Proving the basic laws of ROOL in a weakest precondition semantics

Márcio Cornélio   Ana Cavalcanti   Paulo Borba   Augusto Sampaio

Centro de Informática
Universidade Federal de Pernambuco
50740-50 Recife PE Brazil
{mlc2,alcc,phmb,acas@di.ufpe.br}

Technical Report

September, 2000

Abstract. In this report we present the proof of a set of basics laws of ROOL, an object-oriented language similar to Java that includes specification constructs from refinement calculi. The proofs of the laws are developed in the weakest precondition semantics of ROOL.

1 Introduction

The laws of imperative programming are well-established and have been useful both for assisting software development and providing precise axiomatic programming language semantic definition [5,4]. In fact, besides being used as guidelines to informal programming practices, programming laws establish a sound basis for formal and rigorous software development methods. Moreover, axiomatic semantic defintions are an important tool for the design of correct compilers and code optimizers [3].

In this report we present the proofs of the basic algebraic laws of ROOL (Refinement Object-Oriented Language) [2], an object-oriented language based on Java, but with a copy semantics rather than a reference semantics. ROOL has been specially designed to allow reasoning about object-oriented programs as specifications, hence it mixes both kinds if constructs in the style of Morgan's refinement calculus [4]. The laws of commands of ROOL are similar to the laws of imperative languages. Furthermore, there are laws for commands which support object-oriented features, e.g. method calls.

The laws proved here in the weakest precondition semantics of ROOL [2,1] were presented in [6]. Such laws deals with small and medium grain constructs. Besides clarifying aspects of the semantics of ROOL, these laws serve as a basis for deriving more elaborate laws for practical applications of program transformation.

2 Lemmas

In this section, we present some lemmas that will be useful in the proofs of laws of ROOL in the remaining sections.

Lemma 1

$$
\begin{array}{ll}
[\![\Gamma \rhd \mathbf{skip}\ : \mathbf{com}]\!]\eta\ \psi & \\
= [\![\Gamma \rhd\ : [\mathbf{true}, \mathbf{true}]\ : \mathbf{com}]\!]\eta\ \psi & \text{[by definition of } \mathbf{skip}\text{]} \\
= \mathbf{true} \wedge \mathbf{true} \Rightarrow \psi & \text{[by the semantics of specification statement]} \\
= \psi & \text{[by predicate calculus]}
\end{array}
$$

Lemma 2

$$
\begin{array}{ll}
[\![\Gamma \rhd \mathbf{abort}\ : \mathbf{com}]\!]\eta\ \psi & \\
= [\![\Gamma \rhd x : [\mathbf{false}, \mathbf{true}]\ : \mathbf{com}]\!]\eta\ \psi & \text{[by definition of } \mathbf{abort}\text{]} \\
= \mathbf{false} \wedge (\forall\, x : T \bullet \mathbf{true} \Rightarrow \psi) & \\
 & \text{[by the semantics of specification statement]} \\
= \mathbf{false} & \text{[by predicate calculus]}
\end{array}
$$

Lemma 3 *If x is not free in c and ψ, then x is not free in*

$$[\![\Gamma, N \rhd c : \mathbf{com}]\!]\eta\ \psi$$

Proof Straightforward induction.

Lemma 4 *For a typing environment Γ, a class N, a proper environment η, a command c, a predicate ψ, and x a variable of type T not free in c and ψ, if y is not free in c, then*

$$[\![\Gamma;\ x : T, N \rhd c : \mathbf{com}]\!]\eta\ \psi = [\![\Gamma, N \rhd c : \mathbf{com}]\!]\eta\ \psi$$

Proof

$$\begin{array}{lr}
[\![\Gamma;\ x : T, N \rhd c : \mathbf{com}]\!]\eta\ \psi & \\
= [\![\Gamma;\ x : T, N \rhd c[y/x][x/y] : \mathbf{com}]\!]\eta\ \psi & [\text{by } y \text{ not free in } c] \\
= ([\![\Gamma, N \rhd c[y/x] : \mathbf{com}]\!]\eta\ \psi[x/y])[x/y] & [\text{by Lemma 13-[1]}] \\
= ([\![\Gamma, N \rhd c : \mathbf{com}]\!]\eta\ \psi[x/y])[x/y] & [\text{by } y \text{ not free in } c] \\
= ([\![\Gamma, N \rhd c : \mathbf{com}]\!]\eta\ \psi)[x/y] & [\text{by } x \text{ not free in } \psi] \\
= [\![\Gamma, N \rhd c : \mathbf{com}]\!]\eta\ \psi & [\text{by Lemma 3}]
\end{array}$$

3 Proofs of laws

3.1 Assignment

Law 3.1.1 <:= skip> $(le := le) = \mathbf{skip}$, provided $le \neq \mathbf{error}$

Proof

$$\begin{array}{lr}
[\![\Gamma \rhd le := le\ : \mathbf{com}]\!]\eta\ \psi & \\
= le \neq \mathbf{error} \wedge \psi[le/le] & [\text{by the semantics of assignment}] \\
= \psi & [\text{by the hypothesis and a property of substitution}] \\
= [\![\Gamma \rhd \mathbf{skip}\ : \mathbf{com}]\!]\eta\ \psi & [\text{by Lemma 1}]
\end{array}$$

Law 3.1.2 <:= identity > $(le, le_1 := e, le_1) = (le := e)$, provided $e \neq \mathbf{error}$

Proof

$$\begin{array}{lr}
[\![\Gamma \rhd le, le_1 := e, le_1\ : \mathbf{com}]\!]\eta\ \psi & \\
= e \neq \mathbf{error} \wedge le_1 \neq \mathbf{error} \wedge \psi[e, le_1/le, le_1] & \\
& [\text{by the semantics of assignment}] \\
= e \neq \mathbf{error} \wedge \psi[e/le] & [\text{by the hypothesis and a property of substitution}] \\
= [\![\Gamma \rhd le := e\ : \mathbf{com}]\!]\eta\ \psi & [\text{by the semantics of assignment}]
\end{array}$$

Law 3.1.3 <:= symmetry> If i ranges over $1..n$ and π is any permutation of $1..n$, then $(le_i := e_i) = (le_{\pi(i)} := e_{\pi(i)})$, provided $e_i \neq \textbf{error}$

Proof

$$
\begin{aligned}
& [\![\mathit{\Gamma} \triangleright le_i := e_i \ : \textbf{com}]\!] \eta\ \psi \\
& = le_i \neq \textbf{error} \wedge \psi[e_i / le_i] && \text{[by the semantics of assignment]} \\
& = le_{\pi(i)} \neq \textbf{error} \wedge \psi[e_{\pi(i)} / le_{\pi(i)}] && \text{[by a property a substitution]} \\
& = [\![\mathit{\Gamma} \triangleright le_{\pi(i)} := e_{\pi(i)} \ : \textbf{com}]\!] \eta\ \psi && \text{[by the semantics of assignment]}
\end{aligned}
$$

3.2 Conditional

Law 3.2.1 < **if** symmetry> If i ranges over $1..n$ and π is any permutation of $1..n$, then $\textbf{if}\ []i \bullet \psi_i \ \rightarrow\ c_i\ \textbf{fi} = \textbf{if}\ []i \bullet \psi_{\pi(i)} \ \rightarrow\ c_{\pi(i)}\ \textbf{fi}$

Proof

$$
\begin{aligned}
& [\![\mathit{\Gamma} \triangleright \textbf{if}[]i \bullet \psi_i \ \rightarrow\ c_i\ \textbf{fi} : \textbf{com}]\!] \eta\ \psi \\
& = (\vee\ i \bullet \psi_i) \wedge (\wedge\ i \bullet \psi_i \Rightarrow [\![\mathit{\Gamma} \triangleright c_i : \textbf{com}]\!] \eta\ \psi) \\
& && \text{[by the semantics of alternation]} \\
& = (\vee\ i \bullet \psi_{\pi(i)}) \wedge (\wedge\ i \bullet \psi_{\pi(i)} \Rightarrow [\![\mathit{\Gamma} \triangleright c_{\pi(i)} : \textbf{com}]\!] \eta\ \psi) \\
& && \text{[by commutativity of disjunction and conjunction]} \\
& = [\![\mathit{\Gamma} \triangleright \textbf{if}[]i \bullet \psi_{\pi(i)} \ \rightarrow\ c_{\pi(i)}\ \textbf{fi} : \textbf{com}]\!] \eta\ \psi && \text{[by the semantics of alternation]}
\end{aligned}
$$

Law 3.2.2 < **if** true guard> $\textbf{if true} \ \rightarrow\ c\ \textbf{fi} = c$

Proof

$$
\begin{aligned}
& [\![\mathit{\Gamma} \triangleright \textbf{if true} \ \rightarrow\ c\ \textbf{fi} : \textbf{com}]\!] \eta\ \psi \\
& = \textbf{true} \wedge \textbf{true} \Rightarrow [\![\mathit{\Gamma} \triangleright c : \textbf{com}]\!] \eta\ \psi && \text{[by the semantics of alternation]} \\
& = [\![\mathit{\Gamma} \triangleright c : \textbf{com}]\!] \eta\ \psi
\end{aligned}
$$

Law 3.2.3 < **if** false unity> $\textbf{if false} \ \rightarrow\ c\ []\ \psi_i \ \rightarrow\ c_i\ \textbf{fi} = \textbf{if}\ \psi_i \ \rightarrow\ c_i\ \textbf{fi}$

Proof

$$
\begin{aligned}
& [\![\mathit{\Gamma} \triangleright \textbf{if false} \ \rightarrow\ c\ []\ \psi_i \ \rightarrow\ c_i\ \textbf{fi} : \textbf{com}]\!] \eta\ \psi \\
& = (\vee\ i \bullet \psi_i \vee \textbf{false}) \wedge (\textbf{false} \Rightarrow [\![\mathit{\Gamma} \triangleright c : \textbf{com}]\!] \eta\ \psi) \wedge \\
& (\wedge\ i \bullet \psi_i \Rightarrow [\![\mathit{\Gamma} \triangleright c_i : \textbf{com}]\!] \eta\ \psi) && \text{[by the semantics of alternation]} \\
& = (\vee\ i \bullet \psi_i) \wedge (\wedge\ i \bullet \psi_i \Rightarrow [\![\mathit{\Gamma} \triangleright c_i : \textbf{com}]\!] \eta\ \psi) && \text{[by predicate calculus]} \\
& = [\![\mathit{\Gamma} \triangleright \textbf{if}\ \psi_i \ \rightarrow\ c_i\ \textbf{fi} : \textbf{com}]\!] \eta\ \psi && \text{[by the semantics of alternation]}
\end{aligned}
$$

Law 3.2.4 < **if abort** unity> **if** () **fi** = **abort**

Proof

$[\![\Gamma \rhd \textbf{if}\ ()\ \textbf{fi} : \textbf{com}]\!]\eta\ \psi$
$= \textbf{false}$ [by the semantics of alternation and predicate calculus]
$= [\![\Gamma \rhd \textbf{abort} : \textbf{com}]\!]\eta\ \psi$ [by Lemma 2]

Law 3.2.5 < **if** - $\vee$ distrib1> **if** $\psi_1 \rightarrow c[]\psi_2 \rightarrow c[](\psi_i \rightarrow c_i)$ **fi** =
if $(\psi_1 \vee \psi_2) \rightarrow c\ []\ ([]i \bullet \psi_i \rightarrow c_i)$ **fi**

