Finiteness in a Minimalist Foundation

Francesco Ciraulo[1] and Giovanni Sambin[2]

[1] Università di Palermo, Dipartimento di Matematica ed Applicazioni,
Via Archirafi 34, 90123 Palermo, Italy
ciraulo@math.unipa.it
http://www.math.unipa.it/∼ciraulo
[2] Università di Padova, Dipartimento di Matematica Pura ed Applicata,
Via Trieste 63, 35121 Padova, Italy
sambin@math.unipd.it
http://www.math.unipd.it/∼sambin/

Abstract. We analyze the concepts of finite set and finite subset from the perspective of a minimalist foundational theory which has recently been introduced by Maria Emilia Maietti and the second author. The main feature of that theory and, as a consequence, of our approach is compatibility with other foundational theories such as Zermelo-Fraenkel set theory, Martin-Löf's intuitionistic Type Theory, topos theory, Aczel's CZF, Coquand's Calculus of Constructions. This compatibility forces our arguments to be constructive in a strong sense: no use is made of powerful principles such as the axiom of choice, the power-set axiom, the law of the excluded middle.

Keywords: minimalist foundation, finite sets, finite subsets, type theory, constructive mathematics.

1 Introduction

The behaviour of a mathematical object and the properties it possesses are influenced by the foundational assumptions one accepts. That is true also for the apparently clear concepts of finite set and finite subset of a given set. For this reason, it seems interesting to know a stock of properties about finiteness which are true in all foundational theories (or, at least, in the most used ones).

Maria Emilia Maietti and the second author have recently proposed (see [5]) a foundational theory which is "minimalist" in the sense that it can be seen as the common core of some of the most used foundations, namely, Zermelo-Fraenkel set theory, topos theory, Martin-Löf's Type Theory, Aczel's CZF, Coquand's Calculus of Constructions. A peculiarity of this minimalist foundation is that it is based on two levels of abstraction: an extensional theory to develop mathematics in more or less the usual informal way (see [4]) and an underlying intensional type theory called "minimal Type Theory" ("mTT" from now on) on which mathematics is formalized (see [5]). Therefore, our task of speaking about finiteness independently from foundations acquires a more precise form: to study finiteness from the perspective of this minimalist foundation, and hence

M. Miculan, I. Scagnetto, and F. Honsell (Eds.): TYPES 2008, LNCS 4941, pp. 51–68, 2008.

eventually in terms of mTT. Accomplishing this task is the aim of the present paper.

Thanks to the reasons explained above, the definitions and results in the present paper are constructive in a strong sense: no use is made of powerful principles such as the axiom of choice, the power-set axiom, the principle of excluded middle. In fact, each of these principles breaks compatibility with at least one of the above foundational theories.

The present work can be seen as a sequel to [9] because all the definitions and properties stated there, even if originally intended for Martin-Löf's theory, remain valid when viewed from the point of view of mTT since they do not need any application of the axiom of choice. For the same reason, a large part of [6] and [8] can be read as an explanation of the formal system mTT. For all those notions which are used but not explained in this paper, we refer to [5] and [6].

2 Minimal Type Theory: A Brief Introduction

The type theory mTT can be formalized as a variant of Martin-Löf's theory (see [6] and [8]); thus we feel free to use all the standard notation developed for Type Theory, mainly, the set constructors Σ and Π. The main difference between the two systems is that mTT identifies each proposition with a particular set (namely the set of all its proofs), but not the converse which Martin-Löf's theory does, instead. That implies that the usual identification between logical constants and set constructors cannot be performed any longer. In other words, in mTT every logical constant needs an independent definition; for example, the always false proposition, written $\bot$, has to be kept distinct from $N(0)$ (the set with no elements; see below) simply because $N(0)$ is not a proposition. As a consequence, the axiom of choice is no longer provable in mTT.[1] To see this, let us briefly explain the difference between $(\Sigma\ x \in A)B(x)$ (disjoint union) and $(\exists\ x \in A)$ $B(x)$ (existential quantifier) in mTT. Both are sets, but only the latter is a proposition. Their formation and introduction rules are formally the same, but their elimination rules, namely

$$\frac{\begin{array}{c}[z \in (\Sigma\ x \in A)B(x)]\\ \vdots \\ C(z)\ set\end{array} \qquad d \in (\Sigma\ x \in A)B(x) \quad \begin{array}{c}[x \in A,\ y \in B(x)]\\ \vdots \\ m(x,y) \in C(< x, y >)\end{array}}{El_{\Sigma}(d,m) \in C(d)} \tag{1}$$

$$\frac{C\ prop \quad d \in (\exists\ x \in A)B(x) \qquad \begin{array}{c}[x \in A,\ y \in B(x)]\\ \vdots \\ m(x,y) \in C\end{array}}{El_{\exists}(d,m) \in C}\ \exists\text{ - elimination} \tag{2}$$

[1] Note that the absence of the axiom of choice is necessary to keep compatibility with topos theory (see [5] for more details).

differ because the proposition C in the $\exists$-elimination rule cannot depend on a proof of $(\exists\ x \in A)B(x)$. This apparently small limitation is enough to make the axiom of choice non-deducible. Here for " the axiom of choice" we mean the following proposition:

$$(\forall x \in A)(\exists y \in B(x))C(x,y) \rightarrow (\exists f \in (\Pi\ x \in A)B(x))(\forall x \in A)C(x, f(x)) \quad (3)$$

(where $f(x)$ stands for $Ap(f,x)$, the element of $B(x)$ which is obtained by applying the function f to the input x in A). On the contrary, the set

$$(\Pi x \in A)(\Sigma x \in B(x))C(x,y) \rightarrow (\Sigma f \in (\Pi x \in A)B(x))(\Pi x \in A)C(x, f(x)) \quad (4)$$

can be proved to be inhabited. The reason for that stands in the fact that the second (or right) projection can be defined with respect to Σ, but not with respect to $\exists$. Provided that c is an element of $(\Sigma\ x \in A)B(x)$ (respectively $(\exists x \in A)B(x)$), then the first (or left) projection, written $p(c)$ is the element $El_{\Sigma}(c,m)$ (respectively $El_{\exists}(c,m)$) obtained by elimination with A in place of C and x in place of $m(x,y)$; of course, $p(< a,b >) = a$ by equality. The second projection is obtained, in the case of Σ, by taking $m(x,y)$ to be y; this forces $C(x)$ to be $B(x)$. Hence, this technique cannot be used in the case of $\exists$.

Summing up, from a proof $c \in (\exists x \in A)B(x)$ we are able to construct an element $p(c) \in A$ which, from a metalinguistic level, can be seen to satisfy B; nevertheless, we are not able to construct a proof of $B(p(c))$ within the system mTT. This fact is intimately related to the fact that, even if the axiom of choice is non-deducible within the system, it in fact holds on a metalinguistic level as long as the pure system mTT is considered; this happens because of our constructive interpretation of quantifiers. Of course, not all the extensions of mTT (e.g. topos theory) share this property and hence we cannot expect to prove the axiom of choice within our system.

By the way, note that the usual logical rule of $\exists$-elimination can be obtained from the above one by suppressing all proof terms; so:

$$\frac{C\ prop \quad (\exists\ x \in A)B(x)\ true \quad \begin{array}{c}[x \in A,\ B(x)\ true]\\ \vdots \\ C\ true\end{array}}{C\ true}\ \text{logical } \exists \text{ - elimination.} \quad (5)$$

This rule says that if we want to infer C (which does not depend on $x \in A$) from $(\exists x \in A)B(x)$, then we can assume to have an arbitrary $x \in A$ and a proof of $B(x)$; of course, that does not mean we are using first and second projection.

