Building up a toolbox for Martin-Löf's type theory. Part I: subset theory

Giovanni Sambin - Silvio Valentini
Dipartimento di Matematica Pura ed Applicata, Università di Padova
Via Belzoni 7, I–35131 Padova, Italy
e-mail: sambin,valentini@math.unipd.it

a Per Martin-Löf
maestro ed amico

Contents

1 Introduction

A few words of introduction must be used to explain why this long Introduction. The present work originates from the need of subsets in the practical development of a constructive approach to topology (see [S87], [S97] and references therein) and most of what we present here is the answer to problems actually encountered. The solution we arrived at is inspired by a philosophical attitude, and this too has become clear along the way. Thus the aim of this Introduction is to explain such attitude and to make the resulting principles explicit, which might help to understand better some of the technical choices.

1.1 Foreword

Beginning in 1970, Per Martin-Löf has developed an intuitionistic type theory (henceforth type theory tout-court) as a constructive alternative to the usual foundation of mathematics based on classical set theory. We assume the reader is aware at least of the main peculiarities of type theory, as formulated in [ML84] or [NPS90]; here we recall some of them to be able to introduce our point of view.

The form of type theory is that of a logical calculus, where inference rules to derive judgements are at the same time set theoretic constructions, because of

the "propositions-as-sets"[1] interpretation. The spirit of type theory - expressing our interpretation in a single sentence - is to adopt those notions and rules which keep total control of the amount of information contained in the different forms of judgement. We now briefly justify this claim.

First of all, the judgement asserting the truth of a proposition A, which from an intuitionistic point of view means the existence of a verification of A, in type theory is replaced by the judgement $a \in A$ which explicitly exhibits a verification a of A. In fact, it would be unwise, for a constructivist, to through away the specific verification of A which must be known to be able to assert the existence of a verification!

The judgement that A is a set, which from an intuitionistic point of view means that there exists an inductive presentation of A, is treated in type theory in a quite similar way (even if in this case no notation analogous to $a \in A$ is used) since the judgement A *set* in type theory becomes explicit knowledge of the specific inductive presentation of A. In fact, the rules for primitive types and for type constructors are so devised that whenever a judgement A *set* is proved, it means that one has also complete information on the rules which describe how canonical elements of A are formed. Such property, which might look as a peculiarity of type theory, is as a matter of fact necessary in order to give a coherent constructive treatment of quantifiers. Consider for instance universal quantification, and give for granted that an intuitionistically meaningful explanation of universal quantification is possible only for domains with an inductive presentation, that is for what have been called sets above (by the way, this is the reason why the distinction between sets and types is so basic in type theory, see [ML84]). Then the pure knowledge that A is a set is sufficient to say that universal quantification over A gives rise to propositions; however, it would be unwise to forget which specific rules generate A inductively, since, in general, a method verifying a universally quantified proposition over A can be produced, by means of an elimination rule, only by direct reference to the method by which A is generated.

Summing up, we see not only that type theory is inspired by the principle of control of information, but also that the same principle should be at the base of any coherent treatment of sets and propositions, if it has to be both intuitionistic and free of wastes.

Coming back to the formalism in which type theory is expressed, one can see that the principle of keeping control of information is revealed also at the level of syntax, since most inference rules are formulated in a fully analytic style, i.e. everything which appears in the premises is present somehow also in the conclusion. A consequence is, for instance, that the derivation of a judgement $a \in A$ is so detailed that a is *ipso facto* a program which satisfies the requirements specified by A. This is why type theory is particularly interesting for computer science.

However, our experience in developing pieces of actual mathematics within

[1] Called "formulae-as-types" in [H80]. A little warning on terminology is here necessary: we use "set" exactly as in [ML84], while "category" of [ML84] is here replaced with "type"as in [NPS90].

type theory has brought us to believe that "orthodox" type theory is not suitable because its control of information is too strict for this purpose. In fact, the fully analytic character of type theory becomes a burden when dealing with the synthetic methods of mathematics, which "forget" or give for granted most of the details. This, in our opinion, could be the reason why type theory has collected, up to now, more interest among logicians and computer scientists as a formal system than among mathematicians as a foundational theory.

We claim that there is no intrinsic reason why it should remain so, and that actually it is only a matter of developing a stock of "utilities", that is, of building up a toolbox which covers the territory between the basic formalism and mathematical practice; after all, this happened for classical set theory ZF long ago. In other words, the situation seems analogous to that of a programmer who, maybe because of a particular skill with the machine language, has not yet developed those higher level constructs and languages which allow to save time and mental energy, and thus in the end are necessary to free the mind for a common human, i.e. abstract, comprehension.

So our general aim is to build up those tools, that is definitions and rules which "forget" some information, and thus allow a higher level of abstraction, which can make type theory more handy and suitable to work out (intuitionistic) mathematics basing on mathematical intuition, as it has been and should be.

1.2 Contents

Here, completing the work first annunced in [SV93], we make a substantial step in the direction stated above and show how to develop a predicative theory of subsets within type theory.[2] A few years' experience in developing topology in the framework of type theory has taught us that a more liberal treatment of subsets is needed than what could be achieved by remaining literally inside type theory and its traditional notation. In fact, to be able to work freely with subsets in the usual style of mathematics one must come to conceive them like any other mathematical object (which technically means for instance that the judgement that something is a subset can be taken as assumption) and have access to their usual apparatus (for instance, union and intersection).

Subset theory as developed in [NPS90] does not meet the above demands since, being motivated by programming, its aim is different. We could say, in fact, that the aim of [NPS90] is to apply the usual set-constructors of basic type theory to a wider notion of set, which includes sets obtained by comprehension over a given set; the price *they* have to pay is that the justification of the validity of rules for sets must be given anew.

The way out is to adopt the simple idea that it is not compulsory that a subset be a set. Then one is free to define subsets in a natural way as propositional functions (as first suggested in [ML84], page 64, and explicitly adopted in [S87]), and then to introduce the new notion of element of a subset, in terms of

[2] The second step should be on quotient sets, or abstract data types, or setoids; this explains the optimistic specification "part I" in the title.

which also the other standard notions, like inclusion and extensional equality, arbitrary unions and intersections, singletons and finite subsets, quantifiers and functions defined on subsets can be defined. The resulting subset theory is a sort of type-less set theory localized to a set and we have experienced that it is sufficient for instance for the development of topology. We prove that all of this can be done in type theory without loosing control, that is by "forgetting" only information which can be restored at will. This is reduced to the single fact that, for any set A, the judgment A *true* holds if and only if there exists a such that $a \in A$, and it can be proved once and for all, see [V97]; this is the price *we* have to pay to justify our approach.

Since for all notions related to subsets we adopt essentially the standard notation, the result is that at first sight a page of mathematics written using subset theory looks like a page of standard mathematical writing, and one might easily overlook or forget the underlying substantial novelty, namely that everything is directly formalized in type theory. Far from being a drawback, this is in a sense our main intention, since it would show that one can develop an intuition free from the underlying formalism.

1.3 Philosophical motivations

The attitude illustrated so far in this introduction can be seen as the specific outcome of a more general philosophical position [S91] when applied to type theory, and the results we prove can be seen as fragments of a general program [PV93] not necessarily bound to type theory. Here we describe briefly both the philosophical position and the general program in the form of some principles, just enough to be able to state the connection with the problem of foundations.

To build up an abstract concept from a row flow of data, one must disregard inessential details; in other terms, to simplify the complexity of concrete reality one must idealize over it, and this is obtained by "forgetting" some information. To forget information is the same as to destroy something, in particular if there is no possibility of restoring that information, like when the magnetic memory of a disk is erased. So to abstract involves a certain amount of destruction; our principle is that an abstraction is constructive, that is a reliable tool in getting knowledge which is faithful to reality, not when information is kept as much as possible, but when it is "forgotten" in such a way that it can be restored at will in any moment. This after all is the test to show that an abstraction does not lead astray from reality, that is, that it preserves truth.

It is clear that the first step, and often the only one, to be able to restore what has been "forgotten" is to know, to be aware of, what has been forgotten, and to keep control on it. So the second principle is that constructivism does not consist in a *a priori* self-limitation to full information, which would tie constructivism with reluctance to abstraction (as was the case around the twenties when finitism and intuitionism were somehow identified), but rather in the awareness of the destruction which has been operated to build up a certain abstract concept.

When it comes to mathematical terms, awareness of what has been destroyed or forgotten can sometimes be put in objective terms, and then it takes the

form of a method by which the previous state can be restored. If T' is a theory obtained from a more basic theory T by adding some more abstract constructs and their rules, then a method must be supplied which allows to transform whatever proof in T' into a proof within T *with the same computational content.* This allows to "forget safely", since it guarantees that faithfulness to the more concrete level of T is not lost by the more abstract concepts of T'.

