Type Refinements for the Working Class

Jon Sterling and Darin Morrison

There are two conflicting views which bedevil any discussion of the nature of type theory. First, there is the notion of type theory as an extension or generalization of universal algebra to support interdependency of sorts and operations, possibly subject to an arbitrary equational theory [1, 3]; we will call this *formal type theory*. Typing, in such a setting, is a mere matter of grammar and is nearly always decidable. In hindsight, we may observe that this is the sort of type theory which Martin-Löf first proposed in 1972 [10], even if we will admit that this was not the intention at the time. A model for such a type theory is usually given by interpreting the types or sorts as presheaves or sheaves over contexts of hypotheses, and as such, a proof theoretic interpretation of the hypothetical judgment is inevitable.

Secondly, there is the view of type theory as semi-formal theory of constructions for the Brouwer-Heyting-Kolmogorov interpretation of intuitionistic mathematical language, which we will call *behavioral* or *semantic type theory*. The most widely known development of this program is Martin-Löf's 1979 "extensional" type theory [11, 12], but we must give priority to Dana Scott for inventing this line of research in 1970 with his prophetic report, *Constructive Validity* [13]. Since the 1980s, behavioral type theory has been developed much further in the Nuprl family [2] of proof assistants, including MetaPRL [7] and JonPRL [14].

Martin-Löf's key innovation was the commitment to pervasive functionality (extensionality) as part of the *definitions* of the judgments and the types, in contrast to the state of affairs in formal type theory where functionality is a metatheorem which must be shown to obtain, based on the (somewhat arbitrary) equational theory which has been imposed. Furthermore, models for behavioral type theory interpret the types as partial equivalence relations on only closed terms, and the meaning of the hypothetical judgment is defined separately and uniformly in the logical relations style.

Our position is that these views of type theory are not in conflict, but rather merely describe two distinct layers in a single, harmonious system. From this perspective, formal type theories can do little more than negotiate matters of grammar, and therefore may serve as a syntactic (linguistic) framework for mathematical language, being responsible for the management of variable binding and substitution. On the other hand, the meaning of mathematical statements shall be specified *behaviorally* in the semantic type theory.

The types of the semantic theory can then be said to *refine* the types of the syntactic theory [5, 6, 4], both by placing restrictions on membership and by coarsening equivalence.

Thus far, most developments of behavioral type theory have been built on a *unityped* syntactic framework, and so the relation to type refinements has been difficult to see. In this paper, we contribute a full theory of behavioral refinements over multi-sorted abstract binding trees, a simple formal type theory [4, 15]; this hybrid system allows the deployment of a Nuprl-style type theory over any signature of sorts and operators.

Colors In this paper, we hint at the *modes* of judgments and assertions [4] using colors, marking inputs with `blue` and outputs with `red`. As a rule of thumb, inputs are things which are supplied when checking the correctness of a judgment, and outputs are things which are synthesized in the process.

1 Abstract Binding Trees and Symbols

See [15] for the development of abstract binding trees with symbols.

give a brief description of the framework, and present its rules.

2 Behavioral Refinements

Fixing a signature $\Sigma \equiv \langle \mathcal{S}, \mathcal{O} \rangle$ in the abt framework, we will define the notion of behavioral refinement by propounding several judgments and their semantical explanations. Let us first define the presheaf of τ-sorted expressions, $\mathbf{E}_\tau$ as follows

$$\mathbf{E}_\tau(\Upsilon \parallel \Gamma) \triangleq \{ M \mid \cdot \triangleright \Upsilon \parallel \Gamma \vdash M : \tau \}$$

We will also write $\mathbf{E}_\tau$ for the presheaf $\mathbf{E}_\tau(- \parallel \cdot)$ on **SCtx**.

2.1 Parametric Refinement

The first judgment that will concern us is called *parametric refinement*, $\Upsilon \parallel \phi \sqsubset \tau$, which means that ϕ refines the sort τ under the symbolic parameters Υ. We define this judgment through a meaning explanation in the style of Martin-Löf as follows:

Definition 2.1. To know $\Upsilon \parallel \phi \sqsubset \tau$ (presupposing Υ *sctx* and τ *sort*) is to know, for any $\Upsilon \xhookrightarrow{\rho} \Upsilon'$, what it means for any $M, N \in \mathbf{E}_\tau(\Upsilon')$ to be equated by ϕ (written $\phi\{\rho\}(M, N)$), such that $\phi\{\rho\}(-,-)$ is a partial equivalence relation on $\mathbf{E}_\tau(\Upsilon')$. Morever, that for any $\Upsilon' \xhookrightarrow{\rho'} \Upsilon''$, from $\phi\{\rho\}(M, N)$ we may conclude $\phi\{\rho' \circ \rho\}(M\rho', N\rho')$.

