Slide 1

Specification and Verification of a Formal System for Non-mutual Structural Recursion

Andreas Abel

December 17, 1999

Slide 2

Terms

$s, t, \vec{t}$	$::=$	x, $\lambda x.t$, $\mathrm{fun}\, g(x) = t$, $t\, s$,	*function space*	$\sigma \to \tau$
		$\mathrm{in}_j(t)$, $\mathrm{case}(t, \vec{x.t})$,	*coproduct*	$\Sigma\vec{\sigma}$
		$(\vec{t})$, $\mathrm{pi}_j(t)$,	*product*	$\Pi\vec{\sigma}$
		$\mathrm{fold}(t)$, $\mathrm{unfold}(t)$	*inductive type*	$\mu X.\sigma$

$$\sigma(\mu X.\sigma(X)) \underset{\text{unfold}}{\overset{\text{fold}}{\rightleftarrows}} \mu X.\sigma(X)$$

Named function introduction:

$$\frac{t \in \mathrm{Tm}^{\tau}[\Gamma, x^{\Pi\vec{\sigma}}, g^{\Pi\vec{\sigma}\to\tau}] \qquad \vdash g(x)\ \mathrm{sr}\ t}{\mathrm{fun}\, g^{\Pi\vec{\sigma}\to\tau}(x^{\Pi\vec{\sigma}}) = t \in \mathrm{Tm}^{\Pi\vec{\sigma}\to\tau}[\Gamma]}$$

Slide 3

Dependencies

$$\Delta = \{y \ R \ t\} \qquad \text{where } y \in \mathrm{TmVar}^{\sigma}, t \in \mathrm{Tm}^{\tau}, R \in \{<^{\mathrm{Tm}}_{\sigma,\tau}, \leq^{\mathrm{Tm}}_{\sigma,\tau}\}$$

Judgements

$\Delta \vdash s \ R \ t$	$R \in \{<^{\mathrm{Tm}}, \leq^{\mathrm{Tm}}\}$	*structural ordering*
$\Delta \vdash (\vec{s}) \prec_{\pi} t$		*lexicographic ordering*
$\Delta \vdash g(x) \ \mathrm{sr} \ t$		g *structural recursive in* t

Slide 4

Structural Ordering

Right hand side rules ($R \in \{<^{\mathrm{Tm}}, \leq^{\mathrm{Tm}}\}$):

$$(\mathrm{RcaseR}) \quad \frac{\Delta, x_i \leq^{\mathrm{Tm}} s \vdash s_i \ R \ t \quad \text{for } i = 1, \ldots, n}{\Delta \vdash \mathrm{case}(s, \vec{x.s}) \ R \ t}$$

$$(\mathrm{RpiR}) \quad \frac{\Delta \vdash s \ R \ t}{\Delta \vdash \mathrm{pi}_j(s) \ R \ t}$$

$$(\mathrm{RappR}) \quad \frac{\Delta \vdash s \ R \ t}{\Delta \vdash s \ a \ R \ t} \qquad (\mathrm{RunfR}) \quad \frac{\Delta \vdash s \leq^{\mathrm{Tm}} t}{\Delta \vdash \mathrm{unfold}(s) \ R \ t}$$

Slide 5

Left hand side rules ($R \in \{<^{\mathrm{Tm}}, \leq^{\mathrm{Tm}}\}$):

$$(\text{RcaseL}) \quad \frac{\Delta, x_i \leq^{\mathrm{Tm}} t, y\ R\ t_i, \Delta' \vdash p \text{ for } i=1,...,n}{\Delta, y\ R\ \mathrm{case}(t, \vec{x.t}), \Delta' \vdash p}$$

$$(\text{RpiL}) \quad \frac{\Delta, y\ R\ t, \Delta' \vdash p}{\Delta, y\ R\ \mathrm{pi}_j(t), \Delta' \vdash p}$$

$$(\text{RappL}) \quad \frac{\Delta, y\ R\ s, \Delta' \vdash p}{\Delta, y\ R\ s\ a, \Delta' \vdash p} \qquad (\text{RunfL}) \quad \frac{\Delta, y <^{\mathrm{Tm}} t, \Delta' \vdash p}{\Delta, y\ R\ \mathrm{unfold}(t), \Delta' \vdash p}$$

