Proofs for Higher-Order SMT and Beyond

Chad E. Brown[1], Mikoláš Janota[2], and Cezary Kaliszyk[3]

[1] Czech Technical University in Prague
Czech Institute of Informatics, Robotics and Cybernetics
Prague, Czech Republic
[2] Czech Technical University in Prague
Czech Institute of Informatics, Robotics and Cybernetics
Prague, Czech Republic
Mikolas.Janota@cvut.cz
[3] University of Innsbruck
Innsbruck, Austria
cezary.kaliszyk@uibk.ac.at

Abstract

to do

1 Introduction

A preliminary proposal for SMT-LIB Version 3.0 was recently published online [**?**]. According to this proposal, there are plans to extend SMT in serious ways, essentially bringing an expressive power somewhere between Church's simple type theory [**?**] (by including arrow types) and the Calculus of Inductive Constructions [**?**, **?**, **?**] (by including dependent types and inductively defined types). In addition, a working group on SMT proofs was announced [**?**] with the goal of developing a standard for "producing independently checkable proofs." Of course, having a standard notion of proof for SMT3 will require clarifying the intended semantics of SMT3 so that there is precision about what sets of formulas should be unsatisfiable (so there might be a "proof" of inconsistency) or satisfiable (so there might be a "model"). We consider the possibility of using higher-order set theory via the well-known Werner-Aczel semantics of Calculus of Inductive Constructions [] to provide both a clear semantics and a notion of checkable proof that is likely to be sufficient for SMT3 as well as possible future extensions. We also give examples to demonstrate the feasability of the approach.

2 Models and Proofs in General

In the best case scenario a logic provides a clear definition of propositions, a rigorous definition of when a proposition is provable and a class of interpretations with a satisfaction relation. A proposition is considered valid if it is true in every interpretation in the class. The logic satisfies soundness and completeness if provability coincides with validity. The most well-known case is classical first-order logic with any number of proof systems and interpretations given by Tarski-style semantics.

Church's simple type theory provides another example of such a logic. In Church's original paper [**?**] there is a clear definition of types, terms (some of which are propositions) and a Hilbert style proof system. Henkin [**?**] later gave a notion of semantics for which a completeness result could be proven. (Technically Henkin's interpretations were not all sound with respect to Church's functional extensionality axiom, but this was corrected by Andrews [**?**].) An equality-based version of Church's simple type theory with a Hilbert style proof system and a notion

of interpretation (called *general models*) following the Henkin-Andrews approach is presented in [**?**]. Furthermore in [**?**] one can find proofs of soundness, completeness and the usual results associated with first-order logic such as the Lowenheim-Skolem Theorem and the Compactness Theorem.

For more serious extensions of Church's simple type theory – such as the Calculus of Inductive Constructions – there does not seem to be an effort to create a Henkin-Andrews notion of interpretation for which one could prove soundness and completeness. Instead research into semantics for type theories has tended to go in the direction of category theory [**?**, **?**] and the most interesting interpretations are not classical.

In terms of soundness alone, there is one well-known set theoretic interpretation of type theories like the Calculus of Inductive Constructions. The interpretation is classical, extensional and satisfies proof irrelevance.[1] It was described by Werner [**?**] and Aczel [**?**] with more details found in the works of Werner, Lee and Barras [**?**, **?**]. In this model, the universe of propositions is interpreted as a two element set – one of which is empty (having no proofs) representing "false" and the other being a singleton (having one proof) representing "true." Being a two element set makes it essentially the same as the interpretation of the type of booleans, as seems to be the intended treatment of propositions as booleans in SMT. Types are interpreted as sets (including the empty set) which live in some universe closed under various set theoretic operations. Coq is a well-known proof assistant based on the Calculus of Inductive Constructions (CIC) and each type universe is closed under the formation of (dependent) function types and inductively defined types. The Werner-Aczel style of interpretation would interpret each of Coq's universes as a set U closed under the corresponding set-theoretic operations (e.g., if A and B are in the set U, then the set B^A of functions is in the set U).

An alternative to attempting to obtain a Henkin-Andrews style semantics for which soundness and completeness can be proven is to simply take the standard set theoretic semantics *but* allow the model of the underlying set theory to change. That is, instead of defining a proposition as valid if it is true in every standard set theoretic interpretation, one could define it as being valid if it is true in every standard set theoretic interpretation living in a model of, say, first-order ZFC. Validity would then become recursively enumerable again and we clearly have a complete proof system (given by any proof system for first-order ZFC). We explore this possibility in this paper, except we use higher-order Tarski Grothendieck (HOTG) as described in [**?**] instead of first-order ZFC. The reason for using higher-order instead of first-order is to make the theory finitely axiomatizable. (We still obtain complete calculi via Henkin-Andrews semantics.) The reason for using Tarski Grothendieck instead of Zermelo Fraenkel is to ensure we have sufficient set theoretic universes for interpreting the type theoretic universes of CIC. For more information, a longer discussion is in the unpublished paper [**?**], from which some of the material form this article was taken.

