Sorting by Maximum Finding (completed)

We conjoin RR to all the remaining assertions in our annotated specification, and then add a new precondition:

$$
\begin{array}{l}
\textbf{coninv}\ \mathsf{a} - 1 \leq \mathsf{b} \wedge \mathsf{a}\ \textbf{to}\ \mathsf{b} \subseteq \textbf{dom}\ \mathsf{X}\ \textbf{in} \\
\quad [\mathsf{X} = \mathsf{X}_0] \\
\quad [RR] \\
\quad \textbf{newvar}\ \mathsf{m}\ \textbf{in} \\
\qquad \vdots \\
\quad [\textbf{ord}_{\leq}\ \mathsf{X}]\mathsf{a}\ \textbf{to}\ \mathsf{b} \wedge RR].
\end{array}
$$

Partitioning

$$L(x) \stackrel{\text{def}}{=} \{X\rceil \mathsf{a}\ \mathbf{to}\ x\} \leq^* \mathsf{r} \qquad R(x) \stackrel{\text{def}}{=} \{X\rceil x\ \mathbf{to}\ \mathsf{b}\} >^* \mathsf{r}$$

$\mathbf{coninv}\ \mathsf{a} - 1 \leq \mathsf{b} \wedge \mathsf{a}\ \mathbf{to}\ \mathsf{b} \subseteq \mathbf{dom}\ \mathsf{X}\ \mathbf{in}$

$[RR]$

$[\mathsf{a} - 1 \leq \mathsf{a} - 1 \leq \mathsf{b} \leq \mathsf{b} \wedge L(\mathsf{a} - 1) \wedge R(\mathsf{b} + 1) \wedge RR]$

$\mathbf{newvar}\ \mathsf{d}\ \mathbf{in}$

$\big(\mathsf{c} := \mathsf{a} - 1\,;\, \mathsf{d} := \mathsf{b} + 1\,;$

$[\mathsf{a} - 1 \leq \mathsf{c} \leq \mathsf{d} - 1 \leq \mathsf{b} \wedge L(\mathsf{c}) \wedge R(\mathsf{d}) \wedge RR]$

$\mathbf{while}\ [\mathbf{vrnt}\!: \mathsf{d} - 1 - \mathsf{c}]\ \mathsf{d} - 1 - \mathsf{c} > 0\ \mathbf{do}$

$[\mathsf{a} \leq \mathsf{c} + 1 \leq \mathsf{d} - 1 \leq \mathsf{b} \wedge L(\mathsf{c}) \wedge R(\mathsf{d}) \wedge$

$\quad \mathsf{c} + 1, \mathsf{d} - 1 \in \mathbf{dom}\ \mathsf{X} \wedge RR]$

$\mathbf{if}\ \mathsf{X}(\mathsf{c} + 1) \leq \mathsf{r}\ \mathbf{then}$

$\quad [\mathsf{a} - 1 \leq \mathsf{c} + 1 \leq \mathsf{d} - 1 \leq \mathsf{b} \wedge L(\mathsf{c} + 1) \wedge R(\mathsf{d}) \wedge RR]$

$\quad \mathsf{c} := \mathsf{c} + 1$

$\mathbf{else\ if}\ \mathsf{X}(\mathsf{d} - 1) > \mathsf{r}\ \mathbf{then}$

$\quad [\mathsf{a} - 1 \leq \mathsf{c} \leq \mathsf{d} - 2 \leq \mathsf{b} \wedge L(\mathsf{c}) \wedge R(\mathsf{d} - 1) \wedge RR]$

$\quad \mathsf{d} := \mathsf{d} - 1$

$\mathbf{else}\ \big([\mathsf{X}(\mathsf{c} + 1) > \mathsf{r} \wedge \mathsf{X}(\mathsf{d} - 1) \leq \mathsf{r} \wedge \mathsf{a} \leq \mathsf{c} + 1 < \mathsf{d} - 1 \leq \mathsf{b} \wedge$

$\qquad L(\mathsf{c}) \wedge R(\mathsf{d}) \wedge \mathsf{c} + 1, \mathsf{d} - 1 \in \mathbf{dom}\ \mathsf{X} \wedge RR]$

$\quad \mathsf{exchange}(\mathsf{c} + 1, \mathsf{d} - 1; \mathsf{X})\,;$

$\quad [\mathsf{a} - 1 \leq \mathsf{c} + 1 \leq \mathsf{d} - 2 \leq \mathsf{b} \wedge L(\mathsf{c} + 1) \wedge R(\mathsf{d} - 1) \wedge RR]$

$\quad \mathsf{c} := \mathsf{c} + 1\,;\, \mathsf{d} := \mathsf{d} - 1\big)\big)$

$[\mathsf{a} - 1 \leq \mathsf{c} \leq \mathsf{b} \wedge L(\mathsf{c}) \wedge R(\mathsf{c} + 1) \wedge RR]$

Encapsulating Partitioning as a Procedure

Since we have shown

$$
\begin{array}{l}
[\mathsf{a}-1 \le \mathsf{b} \wedge \mathsf{a}\ \mathbf{to}\ \mathsf{b} \subseteq \mathbf{dom}\ \mathsf{X} \wedge RR] \\
\mathbf{newvar}\ \mathsf{d}\ \mathbf{in} \\
\quad \big(\mathsf{c} := \mathsf{a}-1\,;\ \mathsf{d} := \mathsf{b}+1\,; \\
\quad \mathbf{while}\ \mathsf{d}-1-\mathsf{c} > 0\ \mathbf{do} \\
\qquad \mathbf{if}\ \mathsf{X}(\mathsf{c}+1) \le \mathsf{r}\ \mathbf{then}\ \mathsf{c} := \mathsf{c}+1\ \mathbf{else} \\
\qquad \mathbf{if}\ \mathsf{X}(\mathsf{d}-1) > \mathsf{r}\ \mathbf{then}\ \mathsf{d} := \mathsf{d}-1\ \mathbf{else} \\
\qquad\quad (\mathsf{exchange}(\mathsf{c}+1, \mathsf{d}-1; \mathsf{X})\,;\ \mathsf{c} := \mathsf{c}+1\,;\ \mathsf{d} := \mathsf{d}-1)\big) \\
[\mathsf{a}-1 \le \mathsf{c} \le \mathsf{b} \wedge \mathsf{a}\ \mathbf{to}\ \mathsf{b} \subseteq \mathbf{dom}\ \mathsf{X} \wedge L(\mathsf{c}) \wedge R(\mathsf{c}+1) \wedge RR],
\end{array}
$$

