Bishop's set theory[1]

Erik Palmgren
Uppsala Universitet
www.math.uu.se/~palmgren

TYPES summer school
Göteborg
August 2005

[1] Errett Bishop (1928-1983) constructivist mathematician.

Introduction - What is a set?

The iterative notion of set (G. Cantor 1890, E. Zermelo 1930)

- sets built up by collecting objects, or other sets, according to some selection criterion $Q(x)$

$$\{x \mid Q(x)\}$$

Frege's "naive" set theory is inconsistent (Russell's paradox). Remedy: introduce size limitations, use explicit set constructions as power sets, products or function sets, start from given sets X

$$\{x \in X \mid Q(x)\}$$

Encoding of mathematical objects as iterative sets

All mathematical objects are built from the empty set (E. Zermelo 1930)

Natural numbers are for example usually encoded as

$$0 = \emptyset \quad 1 = 0 \cup \{0\} = \{\emptyset\} \quad 2 = 1 \cup \{1\} = \{\emptyset, \{\emptyset\}\} \quad \cdots \quad .$$

Pairs of elements can be encoded as $\langle a, b \rangle = \{\{a\}, \{a, b\}\}$. Functions are certain sets of pairs objects ... etc.

Quotient structures are constructed by the method of equivalence classes — only one notion of equality is necessary.

(J.Myhill and P.Aczel (1970s): constructive versions of ZF set theory.)

What is a set? A more basic view

"A set is not an entity which has an ideal existence: a set exists only when it has been defined. To define a set we prescribe, at least implicitly, what we (the constructing intelligence) must do in order to construct an element of the set, and what we must do to show that two elements are equal" (Errett Bishop, Foundations of Constructive Analysis, 1967.)

Martin-Löf type theory conforms to this principle of defining sets.

Abstraction levels

One may disregard the particular representations of set-theoretic constructions, and describe their properties abstractly (in the spirit of Bourbaki).

For instance, the cartesian product of two sets A and B may be described as a set $A \times B$ together with two *projection* functions

$$\pi_1 : A \times B \to A \qquad \pi_2 : A \times B \to B,$$

such that for each $a \in A$ and each $b \in B$ there exists a unique element $c \in A \times B$ with $\pi_1(c) = a$ and $\pi_2(c) = b$. Thus π_k picks out the kth component of the abstract pair.

Reference to the particular encoding of pairs is avoided. This is a good principle in mathematics as well as in program construction.

Some references using Bishop's set theory

E. Bishop and D.S. Bridges (1985). *Constructive Analysis.* Springer-Verlag.

D.S. Bridges and F. Richman (1987). *Varieties of Constructive Mathematics.* London Mathematical Society Lecture Notes, Vol. 97. Cambridge University Press.

R. Mines, F. Richman and W. Ruitenburg (1988). *A Course in Constructive Algebra.* Springer.

Among constructivists, one often says that **constructive mathematics is mathematics based on intuitionistic logic.**

Plan of lectures

(Based on Ch. 3 and 4 of *Type-theoretic foundation of constructive mathematics* by T. Coquand, P. Dybjer, E. Palmgren and A. Setzer, version August 5, 2005.)

1. Introduction

2. Terminology for type theory

3. Intuitionistic logic

4. Sets and equivalence relations

5. Choice sets and axiom of choice

6. Relations and subsets

7. Finite sets and relatives

8. Quotients

9. Universes and restricted power sets

10. Categories

11. Relation to categorical logic

Exercises: see lecture notes.

2. Terminology for type theory

later Martin-Löf	**lect. notes**	**Bishop**	**early M.-L.**	**other**
type	sort		category	kind
set	type	preset	type	
extensional set	set	set		setoid, E-set
function	operation	operation	function	
extensional function	function	function		setoid map, E-function

(Thanks for the table, Peter!)

The application of an operation $f : A \longrightarrow B$ to an element $a : A$ is denoted

$$f\ a$$

Recall: A proposition may be regarded as a type according to the following translation scheme

$(\forall x : A) P\, x$	$(\Pi x : A) P\, x$
$(\exists x : A) P\, x$	$(\Sigma x : A) P\, x$
$P \wedge Q$	$P \times Q$
$P \vee Q$	$P + Q$
$P \Rightarrow Q$	$P \rightarrow Q$
$\top$	N_1
$\bot$	N_0
$\neg P \quad (= P \Rightarrow \bot)$	$P \rightarrow \mathrm{N}_0$

The judgement

A is true

means that there is some p so that $p : A$.

