Can you add power-sets to Martin-Löf intuitionistic set theory?

Maria Emilia Maietti, Silvio Valentini
Dipartimento di Matematica Pura ed Applicata
Università di Padova
via G. Belzoni n.7, I–35131 Padova, Italy
e-mail: maietti,silvio@math.unipd.it

January 11, 2000

Abstract

In this paper we analyze an extension of Martin-Löf's intensional set theory by means of a set contructor $\mathcal{P}$ such that the elements of $\mathcal{P}(S)$ are the subsets of the set S.

Since it seems natural to require some kind of extensionality on the equality among subsets, it turns out that such an extension cannot be constructive. In fact we will prove that this extension is classic, that is $(A \vee \neg A)$ *true* holds for any proposition A.

Mathematics Subject Classification: 03B15, 03B20.
Keywords: Intuitionistic set theory, topos theory.

1 Introduction

In [GR94] it is shown that the proof theoretic strength of Martin-Löf's set theory [Mar84, NPS90] with restricted well-orders and the universe of the small sets is that of a subsystem of second order arithmetic with Δ^1_2 comprehension and bar-induction. Thus, it is natural to wonder whether it is possible to enforce it to a theory with the strength of the full comprehension schema by adding a power-set constructor; in fact, this extension is necessary if we want to quantify over the subsets of a given set since in Martin-Löf's set theory quantification is meaningful only on elements of a set.

In the literature there are already examples of constructive set theories with some kind of power-set constructor. For instance, one can think of a *topos* as a "generalized set theory" by associating with any topos its internal language (cf. [Bel88]). The logic underlying such a set theory is the intuitionistic predicate calculus and so any topos can be thought of as an intuitionistic universe of sets. Then, the lack of the rule of excluded middle seems to assure the constructivity of any proof developed within topos theory. The problem of adapting the topos

theoretic approach to Martin-Löf's set theory is due to the impredicativity of the former. Indeed, Martin-Löf's set theory is predicative and provides a fully algorithmic way to construct the elements of the sets and the proofs of the propositions over these sets.

Another approach which should be considered is the Calculus of Constructions by Coquand and Huet, where the power of a set S can be identified with the collection of the functions from S into prop. But, if we identify sets and propositions, which is basic for a constructive explanation of the meaning of Martin-Löf's set theory, the power-set so obtained is *not* a set, since prop cannot be a set and hence also the collection of the functions from a set S to prop cannot be a set. Thus, there is no chance to give a constructive, i.e. intuitionistic and predicative, meaning to quantification over its elements. A second problem with this approach is that in this way we would obtain an intensional notion of power-set, which is not the intended one since we think that equality among subsets has to be understood extensionally. Finally, it can be proved that the strong sum type, which is characteristic in Martin-Löf's set theory, cannot consistently be added to the Calculus of Constructions at the level of propositions (see [Coq90]); thus, this approach cannot have the full strong sum on propositions (see for instance [Luo90]) and hence it cannot be considered an extension of Martin-Löf's set theory.

Of course, there is no reason to expect that a second order construction becomes constructive only because it is added to a theory which is constructive. Indeed, we will prove that even the weaker fragment iTT, which contains only the basic set constructors, i.e. no universes and no well-orders, and the *intensional* equality, cannot be extended with a power-set constructor in a way compatible with the usual semantical explanation of the connectives, if the power-set is the collection of all the subsets of a given set equipped with extensional equality expressed in a uniform way at the propositional level. In fact, by using the so called intuitionistic axiom of choice, it is possible to prove that, given any power-set constructor, which satisfies the conditions that we will illustrate in the next section, classical logic arises (see also [Hof95] page 170, where it is suggested that a similar result holds in the setoid model built upon the Calculus of Constructions). A crucial point in carrying on our proof is the uniformity of the equality condition expressing extensionality on the power-set. This is to be contrasted with the proofs of similar results already proposed in the literature, after Diaconescu's original proof in [Dia75], where proof-irrelevance of propositions, which does not hold in constructive type theory, is used.

2 $iTT^P = iTT$ + power-sets

To express the rules and the conditions that we are going to require on the power-set we need to use judgements of the form A *true* (see [Mar84]) and hence it is convenient to recall their main property: A *true* holds if and only if there exists a proof-element a such that $a \in A$ holds (for a formal approach to

this topic see [Val95]). In particular, the following rule is admissible

$$\text{(True Introduction)} \quad \frac{a \in A}{A \; true}$$

as well as all the rules of the intuitionistic predicative calculus with equality, where the judgement $A \; true$ is the type theoretic interpretation of $\vdash A$ (see [Mar84] for the definition of the embedding of the intuitionistic predicative calculus within iTT). Here, we only recall the rules for the set of the intensional propositional equality Id (see [NPS90], page 61) which plays a central role in this paper (for sake of clearness, supposing A is a set and $a, b \in A$, we will write $a =_A b$ to mean $\mathsf{Id}(A, a, b)$). The formation and introduction rules are

$$\frac{A \; \mathsf{set} \quad a \in A \quad b \in A}{a =_A b \; \mathsf{set}} \qquad \frac{A = C \quad a = c \in A \quad b = d \in A}{(a =_A b) \; = \; (c =_A d)}$$

$$\frac{A \; \mathsf{set} \quad a \in A}{\mathsf{id}(a) \in a =_A a} \qquad \frac{A \; \mathsf{set} \quad a = b \in A}{\mathsf{id}(a) = \mathsf{id}(b) \in a =_A a}$$

whereas the elimination rule is

$$\frac{c \in a =_A b \quad d(x) \in C(x, x, \mathsf{id}(x)) \qquad \begin{array}{c}[x : A]_1 \\ | \\ C(x, y, z) \; \mathsf{set}\end{array} \qquad \begin{array}{c}[x : A, y : A, z : x =_A y]_1 \\ | \\ \end{array}}{\mathsf{idpeel}(c, d) \in C(a, b, c)} \; 1$$

and, if $C(x, y, z) \; \mathsf{set} \; [x : A, y : A, z : x =_A y]$ and $D(x, y) \; \mathsf{set} \; [x : A, y : A]$, it yields the admissibility of the following two rules:

$$\frac{c \in a =_A b \quad \begin{array}{c}[x : A] \\ | \\ C(x, x, \mathsf{id}(x)) \; true\end{array}}{C(a, b, c) \; true} \qquad \frac{a =_A b \; true \quad \begin{array}{c}[x : A] \\ | \\ D(x, x) \; true\end{array}}{D(a, b) \; true}$$

