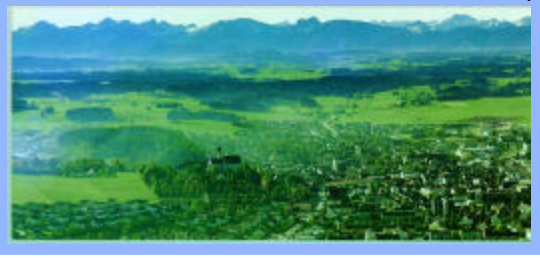
Lecture 3

Relationships Between Sets and Types

Marktoberdorf Summer School, 2003



From ITT (M-L 82) to CTT (Nuprl 2000)

1.	subset types	$\{x : A \mid B\}$	1983	Math
2.	quotient types	$A // E$	1983	Math
3.	direct computation	$\sim$	1986	Proving
4.	general recursion	y	1986	Programming
5.	recursive types	$\mu x.T$	1986	Data types
6.	intersection	$A \cap B$	1987	Logic
7.	partial objects	$\bar{A}$	1992	Prog languages
8.	union	$A \cup B$	1995	Symmetry 6
9.	top	Top	1996	Symmetry 6
10.	subtyping	$\sqsubseteq$	1996	Classes

CS – Math

CS

abstraction

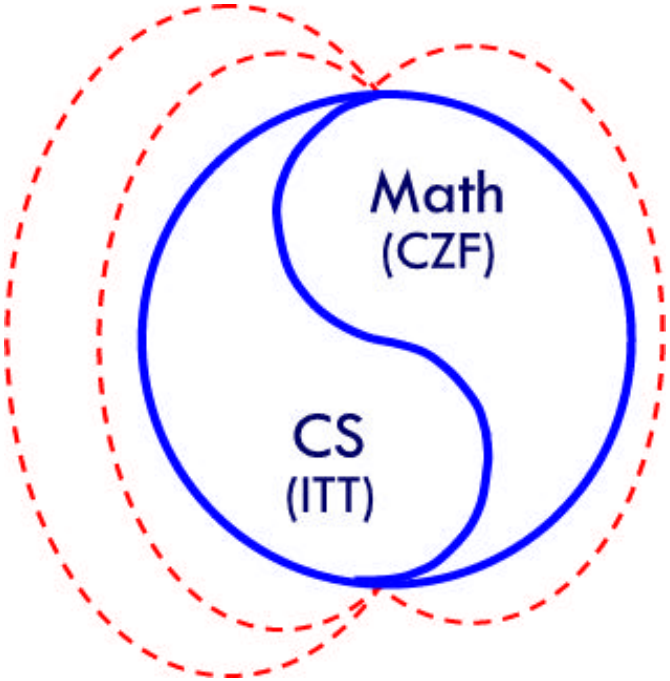
computability

formalism

modularity

classes

theories



Math

abstraction

constructivity

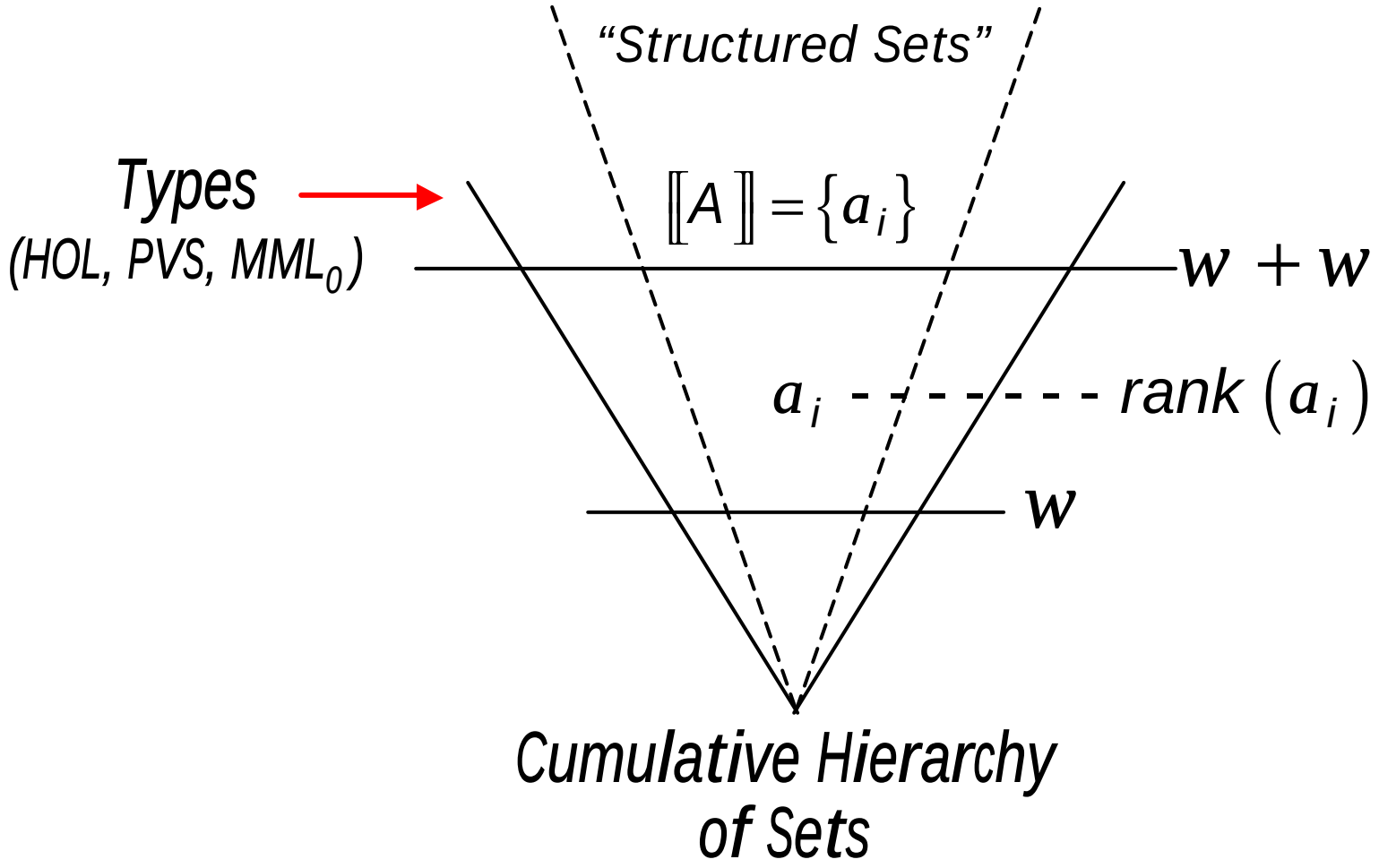
formalism

modularity

categories

theories

Review of Set Theoretic Semantics



Goal of Howe's Approach

Pure Type Theory

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

Type Theory with Set Terms