Then, we say that ϕ *globally refines* τ (written $\phi \sqsubset \tau$) when we have $\cdot \parallel \phi \sqsubset \tau$. Furthermore, when $\Upsilon \parallel \phi \sqsubset \tau$, for any renaming $\Upsilon \xhookrightarrow{\rho} \Upsilon'$ we can clearly define a new refinement $\Upsilon' \parallel \phi\rho \sqsubset \tau$.

Remark 2.2. At this point, it should be noted that this is very similar to the semantical explanation of typehood given in [11], except that we have generalized it to a multi-sorted setting, and that we have fibred the entire apparatus over collections Υ of symbols.

In fact, the complexity of the above meaning explanation is an artifact of the pointwise style in which we have expressed it. Considered internally to the presheaf topos $\mathbf{Set}^{\mathbf{SCtx}}$, a refinement is merely a section of the object of $\mathbf{E}_\tau$-PERs $\mathfrak{per}(\mathbf{E}_\tau)$, defined internally as a subobject of $\Omega^{\mathbf{E}_\tau \times \mathbf{E}_\tau}$:

$$\mathfrak{per}(X) \triangleq \{\phi : \Omega^{X \times X} \mid \mathit{symmetric}(\phi) \wedge \mathit{transitive}(\phi)\}$$

So, $\Upsilon \parallel \phi \sqsubset \tau$ obtains just when we have $\phi \in \mathfrak{per}(\mathbf{E}_\tau)(\Upsilon)$. The benefit of explaining such judgments in terms of the presheaf topos is that we do not need to deal with the complexities of quantifying over renamings, since this is implicit in the definition of the exponential of presheaves,

$$\begin{aligned} B^A(\Upsilon) &\triangleq \mathbf{Set}^{\mathbf{SCtx}}\,[\mathbf{y}(\Upsilon) \times A, B] \\ &\cong \int_{\Upsilon'} (\Upsilon \hookrightarrow \Upsilon') \Rightarrow B(\Upsilon')^{A(\Upsilon')} \end{aligned}$$

2.1.1 Order and Equality of Parametric Refinements

We will write $\Upsilon \parallel \phi \subseteq \psi \sqsubset \tau$ to mean that ϕ is a *subrefinement* of ψ.

Definition 2.3. To know $\Upsilon \parallel \phi \subseteq \psi \sqsubset \tau$ (presupposing $\Upsilon \parallel \phi \sqsubset \tau$ and $\Upsilon \parallel \psi \sqsubset \tau$) , is to know, for any renamings $\Upsilon \xhookrightarrow{\rho} \Upsilon' \xhookrightarrow{\rho'} \Upsilon''$, that from $\phi\{\rho\}(M, N)$ you can conclude $\psi\{\rho' \circ \rho\}(M\rho', N\rho')$ for any $M, N \in \mathbf{E}_\tau(\Upsilon')$.

Two refinements are equal when they denote the same PER. That is, we have $\Upsilon \parallel \phi = \psi \sqsubset \tau$ just when both $\Upsilon \parallel \phi \subseteq \psi \sqsubset \tau$ and $\Upsilon \parallel \psi \subseteq \phi \sqsubset \tau$.

2.2 Parametric Equality

The primary judgment concerning refinements is the parametric equality, $\Upsilon \parallel M = N \in \phi$, which presupposes $\Upsilon' \parallel \phi \sqsubset \tau$ for some Υ' such that we have $\Upsilon' \xhookrightarrow{\rho} \Upsilon$, and $M, N \in \mathbf{E}_\tau(\Upsilon)$. The meaning of this judgment is that M and N are identified by ϕ at Υ:

$$\frac{\phi\{\rho\}(M, N)}{\Upsilon \parallel M = N \in \phi}$$

2.3 Functional Refinement

Next, we define functional refinement $\Upsilon \parallel \Psi \vDash \phi = \psi \sqsubset \tau$ in terms of parametric refinement, simultaneously with parametric context refinement $\Upsilon \parallel \Psi \sqsubset^\star \Gamma$ and functional equality $\Upsilon \parallel \Psi \vDash M = N \in \phi$. We will write $\Upsilon \parallel \Psi \vDash \phi \sqsubset \tau$ as a shorthand for $\Upsilon \parallel \Psi \vDash \phi = \phi \sqsubset \tau$.