We take the occasion to warn the reader that we will often use $a =_S b$, or simply $a = b$, instead of the proposition $Id(S,a,b)$, provided that S is a set; this proposition, however, has to be kept distinct from the judgement $a = b \in S$. Provided that $A\ set$, $B\ set$, $f \in A \rightarrow B$ and $a \in A$ we often write $f(a)$ instead of $Ap(f,a)$.

3 A Constructive Concept of Finiteness

In the framework of mTT, like in other constructive approaches, a collection of objects is called a set when, roughly speaking, we have rules to construct such objects; we reserve the word "element" for an object of a set. It is common practice to distinguish intensional sets from extensional sets (also called setoids) which are (intensional) sets endowed with an equivalence relation. Even if the definitions in the present paper are formulated with regard to sets, they can easily been extended to setoids: it is enough to replace the propositional equality by the equivalence relation of the setoid. Thus the natural framework to set the following results should be the extensional level of the minimal type theory (see [4]).

An example of (intensional) set is N, the set of formal natural numbers.

N-formation

$$\frac{}{N\ set} \tag{6}$$

N-introduction

$$\frac{}{0 \in N} \qquad \frac{n \in N}{s(n) \in N} \tag{7}$$

N-elimination

$$\frac{\begin{array}{c}[z \in N]\\ \vdots \\ C(z)\ set\end{array} \quad c \in N \quad d \in C(0) \quad \begin{array}{c}[x \in N,\ y \in C(x)]\\ \vdots \\ e(x,y) \in C(s(x))\end{array}}{R(c,d,e) \in C(c)} \tag{8}$$

The programm R (for "recursion") performs the following steps. Firstly, it brings c to its canonical form, that will be either 0 or $s(n)$ for some $n \in N$. In the first case it returns $d \in C(0)$ (or, better, the canonical element produced by d); in the second case it evaluates $R(n,d,e)$ and then it computes $e(n, R(n,d,e))$.

N-equality

$$\frac{d \in C(0) \quad \begin{array}{c}[x \in N,\ y \in C(x)]\\ \vdots \\ e(x,y) \in C(s(x))\end{array}}{R(0,d,e) = d \in C(0)} \qquad \frac{n \in N \quad d \in C(0) \quad \begin{array}{c}[x \in N,\ y \in C(x)]\\ \vdots \\ e(x,y) \in C(s(x))\end{array}}{R(s(n),d,e) = e(n, R(n,d,e)) \in C(s(n))} \tag{9}$$

As usual, we write $s^n(0)$ (n an informal natural number) for the canonical element of N which is obtained from 0 by n applications of s. Thus $s^n(0)$ is a shorthand for the formal expression which represents the informal natural number n. When no confusion arises, we will use the symbol n instead of the formal natural number $s^n(0)$. Note that, provided that n and m are two different informal natural numbers, surely the proposition $Id(N, s^n(0), s^m(0))$ cannot be proved within the system, as it is clear by an easy metalinguistic investigation.

Nevertheless neither the proposition $\neg Id(N, s^n(0), s^m(0))$ is deducible, unless the first universe (also called the set of small sets) is defined (actually the boolean universe defined in [4] is enough).

Once the above rules are given, one can define addition in the usual recursive way: let the value of $e(x, y)$ be $s(y)$; then the element $R(b, a, e)$ is what is called $a + b$. Moreover, one can define $a \leq b$ as $(\exists c \in N)(a + c = b)$, where $x = y$ is the proposition $Id(N, x, y)$. Of course, the standard product and a limited subtraction, such as all other recursive functions, can be defined in the standard way.

Another example is the definition of $N(k)$, the standard set with k elements.

$N(k)$**-formation**

$$\frac{k \in N}{N(k)\ set} \qquad \frac{k = k' \in N}{N(k) = N(k')} \tag{10}$$

$N(k)$**-introduction**

$$\frac{n \in N \quad n < k\ true}{n_k \in N(k)} \qquad \frac{n = m \in N \quad n < k\ true}{n_k = m_k \in N(k)} \tag{11}$$

These rules introduce the k canonical elements of the set $N(k)$, namely, 0_k, $(s(0))_k$, $\ldots$, $(s^{k-1}(0))_k$, which, for the sake of brevity, we write 0_k, 1_k, $\ldots$, $(k-1)_k$.

$N(k)$**-elimination**

$$\frac{\begin{array}{c}[z \in N(k)] \\ \vdots \\ C(z)\ set\end{array} \quad c \in N(k) \quad \begin{array}{c}[n \in N,\ n < k\ true] \\ \vdots \\ c_n \in C(n_k)\end{array}}{R_k(c, c_0, \ldots, c_{k-1}) \in C(c)} \tag{12}$$

where R_k is the function that brings c to its canonical form, that will be a certain n_k for some $n < k$, and hence picks the corresponding c_n.

$N(k)$**-equality**

$$\frac{\begin{array}{c}[z \in N(k)] \\ \vdots \\ C(z)\ set\end{array} \quad n \in N \quad n < k\ true \quad \begin{array}{c}[x \in N,\ x < k\ true] \\ \vdots \\ c_x \in C(x_k)\end{array}}{R_k(n_k, c_0, \ldots, c_{k-1}) = c_n \in N(k)} \ . \tag{13}$$

Note that, for $n \in N$ it is possible to prove by induction the proposition $(n < k) \to (n = 0) \vee (n = 1) \vee \ldots (n = (k-1))$, provided that $k \in N$ is fixed. Thus for $x \in N(k)$, it is possible to prove the proposition $(x = 0_k) \vee (x = 1_k) \vee \ldots \vee (x = (k-1)_k)$. This implies that every quantification over $N(k)$ can be replaced by a finite conjunction or disjunction. More precisely, a proposition of the form $(\forall x \in N(k))P(x)$ is equivalent to $P(0_k)\ \&\ P(1_k)\ \&\ \ldots\ \&\ P((k-1)_k)$, while $(\exists x \in N(k))P(x)$ is the same as $P(0_k) \vee \ldots \vee P((k-1)_k)$.

Even if the axiom of choice is not deducible within the system mTT, nevertheless it holds with respect to the sets of the form $N(k)$, in the sense of the following proposition.

Proposition 1. *Let $k \in N$ and $S(x)$ set $[x \in N(k)]$; then the proposition*

$$(\forall x \in N(k))(\exists a \in S(x))P(x,a) \rightarrow (\exists f \in T)(\forall x \in N(k))P(x, f(x)) \tag{14}$$

is deducible, where T is $(\Pi\ x \in N(k))S(x)$.

