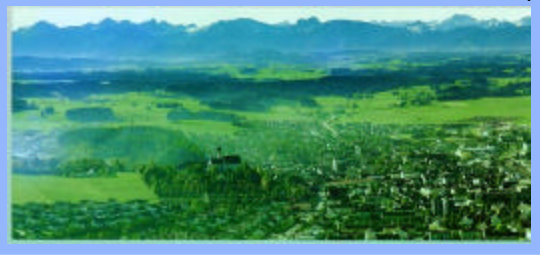
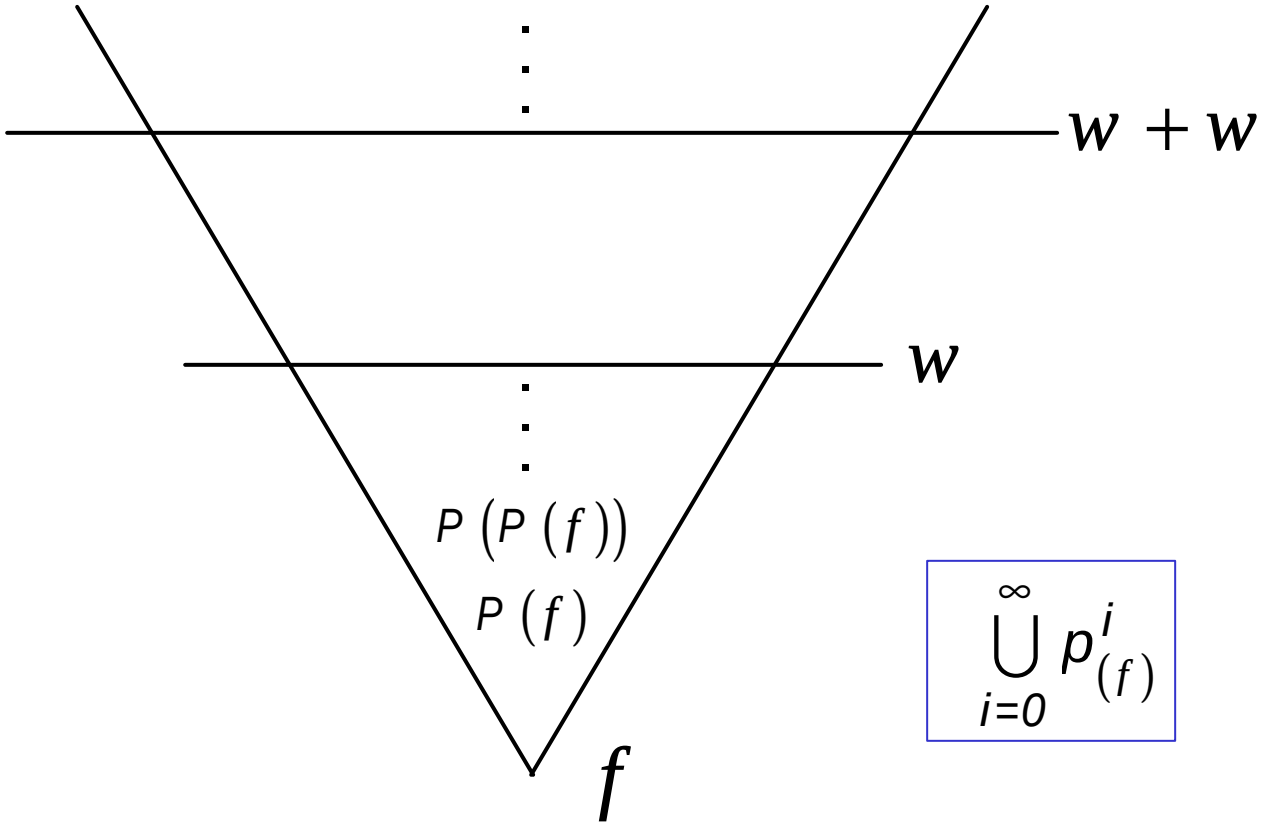
Lecture 2

Set Theoretic Semantics for Type Theory

Marktoberdorf Summer School, 2003



The Cumulative Hierarchy of Sets



Captures the intuition of collecting stages and co-finality… unending stages.

Zermelo Fraenkel Set Theory (ZF)

ZF can be axiomatized in 1st order logic by axioms, 2 axiom schemas (separation, replacement). Axiom of choice is a 9th axiom.

