The Definition of RedPRL, *the people's refinement logic*

The RedPRL Group

May 8, 2016

Contents

Chapter 1

Signatures

Decisively Smash The Formalist Clique!

Chairman Jon

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

1.1 Grammar

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

1.2 Elaboration Semantics

The static semantics for RedPRL 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:

$$\frac{}{\texttt{tac}\ \mathit{sort}} \qquad \frac{}{\texttt{thm}\ \mathit{sort}} \qquad \frac{}{\texttt{exp}\ \mathit{sort}} \qquad \frac{}{\texttt{opid}\ \mathit{sort}} \qquad \frac{}{\texttt{lbl}\ \mathit{sort}}$$

$$\frac{}{\Upsilon \Vdash \texttt{prove} : (.\,\texttt{exp}, .\,\texttt{tac})\,\texttt{thm}} \qquad \frac{}{\Upsilon \Vdash \texttt{depIsect} : (.\,\texttt{exp}, [\texttt{exp}].\,\texttt{exp})\,\texttt{exp}}$$

$$\frac{\Upsilon \ni u : \texttt{lbl}}{\Upsilon \Vdash \texttt{singl}[u] : (.\,\texttt{exp})\,\texttt{exp}} \qquad \frac{\Upsilon \ni u : \texttt{lbl}}{\Upsilon \Vdash \texttt{proj}[u] : (.\,\texttt{exp})\,\texttt{exp}}$$

$$\frac{}{\Upsilon \Vdash \texttt{top} : ()\,\texttt{exp}}$$

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

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 $\Upsilon_\Sigma \in \mathrm{Params}$ be defined as follows:

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

sigexp	::=	$\langle \cdot \rangle$	empty signature
		sigexp symdec.	signature extension
		sigexp sigdec.	
		sigexp rcddec.	
symdec	::=	`Sym` *symbind*	symbol declaration
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
rcddec	::=	`Rcd` $opid\langle[params]\rangle\langle(args)\rangle = \{rows\}$	record declaration
rows	::=	$\langle \cdot \rangle$	empty record rows
		rows, *row*	record rows extension
row	::=	*symid* : *term*	record row
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.

$$
\begin{array}{rcll}
u, v & \in & \mathrm{Sym} & \\
x, y & \in & \mathrm{Var} & \\
\mathfrak{m}, \mathfrak{n} & \in & \mathrm{Metavar} & \\
\sigma, \tau & \in & \mathrm{Sort} & \triangleq \ \{\, \tau \mid \tau \ \mathit{sort} \,\} \\
v & \in & \mathrm{Valence} & \triangleq \ \{\, v \mid v \ \mathit{valence} \,\} \\
\vartheta & \in & \mathrm{Opid} & \triangleq \ \mathrm{Sym} \\
\Upsilon & \in & \mathrm{Params} & \triangleq \ \mathrm{Sym} \xrightarrow{\text{fin}} \mathrm{Sort} \\
\Gamma, \Delta & \in & \mathrm{Ctx} & \triangleq \ \mathrm{Var} \xrightarrow{\text{fin}} \mathrm{Sort} \\
\Theta & \in & \mathrm{Args} & \triangleq \ \mathrm{Metavar} \xrightarrow{\text{fin}} \mathrm{Valence} \\
M, N, A, B, C & \in & \mathrm{Tm}(\Theta, \Upsilon, \tau) & \triangleq \ \{\, M \mid \Theta \triangleright \Upsilon \parallel \ \cdot \vdash M : \tau \,\} \\
D & \in & \mathrm{Decl} & \triangleq \ \coprod_{\Upsilon, \Theta, \tau} \mathrm{Tm}(\Theta, \Upsilon, \tau) \\
\Sigma & \in & \mathrm{Sig} & \triangleq \ \left(\mathrm{Opid} \xrightarrow{\text{fin}} \mathrm{Decl}\right) \cap \left(\mathrm{Sym} \xrightarrow{\text{fin}} \mathrm{Sort}\right)
\end{array}
$$

Figure 1.2: Specification of the semantic objects.

