

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

The **Red**PRL Group

May 8, 2016

# Contents

<b>1</b>	<b>Signatures</b>	<b>2</b>
1.1	Grammar . . . . .	2
1.2	Elaboration Semantics . . . . .	2
<b>2</b>	<b>The Refinement Logic</b>	<b>7</b>
2.1	Forms of Judgment . . . . .	7
2.1.1	Hypothesis Contexts . . . . .	7
2.1.2	Hypothetico-General Sequents . . . . .	7
2.2	Selected Rules . . . . .	9

# 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 **Red**PRL 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 **Red**PRL 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:

$$\begin{array}{c}
 \overline{\text{tac sort}} \quad \overline{\text{thm sort}} \quad \overline{\text{exp sort}} \quad \overline{\text{opid sort}} \quad \overline{\text{lbl sort}} \\
 \hline
 \overline{\Upsilon \Vdash \text{prove} : (. \text{exp}, . \text{tac}) \text{ thm}} \quad \overline{\Upsilon \Vdash \text{depIsect} : (. \text{exp}, [\text{exp}]. \text{exp}) \text{ exp}} \\
 \hline
 \overline{\Upsilon \ni u : \text{lbl}} \quad \overline{\Upsilon \ni u : \text{lbl}} \\
 \hline
 \overline{\Upsilon \Vdash \text{singl}[u] : (. \text{exp}) \text{ exp}} \quad \overline{\Upsilon \Vdash \text{proj}[u] : (. \text{exp}) \text{ exp}} \\
 \hline
 \overline{\Upsilon \Vdash \text{top} : () \text{ exp}}
 \end{array}$$

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

$$\Upsilon_\Sigma(u) \triangleq \begin{cases} \text{opid} & \text{if } u \equiv \vartheta \in \text{dom}(\Sigma) \\ \tau & \text{if } \Sigma(u) \equiv \tau \\ \perp & \text{otherwise} \end{cases}$$

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

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

Figure 1.2: Specification of the semantic objects.

## Symbol Bindings

$$\boxed{\Sigma \vdash \text{sybind} \Longrightarrow (a, \tau)}$$

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

## Metavariable Bindings

$$\boxed{\Sigma \vdash \text{metabind} \Longrightarrow (\mathbf{m}, v)}$$

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

## Parameters

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

$$\overline{\Sigma \vdash \langle \cdot \rangle \Longrightarrow \{\}} \quad (1.3)$$

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

## Arguments

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

$$\overline{\Sigma \vdash \langle \cdot \rangle \Longrightarrow \{\}} \quad (1.5)$$

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

## Symbols

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

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

## Symbol Declarations

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

$$\frac{\Sigma \vdash \text{sybind} \Longrightarrow (u, \sigma)}{\Sigma \vdash \mathbf{Sym} \text{ sybind} \Longrightarrow (u, \sigma)} \quad (1.8)$$

## Operator Declarations

$$\boxed{\Sigma \vdash \text{sigdec} \Rightarrow (\vartheta, D)}$$

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

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

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

## Row Declarations

$$\boxed{\Sigma \vdash_{\Theta}^{\Upsilon \parallel \Gamma} \text{row} \Rightarrow A}$$

$$\frac{\begin{array}{ccc} \Sigma \vdash \text{symid} \Rightarrow u & & \Theta \triangleright \Upsilon_\Sigma \oplus \Upsilon \parallel \Gamma \vdash A : \text{exp} \\ \Sigma \vdash \text{term} \Rightarrow A & & \end{array}}{\Sigma \vdash_{\Theta}^{\Upsilon \parallel \Gamma} \text{symid} : \text{term} \Rightarrow \text{singl}[u](A)} \quad (1.12)$$

## Record Rows

$$\boxed{\Sigma \vdash_{\Theta}^{\Upsilon \parallel \Gamma} \text{rows} \Rightarrow (\Sigma', \Delta, A)}$$

$$\overline{\Sigma \vdash_{\Theta}^{\Upsilon \parallel \Gamma} \langle \cdot \rangle \Rightarrow (\Sigma, \Gamma, \text{top}())} \quad (1.13)$$

$$\frac{\begin{array}{ccc} \Sigma \vdash_{\Theta}^{\Upsilon \parallel \Gamma} \text{rows} \Rightarrow (\Sigma', \Delta, A) & \Sigma'' \triangleq \Sigma' \cup u \mapsto \text{lbl} & C \triangleq \text{depIsect}(A; [r]. [\text{proj}[u](r) / u] B) \\ \Sigma' \vdash_{\Theta}^{\Upsilon \parallel \Delta} \text{row} \Rightarrow B & \Delta' \triangleq \Delta \cup u \mapsto \text{exp} & \end{array}}{\Sigma \vdash_{\Theta}^{\Upsilon \parallel \Gamma} \text{rows}, \text{row} \Rightarrow (\Sigma'', \Delta', C)} \quad (1.14)$$

$$(1.15)$$

## Record Declarations

$$\boxed{\Sigma \vdash \text{rcddec} \Rightarrow \Sigma'}$$

$$\frac{\begin{array}{ccc} \Sigma \vdash \text{params} \Rightarrow \Upsilon & & \Sigma \vdash_{\Theta}^{\Upsilon \parallel \cdot} \text{rows} \Rightarrow (\Sigma', \Gamma, A) \\ \Sigma \vdash \text{args} \Rightarrow \Theta & & \\ \Sigma \vdash \text{opid} \Rightarrow \vartheta & & \end{array}}{\Sigma \vdash \text{Rcd opid} \langle [\text{params}] \rangle \langle (\text{args}) \rangle = \{\text{rows}\} \Rightarrow \Sigma' \cup \vartheta \mapsto \langle \Upsilon, \Theta, \text{exp}, A \rangle} \quad (1.16)$$

