Constructing order completions in type theory

Dagstuhl seminar on Verification and Constructive Algebra

January 5 – 10, 2003

Erik Palmgren

Uppsala universitet

Overview

1. Constructive mathematics and type theory
2. Order completions using Dedekind cuts
3. Completing ordered groups. Real closed fields

1. Constructive mathematics and type theory

A *set* S is a pair $(\underline{S}, =_S)$ where

$\underline{S}$ is a *type* (Bishop: *preset*)

$=_S$ is an *equivalence relation*.

Ex. Types: $Bool$, $Nat = \mathbb{N}$, $\mathbb{N} \times \mathbb{N}$, $\mathbb{N} \to \mathbb{N}$, ...

Ref. E. Bishop and D.S. Bridges. Constructive analysis. Springer 1985.

Mines, Richman, Ruitenburg. A course in constructive algebra. Springer 1988.

Equivalence relations are sometimes decidable

$$=_S : S \times S \to \texttt{Bool} = \{False, True\}$$

Ex. equality on finite data structures, $\cdot \equiv \cdot \pmod{p}$ etc.

... but may be more general

$$=_S : S \times S \to \texttt{Prop}$$

Ex. equality of real numbers: $x =_{\mathbb{R}} \pi$

These constructive sets organise into a category, **CSets**:

Let S and T be sets. An *operation* or *program* $f : \underline{S} \to \underline{T}$ is a *function*, if for all $x, y \in \underline{S}$

$$x =_S y \Longrightarrow f(x) =_T f(y).$$

Remark. The category **CSets** is *almost a topos*, when starting out from the types of Martin-Löf type theory. (Moerdijk and P. APAL 2002). Moreover, countable and dependent choice principles are valid in **CSets**.

Martin-Löf type theory (MLTT) provides a finest equivalence relation $\equiv_S$ to each type S. Then $\overline{S} = (S, \equiv_S)$ is such that for any set T, an operation $f : \underline{S} \to \underline{T}$ is in fact a function $f : \overline{S} \to T$.

This can be used to prove the axiom of choice on sets of the form $\underline{S}$, i.e. *projective sets*.

To every set there is an onto map from a projective set.

Brouwer-Heyting-Kolmogorov interpretation of logic

A mathematical proposition P is *true*, if there is a *proof-object* s witnessing its truth; if so write

$$a :: P$$

We may call s a **complete certificate** for the truth of P.

Ex. $f :: P \Rightarrow Q$ iff f is an operation which to each proof-object $a :: P$ gives a proof-object $f(a) :: Q$.

$s :: (\exists x \in S)P(x)$ iff s is a pair (d, p) where $d \in S$ and $p :: P(d)$.

Proofs-as-Programs: take the proof-objects to be programs of a functional programming language (rather than mental constructions, as Brouwer did).

The next logical step is to let the *proposition be types* (Curry-Howard)

$$A \Longrightarrow (B \Longrightarrow A)$$

$$x \mapsto (y \mapsto x) :: A \longrightarrow (B \longrightarrow A)$$

$$\texttt{False} = \emptyset \text{ and } \texttt{True} = \{\texttt{ok!}\}.$$

The types of common programming languages are too poor to go beyond propositional formulas.

MLTT realised the propositions-as-types principle through the introduction of

Σ-types (dependent record types)	Existential quantifiers
Π-types (dependent function types)	Universal quantifiers
Universes of types	Collections of propositions “Prop”

Ex. The existential statement

there exists an even prime

i.e. $(\exists n \in \mathbb{N}) Even(n) \,\&\, Prime(n)$ can be formalised as the sigma-type with three record fields

$$\textbf{sig}\,\{n :: \mathbb{N}, p :: \mathrm{Even}(n), q :: \mathrm{Prime}(n)\}$$

2. Order completions

The construction of real numbers as Dedekind cuts

$$\text{———} \; L \; \text{———})(\text{———} \; U \; \text{———}$$

played an important role in connection with Russell's original ramified type theory and foundational discussions.

In Russell's theory there would be hierarchies of different real numbers, which is unsatisfactory.

Ramsey's reducibility axiom collapses the hierarchy, but introduces a possible vicious circle. In type-theoretic terms it is a non-wellfounded type, which is inconsistent with recursion on types.

Better and constructive solution: this hierarchy collapses to the first level, provided the cuts are *located*:

$$x < y \Longrightarrow x \in L \text{ or } y \in U\,.$$

The reason is that each cut can be represented by a fundamental sequence, constructed by means of dependent choices.

We shall here consider the problem of completing more general orders than the rationals, in MLTT.

$<$ is a *pseudo-order relation* (Aczel) if :

(P1) $\neg(x < y \,\&\, y < x)$,

(P2) $\neg(x < y) \,\&\, \neg(y < x)$ implies $x = y$,

(P3) $x < y$ implies $x < z$ or $z < y$.

If $<$ is decidable (discrete), then this is just a total order.

The order $<_{\mathbb{R}}$ of constructive real satisfies these axioms, but *not* the trichotomy law

$$x < y \text{ or } x = y \text{ or } x > y.$$

Further examples: 1. $(\mathbb{Q} \times \mathbb{R}, <^*)$ where $<^*$ is the lexicographic order (rationals first)

2. $\mathbb{Q}(t)$ where t is made infinite.

$(S,<)$ is (constructively) *sup-complete* if every lower located $X \subseteq S$ has a supremum.