Parametric context refinement $\Upsilon \parallel \Psi \sqsubset^\star \Gamma$ shall be defined as follows, presupposing Υ *sctx* and Γ *vctx*:

$$\frac{}{\Upsilon \parallel \cdot \sqsubset^\star \cdot}\ \sqsubset^\star_{\mathsf{nil}} \qquad \frac{\Upsilon \parallel \Psi \sqsubset^\star \Gamma \quad \Upsilon \parallel \Psi \vDash \phi \sqsubset \tau}{\Upsilon \parallel \Psi, x : \phi \sqsubset^\star \Gamma, x : \tau}\ \sqsubset^\star_{\mathsf{snoc}}$$

For a context refinement $\Upsilon \parallel \Psi \sqsubset^\star \Gamma$ and a renaming $\Upsilon \xhookrightarrow{\rho} \Upsilon'$, we can define a new context refinement $\Upsilon' \parallel \Psi\rho \sqsubset^\star \Gamma$ by applying ρ pointwise at each of the sort refinements in the context.

Functional refinement $\Upsilon \parallel \Psi \vDash \phi = \psi \sqsubset \tau$ presupposes $\Upsilon \parallel \Psi \sqsubset^\star \Gamma$ and τ *sort*, and is explained by induction on the evidence for its first presupposition.

Case $\dfrac{}{\Upsilon \parallel \cdot \sqsubset^\star \cdot}\ \sqsubset^\star_{\mathsf{nil}}$.

$$\frac{\Upsilon \parallel \phi = \psi \sqsubset \tau}{\Upsilon \parallel \cdot \vDash \phi = \psi \sqsubset \tau}\ \vDash^\sqsubset_{\mathsf{nil}}$$

Case $\dfrac{\Upsilon \parallel \Psi \sqsubset^\star \Gamma \quad \Upsilon \parallel \Psi \vDash \chi \sqsubset \sigma}{\Upsilon \parallel \Psi, x : \chi \sqsubset^\star \Gamma, x : \sigma}\ \sqsubset^\star_{\mathsf{snoc}}$.

To know $\Upsilon \parallel \Psi, x : \chi \vDash \phi = \psi \sqsubset \tau$ is to know, for any renaming $\Upsilon \xhookrightarrow{\rho} \Upsilon'$ and closed terms $M, N \in \mathbf{E}_\sigma(\Upsilon')$, that from $\Upsilon \parallel \Psi\rho \vDash M = N \in \chi\rho$, you can conclude $\Upsilon \parallel \Psi\rho \vDash [M\,/\,x]\,\phi\rho = [N\,/\,x]\,\psi\rho \sqsubset \tau$. In other words:

$$\frac{\begin{array}{l}\forall \Upsilon \xhookrightarrow{\rho} \Upsilon'.\ \forall M, N \in \mathbf{E}_\sigma(\Upsilon').\\ (\Upsilon \parallel \Psi\rho \vDash M = N \in \chi\rho) \Rightarrow (\Upsilon \parallel \Psi\rho \vDash [M\,/\,x]\,\phi\rho = [N\,/\,x]\,\psi\rho \sqsubset \tau)\end{array}}{\Upsilon \parallel \Psi, x : \chi \vDash \phi = \psi \sqsubset \tau}\ \vDash^\sqsubset_{\mathsf{snoc}}$$

2.4 Lazy Computation Systems

In this section we generalize Howe's notion of lazy computation system [8] to the multi-sorted, symbol-parameterized setting. An *lazy computation language* is an abt signature $\Sigma \equiv \langle \mathcal{S}, \mathcal{O} \rangle$ along with a distinguished presheaf $\mathcal{K} : \mathbf{Set}^{\mathbf{SCtx} \times \mathcal{A}_\equiv}$ of *canonical* operators such that $\mathcal{K} \subseteq \mathcal{O}$. For a lazy computation language $\mathsf{L} \equiv \langle \mathcal{S}, \mathcal{O}, \mathcal{K} \rangle$, let us define the covariant

presheaves on **SCtx** $\times$ **Ctx** of open expressions, open values, and open bound terms as follows:

$$\mathbf{E}_\tau(\Upsilon \parallel \Gamma) \triangleq \{ M \mid \cdot \triangleright \Upsilon \parallel \Gamma \vdash M : \tau \}$$
$$\mathbf{V}_\tau(\Upsilon \parallel \Gamma) \triangleq \left\{ M \equiv \vartheta(\vec{E}) \mid M \in \mathbf{E}_\tau(\Upsilon \parallel \Gamma) \wedge \exists a. \mathcal{K} \langle \Upsilon, a \rangle \ni \vartheta \right\}$$
$$\mathbf{B}_\nu(\Upsilon \parallel \Gamma) \triangleq \{ E \mid \cdot \triangleright \Upsilon \parallel \Gamma \vdash E : \nu \}$$