Symbol Bindings

$$\boxed{\Sigma \vdash \mathit{symbind} \Longrightarrow (a, \tau)}$$

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

Metavariable Bindings

$$\boxed{\Sigma \vdash \mathit{metabind} \Longrightarrow (\mathfrak{m}, v)}$$

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

Parameters

$$\boxed{\Sigma \vdash \mathit{params} \Longrightarrow \Upsilon}$$

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

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

Arguments

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

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

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

Symbols

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

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

Symbol Declarations

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

$$\frac{\Sigma \vdash \mathit{symbind} \Longrightarrow (u, \sigma)}{\Sigma \vdash \texttt{Sym}\ \mathit{symbind} \Longrightarrow (u, \sigma)} \tag{1.8}$$

Operator Declarations

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

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

$$\frac{\begin{array}{ll}\Sigma \vdash \mathit{params} \Longrightarrow \Upsilon & \Sigma \vdash \mathit{opid} \Longrightarrow \vartheta \\ \Sigma \vdash \mathit{args} \Longrightarrow \Theta & \Theta \triangleright \Upsilon_\Sigma \oplus \Upsilon \parallel \cdot \vdash M : \texttt{tac} \\ \Sigma \vdash \mathit{term} \Longrightarrow M & \end{array}}{\Sigma \vdash \texttt{Tac}\ \mathit{opid}\langle[\mathit{params}]\rangle\langle(\mathit{args})\rangle = [\mathit{term}] \Longrightarrow (\vartheta, \langle \Upsilon, \Theta, \texttt{tac}, M\rangle)} \tag{1.10}$$

$$\frac{\begin{array}{lll}\Sigma \vdash \mathit{params} \Longrightarrow \Upsilon & \Sigma \vdash \mathit{term}_1 \Longrightarrow P & \Theta \triangleright \Upsilon_\Sigma \oplus \Upsilon \parallel \cdot \vdash P : \texttt{exp} \\ \Sigma \vdash \mathit{args} \Longrightarrow \Theta & \Sigma \vdash \mathit{term}_2 \Longrightarrow M & \Theta \triangleright \Upsilon_\Sigma \oplus \Upsilon \parallel \cdot \vdash M : \texttt{tac}\end{array} \qquad \Sigma \vdash \mathit{opid} \Longrightarrow \vartheta}{\Sigma \vdash \texttt{Thm}\ \mathit{opid}\langle[\mathit{params}]\rangle\langle(\mathit{args})\rangle : [\mathit{term}_1]\ \texttt{by}\ [\mathit{term}_2] \Longrightarrow (\vartheta, \langle \Upsilon, \Theta, \texttt{thm}, \texttt{prove}(P; M)\rangle)} \tag{1.11}$$

Row Declarations

$$\boxed{\Sigma \vdash^{\Upsilon \parallel \Gamma}_{\Theta} \mathit{row} \Longrightarrow A}$$

$$\frac{\begin{array}{ll}\Sigma \vdash \mathit{symid} \Longrightarrow u & \Theta \triangleright \Upsilon_\Sigma \oplus \Upsilon \parallel \Gamma \vdash A : \texttt{exp} \\ \Sigma \vdash \mathit{term} \Longrightarrow A & \end{array}}{\Sigma \vdash^{\Upsilon \parallel \Gamma}_{\Theta} \mathit{symid} : \mathit{term} \Longrightarrow \texttt{singl}[u](A)} \tag{1.12}$$

Record Rows

$$\boxed{\Sigma \vdash^{\Upsilon \parallel \Gamma}_{\Theta} \mathit{rows} \Longrightarrow (\Sigma', \Delta, A)}$$

$$\frac{}{\Sigma \vdash^{\Upsilon \parallel \Gamma}_{\Theta} \langle\ \cdot\ \rangle \Longrightarrow (\Sigma, \Gamma, \texttt{top}())} \tag{1.13}$$

$$\frac{\begin{array}{lll}\Sigma \vdash^{\Upsilon \parallel \Gamma}_{\Theta} \mathit{rows} \Longrightarrow (\Sigma', \Delta, A) & \Sigma'' \triangleq \Sigma' \cup u \mapsto \texttt{lbl} & C \triangleq \texttt{depIsect}(A; [r].\ [\texttt{proj}[u](r)\ /\ u]\ B) \\ \Sigma' \vdash^{\Upsilon \parallel \Delta}_{\Theta} \mathit{row} \Longrightarrow B & \Delta' \triangleq \Delta \cup u \mapsto \texttt{exp} & \end{array}}{\Sigma \vdash^{\Upsilon \parallel \Gamma}_{\Theta} \mathit{rows}, \mathit{row} \Longrightarrow (\Sigma'', \Delta', C)} \tag{1.14}$$

(1.15)

Record Declarations

$$\boxed{\Sigma \vdash \mathit{rcddec} \Longrightarrow \Sigma'}$$

$$\frac{\begin{array}{ll}\Sigma \vdash \mathit{params} \Longrightarrow \Upsilon & \\ \Sigma \vdash \mathit{args} \Longrightarrow \Theta & \Sigma \vdash^{\Upsilon \parallel \cdot}_{\Theta} \mathit{rows} \Longrightarrow (\Sigma', \Gamma, A) \\ \Sigma \vdash \mathit{opid} \Longrightarrow \vartheta & \end{array}}{\Sigma \vdash \texttt{Rcd}\ \mathit{opid}\langle[\mathit{params}]\rangle\langle(\mathit{args})\rangle = \{\mathit{rows}\} \Longrightarrow \Sigma' \cup \vartheta \mapsto \langle \Upsilon, \Theta, \texttt{exp}, A\rangle} \tag{1.16}$$