3 Set Theory

Let us consider the possibility of simply using a Werner-Aczel style (classical, extensional, proof irrelevant) interpretation of SMT3 and take proofs to be proofs of the resulting set theoretic propositions. Since type theory is the dominant paradigm in interactive theorem proving at the moment, the possibility of using set theory might be dismissed out of hand. A common objection is that set theory requires infinitely many axioms, though this is no longer true if one works in a slightly stronger set theory than first-order ZFC axiomatized in Church's type

[1] Proof irrelevance means all proofs of a given proposition are equal.

theory. Furthermore, a natural deduction proof system for Church's type theory has a well known notion of proof term. To make the case that the option of using set theory should at least be considered, we assert three claims.

Claim 1: Set theory has been the most commonly accepted foundation of mathematics for over a century, and continues to remain so.

Claim 2: Church's simple type theory is a concise language extending first-order logic in which many set theories have a finite axiomatization.

Claim 3: The Curry-Howard correspondence [**?**] gives a well-understood notion of proof term for a natural deduction proof system for an appropriate presentation of Church's simple type theory.

Together these assertions are intended to make clear that using proof terms for a formal set theory is based on a long history and does not require novel ideas. The first axiom system for set theory dates back to Zermelo in 1908 [**?**] and even the addition of Tarski universes dates back to 1938 [**?**]. A typical complaint about set theory is that it has no finite first-order axiomatization, and so one might think schemes are required. However, if we pass from first-order logic to Church's type theory it becomes easy to write second-order axioms that would otherwise be schemes of infinitely many first-order axioms [**?**, **?**, **?**, **?**].[2] Church's type theory dates back to 1940 [**?**] and Henkin's completeness result dates back to 1950 [**?**]. As mentioned above, Church's type theory satisfies the usual first-order properties (relative to Henkin-Andrews semantics), so using it as the underlying logic instead of first-order logic is not such a radical change. Finally we note that the earliest proof checker, AUTOMATH [**?**, **?**], dates back to 1968. AUTOMATH represented proofs using a Curry-Howard style proof representation (independently created by de Bruijn). In summary, all the ideas for having a clear, simple formulation of set theory (with a finite presentation) – including a notion of checkable proofs – are over half a century old. They are mature, well-understood ideas. The worst one could say about some of the ideas is that they may be out of fashion at the moment, but fashion is hardly a reason to dismiss the ideas.

It is certainly conceivable that proof terms for propositions obtained by translating from SMT3 problems to set theory via the Werner-Aczel approach might turn out to be impractical, either because the proof terms are too large or because their correctness is overly difficult to check. In order to make a preliminary judgment about the practicality of the approach, let us consider a few examples.

4 Examples

We now consider a few examples. All the examples will only use features of SMT2. In each case we will show the result of translating the problem to a formal set theory and note there is either a formal proof of the set theoretic proposition or a formal proof of its negation. We briefly describe the proofs in each case. For the formal set theory we will use the Megalodon system[3] (the successor to the Egal system [**?**]). Megalodon can also produce Proofgold (Curry-Howard style) proof terms[4] presented in a simple to parse prefix notation.[5] While the Proofgold checker can be used for type checking and proof checking the data, we claim that it is straightforward to implement an independent proof checker. We allow ourselves to freely use previous definitions

[2] These second-order axioms are technically stronger than the first-order versions, but this is of no concern here.

[3] http://grid01.ciirc.cvut.cz/~chad/megalodon-1.8.tgz.

[4] https://prfgld.github.io

[5] The full data is available at http://grid01.ciirc.cvut.cz/~chad/smtsempfs.tgz.

or previously proven results (if they have been previously proven in Megalodon and published in Proofgold documents). That is, we do not need the proof term to contain a justification back to the axioms of set theory, but only back to previously proven results.

We will only make use of the SMT2 sorts for booleans, integers and arrays. The intended interpretations of these types are given by the SMT-LIB Standard: Version 2.6 [**?**] (in text form) as follows.

- Booleans (Page 37 of [**?**]):

```
"For every expanded signature Sigma, the instance of Core with that
 signature is the theory consisting of all Sigma-models in which:
- the sort Bool denotes the set {true, false} of Boolean values;
- for all sorts s in Sigma,
  - (= s s Bool) denotes the function that returns true iff its two
    arguments are identical;
  - (distinct s s Bool) denotes the function thatreturns true iff its
    two arguments are not identical;
  - (ite Bool s s) denotes the function thatreturns its second
    argument or its third depending on whether its first argument is true
    or not;
- the other function symbols of Core denote the standard Boolean
  operators as expected."
```

  The obvious two element set to take as the interpretation of the type of booleans is the ordinal $2 = \{0, 1\}$ with 0 interpreting false and 1 interpreting true.

