Constructive completions of ordered sets, groups and fields

Erik Palmgren*

March 11, 2003

Abstract

In constructive mathematics it is of interest to consider a more general, but classically equivalent, notion of linear order, so called pseudo-order. The prime example is the order of the constructive real numbers. We examine two kinds of constructive completions of pseudo-orders: order completions of pseudo-orders and Cauchy completions of (nonarchimedean) ordered groups and fields. It is shown how these can be predicatively defined in type theory, also when the underlying set is non-discrete. Provable choice principles, in particular a generalisation of dependent choice, are used for showing set-representability of cuts.

Key words: ordered sets, ordered groups, ordered fields, completions, constructivism, predicativity.

Mathematics Subject Classification 2000: 03F60, 06A05, 06B23, 06F20, 12J15, 12J25.

1 Introduction

In this paper we investigate the problem of obtaining constructive order completions of arbitrary ordered sets, and Cauchy completions of non-archimedean groups and fields. The classical theory can be found in Dales and Woodin [4] and Scott [16]. The use of pseudo-orders is inspired by Aczel's presentation of the Dedekind construction; see [2].

Consider first the archimedean case. A well-known construction of real numbers is in terms of symmetric Dedekind cuts of rational numbers

$$—— L ——)(—— U ——$$

Taking the rational numbers as given, this construction can be made in a topos [9], in Church's simple theory of types, in intuitionistic higher order

*The author is supported by a grant from the Swedish Research Council (VR).

logic, or in similar systems which allow power sets and full separation. In Russell's original ramified theory of types, the power sets are stratified. This leads to a hierarchy of different real number systems. H. Weyl demonstrated in [18] that the first level of such a hierarchy could account for parts of analysis. We refer to Simpson [17] (in particular p. 18 and p. 404) for a thorough study of classical systems related to Weyl's. In constructive, predicative systems, such as Martin-Löf type theory, this hierarchy collapses to the first level, provided the cuts are located in an affirmative way:

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

The reason is that each cut can be represented by a fundamental sequence, constructed by means of dependent choices. One kind of construction relies on the fact that the rational numbers satisfy the trichotomy law

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

A second construction starts out from an ordered group, which for each $\varepsilon > 0$ gives elements on each side of the cut, with distance closer than ε (see Section 5). A novel construction of this second kind, due to Peter Aczel ([2]), avoids choice but uses a kind of collection principle to obtain set-representability.

Here we shall first consider orders without algebraic structure. The Dedekind completion method may classically be applied also to general dense unbounded linear orders. Constructively, there is the difficulty that many orders of interest satisfy merely the so-called *co-transitivity* property

$$x < y \Longrightarrow x < z \text{ or } z < y. \tag{1}$$

Which disjunct is true thus depends on the proof-object for $x < y$. In this paper we first show that this property is indeed sufficient (Section 3) and then address the question of the predicative representability of cuts in co-transitive orders (Section 4 and 8). We show that the answer is affirmative in Martin-Löf type theory with W-types and certain (small) universes. The new dependent choice principle is presented in Section 7. In sections 5 and 6 we complete ordered groups and fields, using so-called Cauchy cuts.

It remains an interesting open question whether it is possible to prove, constructively, that every pseudo-ordered field has real closed extension. A positive answer would generalise an extension theorem of Holkott (1941) and Lombardi and Roy [7] on discrete ordered fields.

2 Pseudo-orders

The order relation of constructive real numbers satisfies the following axioms

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

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

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

Any order satisfying (P1)-(P3) is called a *pseudo-order* (following P. Aczel). Defining $x \leq y$ to be $\neg(y < x)$ the axiom (P1) can be read as

$$x < y \rightarrow x \leq y.$$

Lemma 2.1 *Any pseudo-order $<$ is transitive and $\leq$ is a partial order.* $\square$

An element x is an *upper bound* of a set M, if for every $y \in M$, $y \leq x$. The lower bound is defined dually.

Proposition 2.2 *Let $<$ be a pseudo-order which is discrete (or decidable), i.e. such that for all x, y*

$$x < y \text{ or } \neg(x < y).$$

Then $<$ satisfies the trichotomy law. $\square$

By this proposition a pseudo-order is, from a classical point of view, simply a linear order. Unlike a linear order, a pseudo-order does not guarantee that the supremum of any two elements exists:

$$(\forall xy)(\exists z)[x \leq z \,\&\, y \leq z \,\&\, (\forall u)(x \leq u \,\&\, y \leq u \Rightarrow z \leq u)] \tag{2}$$

The following example demonstrates that this existence statement is not a consequence of the axioms of a pseudo-order in intuitionistic first order logic.