## Signatures

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

$$\overline{\vdash \langle \cdot \rangle \Longrightarrow \{\}} \quad (1.17)$$

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

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

$$\frac{\vdash \textit{sigexp} \Longrightarrow \Sigma \quad \Sigma \vdash \textit{rcdddec} \Longrightarrow \Sigma'}{\vdash \textit{sigexp rcdddec.} \Longrightarrow \Sigma'} \quad (1.20)$$

# 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  $\Theta \triangleright mctx$  and a symbol context  $\Upsilon \triangleright sctx$ :

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

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

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

#### 2.1.2 Hypothetico-General Sequents

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

$$H \gg_{\Theta}^{\Upsilon} \text{conclusion} \rightsquigarrow \text{synthesis} \quad (\text{Sequent})$$

We also use a *generic sequent* which closes over variables in  $\Gamma$ :

$$[\Gamma] \mid H \gg_{\Theta}^{\Upsilon} \text{conclusion} \rightsquigarrow \text{synthesis} \quad (\text{Generic Sequent})$$

#### Forms of Conclusion

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

$$\frac{\Theta \triangleright \Upsilon \parallel \Gamma \vdash A : \text{exp}}{\Theta \triangleright \Upsilon \parallel \Gamma \vdash [A \text{ true}_{\tau}] \text{ concl} \rightsquigarrow \tau} \text{ Truth}$$

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



$$\begin{array}{c}
\frac{\Theta \triangleright \Upsilon \parallel \Gamma \vdash M : \tau \quad \Theta \triangleright \Upsilon \parallel \Gamma \vdash A : \mathbf{exp}}{\Theta \triangleright \Upsilon \parallel \Gamma \vdash [M \in_\tau A] \text{ concl} \rightsquigarrow \mathbf{exp}} \text{ Membership} \\
\\
\frac{\Theta \triangleright \Upsilon \parallel \Gamma \vdash R : \tau \quad \Theta \triangleright \Upsilon \parallel \Gamma \vdash A : \mathbf{exp}}{\Theta \triangleright \Upsilon \parallel \Gamma \vdash [R \text{ synth}_\tau] \text{ concl} \rightsquigarrow \mathbf{exp}} \text{ Membership Synthesis} \\
\\
\frac{\Theta \triangleright \Upsilon \parallel \Gamma \vdash R : \tau \quad \Theta \triangleright \Upsilon \parallel \Gamma \vdash S : \tau \quad \Theta \triangleright \Upsilon \parallel \Gamma \vdash A : \mathbf{exp}}{\Theta \triangleright \Upsilon \parallel \Gamma \vdash [R = S \text{ synth}_\tau] \text{ concl} \rightsquigarrow \mathbf{exp}} \text{ Equality Synthesis} \\
\\
\frac{\Theta \triangleright \Upsilon \parallel \Gamma \vdash A : \mathbf{exp}}{\Theta \triangleright \Upsilon \parallel \Gamma \vdash [A \text{ type}] \text{ concl} \rightsquigarrow \mathbf{lvl}} \text{ Level Synthesis}
\end{array}$$

### 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  $H \gg_{\Theta}^{\Upsilon} C \rightsquigarrow S$  is a meaningful judgment in case the following presuppositions obtain:

1.  $\Theta \text{ mctx}$
2.  $\Upsilon \text{ sctx}$
3.  $\Theta \triangleright \Upsilon \parallel H \text{ hypctx}$
4.  $\Theta \triangleright \Upsilon \parallel |H| \vdash [C] \text{ concl} \rightsquigarrow \tau$
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  $[\Gamma] \mid H \gg_{\Theta}^{\Upsilon} C \rightsquigarrow E$  is presupposes the following:

1.  $\Theta \text{ mctx}$
2.  $\Upsilon \text{ sctx}$
3.  $\Theta \triangleright \Upsilon \parallel H \text{ hypctx}$
4.  $\Gamma \text{ vctx}$  and  $\Gamma \subseteq |H|$
5.  $\Theta \triangleright \Upsilon \parallel |H| \vdash [C] \text{ concl} \rightsquigarrow \tau$
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  $\Gamma$  of the hypothetical context  $H$  for later substitution. This provides a hygienic way 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  $\Gamma$ .

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

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

$$\frac{H \gg_{\Theta}^{\Upsilon} M = M \in_{\tau} A \rightsquigarrow \mathbf{Ax}}{H \gg_{\Theta}^{\Upsilon} M \in_{\tau} A \rightsquigarrow \mathbf{Ax}}$$

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

$$\frac{\begin{array}{l} H \gg_{\Theta}^{\Upsilon} R \text{ synth}_{\tau} \rightsquigarrow A_1 \quad H \gg_{\Theta}^{\Upsilon} A_1 \text{ type} \rightsquigarrow i \\ H \gg_{\Theta}^{\Upsilon} S \text{ synth}_{\tau} \rightsquigarrow A_2 \quad H \gg_{\Theta}^{\Upsilon} A_1 = A_2 \in_{\text{exp}} \mathbb{U}_i \rightsquigarrow \mathbf{Ax} \end{array}}{H \gg_{\Theta}^{\Upsilon} R = S \text{ synth}_{\tau} \rightsquigarrow A_1}$$