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

Issues with ML-82, Alf, and Nuprl Type Theories

1. The computation system is untyped; terms are polymorphic.

$\lambda x.x \;?\; A \to A$ for any A including void

$\lambda x.1 \;?\; \mathbb{Z} \to \mathbb{Z}$

$\lambda x.1 \;?\; \mathbb{N} \to \mathbb{N}$

$<0,1> \;?\; \mathbb{N} \times \mathbb{N}$

$<0,1> \;?\; \mathbb{N} \times \mathbb{Z}$

Issues with ML-82, Alf, and Nuprl Type Theories

2. Sequent hypotheses are dependent, and sequents assert functionality.

$$x_1 : A_1, x_2 : A_2(x_1) \vdash G(x_1, x_2)\ ext\ \ g(x_1, x_2)$$

Notice, A_1 is assumed to be a type, and $A_2(a)$ is assumed to be a type for all $a \in A_1$, and the sequent asserts that $G(a_1, a_2)$ is a type for all $a_1 \in A, a_2 \in A_2(a_1)$ and $g(a_1, a_2) \in G(a_1, a_2)$. Moreover, g is a function respecting equality on A_1, A_2.

It would seem that

$$x_2 : A_2(x_1), x_1 : A_1 \vdash G(x_1, x_2)\ ext\ \ g(x_1, x_2)$$

would not make sense.