This, we believe, is the only reasonable way for a constructivist to extract a philosophical and mathematical value out of Hilbert's program. To obtain a foundation which justifies itself, in Hilbert's view it is necessary to rely on a part of mathematics, called real mathematics, which has to be safe beyond any doubt and without any proof. In Hilbert's conception this is identified with finitistic mathematics, that is manipulation of concrete objects; here instead real mathematics is identified with type theory, which is of course far richer than finitistic mathematics but still serves the purpose. In fact, on one hand the contentual explanation of judgements and rules and on the other hand its interpretation as a programming language (the modern "manipulation of concrete objects") indeed make it reliable beyond doubts and without any proof.

Hilbert was right, of course, in saying that mathematics can not be restricted to real mathematics; in fact, even the most radical constructivist certainly uses more abstract notions or ideas, even if they do not appear in his communications. But which abstract notions can be accepted? We here propose an answer. It is well known that Hilbert's view puts no limitation, as long as the consistency of the formalism in which ideal mathematics is expressed is proved within real mathematics. This can not be accepted by a constructivist, since a consistency proof is not enough to restore, once and for all, the constructive meaning, i.e. faithfulness to the concrete reality of computations. After all, even classical logic is consistent, and with a finitistic proof! So the program is to analyse, case by case, how a certain abstract notion is linked with real mathematics; when it is clear which concrete aspects are forgotten and how they can be restored by a suitable method, then that abstract notion can be used freely and safely. In this paper we show how this is possible for the theory of subsets, and thus we accomplish a fragment of the constructive version of Hilbert's program, which we have called the Camerino program from the place where we spoke about it for the first time [PV93]. The aim is, paradoxically, to save the intuition of an intuitionist from the rigidity of formal systems by supplying safe bridges between intuition and computation.

2 Reconstructing subset theory

2.1 The notion of subset

In classical mathematics a subset U of a set S is usually defined to be a set such that if $a \in U$ then $a \in S$. Importing in type theory this definition as it stands, however, would give a notion of subset not general enough to include all examples of what is undoubtly to be considered a subset. In fact, if S is a set

and $U : (x : S)$ *prop* is a propositional function[3] over S, then we surely want the collection of elements of S satisfying U, usually written $\{x \in S |\ U(x)\}$, to be a subset of S. In ZF, $\{x \in S |\ U(x)\}$ would be a set, by the separation principle; in type theory, however, no form of the separation principle is justified, since in general there are no rules telling how the canonical elements of the collection $\{x \in S |\ U(x)\}$ are formed. In fact, a is an element of $\{x \in S |\ U(x)\}$ if $a \in S$ and $U(a)$ is true, that is if there exists b s.t. $b \in U(a)$, but this form of judgement is not one of the four forms of judgements considered in type theory and hence there is no canonical way to reach the conclusion that such b exists. For example, if $U(x)$ is the property "the Turing machine with index x does not stop on input x", then there are no effective rules to generate $\{x \in N |\ U(x)\}$. Thus, the conclusion is that we want $\{x \in S |\ U(x)\}$ to be a subset of S for any property U, but also that it does not need to be a set.

A second observation is that in ordinary mathematics, operations like union and intersection are freely defined on the class of all sets, while at the opposite extreme in type theory there is no operation of union or intersection in the ordinary sense available on sets. In fact, the result of any operation of set-formation gives rise to a set whose elements are specific of the constructed set, and thus, for instance, we could not have a common statement like $a \in S \cap T$ iff $a \in S$ and $a \in T$, because if $\cap$ were a set-constructor then $S \cap T$ would be a set different from S and T, and hence its elements could not be in common with S and T. As we will soon see, however, such set-theoretic operations can easily be defined on subsets of a set, as soon as we do not require a subset to be a set.

We are thus led to take the step of relaxing the requirement that a subset be a set. Therefore a subset will not have canonical elements, nor rules of elimination or of equality.

Two ways of defining subsets are traditionally available which do not require a subset to be a set.

The first is that a subset of S is given by a property $U(x)$ with x ranging over S; while in a classical perspective it can be conceived that there are many more subsets than properties, from a constructive point of view there is no sense in assuming the existence of a subset unless we can specify it, namely by a property. Thus the conclusion would be that a subset U of S is nothing but a propositional function U over S.

The second conception of subset of S, namely as a function $f : S \to \{0, 1\}$ usually called characteristic function, brings in the end to the same conclusion, as we now see. Classically, any function $f : S \to \{0, 1\}$ gives rise to a property over S, namely the property $f(x) = 1$, and, given a property $U(x)$ over S, the associated function is

$$f_U(x) = \begin{cases} 1 & \text{if } U(x) \textit{ true} \\ 0 & \text{otherwise} \end{cases}$$

If we transfer this as it stands into type theory, we obtain a notion of subset which is too narrow. In fact, due to the different notion of function, the above

[3]Which means that U applied to x, for $x \in S$, is a proposition, written $U(x)$ *prop* $[x : S]$.

argument, when properly translated in type theory, gives a bijective correspondence between functions $S \to \{0,1\}$ and *decidable* propositional functions over S (for a detailed proof, see for instance [V96]).

However, in the classical conception the above definition of f_U can be seen just as a different way of denoting the propositional function U itself. In fact, classically a proposition is just a way to denote a truth value [F92], so $\{0,1\}$ can be identified with the set of values of propositions. Given such a reading, the intuitionistic analogue of a characteristic function is a function from S into the type of intuitionistic propositions, i.e. a propositional function over S.

So both traditional approaches lead to the same intuitionistic version. We thus put:

Definition 2.1 (Definition of subset) *For any set S, a propositional function U with argument ranging in S is called a subset of S, and is written $U \subseteq S$.*

Thus we can think that a subset U of S is obtained by abstracting the variable x in the judgement $U(x)$ *prop* $[x : S]$, i.e. $U \equiv (x : S)\, U(x)$. The same effect is usually expressed with the brace notation to form a subset $\{x \in S |\ U(x)\}$, which does not depend on x any longer. So we put:

$$\{x \in S |\ U(x)\} \equiv U \equiv (x : S)\ U(x)$$

However, it must be said explicitly that, even if we adopt the common expression $\{x \in S |\ U(x)\}$ for a subset, it remains true that a subset is a propositional function and hence a subset can *never* coincide with a set, for the simple reason that propositional functions are of a type different from that of sets.

By similar reasons, the notion of subset is not automatically accompanied by that of element of a subset: writing $a \in \{x \in S |\ U(x)\}$, for $a \in S$, does never give a well formed expression and, on the other hand, writing $u : U$ would mean $(x : S)\ u(x) : (x : S)\ U(x)$, which corresponds to the judgment $u(x) \in U(x)\ [x : S]$ in the notation of [ML84], and hence has nothing to do with the intuitive notion of element of the subset U. So this notion has to be introduced anew, because only in virtue of it an extensional theory of subsets can be reconstructed like that of usual mathematical practice; indeed, we surely want two subsets to be equal iff they have the same elements.

It is worth noting that much of what we are going to do in the case of subsets extends to relations in a natural way. In fact, contrary to the classical approach, a relation in type theory is just a propositional function with several arguments and thus it is a straightforward generalization of the notion of subset.

2.2 Elements of a subset

Given a set S and a subset $U \subseteq S$, the intuitive idea is that the element a of S is an element of U when the property U holds on a. In type theory, this is expressed by requiring $U(a)$ *true*, which means that there exists b such that $b \in U(a)$. However, as in mathematical practice, we surely wish not to bother about the information of the specific b which makes $U(a)$ true: for a to be an

element of U, it is the pure existence of a proof which is required and not the actual specific verification, which we want to "forget"[4]. The theorem in [V97] tells that we can restore such information when wished, at the cost of some metamathematical work.

In the same time, it is essential to keep the information of which element a is (see for instance $\subseteq_S$-elimination in proposition 2.4), and thus express "U holds on a" rather than "$U(a)$ $true$". In fact, $U(a)$ may loose the information of which element a is considered without the possibility of restoring it from $U(a)$ $true$. For instance, if $U \equiv (x : S)\ N$, where N is the set of natural numbers, then $U(a) \equiv ((x : S)\ N)(a) = N$ is true, but there is no way to recover the element a to which U is applied.

Therefore, what we wish is a proposition $a\ \epsilon_S\ U$ which, besides giving $U(a)$ $true$, "recalls" which a is considered, that is, which satisfies

$$(*)\ a\ \epsilon_S\ U\ true \text{ iff } U(a)\ true \text{ and } a \in S$$

Note that the right side of $(*)$ is the conjunction of two judgements, which is usually not treated in type theory: this is the problem we have to face.