The hierarchy is defined as:

$$Z_0 = f$$

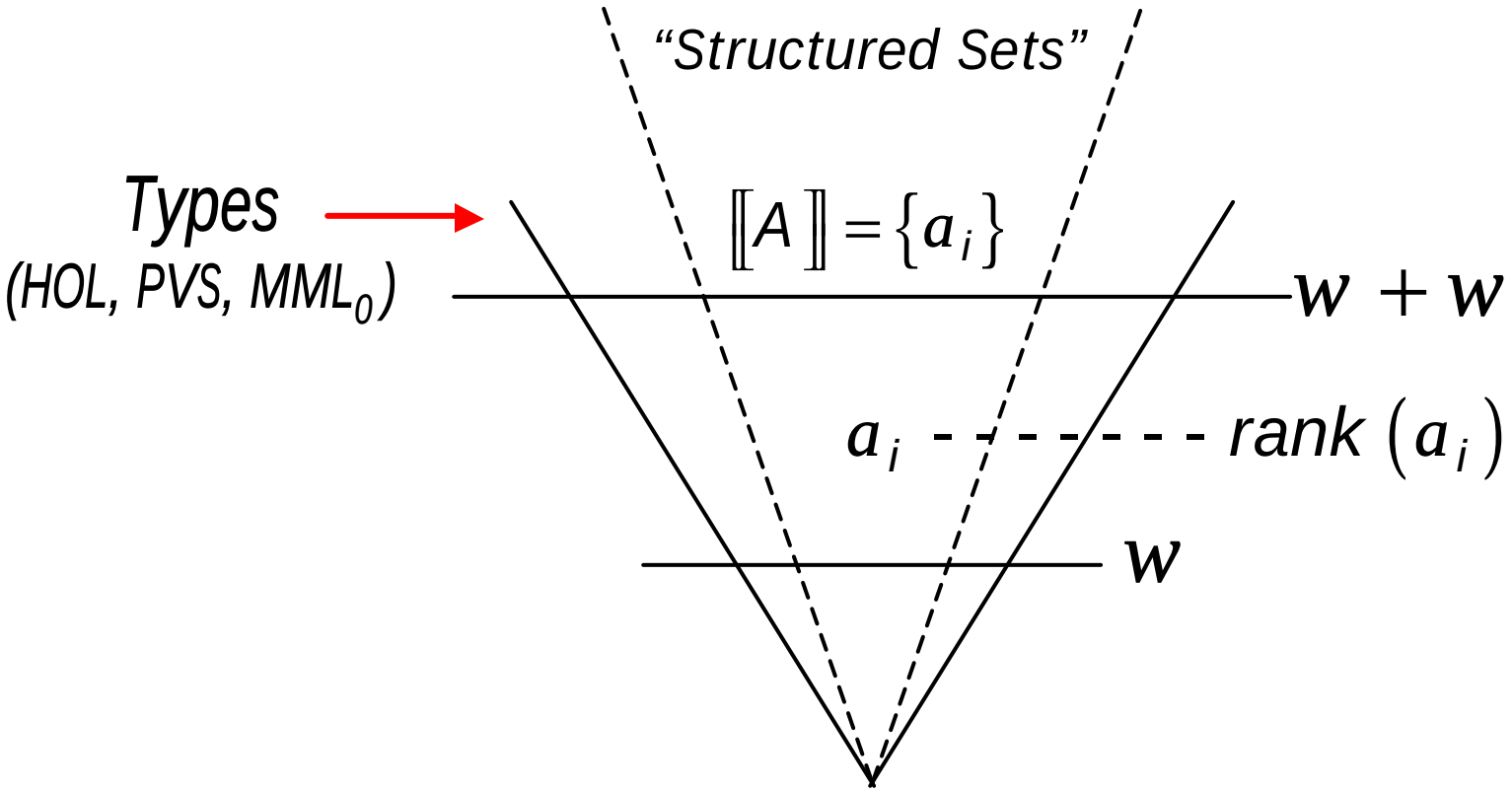
$$Z_a = \bigcup_{b<a} Z_b$$

$$Z_{a+1} = P(Z_a)$$

$$Z = \bigcup_{a \in Ord} Z_a$$

Every ZF set x is in some Z_α; its rank is the least such ordinal α.