we may define the procedure

$$
\begin{array}{l}
\mathsf{partition}(\mathsf{a}, \mathsf{b}, \mathsf{r}; \mathsf{c}, \mathsf{X}) = \mathbf{newvar}\ \mathsf{d}\ \mathbf{in} \\
\quad \big(\mathsf{c} := \mathsf{a}-1\,;\ \mathsf{d} := \mathsf{b}+1\,; \\
\quad \mathbf{while}\ \mathsf{d}-1-\mathsf{c} > 0\ \mathbf{do} \\
\qquad \mathbf{if}\ \mathsf{X}(\mathsf{c}+1) \le \mathsf{r}\ \mathbf{then}\ \mathsf{c} := \mathsf{c}+1\ \mathbf{else} \\
\qquad \mathbf{if}\ \mathsf{X}(\mathsf{d}-1) > \mathsf{r}\ \mathbf{then}\ \mathsf{d} := \mathsf{d}-1\ \mathbf{else} \\
\qquad\quad (\mathsf{exchange}(\mathsf{c}+1, \mathsf{d}-1; \mathsf{X})\,;\ \mathsf{c} := \mathsf{c}+1\,;\ \mathsf{d} := \mathsf{d}-1)\big),
\end{array}
$$

and then use the specification

$$
\begin{array}{l}
[\mathsf{a}-1 \le \mathsf{b} \wedge \mathsf{a}\ \mathbf{to}\ \mathsf{b} \subseteq \mathbf{dom}\ \mathsf{X} \wedge RR] \\
\mathsf{partition}(\mathsf{a}, \mathsf{b}, \mathsf{r}; \mathsf{c}, \mathsf{X}) \\
[\mathsf{a}-1 \le \mathsf{c} \le \mathsf{b} \wedge \mathsf{a}\ \mathbf{to}\ \mathsf{b} \subseteq \mathbf{dom}\ \mathsf{X} \wedge L(\mathsf{c}) \wedge R(\mathsf{c}+1) \wedge RR]
\end{array}
$$

to reason about calls of partition.

Inference for Simple Recursive Procedures

In the case of partial correctness, if c contains recursive calls, one can assume $\{p\}\ h(x_1, \cdots, x_m; y_1, \cdots, y_n)\ \{q\}$ in proving $\{p\}\ c\ \{q\}$:

Simple Recursive Procedures (SRPROC)

When $h(x_1, \cdots, x_m; y_1, \cdots, y_n) = c$,

$$\frac{\begin{array}{c}\{p\}\ h(x_1, \cdots, x_m; y_1, \cdots, y_n)\ \{q\} \\ \vdots \\ \{p\}\ c\ \{q\}\end{array}}{\{p\}\ h(x_1, \cdots, x_m; y_1, \cdots, y_n)\ \{q\}.}$$

Quicksort

We expect quicksort to satisfy

$$\{\mathsf{a}-1 \leq \mathsf{b} \wedge \mathsf{a} \textbf{ to } \mathsf{b} \subseteq \textbf{dom } \mathsf{X} \wedge RR\}$$
$$\mathsf{quicksort}(\mathsf{a},\mathsf{b};\mathsf{X})$$
$$\{\mathsf{a}-1 \leq \mathsf{b} \wedge \mathsf{a} \textbf{ to } \mathsf{b} \subseteq \textbf{dom } \mathsf{X} \wedge \textbf{ord}_{\leq}\ \mathsf{X}\rceil\mathsf{a} \textbf{ to } \mathsf{b} \wedge RR\}.$$

Under this assumption:

$$
\begin{array}{l}
\textbf{coninv } \mathsf{a}-1 \leq \mathsf{b} \wedge \mathsf{a} \textbf{ to } \mathsf{b} \subseteq \textbf{dom } \mathsf{X} \textbf{ in} \\
\quad \{RR\} \\
\quad \textbf{if } \mathsf{a} < \mathsf{b} \textbf{ then} \\
\quad\quad \textbf{newvar } \mathsf{c} \textbf{ in} \\
\quad\quad\quad \big(\text{“Prepare”} \ ; \\
\quad\quad\quad \{\mathsf{a}-1 < \mathsf{c} < \mathsf{b} \wedge \{\mathsf{X}\rceil\mathsf{a} \textbf{ to } \mathsf{c}\} \leq^{*} \{\mathsf{X}\rceil\mathsf{c}+1 \textbf{ to } \mathsf{b}\} \wedge RR\} \\
\quad\quad\quad \mathsf{quicksort}(\mathsf{a},\mathsf{c};\mathsf{X}) \ ; \\
\quad\quad\quad \{\mathsf{a}-1 < \mathsf{c} < \mathsf{b} \wedge \{\mathsf{X}\rceil\mathsf{a} \textbf{ to } \mathsf{c}\} \leq^{*} \{\mathsf{X}\rceil\mathsf{c}+1 \textbf{ to } \mathsf{b}\} \wedge \\
\quad\quad\quad\quad \textbf{ord}_{\leq}\ (\mathsf{X}\rceil\mathsf{a} \textbf{ to } \mathsf{c}) \wedge RR\} \\
\quad\quad\quad \mathsf{quicksort}(\mathsf{c}+1,\mathsf{b};\mathsf{X}) \\
\quad\quad\quad \{\mathsf{a}-1 < \mathsf{c} < \mathsf{b} \wedge \{\mathsf{X}\rceil\mathsf{a} \textbf{ to } \mathsf{c}\} \leq^{*} \{\mathsf{X}\rceil\mathsf{c}+1 \textbf{ to } \mathsf{b}\} \wedge \\
\quad\quad\quad\quad \textbf{ord}_{\leq}\ (\mathsf{X}\rceil\mathsf{a} \textbf{ to } \mathsf{c}) \wedge \textbf{ord}_{\leq}\ (\mathsf{X}\rceil\mathsf{c}+1 \textbf{ to } \mathsf{b}) \wedge RR\}\big) \\
\quad \textbf{else skip} \\
\quad \{\textbf{ord}_{\leq}\ \mathsf{X}\rceil\mathsf{a} \textbf{ to } \mathsf{b} \wedge RR\}.
\end{array}
$$