It can be shown that $(*)$ is equivalent to the following two conditions together

- for every $a \in S,\ a\ \epsilon_S\ U\ true$ iff $U(a)\ true$
- if $a\ \epsilon_S\ U\ true,$ then $a \in S$

To develop subset theory more smoothly, however, it is convenient to adopt an apparently stronger formulation in which the first condition is expressed by a proposition, namely the following conditions:

1. $(\forall x \in S)\ (x\ \epsilon_S\ U \leftrightarrow U(x))\ true$
2. if $a\ \epsilon_S\ U\ true,$ then $a \in S$

From now on, we will refer to them as the first and second ϵ-condition; we will see that they are all what is needed to be able to develop all of subset theory.

Now, to solve the ϵ-conditions, that is to find a proposition which satisfies them, the crucial remark is that there is substantially one way to include the information given by the judgement $a \in S$ into a proposition, and that is $Id(S, a, a)$. In fact, it is easy to prove that $a \in S$ if and only if $Id(S, a, a)$ $true$: one direction is just the rule of Id-introduction, while the other is obtained by a simple metamathematical argument, namely that from a proof of $Id(S, a, a)$ $true$ one can effectively obtain a proof of $Id(S, a, a)$ $prop$, which in turn must include a proof of $a \in S$. Note that requiring a *formal* equivalence would not make sense.

Thus we simply put

$$x\ \epsilon_S\ U \equiv\ U(x)\ \&\ Id(S, x, x)$$

[4] After the talk in Venice, Prof. de Bruijn has kindly called our attention to his notion of proof-irrelevance [B80], which seems connected with our idea of "forgetting".

The verification of the ϵ-conditions is immediate; let us note explicitly, however, that to prove $U(x)$ & $Id(S,x,x) \leftrightarrow U(x)\ true$ the knowledge of $x \in S$ is essential. This agrees perfectly with the informal requirement that the proposition $a\ \epsilon_S\ U$ must coincide with $U(a)$ when $a \in S$ is known, but differs from $U(a)$ since it keeps track of a by containing knowledge of $a \in S$.

Other solutions of the ϵ-conditions are possible. The one proposed above can be seen as the proposition corresponding to "$U(a)$ *true* & $a \in S$" which means "there exists b such that $b \in U(a)$ and $a \in S$". If we formalize it directly, we obtain $(\exists z \in U(a))\ Id(S,a,a)$, which is exactly $U(a)$ & $Id(S,a,a)$, by the definition of & (see [ML84] p. 43). If we note that "there exists b such that $b \in U(a)$ and $a \in S$" is equivalent to "there exists $c \in \Sigma(S,U)$ such that $p(c) = a \in S$", we reach another solution for the ϵ-conditions, namely $(\exists z \in \Sigma(S,U))\ Id(S,p(z),a)$ (see also section 2.4).

However, the particular form of the solution is inessential, as long as it satisfies the ϵ-conditions. We thus put:

Definition 2.2 *Let S be any set and U any subset of S. If $(x:S)\ x\ \epsilon_S\ U$ is any propositional function satisfying the ϵ-conditions, we say that a is an element of U when $a\ \epsilon_S\ U$ is true.*

Since $a\ \epsilon_S\ U$ is a proposition for any $a \in S$ and $U \subseteq S$, the property of being an element of U respects equality of elements of S; in fact,

$$\text{(substitution of elements)} \quad \frac{Id(S,a,b)\ true \quad a\ \epsilon_S\ U\ true}{b\ \epsilon_S\ U\ true}$$

is a consequence of the Id-elimination rule (cf. [NPS90], p. 64).

The few simple steps taken above are enough to develop a theory of subsets. The usual relations (like inclusion and extensional equality), operations on subsets (like finitary and infinitary union and intersection) and other usual tools (families indexed over a subset, quantifiers ranging over a subset, the image of a function between sets, functions defined on subsets, finite subsets, etc.) can be introduced in a straightforward way by means of the above ϵ-conditions and intuitionistic logic. We repeat such work here with some detail, of course not expecting to produce surprise, but to give a direct feeling (experience) that ϵ-conditions are really enough, and that they allow a complete formalization which is faithful to usual intuitions and practice.

In this way subset theory, even if type-less, is developed in a predicative way, a fact which is inherited directly from type theory.

2.3 Inclusion and equality between subsets

Given two subsets U and V of a set S, it is usual to say that U is included in V if every element of U is also an element of V. We thus put:

Definition 2.3 (Inclusion) *For any $U, V \subseteq S$, we define the inclusion of U into V by*

$$U \subseteq_S V \equiv (\forall x \in S)\ (x\ \epsilon_S\ U \to x\ \epsilon_S\ V)$$

Thus, contrary to $U \subseteq S$, $U \subseteq_S V$ is a proposition even if often, as in usual mathematical practice, we write $U \subseteq_S V$ to mean $U \subseteq_S V\ true$.

By the first ϵ-condition, $U \subseteq_S V \leftrightarrow (\forall x \in S)(U(x) \to V(x))$ is true; this tells that $U \subseteq_S V$ could equivalently be defined as $(\forall x \in S)(U(x) \to V(x))$.

The usual basic rules connecting membership with inclusion are immediately derivable from the above definition by means of the ϵ-conditions; they confirm the understanding that $U \subseteq_S V$ is true if and only if every element of U is also an element of V.

Proposition 2.4 *For any S set and $U, V \subseteq S$, the following rules are derivable:*

$\subseteq_S$*-introduction*

$$\frac{\begin{array}{c}[x\ \epsilon_S\ U\ true]_1 \\ | \\ x\ \epsilon_S\ V\ true\end{array}}{U \subseteq_S V\ true}\ 1$$

$\subseteq_S$*-elimination*

$$\frac{a\ \epsilon_S\ U\ true \quad U \subseteq_S V\ true}{a\ \epsilon_S\ V\ true}$$

Proof. A derivation of $\subseteq_S$-introduction is:

$$\dfrac{\dfrac{\dfrac{\dfrac{S\ set \quad U \subseteq S \quad [x \in S]_2}{x\ \epsilon_S\ U\ prop}}{[x\ \epsilon_S\ U\ true]_1}}{\begin{array}{c}x\ \epsilon_S\ V\ true \\ \hline x\ \epsilon_S\ U \to x\ \epsilon_S\ V\ true\end{array}\ 1}}{U \subseteq_S V\ true}\ 2$$

and a derivation of $\subseteq_S$-elimination is:

$$\dfrac{a\ \epsilon_S\ U\ true \qquad \dfrac{U \subseteq_S V\ true \qquad \dfrac{a\ \epsilon_S\ U\ true}{a \in S}\ \text{second } \epsilon\text{-cond.}}{a\ \epsilon_S\ U \to a\ \epsilon_S\ V\ true}\ \forall\text{-elim.}}{a\ \epsilon_S\ V\ true}$$

Since $\subseteq_S$ is defined in terms of the connective of implication, it inherits all its properties. For instance, $\subseteq_S$ is a preorder on subsets, with a top and a bottom element:

Proposition 2.5 *For any S set and any $U, V, W \subseteq S$,*

$$\textit{reflexivity} \qquad U \subseteq_S U$$

$$\textit{transitivity} \quad \frac{U \subseteq_S V \qquad V \subseteq_S W}{U \subseteq_S W}$$

Moreover, putting $\top_S \equiv \{x \in S |\ Id(S,x,x)\}$ *and* $\bot_S \equiv \emptyset_S \equiv \{x \in S |\ \neg Id(S,x,x)\}$ *we obtain*

$$\textit{top} \qquad U \subseteq_S \top_S$$

$$\textit{bottom} \quad \emptyset_S \subseteq_S U$$

While the first two statements are an immediate consequence of $\subseteq_S$-rules (and in turn of reflexivity and transitivity of implication), the second two follow by logic from $(\forall x \in S)\ (x\ \epsilon_S\ U \to Id(S,x,x))$ *true* and by ex falso quodlibet, respectively, whatever propositional function U is.

Equality between subsets is usually defined by extensionality, that is, for any $U, V \subseteq S$, U and V are said to be equal if they have the same elements. We thus put:

Definition 2.6 (Extensional equality) *For any* U, V *subsets of the set* S*, we define extensional equality of* U *and* V *to be the proposition:*

$$U =_S V \equiv (\forall x \in S)\ (x\ \epsilon_S\ U \leftrightarrow x\ \epsilon_S\ V).$$

We say that the subset U *is extensionally equal, or just equal, to the subset* V *if* $U =_S V$ *true.*

The subsets U and V are (extensionally) equal if and only if for any $a \in S$, $a\ \epsilon_S\ U$ *true* iff $a\ \epsilon_S\ V$ *true*, and thus, by the first ϵ-condition, $U(a)$ *true* iff $V(a)$ *true*. Such equality must be distinguished from the stronger equality $U(x) = V(x)\ [x : S]$, which means that, for any $a \in S$, $b \in U(a)$ if and only if $b \in V(a)$, which is one of the basic judgements of type theory, and which could be called the *intensional* equality of the subsets U and V (since it requires U and V to have the same elements *and*, for each of them, with the same proofs).