Review of Set Theoretic Semantics



The Cumulative Hierarchy of Sets

Goal of Howe's Approach

Pure Type Theory

$$\frac{a_1, a_2, \ldots, a_i \ldots \quad f\ (a) \quad f \Downarrow \lambda x.b \quad p \Downarrow < a, b >}{\lambda x.b \quad < a, b > \quad c_i\left(\overline{a}\right) \quad \mathbb{U}_i}$$

enlarge

Type Theory with Set Terms

$$\frac{a_1, a_2, \ldots, a_i \ldots \quad a_1, a_2, \ldots, a_i \ldots \quad A \quad \hat{g}_A \quad f\ (a) \quad \hat{j}\left(\hat{a}\right) \quad f \Downarrow \lambda x.b \quad f \Downarrow \hat{j} \quad c_i\left(\overline{a}\right) \Downarrow c_i\left(\overline{a}\right)}{\lambda x.b \quad a \mapsto b \quad < a, b > \quad < \hat{a}, \hat{b} > \quad c_i\left(\overline{a}\right) \quad c_i\left(\hat{a}\right)}$$

Howe's Meaning Functions

Howe's Approach to Set-theoretic Semantics:

Like Pitts, Dybjer, Troelstra and other, Doug Howe maps types into sets; for A, a type,

$$[\![A]\!] \text{ is a set.}$$

However, he introduces new ideas to handle functionality, polymorphism, subtyping, quotient types, and types as objects (universes). For instance,

$[\![\lambda x.x]\!]_{A \to A}$ is an element j of $[\![A \to A]\!]$

and he writes that $j \lhd \lambda x.x$.

Limitations of Set Embedding

Unlike with PVS and HOL, no embedding can cover all of Nuprl because

- Recursive types allow $T = (T \to \mathbb{B}) \to \mathbb{B}$
- Domains all absolutely unsolvable problems

But Howe gets a very substantial part and Moran extends to more. This raises the issue of sub-theories of domains and recursive types.

Goal of Howe's Approach

- Extend the family of "structured sets"
- Create constants for all "structured sets"
- Extend evaluation to all terms
- Define approximation (covering)

$$a_i \lhd a_i$$

to relate sets a_i to terms a_i

Howe's Method

1. Encode type terms and types into sets in the cumulative hierarchy W

$$\begin{array}{ll} < ty , g > & g \\ < fn , j > & j \\ < c_i < a_1 , \ldots , a_n >> & c_i \left(\overline{a} \right) \end{array}$$

2. Define a subset of W with a unique meaning property; call it V.

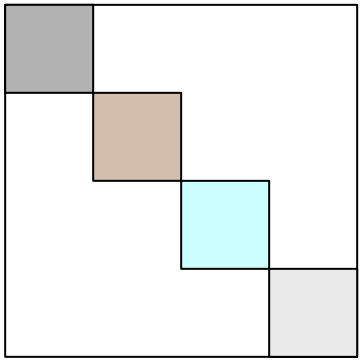
3. Define a term model for all V sets; call it T_0.

4. Define evaluation and approximation on T_0; this provides a computational type theory with set oracles.

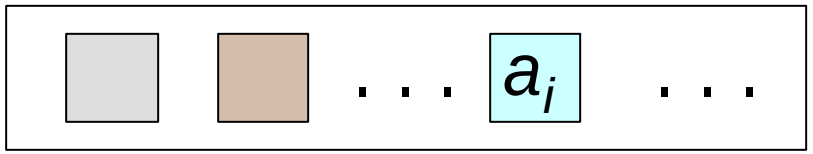
I present a variant used by Evan Moran to extend Howe's results.

Howe's Semantics

We think of types as collections of equivalence classes of terms:



or



We need to allow sets representing equivalence classes a_i into types

$a_1, a_2, \ldots, a_n$ written $g\{a_1, a_2, \ldots, a_n\}$

where a_i covers a_i (a_i approximates a_i) $a_i \lhd a_i$

Disjointness and Incompatibility

The equivalence classes are disjoint, of course.

$$A = \boxed{a_1 \quad a_2 \quad \ldots \quad a_i \quad \ldots}$$

if $a_i \cap a_j \neq 0$ then

$$a_i = a_j$$

The set elements must also be incompatible:

$$g_A = \{a_1, a_2, \ldots, a_i\}$$

$con(a_i, a_j)$ implies $a_i = a_j$

For each $a_i \in A$ there will be a unique $a_i \in g_A$, $a_i \lhd a_i$.