A non-void $X \subseteq S$ is *lower located,* if for all $a < b$ either a is less than some element of X or b is an upper bound of X

For a dense, unbounded pseudo-order $(S,<)$, let $\overline{S}$ denote the collection of bounded located cuts (L,U).

Order this collection as follows

$$(L,U) < (L',U') \iff L' \cap U \text{ non-void.}$$

This order is illustrated by:

$$\text{———— } L' \text{ ————————)(———— } U' \text{ ————}$$
$$\text{———— } L \text{ —————)(—————— } U \text{ ——————}$$

Theorem $\overline{S}$ is the sup-complete and inf-complete extension of S (and this is unique up to isomorphism).

One problem remains, we do not know that the $\overline{S}$ collection forms a set! The naive idea of finding a representing seems to be blocked by the fact $<$ does not satisfy the trichotomy law.

W-types: these are *initial term algebras* $W(I,B)$ where the operations may be infinitary. To each operation $i \in I$ a set B_i of argument indices is associated. If $B_i = \emptyset$ the operation is of course a constant.

From arguments $f : B_i \to W = W(I,B)$, we form a new term $\mathrm{sup}_i(f)$.

For suitable choices of I and B, $W(I,B)$ can be isomorphic to $\mathbb{N}$ or the countable branching, well-founded trees. There are recursion and induction principles associated with these.

Well-founded Choice Thm: Suppose that X is a set, P is a predicate on X and that $R_{i,u}$ is a binary relation on X when $i : I, u : B(i)$. If, for all $i : I$ and $g : B_i \to X$

$$(\forall u : B_i)\, P(gu) \Rightarrow (\exists y : X) P(y) \wedge (\forall u : B_i)\, R_{i,u}(gu, y)$$

then there is a choice function $f : W \to X$ such that $P(f(v))$ for each $v : W$, and moreover

$$(\forall i : I)(\forall h : B_i \to W)(\forall u : B_i)\, R_{i,u}(f(hu), f(\mathrm{sup}_i h))$$

Theorem The collection $\overline{S}$ is isomorphic to a set.

By employing well-founded choice with respect to the W-type

$$W = W(S \times S, B)$$

where $B_{(x,y)} = x < y$, one can show that a universe $\mathcal{U}$ containing W, S and some other basic sets is sufficient to represent the cuts as members of the restricted power set

$$\mathcal{P}_{\mathcal{U}}(S) = S \to \mathcal{U}.$$

Remark In an extension of constructive set theory countable dependent choice is enough (Aczel).

3. Ordered groups and fields

$K = (K, +, \cdot, 0, 1, P)$ is an *ordered (Heyting) field* if K is a commutative ring with 1, and has a positivity P satisfying

$$1 \in P,\ 0 \notin P$$

$$x, y \in P \Longrightarrow x + y, xy \in P$$

$$-x \notin P,\ x \notin P \Longrightarrow x = 0 \ (*)$$

$$-x \in P \text{ or } x \in P \Longrightarrow x \text{ invertible}$$

$$x + y \in P \Longrightarrow x \in P \text{ or } y \in P.$$

The constructive real numbers $\mathbb{R}$ is a typical example of a ordered Heyting field. It is also real closed in the sense that for polynomials $p(x)$ and $u < v$

$$p(u) < 0 < p(v) \Longrightarrow (\exists x \in (u,v))p(x) = 0.$$

An ordered field satisfying this axiom we call *real closed field* (RCF). If the tightness condition (*) is replaced by trichotomy, we have a *discrete* ordered field.

A cheap quantifier elimination result

By Barr's theorem it follows that, for so-called geometric theories T, we have that if T derives a geometric implication φ classically, then it derives φ intuitionistically.

We observe that discrete RCF (DRCF) is a geometric theory and that the basic elimination lemma can also be stated as a geometric implication.

Corollary: Intuitionistic DRCF enjoys quantifier elimination, and indeed *proves* PEM.

Cf. Delzell (1996) states that Tarski's original theorem is intuitionistic.

The discrete RCF (DRCF) has been well studied from a constructive point of view.

Holkott (1941), Roy and Lombardi (1997) constructs real closures of discrete ordered field.

Question: can this be extended to Heyting ordered fields?

Caution: If $\mathbb{R}^*$ is an extension of $\mathbb{R}$ containing some infinitesimal $\varepsilon > 0$, then for any $x \in \mathbb{R}$, we have $0 < x$, or $x < \varepsilon$ and so $x \leq 0$. This is *constructively impossible.*

Cauchy completion of ordered groups

An abelian group $(G,+,0)$ is *pseudo-ordered* if $<$ is a pseudo-order of G such that

$$x < y \Longrightarrow x+z < y+z.$$

Ex. Let G_2 be the product group $\mathbb{Q} \times \mathbb{Q}$ lexicographically ordered by $<^*$.

Suppose that $<$ is dense and G nontrivial. A *Cauchy cut* (L,U) in G (Dales-Woodin 1996) satisfies instead of locatedness, a stronger condition:

$(\forall \varepsilon > 0)(\exists x \in L)(\exists y \in U)\ y < x + \varepsilon.$

In case G is archimedean Cauchy-cuts and Dedekind cuts coincide.

In G_2 the following is a Dedekind cut, but not a Cauchy cut:

$$L = \{(p,x) \in G_2 : p \leq 0\} \qquad U = \{(p,x) \in G_2 : p > 0\}.$$

Theorem Let G be a non-trivial, dense, pseudo-ordered group. The set of Cauchy cuts form a Cauchy complete pseudo-ordered group.

(The fact that the cuts form a set can be proved by a straightforward type theoretic choice.)