By the definitions, it is immediate that the proposition

$$(U =_S V) \leftrightarrow (U \subseteq_S V\ \&\ V \subseteq_S U)$$

holds. Actually, $=_S$ is the equivalence relation on subsets induced by the pre-order $\subseteq_S$ by forcing symmetry to hold. As for properties of $\subseteq_S$, the properties characterizing equivalences, in this case

$$\text{reflexivity} \qquad U =_S U$$

$$\text{symmetry} \qquad U =_S V \to V =_S U$$

$$\text{transitivity} \quad U =_S V\ \&\ V =_S W \to U =_S W$$

can also be seen as inherited from the properties of the logical connective $\leftrightarrow$.

Once the notion of equality has been clarified, the definition of the type of subsets of a given set S is completed:

Definition 2.7 (Power of a set) *For any set* S*, the type of all subsets of* S *equipped with extensional equality is called the power of* S *and is denoted by* $\mathcal{P}S$*.*

When a function (or operation) is to be defined on $\mathcal{P}S$, one must take care to check that it is well defined on $\mathcal{P}S$, that is, that it respects extensional equality; in the sequel this verification is sometime not spelled out.

2.4 Subsets as images of functions

The notion of subset can be further illustrated, after the introduction of extensional equality, by looking at it from a slightly different perspective.

For any set S, and any set I, a function $f(i) \in S\ [i : I]$ is usually associated with the subset of S whose elements are those $a \in S$ for which there exists $i \in I$ such that $Id(S, f(i), a)$ *true*. Here this is achieved simply by defining the image of a function as follows:

Definition 2.8 (Image of a set along a function) *For any sets S and I, and for any function $f(i) \in S\ [i : I]$, the subset of S defined by:*

$$Im_f[I] \equiv \{x \in S|\ (\exists i \in I)\ Id(S, f(i), x)\}$$

is called the image of I along f. Alternative notations for $Im_f[I]$ include $\{f(i)|\ i \in I\}$ and $f[I]$. More generally, given a function with n arguments

$$f(i_1, \ldots, i_n) \in S\ [i_1 : I_1, \ldots, i_n : I_n]$$

the image of $I_1, \ldots, I_n$ along f is defined by

$$Im_f[I_1, \ldots, I_n] \equiv \{x \in S|\ (\exists i_1 \in I_1) \ldots (\exists i_n \in I_n)\ Id(S, f(i_1, \ldots, i_n), x)\}$$

The definition of image associates a subset of a set S with a function into S. Actually, this brings to an alternative characterization of subsets since the converse can also be proved (see [ML84], page 64). In fact, every subset U of S is extensionally equal to the image of some set I along some function $f(i) \in S\ [i : I]$ or, in more informal and suggestive words, we could say that subsets are just one function apart from sets:

Theorem 2.9 *Every subset U of a set S is extensionally equal to the image of the set $\Sigma(S, U)$ along the left projection $p(i) \in S\ [i : \Sigma(S, U)]$; in symbols,*

$$U =_S Im_p[\Sigma(S, U)]$$

that is, by unwinding definitions,

$$U =_S \{x \in S|\ (\exists i \in \Sigma(S, U))\ Id(S, p(i), x)\}$$

holds for every set S and $U \subseteq S$.

Proof. By the definitions and the ϵ-conditions, the claim $U =_S p[\Sigma(S, U)]$ becomes

$$(\forall x \in S)\ (U(x) \leftrightarrow (\exists y \in \Sigma(S, U))\ Id(S, p(y), x))$$

To prove it, assume that a is an arbitrary element of S, and that $z \in U(a)$. Then $\langle a, z\rangle \in \Sigma(S, U)$, thus $p(\langle a, z\rangle) = a \in S$, hence $r(a) \in Id(S, p(\langle a, z\rangle), a)$, and so $\langle\langle a, z\rangle, r(a)\rangle \in (\exists y \in \Sigma(S, U))\ Id(S, p(y), a)$. This proves that $\lambda z.\langle\langle a, z\rangle, r(a)\rangle$ is the term making $U(a) \to (\exists y \in \Sigma(S, U))\ Id(S, p(y), a)$ true.

To prove the converse, assume $z \in (\exists y \in \Sigma(S,U))\ Id(S,p(y),a)$. Then $p(z) \in \Sigma(S,U)$ and hence $q(p(z)) \in U(p(p(z)))$ which, together with the fact that $q(z) \in Id(S,p(p(z)),a)$, gives (see [NPS90], page 64) $subst(q(p(z)),q(z)) \in U(a)$, as wished.

The theorem above gives further evidence to the fact that the notion of being an element of a subset is the result of disregarding some information. Given a function $f(i) : S\ [i : I]$, the subset $Im_f[I]$ can be seen as the result of a process with two different abstraction steps. First, we realize that to know that a is an element in $Im_f[I]$ we can abstract on the particular argument i such that $Id(S,f(i),a)\ true$ and prove only $c \in (\exists i : I)\ Id(S,f(i),a)$ for some c. Note however that, due to the constructive meaning of existential quantification in type theory, a specific element $i \in I$ such that $Id(S,f(i),a)\ true$ can immediately be obtained from c. So, the second step, where we really forget some information, is to say that a is in $Im_f(I)$ if and only if $(\exists i : I)\ Id(S,f(i),a)\ true$.

Now let us consider the case of the function $p(z) \in S\ [z : \Sigma(S,U)]$, for some subset $U \subseteq S$. Then the above considerations bring to the conclusion that a is in $Im_p[\Sigma(S,U)]$ if and only if $(\exists z : \Sigma(S,U))\ Id(S,p(z),a)\ true$. By the theorem above, $a\ \epsilon_S\ U\ true$ is equivalent to a is in $Im_p[\Sigma(S,U)]$, and hence also to $(\exists z : \Sigma(S,U))\ Id(S,p(z),a)\ true$. It is then interesting to observe that to pass from a given verification of $(\exists z : \Sigma(S,U))\ Id(S,p(z),a)$ to the judgement $(\exists z : \Sigma(S,U))\ Id(S,p(z),a)\ true$ means to forget the verification making $U(a)\ true$ without forgetting a, since a appears explicitly in the proposition itself. To supply all the details we left out amounts to find a proof of

$$(\exists z : \Sigma(S,U))\ Id(S,p(z),a)\ \leftrightarrow\ U(a)\ \&\ Id(S,a,a)\ true.$$

It is interseting to note that, since $U(a)\ \&\ Id(S,a,a)$ is the "canonical" solution of the ϵ-conditions, the above equivalence gives an alternative, and more formal, proof of the fact that also $(\exists z : \Sigma(S,U))\ Id(S,p(z),a)$ is a solution of the ϵ-conditions, as we already stated in section 2.2.

2.5 Singletons and finite subsets

Every element a of a set S is equal to any element b making the propositional function $(x : S)\ Id(S,x,a)$ true at b; such triviality means that for any $a \in S$ we can intuitively form the singleton $\{a\}$ by putting

$$\{a\} \equiv \{x \in S|\ Id(S,x,a)\}$$

And then the idea is that a finite subset is the union of a finite number of singletons; so if $a_0,\ldots,a_{n-1} \in S$, for some natural number n, we put

$$\begin{array}{rcl} \{a_0,\ldots,a_{n-1}\} & \equiv & \{a_0\} \cup \{a_1\} \cup \ldots \cup \{a_{n-1}\} \\ & \equiv & \{x \in S|\ Id(S,x,a_0) \vee \ldots \vee Id(S,x,a_{n-1})\} \end{array}$$

But what does it mean, more precisely, to give $a_0,\ldots,a_{n-1} \in S$? It means that a is a function from $N(n)$, a set with n elements, into S, and $a_0,\ldots,a_{n-1}$ are its values.

It is easy to define a family of sets $N(n)$ *set* $[n : N]$ such that $N(0)$ has no elements and, for $n > 0$, the elements of $N(n)$ are $0_n, \ldots, (n-1)_n$. Then a singleton is the image of a function $a : N(1) \to S$, and a finite subset of S with n elements is the image of a function $a : N(n) \to S$. We thus put:

Definition 2.10 (Singletons and finite subsets) *For every set S, a subset U of S is said to be finite if U is extensionally equal to the image of some function $a \in N(n) \to S$, for some $n \in N$; more formally U is finite if*

$$(\exists z \in \Sigma(N, (n)\ N(n) \to S))\ (U =_S Im_{q(z)}[N(p(z))])\ true$$

In particular, the empty subset of S is also finite, being equal to the image of a function from $N(0)$ into S.