Issues with ML-82, Alf, and Nuprl Type Theories

3. There is natural subtyping.

$$\{i : \mathbb{Z} \mid 0 \leq i\} \sqsubseteq \mathbb{Z}$$

$$\{n : \mathbb{N} \mid prime\,(n)\} \sqsubseteq \mathbb{N}$$

$A \sqsubseteq A\ //\ E$ discussed below

Issues with ML-82, Alf, and Nuprl Type Theories

4. Subtyping in general

$$A \sqsubseteq B \quad \textit{iff} \quad a = a' \textit{ in } A \Rightarrow a = a' \textit{ in } B$$

Here are the properties:

$$\frac{A \sqsubseteq A' \qquad B \sqsubseteq B'}{\begin{array}{ll} A \times A' & \sqsubseteq A' \times B' \\ A + B & \sqsubseteq A' + B' \\ A' \to B & \sqsubseteq A \to B' \end{array}}$$

Issues with ML-82, Alf, and Nuprl Type Theories

5. Record subtyping is derived.

   Polymorphic functions and the subtyping relation allow an elegant and natural definition of records and dependent records.

Records using labels

One approach to records is to take labels, L, as indexes into components.

Given	$\{x : A;\ y : B;\ z : C\}$
take	$L = \{x, y, z\},\ L \sqsubseteq Atom$
Define	$Sig : L \rightarrow U_i$ by if $j = x$ then A else if $j = y$ then B else C

Define the record type as $x : L \rightarrow Sig(x)$.

Records as functions

We now take

$$\{x : A;\ y : B;\ z : C\} == x : L \rightarrow Sig(x).$$

for $r ? \{x : A;\ y : B;\ z : C\}$,

let $r.i == r(i)$

so $r.x ? A,\ r.y ? B,\ r.z ? C$

Records extension using labels

Consider $\{x : A;\ y : B;\ z : C;\ w : D\}$.

Is this a subrecord of $\{x : A;\ y : B;\ z : C\}$?

To examine this, let $L' = \{x, y, z, w\}$.

Notice $L \sqsubseteq L'$.

Define $Sig'(i) = \text{if } i = w \text{ then } D \text{ else } Sig(i)$.

Notice $x : L' \to Sig'(x) \sqsubseteq x : L \to Sig(x)$

because $L \sqsubseteq L'$ and $Sig'(x) = Sig(x)$ for $x \in L$.

Record extension depends on function polymorphism

$$x : L' \to Sig'(x) \sqsubseteq x : L \to Sig(x)$$

because any function r' in $x : L' \to Sig'(x)$ is a function in $x : L \to Sig(x)$.

Given inputs from L, x and y, $r'(x) ? Sig'(x)$ and $Sig'(x) = Sig(x)$, $r'(y) ? Sig'(y) = Sig(y)$.

Record subtyping depends on polymorphic functions

Let $R_3 = \{x_1 : A_1;\ x_2 : A_2;\ x_3 : A_3\}$

$R_4 = \{x_1 : A_1; \ldots; x_4 : A_4\}$.

Note $R_4 \sqsubseteq R_3$.

If $r \ ? R_4$, then $r(x_i)$ is defined for

$$x_i \ ? \{x_1, \ldots, x_4\},$$

hence it is defined for $x_i \ ? \{x_1, \ldots, x_3\}$.

Records and variant types

RECORDS

$$\{x : A\} \;=\; \{x\} \to A$$

$$\{x : A; y : B; z : C\} \;==\; \{x : A\} \cap \{y : B\} \cap \{z : C\}$$

VARIANT TYPES

$$\{x \;\; of \;\; A\} \;=\; \{x\} \times A$$

$$(x \;\; of \;\; A \mid y \;\; of \;\; B \mid z \;\; of \;\; C) \;==\; (x \;\; of \;\; A) \cup (y \;\; of \;\; B) \cup (z \;\; of \;\; C)$$

Equalities Differ

6. ML-82, Alf, Nuprl base equality on sets is structural

$$A \times B = A' \times B' \quad iff \quad A = A' \; and \; B = B'$$
$$A \to B = A' \to B' \; iff \quad A = A' \; and \; B = B'$$
$$A + B = A' + B' \quad iff \quad A = A' \; and \; B = B'$$

Set equality is extensional; $g = g' \; iff \; x \in g \; iff \; x \in g'$.