Relations and predicates on types

A *predicate P on a type X* is a family of propositions $P\,x$ $(x : X)$.

A *relation R between types X and Y* is a family of propositions $R\,x\,y$ $(x : X, y : Y)$. If $X = Y$, we say that R is a *binary relation* on X.

A binary relation R on X is an *equivalence relation* if there are functions ref, sym and tra with

$$ref\ a : R\,a\,a \quad (a : X),$$

$$sym\ a\ b\ p : R\,b\,a \quad (a : X, b : X, p : R\,a\,b),$$

$$tra\ a\ b\ c\ p\ q : R\,a\,c \quad (a, b, c : X, p : R\,a\,b, q : R\,b\,c).$$

We may suppress the proof objects and simply write, for instance in the last line

$$R\ a\ c\ \mathrm{true} \qquad (a, b, c : X, R\ a\ b\ \mathrm{true}, R\ b\ c\ \mathrm{true}),$$

which is equivalent to

$$(\forall a : X)(\forall b : X)(\forall c : X)(R\ a\ b \wedge R\ b\ c \Rightarrow R\ a\ c)\ \mathrm{true}.$$

3. Intuitionistic logic

The logic governing the judgements of the form

$$A \text{ true}$$

is intuitionistic logic. It is best described by considering the derivation rules for natural deduction and then remove the Reductio Ad Absurdum rule (principle of indirect proof):

Derivation rules:

$$\frac{A \qquad B}{A \wedge B}\,(\wedge I) \qquad\qquad \frac{A \wedge B}{A}\,(\wedge E1) \qquad \frac{A \wedge B}{B}\,(\wedge E2)$$

$$\dfrac{\begin{array}{c}\overline{A}^{h}\\ \vdots \\ B\end{array}}{A \longrightarrow B}(\longrightarrow I, h)$$

$$\dfrac{A \longrightarrow B \qquad A}{B}\ (\longrightarrow E)$$

$$\dfrac{A}{A \vee B}\ (\vee I1) \qquad \dfrac{B}{A \vee B}\ (\vee I2)$$

$$\dfrac{A \vee B \qquad \begin{array}{c}\overline{A}^{h_1}\\ \vdots \\ C\end{array} \qquad \begin{array}{c}\overline{B}^{h_2}\\ \vdots \\ C\end{array}}{C}\ (\vee E, h_1, h_2)$$

$$\dfrac{A}{(\forall x)A}\ (\forall I) \qquad \dfrac{(\forall x)A}{A[t/x]}\ (\forall E)$$

$$\frac{A[t/x]}{(\exists x)A}\ (\exists I)$$

$$\frac{(\exists x)A \qquad \begin{matrix}\overline{A}^{\,h} \\ \vdots \\ C\end{matrix}}{C}\ (\exists E, h)$$

$$\frac{\bot}{A}\ (\bot E)$$

$$\frac{\begin{matrix}\overline{\neg A}^{\,h} \\ \vdots \\ \bot\end{matrix}}{A}\ (RAA, h)$$

4. Sets and equivalence relations

Definition A *set* X is a type $\underline{X}$ together with an equivalence relation $=_X$ on $\underline{X}$. Write this as

$$X = (\underline{X}, =_X).$$

We shall also write $x \in X$ for $x : \underline{X}$.

Remark

In Bishop (1967) $\underline{X}$ is called a *preset,* rather than a type.

In the type theory community $X = (\underline{X}, =_X)$ is often known as a *setoid*.

Examples Let N be the type of natural numbers. Define equivalence relations

$x =_{\mathbb{N}} y$ iff $\mathrm{Tr}\,(\mathrm{eq}_{\mathrm{N}}\, x\, y)$

(Here $\mathrm{eq}_N : N \to N \to \mathrm{Bool}$ is the equality tester for N and $\mathrm{Tr}\ \mathrm{tt} = \top$ and $\mathrm{Tr}\ \mathrm{ff} = \bot$)

$x =_n y$ iff $x - y$ is divisble by n

Then

- $\mathbb{N} = (\mathrm{N}, =_{\mathbb{N}})$ is the *set of natural numbers*
- $\mathbb{Z}_n = (\mathrm{N}, =_n)$ is the *set of integers modulo* n*.*

Functions vs operations

What is usually called functions in type theory, we call here *operations*.