Example 2.3 Consider the set $D = \{0, \alpha, \beta, 1\}$ of four distinct elements. Let $<_a$ be the strict partial order of D where 0 is the bottom element, 1 is the top element and α and β are unrelated. There are two ways to extend it to a total order: let $<_b$ and $<_c$ be the total orders given by $0 < \alpha < \beta < 1$ and $0 < \beta < \alpha < 1$, respectively. From this we build a Kripke model $\mathcal{M}$ with $K = \{a, b, c\}$ as the set of states (worlds), D as the constant domain of quantification, and $<_x$ as the interpretation of the order relation at state $x \in K$. The states are partially ordered by $\sqsubseteq$, such that a is the bottom element and b and c are unrelated. Then $x \sqsubseteq y$ implies that the relation $<_y$ extends $<_x$. It is now straightforward to check that the universal closure of (P1) – (P3) holds in $\mathcal{M}$. Assuming that (2) holds yields for $x = \alpha$ and $y = \beta$ some $\gamma \in D$ with

$$a \Vdash \alpha \leq \gamma \,\&\, \beta \leq \gamma, \tag{3}$$

and

$$a \Vdash (\forall u)(\alpha \leq u \,\&\, \beta \leq u \Rightarrow \gamma \leq u). \tag{4}$$

Now $a \Vdash \alpha \leq \gamma$ is equivalent to the statement that for all k: $k \nVdash \gamma < \alpha$. But this implies $\gamma = 1$ or $\gamma = \alpha$. Similarly, $a \Vdash \beta \leq \gamma$ implies $\gamma = 1$ or $\gamma = \beta$. The only possibility is thus that $\gamma = 1$. Now (4) implies that, at the later state $b \sqsupseteq a$, we have for all u

$$b \Vdash \alpha \leq u \,\&\, \beta \leq u \Longrightarrow b \Vdash 1 \leq u.$$

Now $u = \beta$ satisfies the antecedent, since $\alpha <_b \beta$. Hence $b \Vdash 1 \leq \beta$, which contradicts $\beta <_b 1$. We conclude that existence of the supremum of two elements is not provable, using intuitionistic logic, from the axioms for a pseudo-order. A dual argument shows that binary infima do not exist in this model. □

Remark 2.4 Related intuitionistic theories of strict (partial) order, but with axioms for minima and maxima are studied by Negri (1999).

For dense pseudo-orders the following is in many cases a useful substitute.

Lemma 2.5 *Let $(S, <)$ be a dense, pseudo-ordered set. Suppose the elements $a_1, \ldots, a_m, b_1, \ldots, b_n \in S$, $m, n \geq 1$, are such that $a_i < b_j$, for all i and j. Then there is $x \in S$ with*

$$a_i < x < b_j$$

for all i and j.

Proof. Do induction on m and n and use co-transitivity. □

Remark 2.6 To prove the existence of arbitrary large pseudo-orders seems to be difficult in the constructive setting. We can however show that each discrete set D is embedded in a pseudo-order inside a Kripke model. Let D^* be the set of finite strings of distinct elements from D. Order D^* by the subsequence ordering. Then order $D^* \times D^*$ by the coordinate-wise subsequence order $\sqsubseteq$. Consider now the subset K of this set consisting of $w = (a_1 \cdots a_m; b_1 \cdots b_n)$ where all elements are distinct. For such w let $<_w$ be the partial order where $a_1 < \cdots < a_m < x < b_1 < \cdots < b_n$ for each x in $D_w = D \backslash \{a_1, \ldots, a_m, b_1, \ldots, b_n\}$. All elements of D_w are unrelated. Thus $<_w$ is a finite approximation of a total order of D, and $<_w \subseteq <_{w'}$ for $w \sqsubseteq w'$. The resulting Kripke model can now be checked to verify the axioms of a pseudo-order.

Let **LO** be the category of pseudo-orders with maps, that satisfy

$$f(x) <' f(y) \Longrightarrow x < y,$$

as morphisms. The contraposition of this implication states that f is monotone with respect to $\leq$

$$x \leq y \Longrightarrow f(x) \leq f(y).$$

(Classically speaking, this is thus the category of linear orders, see [9]). Denote by **SO** the category of pseudo-orders with *order preserving maps* f

$$x < y \Longleftrightarrow f(x) <' f(y)$$

as morphisms. The requirement $\Leftarrow$ is not needed if $<$ is discrete. Every such f is clearly 1-1, by contraposition.

3 Completion of pseudo-orders

Let $(S, <)$ be a pseudo-order. A subset $L \subseteq S$ is called a *lower cut* if

(L1) $q \in L$ whenever $q < r$ and $r \in L$,

(L2) for every $q \in L$ there is some $r \in L$ with $q < r$.

The second axiom is the *openness* axiom. An *upper cut* $U \subseteq S$ is defined similarly replacing $<$ by the reverse relation $>$. The axioms are then called (U1) and (U2). The pair (L, U) is called a *cut* if $p < q$ whenever $p \in L$ and $q \in U$. The cut is *located* if

$$p < q \Longrightarrow p \in L \text{ or } q \in U.$$

It is *bounded*, if both L and U are non-void. A bounded, located cut is called a *Dedekind cut*.