The rules for the set $\mathcal{P}(S)$ depend on the definition of what a subset is within iTT. Following a long tradition, we identify a subset of S with a propositional function on S, i.e., provided that $U(x) \; \mathsf{set} \; [x : S]$, we say that $U \equiv (x : S) \; U(x)$ is a subset of S, and hence, we say that an element $a \in S$ is an element of U if $U(a)$ is inhabited, i.e. the judgement $U(a) \; true$ holds (cf. [dB80] and [SV95] for a detailed discussion on this topic).

Thus, provided that we want to have an extensional equality between subsets, we are forced to consider equal two subsets U and V of S if and only if they have the same elements, i.e. $U(x) \leftrightarrow V(x) \; true \; [x : S]$.

The will to construct a set out of the collection of the propositional functions over a set equipped with an equality relation between propositional functions based on equi-provability is the point where classical logic breaks into the system. Inspired by the previous explanations, here we propose the following formation and introduction rules for $\mathcal{P}(S)$:

Formation

$$\frac{S \text{ set}}{\mathcal{P}(S) \text{ set}} \qquad \frac{S = T}{\mathcal{P}(S) = \mathcal{P}(T)}$$

Introduction

$$\frac{U(x) \text{ set } [x : S]}{\{(x : S)\ U(x)\} \in \mathcal{P}(S)}$$

Now, we should formulate the next rules for the set $\mathcal{P}(S)$, i.e. the equality introduction rule, the elimination rule and the equality rule. But the aim of this paper is to show that it is actually impossible to formulate any rules which make valid the conditions that we are are going to discuss in the following and that seem to be necessary to make $\mathcal{P}(S)$ the power-set of S, because otherwise we would obtain a Heyting semantics for classical logic.

As already said, it is necessary to formalize the fact that the equality between subsets is extensional; otherwise, $\mathcal{P}(S)$ would not be the set of the subsets of S but the collection of the propositional functions over S, and to add this collection as a set is not consistent (see [Jac89]). Thus, one seems to be forced to require that, whenever the two subsets U and V of S are equal, that is if $U(x) \leftrightarrow V(x)\ true\ [x : S]$ then $\{(x : S)\ U(x)\} = \{(x : S)\ V(x)\} \in \mathcal{P}(S)$. However, as noted by Peter Aczel after reading a preliminary version of this work, this should not be a formal rule for the set $\mathcal{P}(S)$ since the use of an extensional equality rule for power-sets does not fit with the idea of treating the judgemental equalities as definitional, which is basic in iTT. To avoid this problem, we require here a weaker condition, which is a consequence of the judgemental equality above.

Equality introduction condition
Let $U(x) \leftrightarrow V(x)\ true\ [x : S]$. Then there exists a proof-term $\mathsf{c}(U, V)$ such that $\mathsf{c}(U, V) \in \{(x : S)\ U(x)\} =_{\mathcal{P}(S)} \{(x : S)\ V(x)\}$.

Also this condition does not follow completely the general approach used in Martin-Löf's set theory since some information is lost in the path from the premise to the conclusion, i.e. the proof term which testifies that $U(x) \leftrightarrow V(x)\ true\ [x : S]$. For this reason we do not want to consider it a formal rule. In the following we will prove that this lack of information is one of the main point in obtaining classical logic by adding the power-set constructor and this fact suggests that there is still some hope to be able to add a power-set constructor to constructive set-theory. For instance, one could consider the following rule

$$\frac{f(x) \in U(x) \leftrightarrow V(x)\ [x : S]}{\mathsf{c}(U, V, f) \in \{(x : S)\ U(x)\} =_{\mathcal{P}(S)} \{(x : S)\ V(x)\}}$$

and in this case it would be no more possible to carry on our proof to its end. In any case it is worth noting that this approach is not sufficient in most of the actual implementations of constructive set theory. Indeed, they use pattern-matching instead of elimination rules and thus they validate stronger conditions,

as the uniqueness of equality proofs [HS95] which allows to obtain classical logic also with this rule.

The elimination and the equality rules are even more problematic. In fact it is difficult to give a plain application of the standard approach that requires to obtain the elimination rule out of the introduction rule(s) (see [Mar71]). In fact, the introduction rule does not act over elements of a set but over elements of the collection $((x : S)\ \mathsf{set})_{\leftrightarrow}$. Thus, if one wants to follow for $\mathcal{P}(S)$ the general pattern for a quotient set, he could look for a rule similar to the following:

$$\frac{\begin{array}{cccc} & [Y : (x : S)\ \mathsf{set}] & [Y, Z : (x : S)\ \mathsf{set}, Y(x) \leftrightarrow Z(x)\ true\ [x : S]] \\ & \vert & \vert \\ c \in \mathcal{P}(S) & d(Y) \in C(\{Y\}) & d(Y) = d(Z) \in C(\{Y\}) \end{array}}{\mathsf{P}_{\mathsf{rec}}(c, d) \in C(c)}$$

But this rule requires the use of variables for propositional functions, which are difficult to justify since prop is not a set.

Moreover, a standard equality rule should be something similar to the following

$$\frac{\begin{array}{cccc} [x : S] & [Y : (x : S)\ \mathsf{set}] & [Y, Z : (x : S)\ \mathsf{set}, Y(x) \leftrightarrow Z(x)\ true\ [x : S]] \\ \vert & \vert & \vert \\ U(x)\ \mathsf{set} & d(Y) \in C(\{Y\}) & d(Y) = d(Z) \in C(\{Y\}) \end{array}}{\mathsf{P}_{\mathsf{rec}}(\{(x : S)\ U(x)\}, d) = d((x : S)\ U(x)) \in C(\{(x : S)\ U(x)\})}$$

These rules are a direct consequence of the introduction rule and the equality introduction condition and they are already not completely within standard Martin-Löf's set theory. But, the problem is that, as they stand, they are not sufficient to make $\mathcal{P}(S)$ the set of the subsets of S. For instance, there is no way to obtain a proposition out of an element of $\mathcal{P}(S)$ and this does not fit with the introduction rule. Thus, to deal with the set $\mathcal{P}(S)$, one should add some rules which links its elements both with the elements of the type set and with those of the collection $\mathsf{set}_{\leftrightarrow}$, whose elements are propositions but whose equality is induced by the logical equivalence.