Disjointness and Incompatibility

The key condition for functions is:

j $\quad \boxed{< a_1, b_1 >, < a_2, b_2 >, \ldots, < a_i, b_i >, \ldots}$

j' $\quad \boxed{< a'_1, b'_1 >, < a'_2, b'_2 >, \ldots, < a'_i, b'_i >, \ldots}$

If for all $< a, b >, < a', b' >$

$con(a_i, a'_i)$ implies $con(b_i, b'_i)$

then

$con(j, j')$

Compatibility (Consistency) **Examples**

- $0 \mapsto 0$ and $1 \mapsto 1$ are compatible (consistent) since $j\,\{<0,0>\}$ and $j\,\{<1,1>\}$ have a non-empty intersection, $j\,\{<0,0>,<1,1>\}$.

- $0 \mapsto (0 \mapsto 0)$ and $0 \mapsto (1 \mapsto 1)$ are compatible, i.e. $j\,\{<0, j\,\{<0,0>\}>\}$ *con* $j\,\{<0, j\,\{<1,1>\}>\}$ since 0 *con* 0 and $j\,\{<0,0>\}$ *con* $j\,\{<1,1>\}$.

Membership and Approximation

If the type A is interpreted as the set g_A, then for each $a \in A$, there is a unique α such that

$$\alpha \lhd a.$$

We will say $[\![A]\!] = g_A$ and $[\![a]\!]_A = \alpha$.

Uniqueness Theorem

For any term t *in* T_0,

1. *If* $g_1 \lhd t$ *and* $g_2 \lhd t$, *then* $g_1 = g_2$
2. *For all* $g \in V$ *and* $a_1, a_2 \in g$,

   if $a_1 \lhd t$ *and* $a_2 \lhd t$, *then* $a_1 = a_2$

The Term Language T_0

Howe defines a term language, T_0, that includes the Nuprl terms with binding, such as

$$x : A \to B,\ x : A \times B,\ l\, x.b,\ x : A \cap B,$$
$$less\,(n;m;a;b),\ decide\,(p;x.a;y.b),\ \ldots$$

T_0 includes the constructors and constants, such as

$$\mathbb{U}_i,\ nat\,\{n\},\ pair\,(a;b),\ inl\,(a),\ inr\,(b),\ ap\,(f;a),\ \ldots$$

T_0 includes constants for all of the g, j, x, $c_i\,(\overline{a})$ sets. Howe uses $\hat{g}$, $\hat{j}$, $\hat{x}$ to denote the set terms.

The Term Language T_0

Howe extends the evaluation relation to all terms, for example:

$$ap\,(\lambda x.b\,;a) \Downarrow c \quad \textit{if} \quad b\,[a\,/\,x] \Downarrow c$$

$$less\,(0;1;a\,;b) \Downarrow c \quad \textit{if} \quad a \Downarrow c$$

For instance, $ap\left(\lambda x.x\,;\hat{j}\right) \Downarrow \hat{j}$.

Evaluation Rules

$$\frac{f \Downarrow \hat{f} \quad (a, b) ? f \quad a \triangleleft a}{f\ (a) \Downarrow \hat{b}}\,(ap_f) \qquad \frac{f \Downarrow \lambda x.b \quad b\,[a / x] \Downarrow v}{f\ (a) \Downarrow v}\,(ap_\lambda)$$

$$\frac{}{\hat{g} \Downarrow \hat{g}} \qquad \frac{}{\lambda x.b \Downarrow \lambda x.b} \qquad \frac{}{c_i\,(\overline{a}) \Downarrow c_i\,(\overline{a})}$$

Approximation Rules

$$\frac{e \Downarrow v \quad a \lhd v}{a \lhd e} \qquad \frac{?j \quad a_j \lhd a_j}{c_i\left(\hat{a}_1, \ldots, \hat{a}_n\right) \lhd c_i\left(\hat{a}_1, \ldots, \hat{a}_n\right)}$$

$$\frac{?(a, b) ? f \quad b \lhd b\left[\hat{a} / x\right]}{f \lhd \lambda x . b}^{\dagger}$$

† Howe does not use this rule because it is unproven when the non-determinism of functions on quotient types is allowed.

Examples

Let $j = \{<0,4>,<1,5>\}$ $j' = \{<0,2>\}$

$y = \{<j,17>,<j',18>\}$

$\hat{j}(0+0) \Downarrow 4$ because $0 \lhd 0+0$

$\hat{j} \lhd l\,x.x + 4$ but not $\hat{j}' \lhd l\,x.x + 4$

$\hat{y}(l\,x.x + 4) \Downarrow 17$

The Substitution Lemma

If $a \lhd a$ then for any term e,

$b \lhd e\left[a / x\right]$ implies $b \lhd e\left[a / x\right]$

The intuition is that for any demonstration of $b \lhd e\left[a / x\right]$, if it does not examine a, then it also establishes $b \lhd e\left[a / x\right]$.