Proof

$[\![\Gamma \rhd \textbf{if}\ \psi_1 \rightarrow c[]\psi_2 \rightarrow c[]([]i \bullet \psi_i \rightarrow c_i)\ \textbf{fi} : \textbf{com}]\!]\eta\ \psi$
$= (\vee\ i \bullet \psi_i \vee \psi_1 \vee \psi_2) \wedge (\psi_1 \Rightarrow [\![\Gamma \rhd c : \textbf{com}]\!]\eta\ \psi)$
$\wedge\ (\psi_2 \Rightarrow [\![\Gamma \rhd c : \textbf{com}]\!]\eta\ \psi) \wedge (\wedge\ i \bullet \psi_i \Rightarrow [\![\Gamma \rhd c_i : \textbf{com}]\!]\eta\ \psi)$
[by the semantics of alternation]
$= (\vee \bullet\ \psi_i \vee \psi_1 \vee \psi_2) \wedge (\psi_1 \vee \psi_2 \Rightarrow [\![\Gamma \rhd c : \textbf{com}]\!]\eta\ \psi) \wedge$
$\wedge\ (\wedge\ i \bullet \psi_i \Rightarrow [\![\Gamma \rhd c_i : \textbf{com}]\!]\eta\ \psi)$
[by predicate calculus]
$= [\![\Gamma \rhd \textbf{if}\ (\psi_1 \vee \psi_2) \rightarrow c\ []\ ([]i \bullet \psi_i \rightarrow c_i) : \textbf{com}]\!]\eta\ \psi$
[by the semantics of alternation]

Law 3.2.6 < **if** elim> If i ranges over $1..n$ and $\neg\ (\psi \wedge \psi_i)$, for all i, then
if $\psi \rightarrow$ (**if** $\psi \rightarrow c\ []\ ([]i \bullet \psi_i \rightarrow c_i)$ **fi**)[] $([]j \bullet \psi_j \rightarrow c_j)$ **fi** =
if $\psi \rightarrow c\ []\ ([]j \bullet \psi_j \rightarrow c_j)$ **fi**

Proof

$[\![\Gamma \rhd \textbf{if}\ \psi \rightarrow (\textbf{if}\ \psi \rightarrow c\ []\ (\psi_i \rightarrow c_i)\ \textbf{fi})[]\ \psi_j \rightarrow c_j\ \textbf{fi} : \textbf{com}]\!]\eta\ \psi$
$= (\vee\ j \bullet \psi_j \vee \psi) \wedge (\psi \Rightarrow (\textbf{if}\ \psi \rightarrow c([]i \bullet \psi_i \rightarrow c_i)) \wedge (\psi_j \Rightarrow [\![\Gamma \rhd c_j : \textbf{com}]\!]\eta\ \psi)$
[by the semantics of alternation]
$= (\vee\ j \bullet \psi_j \vee \psi) \wedge (\psi \Rightarrow (([]i \bullet \psi_i \vee \psi) \wedge (\psi \Rightarrow [\![\Gamma \rhd c : \textbf{com}]\!]\eta\ \psi) \wedge$
$([]i \bullet \psi_i \Rightarrow [\![\Gamma \rhd c_i : \textbf{com}]\!]\eta\ \psi))) \wedge ([]j \bullet \psi_j \Rightarrow [\![\Gamma \rhd c_j : \textbf{com}]\!]\eta\ \psi)$
[by the semantics of alternation]
$= (\vee\ j \bullet \psi_j \vee \psi) \wedge (\neg\ \psi \vee (([]i \bullet \psi_i \vee \psi) \wedge (\psi \Rightarrow [\![\Gamma \rhd c : \textbf{com}]\!]\eta\ \psi) \wedge$
$([]i \bullet \psi_i \Rightarrow [\![\Gamma \rhd c_i : \textbf{com}]\!]\eta\ \psi))) \wedge ([]j \bullet \psi_j \Rightarrow [\![\Gamma \rhd c_j : \textbf{com}]\!]\eta\ \psi)$
[by predicate calculus]
$= (\vee\ j \bullet \psi_j \vee \psi) \wedge (\neg\ \psi \vee (([]i \bullet \psi_i \vee \psi) \wedge$

$(\neg\,\psi \vee [\![\Gamma \rhd c : \mathbf{com}]\!]\eta\ \psi) \wedge (\psi_i \vee [\![\Gamma \rhd c_i : \mathbf{com}]\!]\eta\ \psi))) \wedge$
$([]j \bullet \psi_j \Rightarrow [\![\Gamma \rhd c_j : \mathbf{com}]\!]\eta\ \psi)$

[by predicate calculus]

$= (\vee\ j \bullet \psi_j \vee \psi) \wedge (([]i \bullet \psi_i \vee \psi \vee \neg\,\psi) \wedge (\neg\,\psi \vee [\![\Gamma \rhd c : \mathbf{com}]\!]\eta\ \psi)$
$\wedge ([]i \bullet \psi_i \neg\,\psi \vee \neg\,\psi \vee [\![\Gamma \rhd c_i : \mathbf{com}]\!]\eta\ \psi)) \wedge ([]j \bullet \psi_j \Rightarrow [\![\Gamma \rhd c_j : \mathbf{com}]\!]\eta\ \psi)$

[by predicate calculus]

$= (\vee\ j \bullet \psi_j \vee \psi) \wedge ((\neg\,\psi \vee [\![\Gamma \rhd c : \mathbf{com}]\!]\eta\ \psi)$
$\wedge ([]i \bullet \psi_i \neg\,\psi \vee \neg\,\psi \vee [\![\Gamma \rhd c_i : \mathbf{com}]\!]\eta\ \psi)) \wedge ([]j \bullet \psi_j \Rightarrow [\![\Gamma \rhd c_j : \mathbf{com}]\!]\eta\ \psi)$

[by predicate calculus]

$= (\vee\ j \bullet \psi_j \vee \psi) \wedge (\neg\,\psi \vee [\![\Gamma \rhd c : \mathbf{com}]\!]\eta\ \psi)$
$\wedge (\neg\,\psi \vee [\![\Gamma \rhd c : \mathbf{com}]\!]\eta\ \psi) \wedge ((([]i \bullet \psi_i \neg\,\psi \vee \neg\,\psi) \vee [\![\Gamma \rhd c_i : \mathbf{com}]\!]\eta\ \psi)$
$\wedge ([]j \bullet \psi_j \Rightarrow [\![\Gamma \rhd c_j : \mathbf{com}]\!]\eta\ \psi)$

[by predicate calculus]

$= (\vee\ j \bullet \psi_j \vee \psi) \wedge (\neg\,\psi \vee [\![\Gamma \rhd c : \mathbf{com}]\!]\eta\ \psi) \wedge (\neg\,\psi \vee [\![\Gamma \rhd c : \mathbf{com}]\!]\eta\ \psi)$
$\wedge (\mathbf{true} \vee [\![\Gamma \rhd c_i : \mathbf{com}]\!]\eta\ \psi) \wedge ([]j \bullet \psi_j \Rightarrow [\![\Gamma \rhd c_j : \mathbf{com}]\!]\eta\ \psi)$

[by the hypothesis]

$= (\vee\ j \bullet \psi_j \vee \psi) \wedge (\neg\,\psi \vee [\![\Gamma \rhd c : \mathbf{com}]\!]\eta\ \psi)$
$\wedge (\mathbf{false} \Rightarrow [\![\Gamma \rhd c_i : \mathbf{com}]\!]\eta\ \psi \wedge ([]j \bullet \psi_j \Rightarrow [\![\Gamma \rhd c_j : \mathbf{com}]\!]\eta\ \psi)$

[by predicate calculus]

$= (\vee\ j \bullet \psi_j \vee \psi) \wedge (\neg\,\psi \vee [\![\Gamma \rhd c : \mathbf{com}]\!]\eta\ \psi)$
$\wedge ([]j \bullet \psi_j \Rightarrow [\![\Gamma \rhd c_j : \mathbf{com}]\!]\eta\ \psi)$

[by predicate calculus]

$= (\vee\ j \bullet \psi_j \vee \psi) \wedge (\psi \Rightarrow [\![\Gamma \rhd c : \mathbf{com}]\!]\eta\ \psi)$
$\wedge ([]j \bullet \psi_j \Rightarrow [\![\Gamma \rhd c_j : \mathbf{com}]\!]\eta\ \psi)$

[by predicate calculus]

$= [\![\Gamma \rhd \mathbf{if}\ \psi\ \rightarrow\ c\ []\ ([]j \bullet \psi_j\ \rightarrow\ c_j)\ \mathbf{fi} : \mathbf{com}]\!]\eta\ \psi)$

[by the semantics of alternation]

Law 3.2.7 < **if**- $\vee$ distrib2>
$\mathbf{if}\ \psi_1\ \rightarrow\ c_1\ []\ \neg\,\psi_1\ \rightarrow\ (\mathbf{if}\ \psi_2\ \rightarrow\ c_1\ []\ \neg\,\psi_2\ \rightarrow\ c_2\ \mathbf{fi})\ \mathbf{fi} =$
$\mathbf{if}\ (\psi_1 \vee \psi_2)\ \rightarrow\ c_1[]\neg\,(\psi_1 \vee \psi_2)\ \rightarrow\ c_2\ \mathbf{fi}$

Proof

$[\![\Gamma \rhd \mathbf{if}\ \psi_1\ \rightarrow\ c_1\ []\ \neg\,\psi_1\ \rightarrow\ (\mathbf{if}\ \psi_2\ \rightarrow\ c_1\ []\ \neg\,\psi_2\ \rightarrow\ c_2\ \mathbf{fi})\ \mathbf{fi} : \mathbf{com}]\!]\eta\ \psi$
$= (\psi_1 \vee \neg\,\psi_1) \wedge (\psi_1 \Rightarrow [\![\Gamma \rhd c_1 : \mathbf{com}]\!]\eta\ \psi) \wedge$
$(\neg\,\psi_1 \Rightarrow [\![\Gamma \rhd \mathbf{if}\ \psi_2\ \rightarrow\ c_1\ []\ \neg\,\psi_2\ \rightarrow\ c_2\ \mathbf{fi} : \mathbf{com}]\!]\eta\ \psi)$

[by the semantics of alternation]

$= (\psi_1 \Rightarrow [\![\Gamma \rhd c_1 : \mathbf{com}]\!]\eta\ \psi) \wedge (\neg\, \psi_1 \Rightarrow ((\psi_2 \vee \neg\, \psi_2) \wedge$
$(\psi_2 \Rightarrow [\![\Gamma \rhd c_1 : \mathbf{com}]\!]\eta\ \psi) \wedge$
$(\neg\, \psi_2 \Rightarrow [\![\Gamma \rhd c_2 : \mathbf{com}]\!]\eta\ \psi)))$

[by the semantics of alternation and predicate calculus]

$= (\psi_1 \Rightarrow [\![\Gamma \rhd c_1 : \mathbf{com}]\!]\eta\ \psi) \wedge (\neg\, \psi_1 \Rightarrow ((\psi_2 \Rightarrow [\![\Gamma \rhd c_1 : \mathbf{com}]\!]\eta\ \psi) \wedge$
$(\neg\, \psi_2 \Rightarrow [\![\Gamma \rhd c_2 : \mathbf{com}]\!]\eta\ \psi)))$

[by predicate calculus]