Proof. Let $Q(x)$ be $(\exists a \in S(x))P(x,a)$; then $(\forall x \in N(k))Q(x)$ is equivalent to $Q(0_k)$ & ... & $Q((k-1)_k)$. Thus, we can replace $(\forall x \in N(k))Q(x)$ with the k assumptions $(\exists a \in S(n_k))P(n_k, a)$, $n = 0, \ldots, k-1$. By $\exists$-elimination k times, we can assume $P(0_k, a_0)$, ..., $P((k-1)_k, a_{k-1})$, where each a_i is an element of $S(i_k)$, $i = 0, \ldots, k-1$. By $N(k)$-elimination, we can construct a family $R(x, a_0, \ldots, a_{k-1}) \in S(x)$ and then a function $f \in (\Pi\ x \in N(k))S(x)$, where f is $\lambda x.R(x, c_0, \ldots, c_{k-1})$, such that $P(x, f(x))$ holds for all $x \in N(k)$. Thus the proposition $(\exists f \in (\Pi\ x \in N(k))S(x))(\forall x \in N(k))P(x, f(x))$ can be inferred from $P(n_k, a_n)$, $n = 0, \ldots, k-1$ and then, since it does not depend on any a_n, directly from $(\exists a \in S(x))P(x,a)$, $x \in N(k)$.

A classical definition says that a set is finite if it is not infinite, where it is infinite if there exists a one-to-one correspondence between it and one of its proper subsets. An alternative way is to consider the sets of the form $N(k)$ as prototypes of the finite sets and, hence, to call a set finite if it is in a bijective correspondence with $N(k)$, for some $k \in N$. That is just the definition given by Brouwer in [3] and then by Troelstra and van Dalen in [10]. Of course, several other notions are possible (see section 5; see also [11]). For example, following [3], we could say that a set is (numerically) bounded if it cannot have a subset of cardinality n, for some natural number n. Otherwise, following [10], we could say that a set is finitely indexed or finitely enumerable or listable if there exists a surjective function from some $N(k)$ onto it.

From a classical point of view, that is in the framework of Zermelo-Fraenkel set theory with choice, the above definitions turn out to be all equivalent; the same does not happen in other foundations (see [11] for counterexamples in intuitionistic mathematics). So we have to make a choice; of course, we look for the most simple, natural and effective one. What we do is to adopt the following (see "finitely indexed" in [10]). Provided that A *set*, B *set* and $f \in A \rightarrow B$ we write $f(A) = B$ for the proposition $(\forall b \in B)(\exists a \in A)Id(B, b, Ap(f, a))$; in other words, $f(A) = B$ *true* is the judgement "f is surjective".

Definition 1 (finite set). *Let S be a set; S is said to be* finite *if the proposition $(\exists k \in N)(\exists f \in N(k) \rightarrow S)(f(N(k)) = S)$, which we shortly denote by* $\mathrm{Fin}(S)$, *is true.*

Proposition 2. *If I is a finite set and $(\exists g \in I \rightarrow S)(g(I) = S)$ is true, then S is finite.*

Proof. The proof is quite obvious; however we give a sketch of it in order to show that it can be carried out within mTT. By $\exists$-elimination (twice) on $\mathrm{Fin}(I)$, we can assume $k \in N$, $f \in N(k) \rightarrow I$ and $f(N(k)) = I$. Again by $\exists$-elimination, we can assume $g \in I \rightarrow S$ and $g(I) = S$. The function $\lambda x.g(f(x)) \in N(k) \rightarrow S$ is surjective and thus $\mathrm{Fin}(S)$ is true, regardless of the particular k, f and g.

It is possible to give also the notion of unary set, i.e. a set with at most one element. Trivially, every unary set is finite too.

Definition 2 (unary set). *Let S be a set; we say that S is* unary *if the proposition* $(\exists k \in N)(k \leq s(0)\ \&\ (\exists f \in N(k) \rightarrow S)(f(N(k)) = S))$ *is true.*

Given a set I and a set-indexed family of sets $S(i)$ *set* $[i \in I]$, it is possible to construct their *indexed sum* (or *disjoint union*), written $(\Sigma\ i \in I)S(i)$. Its canonical elements are couples of the kind $< i, a >$ with $i \in I$ and $a \in S(i)$. The following lemma and the subsequent proposition say that finite sets have the expected behavior with respect to indexed sums.

Lemma 1. *Let $k \in N$ and $n(x) \in N[x \in N(k)]$; then $(\Sigma\ x \in N(k))N(n(x))$ is finite.*

Proof. Let $m = n(0_k) + n(1_k) + \ldots + n((k-1)_k) \in N$ and consider the function $f \in N(m) \rightarrow (\Sigma\ x \in N(k))N(n(x))$ defined by the following m conditions:

$$\begin{array}{ccc}
0_m & \longmapsto & < 0_k\ ,\ 0_{n(0_k)} > \\
1_m & \longmapsto & < 0_k\ ,\ 1_{n(0_k)} > \\
\vdots & \vdots & \vdots \\
(n(0_k)-1)_m & \longmapsto & < 0_k\ ,\ (n(0_k)-1)_{n(0_k)} > \\
(n(0_k))_m & \longmapsto & < 1_k\ ,\ 0_{n(1_k)} > \\
\vdots & \vdots & \vdots \\
\vdots & \vdots & \vdots \\
(m-1)_m & \longmapsto & < (k-1)_k\ ,\ (n((k-1)_k)-1)_{n((k-1)_k)} >
\end{array} \tag{15}$$

The idea is trivial: we perform k stages: firstly, we enumerate the $n(0_k)$ elements of $N(n(0_k))$, then the $n(1_k)$ elements of $A(n(1_k))$ and so on till we reach the last element in $N(n((k-1)_k))$.

Proposition 3. *Let $A(i)$ set $[i \in I]$ be a finite set-indexed family of finite sets, that is, let I and each of the $A(i)$ be finite. Then $(\Sigma\ i \in I)A(i)$ is finite.*

Proof. By $\exists$-elimination on $\mathrm{Fin}(I)$, we can assume $k \in N$, $f \in N(k) \rightarrow I$ and $f(N(k)) = I$.

Firstly, let $Q(i)$ *prop* $[i \in I]$ be an arbitrary propositional function over I. From $f \in N(k) \rightarrow I$ we can infer $(\forall i \in I)Q(i) \rightarrow (\forall x \in N(k))Q(f(x))$ *true*. Also, from $f(N(k)) = I$ we can infer $(\forall x \in N(k))Q(f(x)) \rightarrow (\forall i \in I)Q(i)$. Thus $(\forall i \in I)Q(i)$ is equivalent to $(\forall x \in N(k))Q(f(x))$, provided that the assumptions at the very beginning of the proof hold.

Now let $Q(i) \equiv \mathrm{Fin}(A(i)) \equiv (\exists n \in N)(\exists g \in N(n) \rightarrow A(i))(g(N(n)) = A(i))$. Thus $(\forall i \in I)\mathrm{Fin}(A(i))$ is equivalent to $(\forall x \in N(k))\mathrm{Fin}(A(f(x)))$. Hence, by proposition 1 applied twice, we can infer the existence of $n \in N(k) \rightarrow N$ and $g \in (\Pi\ x \in N(k))(N(n(x)) \rightarrow A(f(x)))$ such that $g(x)(N(n(x))) = A(f(x))$, that is $g(x)$ is surjective, for all $x \in N(k)$.

Let $h \in (\Sigma\ x \in N(k))N(n(x)) \to (\Sigma\ i \in I)A(i)$ be the function defined by $h \equiv \lambda z. < f(p(z)), g(p(z))(q(z)) >$, that is $h(< x, y >) =< f(x), g(x)(y) >$. The function h is surjective and the thesis follows by the previous lemma and proposition 2.

As a corollary one gets that the cartesian product $A \times B$ of two finite sets is finite too.