However, we can define extensional type equality

$$A \equiv B \quad iff \quad A \sqsubseteq B \;\; \& \;\; B \sqsubseteq A.$$

Note, function equality is extensional in type theory:

$$f = g \; in \; A \to B \quad iff \quad f(x) = g(x) \text{ for all } x \; ? \; A.$$

Issues with ML-82, Alf, and Nuprl Type Theories

7. Nuprl uses quotient types.

We can define new equalities on a type, say $\mathbb{Z}$, to create a new type.

Let E_k denote the equivalence relation on $\mathbb{Z}$

$$x = y \mod k$$

Let $\mathbb{Z}_k = \mathbb{Z} // E_k$.

For example,

in $\mathbb{Z}_2$ all elements equal one of $0, 1$;

in $\mathbb{Z}_6$ all elements equal one of $0, 1, 2, 3, 4, 5$.

Issues with ML-82, Alf, and Nuprl Type Theories

8. Types are objects in ML-82, Alf, and Nuprl.

$\mathbb{U}_1$ is a universe whose objects are (codes) for types.

$$\frac{A \in \mathbb{U}_i \quad \text{for } x \in A, \quad B \in \mathbb{U}_i}{x : A \times B \in \mathbb{U}_i \qquad x : A \to B \in \mathbb{U}_i} \qquad \frac{F : \mathbb{U}_i \to \mathbb{U}_i \quad \text{monotone}}{\text{mx}.F \in \mathbb{U}_i}$$

$\mathbb{N}, \mathbb{B}, \mathit{void} \in \mathbb{U}_i$ for all i $\quad \mathbb{U}_{i+1} \in \mathbb{U}_i$

Issues with Nuprl Type Theories

9. Some Nuprl theorems contradict classical set theory and classical logic.

   (a) Nuprl can solve this recursion equation on types:

$$T = (T \to \mathbb{B}) \to \mathbb{B}$$

   using $m X . (X \to \mathbb{B}) \to \mathbb{B}$.

   (b) Nuprl's domain theory (bar types) includes this result:

$$\neg \exists h : \overline{\mathbb{N}} \to \mathbb{B}.\ \ ?x : \overline{\mathbb{N}}. \left(h(x) = t \ \ \textit{iff} \ \ x \downarrow\right)$$

Nuprl has Union and Intersection

10. The types $A \cup B$, $\bigcup_{x \in A} B_x$, $A \cap B$, $\bigcap_{x \in A} B_x$, $x : A \cap B$ all violate Howe's construction as outlined.