Again, we don't want to propose any particular rule since we are going to show that there can be no suitable rule, but we simply require that two conditions, which should be a consequence of such rules, are satisfied. The first condition is:

Elimination condition
Let $c \in \mathcal{P}(S)$ and $a \in S$. Then there exists a proposition $a \varepsilon c$.

This condition is suggested by the elimination rule that we have considered. In fact, a free use of the elimination rule with $C(z) \equiv \mathsf{set}_{\leftrightarrow}$ allows to obtain that $\mathsf{P}_{\mathsf{rec}}(c, (Y)\ Y(a))$ is an element of $\mathsf{set}_{\leftrightarrow}$ and hence that it is a proposition and we can identify such a proposition with $a \varepsilon c$. Of course, the above condition is problematic because it requires the existence of a proposition but it gives no knowledge about it; in particular it is not clear if one has to require a new

proposition (which are its canonical elements? which are its introduction and elimination rules?) or an old one (which proposition should one choose?).

As a consequence of the suggested equality rule, we require the following equality condition.

Equality condition
Suppose $U(x)$ set $[x : S]$ and $a : S$ then $a\varepsilon\{(x : S)\ U(x)\} \leftrightarrow U(a)$ *true*.

This condition can be justified in a way similar to the justification of the elimination condition, but using the equality rule instead of the elimination rule; in fact, supposing $U(x)$ set $[x : S]$ and $a : S$, the equality rule allows to obtain that $a\varepsilon\{(x : S)\ U(x)\}$ and $U(a)$ are equal elements of $\mathsf{set}_{\leftrightarrow}$ which yields our condition. This condition cannot be justified from a semantical point of view since we have no way to recover the proof element for its conclusion; this is the requirement which allows us to develop our proof in the next section without furnishing term constructors for classical logic.

It is worth noting that no form of η-equality, like

$$\frac{c \in \mathcal{P}(S)}{\{(x : S)\ x\varepsilon c\} = c \in \mathcal{P}(S)} \quad x \notin VF(c),$$

is required on $\mathcal{P}(S)$, but its validity is a consequence of the suggested elimination rule for $\mathcal{P}(S)$ at least within the extensional version of Martin-Löf's set theory eTT. This theory is obtained from iTT by substituting the intensional equality proposition by the extensional equality proposition $\mathsf{Eq}(A, a, b)$ which allows to deduce $a = b \in A$ from a proof of $\mathsf{Eq}(A, a, b)$. The problem with extensional equality is that it causes the lack of decidability of the equality judgement; for this reason it is usually rejected in the present version of the theory. To prove the η-equality in eTT let us assume that Y is a subset of S and that $x : S$, then $Y(x)$ set and hence $x\varepsilon\{Y\} \leftrightarrow Y(x)$ *true* holds because of the equality condition and it yields $\mathsf{Eq}(\mathcal{P}S, \{(x : S)\ x\varepsilon\{Y\}\}, \{Y\})$; thus, if $c \in \mathcal{P}S$, by using the elimination rule one obtains $\mathsf{Eq}(\mathcal{P}S, \{(x : S)\ x\varepsilon c\}, c)$ and hence $\{(x : S)\ x\varepsilon c\} = c \in \mathcal{P}S$. Note that the last step is not allowed in iTT^P.

3 iTT^P is consistent

It is well known that by adding as a set to iTT the collection $\mathcal{P}(\mathbb{1})$, whose elements are (the code for) the non-dependent sets, but using an equality between its elements induced by the *intensional* equality between sets, one obtains an inconsistent extension of iTT [Jac89]. On the contrary, we will prove that any extension of iTT with a power-set as proposed in the previous section, i.e. where the equality between two elements of a power-set is induced by the provability equivalence, is consistent or at least it is not inconsistent because of the rules we proposed on the power-sets and the conditions we required.

The easiest way to prove such a result is to show first that iTT^P can be embedded in the extensional theory eTT^{Ω}, which is an extension of the extensional

version of type theory eTT only with the power-set $\Omega \equiv \mathcal{P}(\mathbb{1})$ of all the subsets of the one element set $\mathbb{1}$. Then we will prove that such a theory is consistent.

Thus we have the following formation and introduction rules

$$\Omega \ \mathsf{set} \qquad \Omega = \Omega \qquad \frac{U(x) \ \mathsf{set} \ [x : \mathbb{1}]}{\{(x : \mathbb{1}) \ U(x)\} \in \Omega}$$

Moreover, we require that the introduction equality condition holds, i.e. if $U(x) \leftrightarrow V(x) \ true \ [x : \mathbb{1}]$ then there exists a proof-term $\mathsf{c}(U, V)$ such that

$$\mathsf{c}(U, V) \in \{(x : \mathbb{1}) \ U(x)\} =_{\Omega} \{(x : \mathbb{1}) \ V(x)\}$$

where if $x, y : \Omega$ then $x =_{\Omega} y$ is the abbreviation for the extensional propositional equality set $\mathsf{Eq}(\Omega, x, y)$.