Reasoning about the First Call of $\mathsf{quicksort}$

From

$$\begin{array}{l}\{\mathsf{a}-1\leq\mathsf{b}\wedge\mathsf{a}\ \mathbf{to}\ \mathsf{b}\subseteq\mathbf{dom}\ \mathsf{X}\wedge RR\}\\ \mathsf{quicksort}(\mathsf{a},\mathsf{b};\mathsf{X})\\ \{\mathsf{a}-1\leq\mathsf{b}\wedge\mathsf{a}\ \mathbf{to}\ \mathsf{b}\subseteq\mathbf{dom}\ \mathsf{X}\wedge\mathbf{ord}_{\leq}\ \mathsf{X}\rceil\mathsf{a}\ \mathbf{to}\ \mathsf{b}\wedge RR\},\end{array}$$

substituting c for b and X_1 for X_0 gives

$$\begin{array}{l}\{\mathsf{a}-1\leq\mathsf{c}\wedge\mathsf{a}\ \mathbf{to}\ \mathsf{c}\subseteq\mathbf{dom}\ \mathsf{X}\wedge\\ \quad\mathsf{X}\rceil\mathsf{a}\ \mathbf{to}\ \mathsf{c}\sim\mathsf{X}_1\rceil\mathsf{a}\ \mathbf{to}\ \mathsf{c}\wedge\\ \quad\mathsf{X}\rceil(\mathbf{dom}\ \mathsf{X}-\mathsf{a}\ \mathbf{to}\ \mathsf{c})=\mathsf{X}_1\rceil(\mathbf{dom}\ \mathsf{X}-\mathsf{a}\ \mathbf{to}\ \mathsf{c})\}\\ \mathsf{quicksort}(\mathsf{a},\mathsf{c};\mathsf{X})\\ \{\mathsf{a}-1\leq\mathsf{c}\wedge\mathsf{a}\ \mathbf{to}\ \mathsf{c}\subseteq\mathbf{dom}\ \mathsf{X}\wedge\mathbf{ord}_{\leq}\ \mathsf{X}\rceil\mathsf{a}\ \mathbf{to}\ \mathsf{c}\wedge\\ \quad\mathsf{X}\rceil\mathsf{a}\ \mathbf{to}\ \mathsf{c}\sim\mathsf{X}_1\rceil\mathsf{a}\ \mathbf{to}\ \mathsf{c}\wedge\\ \quad\mathsf{X}\rceil(\mathbf{dom}\ \mathsf{X}-\mathsf{a}\ \mathbf{to}\ \mathsf{c})=\mathsf{X}_1\rceil(\mathbf{dom}\ \mathsf{X}-\mathsf{a}\ \mathbf{to}\ \mathsf{c})\}.\end{array}$$

Reasoning about the First Call (continued)

Then the rules of constancy and existential quantification give the central step in:

$$
\begin{array}{l}
\{\mathsf{a} - 1 < \mathsf{c} < \mathsf{b} \wedge \mathsf{a}\ \mathbf{to}\ \mathsf{b} \subseteq \mathbf{dom}\ \mathsf{X} \wedge \\
\quad \{\mathsf{X}\rceil\mathsf{a}\ \mathbf{to}\ \mathsf{c}\} \leq^* \{\mathsf{X}\rceil\mathsf{c}+1\ \mathbf{to}\ \mathsf{b}\} \wedge RR\} \\
\{\mathsf{a} - 1 \leq \mathsf{c} \wedge \mathsf{a}\ \mathbf{to}\ \mathsf{c} \subseteq \mathbf{dom}\ \mathsf{X} \wedge \\
\quad \mathsf{c} < \mathsf{b} \wedge \{\mathsf{X}\rceil\mathsf{a}\ \mathbf{to}\ \mathsf{c}\} \leq^* \{\mathsf{X}\rceil\mathsf{c}+1\ \mathbf{to}\ \mathsf{b}\} \wedge \\
\quad \mathsf{X}\rceil\mathsf{a}\ \mathbf{to}\ \mathsf{b} \sim \mathsf{X}_0\rceil\mathsf{a}\ \mathbf{to}\ \mathsf{b} \wedge \\
\quad \mathsf{X}\rceil(\mathbf{dom}\ \mathsf{X} - \mathsf{a}\ \mathbf{to}\ \mathsf{b}) = \mathsf{X}_0\rceil(\mathbf{dom}\ \mathsf{X} - \mathsf{a}\ \mathbf{to}\ \mathsf{b})\} \\
\{\exists \mathsf{X}_1.\ \mathsf{a} - 1 \leq \mathsf{c} \wedge \mathsf{a}\ \mathbf{to}\ \mathsf{c} \subseteq \mathbf{dom}\ \mathsf{X} \wedge \\
\quad \mathsf{X}\rceil\mathsf{a}\ \mathbf{to}\ \mathsf{c} \sim \mathsf{X}_1\rceil\mathsf{a}\ \mathbf{to}\ \mathsf{c} \wedge \\
\quad \mathsf{X}\rceil(\mathbf{dom}\ \mathsf{X} - \mathsf{a}\ \mathbf{to}\ \mathsf{c}) = \mathsf{X}_1\rceil(\mathbf{dom}\ \mathsf{X} - \mathsf{a}\ \mathbf{to}\ \mathsf{c}) \wedge \\
\quad \mathsf{c} < \mathsf{b} \wedge \{\mathsf{X}_1\rceil\mathsf{a}\ \mathbf{to}\ \mathsf{c}\} \leq^* \{\mathsf{X}_1\rceil\mathsf{c}+1\ \mathbf{to}\ \mathsf{b}\} \wedge \\
\quad \mathsf{X}_1\rceil\mathsf{a}\ \mathbf{to}\ \mathsf{b} \sim \mathsf{X}_0\rceil\mathsf{a}\ \mathbf{to}\ \mathsf{b} \wedge \\
\quad \mathsf{X}_1\rceil(\mathbf{dom}\ \mathsf{X} - \mathsf{a}\ \mathbf{to}\ \mathsf{b}) = \mathsf{X}_0\rceil(\mathbf{dom}\ \mathsf{X} - \mathsf{a}\ \mathbf{to}\ \mathsf{b})\} \\
\mathsf{quicksort}(\mathsf{a}, \mathsf{c}; \mathsf{X}) \\
\{\exists \mathsf{X}_1.\ \mathsf{a} - 1 \leq \mathsf{c} \wedge \mathsf{a}\ \mathbf{to}\ \mathsf{c} \subseteq \mathbf{dom}\ \mathsf{X} \wedge \mathbf{ord}_{\leq}\ \mathsf{X}\rceil\mathsf{a}\ \mathbf{to}\ \mathsf{c} \wedge \\
\quad \mathsf{X}\rceil\mathsf{a}\ \mathbf{to}\ \mathsf{c} \sim \mathsf{X}_1\rceil\mathsf{a}\ \mathbf{to}\ \mathsf{c} \wedge \\
\quad \mathsf{X}\rceil(\mathbf{dom}\ \mathsf{X} - \mathsf{a}\ \mathbf{to}\ \mathsf{c}) = \mathsf{X}_1\rceil(\mathbf{dom}\ \mathsf{X} - \mathsf{a}\ \mathbf{to}\ \mathsf{c}) \wedge \\
\quad \mathsf{c} < \mathsf{b} \wedge \{\mathsf{X}_1\rceil\mathsf{a}\ \mathbf{to}\ \mathsf{c}\} \leq^* \{\mathsf{X}_1\rceil\mathsf{c}+1\ \mathbf{to}\ \mathsf{b}\} \wedge \\
\quad \mathsf{X}_1\rceil\mathsf{a}\ \mathbf{to}\ \mathsf{b} \sim \mathsf{X}_0\rceil\mathsf{a}\ \mathbf{to}\ \mathsf{b} \wedge \\
\quad \mathsf{X}_1\rceil(\mathbf{dom}\ \mathsf{X} - \mathsf{a}\ \mathbf{to}\ \mathsf{b}) = \mathsf{X}_0\rceil(\mathbf{dom}\ \mathsf{X} - \mathsf{a}\ \mathbf{to}\ \mathsf{b})\} \\
\quad \vdots
\end{array}
$$