Beside the Σ operator, another common constructor for sets is the so-called *dependent* (or *cartesian*) *product*, written Π, which includes the set of functions between two sets as a special case. The canonical elements of $(\Pi\ i \in I)S(i)$ are functions of the kind $\lambda x.f(x)$ with $x \in I$ and $f(x) \in S(x)$. The behavior of Π with respect to finiteness is described in the following lemma and proposition.

Lemma 2. *Let $k \in N$ and $n(x) \in N[x \in N(k)]$; then $(\Pi\ x \in N(k))N(n(x))$ is finite.*

Proof. Let $m = n(0_k) \cdot n(1_k) \cdot \ldots \cdot n((k-1)_k) \in N$ and consider the function $f \in N(m) \to (\Pi\ x \in N(k))N(n(x))$ defined by the following m conditions (we suppress indexes):

$$0 \longmapsto \begin{cases} 0 & \mapsto 0 \\ 1 & \mapsto 0 \\ \vdots & \vdots\ \vdots \\ k-1 & \mapsto 0 \end{cases} \qquad 1 \longmapsto \begin{cases} 0 & \mapsto 0 \\ 1 & \mapsto 0 \\ \vdots & \vdots\ \vdots \\ k-1 & \mapsto 1 \end{cases} \qquad \ldots$$

$$\frac{m}{n(0)} - 1 \longmapsto \begin{cases} 0 & \mapsto \quad 0 \\ 1 & \mapsto \quad n(1)-1 \\ \vdots & \vdots \qquad \vdots \\ k-1 & \mapsto n(k-1)-1 \end{cases} \qquad \frac{m}{n(0)} \longmapsto \begin{cases} 0 & \mapsto 1 \\ 1 & \mapsto 0 \\ \vdots & \vdots\ \vdots \\ k-1 & \mapsto 0 \end{cases} \qquad \ldots \tag{16}$$

$$\ldots \qquad \ldots \qquad m-1 \longmapsto \begin{cases} 0 & \mapsto \quad n(0)-1 \\ 1 & \mapsto \quad n(1)-1 \\ \vdots & \vdots \qquad \vdots \\ k-1 & \mapsto n(k-1)-1 \end{cases}$$

Proposition 4. *Let $k \in N$ and $A(x)$ set $[x \in N(k)]$ be a family of finite sets indexed by $N(k)$. Then $(\Pi\ x \in N(k))A(x)$ is finite.*

Proof. As in the proof of the previous proposition, from $(\forall x \in N(k))\mathrm{Fin}(A(x))$, we can construct $n \in N(k) \to N$ and $g \in (\Pi\ x \in N(k))(N(n(x)) \to A(x))$ such that $g(x)(N(n(x))) = A(x)$, that is $g(x)$ is surjective, for all $x \in N(k)$.

Let $h \in (\Pi\ x \in N(k))N(n(x)) \to (\Pi\ x \in N(k))A(x)$ be the function defined by $\lambda z.(\lambda x.g(x)(z(x)))$, that is $h(\lambda x.f(x)) = \lambda x.g(x)(f(x))$. Note that it is surjective and apply the previous lemma and proposition 2.

As a corollary, the set of functions $N(k) \to S$ is finite provided that $k \in N$ and S is a finite set.

Note that we cannot generalize the previous proposition to the case of an arbitrary finite set I in place of $N(k)$. That is so because proving finiteness of $(\Pi\ i \in I)A(i)$ would need the construction of a partial inverse of the surjective function giving finiteness of I (think of the special case $I \to A$). The point is that such a construction of a partial inverse cannot be performed if the axiom of choice is missing. Hence, finiteness of $A \to B$ does not follow from finiteness of A and B.

Incidentally, note that if both the axiom of choice and the first universe (or, simply, the boolean universe of [4]) are adopted, then a finite set become exactly a set that can be put in a bijective correspondence with some $N(k)$ (see Brouwer's definition of finite set in [3]). In fact, if S is finite, then there exists an onto map $f : N(k) \to S$; thus, by choice, we can construct a partial inverse, say g, whose image is in a one to one correspondence with S. Now, since equality in $N(k)$ is decidable (thanks to the existence of either the first or the boolean universe), we can count the elements of $g(S)$; let n be this number. Then it is possible to construct a bijection between $N(n)$ and S.

4 Finite Subsets

Before turning our attention to finite subsets, we have to introduce the notion of subset we are going to use. Following [9], a subset of a given set S is represented by a first order (that is, with variables ranging only over sets) propositional function with at most one free variable over that set. A propositional function over S is of the kind $U(x)\ prop\ [x \in S]$; thus $U(x)$ is a proposition provided $x \in S$. We write U, or also $\{x \in S : U(x)\}$, when we think of it as a subset of S. We write $U \subseteq S$ to express that U is a subset of S. The membership relation between an element $a \in S$ and a subset $U \subseteq S$ is written $a\ \epsilon_S\ U$ (or $a\ \epsilon\ U$ when no confusion arises) and is defined as the proposition $Id(S, a, a)\ \&\ U(a)$, where $U(x)$ is a propositional function which represents U. Note that $a\ \epsilon\ U$ is a proposition provided that $a \in S$ and $U \subseteq S$; that is,

$$(a\ \epsilon_S\ U)\ prop\ [a \in S,\ U(x)\ prop\ [x \in S]]\ . \tag{17}$$

Hence, $a\ \epsilon\ U$ is not a judgement, but only a proposition; moreover $a\ \epsilon\ U$ is true exactly when $U(a)$ is true and $a \in S$. Thus, from $(a\ \epsilon\ U)\ true$ we can derive the judgement $a \in S$; note that the proposition $Id(S, a, a)$ is introduced just to keep trace of the element a, since $U(a)$ could loose the information about it (see [9] for further explanations).

Given two subsets, say U and V, i.e. two propositional functions over S, we say that U is included in V when the proposition $(\forall x \in S)(x\ \epsilon\ U \to x\ \epsilon\ V)$, written $U \subseteq V$, is true. Of course, $U = V$ is the proposition $(U \subseteq V)\ \&\ (V \subseteq U)$; hence, equality between subsets is extensional; in other words, a subset is a class of equivalent propositional functions. Important examples of subsets are: the empty subset, written $\emptyset$, that corresponds to the propositional function $\bot\ prop\ [x \in S]$, where $\bot$ is the false proposition; the total subset, denoted by $\top_S$ or simply by S, that corresponds to the always true propositional function $\top\ prop\ [x \in S]$;

the singletons $\{a\}$ for $a \in S$ i.e. the propositional functions $x = a$ (or, better, $Id(S, x, a)$ *prop* $[x \in S]$).[2] Finally, operations on subsets are defined by reflecting the corresponding connectives (of intuitionistic logic). For example, provided that U and V are represented by $U(x)$ and $V(x)$ respectively, $U \cap V$ is represented by the propositional function $U(x)$ & $V(x)$; in other words, $x \epsilon U \cap V$ if and only if $(x \epsilon U)$ & $(x \epsilon V)$. Infinitary operations are also available, such as the union of a set-indexed family of subsets (more details can be found in [9]). Note that an operation corresponding to implication is also definable; in particular, given a subset U represented by $U(x)$, we denote by $-U$ the subset represented by $\neg\, U(x) \equiv U(x) \to \bot$.

We write $\mathcal{P}S$ for the collection of all subsets of the set S; it is surely not a set in the framework of mTT: assuming the powerset axiom breaks compatibility with predicative foundations, e.g. Martin-Löf's type theory (for more details on this, see [5]). To be precise, $\mathcal{P}S$ is an extensional collection, namely the quotient over logical equivalence of the collection of all propositional functions over S.

