Constructive Set Theory in Nuprl Type Theory

June 14, 2018

1 Aczel's two set theories

Aczel proposed CZF as a foundation for constructive mathematics and gave an interpretation of it in Martin-Löf type theory. He then extended the theory with the Regular Extension Axiom and gave an interpretation of that using Martin-Löf type theory with W-types. Later, he studied non-wellfounded set theory with an *anti-foundation axiom*. Ingrid Lindstrom gave an interpretation of that theory in Martin-Löf type theory.

The motivation for CZF as a foundation for constructive mathematics may still be relevant for some, but we prefer to work directly in type theory—in particular, Nuprl. However, the interpretations of CZF and its non-wellfounded version are interesting and illustrate the use of some interesting types in Nuprl.

2 W-types and co-W-types

When A is a type and forall $a \in A$, $B(a)$ is a type, then the W-type, $W(A, a.B(a))$ is the least fixed point of

$$W \equiv a\!:\!A \times (B(a) \to W)$$

and the co-W-type is the greatest fixed point of the same equation. A member, $\text{wsup}(a, f)$, of either type, is a pair $\langle a, f \rangle$ where $a \in A$ and f is a function with domain $B(a)$ that "enumerates" the "elements" of $\text{wsup}(a, f)$.

Since the W-type is the least fixed point it has an induction prinicple, and since the co-W-type is the greatest fixed point, it has a *co-induction* principle.

Some type theories take one or both of these types as primitive, but in Nuprl they are not primitive but are constructed from the other primitive types.

The co-W-type is constructed as the intersection $\bigcap_{n:\mathbb{N}} F^n(Top)$ where $F(W) = a : A \times (B(a) \to W)$. Its co-induction principle come from this definition and the induction principle for $\mathbb{N}$.

The W-type is constructed by defining the *subtype* of the co-W-type consisting of the well-founded trees. The induction principle for the W-type comes from this definition and the principle of Bar-Induction which is a rule in Nuprl.

3 Aczel's interpretation of CZF

Aczel interpreted Set $= W(\mathbb{U}, T.T)$ where $\mathbb{U}$ is a *universe* of types. Set equality $s_1 \doteq s_2$ is then defined inductively, and set member $s_1 \in s_2$ is defined in terms of that. This all works well in Nuprl and we can define Aczel's *regular extension* of a set because the universe $\mathbb{U}$ contains the W-types.

The usual development of CZF makes use of first-order formulas and the *classes* that they define. In Nuprl, we can dispense with formulas and instead use *propositions* about sets. A proposition is just a type, so a proposition about sets is a function $P \in \text{Set} \to \mathbb{U}'$. If $\mathbb{U}'$ is a higher universe than $\mathbb{U}$ then the proposition corresponds to a *proper class*, and if $\mathbb{U}' = \mathbb{U}$ then it corresponds to a *restricted class* (the separation axiom in CZF holds only for restricted clasess).

4 Interpreting non-wellfounded sets

Lindstrom's interpretation in type theory of Aczel's non-wellfounded sets was somewhat complicated. We can simply take the interpretation to be coSet $= coW(\mathbb{U}, T.T)$ using the co-W-type. But, for this to work, we need to define the set equality $s_1 \doteq s_2$ on this co-W-type. We can no longer use Aczel's inductive definition, but we would like the definition to coincide with Aczel's definition on the well-founded sets.

To make such a definition, we need the right concept of *bisimulation* on co-W-types. The bisimulation equivalence of two members x and y of the co-W-type is the same as a *winning strategy* for the second player in a game $G(x, y)$.

Because there is nothing about the game $G(x, y)$ that is decidable, the right definition for "winning strategy for second player" is surprisingly tricky. This is because it is "very dependent". A strategy is a function s that takes a sequence of moves – that follow strategy s–and gives the next move. We have figured out how to get the right definition of this "very dependent" concept using two mutually recursive families of types that use Nuprl's *dependent intersection type*, $a\!:\!A \cap B(a)$.

With this interpretation, the well-founded sets are simply a subtype of the non-wellfounded sets. Things like the union, pair, ordered pair, etc. are defined for the co-Sets and the Sets are "closed" under these operations. This "unification" of the interpretations of the two theories may be a new result, but even if not, it is an nice application of some of the most interesting features of Nuprl's type theory.

Much of this interpretation is relatively straightforward and can be discussed quickly. The novel part is our new definition for winning strategies, so the theory includes some results in what we can call *constructive game theory*.