$$(\{0\} \to \{0\}) \cup (\{1\} \to \{1\})$$

includes $0 \mapsto 0$ and $1 \mapsto 1$ but no

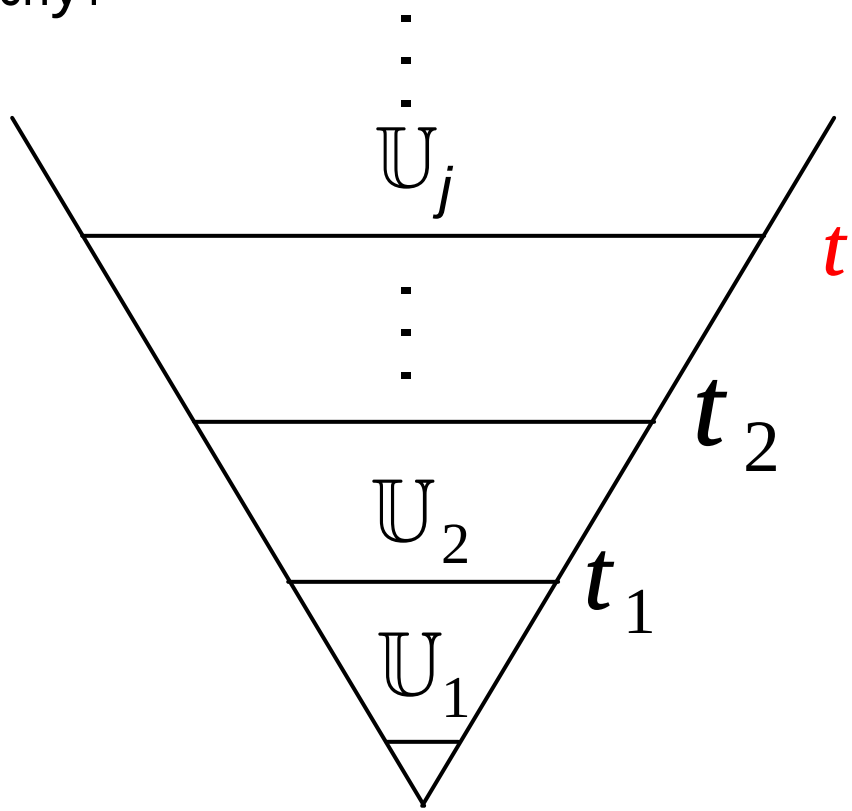
$$a \mapsto b$$

can approximate both.

Extending Set Theoretic Semantics to ML-82, Alf, Nuprl

Can we account for these ideas in set theory?

Can we embed ML-82, Alf, and Nuprl into the cumulative hierarchy?



t_i are inaccessible cardinals

Coping With Issues

1.	Polymorphism	– use $j = j'$
2.	Functionality	– use set equality and uniqueness
3-5.	Subtyping	– follows from polymorphism
6.	Equality	– use extensional equlaity
7.	Quotient types	– introduce limited non-determinism
8.	Universes	– use inaccessible cardinals (reflection)
9.	Non-classical results	– restrict to core Nuprl
10.	Unions, intersections	– consult Evan Moran

Extending Approximation on Functions

Definition For a, b in V, define the following preorder, $a \leq b$, by induction on the rank of a:

1. $g \leq g$.
2. $c_i(a_1, \ldots, a_n) \leq c_i(a_1', \ldots, a_n')$ if $a_j \leq a_j'$ $1 \leq j \leq n$.
3. $f \leq f'$ if for all $< a, b >? f$, there exist $< a', b' >? f'$ such that $a' \leq a$ and $b \leq b'$ (note the contravariance in the first argument).
4. $x \leq x'$ if for all $a' ? x'$ there is $a ? x$ with $a \leq a'$.

Incorporate $\leq$ into $\lhd$ by concluding $a \lhd b$.

Capturing Record Polymorphism in Howe's Model

Consider $\{x : \mathbb{N}; y : \mathbb{N}; z : \mathbb{N}\} \sqsubseteq \{x : \mathbb{N}; y : \mathbb{N}\}$ with $r(x) = 0, r(y) = 1, r(z) = 2.$

Let $y_1 = j\ \{< x, 0 >, < y, 1 >\}$

$y_2 = j\ \{< x, 0 >, < y, 1 >, < z, 2 >\}$

Note $y_1 \leq y_2$, since for each $< a, b >$ in y_1 there is some $a' \leq a$, $b = b'$.

Note, $y_2 \lhd l x.r(x) \in \{x : \mathbb{N}; y : \mathbb{N}; z : \mathbb{N}\}$, and since $y_1 = y_2$, we have $y_1 \lhd l x.r(x)$. Thus, $l x.r(x)\ ?\ \{x : \mathbb{N}; y : \mathbb{N}; z : \mathbb{N}\}$ as well.

Example

If $\hat{j} \in \mathbb{Z}_2 \to \mathbb{B}$ then $\hat{j}$? $\mathbb{Z}_6 \to \mathbb{B}$.

This follows from Approx. Theorem (Thm 2.2).

If $a \leq b$ and $b \lhd \hat{j}$, then $a \lhd \hat{j}$, finding

$$j_1 \text{ ? } \mathbb{Z}_2 \to B, \quad j_2 \text{ ? } \mathbb{Z}_6 \to B$$

where $j_2 = j_1$ and $j_1 = \hat{j}$.

Imagine $\hat{j}$ tests evenness.