Now, the condition on the existence of a proposition $a \varepsilon c \ \mathsf{set} \ [a : \mathbb{1}, c : \Omega]$ can be satisfied by putting, for any $c \in \Omega$,

$$a \varepsilon c \equiv (c =_{\Omega} \top_{\mathbb{1}})$$

where $\top_{\mathbb{1}} \equiv \{(x : \mathbb{1}) \ x =_{\mathbb{1}} x\}$; here, any reference to the element a disappears in the definiens because all the elements in $\mathbb{1}$ are equal. Finally, we require that

$$\text{if} \ \ U(x) \ \mathsf{set} \ [x : \mathbb{1}] \ \ \text{then} \ \ (\{(x : \mathbb{1}) \ U(x)\} =_{\Omega} \top_{\mathbb{1}}) \leftrightarrow U(w) \ true \ [w : \mathbb{1}]$$

Now, any power-set can be defined by putting

$$\mathcal{P}(S) \equiv S \to \Omega$$

since, for any proposition $U(x) \ \mathsf{set} \ [x : S]$, one obtains an element in $\mathcal{P}(S)$ by putting

$$\{(x : S) \ U(x)\} \equiv \lambda((x : S) \ \{(w : \mathbb{1}) \ U(x)\})$$

where we suppose that w does not appear free in $U(x)$, which is in fact an element in $S \to \Omega$. Then the equality introduction condition holds provided that the propositional equality on functions is at least weakly extensional, i.e. for $f, g : A \to B$, $(\forall x \in A) \ (f(x) =_B g(x)) \ \to (\lambda x.f(x) =_{A \to B} \lambda x.g(x))$ is inhabited, as it happens when the extensional version of type theory is considered.

Moreover, for any element $c \in \mathcal{P}(S)$, i.e. a function from S into Ω, and any element $a \in S$, one obtains a proposition by putting

$$a \varepsilon c \equiv (c(a) =_{\Omega} \top_{\mathbb{1}})$$

which indeed satisfies the required equality condition.

Thus, any proof of $c \in \bot$ in iTT^P, i.e. any inconsistency in iTT^P, can be reconstructed in eTT^{Ω}. Hence, it is sufficient to show that this new theory is consistent and this will be done by defining an interpretation $\mathcal{I}$ of this theory into Zermelo-Fraenkel set theory with the axiom of choice ZFC.

The basic idea is to interpret any non-dependent set A into a set $\mathcal{I}(A)$ of ZFC and, provided that

$\mathcal{I}(A_1)$ is a set of ZFC,
$\mathcal{I}(A_2)$ is a map ¿from $\mathcal{I}(A_1)$ into the collection of all sets of ZFC,
$\ldots$,
$\mathcal{I}(A_n)$ is a map from the disjoint union

$$\biguplus_{\alpha_1 \in \mathcal{I}(A_1), \ldots, \alpha_{n-2} \in \mathcal{I}(A_{n-2})(\langle \alpha_1, \ldots, \alpha_{n-3} \rangle)} \mathcal{I}(A_{n-1})(\langle \alpha_1, \ldots, \alpha_{n-2} \rangle)$$

into the collection of all sets of ZFC, then the dependent set

$$A(x_1, \ldots, x_n) \text{ set } [x_1 : A_1, \ldots, x_n : A_n(x_1, \ldots, x_{n-1})],$$

i.e. the propositional function $A : (x_1 : A_1) \ldots (x_n : A_n(x_1, \ldots, x_{n-1}))$ set, is interpreted into a map from the disjoint union

$$\biguplus_{\alpha_1 \in \mathcal{I}(A_1), \ldots, \alpha_{n-1} \in \mathcal{I}(A_{n-1})(\langle \alpha_1, \ldots, \alpha_{n-2} \rangle)} \mathcal{I}(A_n)(\langle \alpha_1, \ldots, \alpha_{n-1} \rangle)$$

into the collection of all sets of ZFC.

Since the axiom of replacement allows to avoid the use of maps into the *collection* of all sets, which can be substituted by indexed families of sets, all the interpretation can be explained within basic ZFC, but we think that the approach we use here is more perspicuous and well suited for the interpretation of a theory like eTT^{Ω} where propositional functions have to be considered.

The interpretation $\mathcal{I}(a)$ of a closed term $a \in A$, where A is a non-dependent set, will be an element of the set $\mathcal{I}(A)$ whereas the interpretation of a not-closed term

$$a(x_1, \ldots, x_n) \in A(x_1, \ldots, x_n) \ [x_1 : A_1, \ldots, x_n : A_n(x_1, \ldots, x_{n-1})],$$

i.e. the function-element $a : (x_1 : A_1) \ldots (x_n : A_n(x_1, \ldots, x_{n-1}))\ A(x_1, \ldots, x_n)$, is a function $\mathcal{I}(a)$ which, when applied to the element

$$\alpha \in \biguplus_{\alpha_1 \in \mathcal{I}(A_1), \ldots, \alpha_{n-1} \in \mathcal{I}(A_{n-1})(\langle \alpha_1, \ldots, \alpha_{n-2} \rangle)} \mathcal{I}(A_n)(\langle \alpha_1, \ldots, \alpha_{n-1} \rangle)$$

gives the element $\mathcal{I}(a)(\alpha)$ of the set $\mathcal{I}(A)(\alpha)$.

Now, for the basic sets we put: $\mathcal{I}(\bot) \equiv \emptyset$, $\mathcal{I}(\mathbb{1}) \equiv \{\emptyset\}$ and $\mathcal{I}(\mathsf{Bool}) \equiv \{\emptyset, \{\emptyset\}\}$ and there is an obvious interpretation of their elements. Moreover, the sets $\Sigma(A, B)$ and $\Pi(A, B)$ (or, equivalently, the propositions $(\exists x \in A)\ B(x)$ and $(\forall x \in A)\ B(x)$) are interpreted respectively in the disjoint union and the indexed product of the interpretation of $B(x)$ indexed on the elements of the interpretation of A. The disjoint sum set $A + B$ is interpreted in the disjoint union of the interpretation of A and B and the interpretation of the extensional equality proposition $a =_A b$ is the characteristic function of the equality of the interpretation of a and b.

Finally, the interpretation of the set Ω is the set $\{\emptyset, \{\emptyset\}\}$.

Moreover, the judgement $A(x_1, \ldots, x_n)$ *true* $[\Gamma]$ is interpreted in $\mathcal{I}(A)(\gamma) \neq \emptyset$ for every $\gamma \in \mathcal{I}(\Gamma)$, which gives $\mathcal{I}(A) \neq \emptyset$ when A is a non-dependent set.