Remark 3.1 *Partial cuts*, i.e. cuts which are not necessarily located or bounded, are of interest as extended real numbers in functional analysis (Richman 1997). $\square$

What are the principal cuts? Consider the sets

$$L_t = \{q \in S : q < t\} \qquad U_t = \{r \in S : t < r\}.$$

Then $(S, <)$ is dense if, and only if, L_t is a lower cut for each t, or equivalently U_t is an upper cut for each t. Moreover $(S, <)$ is unbounded upward if, and only if, U_t is non-void for each t. Similarly, $(S, <)$ is unbounded downward if, and only if, L_t is non-void for each t. Thus, if (S,<) is an unbounded, dense pseudo-order, then

$$\hat{t} = (L_t, U_t)$$

is a Dedekind cut for each $t \in S$. A trivial example of such an order is the empty set. The prime non-trivial examples are $(\mathbb{Q}, <)$ and $(\mathbb{R}, <)$.

Remark 3.2 *One-sided cuts.* For a dense unbounded pseudo-order S it suffices to specify only one side of the cut. First we observe that if (L, U) and (L, U') belong to $\bar{S}$ then $U = U'$. Indeed, if $x \in U$, then take $y \in U$ with $y < x$. Then $x \in U'$, since $y \in L$ is impossible. Similarly $U' \subseteq U$.

We note that a subset L that is part of $(L, U) \in \bar{S}$, satisfies in addition to (L1) and (L2), also the conditions

(L3) L is inhabited,

(L4) there is some y_0 so that for all $x \in L$, $x < y_0$,

(L5) for any $x < y$, $x \in L$ or y is an upper bound of L.

Suppose now that $L \subseteq S$ satisfies (L1) – (L5). Define

$$U^* = \{v \in S : (\exists y \in S) y < v \,\&\; y \text{ is an upper bound of } L\}.$$

By density and unboundedness, U^* satisfies (U1) and (U2) and is non-void. Clearly $x < y$ whenever $x \in L$ and $y \in U^*$. Suppose $x < y$. Pick by density $x < y' < y$. Thus by (L5) $x \in L$ or y' is an upper bound of L. In the latter case $y \in U^*$. Thus we have that $(L, U^*) \in \bar{S}$. □

Let S and T be pseudo-orders. An order preserving map $f : S \to T$ has the *intermediate value property* (IVP) if

$$f(x) < c < d < f(y) \Longrightarrow (\exists a \in S) c < f(a) < d,$$

equivalently $f[S]$ is dense in every interval $(f(x), f(y))$. Let **DO** be the category where the objects are unbounded, dense pseudo-orders and the morphisms are order preserving maps with the intermediate value property.

Lemma 3.3 **DO** *is a category.* □

It is easy to multiply the examples in this category by the following construction. Let $(L, <_L)$ be any discrete pseudo-order, i.e. a linear order. Let $(S, <_S)$ be an object of the category **DO**. Then consider the cartesian product $(L \times S, <^*)$ ordered lexicographically:

$$(p, x) <^* (q, y) \Longleftrightarrow p <_L q \text{ or } p = q \,\&\, x <_S y.$$

This is again an object of the category.

The morphisms of **DO** are lower and upper continuous with respect to the ordering, as the next lemma shows. Note however that inclusion map of $\{0 < 2\} \times \mathbb{Q}$ into $\{0 < 1 < 2\} \times \mathbb{Q}$ is continuous, but fails to have IVP.

Lemma 3.4 *Each morphism $f : S \to T$ in* **DO** *satisfies*

(a) If $c < f(x)$, then for some $a \in S$: $a < x$ and $c < f(a)$.

(b) If $f(x) < d$, then for some $b \in S$: $x < b$ and $f(b) < d$.

Proof. We prove (a), part (b) is similar. Suppose $c < f(x)$. By unboundedness, take $x_2 < x_1 < x$. Thus $f(x_2) < f(x_1)$ and we may compare this pair with c. Thus (P3) gives, $c < f(x_1)$, in which case we let $a = x_1$, or $f(x_2) < c$. In the latter case, we have $f(x_2) < c < f(x)$. By density there is d with

$$f(x_2) < c < d < f(x).$$

Thus by IVP, there is a with $c < f(a) < d$. But $f(a) < f(x)$, so by order preservation, $a < x$. $\Box$

Lemma 3.5 *Let $f, g : S \to T$ be morphisms in* **DO** *with $f(x) = g(x)$ for all $x \in M$ on some dense $M \subseteq S$. Then $f = g$.*

Proof. Let $x \in S$ be arbitrary. First suppose $f(x) < g(x)$. By Lemma 3.4 we get $x < b$ with $f(b) < g(x)$. By density pick $u \in M$ with $x < u < b$. Hence by order preservation and the assumption

$$g(x) < g(u) = f(u) < f(b).$$

But this contradicts $f(b) < g(x)$. Similarly one shows that $g(x) < f(x)$ is impossible. Hence $f(x) = g(x)$. $\Box$