Approximation Theorem (Thm 2.2, p.24)

If $a = b$ and $b \lhd e$ then $a \lhd e$

Subtyping Fails Without Approximation

$$\mathbb{Z}_2 \to \mathbb{B} \sqsubseteq \mathbb{Z}_6 \to \mathbb{B}$$

but $j_1 = \{<[0]_2, t>, <[1]_2, f>\}$? $\mathbb{Z}_2 \to \mathbb{B}$ is too small to be in $\mathbb{Z}_6 \to \mathbb{B}$; compare to

$$j_2 =$$

$$\{<[0]_6, t>, <[1]_6, f>, <[2]_6, t>, <[3]_6, f>, <[4]_6, t>, <[5]_6, f>\}$$

$$j_2 \leq j_1 \text{ and } j_1 \leq \hat{j}$$

Comparing Types and Sets

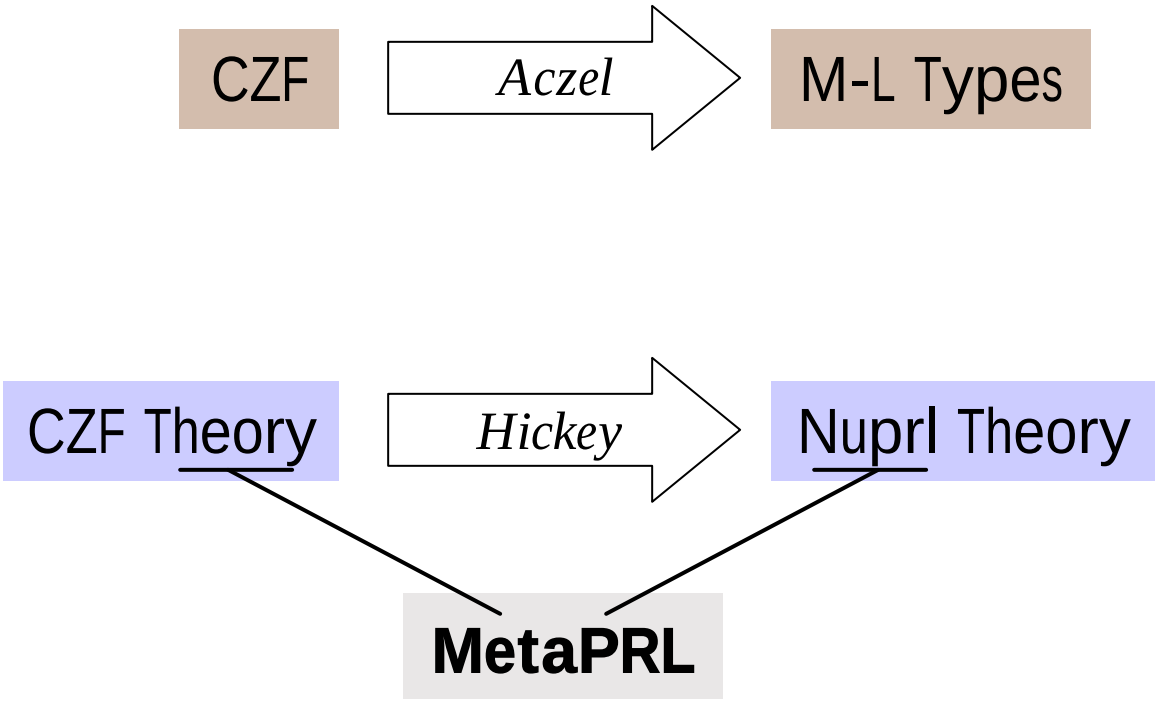
We have seen embeddings of types into "'structured sets." This is one relationship between types and sets, but not the only interesting one.

Peter Aczel showed in 1976 how to treat sets as types by mapping a version of constructive set theory, CZF, into Martin-Löf type theory.

Over the years he extended CZF with inductive definitions and choice principles so that *ZFC = CZF + Choice.* This holds also for CZF with universes (in accessible cardinals), CZF_i.