Definition. A *function* f from the set X to the set Y is a pair $(\underline{f}, \mathrm{ext}_f)$ where $\underline{f} : \underline{X} \to \underline{Y}$ is an operation so that

$$(\mathrm{ext}_f\ a\ b\ p) : \underline{f}\ a =_Y \underline{f}\ b \quad (a, b : \underline{X}, p : a =_X b).$$

To conform with usual mathematical notation, function application will be written

$$f(a) =_{\mathrm{def}} \underline{f}\ a$$

Two functions $f, g : X \to Y$ are *extensionally equal*, $f =_{[X \to Y]} g$, if there is e with

$$e\ a : f(a) =_Y g(a) \quad (a \in X).$$

Set constructions

The product of sets A and B is a set $P = (\underline{P}, =_P)$ where $\underline{P} = \underline{A} \times \underline{B}$ (cartesian product as types) and the equality is defined by

$(x,y) =_P (u,v)$ iff $x =_A u$ and $y =_B v$.

Standard notation for this P is $A \times B$. Projection function are $\pi_1(x,y) = x$ and $\pi_1(x,y) = y$. This construction can be verified to satisfy the abstract property (page 5). (It can as well be expressed by the categorical universal property for products.)

The disjoint union $A \dot{\cup} B$ (or $A + B$) is definied by considering the corresponding type construction.

The functions from A to B form a set B^A defined to be the type

$$(\Sigma f : \underline{A} \to \underline{B})(\forall x, y : \underline{A})[x =_A y \to f\,x =_B f\,y],$$

together with the equivalence relation

$$(f, p) =_{B^A} (g, q) \iff_{\mathrm{def}} (\forall x : \underline{A})\, f\,x =_B g\,x.$$

The evaluation function $\mathrm{ev}_{A,B} : B^A \times A \to B$ is given by

$$\mathrm{ev}_{A,B}((f, p), a) = f\,a$$

Proposition. Let A, B and X be sets. For every function $h : X \times A \to B$ there is a unique function $\hat{h} : X \to B^A$ with

$$\mathrm{ev}_{A,B}(\hat{h}(x), y) = h(x, y) \qquad (x \in X, y \in A).$$

A set X is called *discrete,* if for all $x, y \in X$

$$(x =_X y) \lor \neg (x =_X y).$$

In classical set theory all sets are discrete. This is not so constructively, but we have

Proposition. The unit set $\mathbf{1}$ and the set of natural numbers $\mathbb{N}$ are both discrete. If X and Y are discrete sets, then $X \times Y$ and $X + Y$ are discrete too.

However, the assumption that $\mathbb{N}^{\mathbb{N}}$ is discrete implies a nonconstructive principle (WLPO):

$$(\forall n \in \mathbb{N}) f(n) = 0 \lor \neg(\forall n \in \mathbb{N}) f(n) = 0$$

Coarser and finer equivalences

An equivalence relation $\sim$ is *finer* than another equivalence relation $\approx$ on a type $\underline{A}$ if for all $x, y : A$

$$x \sim y \Longrightarrow x \approx y.$$

It is easy to prove by induction that $=_{\mathbb{N}}$ is the finest equivalence relation on N.

If there is a finest equivalence relation $=_A$ on a type $\underline{A}$, the set $A = (\underline{A}, =_A)$ has the *substitutivity property*

$$x =_A y \Longrightarrow (P x \Leftrightarrow P y)$$

for any predicate P on the type $\underline{A}$.

Sets are rarely substitutive, and the notion is not preseved by isomorphisms. $\mathbb{Z}_n$ as constructed above is not substitutive; an isomorphic construction yields substitutivity.

Theorem. To any type $\underline{A}$, the identity type construction Id assigns a finest equivalence $\mathrm{Id}\,\underline{A}$. The resulting set, also denoted $\underline{A}$, is substitutive.

Remark. Substitutive sets are however very convenient for direct formalisation in e.g. Agda, as extensionality proofs can be avoided.

5. Choice sets and axiom of choice

A set S is a *choice set,* if for any surjective function $f : X \longrightarrow S$, there is right inverse $g : S \longrightarrow X$, i.e.

$$f(g(s)) = s \qquad (s \in S).$$

Theorem. Every substitutive set is a choice set.

(Zermelo's) Axiom of Choice may be phrased thus:

Every set is a choice set.

Theorem. Zermelo's AC implies the law of excluded middle.

Though Zermelo's AC is incompatible with constructivism, there is related axiom (theorem of type theory) freely used in Bishop constructivism.

Theorem. For any set A there is a choice set $\underline{A}$ and surjective function $p : \underline{A} \rightarrow A$. (In categorical logic often referred to as "existence of enough projectives".)