Slide 6

Reflexivity and transitivity:

$$(\leq^{\mathrm{Tm}}\text{refl}) \quad \frac{}{\Delta \vdash t \leq^{\mathrm{Tm}} t}$$

$$(<^{\mathrm{Tm}}\text{transL}) \quad \frac{\Delta \vdash s\ R\ t \qquad y <^{\mathrm{Tm}} s \in \Delta \qquad R \in \{<^{\mathrm{Tm}}, \leq^{\mathrm{Tm}}\}}{\Delta \vdash y <^{\mathrm{Tm}} t}$$

$$(<^{\mathrm{Tm}}\text{transR}) \quad \frac{\Delta \vdash s <^{\mathrm{Tm}} t \qquad y\ R\ s \in \Delta \qquad R \in \{<^{\mathrm{Tm}}, \leq^{\mathrm{Tm}}\}}{\Delta \vdash y <^{\mathrm{Tm}} t}$$

$$(\leq^{\mathrm{Tm}}\text{trans}) \quad \frac{\Delta \vdash s\ R\ t \qquad y\ S\ s \in \Delta \qquad R, S \in \{<^{\mathrm{Tm}}, \leq^{\mathrm{Tm}}\}}{\Delta \vdash y \leq^{\mathrm{Tm}} t}$$

Slide 7

Lexicographic Ordering

$$(\text{lex}<^{\text{Tm}}) \quad \frac{\Delta \vdash s_{\pi(k)} <^{\text{Tm}} \text{pi}_{\pi(k)}(t)}{\Delta \vdash^{k} (\vec{s}) \prec_{\pi}^{\text{Tm}} t}$$

$$(\text{lex}\leq^{\text{Tm}}) \quad \frac{\Delta \vdash s_{\pi(k)} \leq^{\text{Tm}} \text{pi}_{\pi(k)}(t) \qquad \Delta \vdash^{k+1} (\vec{s}) \prec_{\pi}^{\text{Tm}} t}{\Delta \vdash^{k} (\vec{s}) \prec_{\pi}^{\text{Tm}} t}$$

$$\Delta \vdash (\vec{s}) \prec_{\pi}^{\text{Tm}} t \quad :\Longleftrightarrow \quad \Delta \vdash^{1} (\vec{s}) \prec_{\pi}^{\text{Tm}} t$$

Slide 8

Structural Recursion

$$(\text{srvar}) \quad \frac{y \neq g}{\Delta \vdash \text{sr } y} \qquad (\text{srin}) \quad \frac{\Delta \vdash \text{sr } t}{\Delta \vdash \text{sr } \text{in}_j(t)}$$

$$(\text{srcase}) \quad \frac{\Delta \vdash \text{sr } s \qquad \Delta, x_i \leq^{\text{Tm}} s \vdash \text{sr } t_i \quad \text{for } i = 1, \ldots, |\vec{t}|}{\Delta \vdash \text{sr } \text{case}(s, \vec{x.t})}$$

$$(\text{srtup}) \quad \frac{\Delta \vdash \text{sr } t_i \quad \text{for } i = 1, \ldots, |\vec{t}|}{\Delta \vdash \text{sr } (\vec{t})} \qquad (\text{srpi}) \quad \frac{\Delta \vdash \text{sr } t}{\Delta \vdash \text{sr } \text{pi}_j(t)}$$

$$(\text{srlam}) \quad \frac{\Delta \vdash \text{sr } t \qquad y \neq x}{\Delta \vdash \text{sr } \lambda y.\, t} \qquad (\text{srapp}) \quad \frac{\Delta \vdash \text{sr } t \qquad \Delta \vdash \text{sr } s}{\Delta \vdash \text{sr } t\, s}$$

$$(\text{srapprec}) \quad \frac{\Delta \vdash \text{sr } (\vec{a}) \qquad \Delta \vdash (\vec{a}) \prec_{\pi}^{\text{Tm}} x}{\Delta \vdash \text{sr } g(\vec{a})}$$

Slide 9

Values

$$v, \vec{v} ::= \mathrm{in}_j(v), (\vec{v}), \mathrm{fold}(v), \lambda x.t, \mathrm{fun}\, g(x) = t$$

Operational Semantics

$$\text{(opvar)}\quad \frac{}{\langle x; e, x = v\rangle \downarrow v} \qquad \text{(opin)}\quad \frac{\langle t; e\rangle \downarrow v}{\langle \mathrm{in}_j(t); e\rangle \downarrow \mathrm{in}_j(v)}$$

$$\text{(opcase)}\quad \frac{\langle t; e\rangle \downarrow \mathrm{in}_j(w) \qquad \langle t_j; e, x_j = w\rangle \downarrow v^{\tau}}{\langle \mathrm{case}(t, \overrightarrow{x.t}); e\rangle \downarrow v}$$

$$\text{(optup)}\quad \frac{\langle t_i; e\rangle \downarrow v_i \ \text{for } 1 \le i \le n}{\langle (\vec{t}); e\rangle \downarrow (\vec{v})} \qquad \text{(oppi)}\quad \frac{\langle t; e\rangle \downarrow (\vec{v})}{\langle \mathrm{pi}_j(t); e\rangle \downarrow v_j}$$

$$\text{(opfold)}\quad \frac{\langle t; e\rangle \downarrow v}{\langle \mathrm{fold}(t); e\rangle \downarrow \mathrm{fold}(v)} \qquad \text{(opunfold)}\quad \frac{\langle t; e\rangle \downarrow \mathrm{fold}(v)}{\langle \mathrm{unfold}(t); e\rangle \downarrow v}$$