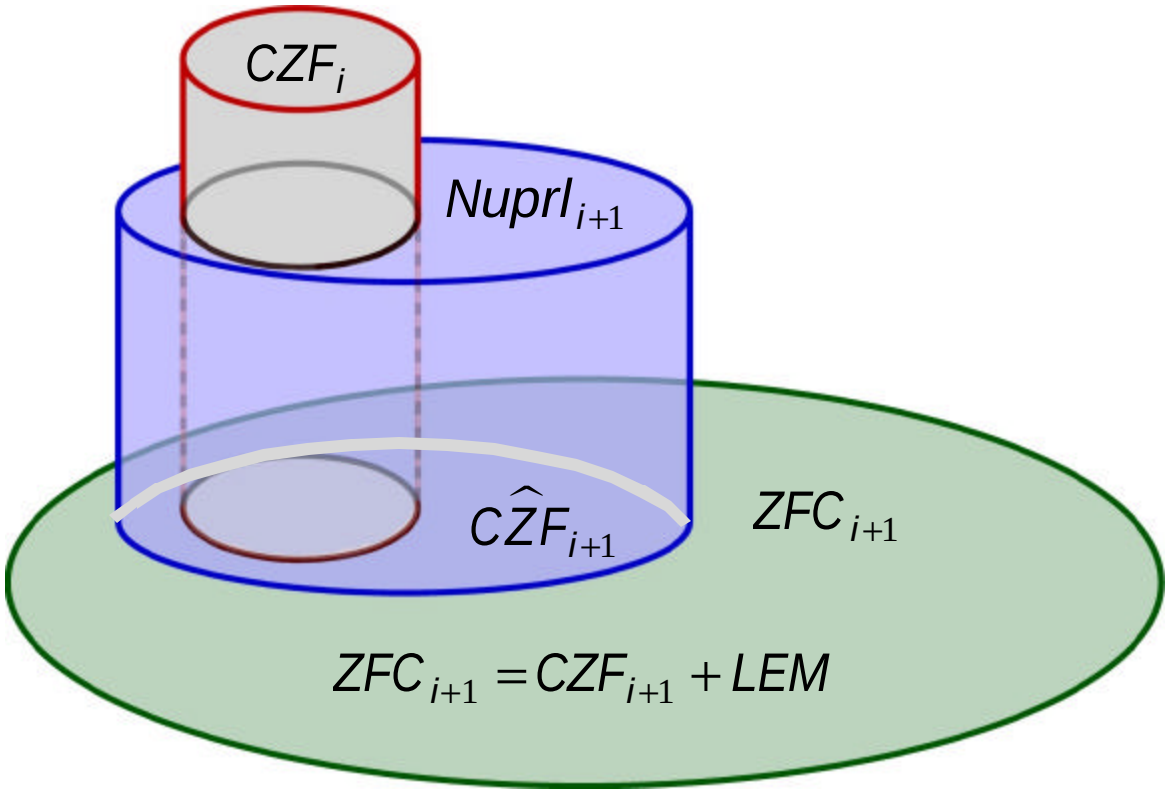
Jason Hickey formalized Aczel's construction in MetaPRL.

Formally Embedding Sets into Types



Interesting Observation

If we combine Howe's result and Aczel's, we get this situation:



How are $C\hat{Z}F_i$ and ZFC_i related?

Theorem (Moran) : $C\hat{Z}F_i \cong ZFC_i$

Aczel's Embedding – 1

Aczel introduces the type Set with Martin-Löf style rules.

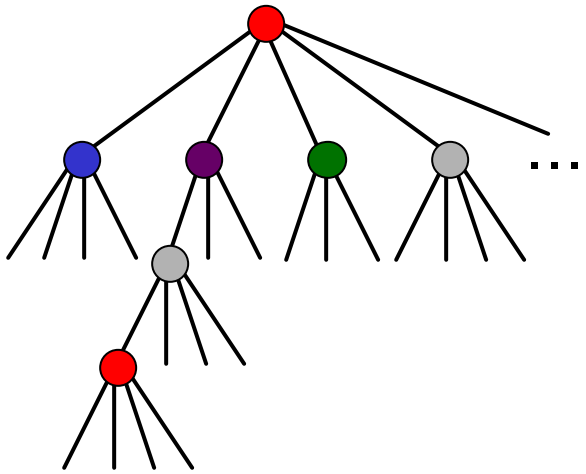
If $A \in \mathbb{U}_1$ and $f(x) \in Set$ for all $x \in A$,
then $\{ f(x) \mid x \in A \} \in Set$.