Subsets of a set S can be identified with images under functions with S as their codomain. In fact, let $U(x)$ *prop* $[x \in S]$ then it is also $U(x)$ *set* $[x \in S]$; thus we can construct $(\Sigma\ x \in S)U(x)$ and the function $\lambda x.p(x) : (\Sigma\ x \in S)U(x) \to S$, where p is the first projection; that is, provided that $a \in S$ and $\pi \in U(a)$, we map each $< a, \pi >$ to a. Thus an element $a \in S$ is in the image of $\lambda x.p(x)$ if and only if there exists a proof π of $U(a)$. Vice versa, provided that I *set* and $f : I \to S$, then the propositional function $(\exists i \in I)(x = f(i))$ *prop* $[x \in S]$ defines a subset of S which is exactly the image of I under f.

Following the same pattern as for sets, we give the following.

Definition 3 (finite (unary) subset). *A subset K of a set S is* finite *(*unary*) if it is the image of a function $f : N(k) \to S$, for some $k \in N$ ($k = 0, 1$); that is, K can be represented by the propositional function (in the free variable x): $(\exists i \in N(k))(x = f(i))$.*

The collection of all finite (unary) subsets of S is denoted by $\mathcal{P}_\omega S$ ($\mathcal{P}_1 S$, respectively). It follows directly from the definition that every unary subset is finite too; so we can think of $\mathcal{P}_1 S$ as included in $\mathcal{P}_\omega S$. Trivially, S (in the sense of $\top_S$) belongs to $\mathcal{P}_\omega S$ ($\mathcal{P}_1 S$) if and only if S is finite (unary) as a set.

The above definition is just the same as in [9] and coincides with the notion of finitely indexed as given in [10].

Until the end of this section, we will prove some basic properties about finite (and unary) subsets. First of all, we give a natural characterization in terms of finite sequences of elements, i.e. lists. So we need to introduce the set constructor List, which is defined by the following rules.

List-**formation**

$$\frac{S\ set}{\mathrm{List}(S)\ set} \tag{18}$$

[2] Note that, since the symbol S can represent both a set and the total subset of that set, $U \subseteq S$ can denote both a judgement and a proposition. Which case occurs will be clear from the context.

List-**introduction**

$$\frac{}{\mathrm{nil} \in \mathrm{List}(S)} \qquad \frac{l \in \mathrm{List}(S) \quad a \in S}{\mathrm{cons}(l, a) \in \mathrm{List}(S)} \tag{19}$$

that is, lists are recursively constructed starting from the empty list nil and adding elements of S one at a time (cons can be thought of as the function that attaches an element at the end of a given list).

List-**elimination**

$$\frac{\begin{array}{c}[x \in \mathrm{List}(S)] \\ \vdots \\ A(x)\ set\end{array} \quad l \in \mathrm{List}(S) \quad a \in A(\mathrm{nil}) \quad \begin{array}{c}[x \in \mathrm{List}(S),\ y \in S,\ z \in A(x)] \\ \vdots \\ f(x, y, z) \in A(\mathrm{cons}(x, y))\end{array}}{LR(a, f, l) \in A(l)} \tag{20}$$

that is, if we have an element in $A(\mathrm{nil})$ and every time we know an element in $A(x)$ we can construct (by means of the function f) an element of $A(\mathrm{cons}(x, y))$, then we are able to construct an element in $A(l)$ for every list l. In other words, we have a function LR (for "list recursion") that for every list l returns a value in $A(l)$ depending on the method f and the starting value $a \in A(\mathrm{nil})$.

An important consequence of this last rule is that we can use induction when proving a certain property about lists. Remember that every proposition is also a set (an element is just a proof, a verification); then the elimination rule yields:

$$\frac{\begin{array}{c}[x \in \mathrm{List}(S)] \\ \vdots \\ P(x)\ prop\end{array} \quad l \in \mathrm{List}(S) \quad P(\mathrm{nil})\ true \quad \begin{array}{c}[x \in \mathrm{List}(S),\ y \in S,\ P(x)\ true] \\ \vdots \\ P(\mathrm{cons}(x, y))\ true\end{array}}{P(l)\ true}\ induction. \tag{21}$$

Finally we have two equality rules which we state without writing again all the hypotheses.

$$LR(a, f, \mathrm{nil}) = a \qquad LR(a, f, \mathrm{cons}(l, b)) = f(l, b, LR(a, f, l)). \tag{22}$$

These conditions can be read, of course, as a recursive definition of the function LR.

In order to continue with our simultaneous treatment of finite and unary subsets, we need to define the set of sequences of length at most one, written $\mathrm{List}_1(S)$. The rules for it are obtained as a slight modification of those for $\mathrm{List}(S)$ and hence we do not write them down in all details. We give only the introduction rules, as an example:

$$\frac{}{\mathrm{nil} \in \mathrm{List}_1(S)} \qquad \frac{a \in S}{\mathrm{cons}(\mathrm{nil}, a) \in \mathrm{List}_1(S)}\ . \tag{23}$$

Even if not formally right, we can conceive of $\mathrm{List}_1(S)$ as included in $\mathrm{List}(S)$ in order to avoid boring distinctions.

Sometimes we write [ ] instead of nil, $[a]$ instead of $\mathrm{cons}(\mathrm{nil}, a)$, $[a, b]$ instead of $\mathrm{cons}(\mathrm{cons}(\mathrm{nil}, a), b)$ and so on.

$\mathrm{List}(S)$ can be endowed with a binary operation, called concatenation and written $*$, which is recursively defined by the following clauses:

$$\begin{cases} l * \mathrm{nil} =_{def} l \\ l * \mathrm{cons}(m, a) =_{def} \mathrm{cons}(l * m, a) \end{cases} \tag{24}$$

where l,m are in $\mathrm{List}(S)$ and $a \in S$.

Finally, we would like to define a function dec (for "de-construct") from $\mathrm{List}(S)$ to $\mathcal{P}S$; of course, formally we will have

$$(\mathrm{dec}(l)(x)\ prop\ [x \in S])[l \in \mathrm{List}(S)] \tag{25}$$

because we want $\mathrm{dec}(l)$ to be a subset of S (that is a propositional function over S) for any $l \in \mathrm{List}(S)$. Let us define dec recursively as follows[3]:

$$\begin{cases} \mathrm{dec}(\mathrm{nil})(x) \ \equiv\ \bot(x) \\ \mathrm{dec}(\mathrm{cons}(l, a))(x) \ \equiv\ \mathrm{dec}(l)(x) \vee Id(S, x, a) \end{cases} . \tag{26}$$

Proposition 5 (a characterization of finite (unary) subsets). *Let S be a set and $K \subseteq S$. K is finite (unary) if and only if $\exists\ l \in \mathrm{List}(S)$ ($\exists\ l \in \mathrm{List}_1(S)$) such that K is equal to $\mathrm{dec}(l)$ in $\mathcal{P}S$.*

Proof. Suppose K is finite (unary); then, by $\exists$-elimination, we can assume to know a number k ($k = 0, 1$) and a function f from $N(k)$ to S, such that $K = f(N(k))$. Now consider the list $l_f = [f(0_k), \ldots, f((k-1)_k)]$ and remember that $(\exists i \in N(k))(x = f(i))$ is equivalent to $(x = f(0_k)) \vee (x = f(1_k)) \vee \ldots \vee (x = f((k-1)_k))$. In other words, $x \,\epsilon\, f(N(k))$ and $x \,\epsilon\, \mathrm{dec}(l_f)$ are equivalent.