As a consequence, Dependent Choice is valid (see notes, p. 76).

Theorem. If A and B are choice sets, then so are $A \times B$ and $A + B$.

6. Relations and subsets

Definition A *(extensional) property* P of the set X is a family of propositions $P\,x$ $(x \in X)$ with

$$x =_X y, P\,x \Longrightarrow P\,y.$$

We also say that P is a *predicate* on X.

A *relation* R between sets X and Y is a family of propositions $R\,x\,y$ $(x \in X, y \in Y)$ such that

$$x =_X x', y =_Y y', R\,x\,y \Longrightarrow R\,x'\,y'.$$

The relation is *univalent* if $y =_Y y'$, whenever $R\,x\,y$ and $R\,x\,y'$.

Write $P(x)$, $R(x,y)$ etc. in the extensional situation.

Restatement of choice principles for relations.

The following is the theorem of *unique choice.*

Thm. Let R be a univalent relation between the sets X and Y. It is total if, and only if, there exists a function $f : X \longrightarrow Y$, called a *selection function,* such that

$$R(x, f(x)) \qquad (x \in X).$$

(This function is necessarily unique if it exists.)

An alternative characterisation of choice sets is

Thm. A set X is a choice set iff for every set Y, each total relation R between X and Y has a selection function $g : X \longrightarrow Y$ so that

$$R(x, g(x)) \qquad (x \in X).$$

Dependent choice

Dependent choice. Let A be a set which is the surjective image of a choice set. Let R be a binary relation on A such that

$$(\forall x \in A)(\exists y \in A)R(x,y).$$

Then for each $a \in A$, there exists a function $f : \mathbb{N} \to A$ with $f(0) = a$ and

$$R(f(n), f(n+1)) \qquad (n \in \mathbb{N}).$$

Proof. Let $p : P \to A$ be surjective, where P is a choice set. By surjectivity, we have

$$(\forall u \in P)(\exists v \in P)R(p(u), p(v)).$$

Since P is a choice set we find $h : P \to P$ with $R(p(u), p(h(u)))$ for all $u \in P$.

For $a \in A$, there is $b_0 \in P$ with $a = p(b_0)$.

Define by recursion $g(0) = b_0$ and $g(n+1) = h(g(n))$, and let $f(n) = p(g(n))$. Thus $R(p(g(n)), p(g(n+1)))$, so f is indeed the desired choice function. $\Box$

Remark Thus we have proved the general dependent choice theorem in type theory with identity types. We also get another proof of countable choice, without requiring a particular subsititutive construction of natural numbers.

Subsets as injective functions

Let X be a set. A *subset* of X is a pair $S = (\partial S, \iota_S)$ where ∂S is a set and $\iota_S : \partial S \to X$ is an injective function.

An element $a \in X$ is a *member of S* (written $a \in_X S$) if there exists $d \in \partial S$ with $a =_X \iota_S(d)$.

Inclusion $\subseteq_X$ and equality $\equiv_X$ of subsets of X can be defined in the usual logical way.

Prop. For subsets A and B of X, the inclusion $A \subseteq_X B$ holds iff there is a function $f : \partial A \to \partial B$ with $\iota_B \circ f = \iota_A$. (Such f are unique and injective.)

The subsets are equal iff f is a bijection.

Separation of subsets

For a property P on a set X, the subset

$$\{x \in X \mid P(x)\} = \Big(\{x \in X : P(x)\}, \iota\Big)$$

is defined by the data:

$$\underline{\{x \in X : P(x)\}} =_{\mathrm{def}} (\Sigma x \in X) P(x)$$

and

$$\langle x, p \rangle =_{\{x \in X :\, P(x)\}} \langle y, q \rangle \iff_{\mathrm{def}} x =_X y$$

and $\iota(\langle x, p \rangle) =_{\mathrm{def}} x$.

(Note the pedantic syntactic distinction of ":" and "|".)

Note that

$$
\begin{aligned}
a \in_X \{x \in X \mid P(x)\} &\Leftrightarrow (\exists d \in \{x \in X \ : \ P(x)\})\, a = \iota(d) \\
&\Leftrightarrow (\exists x \in X)(\exists p : \underline{P}\, x)\, a = \iota(\langle x, p \rangle) \\
&\Leftrightarrow \underline{P}\, a \\
&\Leftrightarrow P(a)
\end{aligned}
$$

The usual set-theoretic operations $\cap$, $\cup$, $\overline{(\ \ )}$ can now be defined "logically" for subsets.