$= (\neg\, \psi_1 \vee [\![\Gamma \rhd c_1 : \mathbf{com}]\!]\eta\ \psi) \wedge (\psi_1 \vee ((\neg\, \psi_2 \vee [\![\Gamma \rhd c_1 : \mathbf{com}]\!]\eta\ \psi) \wedge$
$(\psi_2 \vee [\![\Gamma \rhd c_2 : \mathbf{com}]\!]\eta\ \psi))$

[by predicate calculus]

$= (\neg\, \psi_1 \vee [\![\Gamma \rhd c_1 : \mathbf{com}]\!]\eta\ \psi) \wedge ((\psi_1 \vee \neg\, \psi_2 \vee [\![\Gamma \rhd c_1 : \mathbf{com}]\!]\eta\ \psi) \wedge$
$(\psi_1 \vee \psi_2 \vee [\![\Gamma \rhd c_2 : \mathbf{com}]\!]\eta\ \psi))$

[by predicate calculus]

$= ([\![\Gamma \rhd c_1 : \mathbf{com}]\!]\eta\ \psi(\neg\, \psi_1 \wedge (\psi_1 \vee \neg\, \psi_2))) \wedge (\psi_1 \vee \psi_2 \vee [\![\Gamma \rhd c_2 : \mathbf{com}]\!]\eta\ \psi)$

[by predicate calculus]

$= ([\![\Gamma \rhd c_1 : \mathbf{com}]\!]\eta\ \psi \vee ((\neg\, \psi_1 \wedge \psi_1) \vee (\neg\, \psi_1 \wedge \neg\, \psi_2)) \wedge (\psi_1 \vee \psi_2 \vee [\![\Gamma \rhd c_2 : \mathbf{com}]\!]\eta\ \psi)$

[by predicate calculus]

$= ([\![\Gamma \rhd c_1 : \mathbf{com}]\!]\eta\ \psi \vee (\neg\, (\psi_1 \vee \psi_2)) \wedge (\psi_1 \vee \psi_2 \vee [\![\Gamma \rhd c_2 : \mathbf{com}]\!]\eta\ \psi)$

[by predicate calculus]

$= ((\psi_1 \vee \psi_2) \Rightarrow [\![\Gamma \rhd c_1 : \mathbf{com}]\!]\eta\ \psi) \wedge (\neg\, (\psi_1 \vee \psi_2) \Rightarrow [\![\Gamma \rhd c_2 : \mathbf{com}]\!]\eta\ \psi)$

[by predicate calculus]

$= [\![\Gamma \rhd \mathbf{if}\ (\psi_1 \vee \psi_2) \ \rightarrow\ c_1 [\!]\neg\, (\psi_1 \vee \psi_2) \ \rightarrow\ c_2\ \mathbf{fi} : \mathbf{com}]\!]\eta\ \psi$

[by the semantics of alternation]

Law 3.2.8 $<$ **if**- $\vee$ distrib$>$
$\mathbf{if}\ \psi_1 \ \rightarrow\ (\mathbf{if}\ \psi_2 \ \rightarrow\ c_1\ [\!]\ \neg\, \psi_2 \ \rightarrow\ c_2\ \mathbf{fi})\ [\!]\ \neg\, \psi_1 \ \rightarrow\ c_2\ \mathbf{fi} =$
$\mathbf{if}\ (\psi_1 \wedge \psi_2) \ \rightarrow\ c_1\ [\!]\ \neg\, (\psi_1 \wedge \psi_2) \ \rightarrow\ c_2\ \mathbf{fi}$

Proof

$[\![\Gamma \rhd \mathbf{if}\ \psi_1 \ \rightarrow\ (\mathbf{if}\ \psi_2 \ \rightarrow\ c_1\ [\!]\ \neg\, \psi_2 \ \rightarrow\ c_2\ \mathbf{fi})\ [\!]\ \neg\, \psi_1 \ \rightarrow\ c_2\ \mathbf{fi} : \mathbf{com}]\!]\eta\ \psi$
$= (\psi_1 \vee \neg\, \psi_1) \wedge (\psi_1 \Rightarrow [\![\Gamma \rhd \mathbf{if}\ \psi_2 \ \rightarrow\ c_1\ [\!]\ \neg\, \psi_2 \ \rightarrow\ c_2\ \ : \mathbf{com}]\!]\eta\ \psi) \wedge$
$(\neg\, \psi_1 \Rightarrow [\![\Gamma \rhd c_2 : \mathbf{com}]\!]\eta\ \psi$ [by the semantics of alternation]
$= (\psi_1 \vee \neg\, \psi_1) \wedge (\psi_1 \Rightarrow ((\psi_2 \vee \neg\, \psi_2) \wedge$
$(\psi_2 \Rightarrow [\![\Gamma \rhd c_1 : \mathbf{com}]\!]\eta\ \psi) \wedge (\neg\, \psi_2 \Rightarrow [\![\Gamma \rhd c_2 : \mathbf{com}]\!]\eta\ \psi))) \wedge (\neg\, \psi_1 \Rightarrow [\![\Gamma \rhd c_2 : \mathbf{com}]\!]\eta\ \psi$

[by the semantics of alternation]

$= (\psi_1 \Rightarrow ((\psi_2 \Rightarrow [\![\Gamma \rhd c_1 : \mathbf{com}]\!]\eta\ \psi) \wedge (\neg\, \psi_2 \Rightarrow [\![\Gamma \rhd c_2 : \mathbf{com}]\!]\eta\ \psi))) \wedge$
$(\neg\, \psi_1 \Rightarrow [\![\Gamma \rhd c_2 : \mathbf{com}]\!]\eta\ \psi)$ [by predicate calculus]

$= (\neg\, \psi_1 \vee ((\neg\, \psi_2 \vee [\![\Gamma \rhd c_1 : \mathbf{com}]\!]\eta\ \psi) \wedge (\psi_2 \vee [\![\Gamma \rhd c_2 : \mathbf{com}]\!]\eta\ \psi))) \wedge$
$(\psi_1 \vee [\![\Gamma \rhd c_2 : \mathbf{com}]\!]\eta\ \psi)$ [by predicate calculus]
$= (\neg\, \psi_1 \vee \neg\, \psi_2 \vee [\![\Gamma \rhd c_1 : \mathbf{com}]\!]\eta\ \psi) \wedge (\neg\, \psi_1 \vee \psi_2 \vee [\![\Gamma \rhd c_2 : \mathbf{com}]\!]\eta\ \psi))) \wedge$
$(\psi_1 \vee [\![\Gamma \rhd c_2 : \mathbf{com}]\!]\eta\ \psi)$ [by predicate calculus]
$= (\neg\, (\psi_1 \wedge \psi_2) \vee [\![\Gamma \rhd c_1 : \mathbf{com}]\!]\eta\ \psi) \wedge (\neg\, \psi_1 \vee \psi_2 \vee [\![\Gamma \rhd c_2 : \mathbf{com}]\!]\eta\ \psi))) \wedge$
$(\psi_1 \vee [\![\Gamma \rhd c_2 : \mathbf{com}]\!]\eta\ \psi)$ [by predicate calculus]
$= (\neg\, (\psi_1 \wedge \psi_2) \vee [\![\Gamma \rhd c_1 : \mathbf{com}]\!]\eta\ \psi) \wedge$
$((\neg\, \psi_1 \wedge \psi_1) \vee (\psi_1 \wedge \psi_2) \vee [\![\Gamma \rhd c_2 : \mathbf{com}]\!]\eta\ \psi)$ [by predicate calculus]
$= (\neg\, (\psi_1 \wedge \psi_2) \vee [\![\Gamma \rhd c_1 : \mathbf{com}]\!]\eta\ \psi) \wedge ((\psi_1 \wedge \psi_2) \vee [\![\Gamma \rhd c_1 : \mathbf{com}]\!]\eta\ \psi)$
[by predicate calculus]
$= ((\psi_1 \wedge \psi_2) \Rightarrow [\![\Gamma \rhd c_1 : \mathbf{com}]\!]\eta\ \psi) \wedge (\neg\, (\psi_1 \wedge \psi_2) \Rightarrow [\![\Gamma \rhd c_2 : \mathbf{com}]\!]\eta\ \psi)$
[by predicate calculus]
$= ((\psi_1 \wedge \psi_2) \vee \neg\, (\psi_1 \wedge \psi_2)) \wedge$
$((\psi_1 \wedge \psi_2) \Rightarrow [\![\Gamma \rhd c_1 : \mathbf{com}]\!]\eta\ \psi) \wedge (\neg\, (\psi_1 \wedge \psi_2) \Rightarrow [\![\Gamma \rhd c_2 : \mathbf{com}]\!]\eta\ \psi)$
[by predicate calculus]
$= [\![\Gamma \rhd \mathbf{if}\ (\psi_1 \wedge \psi_2)\ \rightarrow\ c_1\ [\,]\ \neg\, (\psi_1 \wedge \psi_2)\ \rightarrow\ c_2\ \mathbf{fi} : \mathbf{com}]\!]\eta\ \psi$
[by the semantics of alternation]

Law 3.2.9 If i ranges over $1..n$ and $\neg\, (\psi \wedge \psi_i)$, for all i, then
$\mathbf{if}\ [\,]i \bullet \psi_i\ \rightarrow\ c_i\ \mathbf{fi} \sqsubseteq \mathbf{if}\ ([\,]i \bullet \psi_i\ \rightarrow\ c_i)\ [\,]\ \psi\ \rightarrow\ c\ \mathbf{fi}$

Proof

$[\![\Gamma \rhd \mathbf{if}\ [\,]i \bullet \psi_i\ \rightarrow\ c_i\ \mathbf{fi} : \mathbf{com}]\!]\eta\ \psi$
$= (\vee\ i \bullet \psi_i) \wedge (\wedge\ i \bullet \psi_i \Rightarrow [\![\Gamma \rhd c_i : \mathbf{com}]\!]\eta\ \psi)$ [by the semantics of alternation]
$\Rightarrow (\vee\ i \bullet \psi_i \vee \psi) \wedge (\wedge\ i \bullet \psi_i \Rightarrow [\![\Gamma \rhd c_i : \mathbf{com}]\!]\eta\ \psi) \wedge (\psi \Rightarrow [\![\Gamma \rhd c : \mathbf{com}]\!]\eta\ \psi))$
[by the hypothesis]
$= [\![\Gamma \rhd \mathbf{if}\ ([\,]i \bullet \psi_i\ \rightarrow\ c_i)\ [\,]\ \psi\ \rightarrow\ c\ \mathbf{fi} : \mathbf{com}]\!]\eta\ \psi$
[by the semantics of alternation]

Law 3.2.10 If i ranges over $1..n$ and $\psi \Rightarrow \vee\ i \bullet \psi_i$, then
$\mathbf{if}\ \psi\ \rightarrow\ c\ [\,]\ ([\,]i \bullet \psi_i\ \rightarrow\ c_i)\ \mathbf{fi} \sqsubseteq \mathbf{if}\ ([\,]i \bullet \psi_i\ \rightarrow\ c_i)\ \mathbf{fi}$