- Integers (Page 38 of [**?**]):

```
"For every expanded signature Sigma, the instance of Ints with that
signature is the theory consisting of all Sigma-models that interpret
- the sort Int as the set of all integers,
- the function symbols of Ints as expected."
```

  We fix a set theoretic representation of integers (described below) and use this fixed set to interpret the type of integers and the relevant operations.

- Arrays (Page 39 of [**?**]):

```
"For every expanded signature Sigma, the instance of ArraysEx with
 that signature is the theory consisting of all Sigma-models that
 satisfy all axioms of the form below, for all sorts s1, s2 in Sigma:

 (forall ((a (Array s1 s2)) (i s1) (e s2))
      (= (select (store a i e) i) e))

 (forall ((a (Array s1 s2)) (i s1) (j s1) (e s2))
      (=> (distinct i j) (= (select (store a i e) j) (select a j))))

 (forall ((a (Array s1 s2)) (b (Array s1 s2)))
      (=> (forall ((i s1)) (= (select a i) (select b i))) (= a b)))"
```

  It is not difficult to see that a set satisfying the last axiom will be isomorphic to a set of functions and in the isomorphic representation `select` can be assumed to be functional

application. We will apply this simplification below. The only remaining condition is that the set of functions is closed under the `store` function which (possibly) changes the value of the function on one input.

4.1 Induction

As a first simple example we consider induction on the natural numbers. Here the natural numbers are considered as a predicate over the sort Int.

In SMT2 format we can assert induction fails (which should be unsatisfiable) by giving a predicate p which holds for 0 and is closed under successor but does not hold for all integers $n \geq 0$. Here is the SMT2 specification:

```
(declare-fun p (Int) Bool)
(assert (p 0))
(assert (forall ((?n Int)) (=> (<= 0 ?n) (=> (p ?n) (p (+ ?n 1))))))
(assert (not (forall ((?n Int)) (=> (<= 0 ?n) (p ?n)))))
```

To translate this into a set theoretical statement, we must give a specific set representing integers. For natural numbers a reasonable option is to take the finite ordinals (the members of ω). As part of a formalization of Conway's surreal numbers [**?**] we also have a $-$ operation on all surreal numbers (including ordinals). The details are not important here, but it is sufficient to note that $-0 = 0$, $-n \notin \omega$ if $n \in \omega$ and $--x = x$ for all surreal numbers x. We take int to be the set $\omega \cup \{-n | n \in \omega\}$ and use int as the fixed interpretation of the sort Int. In the Megalodon preamble file we use this definition appears as follows:

```
Definition int : set := omega :\/: {- n|n :e omega}.
```

We also have a binary operation $+$ on surreal numbers which behaves as expected on int, as well as orderings $<$ and $\leq$ on surreal numbers. In general we will not give details about definitions unless they are relevant. We will only state some relevant properties we use, but emphasize that all properties we use have been previously proven in Megalodon and published into the Proofgold chain. There are no goals left open.

We have chosen to locally define `bp` as follows:

```
Let bp : set -> prop := fun b => 0 :e b.
```

We briefly consider the behavior of `bp` when applied to booleans (members of the set $\{0, 1\}$). The negation of `bp` 0 is $0 \notin 0$ which is provable, so `bp` 0 acts as the false proposition. On the other hand `bp` 1 is $0 \in 1$ which is provable, so `bp` 0 acts as the true proposition. Such local definitions act more as notation that is translated away. Other definitions would also work.

The statement of the set theoretic translation of the SMT2 problem appears as follows in Megalodon:

```
Theorem example1ind_unsat:
  forall p :e Bool :^: int,
       bp (p 0)
    -> (forall n :e int, 0 <= n -> bp (p n) -> bp (p (n + 1)))
    -> ~(forall n :e int, 0 <= n -> bp (p n))
    -> False.
```

Essentially that statement says the three (translated) assertions lead to a contradiction. Note that since p 0 is a boolean (a set which is a member of $\{0, 1\}$), the coercion `bp` is used to create the corresponding proposition whenever necessary.

The proof in Megalodon proceeds as follows: we assume p is in the set 2^{int} and assume the three properties hold. In the preamble there is a predicate nat_p that holds for the finite ordinals. A previously proven induction principle is included:

```
nat_ind : forall p:set->prop,
     p 0
  -> (forall n, nat_p n -> p n -> p (ordsucc n))
  -> forall n, nat_p n -> p n.
```

This induction principle will form the core of the current proof.

We first prove nonnegative integers satisfy nat_p.

```
claim L1: forall n :e int, 0 <= n -> nat_p n.
```

The proof of this claim relies on results about surreal numbers, the $-$ operation and the $<$ and $\leq$ relations.

We next prove $n + 1 = \mathsf{ordsucc}\ n$ for n satisfying nat_p.

```
claim L2: forall n, nat_p n -> n + 1 = ordsucc n.
```

The proof of this claim uses previously proven results relating the behavior of the surreal number operation $+$ on natural numbers.