A subset S of X is *decidable*, or *detachable,* if for all $a \in X$

$$a \in_X S \vee \neg(a \in_X S).$$

Union of subsets: logical definition.

Let $A = (\partial A, \iota_A)$ and $B = (\partial B, \iota_B)$ be subsets of X.

Their union is the following subset of X

$$A \cup B = \{z \in X \mid z \in_X A \text{ or } z \in_X B\}.$$

Taking $U = A \cup B$ apart as $U = (\partial U, \iota_U)$ we see that $\underline{\partial U}$ is

$$(\Sigma z : \underline{X})(z \in_X A \text{ or } z \in_X B) \quad = \quad (\Sigma z : \underline{X})((z \in_X A) + (z \in_X B)).$$

whereas $\iota_U(z, p) = z$.

Complement

The complement of the subset A of X is defined as

$$\overline{A} = \{z \in X \mid \neg z \in_X A\}.$$

For $\overline{A} = (\partial C, \iota_C)$ we have

$$\underline{\partial C} = (\Sigma z : \underline{X})((z \in_X A) \rightarrow \bot).$$

That A is a decidable subset of X can be expressed as $A \cup \overline{A} = X$.

The decidable subsets form a boolean algebra.

Partial functions

A *partial function* f from A to B consists of a subset $(\mathrm{D}_f, \mathrm{d}_f)$ of A, its *domain of definition* (denoted $\operatorname{dom} f$) and a function $\mathrm{m}_f : \mathrm{D}_f \to B$. We write this with a special arrow symbol as $f : A \rightharpoondown B$.

Such $f : A \rightharpoondown B$ is *total* if its domain of definition equals A as a subset, or equivalently, if d_f is an isomorphism.

Another partial function *$g : A \rightharpoondown B$ extends f,* writing $f \subseteq g : A \rightharpoondown B$, if for each $s \in \mathrm{D}_f$ there exists $t \in \mathrm{D}_g$ with $\mathrm{d}_f(s) = \mathrm{d}_g(t)$ and $\mathrm{m}_f(s) = \mathrm{m}_g(t)$. If both $f \subseteq g$ and $g \subseteq f$, we define f and g to be equal as partial functions.

Example. Let $F = (F, \cdot, +, 0, 1)$ be a field, and let

$$U = \{x \in F \mid (\exists y \in F) x \cdot y = 1\}$$

be the subset of invertible elements. Define a function $\mathrm{m}_r : \partial U \to F$ to be $\mathrm{m}_r(x) = y$, where y is unique such that $x \cdot y = 1$. Thus the reciprocal is a partial function $r = (\cdot)^{-1} : F \rightharpoonup F$.

In fact, for any univalent relation R between sets X and Y there is partial function $f_R = (D, d, m)$ given by

$$\partial D = \{u \in X \times Y : R(\pi_1(u), \pi_2(u))\}$$

$d = \pi_1 \circ \iota_D$ and $m = \pi_2 \circ \iota_D$.

Example For any pair of subsets A and B of X that are disjoint $A \cap B = \emptyset$, we may define a partial characteristic function

$$\chi : X \rightharpoondown \{0,1\}$$

satisfying

$\chi(z) = 0$ iff $z \in_X A$,

$\chi(z) = 1$ iff $z \in_X B$,

by considering the univalent relation $R(z,n)$:

$$(z \in_X A \wedge n = 0) \vee (z \in_X B \wedge n = 1).$$

Partial functions are composed in the following manner: if $f : A \rightharpoondown B$ and $g : B \rightharpoondown C$, define the composition $h = g \circ f : A \rightharpoondown C$ by

$$\mathrm{D}_h = \{(s,t) \in \mathrm{D}_f \times \mathrm{D}_g : \mathrm{m}_f(s) = \mathrm{d}_g(t)\}$$

The function $\mathrm{d}_h : \mathrm{D}_h \to A$ given by composing the projection to D_f with d_d is injective. The function $\mathrm{m}_h : \mathrm{D}_h \to C$ is defined by the composition of the projection to D_g and d_g.

7. Finite sets and relatives

The *canonical n-element set* is

$$\mathbb{N}_n = \{k \in \mathbb{N} : k < n\} \hookrightarrow \mathbb{N}.$$

Any set X isomorphic to such a set is called *finite.* It may be written

$$\{x_0, \ldots, x_{n-1}\}$$

where $k \mapsto x_k : \mathbb{N}_n \to X$ is the isomorphism.