Reasoning about the First Call (continued)

$$
\begin{array}{l}
\quad\vdots \\
\{\exists \mathsf{X}_1.\ \mathsf{a}-1 \leq \mathsf{c} \wedge \mathsf{a}\ \mathbf{to}\ \mathsf{c} \subseteq \mathbf{dom}\ \mathsf{X} \wedge \mathbf{ord}_{\leq}\ \mathsf{X}\rceil\mathsf{a}\ \mathbf{to}\ \mathsf{c} \wedge \\
\quad \mathsf{X}\rceil\mathsf{a}\ \mathbf{to}\ \mathsf{c} \sim \mathsf{X}_1\rceil\mathsf{a}\ \mathbf{to}\ \mathsf{c} \wedge \\
\quad \mathsf{X}\rceil(\mathbf{dom}\ \mathsf{X} - \mathsf{a}\ \mathbf{to}\ \mathsf{c}) = \mathsf{X}_1\rceil(\mathbf{dom}\ \mathsf{X} - \mathsf{a}\ \mathbf{to}\ \mathsf{c}) \wedge \\
\quad \mathsf{c} < \mathsf{b} \wedge \{\mathsf{X}_1\rceil\mathsf{a}\ \mathbf{to}\ \mathsf{c}\} \leq^* \{\mathsf{X}_1\rceil\mathsf{c}+1\ \mathbf{to}\ \mathsf{b}\} \wedge \\
\quad \mathsf{X}_1\rceil\mathsf{a}\ \mathbf{to}\ \mathsf{b} \sim \mathsf{X}_0\rceil\mathsf{a}\ \mathbf{to}\ \mathsf{b} \wedge \\
\quad \mathsf{X}_1\rceil(\mathbf{dom}\ \mathsf{X} - \mathsf{a}\ \mathbf{to}\ \mathsf{b}) = \mathsf{X}_0\rceil(\mathbf{dom}\ \mathsf{X} - \mathsf{a}\ \mathbf{to}\ \mathsf{b})\} \\
\{\exists \mathsf{X}_1.\ \mathsf{a}-1 \leq \mathsf{c} \wedge \mathbf{ord}_{\leq}\ \mathsf{X}\rceil\mathsf{a}\ \mathbf{to}\ \mathsf{c} \wedge \\
\quad \mathsf{X}\rceil\mathsf{a}\ \mathbf{to}\ \mathsf{c} \sim \mathsf{X}_1\rceil\mathsf{a}\ \mathbf{to}\ \mathsf{c} \wedge \mathsf{X}\rceil\mathsf{c}+1\ \mathbf{to}\ \mathsf{b} = \mathsf{X}_1\rceil\mathsf{c}+1\ \mathbf{to}\ \mathsf{b} \wedge \\
\quad \mathsf{X}\rceil(\mathbf{dom}\ \mathsf{X} - \mathsf{a}\ \mathbf{to}\ \mathsf{b}) = \mathsf{X}_1\rceil(\mathbf{dom}\ \mathsf{X} - \mathsf{a}\ \mathbf{to}\ \mathsf{b}) \wedge \\
\quad \mathsf{c} < \mathsf{b} \wedge \{\mathsf{X}_1\rceil\mathsf{a}\ \mathbf{to}\ \mathsf{c}\} \leq^* \{\mathsf{X}_1\rceil\mathsf{c}+1\ \mathbf{to}\ \mathsf{b}\} \wedge \\
\quad \mathsf{X}_1\rceil\mathsf{a}\ \mathbf{to}\ \mathsf{b} \sim \mathsf{X}_0\rceil\mathsf{a}\ \mathbf{to}\ \mathsf{b} \wedge \\
\quad \mathsf{X}_1\rceil(\mathbf{dom}\ \mathsf{X} - \mathsf{a}\ \mathbf{to}\ \mathsf{b}) = \mathsf{X}_0\rceil(\mathbf{dom}\ \mathsf{X} - \mathsf{a}\ \mathbf{to}\ \mathsf{b})\} \\
\{\mathsf{a}-1 \leq \mathsf{c} \wedge \mathbf{ord}_{\leq}\ \mathsf{X}\rceil\mathsf{a}\ \mathbf{to}\ \mathsf{c} \wedge \\
\quad \mathsf{c} < \mathsf{b} \wedge \{\mathsf{X}\rceil\mathsf{a}\ \mathbf{to}\ \mathsf{c}\} \leq^* \{\mathsf{X}\rceil\mathsf{c}+1\ \mathbf{to}\ \mathsf{b}\} \wedge \\
\quad \mathsf{X}\rceil\mathsf{a}\ \mathbf{to}\ \mathsf{b} \sim \mathsf{X}_0\rceil\mathsf{a}\ \mathbf{to}\ \mathsf{b} \wedge \\
\quad \mathsf{X}\rceil(\mathbf{dom}\ \mathsf{X} - \mathsf{a}\ \mathbf{to}\ \mathsf{b}) = \mathsf{X}_0\rceil(\mathbf{dom}\ \mathsf{X} - \mathsf{a}\ \mathbf{to}\ \mathsf{b})\} \\
\{\mathsf{a}-1 < \mathsf{c} < \mathsf{b} \wedge \{\mathsf{X}\rceil\mathsf{a}\ \mathbf{to}\ \mathsf{c}\} \leq^* \{\mathsf{X}\rceil\mathsf{c}+1\ \mathbf{to}\ \mathsf{b}\} \wedge \\
\quad \mathbf{ord}_{\leq}\ (\mathsf{X}\rceil\mathsf{a}\ \mathbf{to}\ \mathsf{c}) \wedge RR\}.
\end{array}
$$