The interpretation of all the terms is straightforward; thus, here we only illustrate the interpretation of the elements related to the set Ω:

$$\mathcal{I}(\{(x : \mathbb{1})\ U(x)\}) \equiv \begin{cases} \emptyset & \text{if } \mathcal{I}(U(*)) = \emptyset \\ \{\emptyset\} & \text{if } \mathcal{I}(U(*)) \neq \emptyset \end{cases}$$

and $\mathcal{I}(\mathsf{c}(U, V)) \equiv \emptyset$.

After these definitions, for any subset U of $\mathbb{1}$, $\mathcal{I}((\{(x : \mathbb{1})\ U(x)\} =_\Omega \top_\mathbb{1}) \leftrightarrow U(*)) \neq \emptyset$ by the axiom of choice and hence the equality condition is valid.

It is tedious, but straightforward, to check that all the rules of eTT^Ω are valid in this interpretation and hence that any proof of the judgement $a \in \bot$ within eTT^Ω, i.e. any form of inconsistency, would result in a proof that there is some element in $\emptyset$, that is an inconsistency in ZFC.

4 iTT^P is classical

We are going to prove that iTT^P gives rise to classical logic, i.e. for any proposition A the judgement $A \vee \neg A$ *true* holds. Even if iTT^P is *not* a topos, the proof that we show here is obtained by adapting to our framework an analogous result stating that any topos satisfying the axiom of choice is boolean. Among the various proofs of this result (cf. for instance [LS86],[Bel88]), which goes back to Diaconescu's work showing that one obtains ZF by adding the axiom of choice to IZF [Dia75], we choose to translate the proof of Bell [Bel88], because it is very well suited to work in iTT^P since it is almost completely developed within local set theory instead that in topos theory, except for the use of a choice rule.

In iTT^P the result is a consequence of the strong elimination rule for disjoint union which allows to prove the so called *intuitionistic axiom of choice*, i.e.

$$> ((\forall x \in A)(\exists y \in B)\ C(x, y)) \to ((\exists f \in A \to B)(\forall x \in A)\ C(x, f(x)))\ \mathit{true}$$

Let us recall the proof [Mar84]. Assume that $h \in (\forall x \in A)(\exists y \in B)\ C(x, y)$ and that $x \in A$. Then $h(x) \in (\exists y \in B)\ C(x, y)$. Let $\mathsf{p}(-)$ and $\mathsf{q}(-)$ be the first and the second projection respectively; then the elimination rule for the set of the disjoint union allows to prove that $\mathsf{p}(h(x)) \in B$ and $\mathsf{q}(h(x)) \in C(x, \mathsf{p}(h(x)))$. Hence, by putting $f \equiv \lambda x.\mathsf{p}(h(x))$ we obtain both $f \in A \to B$ and $\mathsf{q}(h(x)) \in C(x, f(x))$ since, by β-equality, $f(x) \equiv (\lambda x.\mathsf{p}(h(x)))(x) = \mathsf{p}(h(x))$. Finally, we conclude by *true introduction*.

Since in the following we will mainly use the power-set $\mathcal{P}(\mathbb{1})$, we introduce some abbreviations besides of $\Omega \equiv \mathcal{P}(\mathbb{1})$ and $\top_\mathbb{1} \equiv \{(w : \mathbb{1})\ w =_\mathbb{1} w\}$ already used in section 3; let us suppose that U is any proposition and $w : \mathbb{1}$ is a variable which does not appear free in U, then we put $[U] \equiv \{(w : \mathbb{1})\ U\}$ and, supposing $p \in \Omega$, we put $\overline{p} \equiv *\varepsilon p$. Moreover, following a standard practice, supposing A is a proposition, sometimes we will simply write A to assert the judgement A *true*.

It is convenient to state here all the properties of the intensional equality proposition Id that we need in the following. First, we recall two well known

results: Id is an equivalence relation, and if A and B are sets and $a =_A c$ and $f =_{A\to B} g$ then $f(a) =_B g(c)$ (for a proof see [NPS90], page 64).

Moreover, the following properties of Id are specific of the new set Ω. They are similar to the properties that the set Id enjoys when it is used on elements of the set U_0, i.e. the universe of the small sets, which we will not use at all. In fact, Ω resembles this set, but it also differs because of the considered equality and because a code for each set is present in Ω whereas only the codes for the small sets can be found in U_0.

Lemma 4.1 *If $p =_\Omega q$ then $\overline{p} \leftrightarrow \overline{q}$.*

Proof. Let $x \in \Omega$; then $\overline{x} \leftrightarrow \overline{x}$ and hence $\overline{p} \leftrightarrow \overline{q}$ is a consequence of $p =_\Omega q$ by Id-elimination. 2

Lemma 4.2 $\neg(\mathsf{true} =_{\mathsf{Bool}} \mathsf{false})$.

Proof. Let $x \in \mathsf{Bool}$; then $\mathsf{if}\ x\ \mathsf{then}\ [\mathbb{1}]\ \mathsf{else}\ [\bot] \in \Omega$. Now, suppose that $\mathsf{true} =_{\mathsf{Bool}} \mathsf{false}$, then $\mathsf{if\ true\ then}\ [\mathbb{1}]\ \mathsf{else}\ [\bot] =_\Omega \mathsf{if\ false\ then}\ [\mathbb{1}]\ \mathsf{else}\ [\bot]$ which yields $[\mathbb{1}] =_\Omega [\bot]$ by boole-equality and transitivity. Thus, by the previous lemma $\overline{[\mathbb{1}]} \leftrightarrow \overline{[\bot]}$, but $\overline{[\mathbb{1}]} \leftrightarrow \mathbb{1}$ and $\overline{[\bot]} \leftrightarrow \bot$ by the equality condition; hence $\bot$ *true* and thus, by discharging the assumption $\mathsf{true} =_{\mathsf{Bool}} \mathsf{false}$, we obtain the result. 2

Now, we will start the proof of the main result of this section. The trick to internalize the proof in [Bel88] within iTT^P is stated in the following lemma.