Since $x_j = x_k$ iff $j = k$, we can always decide whether two elements of a finite set are equal by comparison of indices.

A related notion is more liberal:

A set X is called *subfinite,* or *finitely enumerable,* if there is, for some $n \in \mathbb{N}$, a surjection $x : \mathbb{N}_n \to X$.

Here we are only required to enumerate the elements, not tell them apart.

We can always tell whether a subfinite set is empty by checking if $n = 0$.

Remark. A subset of a finite set need not be finite, or even subfinite. Consider

$$\{0 \in \mathbb{N}_1 : P\}$$

where P is some undecided proposition.

Some basic properties

Let X and Y be sets. Then:

(i) X finite $\Longleftrightarrow X$ subfinite and discrete

(ii) X subfinite, $f : X \to Y$ surjective $\Longrightarrow Y$ subfinite

(iii) Y discrete, $f : X \to Y$ injective $\Longrightarrow X$ discrete

(iv) Y discrete, $X \hookrightarrow Y \Longrightarrow X$ discrete

(v) Y finite, $X \hookrightarrow Y$ decidable $\Longrightarrow X$ finite.

8. Quotients

Let $X = (\underline{X}, =_X)$ be a set and let $\sim$ be a relation on this set. Then by the extensionality of the relation

$$x =_X y \Longrightarrow x \sim y. \tag{1}$$

Thus if $\sim$ is an equivalence relation on X

$$X/\sim = (\underline{X}, \sim)$$

is a set, and $q : X \to X/\sim$ defined by $q(x) = x$ is a surjective function.

We have the following extension property. If $f : X \to Y$ is a function with

$$x \sim y \Longrightarrow f(x) =_Y f(y), \tag{2}$$

then there is a unique function $\overline{f} : X/\sim \to Y$ (up to extensional equality) with

$$\overline{f}(i(x)) =_Y f(x) \qquad (x \in X).$$

We have constructed *the quotient of X with respect to $\sim$*: $\quad q : X \to X/\sim$

Remark. Every set is a quotient of a choice set. Namely, X is the quotient of $\underline{X}$ w.r.t. $=_X$.

Proposition. A set is subfinite iff it is the quotient of a finite set.

9. Universes and restricted powersets

A general problem with (or feature of) predicative theories like Martin-Löf type theory is their inability to define a set of *all* subsets of a given set. It is, though, often sufficient to consider certain restricted classes of subsets in a certain situation.

A *set-indexed family $\mathcal{F} = (F, I)$ of subsets* of a given set X consists of an *index set* $I = (\underline{I}, =_I)$ and a subset F_i of X for each $i : \underline{I}$, which are such that if $i =_I j$ then F_i and F_j are equal as subsets of X.

A subset S of X *belongs to the family $\mathcal{F}$*, written $S \in \mathcal{F}$, if $S = F_i$ (as subsets of X) for some $i \in I$.

Consider any family of types $\mathcal{U} = (T, U)$, where $T\,i$ is a type for each $i : U$. It represents a collection of sets, the $\mathcal{U}$-sets, as follows.

First, a *$\mathcal{U}$-representation* of a set is a pair $r = (i_0, e)$ where $i_0 : I$ and $e : T\,i_0 \times T\,i_0 \rightarrow U$ is an operation so that

$$a =_r b \Leftrightarrow_{\mathrm{def}} T(e\,a\,b)$$

defines an equivalence relation on the type $T\,i_0$. Then this is a set

$$\hat{r} = (T\,i_0, =_r).$$

A set X is *$\mathcal{U}$-representable,* or simply a *$\mathcal{U}$-set*, if it is in bijection with $\hat{r}$ for some $\mathcal{U}$-representation r. The $\mathcal{U}$-sets defines, in fact, a full subcategory of the category of sets, equivalent to a small category.

Example For $U = \mathrm{N}$ and $T\,n = \mathrm{N}_n$, the $(\mathrm{N}, \mathrm{N}_{(-)})$-sets are the finite sets.

Restricted power sets

For any set X and any family of types $\mathcal{U}$, define the family $\mathcal{R}_{\mathcal{U}}(X)$ of subsets of X as follows.

- Its index set I consists of triples (r, m, p) where r is a $\mathcal{U}$-representation, $m : \hat{r} \to X$ is a function and p is a proof that m is injective.

- Two such triples (r, m, p) and (s, n, q) are equivalent, if $(\hat{r}, m)$ and $(\hat{s}, n)$ are equal as subsets.