Reasoning about "Prepare"

$$
\begin{array}{l}
\textbf{coninv}\ \mathsf{a} - 1 \leq \mathsf{b} \wedge \mathsf{a}\ \textbf{to}\ \mathsf{b} \subseteq \textbf{dom}\ \mathsf{X}\ \textbf{in} \\
\quad \{\mathsf{a} < \mathsf{b} \wedge RR\} \\
\quad \textbf{if}\ \mathsf{X}(\mathsf{a}) > \mathsf{X}(\mathsf{b})\ \textbf{then} \\
\qquad \{\mathsf{a} < \mathsf{b} \wedge \mathsf{X}(\mathsf{a}) > \mathsf{X}(\mathsf{b}) \wedge RR\} \\
\qquad \{\mathsf{a} < \mathsf{b} \wedge [\,\mathsf{X} \mid \mathsf{a}\colon \mathsf{X}(\mathsf{b}) \mid \mathsf{b}\colon \mathsf{X}(\mathsf{a})\,](\mathsf{a}) \leq [\,\mathsf{X} \mid \mathsf{a}\colon \mathsf{X}(\mathsf{b}) \mid \mathsf{b}\colon \mathsf{X}(\mathsf{a})\,](\mathsf{b}) \wedge \\
\qquad\quad \mathsf{a}, \mathsf{b} \in \textbf{dom}\ \mathsf{X} \wedge RR\} \\
\qquad \mathsf{exchange}(\mathsf{a}, \mathsf{b}; \mathsf{X}) \\
\quad \textbf{else skip}\ ; \\
\quad \{\mathsf{a} < \mathsf{b} \wedge \mathsf{X}(\mathsf{a}) \leq \mathsf{X}(\mathsf{b}) \wedge RR\} \\
\quad \textbf{newvar}\ \mathsf{r}\ \textbf{in} \\
\qquad \big(\{\mathsf{a} < \mathsf{b} \wedge \mathsf{X}(\mathsf{a}) \leq (\mathsf{X}(\mathsf{a}) + \mathsf{X}(\mathsf{b})) \div 2 \leq \mathsf{X}(\mathsf{b}) \wedge RR\} \\
\qquad \mathsf{r} := (\mathsf{X}(\mathsf{a}) + \mathsf{X}(\mathsf{b})) \div 2\ ; \\
\qquad \{\mathsf{a} \leq \mathsf{b} - 1 \wedge \mathsf{X}(\mathsf{a}) \leq \mathsf{r} \leq \mathsf{X}(\mathsf{b}) \wedge \mathsf{a} + 1\ \textbf{to}\ \mathsf{b} - 1 \subseteq \textbf{dom}\ \mathsf{X} \wedge RR\} \\
\qquad \mathsf{partition}(\mathsf{a} + 1, \mathsf{b} - 1, \mathsf{r}; \mathsf{c}, \mathsf{X}) \\
\qquad \{\mathsf{a} \leq \mathsf{c} \leq \mathsf{b} - 1 \wedge \mathsf{X}(\mathsf{a}) \leq \mathsf{r} \leq \mathsf{X}(\mathsf{b}) \wedge \\
\qquad\quad \{\mathsf{X}\rceil \mathsf{a} + 1\ \textbf{to}\ \mathsf{c}\} \leq^* \mathsf{r} \wedge \{\mathsf{X}\rceil \mathsf{c} + 1\ \textbf{to}\ \mathsf{b} - 1\} >^* \mathsf{r} \wedge RR\} \\
\qquad \{\mathsf{a} \leq \mathsf{c} \leq \mathsf{b} - 1 \wedge \\
\qquad\quad \{\mathsf{X}\rceil \mathsf{a}\ \textbf{to}\ \mathsf{c}\} \leq^* \mathsf{r} \wedge \{\mathsf{X}\rceil \mathsf{c} + 1\ \textbf{to}\ \mathsf{b}\} \geq^* \mathsf{r} \wedge RR\}\big) \\
\quad \{\mathsf{a} - 1 < \mathsf{c} < \mathsf{b} \wedge \{\mathsf{X}\rceil \mathsf{a}\ \textbf{to}\ \mathsf{c}\} \leq^* \{\mathsf{X}\rceil \mathsf{c} + 1\ \textbf{to}\ \mathsf{b}\} \wedge RR\}.
\end{array}
$$

Closing the Circle of Recursion

We have shown

$$
\begin{array}{l}
\textbf{coninv}\ \mathsf{a} - 1 \leq \mathsf{b} \wedge \mathsf{a}\ \textbf{to}\ \mathsf{b} \subseteq \textbf{dom}\ \mathsf{X}\ \textbf{in} \\
\quad \{RR\} \\
\quad \textbf{if}\ \mathsf{a} < \mathsf{b}\ \textbf{then} \\
\quad\quad \textbf{newvar}\ \mathsf{c}\ \textbf{in} \\
\quad\quad\quad \big(\textbf{if}\ \mathsf{X}(\mathsf{a}) > \mathsf{X}(\mathsf{b})\ \textbf{then}\ \mathsf{exchange}(\mathsf{a}, \mathsf{b}; \mathsf{X})\ \textbf{else skip}\ ; \\
\quad\quad\quad \textbf{newvar}\ \mathsf{r}\ \textbf{in} \\
\quad\quad\quad\quad (\mathsf{r} := (\mathsf{X}(\mathsf{a}) + \mathsf{X}(\mathsf{b})) \div 2\ ; \mathsf{partition}(\mathsf{a}+1, \mathsf{b}-1, \mathsf{r}; \mathsf{c}, \mathsf{X}))\ ; \\
\quad\quad\quad \mathsf{quicksort}(\mathsf{a}, \mathsf{c}; \mathsf{X})\ ; \mathsf{quicksort}(\mathsf{c}+1, \mathsf{b}; \mathsf{X})\big) \\
\quad \textbf{else skip} \\
\quad \{\textbf{ord}_{\leq}\ \mathsf{X}\rceil \mathsf{a}\ \textbf{to}\ \mathsf{b} \wedge RR\}.
\end{array}
$$

Thus if we define

$$
\begin{array}{l}
\mathsf{quicksort}(\mathsf{a}, \mathsf{b}; \mathsf{X}) = \\
\quad \textbf{if}\ \mathsf{a} < \mathsf{b}\ \textbf{then} \\
\quad\quad \textbf{newvar}\ \mathsf{c}\ \textbf{in} \\
\quad\quad\quad \big(\textbf{if}\ \mathsf{X}(\mathsf{a}) > \mathsf{X}(\mathsf{b})\ \textbf{then}\ \mathsf{exchange}(\mathsf{a}, \mathsf{b}; \mathsf{X})\ \textbf{else skip}\ ; \\
\quad\quad\quad \textbf{newvar}\ \mathsf{r}\ \textbf{in} \\
\quad\quad\quad\quad (\mathsf{r} := (\mathsf{X}(\mathsf{a}) + \mathsf{X}(\mathsf{b})) \div 2\ ; \mathsf{partition}(\mathsf{a}+1, \mathsf{b}-1, \mathsf{r}; \mathsf{c}, \mathsf{X}))\ ; \\
\quad\quad\quad \mathsf{quicksort}(\mathsf{a}, \mathsf{c}; \mathsf{X})\ ; \mathsf{quicksort}(\mathsf{c}+1, \mathsf{b}; \mathsf{X})\big) \\
\quad \textbf{else skip},
\end{array}
$$

then $\mathsf{quicksort}$ satisfies our original assumption.