We can now prove the most important subclaim:

```
claim L3: forall n, nat_p n -> bp (p n).
```

This claim is proven using nat_ind and L2 as well as a variety of results about the behavior of natural numbers as surreal numbers relative to the relations $<$ and $\leq$.

From the first and third claim it is easy to obtain a proof

$$\forall n \in \mathsf{int}.0 \leq n \to \mathsf{bp}\ (p\ n)$$

contradicting the last assumption of the problem and leading to a proof of False as desired.

4.2 Pigeonhole

Our second example will be two versions of the Pigeonhole Principle. We use arrays from integers to integers (with some constraints) to play the role of functions from finite ordinals to finite ordinals. In the first version we will state that every array acting as a function from $\{0, \ldots, n\}$ to $\{0, \ldots, n-1\}$ is not injective. In SMT2 format we assert the negation of this statement as follows:

```
(assert
 (not
  (forall
   ((?n Int))
   (=> (>= ?n 0)
       (forall
        ((?f (Array Int Int)))
        (=> (forall ((?i Int))
               (=> (and (<= 0 ?i) (<= ?i ?n))
                   (and (<= 0 (select ?f ?i)) (< (select ?f ?i) ?n))))
            (exists ((?i Int) (?j Int))
                (and (<= 0 ?i) (< ?i ?j) (<= ?j ?n)
                     (= (select ?f ?i) (select ?f ?j)))))))))))
```

In order to translate this SMT2 problem into a statement of formal set theory we must interpret arrays. We will translate to a statement that universally quantifies over appropriate interpretations of arrays. An interpretation of arrays is a (meta-)function *Array* taking two sets and returning a set satisfying the following property:

```
Definition Array_interp : (set -> set -> set) -> prop
  := fun Array =>
          (forall X Y, Array X Y c= Y :^: X)
       /\ (forall X Y, forall f :e Array X Y, forall x :e X, forall y :e Y,
                  (fun u :e X => if u = x then y else f u) :e Array X Y).
```

That is: for sets X and Y, $Array\ X\ Y$ must be a set of functions from X to Y that is closed under changing one value.[6]

Translating this to the formal set theory of Megalodon we have the following theorem:

```
Theorem PigeonHoleArrays_1_unsat :
  forall Array:set -> set -> set,
    Array_interp Array ->
    ~(forall n :e int, 0 <= n ->
      forall f :e Array int int,
         (forall i :e int, 0 <= i /\ i <= n ->
                           0 <= f i /\ f i < n)
      -> (exists i j :e int, 0 <= i /\ i < j /\ j <= n /\ f i = f j))
    -> False.
```

Again $-$ is the unary minus on surreal numbers and $<$ and $\leq$ are relations on surreal numbers. In this case there are a few facts about integers which had not been previously proven, so we proved them before proving the theorem above. Here we simply state these results:

```
Theorem NegIntNat : forall x :e int, x < 0 -> nat_p (- x).

Theorem PosIntNat: forall x :e int, 0 < x -> nat_p x.

Theorem NNegIntNat1: forall x :e int, ~(x < 0) -> nat_p x.

Theorem NNegIntNat2: forall x :e int, 0 <= x -> nat_p x.
```

Using these results, along with a few others, we can prove a contradiction by reducing to the following previously proven version of the Pigeonhole principle:

```
PigeonHole_nat :
 forall n, nat_p n ->
 forall f:set -> set,
       (forall i :e ordsucc n, f i :e n)
   -> ~(forall i j :e ordsucc n, f i = f j -> i = j).
```

A second version of the Pigeonhole principle states that every (array acting as an) injective function from $\{0, \ldots, n-1\}$ into $\{0, \ldots, n-1\}$ is surjective. As an SMT2 problem this can be stated as follows:

```
(assert
 (not
```

[6] Note that this allows the set of arrays to be empty. If all types in SMT3 will be assumed to be nonempty, then this definition should be changed.

```
(forall
 ((?n Int))
 (=> (>= ?n 0)
     (forall
      ((?f (Array Int Int)))
      (=> (forall ((?i Int))
            (=> (and (<= 0 ?i) (< ?i ?n))
                (and (<= 0 (select ?f ?i)) (< (select ?f ?i) ?n))))
          (=> (forall ((?i Int) (?j Int))
                (=> (and (<= 0 ?i) (< ?i ?n) (<= 0 ?j) (< ?j ?n)
                         (= (select ?f ?i) (select ?f ?j)))
                    (= ?i ?j)))
              (forall
               ((?j Int))
               (=> (and (<= 0 ?j) (< ?j ?n))
                   (exists ((?i Int))
                     (and (<= 0 ?i) (< ?i ?n) (= (select ?f ?i) ?j))))))))))))
```

The corresponding Megalodon theorem looks as follows:

```
Theorem PigeonHoleArrays_2_unsat :
  forall Array:set -> set -> set,
    Array_interp Array ->
    ~(forall n :e int, 0 <= n ->
      forall f :e Array int int,
         (forall i :e int, 0 <= i /\ i < n ->
                           0 <= f i /\ f i < n)
      -> (forall i j :e int,
                0 <= i /\ i < n /\ 0 <= j /\ j < n /\ f i = f j
                    -> i = j)
      -> (forall j :e int, 0 <= j /\ j < n
            -> exists i :e int, 0 <= i /\ i < n /\ f i = j))
    -> False.
```