Given the above definition, the assertion "U is finite" is just a proposition with parameter U. This allows for instance to express rigorously in type theory a statement of the form "there exists a finite subset U_0 of U such that $\ldots U_0 \ldots$" by

$$(\exists z \in \Sigma(N, (n)\ N(n) \to S))\ (Im_{q(z)}[N(p(z))] \subseteq_S U\ \&\ \ldots Im_{q(z)}[N(p(z))] \ldots)$$

(a typical example is the definition of Stone cover in [S87]).

Proposition 2.11 *For any set S, if U is a finite subset of S, then either U is empty or there exist a natural number $n > 0$ and $a_0, \ldots, a_{n-1} \in S$ such that $U =_S \{a_0, \ldots, a_{n-1}\}$.*

Proof. The proof is nothing but working out definitions, using properties of finite sets, and fixing notation. U finite means that

$$(\exists z \in \Sigma(N, (n)\ N(n) \to S))\ (U =_S Im_{q(z)}[N(p(z))])\ true$$

If w is one of its verifications then $p(w) \in \Sigma(N, (n)\ N(n) \to S))$, and so $n \equiv p(p(w))$ is a natural number and $a \equiv q(p(w))$ is a function in $N(n) \to S$. Then $U =_S Im_a[N(n)]$ holds. If n is zero we have finished since $Im_a[N(n)]$ is empty. Otherwise, by definition of image, $x\ \epsilon_S\ Im_a[N(n)]\ true$ if and only if $(\exists i \in N(n))\ Id(S, a(i), x)\ true$. Then, writing a_i for $a(i_n)$, by the rule of $N(n)$-elimination we have

$$(x\ \epsilon_S\ Im_a[N(n)]) \leftrightarrow (Id(S, x, a_0) \vee Id(S, x, a_1) \vee \ldots \vee Id(S, x, a_{n-1}))\ true$$

as wished.

Set theoretic operations can be defined among finite subsets which give a finite subset as result. For instance, suppose that U and V are finite subsets determined by the elements c and d in $\Sigma(N, (n)\ N(n) \to S)$, i.e. $U =_S Im_{q(c)}[N(p(c))]$ and $V =_S Im_{q(d)}[N(p(d))]$. Then the union of U and V is the finite subset determined by $\langle p(c) + p(d), \lambda x.\ if\ x < p(c)\ then\ q(c)(x)\ else\ q(d)(x - p(c)) \rangle$. On the other hand, intersection between the finite subsets U and V, determined by

c and d, cannot be determined by an element in $\Sigma(N, (n)\ N(n) \to S)$ unless equality among elements of S is decidable. In fact, suppose that there exists a function g such that $g(c,d) \in \Sigma(N, (n)\ N(n) \to S)$ determines the finite subset which corresponds to the intersection of U and V. Then consider the case in which U and V are the singletons $\{a\}$ and $\{b\}$ for $a, b \in S$, i.e. U and V are determined by $\langle 1, \lambda x.a\rangle$ and $\langle 1, \lambda x.b\rangle$ in $\Sigma(N, (n)\ N(n) \to S)$ respectively. Then the subset determined by $g(\langle 1, \lambda x.a\rangle, \langle 1, \lambda x.b\rangle)$ is either a singleton or empty according to whether $Id(S, a, b)$ is true or not. Hence $p(g(\langle 1, \lambda x.a\rangle, \langle 1, \lambda x.b\rangle)) \in N$ is equal to 1 if and only if $Id(S, a, b)$ *true*, which allows to decide on the equality of a and b since equality in N is decidable[5].

Many usual properties of singletons and finite subsets are obtained by intuitionistic logic from the above definitions. We give the following proposition as a sample:

Proposition 2.12 *For any S set, $U \subseteq S$ and $a \in S$,*

$$a\ \epsilon_S\ U\ true\ \textit{iff}\ \{a\} \subseteq_S U\ true$$

Proof. Assume $a\ \epsilon_S\ U\ true$ and let $x\ \epsilon_S\ \{a\}\ true$; then $Id(S, x, a)\ true$, and hence by the rule of substitution on elements $x\ \epsilon_S\ U\ true$, so that, by $\subseteq_S$-introduction $\{a\} \subseteq_S U\ true$. Conversely if $\{a\} \subseteq_S U\ true$ then, by $\subseteq_S$-elimination, $a\ \epsilon_S\ U\ true$ because obviously $a\ \epsilon_S\ \{a\}\ true$.

However, some other common properties require new definitions to be expressed. An example is for instance $U =_S \bigcup_{a \epsilon_S U} \{a\}$, where the notion of union indexed over a subset is necessary (see section 2.9).

2.6 Finitary operations on subsets

One of the main reasons for the definition of subsets as propositional functions is that it allows to define operations on subsets with a subset as value. We begin with usual set-theoretic operations.

Definition 2.13 (Finitary operations on subsets) *For any $U, V \subseteq S$, we define*

$$\begin{array}{lrl} \textit{intersection}: & U \cap V & \equiv \{x \in S |\ U(x)\ \&\ V(x)\} \\ \textit{union}: & U \cup V & \equiv \{x \in S |\ U(x) \vee V(x)\} \\ \textit{implication}: & U \Rightarrow V & \equiv \{x \in S |\ U(x) \to V(x)\} \\ \textit{opposite}: & -U & \equiv \{x \in S |\ \neg U(x)\} \end{array}$$

[5] A solution to the problem of intersection exists, but it requires a more complex definition of finite subset, for which proposition 2.11 fails. The intuitive idea is that, given a finite set J and, for any $j \in J$, a finite set $I(j)$, a subset is finite if it is extensionally equal to the subset $\{x \in S |\ \bigvee_{j \in J}(\bigwedge_{i \in I(j)} x = a_{ji})\}$. More formally, the finite subsets are determined by the elements of the set $\Sigma(N, (n)\ \Sigma(N(n) \to N, (k)\ \Pi(N(n), (x)\ N(k(x)) \to S)))$. It can be shown that this definition reduces to the one in the main text if the equality of S is decidable.

Note the common pattern of the above definitions: an operation on subsets, i.e. propositional functions, is obtained by lifting (through abstraction) a connective acting on propositions. More formally, if $\bullet$ is a given connective, then the corresponding operation on subsets $\circ$ is defined by

$$\circ \equiv (S : set)(U : (x : S)\ prop)(V : (x : S)\ prop)(x : S)(U(x) \bullet V(x))$$

and hence $\circ : (S : set)(U : (x : S)\ prop)(V : (x : S)\ prop)(x : S)\ prop$. This is the direct link between "subset-theoretic" operations and intuitionistic logical connectives. It is also clear that all of the above operations on subsets respect extensional equality, by the logical metatheorem of replacement of equivalent propositions.

The following proposition tells that each of them can be characterized in terms of elements in the expected, traditional way:

Proposition 2.14 *For any $U, V \subseteq S$ and any $a \in S$, the following hold*

$$\begin{array}{rcl} a\ \epsilon_S\ U \cap V\ true & \textit{iff} & a\ \epsilon_S\ U\ \&\ a\ \epsilon_S\ V\ true \\ a\ \epsilon_S\ U \cup V\ true & \textit{iff} & a\ \epsilon_S\ U \vee a\ \epsilon_S\ V\ true \\ a\ \epsilon_S\ U \Rightarrow V\ true & \textit{iff} & a\ \epsilon_S\ U \rightarrow a\ \epsilon_S\ V\ true \\ a\ \epsilon_S\ {-U}\ true & \textit{iff} & \neg(a\ \epsilon_S\ U)\ true \end{array}$$

Proof. Under the assumption $a \in S$, the judgement $a\ \epsilon_S\ U \cap V\ true$ is equivalent to $((x : S)\ U(x)\ \&\ V(x))(a)\ true$, that is $U(a)\ \&\ V(a)\ true$, which in turn is equivalent to $a\ \epsilon_S\ U\ \&\ a\ \epsilon_S\ V\ true$ by the first ϵ-condition.

Exactly the same argument applies to all other operations.

Even if $a\ \epsilon_S\ U$ and $U(a)$ are logically equivalent under the assumption that $a \in S$, note that it is the use of the ϵ-notation which allows to make evident an intuitive content which otherwise would be completely hidden in the syntactic rule of reduction by which for instance $(U\&V)(a)$ and $U(a)\ \&\ V(a)$ are just equal expressions. This is one of the main reasons for introducing it.

As for inclusion and equality, the properties of operations on subsets are an immediate consequence of the properties of the corresponding logical connective used to define them.