- For index $(r, m, p) \in I$, the corresponsing subset of X is $F_{(r,m,p)} = (\hat{r}, m)$.

Proposition A subset $S = (\partial S, \iota_S)$ of X belongs to $\mathcal{R}_{\mathcal{U}}(X)$ iff ∂S is a $\mathcal{U}$-set.

Unless $\mathcal{U}$ has some closure properties, $\mathcal{R}_{\mathcal{U}}(X)$ will not be closed under usual set-theoretic operations. We review some common such properties below. Suppose that $\mathcal{U}$ is a type-theoretic universe.

- If $\mathcal{U}$ is closed under Σ, then $\mathcal{R}_{\mathcal{U}}(X)$ is closed under binary $\cap$, and $\bigcup_{i \in I}$ indexed by $\mathcal{U}$-sets I.

- If $\mathcal{U}$ is closed under Π, then $\mathcal{R}_{\mathcal{U}}(X)$ is closed under $\bigcap_{i \in I}$ indexed by $\mathcal{U}$-sets I, and the binary set operation

$$(A \Rightarrow B) = \{x \in X : x \in A \Rightarrow x \in B\}.$$

- If $\mathcal{U}$ is closed under $+$, then $\mathcal{R}_{\mathcal{U}}(X)$ is closed under binary $\cup$.

- If $\mathcal{U}$ contains an empty type, then $\mathcal{R}_{\mathcal{U}}(X)$ contains $\emptyset$.

Standard Martin-Löf type universes $\mathcal{U}$ (see Martin-Löf 1984) satisfies indeed the conditions above. Recall from Dybjer's lecture how such universes are defined:

$$
\begin{array}{rcl@{\qquad}rcl}
\hat{\mathrm{N}} & : & U & T\ \hat{\mathrm{N}} & = & \mathrm{N} \\
\widehat{\mathrm{N}_0} & : & U & T\ \widehat{\mathrm{N}_0} & = & \mathrm{N}_0 \\
\widehat{\mathrm{N}_1} & : & U & T\ \widehat{\mathrm{N}_1} & = & \mathrm{N}_1 \\
(\hat{+}) & : & U \to U \to U & T\ (a \hat{+} b) & = & T\ a + T\ b \\
\hat{\Sigma} & : & (a : U) \to (T\ a \to U) \to U & T\ (\hat{\Sigma}\ a\ b) & = & \Sigma\ (T\ a)\ (\lambda x.T\ (bx)) \\
\hat{\Pi} & : & (a : U) \to (T\ a \to U) \to U & T\ (\hat{\Pi}\ a\ b) & = & \Pi\ (T\ a)\ (\lambda x.T\ (bx)) \\
 & \vdots & & & \vdots &
\end{array}
$$

10. Categories

We use a definition of category where no equality relation between objects is assumed, as introduced in type theory by P. Aczel 1993, P. Dybjer and V. Gaspes 1993. Such categories are adequate for developing large parts of elementary category theory inside type theory (Huet and Saibi 2000).

A *small E-category* $\mathbf{C}$ consists of a type Ob of *objects* (no equivalence relation between objects is assumed) and for all $A,B : \mathrm{Ob}$ there is a set $\mathrm{Hom}(A,B)$ of *morphisms from A to B*. There is a identity morphism $\mathrm{id}_A \in \mathrm{Hom}(A,A)$ for each $A : \mathrm{Ob}$. There is a composition function $\circ : \mathrm{Hom}(B,C) \times \mathrm{Hom}(A,B) \to \mathrm{Hom}(A,C)$. These data satisfy the equations $\mathrm{id} \circ f = f$, $g \circ \mathrm{id} = g$ and $f \circ (g \circ h) = (f \circ g) \circ h$.

For a *locally small E-category* we allow Ob to be a sort.

Example. *The category of sets,* **Sets**, has as objects sets. The set of functions from A to B is denoted $\mathrm{Hom}(A,B)$. The category **Sets** is locally small, but not small.

Example. The *discrete category given by a set $A = (\underline{A}, =_A)$.* The objects of the category are the elements of $\underline{A}$. Define $\mathrm{Hom}(a,b)$ as the type (of proofs of) $a =_A b$. Any two elements of this type are considered equal. (The proofs of reflexivity and transitivity provide id and $\circ$ respectively. Also the proof of symmetry, gives that two objects a and b are isomorphic if, and only if, $a =_A b$.) Denote the discrete category by $A^{\#}$. This is a small category.