Lemma 4.3 *For any proposition A, if A true then*

$$\mathsf{c}((w : \mathbb{1})\ A, (w : \mathbb{1})\ w =_{\mathbb{1}} w) \in [A] =_\Omega \top_{\mathbb{1}}$$

and hence $[A] =_\Omega \top_{\mathbb{1}}$ true; moreover, if $[A] =_\Omega \top_{\mathbb{1}}$ true then A true.

Proof. If A *true* then $A \leftrightarrow (w =_{\mathbb{1}} w)$ *true* $[w : \mathbb{1}]$; hence, by the equality introduction condition, $\mathsf{c}((w : \mathbb{1})\ A, (w : \mathbb{1})\ w =_{\mathbb{1}} w) \in [A] =_\Omega \top_{\mathbb{1}}$, and thus $[A] =_\Omega \top_{\mathbb{1}}$ *true* by *true-introduction*; on the other hand, if $[A] =_\Omega \top_{\mathbb{1}}$ *true* then $\overline{[A]} \leftrightarrow \overline{\top_{\mathbb{1}}}$ by lemma 4.1, but $\overline{[A]} \leftrightarrow A$ and $* =_{\mathbb{1}} * \leftrightarrow \overline{\top_{\mathbb{1}}}$ by the equality condition, and hence A *true* since $* =_{\mathbb{1}} *$ *true*. 2

After this lemma, for any proposition A it is possible to obtain a logically equivalent proposition, i.e. $[A] =_\Omega \top_{\mathbb{1}}$, such that, if A *true*, the proof element $\mathsf{c}((w : \mathbb{1})\ A, (w : \mathbb{1})\ w =_{\mathbb{1}} w)$ of $[A] =_\Omega \top_{\mathbb{1}}$ has no memory of the proof element which testifies the truth of A. We will see that this property is crucial to get the main result. We will use the above lemma immediately in the next one where, instead of the proposition $\overline{\mathsf{p}(w)} \vee \overline{\mathsf{q}(w)}\ \mathsf{set}\ [w : \Omega \times \Omega]$, we write $[\overline{\mathsf{p}(w)} \vee \overline{\mathsf{q}(w)}] =_\Omega \top_{\mathbb{1}}\ \mathsf{set}\ [w : \Omega \times \Omega]$ in order to avoid that the proof-term in the main statement depends on the truth of the first or of the second disjunct.

Proposition 4.4 *In iTT^P the following proposition*

$$(\forall z \in \Sigma(\Omega \times \Omega, (w)\ [\overline{\mathsf{p}(w)}\ \vee\ \overline{\mathsf{q}(w)}] =_\Omega \top_{\mathbb{1}}))$$
$$(\exists x \in \mathsf{Bool})\ (x =_{\mathsf{Bool}} \mathsf{true}\ \rightarrow\ \overline{\mathsf{p}(\mathsf{p}(z))})\ \wedge\ (x =_{\mathsf{Bool}} \mathsf{false}\ \rightarrow\ \overline{\mathsf{q}(\mathsf{p}(z))})$$

is true.

Proof. Suppose $z \in \Sigma(\Omega \times \Omega, (w)\ [\overline{\mathsf{p}(w)}\ \vee\ \overline{\mathsf{q}(w)}] =_\Omega \top_{\mathbb{1}})$ then $\mathsf{p}(z) \in \Omega \times \Omega$ and $\mathsf{q}(z)$ is a proof of $[\overline{\mathsf{p}(\mathsf{p}(z))}\ \vee\ \overline{\mathsf{q}(\mathsf{p}(z))}] =_\Omega \top_{\mathbb{1}}$. Thus, by lemma 4.3, $\overline{\mathsf{p}(\mathsf{p}(z))}\ \vee\ \overline{\mathsf{q}(\mathsf{p}(z))}$. Now, the result can be proved by $\vee$-elimination. In fact, if $\overline{\mathsf{p}(\mathsf{p}(z))}$ *true* then $\mathsf{true} =_{\mathsf{Bool}} \mathsf{true} \rightarrow \overline{\mathsf{p}(\mathsf{p}(z))}$; moreover, $\neg(\mathsf{true} =_{\mathsf{Bool}} \mathsf{false})$ by lemma 4.2 and hence $\mathsf{true} =_{\mathsf{Bool}} \mathsf{false} \rightarrow \overline{\mathsf{q}(\mathsf{p}(z))}$. Thus we obtain that

$$(\exists x \in \mathsf{Bool})\ (x =_{\mathsf{Bool}} \mathsf{true} \rightarrow \overline{\mathsf{p}(\mathsf{p}(z))})\ \wedge\ (x =_{\mathsf{Bool}} \mathsf{false} \rightarrow \overline{\mathsf{q}(\mathsf{p}(z))})$$

On the other hand, by a similar proof we reach the same conclusion starting from the assumption $\overline{\mathsf{q}(\mathsf{p}(z))}$ *true*. 2

Thus, we can use the intuitionistic axiom of choice to obtain:

Proposition 4.5 *In iTT^P the following proposition*

$$(\exists f \in \Sigma(\Omega \times \Omega, (w)\ [\overline{\mathsf{p}(w)}\ \vee\ \overline{\mathsf{q}(w)}] =_\Omega \top_{\mathbb{1}}) \rightarrow \mathsf{Bool})$$
$$(\forall z \in \Sigma(\Omega \times \Omega, (w)\ [\overline{\mathsf{p}(w)}\ \vee\ \overline{\mathsf{q}(w)}] =_\Omega \top_{\mathbb{1}}))$$
$$(f(z) =_{\mathsf{Bool}} \mathsf{true}\ \rightarrow\ \overline{\mathsf{p}(\mathsf{p}(z))})\ \wedge\ (f(z) =_{\mathsf{Bool}} \mathsf{false}\ \rightarrow\ \overline{\mathsf{q}(\mathsf{p}(z))})$$

is true.