Signatures

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

$$\frac{}{\vdash \langle \cdot \rangle \Longrightarrow \{\}} \tag{1.17}$$

$$\frac{\vdash \mathit{sigexp} \Longrightarrow \Sigma \quad \Sigma \vdash \mathit{sigdec} \Longrightarrow (\vartheta, D)}{\vdash \mathit{sigexp}\ \mathit{sigdec}. \Longrightarrow \Sigma \cup \vartheta \mapsto D} \tag{1.18}$$

$$\frac{\vdash \mathit{sigexp} \Longrightarrow \Sigma \quad \Sigma \vdash \mathit{symdec} \Longrightarrow (u, \sigma)}{\vdash \mathit{sigexp}\ \mathit{symdec}. \Longrightarrow \Sigma \cup u \mapsto \sigma} \tag{1.19}$$

$$\frac{\vdash \mathit{sigexp} \Longrightarrow \Sigma \quad \Sigma \vdash \mathit{rcddec} \Longrightarrow \Sigma'}{\vdash \mathit{sigexp}\ \mathit{rcddec}. \Longrightarrow \Sigma'} \tag{1.20}$$

Chapter 2

The Refinement Logic

2.1 Forms of Judgment

2.1.1 Hypothesis Contexts

First, we develop the syntax of hypothesis contexts with respect to a metavariable context Θ *mctx* and a symbol context Υ *sctx*:

$$\frac{}{\Theta \triangleright \Upsilon \parallel \cdot \ \mathit{hypctx}} \qquad \frac{\Theta \triangleright \Upsilon \parallel H \ \mathit{hypctx} \quad \Theta \triangleright \Upsilon \parallel |H| \vdash A : \mathtt{exp} \quad x \notin H}{\Theta \triangleright \Upsilon \parallel H, x :_\tau A \ \mathit{hypctx}}$$

The *domain* $|H|$ *vctx* of a hypothesis context $\Theta \triangleright \Upsilon \parallel H \ \mathit{hypctx}$ is defined as follows:

$$|\cdot| \triangleq \cdot$$
$$|H, x :_\tau A| \triangleq |H|, x : \tau$$

2.1.2 Hypothetico-General Sequents

RedPRL's refinement logic is organized around several forms of *sequent*, which are schematized as follows, depending on the form of conclusion:

$$H \gg^{\Upsilon}_{\Theta} \mathit{conclusion} \rightsquigarrow \mathit{synthesis} \qquad \text{(Sequent)}$$

We also use a *generic sequent* which closes over variables in Γ:

$$[\Gamma] \mid H \gg^{\Upsilon}_{\Theta} \mathit{conclusion} \rightsquigarrow \mathit{synthesis} \qquad \text{(Generic Sequent)}$$

Forms of Conclusion

The form of synthesis depends on the particular form of conclusion (categorical judgment); we formalize this with the $\Theta \triangleright \Upsilon \parallel \Gamma \vdash \lfloor C \rfloor \ \mathit{concl} \rightsquigarrow \tau$ judgment form, defined as follows:

$$\frac{\Theta \triangleright \Upsilon \parallel \Gamma \vdash A : \mathtt{exp}}{\Theta \triangleright \Upsilon \parallel \Gamma \vdash \lfloor A \ \mathit{true}_\tau \rfloor \ \mathit{concl} \rightsquigarrow \tau} \ \text{Truth}$$

$$\frac{\Theta \triangleright \Upsilon \parallel \Gamma \vdash M : \tau \quad \Theta \triangleright \Upsilon \parallel \Gamma \vdash N : \tau \quad \Theta \triangleright \Upsilon \parallel \Gamma \vdash A : \mathtt{exp}}{\Theta \triangleright \Upsilon \parallel \Gamma \vdash \lfloor M = N \in_\tau A \rfloor \ \mathit{concl} \rightsquigarrow \mathtt{exp}} \ \text{Equality}$$

$$\frac{\Theta \triangleright \Upsilon \parallel \Gamma \vdash M : \tau \quad \Theta \triangleright \Upsilon \parallel \Gamma \vdash A : \mathtt{exp}}{\Theta \triangleright \Upsilon \parallel \Gamma \vdash \lfloor M \in_\tau A \rfloor\ concl \rightsquigarrow \mathtt{exp}}\ \text{Membership}$$