An Invariant for Merging

$$\begin{aligned}
&\mathsf{ax}-1 \le \mathsf{kx}-1 \le \mathsf{bx} \wedge \mathsf{ay}-1 \le \mathsf{ky}-1 \le \mathsf{by} \wedge \mathsf{az}-1 \le \mathsf{kz}-1 \le \mathsf{bz} \wedge \\
&\quad \mathbf{ord}_{\le}\,(\mathsf{X}\rceil\mathsf{kx}\ \mathbf{to}\ \mathsf{bx}) \wedge \mathbf{ord}_{\le}\,(\mathsf{Y}\rceil\mathsf{ky}\ \mathbf{to}\ \mathsf{by}) \wedge \mathbf{ord}_{\le}\,(\mathsf{Z}\rceil\mathsf{az}\ \mathbf{to}\ \mathsf{kz}-1) \wedge \\
&\quad \{\mathsf{Z}\rceil\mathsf{az}\ \mathbf{to}\ \mathsf{kz}-1\} \le^{*} \{\mathsf{X}\rceil\mathsf{kx}\ \mathbf{to}\ \mathsf{bx}\} \cup \{\mathsf{Y}\rceil\mathsf{ky}\ \mathbf{to}\ \mathsf{by}\} \wedge \\
&\quad \#(\mathsf{kx}\ \mathbf{to}\ \mathsf{bx}) + \#(\mathsf{ky}\ \mathbf{to}\ \mathsf{by}) = \#(\mathsf{kz}\ \mathbf{to}\ \mathsf{bz}) \wedge \\
&\quad (\mathsf{X}\rceil\mathsf{ax}\ \mathbf{to}\ \mathsf{kx}-1) \oplus (\mathsf{Y}\rceil\mathsf{ay}\ \mathbf{to}\ \mathsf{ky}-1) \sim (\mathsf{Z}\rceil\mathsf{az}\ \mathbf{to}\ \mathsf{kz}-1),
\end{aligned}$$

where $\oplus$ denotes "concatenation".

Concatenation of Sequences

A *sequence* of length n is a function whose domain is 1 **to** n.

If F and G are sequences of length m and n, then $F \oplus_{\text{seq}} G$, called the *concatenation of F and G* is the sequence of length $m + n$ such that

$$(F \oplus_{\text{seq}} G)(i) = \textbf{if } i \leq m \textbf{ then } F(i) \textbf{ else } G(i - m).$$

Laws about Sequence Concatenation

dom $(F \oplus_{\text{seq}} G)$ is the union of the disjoint sets 1 **to** m and $m + 1$ **to** $m + n$.

$$(F \oplus_{\text{seq}} G)\rceil(1 \textbf{ to } m) \;\simeq\; F$$

$$(F \oplus_{\text{seq}} G)\rceil(m+1 \textbf{ to } m+n) \;\simeq\; G$$

$$(1 \textbf{ to } m) <^* (m+1 \textbf{ to } m+n).$$

But how do we concatenate arbitrary functions?

Disjoint Union

For sets S and T, we define

$$S + T \stackrel{\text{def}}{=} \{\, \langle 1, y \rangle \mid y \in S \,\} \cup \{\, \langle 2, y \rangle \mid y \in T \,\},$$

called the *disjoint union* of S and T. When S and T are ordered, we order $S + T$ lexicographically:

$$\langle x, y \rangle \leq \langle x', y' \rangle \text{ iff } x < x' \vee (x = x' \wedge y \leq y')$$
$$\langle x, y \rangle < \langle x', y' \rangle \text{ iff } x < x' \vee (x = x' \wedge y < y').$$

Laws about Disjoint Union

$$S \subseteq S' \wedge T \subseteq T' \Rightarrow S + T \subseteq S' + T'$$
$$(S + T) \cup (S' + T') \;=\; (S \cup S') + (T \cup T')$$
$$(S + T) \cap (S' + T') \;=\; (S \cap S') + (T \cap T')$$
$$(S + T) - (S' + T') \;=\; (S - S') + (T - T').$$

Concatenation of Arbitrary Functions

If F and G are functions, then $F \oplus G$, called the *concatenation of F and G*, is the function such that

$$\begin{aligned}
\mathbf{dom}\,(F \oplus G) &= (\mathbf{dom}\ F) + (\mathbf{dom}\ G)\\
(F \oplus G)\langle 1, i\rangle &= F(i) \text{ for all } i \in \mathbf{dom}\ F\\
(F \oplus G)\langle 2, j\rangle &= G(j) \text{ for all } j \in \mathbf{dom}\ G.
\end{aligned}$$

Laws about Function Concatenation

$\mathbf{dom}\,(F \oplus G)$ is the union of the disjoint sets $\{1\} \times \mathbf{dom}\ F$ and $\{2\} \times \mathbf{dom}\ G$.

$$(F \oplus G)\rceil(\{1\} \times \mathbf{dom}\ F) \simeq F$$

$$(F \oplus G)\rceil(\{2\} \times \mathbf{dom}\ G) \simeq G$$

$$\{1\} \times \mathbf{dom}\ F <^* \{2\} \times \mathbf{dom}\ G$$

$$(F \oplus G)\rceil(S + T) = (F\rceil S) \oplus (G\rceil T)$$

$$(F \oplus G)\,;H = (F\,;H) \oplus (G\,;H)$$

$$\{F \oplus G\} = \{F\} \cup \{G\}$$

$$\mathbf{ord}_\rho\,(F \oplus G) \Leftrightarrow \mathbf{ord}_\rho\,F \wedge \mathbf{ord}_\rho\,G \wedge \{F\}\rho^*\{G\}.$$

More Laws about Function Concatenation

$$(F \oplus G) \oplus H \;\simeq\; F \oplus (G \oplus H)$$

$$F \oplus [\,] \;\simeq\; F$$

$$[\,] \oplus F \;\simeq\; F$$

$$F \oplus G \;\sim\; G \oplus F$$

$$F \sim F' \wedge G \sim G' \Rightarrow F \oplus G \sim F' \oplus G'$$

$$F \simeq F' \wedge G \simeq G' \Rightarrow F \oplus G \simeq F' \oplus G'$$

$$\mathbf{dom}\ F = S \cup T \wedge S \cap T = \{\} \Rightarrow F \sim (F \rceil S) \oplus (F \rceil T)$$

$$\mathbf{dom}\ F = S \cup T \wedge S <^{*} T \Rightarrow F \simeq (F \rceil S) \oplus (F \rceil T)$$

$$\mathbf{dom}\ F = \mathsf{a}\ \mathbf{to}\ \mathsf{c} \wedge \mathsf{a} - 1 \leq \mathsf{b} \leq \mathsf{c} \Rightarrow$$
$$F \;\simeq\; (F \rceil \mathsf{a}\ \mathbf{to}\ \mathsf{b}) \oplus (F \rceil \mathsf{b} + 1\ \mathbf{to}\ \mathsf{c}).$$

Preimages

For a set U and a function F, we define

$$\mathcal{P}(U, F) \stackrel{\text{def}}{=} \{\, i \mid i \in \mathbf{dom}\ F \wedge F(i) \in U \,\},$$

called the *preimage of* U *under* F.