Now, suppose that A is any proposition; then

$$\langle\langle [A], \top_{\mathbb{1}}\rangle, \mathsf{k}([A], \top_{\mathbb{1}})\rangle \in \Sigma(\Omega \times \Omega, (w)\ [\overline{\mathsf{p}(w)}\ \vee\ \overline{\mathsf{q}(w)}] =_\Omega \top_{\mathbb{1}})$$

where $\mathsf{k}(x, y)$ is short for $\mathsf{c}((w : \mathbb{1})\ \overline{\mathsf{p}(\langle x, y\rangle)}\ \vee\ \overline{\mathsf{q}(\langle x, y\rangle)}, (w : \mathbb{1})\ w =_{\mathbb{1}} w)$.

In fact, $\langle [A], \top_{\mathbb{1}}\rangle \in \Omega \times \Omega$ and $\overline{\top_{\mathbb{1}}}$ *true*, hence $\overline{\mathsf{p}(\langle [A], \top_{\mathbb{1}}\rangle)}\ \vee\ \overline{\mathsf{q}(\langle [A], \top_{\mathbb{1}}\rangle)}$; thus the result follows by lemma 4.3.

Now, let f be the choice function in the proposition 4.5; then

$$f(\langle\langle [A], \top_{\mathbb{1}}\rangle, \mathsf{k}([A], \top_{\mathbb{1}})\rangle) =_{\mathsf{Bool}} \mathsf{true}\ \rightarrow\ \overline{[A]}$$

But

$$(f(\langle\langle [A], \top_{\mathbb{1}}\rangle, \mathsf{k}([A], \top_{\mathbb{1}})\rangle) =_{\mathsf{Bool}} \mathit{true}) \vee (f(\langle\langle [A], \top_{\mathbb{1}}\rangle, \mathsf{k}([A], \top_{\mathbb{1}})\rangle) =_{\mathsf{Bool}} \mathsf{false})$$

since the set Bool is decidable (for a proof see [NPS90], page 177), and hence, by $\vee$-elimination and a little of intuitionistic logic, one obtains that

$$(1)\quad \overline{[A]}\ \vee\ (f(\langle\langle [A], \top_{\mathbb{1}}\rangle, \mathsf{k}([A], \top_{\mathbb{1}})\rangle) =_{\mathsf{Bool}} \mathsf{false})$$

Analogously one can prove that

$$(2)\quad \overline{[A]}\ \vee\ (f(\langle\langle \top_{\mathbb{1}}, [A]\rangle, \mathsf{k}(\top_{\mathbb{1}}, [A])\rangle) =_{\mathsf{Bool}} \mathsf{true})$$

Thus, by using distributivity on the conjunction of (1) and (2), one finally obtains

Proposition 4.6 *For any proposition A in iTT^P the following proposition*

$$(\exists f \in \Sigma(\Omega \times \Omega, (w)\ [\overline{\mathsf{p}(w)}\ \vee\ \overline{\mathsf{q}(w)}] =_\Omega \top_{\mathbb{1}}) \to \mathsf{Bool})$$
$$\overline{[A]} \vee ((f(\langle\langle [A], \top_{\mathbb{1}}\rangle, \mathsf{k}([A], \top_{\mathbb{1}})\rangle) =_{\mathsf{Bool}} \mathsf{false}) \wedge$$
$$(f(\langle\langle \top_{\mathbb{1}}, [A]\rangle, \mathsf{k}(\top_{\mathbb{1}}, [A])\rangle) =_{\mathsf{Bool}} \mathsf{true}))$$

is true.

Now, let us assume $\overline{[A]}$ *true*; then $[A] =_\Omega \top_{\mathbb{1}}$ *true* by lemma 4.3 and hence

$$\langle\langle [A], \top_{\mathbb{1}}\rangle, \mathsf{k}([A], \top_{\mathbb{1}})\rangle =_{\Sigma(\Omega\times\Omega,\ldots)} \langle\langle \top_{\mathbb{1}}, \top_{\mathbb{1}}\rangle, \mathsf{k}(\top_{\mathbb{1}}, \top_{\mathbb{1}})\rangle$$

since $\lambda x.\langle\langle x, \top_{\mathbb{1}}\rangle, \mathsf{k}(x, \top_{\mathbb{1}})\rangle$ is a function from Ω to $\Sigma(\Omega \times \Omega, (w)\ [\overline{\mathsf{p}(w)}\ \vee\ \overline{\mathsf{q}(w)}] =_\Omega \top_{\mathbb{1}})$. Thus

$$f(\langle\langle [A], \top_{\mathbb{1}}\rangle, \mathsf{k}([A], \top_{\mathbb{1}})\rangle) =_{\mathsf{Bool}} f(\langle\langle \top_{\mathbb{1}}, \top_{\mathbb{1}}\rangle, \mathsf{k}(\top_{\mathbb{1}}, \top_{\mathbb{1}})\rangle)$$

where f is the function whose existence is stated by the proposition 4.6.

With the same assumption, also

$$f(\langle\langle \top_{\mathbb{1}}, [A]\rangle, \mathsf{k}(\top_{\mathbb{1}}, [A])\rangle) =_{\mathsf{Bool}} f(\langle\langle \top_{\mathbb{1}}, \top_{\mathbb{1}}\rangle, \mathsf{k}(\top_{\mathbb{1}}, \top_{\mathbb{1}})\rangle)$$

can be proved in a similar way; hence, by transitivity of the equality proposition,

$$f(\langle\langle [A], \top_{\mathbb{1}}\rangle, \mathsf{k}([A], \top_{\mathbb{1}})\rangle) =_{\mathsf{Bool}} f(\langle\langle \top_{\mathbb{1}}, [A]\rangle, \mathsf{k}(\top_{\mathbb{1}}, [A])\rangle)$$

It is worth noting that this result depends mainly on lemma 4.3, and hence on the equality introduction condition whose premise is a "true judgement". Indeed, $\lambda x.\langle\langle x, \top_{\mathbb{1}}\rangle, \mathsf{k}(x, \top_{\mathbb{1}})\rangle$ and $\lambda x.\langle\langle \top_{\mathbb{1}}, x\rangle, \mathsf{k}(\top_{\mathbb{1}}, x)\rangle$ yield equal results when applied to $\top_{\mathbb{1}}$ since they do not depend on the proof-terms used to derive the two judgements

$$(\overline{x} \vee \overline{\top_{\mathbb{1}}}) \leftrightarrow (w =_{\mathbb{1}} w)\ \mathit{true}\ [x : \Omega, w : \mathbb{1}]$$

and

$$(\overline{\top_{\mathbb{1}}} \vee \overline{x}) \leftrightarrow (w =_{\mathbb{1}} w)\ \mathit{true}\ [x : \Omega, w : \mathbb{1}]$$

In the case we admit dependency on the proof-terms in the equality introduction condition we can redo the whole proof if we assume that uniqueness of equality proofs (see the rules in [HS95] or [Hof95]) holds and we replace $\overline{a}$ with $a =_\Omega \top_{\mathbb{1}}$, where $a \in \Omega$, everywhere in the proof in order to get an actual proof-term at this point.