Proof

$[\![\Gamma \rhd \mathbf{if}\ \psi\ \rightarrow\ c\ [\,]\ ([\,]i \bullet \psi_i\ \rightarrow\ c_i)\ \mathbf{fi} : \mathbf{com}]\!]\eta\ \psi$
$= (\psi \Rightarrow [\![\Gamma \rhd c : \mathbf{com}]\!]\eta\ \psi) \wedge ((\vee\ i \bullet \psi_i) \wedge$
$(\wedge\ i \bullet \psi_i \Rightarrow [\![\Gamma \rhd c_i : \mathbf{com}]\!]\eta\ \psi))$ [by the semantics of alternation]
$\Rightarrow (\vee\ i \bullet \psi_i) \wedge (\wedge\ i \bullet \psi_i \Rightarrow [\![\Gamma \rhd c_i : \mathbf{com}]\!]\eta\ \psi)$ [by the hypothesis]
$= [\![\Gamma \rhd \mathbf{if}\ ([\,]i \bullet \psi_i\ \rightarrow\ c_i)\ \mathbf{fi} : \mathbf{com}]\!]\eta\ \psi$ [by the semantics of alternation]

Law 3.2.11 < **if** true guard ref>
if true $\rightarrow$ c [] ([]$i \bullet \psi_i \rightarrow c_i$) **fi** $\sqsubseteq c$

Proof

$[\![\Gamma \rhd \textbf{if true} \rightarrow c \; [] \; ([] i \bullet \psi_i \rightarrow c_i) \; \textbf{fi} : \textbf{com}]\!] \eta \; \psi$
$= (\vee \; i \bullet \psi_i \vee \textbf{true}) \wedge (\textbf{true} \Rightarrow [\![\Gamma \rhd c : \textbf{com}]\!] \eta \; \psi) \wedge$
$(\wedge \; i \bullet \psi_i \Rightarrow [\![\Gamma \rhd c_i : \textbf{com}]\!] \eta \; \psi)$ [by the semantics of alternation]
$= [\![\Gamma \rhd c : \textbf{com}]\!] \eta \; \psi \wedge (\wedge \; i \bullet \psi_i \Rightarrow [\![\Gamma \rhd c_i : \textbf{com}]\!] \eta \; \psi)$
[by predicate calculus]
$\Rightarrow [\![\Gamma \rhd c : \textbf{com}]\!] \eta \; \psi$ [by predicate calculus]

3.3 Recursion

Law 3.3.1 <**rec** fixed point> **rec** X $\bullet$ F(X) = F(**rec** $\bullet$ F(X))

Proof

$[\![\Gamma \rhd \textbf{rec} X \bullet F(X) : \textbf{com}]\!] \eta \; \psi$
$= [\![\Gamma \rhd \mu_X \bullet F(X) : \textbf{com}]\!] \eta \; \psi$ [by the semantics of recursion]
$= [\![\Gamma \rhd F(\mu_X \bullet F(X)) : \textbf{com}]\!] \eta \; \psi$ [by unfolding least fixpoint]
$= [\![\Gamma \rhd F(\textbf{rec} X \bullet F(X)) : \textbf{com}]\!] \eta \; \psi$ [by the semantics of recursion]

Law 3.3.2 <**rec** least fixed point> F(X) $\sqsubseteq$ Y $\Rightarrow$ **rec** X $\bullet$ F(X) $\sqsubseteq$ Y

3.4 Sequential Composition

Law 3.4.1 <;- **skip** unit> (**skip**; c) = c = (c; **skip**)

Proof

$[\![\Gamma \rhd \textbf{skip}; \; c : \textbf{com}]\!] \eta \; \psi$
$= [\![\Gamma \rhd \textbf{skip} : \; \textbf{com}]\!] \eta \; ([\![\Gamma \rhd c : \textbf{com}]\!] \eta \; \psi)$
[by the semantics of sequential composition]
$= [\![\Gamma \rhd \; : [\textbf{true}, \textbf{true}] : \; \textbf{com}]\!] \eta \; ([\![\Gamma \rhd c : \textbf{com}]\!] \eta \; \psi)$
[by the definition of **skip**]
$= [\![\Gamma \rhd c : \textbf{com}]\!] \eta \; \psi$
[by the semantics of spec. statement and predicate calculus]
$= [\![\Gamma \rhd c : \textbf{com}]\!] \eta \; (\textbf{true} \wedge \textbf{true} \Rightarrow \psi)$ [by predicate calculus]

$= [\![\Gamma \rhd c : \mathbf{com}]\!]\eta\ ([\![\Gamma \rhd\ : [\mathbf{true}, \mathbf{true}] :\ \mathbf{com}]\!]\eta\ \psi)$

[by the semantics of specification statement]

$= [\![\Gamma \rhd c : \mathbf{com}]\!]\eta\ ([\![\Gamma \rhd \mathbf{skip} :\ \mathbf{com}]\!]\eta\ \psi)$

[by the definition of **skip**]

$= [\![\Gamma \rhd c;\ \mathbf{skip} : \mathbf{com}]\!]\eta\ \psi$

[by the semantics of sequential composition]

Law 3.4.2 <; -**abort** left zero> **abort**; $c =$ **abort**

Proof

$[\![\Gamma \rhd \mathbf{abort};\ c : \mathbf{com}]\!]\eta\ \psi$

$= [\![\Gamma \rhd \mathbf{abort} : \mathbf{com}]\!]\eta\ ([\![\Gamma \rhd c : \mathbf{com}]\!]\eta\ \psi)$

[by the semantics of sequential composition]

$= [\![\Gamma \rhd x : [\mathbf{false}, \mathbf{true}] : \mathbf{com}]\!]\eta\ ([\![\Gamma \rhd c : \mathbf{com}]\!]\eta\ \psi)$

[by the definition of **abort**]

$= \mathbf{false} \wedge \mathbf{true} \Rightarrow ([\![\Gamma \rhd c : \mathbf{com}]\!]\eta\ \psi)$

[by the semantics of specification statement]

$= \mathbf{false}$ [by predicate calculus]

$= \forall\, x : T \bullet \mathbf{false} \wedge \mathbf{true} \Rightarrow \psi$ [by predicate calculus]

$= [\![\Gamma \rhd x : [\mathbf{false}, \mathbf{true}] : \mathbf{com}]\!]\eta\ \psi$

[by the semantics of specification statement]

$= [\![\Gamma \rhd \mathbf{abort} : \mathbf{com}]\!]\eta\ \psi$ [by the definition of **abort**]

Law 3.4.3 <; -**miracle** left zero> **miracle**; $c =$ **miracle**

Proof

$[\![\Gamma \rhd \mathbf{miracle};\ c : \mathbf{com}]\!]\eta\ \psi$

$= [\![\Gamma \rhd \mathbf{miracle} : \mathbf{com}]\!]\eta\ ([\![\Gamma \rhd c : \mathbf{com}]\!]\eta\ \psi)$

[by the semantics of sequential composition]

$= [\![\Gamma \rhd x : [\mathbf{true}, \mathbf{false}] : \mathbf{com}]\!]\eta\ ([\![\Gamma \rhd c : \mathbf{com}]\!]\eta\ \psi)$

[by the definition of **miracle**]

$= \mathbf{true} \wedge \mathbf{false} \Rightarrow (\forall\, x : T \bullet [\![\Gamma \rhd c : \mathbf{com}]\!]\eta\ \psi)$

[by the semantics of specification statement]

$= \mathbf{true}$ [by predicate calculus]

$= \forall\, x : T \bullet \mathbf{true} \wedge \mathbf{false} \Rightarrow \psi$ [by predicate calculus]

$= [\![\Gamma \rhd x : [\mathbf{true}, \mathbf{false}] : \mathbf{com}]\!]\eta\ \psi$

[by the semantics of specification statement]

$= [\![\Gamma \rhd \mathbf{miracle} : \mathbf{com}]\!] \eta\ \psi$

[by the definition of **miracle**]

Law 3.4.4 <; assoc> $(c_1;\ c_2);\ c_3 = c_1;\ (c_2;\ c_3)$

Proof

$[\![\Gamma \rhd (c_1;\ c_2);\ c_3 : \mathbf{com}]\!] \eta\ \psi$

$= [\![\Gamma \rhd c_1;\ c_2 : \mathbf{com}]\!] \eta\ ([\![\Gamma \rhd c_3 : \mathbf{com}]\!] \eta\ \psi)$

[by the semantics of sequential composition]

$= ([\![\Gamma \rhd c_1 : \mathbf{com}]\!] \eta\ ([\![\Gamma \rhd c_2 : \mathbf{com}]\!] \eta))\ ([\![\Gamma \rhd c_3 : \mathbf{com}]\!] \eta\ \psi)$

[by the semantics of sequential composition]

$= [\![\Gamma \rhd c_1 : \mathbf{com}]\!] \eta\ ([\![\Gamma \rhd c_2 : \mathbf{com}]\!] \eta([\![\Gamma \rhd c_3 : \mathbf{com}]\!] \eta\ \psi))$

[by associativity]

$= [\![\Gamma \rhd c_1 : \mathbf{com}]\!] \eta\ ([\![\Gamma \rhd c_2;\ c_3 : \mathbf{com}]\!] \eta\ \psi)$

[by the semantics of sequential composition]

$= [\![\Gamma \rhd c_1;\ (c_2;\ c_3) : \mathbf{com}]\!] \eta\ \psi$

[by the semantics of sequential composition]

Law 3.4.5 < -**if** left dist> If i ranges over $1..n$
$\mathbf{if}\ []i \bullet \psi_i \rightarrow c_i\ \mathbf{fi};\ c = \mathbf{if}\ []i \bullet \psi_i \rightarrow (c_i;\ c)\ \mathbf{fi}$

Proof

$[\![\Gamma \rhd \mathbf{if}\ []i \bullet \psi_i \rightarrow c_i\ \mathbf{fi};\ c : \mathbf{com}]\!] \eta\ \psi$

$= [\![\Gamma \rhd \mathbf{if}\ []i \bullet \psi_i \rightarrow c_i\ \mathbf{fi} : \mathbf{com}]\!] \eta\ ([\![\Gamma \rhd c : \mathbf{com}]\!] \eta\ \psi)$

[by the semantics of sequential composition]

$= (\vee\ i \bullet \psi_i) \wedge (\wedge\ i \bullet \psi_i \Rightarrow [\![\Gamma \rhd c_i : \mathbf{com}]\!] \eta\ ([\![\Gamma \rhd c : \mathbf{com}]\!] \eta\ \psi))$

[by the semantics of alternation]

$= (\vee\ i \bullet \psi_i) \wedge (\wedge\ i \bullet \psi_i \Rightarrow [\![\Gamma \rhd c_i;\ c : \mathbf{com}]\!] \eta\ \psi)$

[by the semantics of sequential compostion]

$= [\![\Gamma \rhd \mathbf{if}\ []i \bullet \psi_i \rightarrow c_i;\ c\ \mathbf{fi} : \mathbf{com}]\!] \eta\ \psi$

[by the semantics of alternation]

Law 3.4.6 <; -**if** selection> If i and j range over $1..n$ and $\neg\ (\psi_j \wedge \psi_i)$, then for $j \neq i$ we have $[\psi_j]\ \mathbf{if}\ []i \bullet \psi_i \rightarrow c_i\ \mathbf{fi} = [\psi_j];\ c_j$