For a pseudo-order $(S, <)$ let $\bar{S}$ denote the collection of Dedekind cuts (L, U) in $(S, <)$. Order this collection as follows

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

This order is illustrated by:

—— L' ————)(—— U' ——
—— L ———)(——— U ———

Observe that by using the axioms for lower and upper cuts:

$$(L, U) \leq (L', U') \iff L \subseteq L' \text{ and } U' \subseteq U. \tag{5}$$

In predicative theories it is not clear that $\tilde{S}$ is a set. We remark that the collection $\tilde{S}$ of partial cuts in S is not a set in such theories. Let $a < b$ in S. For any proposition P not depending on x consider the partial cut

$$(\{x \in S : x < a \,\&\, P\}, U_b).$$

Assuming $\tilde{S}$ to be a set would imply that the collection of propositions is a set, which is false in predicative type theories. We will return to this problem in Sections 4 – 8.

Lemma 3.6 *If $(S, <)$ is a pseudo-order, then so is $(\bar{S}, <)$.*

Proof. (P1) for $\bar{S}$ follows easily from (P1) for S. (P2) follows immediately from the observation (5). As for (P3) assume that $(L, U) < (L', U')$ so there is some $a \in L' \cap U$. Use the openness (U2) and (L2) to obtain $p \in U$ and $q \in L'$ with $p < a < q$. Now taking an arbitrary cut (L'', U''), its localization property yields $p \in L''$ or $q \in U''$. In the former case $p \in L'' \cap U$, so $(L, U) < (L'', U'')$. The latter case gives similarly $(L'', U'') < (L', U')$. □

Lemma 3.7 *Let $(S, <)$ be a dense, unbounded pseudo-order. Then: the set of principal cuts $\{\hat{a} : a \in S\}$ is dense in $(\bar{S}, <)$, and $(\bar{S}, <)$ is unbounded.*

Proof. Density follows by observing that in the construction involved in (P3) of Lemma 3.6, we have $(L, U) < \hat{a} < (L', U')$. The pair $\hat{a} = (L_a, U_a)$ is a cut, since $(S, <)$ is dense. We check that $\bar{S}$ is unbounded. Let (L, U) be a given cut. In virtue of the unboundedness of A we may pick $a, a' \in L$ and $b, b' \in U$ with $a < a' < b' < b$. Thus $(L_a, U_a) < (L, U) < (L_b, U_b)$. □

Corollary 3.8 *The map $\hat{(\ )} : S \to \bar{S}$ is a morphism in* **DO**.

Proof. By Lemma 3.7 it is sufficient to prove that $\hat{(\ )}$ is order-preserving. Note that for $a, b \in A$, we have $\hat{a} < \hat{b}$ if, and only if, $L_b \cap U_a$ is non-void, if, and only if, $a < c < b$ for some c. The latter is equivalent to $a < b$, by the density of A. □

Consider a morphism $f : (S, <) \to (T, <)$ in **DO**. For any $X \subseteq S$ define

$$\begin{aligned} f_{-}[X] &= \{y \in T : (\exists x \in X)\, y < f(x)\} \\ f_{+}[X] &= \{y \in T : (\exists x \in X)\, f(x) < y\}. \end{aligned}$$

Then for $(L, U) \in \bar{S}$, let

$$\bar{f}(L, U) =_{\text{def}} (f_{-}[L], f_{+}[U]).$$

Lemma 3.9 $\bar{(\ )} :$ **DO** $\to$ **DO** *is a functor.* □

Proof. Let f be as above and $(L, U) \in \bar{S}$. First we need to check that $\bar{f}(L, U) \in \bar{T}$. The case of locatedness is the most interesting. Consider arbitrary $p < q$ in T. Pick $x \in L$ and $y \in U$ so that $x < y$, and hence $f(x) < f(y)$. Then pick p', q' so that $p < p' < q' < q$. Now we compare $p < p'$ to $f(x)$. In case $p < f(x)$, we have $p \in f_{-}[L]$. Otherwise: $f(x) < p'$. Next compare $q' < q$ to $f(y)$. In case, $f(y) < q$, we get $q \in f_{+}[U]$. Otherwise: $q' < f(y)$, and consequently

$$f(x) < p' < q' < f(y).$$

By IVP (twice) pick a, b with $p' < f(a) < f(b) < q'$. Thus $a < b$. By the locatedness of (L, U), we have $a \in L$, in which case $p < f(a)$ yields $p \in f_{-}[L]$, *or* $b \in U$, in which case, $q \in f_{+}[U]$.

To prove the IVP for $\bar{f}$ one reduces it to IVP for f. The remaining properties are straightforward to check. □

We shall prove that $\bar{S}$ is order complete in the constructive sense (Bishop and Bridges 1985).