We'll write $\mathbf{E}_\tau(\Upsilon)$, $\mathbf{V}_\tau(\Upsilon)$ and $\mathbf{B}_\nu(\Upsilon)$ for $\mathbf{E}_\tau(\Upsilon \parallel \cdot)$, $\mathbf{V}_\tau(\Upsilon \parallel \cdot)$ and $\mathbf{B}_\nu(\Upsilon \parallel \cdot)$ respectively, viewed as covariant presheaves on **SCtx**. Then, a *lazy computation system* (lcs) is a lazy computation language $L \equiv \langle \Sigma, \mathcal{K} \rangle$ along with an **SCtx**-indexed $\equiv_\alpha$-functional evaluation relation $\Upsilon \parallel M \Downarrow_\tau^n N$ presupposing $n \in \mathbb{N}$, $M \in \mathbf{E}_\tau(\Upsilon)$ and $N \in \mathbf{V}_\tau(\Upsilon)$, expressing that M evaluates to N in n steps. We will write $\Upsilon \parallel M \Downarrow_\tau N$ to mean that there exists an n such that $\Upsilon \parallel M \Downarrow_\tau^n N$.

Remark 2.4. In any topos $\mathcal{E}$, for an object X we can define the object of relations on X as the exponential $\wp(X) \triangleq \Omega^X$. Then, the data of such a relation is contained in a natural transformation $R : \mathcal{E}[\mathbb{1}, \wp(X)]$.

Fix a sort-indexed family of binary relations on closed expressions $R_\tau : \mathbf{Set}^{\mathbf{SCtx}}\left[\mathbb{1}, \wp\left(\mathbf{E}_\tau^2\right)\right]$; we will also write the relation as a judgment scheme $\Upsilon \parallel M \; R_\tau \; N$. Now, we can always extend R_τ to a new family of relations $R_\nu : \mathbf{Set}^{\mathbf{SCtx}}\left[\mathbb{1}, \wp\left(\mathbf{B}_\nu^2\right)\right]$ for any valence $\nu \equiv \{\vec{\sigma}\}[\vec{\tau}].\,\tau$, defined pointwise as follows:

$$\frac{\begin{array}{l}\forall \vec{w} \# |\Upsilon| \cup \vec{u} \cup \vec{v}. \quad \forall \vec{X} : \mathbf{E}_\tau^{[\vec{\tau}]}(\Upsilon, \vec{w} : \vec{\sigma}). \\ \Upsilon, \vec{w} : \vec{\sigma} \parallel \left[\vec{X} / \vec{x}\right] \{\vec{w} / \vec{u}\} M \; R_\tau \; \left[\vec{X} / \vec{y}\right] \{\vec{w} / \vec{v}\} N\end{array}}{\Upsilon \parallel \mathbb{\lambda}\{\vec{u}\}[\vec{x}].\, M \; R_{\{\vec{\sigma}\}[\vec{\tau}].\,\tau} \; \mathbb{\lambda}\{\vec{v}\}[\vec{y}].\, N}$$

As a matter of convenience, we'll also define this judgment over vectors of bound terms and valences:

$$\frac{\forall (E, F, \nu) \in (\vec{E}, \vec{F}, \vec{\nu}).\, \Upsilon \parallel E \; R_\nu \; F}{\Upsilon \parallel \vec{E} \; R_{\vec{\nu}} \; \vec{F}}$$

Now, we can extend R_τ to a new relation $[R_\tau]$ on closed expressions which respects a single "layer" of computation. We will say $\Upsilon \parallel M \; [R_\tau] \; N$ when, supposing $\Upsilon \parallel M \Downarrow_\tau \vartheta(\vec{E})$ such that $\Upsilon \Vdash_{\mathcal{K}} \vartheta : (\vec{\nu})\,\tau$, for any $\Upsilon \xhookrightarrow{\rho} \Upsilon'$, we have $\Upsilon' \parallel N\rho \Downarrow_\tau \vartheta\rho(\vec{F}\rho)$ and $\Upsilon' \parallel \vec{E}\rho \; R_{\vec{\nu}} \; \vec{F}\rho$.