Laws about Preimages

$$U \subseteq U' \Rightarrow \mathcal{P}(U, F) \subseteq \mathcal{P}(U', F)$$

$$\begin{aligned}
\mathcal{P}(U \cup U', F) &= \mathcal{P}(U, F) \cup \mathcal{P}(U', F) \\
\mathcal{P}(U \cap U', F) &= \mathcal{P}(U, F) \cap \mathcal{P}(U', F) \\
\mathcal{P}(U - U', F) &= \mathcal{P}(U, F) - \mathcal{P}(U', F)
\end{aligned}$$

$$\mathcal{P}(U, F) = \mathbf{dom}\ F \Leftrightarrow \{F\} \subseteq U$$

$$\mathcal{P}(U, F) = \{\} \Leftrightarrow U \text{ and } \{F\} \text{ are disjoint}$$

$$\begin{aligned}
\mathcal{P}(U, F\,;G) &= \mathcal{P}(\mathcal{P}(U, G), F) \\
\mathcal{P}(U, I_{U'}) &= U \cap U' \\
\mathcal{P}(U, F\rceil S) &= \mathcal{P}(U, F) \cap S \\
S \cap \mathbf{dom}\ F &\subseteq \mathcal{P}(\{F\rceil S\}, F) \\
\{F\rceil \mathcal{P}(U, F)\} &= U \cap \{F\} \\
\mathcal{P}(U, F \oplus G) &= \mathcal{P}(U, F) + \mathcal{P}(U, G)
\end{aligned}$$

$$F \sim G \Rightarrow F\rceil\mathcal{P}(U, F) \sim G\rceil\mathcal{P}(U, G)$$

$$F \simeq G \Rightarrow F\rceil\mathcal{P}(U, F) \simeq G\rceil\mathcal{P}(U, G).$$

Intersecting a Function with a Set

For a set U and a function F, we define

$$F \mathbin{\dot\cap} U \stackrel{\text{def}}{=} F \rceil \mathcal{P}(U, F),$$

called the intersection of F with U.

Laws about Function Intersection

$$\begin{aligned}
F \mathbin{\dot\cap} U = F &\Leftrightarrow \{F\} \subseteq U \\
F \mathbin{\dot\cap} U = [\,] &\Leftrightarrow \; U \text{ and } \{F\} \text{ are disjoint} \\
(F \mathbin{\dot\cap} U) \mathbin{\dot\cap} U' &= F \mathbin{\dot\cap} (U \cap U') \\
(F \oplus G) \mathbin{\dot\cap} U &= (F \mathbin{\dot\cap} U) \oplus (G \mathbin{\dot\cap} U) \\
\{F \mathbin{\dot\cap} U\} &= \{F\} \cap U \\
F \sim G &\Rightarrow F \mathbin{\dot\cap} U \sim G \mathbin{\dot\cap} U \\
F \simeq G &\Rightarrow F \mathbin{\dot\cap} U \simeq G \mathbin{\dot\cap} U.
\end{aligned}$$

An Example

$$
\begin{array}{l}
\textbf{coninv}\ \mathsf{a} - 1 \le \mathsf{b} \wedge \mathsf{a}\ \textbf{to}\ \mathsf{b} \subseteq \textbf{dom}\ \mathsf{X}\ \textbf{in} \\
\quad [\mathsf{X} = \mathsf{X}_0] \\
\quad \textbf{newvar}\ \mathsf{d}\ \textbf{in} \\
\qquad \big(\mathsf{c} := \mathsf{a} - 1\,;\ \mathsf{d} := \mathsf{a} - 1\,; \\
\qquad [\mathsf{a} - 1 \le \mathsf{c} \le \mathsf{d} \le \mathsf{b} \wedge \mathsf{X}\rceil \mathsf{a}\ \textbf{to}\ \mathsf{c} \simeq (\mathsf{X}_0\rceil \mathsf{a}\ \textbf{to}\ \mathsf{d})\ \dot{\cap}\ (\mathsf{r}\ \textbf{to}\ \mathsf{s}) \wedge \\
\qquad\quad \mathsf{X}\rceil \mathsf{d} + 1\ \textbf{to}\ \mathsf{b} = \mathsf{X}_0\rceil \mathsf{d} + 1\ \textbf{to}\ \mathsf{b}] \\
\qquad \textbf{while}\ [\textbf{vrnt}\colon \mathsf{b} - \mathsf{d}]\ \mathsf{d} < \mathsf{b}\ \textbf{do} \\
\qquad\quad [\mathsf{a} - 1 \le \mathsf{c} \le \mathsf{d} < \mathsf{b} \wedge \mathsf{X}\rceil \mathsf{a}\ \textbf{to}\ \mathsf{c} \simeq (\mathsf{X}_0\rceil \mathsf{a}\ \textbf{to}\ \mathsf{d})\ \dot{\cap}\ (\mathsf{r}\ \textbf{to}\ \mathsf{s}) \wedge \\
\qquad\qquad \mathsf{X}\rceil \mathsf{d} + 1\ \textbf{to}\ \mathsf{b} = \mathsf{X}_0\rceil \mathsf{d} + 1\ \textbf{to}\ \mathsf{b} \wedge \mathsf{c} + 1, \mathsf{d} + 1 \in \textbf{dom}\ \mathsf{X}] \\
\qquad\quad \textbf{if}\ \mathsf{X}(\mathsf{d} + 1) < \mathsf{r} \vee \mathsf{s} < \mathsf{X}(\mathsf{d} + 1)\ \textbf{then} \\
\qquad\qquad [\mathsf{a} - 1 \le \mathsf{c} \le \mathsf{d} + 1 \le \mathsf{b} \wedge \\
\qquad\qquad\quad \mathsf{X}\rceil \mathsf{a}\ \textbf{to}\ \mathsf{c} \simeq (\mathsf{X}_0\rceil \mathsf{a}\ \textbf{to}\ \mathsf{d} + 1)\ \dot{\cap}\ (\mathsf{r}\ \textbf{to}\ \mathsf{s}) \wedge \\
\qquad\qquad\quad \mathsf{X}\rceil \mathsf{d} + 2\ \textbf{to}\ \mathsf{b} = \mathsf{X}_0\rceil \mathsf{d} + 2\ \textbf{to}\ \mathsf{b}] \\
\qquad\qquad \mathsf{d} := \mathsf{d} + 1 \\
\qquad\quad \textbf{else} \\
\qquad\qquad [\mathsf{a} - 1 \le \mathsf{c} + 1 \le \mathsf{d} + 1 \le \mathsf{b} \wedge \mathsf{c} + 1, \mathsf{d} + 1 \in \textbf{dom}\ \mathsf{X} \wedge \\
\qquad\qquad\quad [\,\mathsf{X} \mid \mathsf{c} + 1\colon \mathsf{X}(\mathsf{d} + 1)\,]\rceil \mathsf{a}\ \textbf{to}\ \mathsf{c} + 1 \simeq \\
\qquad\qquad\qquad (\mathsf{X}_0\rceil \mathsf{a}\ \textbf{to}\ \mathsf{d} + 1)\ \dot{\cap}\ (\mathsf{r}\ \textbf{to}\ \mathsf{s}) \wedge \\
\qquad\qquad\quad [\,\mathsf{X} \mid \mathsf{c} + 1\colon \mathsf{X}(\mathsf{d} + 1)\,]\rceil \mathsf{d} + 2\ \textbf{to}\ \mathsf{b} = \mathsf{X}_0\rceil \mathsf{d} + 2\ \textbf{to}\ \mathsf{b}] \\
\qquad\qquad (\mathsf{X}(\mathsf{c} + 1) := \mathsf{X}(\mathsf{d} + 1)\,;\ \mathsf{c} := \mathsf{c} + 1\,;\ \mathsf{d} := \mathsf{d} + 1)\big) \\
\quad [\mathsf{a} - 1 \le \mathsf{c} \le \mathsf{b} \wedge \mathsf{X}\rceil \mathsf{a}\ \textbf{to}\ \mathsf{c} \simeq (\mathsf{X}_0\rceil \mathsf{a}\ \textbf{to}\ \mathsf{b})\ \dot{\cap}\ (\mathsf{r}\ \textbf{to}\ \mathsf{s})]
\end{array}
$$