Now, by assuming both $\overline{[A]}$ *true* and

$$(f(\langle\langle [A], \top_{\mathbb{1}}\rangle, \mathsf{k}([A], \top_{\mathbb{1}})\rangle) =_{\mathsf{Bool}} \mathsf{false})\ \wedge\ (f(\langle\langle \top_{\mathbb{1}}, [A]\rangle, \mathsf{k}(\top_{\mathbb{1}}, [A])\rangle) =_{\mathsf{Bool}} \mathsf{true})$$

one can conclude $\mathsf{true} =_{\mathsf{Bool}} \mathsf{false}$. On the other hand, we know that $\neg(\mathsf{true} =_{\mathsf{Bool}} \mathsf{false})$ holds by lemma 4.2. Hence $\bot$ follows and so we obtain that the judgement $\neg\overline{[A]}$ *true* holds by discharging the assumption $\overline{[A]}$ *true*. Then, by using proposition 4.6 and a little of intuitionistic logic, we can conclude $(\overline{[A]}\ \vee\ \neg\overline{[A]})$ *true* which, by the equality condition, yields $(A\ \vee\ \neg A)$ *true*. Thus, if we could give suitable rules for the power-sets that allow our conditions to hold and follow the usual meaning for the judgement C *true*, i.e. C *true* holds if and only if there exists a proof element for the proposition C, then we would have a proof element for the proposition $A\ \vee\ \neg A$, which is expected to fail.

5 Conclusion

To help the reader who knows the proof in [Bel88], it may be useful to explain the differences between the original proof and that presented in the previous section. Our proof is not the plain application of Bell's result to iTT^P since iTT^P is not a topos. It is possible to build a topos out of the extensional theory eTT^P obtained by adding a power-set constructor to eTT, if one adds to it also the rule of η-equality for power-sets, like in the end of section 2. However, we showed that it is not necessary to be within a topos to reconstruct Diaconescu's result and that a weaker theory is sufficient.

This fact suggests that it is not possible to extend Martin-Löf's set theory, where sets and propositions are identified and proof-elements can be provided for any provable proposition, to an intuitionistic theory of sets fully equipped with power-sets satisfying the conditions discussed in section 2, provided that we want to preserve the constructive meaning of the connectives. However, observe that the requirement of uniformity in the extensional equality condition is crucial to carry on our proof. Therefore, it seems that there is still some hope to get power-sets in constructive type theory by dropping uniformity. But, it is worth recalling that an analogous proof of excluded middle can be performed also without uniformity if the uniqueness of equality proofs holds. Thus, no constructive power-set can be added if type theory is endowed with pattern matching, which is usually used in most of its actual implementations.

References

[Bel88] J.L. Bell. *Toposes and local set theory: an introduction.* Clarendon Press, Oxford, 1988.

[Coq90] T. Coquand. Metamathematical investigation of a calculus of constructions. In P. Odifreddi, editor, *Logic in Computer Science*, pages 91–122. Academic Press, 1990.

[dB80] N.G. de Bruijn. A survey of the project automath. In J.P. Seldin and J.R. Hindley, editors, *To H. B. Curry: Essays on Combinatory Logic, Lambda Calculus and Formalism*, pages 589–606. Academic Press, London, 1980.

[Dia75] R. Diaconescu. Axiom of choice and complementation. *Proc. Amer. Math. Soc.*, 51:176–178, 1975.

[GR94] E. Griffor and M. Rathjen. The strength of some Martin-Löf's type theories. *Arch. Math. Logic*, 33:347–385, 1994.

[Hof95] M. Hofmann. *Extensional concepts in intensional type theory.* PhD Thesis, University of Edinburgh, 1995.

[HS95] M. Hofmann and T. Streicher. The groupoid interpretation of type theory. In J. Smith G. Sambin, editor, *Twenty five years of Constructive Type Theory*, pages 83–111, Venice, 1995.

[Jac89] B. Jacobs. The inconsistency of higher order extensions of Martin-Löf's type theory. *Journal of Phil. Logic.*, 18:399–422, 1989.

[LS86] J. Lambek and P. J. Scott. *An introduction to higher order categorical logic.*, volume 7 of *Studies in Advanced Mathematics*. Cambridge University Press, 1986.

[Luo90] Z. Luo. *An extended calculus of constructions*. PhD Thesis, University of Edinburgh, 1990.

[Mar71] P. Martin-Löf. Hauptsatz for the intuitionistic theory of iterated inductive definitions. In J.E. Fenstad, editor, *The Second Scandinavian Logic Symposium*. North-Holland Publishing Company, 1971.

[Mar84] P. Martin-Löf. *Intuitionistic Type Theory, notes by G. Sambin of a series of lectures given in Padua, June 1980*. Bibliopolis, Naples, 1984.

[NPS90] B. Nordström, K. Peterson, and J. Smith. *Programming in Martin-Löf's Type Theory, An introduction*. Clarendon Press, Oxford, 1990.

[SV95] G. Sambin and S. Valentini. Building up a tool-box for Martin-Löf's type theory. In J. Smith G. Sambin, editor, *Twenty five years of Constructive Type Theory*, pages 221–244, Venice, 1995.

[Val95] S. Valentini. The forget-restore principle: a paradigmatic example. In J. Smith G. Sambin, editor, *Twenty five years of Constructive Type Theory*, pages 275–283, Venice, 1995.