The Definition of Red JonPRL, *the people's refinement logic*

The JonPRL Group

February 13, 2016

Contents

Chapter 1

Signatures

A *signature* is a collection of definitions, including terms, tactics and theorems.

1.1 Grammar

The grammar of `Red JonPRL` signatures is presented in Figure 1.1. Note that an optional production of sort s is formatted $\langle s \rangle$ in the rules.

sigexp	::=	$\langle \cdot \rangle$	empty signature
		sigexp sigdec.	signature extension
		sigexp symdec.	
sigdec	::=	`Def` *opid*$\langle[params]\rangle\langle(args)\rangle$: *sortid* = [*term*]	operator definition
		`Tac` *opid*$\langle[params]\rangle\langle(args)\rangle$ = [*term*]	tactic definition
		`Thm` *opid*$\langle[params]\rangle\langle(args)\rangle$: [*term*] `by` [*term*]	theorem declaration
symdec	::=	`Sym` *symbind*	symbol declaration
params	::=	$\langle \cdot \rangle$	empty parameter list
		params, *symbind*	parameter list extension
args	::=	$\langle \cdot \rangle$	empty argument list
		args, *metabind*	argument list extension
symbind	::=	*symid* : *sortid*	symbol binding
metabind	::=	*metaid* : *valence*	metavariable binding
valence	::=	$\langle\langle\{sortlist\}\rangle\langle[sortlist]\rangle.\rangle sortid$	valence
sortlist	::=	$\langle \cdot \rangle$	empty sort list
		sortlist, *sortid*	sort list extension

Figure 1.1: Grammar of signature expressions. The identifier sorts *opid*, *sortid*, *symid* and *metaid* can be assumed to be arbitrary strings; the sort *term* is left uninterpreted.

1.2 Static Semantics

The static semantics for `Red JonPRL` signatures begins with a specification of the class of *semantic* objects that will serve as the meanings for the *syntactic* objects defined in Section 1.1. We assume an ambient

abstract binding tree signature such that at least the following facts hold:

$$\overline{\texttt{tac } sort} \qquad \overline{\texttt{thm } sort} \qquad \overline{\texttt{exp } sort} \qquad \overline{\texttt{opid } sort}$$

$$\overline{\Upsilon \Vdash \texttt{prove} : (.\,\texttt{exp},.\,\texttt{tac})\,\texttt{thm}}$$

Then, our semantic objects are defined as in Figure 1.2.

$$
\begin{array}{rcll}
a, b & \in & \text{Sym} & \\
\mathfrak{m}, \mathfrak{n} & \in & \text{Metavar} & \\
\sigma, \tau & \in & \text{Sort} & \triangleq \; \{\, \tau \mid \tau \; sort \,\} \\
v & \in & \text{ProdValence} & \triangleq \; \{\, v \mid v \; valence \,\} \\
\vartheta & \in & \text{Opid} & \triangleq \; \text{Sym} \\
\Upsilon & \in & \text{Params} & \triangleq \; \text{Sym} \xrightarrow{\text{fin}} \text{Sort} \\
\Theta & \in & \text{Args} & \triangleq \; \text{Metavar} \xrightarrow{\text{fin}} \text{ProdValence} \\
M, N & \in & \text{Tm}(\Theta, \Upsilon, \tau) & \triangleq \; \{\, M \mid \Theta \triangleright \Upsilon \parallel \cdot \vdash M : \tau \,\} \\
D & \in & \text{Decl} & \triangleq \; \coprod_{\Upsilon, \Theta, \tau} \text{Tm}(\Theta, \Upsilon, \tau) \\
\Sigma & \in & \text{Sig} & \triangleq \; \left(\text{Opid} \xrightarrow{\text{fin}} \text{Decl} \right) \cap \left(\text{Sym} \xrightarrow{\text{fin}} \text{Sort} \right)
\end{array}
$$

Figure 1.2: Specification of the semantic objects.

A *natural semantics* hinges on the elaboration judgment $E \vdash A \Longrightarrow A'$, which means that the syntactic object A elaborates to the semantic object A' in the environment E. Let the $\Upsilon_\Sigma \in \text{Params}$ be defined as follows:

$$
\Upsilon_\Sigma(u) \triangleq \begin{cases} \texttt{opid} & if \quad u \equiv \vartheta \in \mathbf{dom}(\Sigma) \\ \tau & if \quad \Sigma(u) \equiv \tau \\ \bot & otherwise \end{cases}
$$

Symbol Bindings $\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \boxed{\Sigma \vdash symbind \Longrightarrow (a, \tau)}$

$$\frac{\Sigma \vdash symid \Longrightarrow a \quad \Sigma \vdash sortid \Longrightarrow \tau}{\Sigma \vdash symid : sortid \Longrightarrow (a, \tau)} \tag{1.1}$$

Metavariable Bindings $\qquad\qquad\qquad\qquad\qquad\qquad\qquad \boxed{\Sigma \vdash metabind \Longrightarrow (\mathfrak{m}, v)}$

$$\frac{\Sigma \vdash metaid \Longrightarrow \mathfrak{m} \quad \Sigma \vdash valence \Longrightarrow v}{\Sigma \vdash metaid : valence \Longrightarrow (\mathfrak{m}, v)} \tag{1.2}$$