The Megalodon proof proceeds by reducing to a similar previously proven version of the Pigeonhole Principle. However, it would also be possible to infer the second version from the first version simply by instantiating with an array with one element changed.[7]

4.3 Failure of Schroeder-Bernstein for Arrays

As a final example, we consider the Schroeder-Bernstein property for arrays. That is, we consider whether or not two types α and β must have a bijection between them if there are injections from α into β and β into α. In this case the negation of the property is satisfiable and we give an interpretation of arrays for which the property fails. Usually in logic there is either a proof on the one hand or a model on the other. However, in this case we can also give a proof term for a proof of the negation of the set theoretical property (where the negation is before the quantifier over possible interpretations of arrays).

For the SMT2 problem we let f and g be of appropriate array types and assume f and g are injective. We then assume there does not exist a bijective array.

```
(declare-fun f () (Array Int Int))
(declare-fun g () (Array Int Int))
```

[7] We leave the details to the interested reader.

```
(assert (forall ((?m Int) (?n Int)) (=> (= (select f ?m) (select f ?n)) (= ?m ?n))))
(assert (forall ((?m Int) (?n Int)) (=> (= (select g ?m) (select g ?n)) (= ?m ?n))))
(assert
  (not (exists ((?h (Array Int Int)))
         (and (forall ((?m Int) (?n Int)) (=> (= (select ?h ?m) (select ?h ?n)) (= ?m ?n)))
              (forall ((?n Int)) (exists ((?m Int)) (= (select ?h ?m) ?n)))))))
```

The translation of this problem to a set theoretic proposition in Megalodon appears as follows:

```
  forall Array:set -> set -> set,
     Array_interp Array ->
     (forall f g :e Array int int,
         (forall m n :e int, f m = f n -> m = n)
      -> (forall m n :e int, g m = g n -> m = n)
      -> ~(exists h :e Array int int,
               (forall m n :e int, h m = h n -> m = n)
            /\ (forall n :e int, exists m :e int, h m = n))
      -> False)).
```

This is not provable. However, we can prove the negation of the proposition (if we are careful to put the negation before the quantifier for the interpretation of arrays).

```
Theorem SchroederBernsteinArrays_sat :
  ~(forall Array:set -> set -> set,
     Array_interp Array ->
     (forall f g :e Array int int,
         (forall m n :e int, f m = f n -> m = n)
      -> (forall m n :e int, g m = g n -> m = n)
      -> ~(exists h :e Array int int,
               (forall m n :e int, h m = h n -> m = n)
            /\ (forall n :e int, exists m :e int, h m = n))
      -> False)).
```

The most important choice for proving this negated proposition is properly instantiating for *Array*. We start by defining an injective function from integers to natural numbers which sends negative integers x to $(2(-x)) + 1$ and nonnegative integers x to $2x$.

```
set int_into_nat : set := (fun x :e int => if x < 0 then ordsucc (2 * (- x)) else 2 * x).
```

We can now inductively define the collection of all functions that are the same as `int_into_nat` except on finitely many elements.

```
set ArrayIntInt_p : set -> prop := fun f =>
  forall p:set -> prop,
        p int_into_nat
     -> (forall f, forall x y :e int, p f -> p (fun u :e int => if u = x then y else f u))
     -> p f.
```

Finally we can define *Array* (the term we will use as the instantiation for the quantified variable *Array*) to be the set of all functions unless both arguments are the set of integers, in which case the functions must satisfy `ArrayIntInt_p`.

```
set Array : set -> set -> set :=
```

```
fun A B =>
   if A = int /\ B = int then
     {f :e int :^: int | ArrayIntInt_p f}
   else B :^: A.
```

Intuitively it should be clear that this choice satisfies `Array_interp`. It is also the case that *Array* int int contains no bijection. Formally we prove that every function satisfying `ArrayIntInt_p` has a lower bound and then use this to conclude that such a function cannot be a surjection.

The Megalodon file containing all the definitions and proofs mentioned above is less than 1000 lines. The full Proofgold document (containing the proof terms for each proof) is 108KB.

4.4 Integer Difference Logic

Our final examples will be two small integer difference logic problems from the "job shop" collection from QF_IDL portion of the SMT library. One is satisfiable and the other is unsatisfiable. In both cases we can obtain proof terms for the corresponding set theoretic proposition.

As described in [**?**] satisfiability of a set of atoms of the form $x_1 + -x_0 \leq v_0$, $x_2 + -x_1 \leq v_1$, $\ldots$, $x_0 + -x_{n-1} \leq v_{n-1}$ (where the variables range over integers) can be decided by forming a certain directed graph with edges labeled by integers and checking if there is a negative loop. If there is no negative loop, then values for the variables can be computed from the graph.