Proof

$$
\begin{aligned}
&[\![\Gamma \rhd [\psi_j];\ \textbf{if}\ []i \bullet \psi_i \ \rightarrow\ c_i\ \textbf{fi} : \textbf{com}]\!]\eta\ \psi \\
&= [\![\Gamma \rhd [\psi_j] : \textbf{com}]\!]\eta\ ([\![\Gamma \rhd \textbf{if}\ []i \bullet \psi_i \ \rightarrow\ c_i\ \textbf{fi} : \textbf{com}]\!]\eta\ \psi) \\
&\hfill \text{[by the semantics of sequential composition]} \\
&= [\![\Gamma \rhd\ : [\textbf{true}, \psi_j] : \textbf{com}]\!]\eta\ ([\![\Gamma \rhd \textbf{if}\ []i \bullet \psi_i \ \rightarrow\ c_i\ \textbf{fi} : \textbf{com}]\!]\eta\ \psi) \\
&\hfill \text{[definition of coercion]} \\
&= [\![\Gamma \rhd\ : [\textbf{true}, \psi_j] : \textbf{com}]\!]\eta\ ((\vee\ i \bullet \psi_i) \wedge \psi_i \Rightarrow [\![\Gamma \rhd c_i : \textbf{com}]\!]\eta\ \psi) \\
&\hfill \text{[by the semantics of alternation]} \\
&= \psi_j \Rightarrow (\vee\ i \bullet \psi_i) \wedge \psi_i \Rightarrow [\![\Gamma \rhd c_i : \textbf{com}]\!]\eta\ \psi \\
&\hfill \text{[by the semantics of specification statement]} \\
&= \psi_j \Rightarrow \psi_i \Rightarrow [\![\Gamma \rhd c_i : \textbf{com}]\!]\eta\ \psi \\
&\hfill \text{[by predicate calculus]} \\
&= (\psi_j \wedge \psi_i) \Rightarrow [\![\Gamma \rhd c_i : \textbf{com}]\!]\eta\ \psi \\
&\hfill \text{[by predicate calculus]} \\
&= \psi_j \Rightarrow [\![\Gamma \rhd c_j : \textbf{com}]\!]\eta\ \psi \\
&\hfill \text{[by the hypothesis]} \\
&= [\![\Gamma \rhd\ : [\textbf{true}, \psi_j] : \textbf{com}]\!]\eta\ ([\![\Gamma \rhd c_j : \textbf{com}]\!]\eta\ \psi) \\
&\hfill \text{[by the semantics of specification statement]} \\
&= [\![\Gamma \rhd [\psi_j] : \textbf{com}]\!]\eta\ ([\![\Gamma \rhd c_j : \textbf{com}]\!]\eta\ \psi) \\
&\hfill \text{[definition of coercion]} \\
&= [\![\Gamma \rhd [\psi_j];\ c_j : \textbf{com}]\!]\eta\ \psi \\
&\hfill \text{[by the semantics of sequential composition}
\end{aligned}
$$

Law 3.4.7 <; -:=combination> $(le := e_1;\ le := e_2) = (le := e_2[e_1/le])$

Proof

$$
\begin{aligned}
&[\![\Gamma \rhd (le := e_1;\ le := e_2) : \textbf{com}]\!]\eta\ \psi \\
&= [\![\Gamma \rhd le := e_1 : \textbf{com}]\!]\eta\ ([\![\Gamma \rhd le := e_2 : \textbf{com}]\!]\eta\ \psi \\
&\hfill \text{[by the semantics of sequential composition]} \\
&= [\![\Gamma \rhd le := e_1 : \textbf{com}]\!]\eta\ (e_2 \neq \textbf{error} \wedge \psi[e_2/le]) \\
&\hfill \text{[by the semantics of assignment]} \\
&= e_1 \neq \textbf{error} \wedge (e_2 \neq \textbf{error} \wedge \psi[e_2/le])[e_1/le] \\
&\hfill \text{[by the semantics of assignment]} \\
&= e_1 \neq \textbf{error} \wedge e_2 \neq \textbf{error} \wedge (\psi[e_2/le])[e_1/le] \\
&\hfill \text{[by predicate calculus]} \\
&= [\![\Gamma \rhd le := e_2[e_1/le] : \textbf{com}]\!]\eta\ \psi \qquad \text{[by the semantics of assignment]}
\end{aligned}
$$

Law 3.4.8 < := - right dist> If e is total, then
$le := e;\ \mathbf{if}\ []i \bullet \psi_i \ \rightarrow\ c_i\ \mathbf{fi} = \mathbf{if}\ []i \bullet \psi_i[e/le] \ \rightarrow\ (le := e;\ c_i)\ \mathbf{fi}$

Proof

$$
\begin{aligned}
&[\![\mathit{\Gamma} \rhd le := e;\ \mathbf{if}\ []i \bullet \psi i \ \rightarrow\ c_i\ \mathbf{fi} : \mathbf{com}]\!]\eta\ \psi \\
&= [\![\mathit{\Gamma} \rhd le := e : \mathbf{com}]\!]\eta\ ([\![\mathit{\Gamma} \rhd \mathbf{if}\ []i \bullet \psi_i \ \rightarrow\ c_i\ \mathbf{fi} : \mathbf{com}]\!]\eta\ \psi \\
&\qquad\qquad\qquad\qquad\qquad\qquad \text{[by the semantics of sequential composition]} \\
&= [\![\mathit{\Gamma} \rhd le := e : \mathbf{com}]\!]\eta\ ((\vee\ i \bullet \psi_i) \wedge (\wedge\ i \bullet \psi_i \Rightarrow [\![\mathit{\Gamma} \rhd c_i : \mathbf{com}]\!]\eta\ \psi))) \\
&\qquad\qquad\qquad\qquad\qquad\qquad \text{[by the semantics of alternation} \\
&= e \neq \mathbf{error} \wedge ((\vee\ i \bullet \psi_i) \wedge (\wedge\ i \bullet \psi_i \Rightarrow [\![\mathit{\Gamma} \rhd c_i : \mathbf{com}]\!]\eta\ \psi))[e/le] \\
&\qquad\qquad\qquad\qquad\qquad\qquad \text{[by the semantics of assignment]} \\
&= e \neq \mathbf{error} \wedge (\vee\ i \bullet \psi_i)[e/le] \wedge (\wedge\ i \bullet \psi_i \Rightarrow [\![\mathit{\Gamma} \rhd c_i : \mathbf{com}]\!]\eta\ \psi)[e/le] \\
&\qquad\qquad\qquad\qquad\qquad\qquad [le \text{ not free in } \psi_i] \\
&= (\vee\ i \bullet \psi_i[e/le]) \wedge (\wedge\ i \bullet \psi_i[e/le] \Rightarrow [\![\mathit{\Gamma} \rhd le := e : \mathbf{com}]\!]\eta\ ([\![\mathit{\Gamma} \rhd c_i : \mathbf{com}]\!]\eta\ \psi) \\
&\qquad\qquad\qquad\qquad\qquad\qquad \text{[by the semantics of assignment]} \\
&= (\vee\ i \bullet \psi_i[e/le]) \wedge (\wedge\ i \bullet \psi_i[e/le] \Rightarrow [\![\mathit{\Gamma} \rhd (le := e;\ c_i) : \mathbf{com}]\!]\eta\ \psi) \\
&\qquad\qquad\qquad\qquad\qquad\qquad \text{[by the semantics of sequential composition]} \\
&= [\![\mathit{\Gamma} \rhd \mathbf{if}\ []i \bullet \psi_i[e/le] \ \rightarrow\ (le := e;\ c_i)\ \mathbf{fi} : \mathbf{com}]\!]\eta\ \psi \\
&\qquad\qquad\qquad\qquad\qquad\qquad \text{[by the semantics of alternation]}
\end{aligned}
$$

3.5 Local Variable Block

Law 3.5.1 <**var** symmetry> $\mathbf{var}\ x_1 : T_1 \bullet (\mathbf{var}\ x_2 : T_2 \bullet c\ \mathbf{end})\ \mathbf{end} = \mathbf{var}\ x_2 : T_2 \bullet (\mathbf{var}\ x_1 : T_1 \bullet c\ \mathbf{end})\ \mathbf{end}$

Proof

$$
\begin{aligned}
&[\![\mathit{\Gamma} \rhd \mathbf{var}\ x_1 : T_1 \bullet (\mathbf{var}\ x_2 : T_2 \bullet c\ \mathbf{end})\ \mathbf{end} : \mathbf{com}]\!]\eta\ \psi \\
&= \forall\, x_1 : T_1 \bullet [\![\mathit{\Gamma};\ x_1 : T_1 \rhd \mathbf{var}\ x_2 : T_2 \bullet c\ \mathbf{end} : \mathbf{com}]\!]\eta\ \psi \\
&\qquad\qquad\qquad\qquad\qquad\qquad \text{[by the semantics of local blocks]} \\
&= \forall\, x_1 : T_1 \bullet \forall\, x_2 : T_2 \bullet [\![\mathit{\Gamma};\ x_1, x_2 : T_1, T_2 \rhd c : \mathbf{com}]\!]\eta\ \psi \\
&\qquad\qquad\qquad\qquad\qquad\qquad \text{[by the semantics of local blocks]} \\
&= \forall\, x_2 : T_2 \bullet \forall\, x_1 : T_1 \bullet [\![\mathit{\Gamma};\ x_1, x_2 : T_1, T_2 \rhd c : \mathbf{com}]\!]\eta\ \psi \\
&\qquad\qquad\qquad\qquad\qquad\qquad \text{[by predicate calculus]} \\
&= \forall\, x_2 : T_2 \bullet [\![\mathit{\Gamma};\ x_2 : T_2 \rhd\ \mathbf{var}\ x_1 : T_1 \bullet c\ \mathbf{end} : \mathbf{com}]\!]\eta\ \psi \\
&\qquad\qquad\qquad\qquad\qquad\qquad \text{[by the semantics of local blocks]} \\
&= [\![\mathit{\Gamma} \rhd \mathbf{var}\ x_2 : T_2 \bullet (\mathbf{var}\ x_1 : T_1 \bullet c\ \mathbf{end})\ \mathbf{end} : \mathbf{com}]\!]\eta\ \psi \\
&775 \qquad\qquad\qquad\qquad\qquad \text{[by the semantics of local blocks]}
\end{aligned}
$$

Law 3.5.2 <**var** elim> If x is not free in c, then **var** $x : T \bullet c$ **end** $= c$

Proof

$$
\begin{aligned}
& [\![\Gamma \rhd \mathbf{var}\ x : T \bullet c\ \mathbf{end} : \mathbf{com}]\!]\eta\ \psi \\
& = \forall\, x : T \bullet\ [\![\Gamma;\ x : T \rhd c : \mathbf{com}]\!]\eta\ \psi && \text{[by the semantics of local blocks]} \\
& = \forall\, x : T \bullet\ [\![\Gamma \rhd c : \mathbf{com}]\!]\eta\ \psi && \text{[by } x \text{ not free in } c\text{]} \\
& = [\![\Gamma \rhd c : \mathbf{com}]\!]\eta\ \psi && \text{[by } x \text{ not free in } c \text{ and } \psi \text{ and predicate calculus]}
\end{aligned}
$$

Law 3.5.3 <**var** rename> If x_2 is not free in c, then
var $x_1 : T \bullet c$ **end** $=$ **var** $x_2 : T \bullet c[x_2/x_1]$ **end**