Vice versa, by $\exists$-elimination again, we can assume to have a list, say $l = [a_0, \ldots, a_{k-1}]$, whose length is k and such that $\mathrm{dec}(l) = K$. Then we can define a surjection f_l from $N(k)$ to S by prescribing the k conditions: $f_l(n_k) =_{def} a_n$, for $n = 0, \ldots, k-1$. Now it is easy to realize the equivalence between $x \,\epsilon\, f_l(N(k))$ and $x \,\epsilon\, \mathrm{dec}(l)$.

The previous proposition can be stated informally by saying that $\mathcal{P}_\omega S = (\mathrm{dec}\,(\mathrm{List}(S)), \leftrightarrow)$ and $\mathcal{P}_1 S = (\mathrm{dec}(\mathrm{List}_1(S)), \leftrightarrow)$. In other words $\mathcal{P}_\omega S$ and $\mathcal{P}_1 S$ are set-indexed extensional families. It is also possible to define $\mathcal{P}_\omega S$ as a setoid, that is a quotient set. Indeed, let $\sim$ be the relation over $\mathrm{List}(S)$ defined by $l_1 \sim l_2$ if $\mathrm{dec}(l_1) \leftrightarrow \mathrm{dec}(l_2)$. One sees at once that $\sim$ is an equivalence relation; hence we can consider the setoid $(\mathrm{List}(S), \sim)$. So, $\mathcal{P}_\omega S$ can be identified with $(\mathrm{List}(S), \sim)$; a similar argument holds for $\mathcal{P}_1 S$ and $(\mathrm{List}_1(S), \sim)$. The general idea is that a finite subset is obtained from a list by forgetting (that is, by abstracting from) the order and multiplicity with which items appear in it.

The fact that $\mathcal{P}_\omega S$ and $\mathcal{P}_1 S$ are set-indexed families allows us to treat them almost like sets. First of all, we can quantify over them; in fact, every quantification intended over finite subsets of S can be given a constructive meaning

[3] We write $\bot(x)$ to emphasize that we look at $\bot$ as a propositional function over S.

by quantifying over the set $\mathrm{List}(S)$ and then using the function dec. In particular, an expression like "$(\forall K \in \mathcal{P}_\omega S)(\ldots K \ldots)$" is a shorthand for "$(\forall l \in \mathrm{List}(S))(\ldots \mathrm{dec}(l) \ldots)$". Similarly for $\exists$. Of course a proposition over $\mathcal{P}_\omega S$, say $P(K)$, as to be thought of as a proposition over $\mathrm{List}(S)$ of the kind $Q(l)$ such that $Q(l_1) \leftrightarrow Q(l_2)$ *true* if and only if $\mathrm{dec}(l_1) \leftrightarrow \mathrm{dec}(l_2)$ *true*.

Moreover it is possible to use $\mathcal{P}_\omega S$ to construct new setoids. For example, $\mathrm{List}(\mathcal{P}_\omega S)$ can be defined as the setoid $(\mathrm{List}(\mathrm{List}(S)), \approx)$, where $\{l_0, \ldots, l_{n-1}\} \approx \{k_0, \ldots, k_{m-1}\}$ is $Id(N, n, m)$ & $(\forall i \in N)((i < n) \rightarrow (\mathrm{dec}(l_i) \leftrightarrow \mathrm{dec}(k_i)))$.

However, if one is interested in constructing new objects based on $\mathcal{P}_\omega S$, then it is more convenient to define $\mathcal{P}_\omega S$ (and $\mathcal{P}_1 S$ similarly) by adding to the rules of $\mathrm{List}(S)$ the following ones (and by modifying the elimination rule in order to take the new equality into account; see [7]):

exchange

$$\frac{a \in S \quad b \in S \quad l \in \mathcal{P}_\omega S}{\mathrm{cons}(\mathrm{cons}(l, a), b) = \mathrm{cons}(\mathrm{cons}(l, b), a) \in \mathcal{P}_\omega S} \;; \tag{27}$$

contraction

$$\frac{a \in S \quad l \in \mathcal{P}_\omega S}{\mathrm{cons}(\mathrm{cons}(l, a), a) = \mathrm{cons}(l, a) \in \mathcal{P}_\omega S} \;. \tag{28}$$

It is easy to show that these two rules are enough to force two canonical elements to be equal when they are formed by the same items, regardless of order and repetitions. Thus, for a and b in S, we can infer that $[a, b, b, a, b]$ and $[a, b]$ are equal elements of $\mathcal{P}_\omega S$. Of course, this does not mean that the equality in $\mathcal{P}_\omega S$ is decidable; for example, we can infer $[a] = [b] \in \mathcal{P}_\omega S$ only if $a = b \in S$. In other words, the equality in $\mathcal{P}_\omega S$ is decidable if and only if that of S is.

The usual way of dealing with finite subsets can be reconstructed by means of suitable definitions and derived rules. As an example, let us consider the notion of membership. The idea is that an element $a \in S$ belongs to $l \in \mathcal{P}_\omega S$ if the assumption $a \in S$ has been used in the construction of l. However, by exchange and contraction, one may assume that a is the last item in l. So one can put

$$a \,\epsilon\, l \equiv (\exists m \in \mathcal{P}_\omega S)(l = \mathrm{cons}(m, a)). \tag{29}$$

If $\mathcal{P}_\omega$ is seen as a constructor, then it is possible to construct $\mathcal{P}_\omega \mathcal{P}_\omega S$ and so on. In [12] a proof can be found of the fact that $\mathcal{P}_\omega S$ is finite, provided that S is finite.

However, we prefer to keep our original definition and look at $\mathcal{P}_\omega S$ as an extensional set-indexed collection of subsets of S. The main reason for that is that we are thus allowed to apply to finite subsets all the operations of $\mathcal{P}S$, even if $\mathcal{P}_\omega S$ is not closed under them.

Proposition 6 (basic properties of finite and unary subsets). *Let $\mathcal{P}_\omega S$ and $\mathcal{P}_1 S$ be the collections of all finite and unary subsets of a set S; then:*

i) $\emptyset$ belongs to $\mathcal{P}_1 S$;
ii) $\{a\}$ belongs to $\mathcal{P}_1 S$ for any $a \in S$;
iii) $K \cup L \in \mathcal{P}_\omega S$, for all K and L belonging to $\mathcal{P}_\omega S$.

Proof. For i) and ii) consider the lists nil and cons(nil, a), respectively. With regard to iii) take the concatenation of two lists corresponding to K and L and note that $\mathrm{dec}(l * m) = \mathrm{dec}(l) \vee \mathrm{dec}(m)$; in other words, the concatenation of two lists corresponds to the union of the corresponding finite subsets.

Proposition 7 (induction principle for finite subsets). *Let $P(K)$ be a predicate over $\mathcal{P}_\omega S$ such that:*

1. *$P(\emptyset)$ holds;*
2. *$P(L)$ implies $P(L \cup \{a\})$, for any $a \in S$ and L in $\mathcal{P}_\omega S$;*

then $P(K)$ holds for every K in $\mathcal{P}_\omega S$.