We first consider the problem `jobshop2-2-1-1-4-4-11`. In the problem there are five integer variables s_1^1, s_2^1, s_1^2, s_2^2 and ref. The assertion given in the problem

$$(v_1 \vee v_0) \wedge (v_0 \vee v_1) \wedge (v_3 \vee v_2) \wedge (v_2 \vee v_3) \wedge s_2^1 - s_1^1 \geq 4 \wedge s_2^2 - s_1^2 \geq 4$$
$$\wedge s_2^1 - ref \leq 7 \wedge s_2^2 - ref \leq 7 \wedge s_1^1 - ref \geq 0 \wedge s_1^2 - ref \geq 0$$

where v_1, v_0, v_3 and v_4 are locally defined (via a `let`) to be the atoms $s_1^1 - s_1^2 \geq 4$, $s_1^2 - s_1^1 \geq 4$, $s_2^1 - s_2^2 \geq 4$ and $s_2^2 - s_2^1 \geq 4$, respectively. This problem is unsatisfiable. An informal proof of unsatisfiability proceeds by splitting into two cases via the disjunction $v_3 \vee v_2$. In the v_3 case there is a negative loop given by s_2^1, s_2^2, s_1^2, ref. In the v_2 case there is a negative loop given by s_2^2, s_2^1, s_1^1, ref.

The set theoretic version of the problem can be defined as the following proposition in Megalodon.

```
Definition jobshop2_2_1_1_4_4_11 : prop :=
    forall s1_1 s1_2 s2_1 s2_2 ref :e int,
    forall v_1:prop, v_1 = (4 <= s1_1 + - s2_1)
 -> forall v_0:prop, v_0 = (4 <= s2_1 + - s1_1)
 -> forall v_3:prop, v_3 = (4 <= s1_2 + - s2_2)
 -> forall v_2:prop, v_2 = (4 <= s2_2 + - s1_2)
 -> ((v_1 \/ v_0) /\ (v_0 \/ v_1) /\ (v_3 \/ v_2) /\ (v_2 \/ v_3)
  /\ 4 <= s1_2 + - s1_1 /\ 4 <= s2_2 + - s2_1
  /\ s1_2 + - ref <= 7 /\ s2_2 + - ref <= 7
  /\ 0 <= s1_1 + - ref /\ 0 <= s2_1 + - ref)
 -> False.
```

Note that we have slightly modified the inequalities to all use $\leq$ for simplicity. Also, we combine the unary $-$ with the binary $+$ operator instead of using a binary $-$ operator. Finally, we have replaced the `let` declarations for the v_i's with universally quantified variables and an assumed identity. The proposition above corresponds to the unsatisfiability of the original SMT problem

and it can be proven in set theory using the negative loops mentioned above and the following (formally proven) result.

```
Theorem idl_negcycle_4 : forall x y z w v1 v2 v3 v4,
    SNo x -> SNo y -> SNo z -> SNo w
 -> SNo v1 -> SNo v2 -> SNo v3 -> SNo v4
 -> v1 + v2 + v3 + v4 < 0
 -> y + - x <= v1 -> z + - y <= v2
 -> w + - z <= v3 -> x + - w <= v4
 -> False.
```

The theorem `idl_negcycle_4` is specific to negative loops of length 4, but is also more general since variables range over values satisfying the predicate `SNo`, a predicate true for integers, real numbers, and more (Conway's extension of the real numbers described in [**?**]). While it is relatively easy to prove `idl_negcycle_4` directly, it is somewhat unsatisfying to have the result be specific to cycles of length 4. Fortunately the theorem can be easily proven as a consequence of the following (formally proven) general result about cycles of length n, by induction on n.

```
Theorem SNo_idl_cycle_nonneg : forall n, nat_p n ->
  forall f g:set -> set,
             (forall i :e ordsucc n, SNo (f i))
          -> (forall i :e ordsucc n, SNo (g i))
          -> f (ordsucc n) = f 0
          -> (forall i :e ordsucc n, f (ordsucc i) + - f i <= g i)
          -> 0 <= finite_add_SNo (ordsucc n) g.
```

Note that f corresponds to an $n+1$-tuple (with $fn = f0$) and g corresponds to an n-tuple. The function `finite_add_SNo` takes a natural number n and a function g and returns the sum $\Sigma_{i \in n} gi$.

The final example we consider is `jobshop2-2-1-1-4-4-12` which is a simple modification of the previous example by changing each 7 to 8.

$$(v_1 \vee v_0) \wedge (v_0 \vee v_1) \wedge (v_3 \vee v_2) \wedge (v_2 \vee v_3) \wedge s_2^1 - s_1^1 \geq 4 \wedge s_2^2 - s_1^2 \geq 4$$
$$\wedge s_2^1 - ref \leq 8 \wedge s_2^2 - ref \leq 8 \wedge s_1^1 - ref \geq 0 \wedge s_1^2 - ref \geq 0$$

This makes the problem satisfiable by taking $s_8^1 = -8$, $s_2^1 = -4$, $s_1^2 = -4$, $s_2^2 = 0$ and $ref = -8$.