$$\frac{\Theta \triangleright \Upsilon \parallel \Gamma \vdash R : \tau \quad \Theta \triangleright \Upsilon \parallel \Gamma \vdash A : \mathtt{exp}}{\Theta \triangleright \Upsilon \parallel \Gamma \vdash \lfloor R\ synth_\tau \rfloor\ concl \rightsquigarrow \mathtt{exp}}\ \text{Membership Synthesis}$$

$$\frac{\begin{array}{c}\Theta \triangleright \Upsilon \parallel \Gamma \vdash R : \tau \\ \Theta \triangleright \Upsilon \parallel \Gamma \vdash S : \tau\end{array} \quad \Theta \triangleright \Upsilon \parallel \Gamma \vdash A : \mathtt{exp}}{\Theta \triangleright \Upsilon \parallel \Gamma \vdash \lfloor R = S\ synth_\tau \rfloor\ concl \rightsquigarrow \mathtt{exp}}\ \text{Equality Synthesis}$$

$$\frac{\Theta \triangleright \Upsilon \parallel \Gamma \vdash A : \mathtt{exp}}{\Theta \triangleright \Upsilon \parallel \Gamma \vdash \lfloor A\ type \rfloor\ concl \rightsquigarrow \mathtt{lvl}}\ \text{Level Synthesis}$$

Syntax of Sequents

Now that we have enumerated the forms of conclusion, we can precisely give the syntax of the sequent judgment. We will say that the sequent $H \gg^{\Upsilon}_{\Theta} C \rightsquigarrow S$ is a meaningful judgment in case the following presuppositions obtain:

1. Θ *mctx*
2. Υ *sctx*
3. $\Theta \triangleright \Upsilon \parallel H$ *hypctx*
4. $\Theta \triangleright \Upsilon \parallel |H| \vdash \lfloor C \rfloor\ concl \rightsquigarrow \tau$
5. $\Theta \triangleright \Upsilon \parallel |H| \vdash S : \tau$

The meaning of the sequent judgment is given inductively by a collection of formal rules, which are then related to the *intended semantics* of Nominal Computational Type Theory by a soundness theorem.

Syntax of Generic Sequents

The generic sequent $[\Gamma] \mid H \gg^{\Upsilon}_{\Theta} C \rightsquigarrow E$ is presupposes the following:

1. Θ *mctx*
2. Υ *sctx*
3. $\Theta \triangleright \Upsilon \parallel H$ *hypctx*
4. Γ *vctx* and $\Gamma \subseteq |H|$
5. $\Theta \triangleright \Upsilon \parallel |H| \vdash \lfloor C \rfloor\ concl \rightsquigarrow \tau$
6. $\Theta \triangleright \Upsilon \parallel |H| \setminus \Gamma \vdash E : [\Gamma].\tau$

Notice that the synthesis of a *generic* sequent is always an *abstraction* / binder, which allows a rule to single out some portion Γ of the hypothetical context H for later substitution. This provides a hygienic way to to express refinement rules which introduce a new hypothesis, such as the introduction rule for functions. More generally, the binding of variables in the synthesis to a judgment is an essential part of the Dependent LCF apparatus.

2.2 Selected Rules

The *generic sequent* is introduced as follows, by closing synthesis of the corresponding regular sequent in an abstraction of the variables in Γ.

$$\frac{H \gg^{\Upsilon}_{\Theta} C \rightsquigarrow S}{[\Gamma] \mid H \gg^{\Upsilon}_{\Theta} C \rightsquigarrow [\vec{x}].\ [\vec{x}\ /\ \Gamma]\, S}$$

Membership in checking-mode is defined in terms of equality.

$$\frac{H \gg^{\Upsilon}_{\Theta} M = M \in_{\tau} A \rightsquigarrow \mathtt{Ax}}{H \gg^{\Upsilon}_{\Theta} M \in_{\tau} A \rightsquigarrow \mathtt{Ax}}$$

Dually, equality synthesis is defined in terms of membership synthesis.

$$\frac{\begin{array}{ll} H \gg^{\Upsilon}_{\Theta} R\ \mathit{synth}_{\tau} \rightsquigarrow A_1 & H \gg^{\Upsilon}_{\Theta} A_1\ \mathit{synth} \rightsquigarrow \mathbb{U}_i \\ H \gg^{\Upsilon}_{\Theta} S\ \mathit{synth}_{\tau} \rightsquigarrow A_2 & H \gg^{\Upsilon}_{\Theta} A_1 = A_2 \in_{\mathtt{exp}} \mathbb{U}_i \rightsquigarrow \mathtt{Ax} \end{array}}{H \gg^{\Upsilon}_{\Theta} R = S\ \mathit{synth}_{\tau} \rightsquigarrow A_1}$$