The logical rules of &-elimination say that

$$U \cap V \subseteq_S U \text{ and } U \cap V \subseteq_S V$$

while by &-introduction it is immediate that

$$\frac{W \subseteq_S U \quad W \subseteq_S V}{W \subseteq_S U \cap V}$$

and thus $U \cap V$ is the infimum of U and V with respect to the partial order $\subseteq_S$.

Similarly, by the $\vee$-rules, we have

$$U \subseteq_S U \cup V \text{ and } V \subseteq_S U \cup V$$

and

$$\frac{U \subseteq_S W \quad V \subseteq_S W}{U \cup V \subseteq_S W}$$

which say that $U \cup V$ is the supremum of U and V.

If instead of rules we consider logical truths, then it is immediate that

associativity	$(U \cap V) \cap W$	$=_S$	$U \cap (V \cap W)$
commutativity	$U \cap V$	$=_S$	$V \cap U$
idempotency	$U \cap U$	$=_S$	U

hold, and that the same properties hold for $\cup$.

The link between $\Rightarrow$ and $\subseteq_S$, is given by

$$(U \Rightarrow V) =_S \top_S \quad \text{iff} \quad U \subseteq_S V$$

that is $(\forall x \in S)\ ((x\ \epsilon_S\ U \rightarrow x\ \epsilon_S\ V) \leftrightarrow \top)$ iff $(\forall x \in S)\ (x\ \epsilon_S\ U \rightarrow x\ \epsilon_S\ V)$, which is obvious because $(A \rightarrow B) \leftrightarrow \top$ is logically equivalent to $A \rightarrow B$, for any propositions A and B.

In general, the usual informal argument to prove a certain property of set-theoretic operations is perfectly reflected into a rigorous proof through intuitionistic logic.

2.7 Families of subsets and infinitary operations

We now turn to infinitary operations on subsets. The order of conceptual priority, however, is to deal before with families of subsets. The traditional notion of family of subsets has a simple definition in the present approach:

Definition 2.15 (Set-indexed family of subsets) *A family of subsets of S indexed by a set I is a propositional function $U : (i : I)(x : S)$ prop with two arguments, one in I and one in S. Applying U to an element i of I we obtain a propositional function $U(i)$ on elements of S, i.e. $U(i) \subseteq S$. Following traditional notation, given any $i \in I$, we put*

$$U_i \equiv U(i)$$

Hence the usual notation $(U_i)_{i \in I}$ can be used for a set-indexed family of subsets.

Infinitary operations are easily defined on set-indexed families of subsets. Just as propositional connectives were used to define unary and binary operations, now quantifiers are used to define infinitary operations.

Definition 2.16 (Infinitary operations on families) *For any set-indexed family $(U_i)_{i \in I}$ of subsets of S, we put:*

$$\textstyle\bigcup_{i \in I} U_i \equiv \{x \in S |\ (\exists i \in I)\ U(i, x)\} \equiv (x : S)(\exists i \in I)\ U(i, x)$$

$$\textstyle\bigcap_{i \in I} U_i \equiv \{x \in S |\ (\forall i \in I)\ U(i, x)\} \equiv (x : S)(\forall i \in I)\ U(i, x)$$

Clearly $\bigcup_{i\in I} U_i$ and $\bigcap_{i\in I} U_i$ are subsets of S. Moreover, they behave in the expected way with respect to elements:

Proposition 2.17 *For any set-indexed family $(U_i)_{i\in I}$ of subsets of S, and any $a \in S$:*

$$a \,\epsilon_S \bigcup_{i\in I} U_i \; true \quad \textit{iff} \quad (\exists i \in I)\; (a \,\epsilon_S\, U_i)\; true$$

$$a \,\epsilon_S \bigcap_{i\in I} U_i \; true \quad \textit{iff} \quad (\forall i \in I)\; (a \,\epsilon_S\, U_i)\; true$$

Proof. The proof is perfectly similar to the proof of proposition 2.14.

The standard properties of union are obtained, as expected, from logical properties of the existential quantifier. Given any set-indexed family of subsets $(U_i)_{i\in I}$, for any $j \in I$ the $\exists$-introduction rule gives

$$(\forall x \in S)\; (x \,\epsilon_S\, U_j \to (\exists i \in I)\; x \,\epsilon_S\, U_i)\; true,$$

which says that

$$\text{for all } j \in I, \quad U_j \subseteq_S \bigcup_{i\in I} U_i \tag{1}$$

Note that, since $U_j \subseteq_S \bigcup_{i\in I} U_i$ is a proposition and not a judgement, we could, more formally , express the above as $(\forall j \in I)\; (U_j \subseteq_S \bigcup_{i\in I} U_i)$.

Similarly, for any $x \in S$ and $W \subseteq S$, the rule of $\exists$-elimination

$$\frac{(\exists i \in I)\; x \,\epsilon_S\, U_i \; true \qquad \begin{array}{c}[i \in I, x \,\epsilon_S\, U_i \; true] \\ \vdots \\ x \,\epsilon_S\, W \; true\end{array}}{x \,\epsilon_S\, W \; true}$$

can be put in the form

$$\frac{(\forall i \in I)\; (x \,\epsilon_S\, U_i \to x \,\epsilon_S\, W)}{((\exists i \in I)\; x \,\epsilon_S\, U_i) \to x \,\epsilon_S\, W}$$

which says that

$$\frac{U_i \subseteq W \text{ for all } i \in I}{\bigcup_{i\in I} U_i \subseteq W} \tag{2}$$

Of course, the above two properties (1) and (2) say that union is the supremum of set-indexed families w.r.t. the order $\subseteq_S$.

An equivalent formulation of (1) and (2) together is

$$\bigcup_{i\in I} U_i \subseteq W \text{ iff for all } i \in I,\; U_i \subseteq W$$

which corresponds to

$$(\forall x \in S)\,((\exists i \in I)\, x \,\epsilon_S\, U_i) \to x \,\epsilon_S\, W \quad \text{iff} \quad (\forall i \in I)(\forall x \in S)\,(x \,\epsilon_S\, U_i \to x \,\epsilon_S\, W)$$

which is true by the intuitionistic laws of permutation of quantifers with implication. One can actually prove a somewhat stronger statement, namely

$$(\forall x \in S)\ (((\exists i \in I)\ (x\ \epsilon_S\ U_i) \to x\ \epsilon_S\ W) \leftrightarrow (\forall i \in I)\ (x\ \epsilon_S\ U_i \to x\ \epsilon_S\ W))$$

which can also be expressed in terms of subsets, as

$$(\bigcup_{i\in I} U_i \Rightarrow W) =_S \bigcap_{i\in I} (U_i \Rightarrow W)$$

and shows the use of the subset operation $\Rightarrow$.

Quite similarly, from the rules for $\forall$, one obtains that intersection is the infimum of a set-indexed family $(U_i)_{i\in I}$.

2.8 The power of a set

In this section some facts specific of the type of subsets of a set S, equipped with extensional equality, will be illustrated. Let us stress that the type we are considering is *not* the type of the propositional functions over S, even if a subset of S is the same as a propositional function over S. In fact, a type is determined both by its elements and its equality relation, and we do not consider intensional equality between propositional functions as in [ML84], but extensional equality as defined in definition 2.6.

First of all, we want to analyse the structure of $\mathcal{P}S$, equipped with finitary and infinitary operations, in algebraic terms. The fact that $\mathcal{P}S$ is equipped with extensional equality gives as a consequence that inclusion $\subseteq_S$ is a partial order on $\mathcal{P}S$.

Moreover, $(\mathcal{P}S, \cap)$ and $(\mathcal{P}S, \cup)$ are semilattices[6] because of the results in section 2.6. To show that $(\mathcal{P}S, \cap, \cup)$ is a lattice, we have to check that $\subseteq_S$ is the partial order induced by the semilattice operations $\cap$ and $\cup$, i.e.

$$U \cap V =_S U \text{ iff } U \subseteq_S V \text{ iff } U \cup V =_S V$$

The first equivalence is immediate by logic (and proposition 2.14) once we expand definitions into $(\forall x \in S)\ (x\ \epsilon_S\ U \cap V \leftrightarrow x\ \epsilon_S\ U)$ if and only if $(\forall x \in S)\ (x\ \epsilon_S\ U \to x\ \epsilon_S\ V)$. Similarly, the second equivalence holds because $A \vee B \leftrightarrow B$ iff $A \to B$, for any propositions A and B.