The corresponding set theoretic proposition is given as follows:

```
Definition jobshop2_2_1_1_4_4_12 : prop :=
    forall s1_1 s1_2 s2_1 s2_2 ref :e int,
    forall v_1:prop, v_1 = (4 <= s1_1 + - s2_1)
 -> forall v_0:prop, v_0 = (4 <= s2_1 + - s1_1)
 -> forall v_3:prop, v_3 = (4 <= s1_2 + - s2_2)
 -> forall v_2:prop, v_2 = (4 <= s2_2 + - s1_2)
 -> ((v_1 \/ v_0) /\ (v_0 \/ v_1) /\ (v_3 \/ v_2) /\ (v_2 \/ v_3)
  /\ 4 <= s1_2 + - s1_1 /\ 4 <= s2_2 + - s2_1
  /\ s1_2 + - ref <= 8 /\ s2_2 + - ref <= 8
  /\ 0 <= s1_1 + - ref /\ 0 <= s2_1 + - ref)
 -> False.
```

Since the problem is satisfiable, the proposition cannot be proven. However, we can prove its negation by assuming the proposition holds and applying it to the values above. One must then proven v_0 and v_2 hold (giving all the disjunctions) and prove the remaining inequalities hold.

5 Remarks about Completeness

A common belief is that it is impossible to have a recursively enumerable proof system for higher-order logic. This is in conflict to the fact that many proof systems are complete relative to Henkin-Andrews semantics. The reason for the belief is the essential incompleteness relative to standard set theoretic semantics, as mentioned earlier.

After adding set theoretic axioms to higher-order logic, one obtains categoricity results relative to "standard models." (This has even been formalized in Coq, using what could be called "standard type theoretic models" [**?**].) A consequence is that the continuum hypothesis is true in every standard model or false in every standard model. The natural question (troubling Cantor) is: "which is it?"

This natural question makes no sense from the Formalist point of view. A Formalist only cares if the continuum hypothesis is provable. The continuum hypothesis is independent (even in higher-order set theory) and so it is not provable and its negation is not provable.

The question may concern a Platonist. The unsatisfying answer from the Platonist point of view is that the continuum hypothesis is true in every standard model if and only if the continuum hypothesis is true in the platonic universe of sets. One could say that information about the platonic universe of sets "leaks through" when standard models are used.

Once we pass to Henkin-Andrews models of higher-order set theory, these concerns go away. Even if the continuum hypothesis is true in every standard model, it is false in some Henkin-Andrews models. Likewise, even if the continuum hypothesis is false in every standard model, it is true in some Henkin-Andrews models. Two Platonists who disagree whether or not the continuum hypothesis is "actually" true or false, will still agree that it is true in some Henkin-Andrews models and false in others.

This is the sense in which the proof system for higher-order set theory could be considered "complete." If the higher-order set theory were considered the semantics of SMT3 (via the Werner-Aczel proof irrelevant set theoretic semantics), then one would not expect an SMT3 proof procedure to be complete. (Or, put more positively, a complete proof procedure for SMT3 would be an interesting result.)

6 Possible Research on Intermediate Proof Systems

One objection to taking either CIC or higher-order set theory as a standard for independently checkable proof terms for SMT3 is that it could preempt publishable research on other possible notions of proof objects. However, it is common in the case of programming language research to create various intermediate languages and factor compilation as translations through these intermediate languages. Analogous research could be done on intermediate proof languages. Such languages may not be able to represent unsatisfiability proofs for every possible unsatisfiable SMT3 problem, but could handle special cases (e.g., proofs by induction). It is easy to imagine intermediate languages handling special cases efficiently while the translation from the intermediate language to the full proof terms for CIC or higher-order set theory would be impractical.

7 Conclusion

A finitely axiomatized set theory using Church's type theory instead of first-order logic provides a simple way of obtaining a candidate semantics for SMT3. Via Curry-Howard, we also naturally

obtain a candidate notion of independently checkable proof term.

Acknowledgements

The results were supported by the Ministry of Education, Youth and Sports within the dedicated program ERC CZ under the project POSTMAN no. LL1902. This scientific article is part of the RICAIP project that has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 857306.

References

[1] SMT-LIB version 3.0 - preliminary proposal, 2021. http://smtlib.cs.uiowa.edu/version3.shtml.

[2] Peter Aczel. On relating type theories and set theories. In Thorsten Altenkirch, Wolfgang Naraschewski, and Bernhard Reus, editors, *TYPES*, volume 1657 of *Lecture Notes in Computer Science*, pages 1–18. Springer, 1998.

[3] Sten Agerholm and Michael J. C. Gordon. Experiments with ZF set theory in HOL and Isabelle. In E. Thomas Schubert, Phillip J. Windley, and Jim Alves-Foss, editors, *Higher Order Logic Theorem Proving and Its Applications*, volume 971 of *LNCS*, pages 32–45. Springer, 1995.