Proof

$$
\begin{aligned}
& [\![\Gamma \rhd \mathbf{var}\ x_1 : T \bullet c\ \mathbf{end} : \mathbf{com}]\!]\eta\ \psi \\
& = \forall\, x_1 : T \bullet [\![\Gamma;\ x_1 : T \rhd c\ \mathbf{end} : \mathbf{com}]\!]\eta\ \psi \\
& \qquad \text{[by the semantics of local blocks]} \\
& = \forall\, x_2 : T \bullet ([\![\Gamma;\ x_1 : T \rhd c\ \mathbf{end} : \mathbf{com}]\!]\eta\ \psi)[x_2/x_1] \\
& \qquad \text{[by Lemma 3 and predicate calculus]} \\
& = \forall\, x_2 : T \bullet ([\![\Gamma;\ x_1 : T \rhd c\ \mathbf{end} : \mathbf{com}]\!]\eta)[x_2/x_1]\psi[x_2/x_1] && [x_2 \text{ not free in } c] \\
& = \forall\, x_2 : T \bullet [\![\Gamma;\ x_2 : T \rhd c[x_2/x_1]\psi && \text{[by Lemma 4]} \\
& = [\![\Gamma \rhd \mathbf{var}\ x_2 : T \bullet c[x_2/x_1]\ \mathbf{end} : \mathbf{com}]\!]\eta\ \psi \\
& \qquad \text{[by the semantics of local blocks]}
\end{aligned}
$$

Law 3.5.4 If i ranges over $1..n$ and x is not free in ψ_i, then
if $[]i \bullet \psi_i \rightarrow$ (**var** $x : T \bullet c_i$ **end**) **fi** $=$ **var** $x : T \bullet$ **if** $[]i \bullet \psi_i \rightarrow c_i$ **fi end**

Proof

$$
\begin{aligned}
& [\![\Gamma \rhd \mathbf{if}\ []i \bullet \psi_i \rightarrow (\mathbf{var}\ x : T \bullet c_i\ \mathbf{end})\ \mathbf{fi} : \mathbf{com}]\!]\eta\ \psi \\
& = (\vee\ i \bullet \psi_i) \wedge (\wedge\ i \bullet \psi_i \Rightarrow [\![\Gamma \rhd \mathbf{var}\ x : T \bullet c_i\ : \mathbf{com}]\!]\eta\ \psi) \\
& \qquad \text{[by the semantics of alternation]} \\
& = (\vee\ i \bullet \psi_i) \wedge (\wedge\ i \bullet \psi_i \Rightarrow \forall\, x : T \bullet [\![\Gamma;\ x : T \rhd c_i\ : \mathbf{com}]\!]\eta\ \psi) \\
& \qquad \text{[by the semantics of local blocks]} \\
& = \forall\, x : T \bullet (\wedge\ i \bullet \psi_i \Rightarrow [\![\Gamma;\ x : T \rhd c_i\ : \mathbf{com}]\!]\eta\ \psi) \\
& \qquad \text{[by predicate calculus]} \\
& = \forall\, x : T \bullet [\![\Gamma;\ x : T \rhd \mathbf{if}\ []i \bullet \psi_i \rightarrow c_i\ \mathbf{fi} : \mathbf{com}]\!]\eta\ \psi \\
& \qquad \text{[by the semantics of alternation]} \\
& = [\![\Gamma \rhd \mathbf{var}\ x : T \bullet \mathbf{if}\ []i \bullet \psi_i \rightarrow c_i\ \mathbf{fi}\ \mathbf{end} : \mathbf{com}]\!]\eta\ \psi \\
& \qquad \text{[by the semantics of local blocks]}
\end{aligned}
$$

Law 3.5.5 <**var**-; left dist> If x is not free in c_2, then
var $x : T \bullet c_1$ **end**; $c_2 =$ **var** $x : T \bullet c_1;\ c_2$ **end**

Proof

$$
\begin{aligned}
& [\![\Gamma \rhd \mathbf{var}\ x : T \bullet c_1\ \mathbf{end};\ c_2 : \mathbf{com}]\!]\eta\ \psi \\
& = [\![\Gamma \rhd \mathbf{var}\ x : T \bullet c_1\ \mathbf{end} : \mathbf{com}]\!]\eta\ ([\![\Gamma \rhd c_2 : \mathbf{com}]\!]\eta\ \psi) \\
& \qquad\qquad \text{[by the semantics of sequential composition]} \\
& = \forall\, x : T \bullet [\![\Gamma;\ x : T \rhd c_1\ : \mathbf{com}]\!]\eta\ ([\![\Gamma \rhd c_2 : \mathbf{com}]\!]\eta\ \psi) \\
& \qquad\qquad \text{[by the semantics of local blocks]} \\
& = \forall\, x : T \bullet [\![\Gamma;\ x : T \rhd c_1\ : \mathbf{com}]\!]\eta\ ([\![\Gamma;\ x : T \rhd c_2 : \mathbf{com}]\!]\eta\ \psi) \\
& \qquad\qquad [x \text{ not free in } c \text{ and } \psi] \\
& = \forall\, x : T \bullet [\![\Gamma;\ x : T \rhd c_1;\ c_2\ : \mathbf{com}]\!]\eta\ \psi \\
& \qquad\qquad \text{[by the semantics of sequential composition]} \\
& = [\![\Gamma \rhd \mathbf{var}\ x : T \bullet c_1;\ c_2\ \mathbf{end} : \mathbf{com}]\!]\eta\ \psi \\
& \qquad\qquad \text{[by the semantics of local blocks]}
\end{aligned}
$$

Law 3.5.6 <**var**-; right dist> If x is not free in c_1, then
c_1; **var** $x : T \bullet c_2$ **end** $=$ **var** $x : T \bullet c_1;\ c_2$ **end**

Proof

$$
\begin{aligned}
& [\![\Gamma \rhd c_1;\ \mathbf{var}\ x : T \bullet c_2\ \mathbf{end} : \mathbf{com}]\!]\eta\ \psi \\
& = [\![\Gamma \rhd c_1\ : \mathbf{com}]\!]\eta\ ([\![\Gamma \rhd \mathbf{var} x : T \bullet c_2\ \mathbf{end} : \mathbf{com}]\!]\eta\ \psi) \\
& \qquad\qquad \text{[by the semantics of sequential composition]} \\
& = [\![\Gamma \rhd c_1\ : \mathbf{com}]\!]\eta\ (\forall\, x : T \bullet [\![\Gamma;\ x : T \rhd c_2\ \mathbf{end} : \mathbf{com}]\!]\eta\ \psi) \\
& \qquad\qquad \text{[by the semantics of local blocks]} \\
& = \forall\, x : T \bullet [\![\Gamma \rhd c_1\ : \mathbf{com}]\!]\eta\ (\forall\, x : T \bullet [\![\Gamma;\ x : T \rhd c_2\ \mathbf{end} : \mathbf{com}]\!]\eta\ \psi) \\
& \qquad\qquad [x \text{ not free in } c_1] \\
& = \forall\, x : T \bullet [\![\Gamma \rhd c_1\ : \mathbf{com}]\!]\eta\ ([\![\Gamma;\ x : T \rhd c_2\ \mathbf{end} : \mathbf{com}]\!]\eta\ \psi) \\
& \qquad\qquad \text{[by predicate calculus]} \\
& = \forall\, x : T \bullet [\![\Gamma;\ x : T \rhd c_1;\ c_2\ : \mathbf{com}]\!]\eta\ \psi \\
& \qquad\qquad \text{[by the semantics of sequential composition]} \\
& = [\![\Gamma \rhd \mathbf{var}\ x : T \bullet c_1;\ c_2\ \mathbf{end} : \mathbf{com}]\!]\eta\ \psi \text{[by the semantics of local blocks]}
\end{aligned}
$$

Law 3.5.7 <**var**- := final value> If x is not free in c, then
var $x : T \bullet c;\ x := e$ **end** $=$ **var** $x : T \bullet c$ **end**

Proof

$$
\begin{aligned}
&[\![\Gamma \rhd \mathbf{var}\ x : T \bullet c;\ x := e\ \mathbf{end} : \mathbf{com}]\!]\eta\ \psi \\
&= \forall\, x : T \bullet [\![\Gamma;\ x : T \rhd c;\ x := e\ \ : \mathbf{com}]\!]\eta\ \psi \\
&\hspace{12em} \text{[by the semantics of local blocks]} \\
&= \forall\, x : T \bullet [\![\Gamma;\ x : T \rhd c\ \ : \mathbf{com}]\!]\eta\ ([\![\Gamma;\ x : T \rhd x := e\ \ : \mathbf{com}]\!]\eta\ \psi) \\
&\hspace{12em} \text{[by the semantics of sequential composition]} \\
&= \forall\, x : T \bullet [\![\Gamma;\ x : T \rhd c\ \ : \mathbf{com}]\!]\eta\ (e \neq \mathbf{error} \wedge \psi[e/x]) \\
&\hspace{12em} \text{[by the semantics of assignment]} \\
&= \forall\, x : T \bullet [\![\Gamma;\ x : T \rhd c\ \ : \mathbf{com}]\!]\eta\ \psi \qquad \text{[x not free in ψ]} \\
&= [\![\Gamma \rhd \mathbf{var}\ x : T \bullet c\ \mathbf{end} : \mathbf{com}]\!]\eta\ \psi \qquad \text{[by the semantics of local blocks]}
\end{aligned}
$$

Law 3.5.8 <**var**-; dist>
$\mathbf{var}\ x : T \bullet c_1\ \mathbf{end};\ \mathbf{var}\ x : T \bullet c_2\ \mathbf{end}\ \sqsubseteq\ \mathbf{var}\ x : Tc_1;\ c_2\ \mathbf{end}$

Proof

$$
\begin{aligned}
&[\![\Gamma \rhd \mathbf{var}\ x : T \bullet c_1\ \mathbf{end};\ \mathbf{var}\ x : T \bullet c_2\ \mathbf{end} : \mathbf{com}]\!]\eta\ \psi \\
&= [\![\Gamma \rhd \mathbf{var}\ x : T \bullet c_1\ \mathbf{end} : \mathbf{com}]\!]\eta\ ([\![\Gamma \rhd \mathbf{var}\ x : T \bullet c_2\ \mathbf{end} : \mathbf{com}]\!]\eta\ \psi) \\
&\hspace{12em} \text{[by the semantics of sequential composition]} \\
&= [\![\Gamma \rhd \mathbf{var}\ x : T \bullet c_1\ \mathbf{end} : \mathbf{com}]\!]\eta\ (\forall\, x : T \bullet [\![\Gamma;\ x : T \rhd c_2\ \ : \mathbf{com}]\!]\eta\ \psi) \\
&\hspace{12em} \text{[by the semantics of local blocks]} \\
&= \forall\, x : T \bullet ([\![\Gamma;\ x : T \rhd c_1\ \ : \mathbf{com}]\!]\eta\ (\forall\, x : T \bullet [\![\Gamma;\ x : T \rhd c_2\ \ : \mathbf{com}]\!]\eta\ \psi) \\
&\hspace{12em} \text{[by the semantics of local blocks]} \\
&\Rightarrow \forall\, x : T \bullet ([\![\Gamma;\ x : T \rhd c_1\ \ : \mathbf{com}]\!]\eta\ ([\![\Gamma;\ x : T \rhd c_2\ \ : \mathbf{com}]\!]\eta\ \psi) \\
&\hspace{12em} \text{[by predicate calculus and monotonicity]} \\
&= \forall\, x : T \bullet [\![\Gamma;\ x : T \rhd c_1;\ c_2\ \ : \mathbf{com}]\!]\eta\ \psi \\
&\hspace{12em} \text{[by the semantics of sequential composition]} \\
&= [\![\Gamma \rhd \mathbf{var}\ x : T \bullet c_1;\ c_2\ \mathbf{end} : \mathbf{com}]\!]\eta\ \psi \text{[by the semantics of local blocks]}
\end{aligned}
$$