The next step is to show that $\mathcal{P}S$ is a complete lattice with respect to infinitary union and intersection. The traditional definition is that a lattice $\mathcal{L}$ is complete if any family $(f_i)_{i\in I}$, where I is a set, of elements of $\mathcal{L}$ has a supremum. To express this inside type theory, we lack only the definition of set-indexed family of elements in a type (or in a set):

Definition 2.18 (set-indexed family of elements) *Let C be any type or set. A set-indexed family of elements of C is a function f defined on a set I with values in C. As usual, the notation, $(f_i)_{i\in I}$, where $f_i \equiv f(i)$, is used.*

[6]Here and in the whole paper we adhere to the principle of adopting standard algebraic terminology for structures $(A, f_1, \ldots, f_n)$, where A is a type, and not necessarily a set.

We already used set-indexed family of elements of a type within this paper in section 2.7, where we introduced the notion of set-indexed family of subsets of a set. In general, the foundational reason for introducing set-indexed families of elements of a type is that they allow to give a meaning to quantification over the elements of some sub-types. In fact, given a function f from the set I into the type C, the quantification over the image of f is reduced to a quantification over the set of indexes I. An example coming from mathematical practice is in [SVV96], where we introduced set-based Scott domains, i.e. Scott domains such that the type of compact elements can be indexed by a set.

Now, the definition of complete lattice in our approach is literally as above, but one must be careful that it has a different meaning according to the foundational attitude. In the classical view, any sub-type of $\mathcal{P}S$ can be indexed by a set, while we expect this to be false in type theory. We believe, however, that from a computational point of view it is necessary, but in the same time sufficent, to consider only families of subsets which are set-indexed.

Hence $\mathcal{P}S$ is a complete lattice because we have shown in section 2.7 that any set-indexed family of subsets has both supremum and infimum. It is now easy to prove also:

Theorem 2.19 *For any set S, $\mathcal{P}S = \langle \mathcal{P}S, \cap, \bigcup, \top_S, \bot_S \rangle$ is a frame (alias locale, complete Heyting algebra).*

Proof. After the preceding results, it remains to be proved only that infinitary union distributes over intersection, that is:

$$(\bigcup_{i \in I} U_i \cap W) =_S \bigcup_{i \in I} (U_i \cap W)$$

It is immediate to see that this correspond exactly to a logical law of quantifier shifting, namely $(\forall x \in S)\,((\exists i \in I)\, x \,\epsilon_S\, U_i \,\&\, x \,\epsilon_S\, W \leftrightarrow (\exists i \in I)\,(x \,\epsilon_S\, U_i \,\&\, x \,\epsilon_S\, W))$.

As an example of how a classical theorem is rendered in our notion of power of a set, we give here a constructive version of Cantor's diagonalization theorem:

Theorem 2.20 (Cantor's diagonalization) *Let S be any set. Then for any set-indexed family $(F_x)_{x \in S}$ of subsets of S, there is a subset $D_F \subseteq S$ which is extensionally different from F_x for any $x \in S$.*

Proof. Given the family $(F_x)_{x \in S}$, i.e. $F(x, y)$ *prop* $[x : S, y : S]$, put

$$D_F \equiv (y : S)\ \neg F(y, y)$$

that is $D_F(y) \equiv \neg F(y, y)$. For any $x \in S$, $D_F =_S F_x$ would mean that $(\forall y \in S)\ \neg F(y, y) \leftrightarrow F(x, y)$, which for $y = x$ would give $\neg F(x, x) \leftrightarrow F(x, x)$, which is a contradiction. So for any $x \in S$, it is $\neg(D_F =_S F_x)$

2.9 Quantifiers relative to a subset

The meaning of quantification over a subset U of a set S is that the range of quantification is restricted to elements of U, rather than all elements of S. A common definition in pure logic is that of quantifiers relative to a property; the idea is to adapt it to type theory in such a way to make it visible that U is considered as the domain of quantification.

Definition 2.21 (Quantifiers relative to a subset) *Let S set and $U \subseteq S$. Then, for any propositional function $A(x)$ prop $[x : S, x\ \epsilon_S\ U\ true]$ we put:*

$$(\forall x\ \epsilon_S\ U)\ A(x) \equiv (\forall x \in S)\ (x\ \epsilon_S\ U \rightarrow A(x))$$
$$(\exists x\ \epsilon_S\ U)\ A(x) \equiv (\exists x \in S)\ (x\ \epsilon_S\ U\ \&\ A(x))$$

The operators $(\forall x\ \epsilon_S\ U)$ and $(\exists x_S\ \epsilon_S\ U)$ are called, respectively, the universal and existential quantifier relative to U.

Note that the above definition makes use of the fact, specific to type theory, that $A \rightarrow B$ and $A\ \&\ B$ are propositions provided that A is a proposition and B is a proposition under the assumption that A is true.

It is an easy matter now to check that quantifiers relative to a subset U obey to rules completely similar to those for quantifiers in intuitionistic logic, but with explicit mention of the domain of quantification, as in [ML84]:

$\forall$-introduction

$$\frac{\begin{array}{c}[x\ \epsilon_S\ U\ true] \\ | \\ A(x)\ true\end{array}}{(\forall x\ \epsilon_S\ U)\ A(x)\ true}$$

$\forall$-elimination

$$\frac{a\ \epsilon_S\ U\ true \quad (\forall x\ \epsilon_S\ U)\ A(x)\ true}{A(a)\ true}$$

$\exists$-introduction

$$\frac{a\ \epsilon_S\ U\ true \quad A(a)\ true}{(\exists x\ \epsilon_S\ U)\ A(x)\ true}$$

$\exists$-elimination

$$\frac{(\exists x\ \epsilon_S\ U)\ A(x)\ true \qquad \begin{array}{c}[x\ \epsilon_S\ U\ true, A(x)\ true] \\ | \\ C\ true\end{array}}{C\ true}$$

Such rules are only abbreviations for deductions in type theory. For instance,

the $\forall$-introduction rule relativized to U is an abbreviation of

$$\dfrac{\dfrac{\dfrac{S\ set \quad U \subseteq S \quad [x \in S]_2}{x\ \epsilon_S\ U\ prop}}{[x\ \epsilon_S\ U\ true]_1}}{\dfrac{A(x)\ true}{x\ \epsilon_S\ U \rightarrow A(x)\ true}\ 1}\ 2$$

Once we have access to quantifiers relative to subsets, many of the notions defined on sets can be extended to subsets in a straightforward way; we now see the case of arbitary unions and intersections. Before that, the notion of set-indexed family of subsets must be generalized to subset-indexed families.

Definition 2.22 (Subset-indexed family of subsets) *Let S set, I set and $U \subseteq I$. Then a propositional function $V : (i : I)(y : U(i))(x : S)$ prop is said to be a family of subsets of S indexed on the subset U if the truth of $V(i, y, x)$ does not depend on y, i.e. $V(i, y_1) =_S V(i, y_2)$ for any $y_1, y_2 \in U(i)$; then one can hide the variable y and write*

$$V_i \subseteq S\ [i\ \epsilon_I\ U\ true].$$

The infinitary operations of union and intersection are immediately extended to subset-indexed families of subsets, simply by replacing quantifiers with quantifiers relative to a subset. So, if $V_i \subseteq S\ [i\ \epsilon_I\ U\ true]$, we put

$$\begin{array}{rcl} \bigcup_{i\epsilon_I U} V_i & \equiv & \{x : S |\ (\exists i\ \epsilon_I\ U)\ x\ \epsilon_S\ V_i\} \\ & \equiv & (x : S)(\exists i \in I)\ (i\ \epsilon_I\ U\ \&\ x\ \epsilon_S\ V_i) \end{array}$$

and

$$\begin{array}{rcl} \bigcap_{i\epsilon_I U} V_i & \equiv & \{x : S |\ (\forall i\ \epsilon_I\ U)\ x\ \epsilon_S\ V_i\} \\ & \equiv & (x : S)(\forall i \in I)\ (i\ \epsilon_I\ U \rightarrow x\ \epsilon_S\ V_i) \end{array}$$

As an exercise, we can prove here the property we left out in section 2.5.

Proposition 2.23 *For any S set and $U \subseteq S$,*

$$U =_S \bigcup_{i\epsilon_S U} \{i\}$$

Proof. The subset-indexed family is of course $\{i\} \subseteq S\ [i\ \epsilon_S\ U]$, that is $Id(S, x, i)$ *prop* $[i : S, U(i)\ true, x : S]$. For any $x \in S$, by definitions and intuitionistic logic we have $x\ \epsilon_S\ \bigcup_{i\epsilon_S U}\{i\}$ *true* iff $(\exists i\ \epsilon_S\ U)\ x\ \epsilon_S\ \{i\}$ *true* iff $(\exists i\ \epsilon_S\ U)\ Id(S, x, i)$ *true* iff $(\exists i \in S)\ i\ \epsilon_S\ U\ \&\ Id(S, x, i)$ *true* iff $x\ \epsilon_S\ U$ *true*.