Parameters $\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \boxed{\Sigma \vdash params \Longrightarrow \Upsilon}$

$$\frac{}{\Sigma \vdash \langle \cdot \rangle \Longrightarrow \{\}} \tag{1.3}$$

$$\frac{\Sigma \vdash params \Longrightarrow \Upsilon \quad \Sigma \vdash symbind \Longrightarrow (a, \tau)}{\Sigma \vdash params, symbind \Longrightarrow \Upsilon \cup a \mapsto \tau} \tag{1.4}$$

3

Arguments $\boxed{\Sigma \vdash \mathit{args} \Longrightarrow \Theta}$

$$\overline{\Sigma \vdash \langle \cdot \rangle \Longrightarrow \{\}} \tag{1.5}$$

$$\frac{\Sigma \vdash \mathit{args} \Longrightarrow \Theta \quad \Sigma \vdash \mathit{metabind} \Longrightarrow (\mathfrak{m}, v)}{\Sigma \vdash \mathit{args}, \mathit{metabind} \Longrightarrow \Theta \cup \mathfrak{m} \mapsto v} \tag{1.6}$$

Symbols $\boxed{\Sigma \vdash \mathit{symid} \Longrightarrow u}$

$$\frac{u \notin \mathbf{dom}(\Sigma)}{\Sigma \vdash \mathit{symid} \Longrightarrow u} \tag{1.7}$$

Operator Declarations $\boxed{\Sigma \vdash \mathit{sigdec} \Longrightarrow (\vartheta, D)}$

$$\frac{\begin{array}{ccc} \Sigma \vdash \mathit{params} \Longrightarrow \Upsilon & \Sigma \vdash \mathit{sortid} \Longrightarrow \tau & \Sigma \vdash \mathit{opid} \Longrightarrow \vartheta \\ \Sigma \vdash \mathit{args} \Longrightarrow \Theta & \Sigma \vdash \mathit{term} \Longrightarrow M & \Theta \triangleright \Upsilon_{\Sigma} \oplus \Upsilon \parallel \cdot \vdash M : \tau \end{array}}{\Sigma \vdash \mathtt{Def}\ \mathit{opid}\langle[\mathit{params}]\rangle\langle(\mathit{args})\rangle : \mathit{sortid} = [\mathit{term}] \Longrightarrow (\vartheta, \langle \Upsilon, \Theta, \tau, M \rangle)} \tag{1.8}$$

$$\frac{\begin{array}{cc} \Sigma \vdash \mathit{params} \Longrightarrow \Upsilon & \\ \Sigma \vdash \mathit{args} \Longrightarrow \Theta & \Sigma \vdash \mathit{opid} \Longrightarrow \vartheta \\ \Sigma \vdash \mathit{term} \Longrightarrow M & \Theta \triangleright \Upsilon_{\Sigma} \oplus \Upsilon \parallel \cdot \vdash M : \mathtt{tac} \end{array}}{\Sigma \vdash \mathtt{Tac}\ \mathit{opid}\langle[\mathit{params}]\rangle\langle(\mathit{args})\rangle = [\mathit{term}] \Longrightarrow (\vartheta, \langle \Upsilon, \Theta, \mathtt{tac}, M \rangle)} \tag{1.9}$$

$$\frac{\begin{array}{cccc} \Sigma \vdash \mathit{params} \Longrightarrow \Upsilon & \Sigma \vdash \mathit{term}_1 \Longrightarrow P & \Theta \triangleright \Upsilon_{\Sigma} \oplus \Upsilon \parallel \cdot \vdash P : \mathtt{exp} & \\ \Sigma \vdash \mathit{args} \Longrightarrow \Theta & \Sigma \vdash \mathit{term}_2 \Longrightarrow M & \Theta \triangleright \Upsilon_{\Sigma} \oplus \Upsilon \parallel \cdot \vdash M : \mathtt{tac} & \Sigma \vdash \mathit{opid} \Longrightarrow \vartheta \end{array}}{\Sigma \vdash \mathtt{Thm}\ \mathit{opid}\langle[\mathit{params}]\rangle\langle(\mathit{args})\rangle : [\mathit{term}_1]\ \mathtt{by}\ [\mathit{term}_2] \Longrightarrow (\vartheta, \langle \Upsilon, \Theta, \mathtt{thm}, \mathtt{prove}(P; M) \rangle)} \tag{1.10}$$

Symbol Declarations $\boxed{\Sigma \vdash \mathit{symdec} \Longrightarrow (u, \sigma)}$

$$\frac{\Sigma \vdash \mathit{symbind} \Longrightarrow (u, \sigma)}{\Sigma \vdash \mathtt{Sym}\ \mathit{symbind} \Longrightarrow (u, \sigma)} \tag{1.11}$$

Signatures $\boxed{\vdash \mathit{sigexp} \Longrightarrow \Sigma}$

$$\overline{\vdash \langle \cdot \rangle \Longrightarrow \{\}} \tag{1.12}$$

$$\frac{\vdash \mathit{sigexp} \Longrightarrow \Sigma \quad \Sigma \vdash \mathit{sigdec} \Longrightarrow (\vartheta, D)}{\vdash \mathit{sigexp}\ \mathit{sigdec}. \Longrightarrow \Sigma \cup \vartheta \mapsto D} \qquad \frac{\vdash \mathit{sigexp} \Longrightarrow \Sigma \quad \Sigma \vdash \mathit{symdec} \Longrightarrow (u, \sigma)}{\vdash \mathit{sigexp}\ \mathit{symdec}. \Longrightarrow \Sigma \cup u \mapsto \sigma} \tag{1.13}$$

Chapter 2

Nominal LCF: a language for tactics

This chapter needs to be re-written in light of changes to the Nominal LCF formalism.

Bibliography