Proof. Note that the hypotheses 1 and 2 can be rewritten as $P(\mathrm{dec}(\mathrm{nil}))$ and $(\forall l \in \mathrm{List}(S))(\forall a \in S)(P(\mathrm{dec}(l)) \rightarrow P(\mathrm{dec}(\mathrm{cons}(l, a))))$, while the thesis is $(\forall l \in \mathrm{List}(S))P(\mathrm{dec}(l))$. Thus the statement is just a reformulation of the induction rule for lists with respect to the proposition $Q(l) \equiv P(\mathrm{dec}(l))$.

Proposition 8. *Let S be a set and $K \subseteq S$ be finite (possibly unary). Then it is decidable whether K is empty or inhabited.*

Proof. We prove $(K = \emptyset) \vee (\exists a \in S)(a \,\epsilon\, K)$ by induction on $\mathcal{P}_\omega S$. If $K = \emptyset$, then we are done. Now suppose the statement is true for K and consider the subset $K \cup \{a\}$, for $a \in S$; of course, $a \,\epsilon\, K \cup \{a\}$ and the proof is complete.

Proposition 6 says that $(\mathcal{P}_\omega S, \cup, \emptyset)$ is the sup-semilattice generated by the singletons. In general, the intersection of two finite (unary) subsets cannot be proved to be finite (unary) too. This phenomenon corresponds to the fact that we cannot find the common elements between two given lists unless the equality relation in the underlying set S is decidable. [4]

Proposition 9. *Let S be a set. The following are equivalent:*

1. *the equality in S is decidable;*
2. *$\{a\} \cap \{b\}$ is finite, for all a and b in S;*
3. *$K \cap L$ is finite for all finite K and L;*
4. *$\{a\} \cup -\{a\} = S$ for all $a \in S$;*
5. *$K \cup -K = S$ for all finite K.*

Proof. 1 $\Rightarrow$ 2. If $a = b$ holds, then $\{a\} \cap \{b\}$ is equal to $\{a\}$ which is finite; instead, if $a \neq b$, then a cannot belong to $\{b\}$ and $\{a\} \cap \{b\}$ is empty, hence finite.

2 $\Rightarrow$ 3. Assume $K = \{a_0, \ldots, a_{n-1}\}$ and $L = \{b_0, \ldots, b_{m-1}\}$; then $K = \cup_{i=0}^{n-1}\{a_i\}$, while $L = \cup_{j=0}^{m-1}\{b_j\}$. Thus $K \cap L = \cup_{i,j}(\{a\} \cap \{b\})$, by distributivity of $\cap$ with respect to $\cup$; thus it is finite, since it is the union of finitely many (namely $n \cdot m$) finite subsets.

[4] Of course, the equality in S is decidable if the proposition $(\forall a \in S)(\forall b \in S)(Id(S, a, b) \vee \neg Id(S, a, b))$ is true.

$3 \Rightarrow 4$. Let $a, b \in S$; then $\{a\}$ and $\{b\}$ are finite; thus $\{a\} \cap \{b\}$ is finite and it is decidable whether it is empty or inhabited. If the former holds, then b cannot belong to $\{a\}$, thus $b \,\epsilon\, -\{a\}$. Instead, if the latter holds, then the proposition $(\exists c \in S)(c \,\epsilon\, \{a\} \cap \{b\})$ yields $a = b$; so $b \,\epsilon\, \{a\}$. Since b was arbitrary, $\{a\} \cup -\{a\}$ is the whole S.

$4 \Rightarrow 5$. If $K = \{a_0, \ldots, a_{n-1}\} = \cup_{i=0}^{n-1}\{a_i\}$, then $-K = \cap_{i=0}^{n-1} - \{a_i\}$. By distributivity of $\cup$ with respect to $\cap$, $K \cup -K(x)$ can be seen as the intersection of n subsets of the kind $K \cup -\{a_i\}$ for $i = 1, \ldots, n$. Each of them is a union of $n+1$ subsets and contains $\{a_i\} \cup -\{a_i\}$, which is S by hypothesis; hence $K \cup -K = S$.

$5 \Rightarrow 1$. Let a and b be two arbitrary elements of S. Since $\{b\}$ is finite, then $\{b\} \cup -\{b\} = S$; thus a belongs to it. In other words $(a = b) \vee (a \neq b)$ holds.

Thus, provided that the equality of S is decidable, $\mathcal{P}_\omega S$ is closed under intersection. On the contrary, an arbitrary subset of a finite (unary) subset is not forced to be finite (unary) too, even in the case of a decidable equality. For let P be an arbitrary proposition and read $P \;\&\; Id(N(1), x, 0_1)$ as a propositional function over the finite set $N(1)$. If the subset $\{x \in N(1) \;:\; P \;\&\; (x = 0_1)\}$ were finite, then we could decide whether it is empty or inhabited: in the first case $\neg P$ should hold, otherwise P should; in other words, we could prove the law of excluded middle. Moreover note that the above argument holds even if the existence of the first universe is assumed (thus the equality of $N(1)$ is decidable). Thus we have proved the following.

Proposition 10. *In the framework of mTT, the statement that every subset of a finite (sub)set is also finite is equivalent to the full law of the excluded middle.*

We conclude the present section with a property about finite subsets which was used both in [2] and [12] to prove constructive versions of Tychonoff's theorem.

Proposition 11. *Let S be a set and K,V,W subsets of S. If $K \subseteq V \cup W$ and K is finite (unary), then there exist $V_0 \subseteq V$ and $W_0 \subseteq W$ both finite (unary) such that $K = V_0 \cup W_0$.*

The above proposition looks as intuitively clear: take V_0 and W_0 to be $K \cap V$ and $K \cap W$ respectively. But formally we cannot follow this road because a part of a finite subset is not finite, in general (previous proposition).

Proof. Let us start from the unary case. We can effectively decide if K is the empty subset or a singleton. In the first case take $V_0 = \emptyset = W_0$. Otherwise we have $K = \{a\}$ for some a and, moreover, $a \,\epsilon\, V \cup W$; so either $a \,\epsilon\, V$ or $a \,\epsilon\, W$. In the first case take $V_0 = \{a\}$ and $W_0 = \emptyset$; $W_0 = \{a\}$ and $V_0 = \emptyset$, otherwise.

In order to prove the statement in the finite case, we use induction. If $K = \emptyset$ we can take $V_0 = \emptyset = W_0$. Now assume the theorem to be true for K and prove it for $K \cup \{a\}$. So, let $K \cup \{a\} \subseteq V \cup W$. Then $K \subseteq V \cup W$ and by inductive hypothesis there exist $V_0' \subseteq V$ and $W_0' \subseteq W$ both finite and satisfying $K = V_0' \cup W_0'$; hence $K \cup \{a\} = V_0' \cup W_0' \cup \{a\}$. On the other hand, we know that $a \,\epsilon\, V \cup W$: so, if $a \,\epsilon\, V$, then we can take $V_0 = V_0' \cup \{a\}$ and $W_0 = W_0'$, while if

$a \epsilon W$, then we take $V_0 = V_0'$ and $W_0 = W_0' \cup \{a\}$ (if a belongs to both of them, then both choices are good).

A remark on the last part of the previous proof could be useful. Even if we proceed by cases starting from $a \epsilon V \cup W$, it does not mean we are assuming that we can decide wether $a \epsilon V$ or $a \epsilon W$; what we are doing is just an application of the logical rule called "elimination of disjunction". Thus, the effective construction of V_0 and W_0 strongly depends on the degree of constructiveness of the hypothesis $K \subseteq V \cup W$.