We propose a second exercise: prove that if $U \subseteq_I W$ and $V_i \subseteq S\ [i : I]$, then

$$\bigcup_{i\epsilon_I U} V_i \subseteq_S \bigcup_{i\epsilon_I W} V_i$$

A similar result holds also in the weaker assumption $V_i \subseteq S\ [i\ \epsilon_I\ W]$, but with a more complicated statement and proof.

2.10 Image of a subset and functions defined on a subset

The idea of relativized quantifiers, makes it natural to extend to subsets also the notion of image of a set:

Definition 2.24 (Image of a subset) *Let S and I be sets. Then, given any function $f(i) \in S\ [i : I]$ and any subset U of I, the subset of S defined by:*

$$\begin{array}{rcl} f[U] & \equiv & \{x \in S|\ (\exists i\ \epsilon_I\ U)\ Id(S, f(i), x)\} \\ & \equiv & (x : S)(\exists i \in I)\ (i\ \epsilon_I\ U\ \&\ Id(S, f(i), x)) \end{array}$$

is called the image of U along f. An alternative notation for $f[U]$ is $\{f(x)|\ U(x)\}$. More generally, given a function $f(x_1, \ldots, x_n) \in S\ [x_1 : I_1, \ldots, x_n : I_n]$ and a relation $R(x_1, \ldots, x_n)$ prop $[x_1 : I_1, \ldots, x_n : I_n]$, both with n arguments, the image of R along f is defined by

$$Im_f[R] \equiv (x : S)(\exists i_1 \in I_1) \ldots (\exists i_n \in I_n)\ (R(i_1, \ldots, i_n)\ \&\ Id(S, f(i_1, \ldots, i_n), x))$$

Alternative notations for $Im_f[R]$ include $f[R]$ and $\{f(x_1, \ldots, x_n)|\ R(x_1, \ldots, x_n)\}$.

Of course, if U is the trivial subset $\top_I$, then $f[\top_i] =_S Im_f[I]$. In general, all the expected properties can easily be checked. For instance, for any $U, V \subseteq I$,

$$\frac{U \subseteq_I V}{f[U] \subseteq_S f[V]}$$

follows immediately from definitions by intuitionistic logic. Another instructive exercise is to realize that $f[U] \equiv \cup_{i \epsilon_I U}\{f(i)\}$.

It is also worthwhile to notice that the image $f[U]$ is always extensionally equal to the image $Im_g[J]$ of some set J along some function g: it is enough to consider $J \equiv \Sigma(I, U)$ and $g \equiv \lambda x.f(p(x))$.

If n subsets $U_1 \subseteq I_1, \ldots, U_n \subseteq I_n$ are given, then the image of $U_1, \ldots, U_n$ under f is obtained as a special case, by putting

$$R(i_1, \ldots, i_n) \equiv i_1\ \epsilon_{I_1}\ U_1\ \& \ldots \&\ i_n\ \epsilon_{I_n}\ U_n$$

For instance, given an operation $\cdot : S^2 \to S$, and writing as usual $b \cdot c$ for $\cdot(b, c)$, the image of the two subsets $U, V \subseteq S$ is the subset

$$(x : S)(\exists b, c \in S)\ (b\ \epsilon_S\ U\ \&\ c\ \epsilon_S\ V\ \&\ Id(S, x, b \cdot c))$$

that is

$$(x : S)(\exists b\ \epsilon_S\ U)(\exists c\ \epsilon_S\ V)\ Id(S, x, b \cdot c)$$

which, following the above conventions, is written also $\{b \cdot c|\ b\ \epsilon_S\ U, c\ \epsilon_S\ V\}$ or $\cdot[U, V]$; it is the latter notation which gives raise to $U \cdot V$, which is the standard

notation for such subset used in algebra to mean, for instance, the product of ideals $I \cdot J$ or of subgroups $H \cdot K$, and which we found useful in formal topology.

The notion of function itself can be relativized to a subset in the following sense:

Definition 2.25 (Function defined on a subset) *If S is a set, I is a set and $U \subseteq I$, a function of two arguments $f(i, y) \in S$ $[i : I, y : U(i)]$ is said to be a function from U to S, if the value $f(i, y)$ does not depend on y, that is if $(\forall y, y' \in U(i))Id(S, f(i, y), f(i, y'))$ true; then one can hide the variable y and write simply*

$$f(i) \in S \ [i \ \epsilon_I \ U \ true].$$

The intuitive content of such definition is that, just like the notion of element of a subset U is obtained by "forgetting" the witness y of $U(i)$, so a function f relativized to U is obtained by "forgetting" the second argument of the input. This of course can be done only when the specific value of y is irrelevant for the computation of $f(i, y)$, i.e. when $f(i, y)$ and $f(i, y')$ have the same value for any $y, y' \in U(i)$ as required above.

A similar definition can be given also when f is a function from I and $U(i)$ *set* $[i : I]$ into a type C. In this case, to express the fact that f does not depend on the second argument, the equality in C must be used instead of propositional equality, and thus, in general, the condition can not be expressed by a proposition.

Extending the previous terminology to funtions defined on subsets, a function $f(i) \in C$ $[i \ \epsilon_I \ U]$ is also called a *subset-indexed family* of elements of C. The remark following definition 2.18 applies here equally well. Again, examples are to be found in [SVV96].

3 Farewell

We believe the reader can not but agree that the technical development so far has been quite simple to read. And indeed a useful tool must be simple, so that it is easy to use it (even when difficult to build!).

It is even possible that he has forgotten, as we envisaged in section 1.2, the substantial novelty, namely that all of what we did is inside type theory. And type theory is certainly a warranty for at least twenty-five years.

As always with a tool, however, the right way to judge if it works well is just to use it in practice. The reader can try his hand with some pieces of actual mathematics (as we did with formal topology) or, according to his taste, he can enrich the toolbox itself. We would appreciate a good theory of quotients!

References

[B80] N.G. de Bruijn, *A survey of the project Automath.*, in "To H. B. Curry: Essays on Combinatory Logic, Lambda Calculus and For-

malism", eds J.P. Seldin and J.R. Hyndley, Academic Press, London, 1980, pp. 589-606.

[F92] G. Frege, *Über Sinn und Bedeutung*, Zeitschrift für Philosophie und philosophische Kritik, 1892, pp.25-50.

[H80] W. A. Howard, *The formulae-as-types notion of construction*, in: To H.B. Curry: Essays on combinatory Logic, Lambda Calculus and Formalism, R. Hindley and J.P. Seldin, eds., Academic Press, London 1980, pp. 479-490.

[ML84] P. Martin-Löf, "Intuitionistic type theory", notes by Giovanni Sambin of a series of lectures given in Padua, June 1980, Bibliopolis, Neaples 1984.

[NPS90] B. Nordström, K. Petersson, J. M. Smith, "Programming in Martin-Löf's Type Theory, an introduction", Clarendon Press, Oxford 1990.

[PV93] Paulus Venetus (alias G. Sambin - S. Valentini) *Propositum Cameriniense, sive etiam itinera certaminis ... (italian)*, in: Atti degli Incontri di Logica Matematica vol. viii (XV Incontro), G. Gerla, C. Toffalori, S. Tulipani eds. , Camerino 1993, pp. 115-143.

[S87] G. Sambin, *Intuitionistic formal spaces - a first communication*, in: Mathematical Logic and its Applications, D. Skordev ed., Plenum, New York 1987, pp. 187-204.

[S91] G. Sambin, *Per una dinamica nei fondamenti (italian)*, in: Atti del Congresso "Nuovi problemi della logica e della filosofia della scienza", vol. II, G. Corsi, G. Sambin eds., CLUEB, Bologna 1991, pp.163-210.

[S97] G. Sambin, *Developing topology in a type theoretic setting*, to appear.

[SV93] G. Sambin, S. Valentini, *Building up a tool-box for Martin-Lf's type theory (abstract)*, in: G. Gottlob, A. Leitsch, D. Mundici eds., Computational Logic and Proof Theory. Proceedings of the Third Kurt Gödel Colloquium, KGC'93, Lecture Notes in Computer Science, Springer, Berlin-Heidelberg-New York, 1993, pp. 69-70

[SVV96] G. Sambin, S. Valentini, P. Virgili, *Constructive Domain Theory as a branch of Intuitionistic Pointfree Topology*, Theoretical Computer Science, 159 (1996), pp. 319-341.

[V96] S. Valentini, *Decidability in Intuitionistic Type Theory is functionally decidable*, Mathematical Logic Quarterly 42 (1996), pp. 300-304.

[V97] S. Valentini, *The forget-restore principle: a paradigmatic example*, to appear.