For example, if $a_1, \ldots, a_n$ are sets for $i \in \mathbb{N}_n$, and $f(i) = a_i$, then $\{f(i) \mid i \in \mathbb{N}_n\}$ is a set.

When $n = 0$, then $\{f(i) \mid i \in \mathbb{N}_n\}$ is the empty set.

Aczel's Embedding – 2

When looked at as types, sets have the form of well-founded trees. They look like Brouwer ordinals.



Relating Models of Sets and Types – 1

The following Nuprl recursive type captures Aczel's model of sets as types:

$$m X . \left(I : \mathbb{U}_1 \times I \rightarrow x \right)$$

Let $u \left[\!\left[m X . \left(I : \mathbb{U}_1 \times I \rightarrow x \right) \right]\!\right]$ be the untagged Howe set model of this type. Call it $\overset{\vee}{AC} Z$.

Relating Models of Sets and Types – 2

We can also translate Aczel's type theory definitions of membership and extensional equality.

$$a \overset{\vee}{e} a' = u \left[\!\left[\hat{a}\ e_A\ \hat{a}' \right]\!\right] \neq f$$

$$a \overset{\vee}{=}_A a' = u \left[\!\left[\hat{a}\ =_A\ \hat{a}' \right]\!\right] \neq f$$

Relating Models of Sets and Types – 3

Let M be the sets below the 1st inaccessible cardinal, the sets in Howe's Z_{t_1}.

In classical first-order logic, L, $\check{ACZ}$ and M are models of ZFC. How are they related?

Moran's Theorem

Theorem : $A\overset{\vee}{C}Z \cong M$, that is, there is a surjective map $i : A\overset{\vee}{C}Z \to M$ such that for all a, a' in $A\overset{\vee}{C}Z$

(a) $a \overset{\vee}{e}_A a' \Leftrightarrow i(a) e\, i(a')$

(b) $a \overset{\vee}{=}_A a' \Leftrightarrow i(a) = i(a')$

Aczel's *CZF* Axioms

Equality

$$x = y \;\; \mathit{iff} \;\; ?z.(z \; ? \; x \Leftrightarrow z \; ? \; y)$$

Set Induction Scheme

$$?y.(?x \; ? \; y.P(x) \Rightarrow P(y)) \Rightarrow ?x.P(x)$$

Pairing

$$?z \; (x \in z \wedge y \in z)$$

Union

$$?z.(\forall y \; ? \; x.\forall u \; ? \; y.u \; ? \; z)$$

Restricted Separation

$$?z.(\forall y \; ? \; z.(y \; ? \; x \wedge P(y)) \wedge \forall y \; ? \; x.(P(y) \Rightarrow y \; ? \; z))$$

Aczel's *CZF* Axioms (cont.)

Strong Collection

$?x\ ?a.\ ?y.\ R(x,y) \Rightarrow ?b.\ R'(a,b)$ where $R'(a,b)$ is

$?x\ ?a.\ ?y\ ?b.\ R(x,y)\ ?\ ?y\ ?b.\ ?x\ ?a.\ R(x,y)$

Subset Collection

$?c\ ?u\left(?x\ ?a.\ ?y\ ?b.\ R(x,y) \Rightarrow ?d\ ?c.\ R'(a,d)\right)$

Infinity

$?z.\ Nat(z)$

Summary

- We know that Classical Nuprl is consistent and can share theorems with PVS, HOL, Mizar, … provided it avoids “domains” (bar types) and certain recursive types
- Classical Nuprl can retain $A\ //\ E$, $\cap$, $\cup$, $\sqsubseteq$, Top
- With $\cup$, $\cap$ it becomes a peer theory with classical set theory
- HOL, PVS can consistently add $A\ //\ E$, $\cap$, $\cup$, $\sqsubseteq$, Top