The previous proposition, combined with the fact that we are always able to decide whether a finite subset is inhabited or not, yields the following corollary (see [12]).

Corollary 1. *Let $P(x)$ and $Q(x)$ be two propositional functions over a set S and let $K \subseteq S$ be a finite subset such that for every $x \epsilon K$ either $P(x)$ or $Q(x)$ holds. Then either $P(x)$ holds for every $x \epsilon K$ or there exists some $x \epsilon K$ such that $Q(x)$ holds.*

In fact, from $K \subseteq P \cup Q$ we can infer, as in the previous proposition, $K = P_0 \cup Q_0$ and then decide whether Q_0 is empty or inhabited.

5 Some Other Notions of Finiteness

The notion of finite (sub)set we have adopted all over the present paper looks as the most natural one and, in fact, it is used by many authors (see [2] and [12]) including the present ones (see [1]). On the other hand, such notion lacks some desired properties such as closure under intersection. Hence, one can look for other definitions which enjoy the desired properties. Here we give a brief list of possible alternative notions, each accompanied by a brief report about its properties and disadvantages. For each of the following notions about subsets, a corresponding definition for sets can be obtained by identifying each set with its total subset.

Definition 4 (sub-finite; see [10]). *$U \subseteq S$ is* sub-finite *if $U \subseteq K$ is true, for some K which is finite according to definition 3.*

The collection of all sub-finite subsets is closed both under (arbitrary) intersections and finite unions; on the other hand, it is not set-indexed, in general. Moreover, the computational content carried by a sub-finite subset is very poor; for instance, it is not possible to decide its emptyness.

Definition 5 (bounded; see [3]). *$U \subseteq S$ is* bounded *if $\exists k \in N$ such that $\forall f \in N(k) \to S$*

$$f(N(k)) \subseteq U \to (\exists i, j \in N(k))(i \neq j \;\;\&\;\; f(i) = f(j)) \tag{30}$$

is true; that is, there cannot exist an injective map from $N(k)$ into U (i.e. U has less than k elements).

Contrary to the case of finite subsets, which are always represented by propositional functions of the form $(\exists i \in N(k))(x = f(i))$, for some $k \in N$ and $f \in N(k) \to S$, it appears quite difficult to characterize the propositional functions corresponding to bounded subsets. Also answering the question whether the collection of all bounded subsets is set-indexed or not seems an hard task. This is surely due to the negative, not direct character of this definition.

Proposition 12. *Let S be a set and $U, V \subseteq S$; then:*

1. *if U is finite, then U is bounded;*
2. *if $U \subseteq V$ and V is bounded, then U is bounded;*
3. *if U is sub-finite, then U is bounded.*

Proof. If U is finite, then there exists a number k such that U has at most k elements; so U has less than $k+1$ elements and hence it is bounded.

If V is bounded, then there exists a number k such that no f from $N(k)$ to V can be injective. Consider an arbitrary function f from $N(k)$ to U; of course, it can be seen as a map that take its values in V, hence it can not be injective and U is bounded.

If U is sub-finite, then there exists $K \subseteq S$ such that K is finite and $U \subseteq K$. By item 1, K is bounded; by item 2, U is bounded.

Item 1 in the previous proposition says that every finite (sub)set is bounded. On the contrary, it can not be formally proved that a bounded (sub)set is finite: classical logic seems necessary.

Finally, an interesting generalization of the notion of finite subset is the following one that was proposed to us by Silvio Valentini.

Definition 6 (semi-finite). *$U \subseteq S$ is semi-finite if:*

$$(x \,\epsilon\, U) \leftrightarrow \ \vee_{j \in J} \ (\&_{i \in I(j)} \ \ x = a_{ji}), \tag{31}$$

where $a_{ji} \in S$ and both the set J and each $I(j)$, $j \in J$, are of the form $N(k)$.

Of course, the a_{ji} in the definition above as to be thought of as a map from $(\Sigma \ j \in J)I(j)$ to S. The collection of all semi-finite subsets is closed under finite intersections and unions; moreover, provided that the equality in S is decidable, semi-finiteness collapses to finiteness. Note that a semi-finite subset can be seen, by distributivity, as the intersection of a certain finite family of finite subsets. In other words, as $\mathcal{P}_\omega S$ is the $\cup$-semi-lattice generated by singletons, so the collection of all semi-finite subsets is the lattice generated by them (with respect to intersection and union). Note also that semi-finite subsets form a family indexed by the set $\mathrm{List}(\mathrm{List}(S))$. However, it is no longer decidable if a semi-finite subset is empty or not; in other words, with respect to this definition proposition 8 (and hence proposition 11 and corollary 1) fails.

Acknowledgments. The authors thank Maria Emilia Maietti for a lot of essential suggestions she gave them during long and dense discussions.

References

1. Ciraulo, F., Sambin, G.: Finitary Formal Topologies and Stone's Representation Theorem. Theoretical Computer Science (to appear)
2. Coquand, T.: An Intuitionistic Proof of Tychonoff Theorem. Journal of Symbolic Logic 57(1), 28–32 (1992)
3. van Dalen, D. (ed.): Brouwer's Cambridge Lectures on Intuitionism. Cambridge University Press, Cambridge (1981)
4. Maietty, M.E.: Quotients over Minimal Type Theory. In: Cooper, S.B., Löwe, B., Sorbi, A. (eds.) CiE 2007. LNCS, vol. 4497, Springer, Heidelberg (2007)
5. Maietti, M.E., Sambin, G.: Toward a Minimalist Foundation for Constructive Mathematics. In: Crosilla, L., Schuster, P. (eds.) From Sets and Types to Topology and Analysis: Towards Practicable Foundations for Constructive Mathematics, Oxford UP. Oxford Logic Guides, vol. 48 (2005)
6. Martin-Löf, P.: Intuitionistic Type Theory. Notes by G. Sambin of a series of lectures given in Padua, June 1980. Bibliopolis, Naples (1984)
7. Negri, S., Valentini, S.: Tychonoff's Theorem in the Framework of Formal Topologies. Journal of Symbolic Logic 62(4), 1315–1332 (1997)
8. Nordström, B., Peterson, K., Smith, J.: Programming in Martin-Löf's Type Theory. Clarendon Press, Oxford (1990)
9. Sambin, G., Valentini, S.: Building up a Toolbox for Martin-Löf Type Theory: Subset Theory. In: Sambin, G., Smith, J. (eds.) Twenty-Five Years of Constructive Type Theory. Proceedings of a Congress Held in Venice, October 1995, pp. 221–240. Oxford University Press, Oxford (1998)
10. Troelstra, A.S., van Dalen, D.: Constructivism in Mathematics: An Introduction, vol. 1. NorthHolland, Amsterdam (1988)
11. Veldman, W.: Some Intuitionistic Variations on the Notion of a Finite Set of Natural Numbers. In: de Swart, H.C.M., Bergman, L.J.M. (eds.) Perspectives on negation. Essays in honour of Johan J. de Iongh on his 80th birthday, pp. 177–202. Tilburg Univ. Press, Tilburg (1995)
12. Vickers, S.J.: Compactness in Locales and in Formal Topology. In: Banaschewski, B., Coquand, T., Sambin, G. (eds.) Papers presented at the 2nd Workshop on Formal Topology (2WFTop 2002), Venice, Italy, April 04-06, 2002. Annals of Pure and Applied Logic, vol. 137, pp. 413–438 (2006)