If the derivation depends on a, then since $a \lhd a$ and a is a term, there is more information in a than in any approximation a, and that information will establish the facts used about a to show $b \lhd e\left[a / x\right]$ using a in place of a.

See Working Material, Lemma 2.4, p. 25.

Rationale for the Substitution Lemma

Assume $a \lhd a$ and $b \lhd e\left[\hat{a} \,/\, x\right]$

To say $b \lhd e\left[\hat{a} \,/\, x\right]$ means $a \mapsto b \lhd l\, x.e$.

Thus, $l\, x.e \;?\; g\{a \mapsto b\}$, a singleton set, and

(1) $l\, x.e \in g\{a\} \to g\{b\}$

(2) From $a \lhd a$ we know $a \;?\; g\{a\}$

From (1) and (2) we have $(l\, x.e)a \;?\; g\{b\}$,

thus, $e\left[a \,/\, x\right] ?\; g\{b\}$, and hence

$$b \lhd e\left[a \,/\, x\right].$$

Interpreting Sequents

Given a sequent $x_1 : A_1, \ldots, x_n : A_n \vdash g \ ? \ G$,
a closing substitution cl for it is a sequence of closed terms

$$a_1, \ldots, a_n \quad \text{for} \quad x_1, \ldots, x_n .$$

The x_i are the only free variables in g and G.

The sequent is true *iff* $[\![cl\,(g)]\!]_{cl\,(G)}$ is defined and belongs to $[\![cl\,(G)]\!]$ for all closing substitutions cl such that

$$[\![cl\,(x_i)]\!]_{cl\,(A_i)} \ ? \ [\![cl\,(A_i)]\!] .$$

Interpreting Rules

Given sequents $s, s_1, \ldots, s_k$, the rule

$$\frac{s_1, \ldots, s_k}{s}$$

is sound if the conclusion s is true whenever the premises s_i are true.

Soundness of Core Nuprl in Howe's Semantics

The function elimination rule – no hypotheses case:

$$\frac{\vdash a \ ?\ A \qquad \vdash f \ ?\ (x : A \rightarrow B)}{\vdash f\ (a)\ ?\ B\left[a / x\right]}$$

Soundness – the Meaning of $x : A \to B$

Recall from the Working Material:

$[\![x : A \to B]\!]$ is the set of functions j with domain $[\![A]\!]$ such that for all $< a , b >? j$, $b \; ? \; [\![B [a / x]]\!] = g_a$.

Soundness of Function Elimination – the Premises

The premise $\vdash a \ ? \ A$ is true in Howe's model provided

$$[\![A]\!] = g \quad \text{and} \quad [\![a]\!]_A = a \quad \text{and} \quad a \ ? \ g \, .$$

The premise $f \ ? \ (x : A \to B)$ is true if

$$[\![f]\!]_{x:A \to B} = j_f \quad \text{is in} \quad [\![x : A \to B]\!] .$$

Soundness of Function Elimination – the Conclusion

We need to know that $[\![f\ (a)]\!]_{B[a\ /\ x]}$ is defined, i.e.

there is a b in $[\![B\ [a\ /\ x]]\!]$

$$b \lhd [\![f\ (a)]\!].$$

We know that for any $< a\ ,\ b\ > \in j_f$, $b \in [\![B\ [\widehat{a}\ /\ x]]\!]$, by the premise for f .

To say $[\![a]\!]_A = a$ means $a \lhd a$. (Recall "Membership and Approximation.")

Soundness of Function Elimination – the Conclusion

By the Substitution Lemma,

$$\text{if } g \lhd B\left[\hat{a} \,/\, x\right], \text{ then } g_a \lhd B\left[a \,/\, x\right],$$

$$\text{thus, } g = \left[\!\left[B\left[\hat{a} \,/\, x\right]\right]\!\right] = \left[\!\left[B\left[a \,/\, x\right]\right]\!\right].$$

Likewise, if $b \lhd f\left(\hat{a}\right)$ then $b \lhd f\left(a\right)$.

But by the Substitution Lemma, we know $b \lhd f\left(\hat{a}\right)$, since $j_f \lhd f$ and $b \lhd j_f\left(\hat{a}\right)$.

Hence $\left[\!\left[f\left(a\right)\right]\!\right]_{B\left[a \,/\, x\right]}$? $\left[\!\left[B\left[a \,/\, x\right]\right]\!\right]$ as required.