Slide 10

$$\text{(opapp)}\quad \frac{\langle t; e\rangle \downarrow f \qquad \langle s; e\rangle \downarrow u \qquad f@u \downarrow v}{\langle t\, s; e\rangle \downarrow v}$$

$$\text{(oplam)}\quad \frac{}{\langle \lambda x.t; e\rangle \downarrow \langle \lambda x.t; e\rangle} \qquad \text{(opappvl)}\quad \frac{\langle t; e, x = u\rangle \downarrow v}{\langle \lambda x.t; e\rangle @u \downarrow v}$$

$$\text{(oprec)}\quad \frac{}{\langle \mathrm{fun}\, g(x) = t; e\rangle \downarrow \langle \mathrm{fun}\, g(x) = t; e\rangle}$$

$$\text{(opappvr)}\quad \frac{\langle t; e, g = \langle \mathrm{fun}\, g(x) = t; e\rangle, x = u\rangle \downarrow v}{\langle \mathrm{fun}\, g(x) = t; e\rangle @u \downarrow v}$$

Good Values

$$f \in \mathrm{VAL}^{\sigma\to\tau} \iff \forall u \in \mathrm{VAL}^{\sigma}.\ \exists v \in \mathrm{VAL}^{\tau}.\ f@u \downarrow v$$

Strong Evaluation

Slide 11

$$\begin{aligned} f@u \Downarrow v \quad &:\iff \quad f@u \downarrow v \text{ and } v \in \mathrm{VAL} \\ \langle t; e\rangle \Downarrow v \quad &:\iff \quad \langle t; e\rangle \downarrow v \text{ and } v \in \mathrm{VAL} \text{ and} \\ & \qquad \langle t'; e'\rangle \Downarrow \text{ for every subclosure } \langle t'; e'\rangle \end{aligned}$$

Structural Ordering on Values

Slide 12

(≤refl) $\dfrac{}{v \le v}$

(Rin) $\dfrac{v \mathrel{R} w}{v \mathrel{R} \mathrm{in}_j(w)}$

(Rtup) $\dfrac{v \mathrel{R} w_j \text{ for some } j \in \{1 \dots |\vec{w}|\}}{v \mathrel{R} (\vec{w})}$

(Rarr) $\dfrac{f@u \Downarrow w \qquad v \mathrel{R} w}{v \mathrel{R} f}$

(Rfold) $\dfrac{v \le w}{v \mathrel{R} \mathrm{fold}(w)}$

(lex<) $\dfrac{v_{\pi(k)} < w_{\pi(k)}}{(\vec{v}) \prec^k_\pi (\vec{w})}$

(lex≤) $\dfrac{v_{\pi(k)} \le w_{\pi(k)} \qquad (\vec{v}) \prec^{k+1}_\pi (\vec{w})}{(\vec{v}) \prec^k_\pi (\vec{w})}$

Slide 13

Interpretation of the Structural Ordering

$$\begin{array}{lll} e \models^{\mathrm{wk}} s\ \mathsf{R}^{\mathrm{Tm}}\ t & :\Longleftrightarrow & \langle s; e\rangle \Downarrow v \to \langle t; e\rangle \Downarrow w \to v\ \mathsf{R}\ w \\ e \models s\ \mathsf{R}^{\mathrm{Tm}}\ t & :\Longleftrightarrow & \langle s; e\rangle \Downarrow v\ \&\ \langle t; e\rangle \Downarrow w\ \&\ v\ \mathsf{R}\ w \\ e \models \Delta & :\Longleftrightarrow & \forall p \in \Delta.\ e \models p \end{array}$$

Soundness of the Structural Ordering

$$\frac{\Delta \vdash s\ \mathsf{R}^{\mathrm{Tm}}\ t}{\forall e \models \Delta.\ e \models^{\mathrm{wk}} s\ \mathsf{R}^{\mathrm{Tm}}\ t}\ \mathsf{R} \in \{<^{\mathrm{Tm}}, \leq^{\mathrm{Tm}}, \prec^{\mathrm{Tm}}\}$$

Slide 14

Soundness of Structural Recursion

$$f_0 \equiv \langle \mathrm{fun}\ g(x) = t_0; e_0\rangle \in \mathrm{VAL}$$

We can assume (by wellfoundedness of VAL)

$$\forall w \prec v_0.\ f_0 @ w \Downarrow$$

Lemma.

$$\frac{\Delta \vdash \mathrm{sr}\ \ t \qquad e \models \Delta \qquad \langle g; e\rangle \downarrow f_0 \qquad \langle x; e\rangle \Downarrow v_0}{\langle t; e\rangle \Downarrow}$$