Upper bounds and suprema are defined as usual in terms of the partial order $\leq$ (see Section 2). Let $(S, <)$ be a pseudo-order. A non-void $X \subseteq S$ is *upper located* if for all $a < b$ in either $a < x$ for some $x \in X$, or b is an upper bound of X. (Note that in classical set theory, this condition is vacuously true.) Using co-transitivity we can show that finitely enumerable sets $\{x_1, \ldots, x_n\}$ are upper located in a pseudo-order. A pseudo-order $(S, <)$ is *sup-complete* if for every subset $X \subseteq A$ which is upper located, and has an upper bound in S, the supremum of X exists. *Lower locatedness* and *inf-completeness* are defined as the obvious dual notions. The following is an analogue to the classical result for lattices.

Theorem 3.10 *Suppose that $(S, <)$ is a dense, unbounded, pseudo-order. If $(S, <)$ is sup-complete, then $(S, <)$ is inf-complete.*

Proof. Assume that $X \subseteq S$ has a lower bound, is non-void and is lower located. Then for any $x < y$: x is a lower bound of X or $u < y$ for some $u \in X$. Define the set of strict lower bounds of X

$$Y = \{z \in S : (\forall x \in X)\, z < x\}.$$

It is non-void and has a upper bound, since X has an lower bound and is non-void. To show that Y is upper located, assume $w < z$. By density then take $w < w'' < w' < z$. Since X is lower located, we have that w' is a lower bound of X, in which case $w'' \in Y$ and $w < w''$, *or* we have that for some $u \in X$, $u < z$. In this case $s < u$ for all $s \in Y$, and hence z is an upper bound of Y.

We may thus conclude that $t = \sup Y$ exists. We show that t is the infimum of X. Any $x \in X$ is an upper bound of Y, and so $t \leq x$. Hence t is a lower bound of X. Assume now that u is a lower bound of X. We show that $u \leq t$. Suppose $t < u$ and pick $t < u' < u$ by density. Then $u' < x$ for all $x \in X$. Hence $u' \in Y$, and so by definition of t, $u' \leq t$. Hence $t < t$, which is a contradiction. Thus $u \leq t$. □

Let **CDO** denote the full subcategory of **DO** consisting of those objects that are sup-complete.

Theorem 3.11 $(\bar{\ })$: **DO** $\to$ **CDO** *is a functor.*

Proof. We already know it is a functor into the category **DO**. It suffices to prove that each $\bar{A}$ is sup-complete. Let $X = \{(L_i, U_i) : i \in I\}$ be a non-void set, which has an upper bound and is upper located. Put

$$L = \cup_{i \in I} L_i.$$

Then L is non-void, and satisfies (L1) and (L2) since each L_i does. Let

$$U = \{x \in A : (\exists u)\ u < x \,\&\, (\forall i \in I)\, u \in U_i\},$$

which is the interior of $\cap_{i \in I} U_i$. By density of A, (U2) holds. (U1) is clear by definition. Now X has an upper bound so there is some $(L', U') \in \bar{A}$ with $L_i \subseteq L'$ and $U' \subseteq U_i$ for all $i \in I$). Thus $U' \subseteq \cap_{i \in I} U_i$. Pick $u \in U'$ and $x \in A$ with $u < x$. Hence $x \in U$, so U is non-void. Now $U \subseteq \cap_{i \in I} U_i$, so for any $x \in L$ and $y \in U$, we have $x < y$. It follows that (L, U) is a bounded cut. We prove it is located. Let $q < r$ be elements in A. Again by density, pick an element in between: $q < t < r$. Thus $\hat{q} < \hat{t}$. We now use the lower locatedness of X; this gives two cases.

Case 1: $\hat{q} < (L_i, U_i)$ for some $i \in I$. Thus for some $a \in L_i \cap U_q$. Hence $q < a$, and so $q \in L_i \subseteq L$.

Case 2: $(L_i, U_i) \leq \hat{t}$ for all $i \in I$. Thus $U_t \subseteq U_i$ for each $i \in I$. Now $t < r$ so insert $t < t' < r$. This t' is in each U_i, $i \in I$. Hence $r \in U$.

Thus (L, U) is located. It is clear that it is an upper bound of X. Suppose that $(\hat{L}, \hat{U})$ is another upper bound. Then $L_i \subseteq \hat{L}$ and $\hat{U} \subseteq U_i$. Hence $L \subseteq \hat{L}$ and $\hat{U} \subseteq \cap_{i \in I} U_i$. Now since $\hat{U}$ satisfies (U2): if $x \in \hat{U}$, then for some $y < x$, $y \in \hat{U}$, and hence $y \in \cap_{i \in I} U_i$; this means that $x \in U$. □

Lemma 3.12 *Let A be an object of* **DO**. *For every $g : A \to B$ in* **DO** *where B is in* **CDO**, *there is a unique morphism $h : \bar{A} \to B$ in* **DO** *such that $g = h \circ \hat{(\ )}$.*

Proof. Since $\hat{A}$ is dense in $\bar{A}$, it follows by Lemma 3.7 that h is unique if it exists. For $(L, U) \in \bar{A}$, the image $g[L]$ is indeed upper located (the proof of this is similar to locatedness in Lemma 3.9) so we may define

$$h(L, U) = \sup g[L].$$

Clearly,

$$h(\hat{a}) = \sup g[L_a] \leq g(a).$$

By density $h(\hat{a}) < g(a)$ is impossible. Thus $h(\hat{a}) = g(a)$. Order preservation and IVP of h can be reduced to the same properties of g. □

Corollary 3.13 *The functor* $\bar{(\ )} : \mathbf{DO} \to \mathbf{CDO}$ *is left adjoint to the forgetful functor* $U : \mathbf{CDO} \to \mathbf{DO}$.