[4] P. B. Andrews. *An Introduction to Mathematical Logic and Type Theory: To Truth Through Proof*. Kluwer Academic Publishers, 2nd edition, 2002.

[5] Peter B. Andrews. General models and extensionality. *J. Symb. Log.*, 37:395–397, 1972.

[6] Bruno Barras. Sets in Coq, Coq in Sets. *Journal of Formalized Reasoning*, 3(1), 2010.

[7] Clark Barrett, Pascal Fontaine, and Cesare Tinelli. The SMT-LIB Standard: Version 2.6. Technical report, Department of Computer Science, The University of Iowa, 2017. Available at www.SMT-LIB.org.

[8] Clark Barrett, Pascal Fontaine, and Cesare Tinelli. New working group on SMT proofs, 2021. https://groups.google.com/g/smt-lib/c/a0-U-nU4J68.

[9] Yves Bertot and Pierre Castéran. *Interactive Theorem Proving and Program Development. Coq'Art: The Calculus of Inductive Constructions*. Texts in Theoretical Computer Science. An EATCS Series. Springer, 2004.

[10] Chad E. Brown. Notes on semantics of and proofs for smt, Sep 2021.

[11] Chad E. Brown and Karol Pak. A tale of two set theories. In Cezary Kaliszyk, Edwin C. Brady, Andrea Kohlhase, and Claudio Sacerdoti Coen, editors, *Intelligent Computer Mathematics - 12th International Conference, CICM 2019, Prague, Czech Republic, July 8-12, 2019, Proceedings*, volume 11617 of *Lecture Notes in Computer Science*, pages 44–60. Springer, 2019.

[12] Alonzo Church. A formulation of the simple theory of types. *The Journal of Symbolic Logic*, 5:56–68, 1940.

[13] John H. Conway. *On numbers and games, Second Edition*. A K Peters, 2001.

[14] N. de Bruijn. The Mathematical language AUTOMATH, its usage, and some of its extensions. In *Symposium on Automatic Demonstration*, pages 29–61. Lecture Notes in Mathematics, 125, Springer, 1970.

[15] 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 579–606. Academic Press, 1980.

[16] Michael Gordon. Set theory, higher order logic or both? In Joakim von Wright, Jim Grundy, and John Harrison, editors, *Theorem Proving in Higher Order Logics, TPHOLs'96*, volume 1125 of *LNCS*, pages 191–201. Springer, 1996.

[17] Leon Henkin. Completeness in the theory of types. *The Journal of Symbolic Logic*, 15:81–91, 1950.

[18] W.A. Howard. The formulas-as-types notion of construction. In J.P. Seldin and J.R. Hindley, editors, *To H.B. Curry: Essays on Combinatory Logic, Lambda Calculus and Formalism*, pages 479–490, New York, 1980. Academic Press.

[19] B. Jacobs. *Categorical Logic and Type Theory*. ISSN. Elsevier Science, 1999.

[20] Hyondeuk Kim and Fabio Somenzi. Finite instantiations for integer difference logic. In *2006 Formal Methods in Computer Aided Design*, pages 31–38. IEEE, nov 2006.

[21] Dominik Kirst and Gert Smolka. Categoricity results and large model constructions for second-order ZF in dependent type theory. *Journal of Automated Reasoning*, 2018. First Online: 11 October 2018.

[22] Joachim Lambek and Philip Scott. *Introduction to higher order categorical logic*. Cambridge University Press, Cambridge, UK, 1986.

[23] Gyesik Lee and Benjamin Werner. Proof-irrelevant model of CC with predicative induction and judgmental equality. *Logical Methods in Computer Science*, 7(4), 2011.

[24] Zhaohui Luo. *Computation and reasoning: a type theory for computer science*. Oxford University Press, Inc., New York, NY, USA, 1994.

[25] The Coq development team. *The Coq proof assistant reference manual*. LogiCal Project, 2020. Version 8.12.

[26] Steven Obua. Partizan games in Isabelle/HOLZF. In Kamel Barkaoui, Ana Cavalcanti, and Antonio Cerone, editors, *Theoretical Aspects of Computing - ICTAC 2006*, volume 4281 of *LNCS*, pages 272–286. Springer, 2006.

[27] A. Tarski. Der Aussagenkalkül und die Topologie. *Fundamentae Mathematicae*, 31:103–134, 1938.

[28] Benjamin Werner. Sets in types, types in sets. In Martín Abadi and Takayasu Ito, editors, *TACS*, volume 1281 of *Lecture Notes in Computer Science*, pages 530–346. Springer, 1997.

[29] Ernst Zermelo. Untersuchungen über die Grundlagen der Mengenlehre I. *Mathematische Annalen*, 65:261–281, 1908. English translation, "Investigations in the foundations of set theory" in [**?**], pages 199–215.

A appendix - to do