Definition 2.5 (Computational Approximation)**.** Because $[-_\tau]$ is monotonic, it has a greatest fixed point, which we will call *computational approximation*, $\preccurlyeq_\tau : \mathbf{Set}^{\mathbf{SCtx}}\left[\mathbb{1}, \wp\left(\mathbf{E}_\tau^2\right)\right]$, written pointwise as $\Upsilon \parallel M \preccurlyeq_\tau N$.

Definition 2.6 (Computational Equivalence)**.** Two terms are said to be *computationally equivalent* when they approximate each other:

$$\frac{\Upsilon \parallel M \preccurlyeq_\tau N \quad \Upsilon \parallel N \preccurlyeq_\tau M}{\Upsilon \parallel M \sim_\tau N}$$

References

[1] J. Cartmell. Generalised algebraic theories and contextual categories. *Annals of Pure and Applied Logic*, 32:209 – 243, 1986.

[2] R. L. Constable, S. F. Allen, H. M. Bromley, W. R. Cleaveland, J. F. Cremer, R. W. Harper, D. J. Howe, T. B. Knoblock, N. P. Mendler, P. Panangaden, J. T. Sasaki, and S. F. Smith. *Implementing Mathematics with the Nuprl Proof Development System*. Prentice-Hall, Inc., Upper Saddle River, NJ, USA, 1986.

[3] P. Dybjer. Internal type theory. In S. Berardi and M. Coppo, editors, *Types for Proofs and Programs*, volume 1158 of *Lecture Notes in Computer Science*, pages 120–134. Springer Berlin Heidelberg, 1996.

[4] R. Harper. *Practical Foundations for Programming Languages*. Cambridge University Press, New York, NY, USA, 2016.

[5] R. Harper and R. Davies. Refining Objects (Preliminary Summary). `https://www.cs.cmu.edu/~rwh/papers/lc60/lc60.pdf`, 2014.

[6] R. Harper and W. Duff. Type Refinements in an Open World. `https://www.cs.cmu.edu/~rwh/papers/trow/summary.pdf`, 2015.

[7] J. Hickey, A. Nogin, R. L. Constable, B. E. Aydemir, E. Barzilay, Y. Bryukhov, R. Eaton, A. Granicz, A. Kopylov, C. Kreitz, V. N. Krupski, L. Lorigo, S. Schmitt, C. Witty, and X. Yu. MetaPRL – a modular logical environment. In D. Basin and B. Wolff, editors, *Theorem Proving in Higher Order Logics*, volume 2758 of *Lecture Notes in Computer Science*, pages 287–303. Springer Berlin Heidelberg, 2003.

[8] D. J. Howe. Equality in lazy computation systems. In *Proceedings of Fourth IEEE Symposium on Logic in Computer Science*, pages 198–203.

[9] S. Mac Lane. *Categories for the Working Mathematician*. Number 5 in Graduate Texts in Mathematics. Springer-Verlag, 1971.

[10] P. Martin-Löf. An intuitionistic theory of types, 1972.

[11] P. Martin-Löf. Constructive mathematics and computer programming. In L. J. Cohen, J. Łoś, H. Pfeiffer, and K.-P. Podewski, editors, *Logic, Methodology and Philosophy of Science VI, Proceedings of the Sixth International Congress of Logic, Methodology and Philosophy of Science, Hannover 1979*, volume 104 of *Studies in Logic and the Foundations of Mathematics*, pages 153–175. North-Holland, 1982.

[12] P. Martin-Löf and G. Sambin. *Intuitionistic type theory*. Studies in proof theory. Bibliopolis, Napoli, 1984.

[13] D. Scott. Constructive validity. In M. Laudet, D. Lacombe, L. Nolin, and M. Schtzenberger, editors, *Symposium on Automatic Demonstration*, volume 125 of *Lecture Notes in Mathematics*, pages 237–275. Springer Berlin Heidelberg, 1970.

[14] J. Sterling, D. Gratzer, and V. Rahli. JonPRL. `http://www.jonprl.org/`, 2015.

[15] J. Sterling and D. Morrison. Syntax and Semantics of Abstract Binding Trees. 2015.