It follows that the order-completion is unique up to isomorphism.

Remark 3.14 Consider a dense, unbounded, pseudo-order $(S, <)$ and equip it with the order topology. Then one can show that the partial order $\leq$ is the topological closure of $<$. Mac Neille (1937) introduced a generalization of Dedekind completions to partially ordered sets, see Johnstone (1982). The following defines an order preserving embedding of $(\overline{S}, \leq)$ into that completion

$$(L, U) \mapsto (cl(L), cl(U)).$$

Here $cl(S)$ denotes the topological closure of S.

4 Set-representability: discrete case

We now turn to the problem of representing the collection $\bar{S}$ of bounded, located cuts by a type-theoretic set. First we consider the case where the order $<$ of S is discrete as in Proposition 2.2. Then for any cut $(L, U) \in \bar{S}$ and all $x, y \in S$ one or two of the following possibilities hold:

$n = 1$: $x < y$ and $x \in L$

$n = 2$: $x < y$ and $y \in U$

$n = 3$: $y \leq x$.

By the type-theoretic axiom of choice we find $\theta : S \times S \to \{1, 2, 3\}$ which selects one of the cases $\theta(x, y)$ for each pair (x, y). Now this choice operation[1] represents the cut

$$z \in L \Longleftrightarrow (\exists x \in S) z < x \,\&\, \theta(z, x) = 1$$

$$z \in U \Longleftrightarrow (\exists y \in S) y < z \,\&\, \theta(y, z) = 2$$

The implications from right to left are clear by definition of θ. Suppose that $z \in L$, then there is some $x \in L$ with $z < x$. Then $\theta(z, x) = 3$ is impossible, and $\theta(z, x) = 2$ would mean that $x \in U$, which is false. Hence $\theta(z, x) = 1$. This proves the reverse implication. The case for U is symmetric. The operation $S \times S \to \{1, 2, 3\}$ form a set. Thus it is clear that the cuts $\bar{S}$ can be represented by pairs of subsets of the form

$$(\{z \in S : (\exists x \in S) z < x \,\&\, \theta(z, x) = 1\}, \{z \in S : (\exists y \in S) y < z \,\&\, \theta(y, z) = 2\}).$$

Hence there is no need to refer to arbitrary subsets anymore in this case.

To give a non-trivial example of a discrete order in **DO**, consider the set $\mathbb{Q}(t)$ of rational functions with coefficients in $\mathbb{Q}$ and ordered as

$$p(t) < q(t) \Longleftrightarrow (\exists M)\, (\forall x > M)\, [p(x) < q(x)].$$

[1] Meaning that the equality on $S \times S$ is the weakest possible, i.e. an identity type.

5 Ordered groups

We define the constructive counterpart of a totally ordered group and its completion (see Dales and Woodin [4]).

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

(G1) $x < y$ implies $x + z < y + z$.

Lemma 5.1 *Let G be a pseudo-ordered group. Then for $x = y$, it is a sufficient condition that $x < y + \varepsilon$ and $y < x + \varepsilon$, for each $\varepsilon > 0$.*

Proof. Assume the condition. By (P2) it suffices to show that $\neg x < y$ and $\neg y < x$. Assume $x < y$. Then $\varepsilon = y - x > 0$. But $x < y + \varepsilon = x$. This is impossible. Similarly, one shows that $y < x$ is impossible. □

An element x is called *positive* if $x > 0$. Note that it follows (from co-transitivity and G1) that if $x + y$ is positive, then at least one of x and y is positive. The group is *non-trivial* if it contains some positive element. It is *archimedean,* if for all x and y positive, there exists a natural number n such that $x < ny$. It is *dense* if the order is dense. It is *divisible* if for any x and any natural number n, there exists y with $x = ny$.

The real numbers under addition, and the usual order, constitute a divisible, archimedean group. Every divisible group is dense. The following is sometimes a useful substitute for divisibility.