Families of sets

Families of sets have more structure than in set theory.

A *family F of sets indexed by a set I* is a functor $F : I^{\#} \to \mathbf{Sets}$.

Explication:

For each element a of I, $F(a)$ is a set.

For any proof object $p : a =_I b$, $F(p)$ is function from $F(a)$ to $F(b)$, a so-called *transporter function*.

Moreover, since any two morphisms p and q from a to b in $I^{\#}$ are identified, we have $F(p) = F(q)$. The functoriality conditions thus degenerate to the following:

(a) $F(p) = \mathrm{id}_{F(a)}$ for any $p : a =_I a$.

(b) $F(q) \circ F(p) = F(r)$ for all $p : a =_I b$, $q : b =_I c$, $r : a =_I c$.

Note that each $F(p)$ is indeed an isomorphism, and that $F(q)$ is the inverse of $F(p)$ as soon as $p : a =_I b$ and $q : b =_I a$.

Remark. If each set in the family F is a subset of a fixed set X, i.e. $i_a : F(a) \hookrightarrow X$ and so that $i_a \circ F(r) = i_b$ for $r : a =_I b$, then $(F(a), i_a) = (F(b), i_b)$ as subsets of X, if $a =_I b$.

Remark. Families of sets are treated in essentially this way in (Bishop and Bridges 1985, Exercise 3.2).

Example. Let $\beta : B \to I$ be any function. Define for each $a \in I$ a set

$$\beta^{-1}(a) \equiv \{u \in B : \beta(u) =_I a\},$$

the *fiber of β over a.* Then β^{-1} extends to a functor $I^{\#} \to \mathbf{Sets}$.

This example indicates another way of describing a families of sets indexed by I: as the fibers of a function $\beta : B \to I$. These are in turn precisely the objects of the slice category $\mathbf{Sets}/I$. We have the following equivalence of categories

Thm.

$$\mathbf{Sets}^{I^{\#}} \cong \mathbf{Sets}/I.$$

Constructions:

Given $\beta : B \to I$. Construct functor $\beta^{-1} : I^{\#} \to \mathbf{Sets}$. Define for $r : a =_I b$ a function $\beta^{-1}(r) : \beta^{-1}(a) \to \beta^{-1}(b)$ by

$$\beta^{-1}(r)(u,p) = (u, k_{\beta(u),a,b}(r,p)).$$

Here $k_{a,b,c}$ is the proof object for $b =_I c \to a =_I b \to a =_I c$,

For $F \in \mathbf{Sets}^{I^{\#}}$, define $B = (\Sigma i \in I)F(i)$, where $(a,x) =_B (b,y)$ iff $a =_I b$ and $F(r)(x) =_{F(b)} y$ and $r : a =_I b$. Let $\beta_F : B \to I$ be the first projection.

11. Relation to categorical logic

Category theory provides an abstract way of defining the essential mathematical proporties of sets, in terms of universal constructions.

An *elementary topos* is a category with properties similar to the sets, though neither classical logic (discreteness of sets), or axioms of choice are assumed among these properties.

C. McLarty: *Elementary Categories, Elementary Toposes.* Oxford University Press 1992.

J. Lambek and P.J. Scott: *Introduction to Higher-Order Categorical Logic.* Cambridge University Press 1986.

Also predicative versions of toposes have been developed

I. Moerdijk and E. Palmgren: *Type Theories, Toposes and Constructive Set Theory,* Annals of Pure and Applied Logic 114(2002).

The syntactical category of a type theory

Given is any type theory T including the constructions Σ, Π and $+$ and constants $\mathrm{N}_0, \mathrm{N}_1$. (This can be precised using a logical framework.)

Build a category $\mathcal{S}_T$ of closed terms for sets and functions of T. In this category the standard (Heyting-) algebraic method of interpreting logic can be used.

We associate to any first order formula φ with free variables among $x_1 : X_1, \ldots, x_n : X_n$ a subobject $[\![\varphi]\!]_{x_1,\ldots,x_n}$ of $X_1 \times \cdots \times X_n$ in $\mathcal{S}_T$.

Completeness Theorem. For any first-order formulas φ and ψ whose types are in $\mathcal{S}_T$:

$[\![\varphi]\!]_{x_1,\ldots,x_n} \leq [\![\psi]\!]_{x_1,\ldots,x_n}$ in $\mathcal{S}_T$ iff

$$\vdash_T (\forall x_1 : X_1) \cdots (\forall x_n : X_n)\, (\varphi \rightarrow \psi).$$