Law 3.5.9 <**var**- := initial value>
$\mathbf{var}\ x : T \bullet c\ \mathbf{end}\ \sqsubseteq\ \mathbf{var}\ x : T \bullet x := e;\ c\ \mathbf{end}$

Proof

$$
\begin{aligned}
&[\![\Gamma \rhd \mathbf{var}\ x : T \bullet c\ \mathbf{end} : \mathbf{com}]\!]\eta\ \psi \\
&= \forall\, x : T \bullet [\![\Gamma;\ x : T \rhd c\ \ : \mathbf{com}]\!]\eta\ \psi \qquad \text{[by the semantics of local blocks]} \\
&= (\forall\, x : T \bullet [\![\Gamma;\ x : T \rhd c\ \ : \mathbf{com}]\!]\eta\ \psi)[e/x] \\
&\hspace{12em} \text{[by the hypothesis and x not free in c and ψ]}
\end{aligned}
$$

$= \forall x : T \bullet ([\![\Gamma;\ x : T \rhd c\ \ : \mathbf{com}]\!]\eta\ \psi)[e/x]$ $\quad$ [x not free in e]

$= \forall x : T \bullet e \neq \mathbf{error} \wedge ([\![\Gamma;\ x : T \rhd c\ \ : \mathbf{com}]\!]\eta\ \psi)[e/x]$

[x not free in c and ψ]

$= \forall x : T \bullet [\![\Gamma;\ x : T \rhd x := e\ \ : \mathbf{com}]\!]\eta\ ([\![\Gamma;\ x : T \rhd c\ \ : \mathbf{com}]\!]\eta\ \psi)$

[by the semantics of assignment]

$= \forall x : T \bullet [\![\Gamma;\ x : T \rhd x := e;\ c\ \ : \mathbf{com}]\!]\eta\ \psi$

[by the semantics of sequential composition]

$= [\![\Gamma \rhd \mathbf{var}\ x : T \bullet x := e;\ c\ \mathbf{end} : \mathbf{com}]\!]\eta\ \psi$

[by the semantics of local blocks]

3.6 Angelic Variable Block

Law 3.6.1 <**avar** symmetry> $\mathbf{avar}\ x_1 : T_1 \bullet (\mathbf{avar}\ x_2 : T_2 \bullet c\ \mathbf{end})\ \mathbf{end} = \mathbf{avar}\ x_2 : T_2 \bullet (\mathbf{avar}\ x_1 : T_1 \bullet c\ \mathbf{end})\ \mathbf{end}$

Proof

$[\![\Gamma \rhd \mathbf{avar}\ x_1 : T_1 \bullet (\mathbf{avar}\ x_2 : T_2 \bullet c\ \mathbf{end})\ \mathbf{end} : \mathbf{com}]\!]\eta\ \psi$

$= \exists\, x_1 : T_1 \bullet [\![\Gamma;\ x_1 : T_1 \rhd \mathbf{avar}\ x_2 : T_2 \bullet c\ \mathbf{end} : \mathbf{com}]\!]\eta\ \psi$

[by the semantics of angelic blocks]

$= \exists\, x_1 : T_1 \bullet (\exists\, x_2 : T_2 \bullet [\![\Gamma;\ x_1, x_2 : T_1, T_2 \rhd c : \mathbf{com}]\!]\eta\ \psi$

[by the semantics of angelic blocks]

$= \exists\, x_2 : T_2 \bullet (\exists\, x_1 : T_1 \bullet [\![\Gamma;\ x_1, x_2 : T_1, T_2 \rhd c : \mathbf{com}]\!]\eta\ \psi$

[by predicate calculus]

$= \exists\, x_2 : T_2 \bullet [\![\Gamma;\ x_2 : T_2 \rhd\ \mathbf{avar}\ x_1 : T_1 \bullet c\ \mathbf{end} : \mathbf{com}]\!]\eta\ \psi$

[by the semantics of angelic blocks]

$= [\![\Gamma \rhd \mathbf{avar}\ x_2 : T_2 \bullet (\mathbf{avar}\ x_1 : T_1 \bullet c\ \mathbf{end})\ \mathbf{end} : \mathbf{com}]\!]\eta\ \psi$

[by the semantics of angelic blocks]

Law 3.6.2 <**avar** elim> If x is not free in c, then $\mathbf{avar}\ x : T \bullet c\ \mathbf{end} = c$

Proof

$[\![\Gamma \rhd \mathbf{avar}\ x : T \bullet c\ \mathbf{end} : \mathbf{com}]\!]\eta\ \psi$

$= \exists\, x : T \bullet\ [\![\Gamma;\ x : T \rhd c : \mathbf{com}]\!]\eta\ \psi$ $\quad$ [by the semantics of angelic blocks]

$= \exists\, x : T \bullet\ [\![\Gamma \rhd c : \mathbf{com}]\!]\eta\ \psi$ $\quad$ [x not free in c]

$= [\![\Gamma \rhd c : \mathbf{com}]\!]\eta\ \psi$ $\quad$ [x not free in c and ψ]

Law 3.6.3 <**avar** rename> If x_2 is not free in c, then
$\mathbf{avar}\ x_1 : T \bullet c\ \mathbf{end} = \mathbf{avar}\ x_2 : T \bullet c[x_2/x_1]\ \mathbf{end}$

Proof

$[\![\Gamma \rhd \textbf{avar}\ x_1 : T \bullet c\ \textbf{end} : \textbf{com}]\!]\eta\ \psi$
$= \exists\, x_1 : T \bullet [\![\Gamma;\ x_1 : T \rhd c\ \textbf{end} : \textbf{com}]\!]\eta\ \psi$
[by the semantics of angelic blocks]
$= \exists\, x_2 : T \bullet ([\![\Gamma;\ x_1 : T \rhd c\ \textbf{end} : \textbf{com}]\!]\eta\ \psi)[x_2/x_1]$
[by Lemma 3 and predicate calculus]
$= \exists\, x_2 : T \bullet ([\![\Gamma;\ x_1 : T \rhd c\ \textbf{end} : \textbf{com}]\!]\eta)[x_2/x_1]\psi[x_2/x_1]$ [by x_2 not free in c]
$= \exists\, x_2 : T \bullet ([\![\Gamma;\ x_2 : T \rhd c\ \textbf{end} : \textbf{com}]\!]\eta)\psi$ [by Lemma 4]
$= [\![\Gamma \rhd \textbf{avar}\ x_2 : T \bullet c[x_2/x_1]\ \textbf{end} : \textbf{com}]\!]\eta\ \psi$

Law 3.6.4 If i ranges over $1..n$ and x is not free in ψ_i, then
$\textbf{if}\ []i \bullet \psi_i \rightarrow (\textbf{avar}\ x : T \bullet c_i\ \textbf{end})\ \textbf{fi} = \textbf{avar}\ x : T \bullet \textbf{if}\ []i \bullet \psi_i \rightarrow c_i\ \textbf{fi}\ \textbf{end}$

Proof

$[\![\Gamma \rhd \textbf{if}\ []i \bullet \psi_i \rightarrow (\textbf{avar}\ x : T \bullet c_i\ \textbf{end})\ \textbf{fi} : \textbf{com}]\!]\eta\ \psi$
$= (\vee\ i \bullet \psi_i) \wedge (\wedge\ i \bullet \psi_i \Rightarrow [\![\Gamma \rhd \textbf{avar}\ x : T \bullet c_i\ : \textbf{com}]\!]\eta\ \psi)$
[by the semantics of alternation]
$= (\vee\ i \bullet \psi_i) \wedge (\wedge\ i \bullet \psi_i \Rightarrow \exists\, x : T \bullet [\![\Gamma;\ x : T \rhd c_i\ : \textbf{com}]\!]\eta\ \psi)$
[by the semantics of angelic blocks]
$= \exists\, x : T \bullet (\wedge\ i \bullet \psi_i \Rightarrow [\![\Gamma;\ x : T \rhd c_i\ : \textbf{com}]\!]\eta\ \psi)$
[by predicate calculus]
$= \exists\, x : T \bullet [\![\Gamma;\ x : T \rhd \textbf{if}\ []i \bullet \psi_i \rightarrow c_i\ \textbf{fi} : \textbf{com}]\!]\eta\ \psi$
[by the semantics of alternation]
$= [\![\Gamma \rhd \textbf{avar}\ x : T \bullet \textbf{if}\ []i \bullet \psi_i \rightarrow c_i\ \textbf{fi}\ \textbf{end} : \textbf{com}]\!]\eta\ \psi$
[by the semantics of angelic blocks]

Law 3.6.5 <**avar**-; left dist> If x is not free in c_2, then
$\textbf{avar}\ x : T \bullet c_1\ \textbf{end};\ c_2 = \textbf{avar}\ x : T \bullet c_1;\ c_2\ \textbf{end}$

Proof

$[\![\Gamma \rhd \textbf{avar}\ x : T \bullet c_1\ \textbf{end};\ c_2 : \textbf{com}]\!]\eta\ \psi$
$= [\![\Gamma \rhd \textbf{avar}\ x : T \bullet c_1\ \textbf{end} : \textbf{com}]\!]\eta\ ([\![\Gamma \rhd c_2 : \textbf{com}]\!]\eta\ \psi)$
[by the semantics of sequential composition]
$= \exists\, x : T \bullet [\![\Gamma;\ x : T \rhd c_1\ : \textbf{com}]\!]\eta\ ([\![\Gamma \rhd c_2 : \textbf{com}]\!]\eta\ \psi)$
[by the semantics of angelic blocks]

$$= \exists\, x : T \bullet [\![\Gamma;\ x : T \rhd c_1\ : \mathbf{com}]\!] \eta\ ([\![\Gamma;\ x : T \rhd c_2 : \mathbf{com}]\!] \eta\ \psi)$$

[x not free in c and ψ]

$$= \exists\, x : T \bullet [\![\Gamma;\ x : T \rhd c_1;\ c_2\ : \mathbf{com}]\!] \eta\ \psi$$

[by the semantics of sequential composition]

$$= [\![\Gamma \rhd \mathbf{avar}\ x : T \bullet c_1;\ c_2\ \mathbf{end} : \mathbf{com}]\!] \eta\ \psi$$

[by the semantics of angelic blocks]

Law 3.6.6 <**avar**-; right dist> If x is not free in c_1, then
$c_1;\ \mathbf{avar}\ x : T \bullet c_2\ \mathbf{end} = \mathbf{avar}\ x : T \bullet c_1;\ c_2\ \mathbf{end}$

Proof

$$[\![\Gamma \rhd c_1;\ \mathbf{avar}\ x : T \bullet c_2\ \mathbf{end} : \mathbf{com}]\!] \eta\ \psi$$

$$= [\![\Gamma \rhd c_1\ : \mathbf{com}]\!] \eta\ ([\![\Gamma \rhd \mathbf{avar} x : T \bullet c_2\ \mathbf{end} : \mathbf{com}]\!] \eta\ \psi)$$

[by the semantics of sequential composition]

$$= [\![\Gamma \rhd c_1\ : \mathbf{com}]\!] \eta\ (\exists\, x : T \bullet [\![\Gamma;\ x : T \rhd c_2\ \mathbf{end} : \mathbf{com}]\!] \eta\ \psi)$$