Lemma 5.2 *Let G be a dense, pseudo-ordered group. If $\varepsilon > 0$, then for each positive natural number n, there exists $\delta > 0$ with $0 < n\delta < \varepsilon$.*

Proof. It suffices to prove the case $n = 2$, since the case for larger n can be obtained by iteration. By density, take $0 < \delta' < \varepsilon$. By Lemma 2.5 there exists $0 < \delta < \delta', \varepsilon - \delta'$. Thus $0 < 2\delta < \delta' + \varepsilon - \delta' = \varepsilon$. □

A cut (L, U) in G is called a *Cauchy cut* if for every positive ε there exist $a \in L$ and $b \in U$ with $b < a + \varepsilon$. The group G is *Cauchy complete* if for every Cauchy cut (L, U) there is $t \in G$, with $x < t < y$ for all $x \in L$ and $y \in U$. The latter is written as $L < t < U$. From Lemma 5.1 it follows that such a t must be unique.

Proposition 5.3 *Let G be a non-trivial, dense pseudo-ordered group. Then:*

(i) Every principal cut is a Cauchy cut.

(ii) Every Cauchy cut is a Dedekind cut.

(iii) If G is archimedean, then every Dedekind cut is a Cauchy cut.

Proof. (i) is obvious.

(ii): Let (L, U) be a Cauchy cut. We show that it is located. Suppose that $u < v$. By density pick $u < z < v$, and then take $0 < \varepsilon < z - u, v - z$, by Lemma 2.5. There exists $x \in L$ with $x + \varepsilon \in U$ since we have Cauchy cut. If $u < x$, then $u \in L$. On the other hand, if $x < z$, then $x + \varepsilon < z + \varepsilon < z + v - z = v$, so $v \in U$.

(iii): Assume G is archimedean. Let $\varepsilon > 0$, and take $\varepsilon' > 0$ so that $2\varepsilon' < \varepsilon$ by Lemma 5.2. There are some $x_0 \in L$ and $y_0 \in U$. Since the group is archimedean, there is a positive natural number n so that $n\varepsilon' > y_0 - x_0$. Let $x_k = x_0 + k\varepsilon'$. Thus $x_n > y_0$. Then we can find an index i such that $x_i \in L$ and $x_{i+2} \in U$. (Such an i can be shown to exist by induction on n.) For this index $x_i + \varepsilon > x_{i+2} \in U$. □

To see that part (iii) need not hold if G is non-archimedean we have the following example.

Example 5.4 Consider the group of rationals $\mathbb{Q}$ ordered as usual with $<$. Let $G = \mathbb{Q} \times \mathbb{Q}$ be the product group, and order it lexicographically

$$(p, x) <^* (q, y) \iff p < q \text{ or } p = q \,\&\, x < y.$$

Then $(G, +, (0, 0), <^*)$ is a divisible, non-archimedean, pseudo-ordered group. It is, in fact, totally ordered. The following is a Dedekind cut

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

However, considering an "infinitesimal" $\varepsilon = (0, 1)$ one sees that it cannot be a Cauchy cut.

For G a non-trivial, dense, pseudo-ordered group, let $\tilde{G}$ be the collection of Cauchy cuts. We order $\tilde{G}$ as the Dedekind cuts. Define addition of $x = (L^x, U^x)$ and $y = (L^y, U^y)$ as $x + y = (L', U')$ where

$$\begin{aligned} L' &= \{a \in G : (\exists u \in L^x)(\exists v \in L^y) a < u + v\}, \\ U' &= \{b \in G : (\exists w \in U^x)(\exists z \in U^y) w + z < b\}. \end{aligned}$$

The additive inverse of (L, U) is $(-U, -L)$ where $-S = \{-t : t \in S\}$.

Theorem 5.5 *The Cauchy cuts $\tilde{G}$ of a non-trivial, dense, pseudo-ordered group G form a set (in Martin-Löf type theory). Moreover*

(i) $\tilde{G}$ is a non-trivial, dense, Cauchy-complete, pseudo-ordered group,

(ii) G, considered as the set of principal cuts is a dense, ordered subgroup of $\tilde{G}$.

Proof. First we prove set-representability. Let G^+ be the positive elements of G, more precisely the type

$$(\Sigma\varepsilon \in G)\,(\varepsilon > 0)$$

and where the equality is given by the identity type. Let (L, U) be a Cauchy cut in G. For every $(\varepsilon, q) \in G^+$ choose $\alpha_{(\varepsilon,q)} \in L$, $\beta_{(\varepsilon,q)} \in U$ with $\beta_{(\varepsilon,q)} < \alpha_{(\varepsilon,q)} + \varepsilon$. Since the equality on G^+ is the identity type, α and β may be considered as functions $G^+ \to G$. Let

$$\begin{array}{rcl} L_\alpha & = & \{x \in G : (\exists(\varepsilon, q) \in G^+)\, x < \alpha_{(\varepsilon,q)}\} \\ U_\beta & = & \{y \in G : (\exists(\varepsilon, q) \in G^+)\, \beta_{(\varepsilon,q)} < y\}. \end{array}$$

Clearly $L_\alpha \subseteq L$. For the converse, suppose $x \in L$. Take $y, z \in L$ with $x < y < z$ and let $\varepsilon = z - y$. Let q be the proof-object for $\varepsilon > 0$. Thus $\alpha_{(\varepsilon,q)} \in L$ and $\beta_{(\varepsilon,q)} \in U$ and $\beta_{(\varepsilon,q)} < \alpha_{(\varepsilon,q)} + \varepsilon$. Since $x < y$, we have by co-transitivity, $x < \alpha_{(\varepsilon,q)}$, in which case $x \in L_\alpha$, or we have the case $\alpha_{(\varepsilon,q)} < y$. But since

$$\beta_{(\varepsilon,q)} < \alpha_{(\varepsilon,q)} + \varepsilon < y + \varepsilon = z,$$

the latter case is in fact impossible.