An Example (continued)

Assume

$$\mathsf{a} - 1 \le \mathsf{c} \le \mathsf{d} < \mathsf{b} \wedge \mathsf{X}\rceil\mathsf{a}\ \mathbf{to}\ \mathsf{c} \simeq (\mathsf{X}_0\rceil\mathsf{a}\ \mathbf{to}\ \mathsf{d}) \mathbin{\dot\cap} (\mathsf{r}\ \mathbf{to}\ \mathsf{s}) \wedge \\ \mathsf{X}\rceil\mathsf{d}+1\ \mathbf{to}\ \mathsf{b} = \mathsf{X}_0\rceil\mathsf{d}+1\ \mathbf{to}\ \mathsf{b} \wedge \mathsf{c}+1, \mathsf{d}+1 \in \mathbf{dom}\ \mathsf{X}.$$

Then

$$\begin{aligned}
&(\mathsf{X}_0\rceil\mathsf{a}\ \mathbf{to}\ \mathsf{d}+1) \mathbin{\dot\cap} (\mathsf{r}\ \mathbf{to}\ \mathsf{s}) \\
&\quad \simeq ((\mathsf{X}_0\rceil\mathsf{a}\ \mathbf{to}\ \mathsf{d}) \oplus (\mathsf{X}_0\rceil\mathsf{d}+1\ \mathbf{to}\ \mathsf{d}+1)) \mathbin{\dot\cap} (\mathsf{r}\ \mathbf{to}\ \mathsf{s}) \\
&\quad = ((\mathsf{X}_0\rceil\mathsf{a}\ \mathbf{to}\ \mathsf{d}) \mathbin{\dot\cap} (\mathsf{r}\ \mathbf{to}\ \mathsf{s})) \oplus ((\mathsf{X}_0\rceil\mathsf{d}+1\ \mathbf{to}\ \mathsf{d}+1) \mathbin{\dot\cap} (\mathsf{r}\ \mathbf{to}\ \mathsf{s})) \\
&\quad \simeq (\mathsf{X}\rceil\mathsf{a}\ \mathbf{to}\ \mathsf{c}) \oplus ((\mathsf{X}\rceil\mathsf{d}+1\ \mathbf{to}\ \mathsf{d}+1) \mathbin{\dot\cap} (\mathsf{r}\ \mathbf{to}\ \mathsf{s})).
\end{aligned}$$

If $\mathsf{X}(\mathsf{d}+1) \notin \mathsf{r}\ \mathbf{to}\ \mathsf{s}$ then $\{\mathsf{X}\rceil\mathsf{d}+1\ \mathbf{to}\ \mathsf{d}+1\}$ and $\mathsf{r}\ \mathbf{to}\ \mathsf{s}$ are disjoint sets, so that

$$\begin{aligned}
\cdots &= (\mathsf{X}\rceil\mathsf{a}\ \mathbf{to}\ \mathsf{c}) \oplus [\,] \\
&\simeq \mathsf{X}\rceil\mathsf{a}\ \mathbf{to}\ \mathsf{c}.
\end{aligned}$$

On the other hand, if $\mathsf{X}(\mathsf{d}+1) \in \mathsf{r}\ \mathbf{to}\ \mathsf{s}$ then $\{\mathsf{X}\rceil\mathsf{d}+1\ \mathbf{to}\ \mathsf{d}+1\} \subseteq \mathsf{r}\ \mathbf{to}\ \mathsf{s}$, so that

$$\begin{aligned}
\cdots &= (\mathsf{X}\rceil\mathsf{a}\ \mathbf{to}\ \mathsf{c}) \oplus (\mathsf{X}\rceil\mathsf{d}+1\ \mathbf{to}\ \mathsf{d}+1) \\
&\simeq ([\,\mathsf{X} \mid \mathsf{c}+1{:}\,\mathsf{X}(\mathsf{d}+1)\,]\rceil\mathsf{a}\ \mathbf{to}\ \mathsf{c}) \oplus \\
&\qquad\qquad ([\,\mathsf{X} \mid \mathsf{c}+1{:}\,\mathsf{X}(\mathsf{d}+1)\,]\rceil\mathsf{c}+1\ \mathbf{to}\ \mathsf{c}+1) \\
&\simeq [\,\mathsf{X} \mid \mathsf{c}+1{:}\,\mathsf{X}(\mathsf{d}+1)\,]\rceil\mathsf{a}\ \mathbf{to}\ \mathsf{c}+1.
\end{aligned}$$