[by the semantics of angelic blocks]

$$= \exists\, x : T \bullet [\![\Gamma \rhd c_1\ : \mathbf{com}]\!] \eta\ (\exists\, x : T \bullet [\![\Gamma;\ x : T \rhd c_2\ \mathbf{end} : \mathbf{com}]\!] \eta\ \psi)$$

[x not free in c_1]

$$= \exists\, x : T \bullet [\![\Gamma \rhd c_1\ : \mathbf{com}]\!] \eta\ ([\![\Gamma;\ x : T \rhd c_2\ \mathbf{end} : \mathbf{com}]\!] \eta\ \psi)$$

[by predicate calculus]

$$= \exists\, x : T \bullet [\![\Gamma;\ x : T \rhd c_1;\ c_2\ : \mathbf{com}]\!] \eta\ \psi$$

[by the semantics of sequential composition]

$$= [\![\Gamma \rhd \mathbf{avar}\ x : T \bullet c_1;\ c_2\ \mathbf{end} : \mathbf{com}]\!] \eta\ \psi$$

[by the semantics of angelic blocks]

Law 3.6.7 <**avar**- := final value> If x is not free in c, then
$\mathbf{avar}\ x : T \bullet c;\ x := e\ \mathbf{end}\ =\ \mathbf{avar}\ x : T \bullet c\ \mathbf{end}$

Proof

$$[\![\Gamma \rhd \mathbf{avar}\ x : T \bullet c;\ x := e\ \mathbf{end} : \mathbf{com}]\!] \eta\ \psi$$

$$= \exists\, x : T \bullet [\![\Gamma;\ x : T \rhd c;\ x := e\ : \mathbf{com}]\!] \eta\ \psi$$

[by the semantics of angelic blocks]

$$= \exists\, x : T \bullet [\![\Gamma;\ x : T \rhd c\ : \mathbf{com}]\!] \eta\ ([\![\Gamma;\ x : T \rhd x := e\ : \mathbf{com}]\!] \eta\ \psi)$$

[by the semantics of sequential composition]

$$= \exists\, x : T \bullet [\![\Gamma;\ x : T \rhd c\ : \mathbf{com}]\!] \eta\ (e \neq \mathbf{error} \wedge \psi[e/x])$$

[by the semantics of assignment]

$$= \exists\, x : T \bullet [\![\Gamma;\ x : T \rhd c\ : \mathbf{com}]\!] \eta\ \psi$$ [x not free in ψ]

$$= [\![\Gamma \rhd \mathbf{avar}\ x : T \bullet c\ \mathbf{end} : \mathbf{com}]\!] \eta\ \psi$$ [by the semantics of angelic blocks]

Law 3.6.8 <**avar** - **var** relationship> If x is not free in e, then
avar $x : T \bullet \{x = e\};\ c$ **end** $=$ **var** $x : T \bullet [x = e];\ c$ **end**

$$
\begin{aligned}
& [\![\Gamma \rhd (\textbf{avar}\ x : T \bullet \{x = e\};\ c\ \textbf{end}) : \textbf{com}]\!] \eta\ \psi \\
& = \exists\, x : T \bullet [\![\Gamma;\ x : T \rhd \{x = e\};\ c : \textbf{com}]\!] \eta\ \psi \\
& \hfill \text{[by the semantics of angelic blocks]} \\
& = \exists\, x : T \bullet [\![\Gamma;\ x : T \rhd \{x = e\} : \textbf{com}]\!] \eta\ ([\![\Gamma;\ x : T \rhd c : \textbf{com}]\!] \eta\ \psi) \\
& \hfill \text{[by the semantics of sequential composition]} \\
& = \exists\, x : T \bullet [\![\Gamma;\ x : T \rhd\ : [x = e, \textbf{true}] : \textbf{com}]\!] \eta\ ([\![\Gamma;\ x : T \rhd c : \textbf{com}]\!] \eta\ \psi) \\
& \hfill \text{[by the definition of assumption]} \\
& = \exists\, x : T \bullet x = e \wedge ([\![\Gamma;\ x : T \rhd c : \textbf{com}]\!] \eta\ \psi) \\
& \hfill \text{[by the semantics of specification statement]} \\
& = \forall\, x : T \bullet x = e \Rightarrow ([\![\Gamma;\ x : T \rhd c : \textbf{com}]\!] \eta\ \psi) \qquad \text{[by predicate calculus]} \\
& = \forall\, x : T \bullet [\![\Gamma;\ x : T \rhd\ : [\textbf{true}, x = e] : \textbf{com}]\!] \eta\ ([\![\Gamma;\ x : T \rhd c : \textbf{com}]\!] \eta\ \psi) \\
& \hfill \text{[by the semantics of specification statement]} \\
& = \forall\, x : T \bullet [\![\Gamma;\ x : T \rhd [x = e] : \textbf{com}]\!] \eta\ ([\![\Gamma;\ x : T \rhd c : \textbf{com}]\!] \eta\ \psi) \\
& \hfill \text{[by the definition of coercion]} \\
& = \forall\, x : T \bullet [\![\Gamma;\ x : T \rhd [x = e];\ c : \textbf{com}]\!] \eta\ \psi \\
& \hfill \text{[by the semantics of sequential composition]} \\
& = [\![\Gamma \rhd (\textbf{var}\ x : T \bullet [x = e];\ c\ \textbf{end}) : \textbf{com}]\!] \eta\ \psi \\
& \hfill \text{[by the semantics of angelic blocks]}
\end{aligned}
$$

Law 3.6.9 <**avar**-; dist>
avar $x : T \bullet c_1;\ c_2$ **end** $\sqsubseteq$ **avar** $x : T \bullet c_1$ **end**; **avar** $x : T \bullet c_2$ **end**

Proof

$$
\begin{aligned}
& [\![\Gamma \rhd \textbf{avar}\ x : T \bullet c_1;\ c_2\ \textbf{end} : \textbf{com}]\!] \eta\ \psi \\
& = \exists\, x : T \bullet [\![\Gamma;\ x : T \rhd c_1;\ c_2\ : \textbf{com}]\!] \eta\ \psi \\
& \hfill \text{[by the semantics of angelic blocks]} \\
& = \exists\, x : T \bullet [\![\Gamma;\ x : T \rhd c_1\ : \textbf{com}]\!] \eta\ ([\![\Gamma;\ x : T \rhd c_2\ : \textbf{com}]\!] \eta\ \psi) \\
& \hfill \text{[by the semantics of sequential composition]} \\
& \Rightarrow \exists\, x : T \bullet [\![\Gamma;\ x : T \rhd c_1\ : \textbf{com}]\!] \eta\ (\exists\, x : T \bullet [\![\Gamma;\ x : T \rhd c_2\ : \textbf{com}]\!] \eta\ \psi) \\
& \hfill \text{[by predicate calculus and monotonicity]} \\
& = \exists\, x : T \bullet [\![\Gamma;\ x : T \rhd c_1\ : \textbf{com}]\!] \eta\ ([\![\Gamma \rhd \textbf{avar}\ x : T \bullet c_2\ \textbf{end} : \textbf{com}]\!] \eta\ \psi) \\
& \hfill \text{[by the semantics of angelic blocks]} \\
& = [\![\Gamma \rhd \textbf{avar}\ x : T \bullet c_1\ \textbf{end} : \textbf{com}]\!] \eta\ ([\![\Gamma \rhd \textbf{avar}\ x : T \bullet c_2\ \textbf{end} : \textbf{com}]\!] \eta\ \psi) \\
& \hfill \text{[by the semantics of angelic blocks]}
\end{aligned}
$$

$$= [\![\Gamma \rhd \textbf{avar } x : T \bullet c_1 \textbf{ end}; \textbf{ avar } x : T \bullet c_2 \textbf{ end} : \textbf{com}]\!]\eta\ \psi$$
[by the semantics of sequential composition]

Law 3.6.10 <**avar**- := initial value>
avar $x : T \bullet x := e;\ c$ **end** $\sqsubseteq$ **avar** $x : T \bullet c$ **end**

Proof

$$[\![\Gamma \rhd (\textbf{avar } x : T \bullet x := e;\ c \textbf{ end}) : \textbf{com}]\!]\eta\ \psi$$
$$= \exists\, x : T \bullet [\![\Gamma;\ x : T \rhd x := e;\ c\ : \textbf{com}]\!]\eta\ \psi$$
[by the semantics of angelic blocks]
$$= \exists\, x : T \bullet [\![\Gamma;\ x : T \rhd x := e : \textbf{com}]\!]\eta([\![\Gamma;\ x : T \rhd c : \textbf{com}]\!]\eta\ \psi)$$
[by the semantics of sequential composition]
$$= \exists\, x : T \bullet e \neq \textbf{error} \wedge ([\![\Gamma;\ x : T \rhd c : \textbf{com}]\!]\eta\ \psi)[e/x]$$
[by the semantics of assignment]
$$= \exists\, x : T \bullet [\![\Gamma;\ x : T \rhd c : \textbf{com}]\!]\eta\ \psi[e/x]$$
$$\Rightarrow \exists\, x : T \bullet \exists\, x \bullet [\![\Gamma;\ x : T \rhd c : \textbf{com}]\!]\eta\ \psi$$ [by predicate calculus]
$$= [\![\Gamma \rhd (\textbf{avar } x : T \bullet c \textbf{ end}) : \textbf{com}]\!]\eta\ \psi$$
[by the semantics of angelic blocks]

Law 3.6.11 <**var** - *avar* refinement> **var** $x : T \bullet c$ **end** $\sqsubseteq$ **avar** $x : T \bullet c$ **end**

Proof

$$[\![\Gamma \rhd (\textbf{var } x : T \bullet c \textbf{ end}) : \textbf{com}]\!]\eta\ \psi$$
$$= \forall\, x : T \bullet [\![\Gamma;\ x : T \rhd c : \textbf{com}]\!]\eta\ \psi$$ [by the semantics of angelic blocks]
$$\Rightarrow \exists\, x : T \bullet [\![\Gamma;\ x : T \rhd c : \textbf{com}]\!]\eta\ \psi$$ [by predicate calculus]
$$= [\![\Gamma \rhd (\textbf{avar } x : T \bullet c \textbf{ end}) : \textbf{com}]\!]\eta\ \psi$$
[by the semantics of angelic blocks]

4 Conclusion

In this report we presented the proofs of the basic laws of ROOL [2]. Such laws were introduced in [6] and were proved in the weakest precondition semantics of ROOL [2, 1].

References

1. A. L. C. Cavalcanti and D. Naumann. A Weakes Precondition Semantics for an Object-oriented Language of Refinement - Extended Version. Technical Report CS 9903, Stevens Institute of Technology, September 1999.

2. A. L. C. Cavalcanti and D. Naumann. A weakest precondition semantics for an object-oriented language of refinement. In *FM'99 - Formal Methods*, volume 1709 of *Lecture Notes in Computer Science*, pages 1439–1459, 1999.
3. A. Sampaio. *An Algebraic Approach to Compiler Design*, volume 4. World Scientific, 1997.
4. C. C. Morgan. *Programming from Specifications.* Prentice Hall, secoond edition, 1994.
5. C.A.R. Hoare *et. al.* Laws of programming. *Communications of the ACM*, 30(8):672–686, August 1987.
6. P. Borba and A. Sampaio. The basic laws of ROOL. Technical report, Centro de Informática, Universidade Federal de Pernambuco, Brazil, 2000. To appear in `http://www.cin.ufpe.br/~lmf/coop/papers`.