The proof of $U_\beta = U$ is symmetric. Thus every Cauchy cut is of the form (L_α, U_β) where $\alpha, \beta : G^+ \to G$. Now since $G^+ \to G$ is a set in Martin-Löf type theory, we have proved the first statement of the theorem.

The axioms for a dense, pseudo-ordered group are straightforward to check. It is also easy to check that G is an ordered subgroup of $\tilde{G}$, identifying elements t of G with the principal cuts $\hat{t} = (L_t, U_t)$. As in Lemma 3.6 one proves that G is dense in $\tilde{G}$.

By the above we know that $\tilde{G}$ can be represented by a set. Write for $\alpha \in \tilde{G}$, the corresponding cut in G as (L^α, U^α). Now suppose $(\tilde{L}, \tilde{U})$ is a Cauchy cut in $\tilde{G}$. We are required to find a cut $x = (L', U')$ in $\tilde{G}$ so that $\tilde{L} < x < \tilde{U}$. Let

$$L' = \bigcup_{\alpha \in \tilde{L}} L^\alpha \qquad U' = \bigcup_{\beta \in \tilde{U}} U^\beta.$$

Then it is clear that (L', U') satisfies L1-2, U1-2 and is bounded. Suppose $u \in L'$ and $v \in U'$. Thus $u \in L^\alpha$ and $v \in U^\beta$ for some $\alpha \in \tilde{L}$ and $\beta \in \tilde{U}$. Then $\alpha < \beta$ so $L^\beta \cap U^\alpha$ is inhabited, by w say. Thus $u < w < v$.

We check that $x = (L', U')$ is a Cauchy cut: let ε be positive in G. Take $\alpha \in \tilde{L}$ and $\beta \in \tilde{U}$ with $\beta < \alpha + \varepsilon$. But this means that $L^{\alpha+\varepsilon} \cap U^\beta$ is inhabited, by w say. Hence by the definition of addition there are $u \in L^\alpha, v \in L^\varepsilon = L_\varepsilon$ with $w < u + v$. Hence $w < u + \varepsilon$, and $u \in L'$ and $w \in U'$.

Finally, we check that $\tilde{L} < z < \tilde{U}$. Let $\alpha \in \tilde{L}$. Take $\alpha' > \alpha$ where $\alpha' \in L$. Thus $U_\alpha \cap L_{\alpha'}$ is non-void, and so is

$$U_\alpha \cap L' = \bigcup_{\alpha' \in \tilde{L}} (U_\alpha \cap L_{\alpha'}).$$

Hence $\alpha < x$. Similarly, one shows that $x < \beta$ for $\beta \in \tilde{U}$. $\Box$

6 Ordered fields

Scott [16] observed that the Cauchy cuts can be used for completing fields as well. The notion of Cauchy-completeness can also be expressed by generalised sequences or nets ([4] use ordinals). For establishing basic algebraic properties about fields it is probably easier to work with such nets. We prove first that the methods are equivalent for groups.

Let $(G, <)$ be a pseudo-ordered group. Let $P = (P, \sqsubseteq)$ be a directed pre-order. (Here it seems necessary to allow pre-orders rather than partial orders.) A *Cauchy net on* P is a function $\Phi : P \to G$ such that for every positive ε in G there exists an $\alpha \in P$ such that for all $\beta, \beta' \sqsupseteq \alpha$:

$$-\varepsilon < \Phi(\beta) - \Phi(\beta') < \varepsilon.$$

$\Phi : P \to G$ *converges to* x if for each positive ε in G there is $\alpha \in P$ such that for all $\beta \sqsupseteq \alpha$:

$$-\varepsilon < \Phi(\beta) - x < \varepsilon.$$

Theorem 6.1 *Let G be a dense, non-trivial pseudo-ordered group. Then G is Cauchy-complete if, and only if, for any directed pre-order P, every Cauchy net on P converges to a point in G.*

Proof. $(\Rightarrow)$ Suppose that $\Phi : P \to G$ is a Cauchy net in G. Then

$$L = \{u \in G : (\exists v)(u < v \,\&\, \exists\alpha(\forall\beta \sqsupseteq \alpha) v < \Phi(\beta))\}$$

and

$$U = \{u \in G : (\exists v)(v < u \,\&\, \exists\alpha(\forall\beta \sqsupseteq \alpha)\Phi(\beta) < v)\}.$$

can be checked to be a Cauchy cut. Let x be such that $L < x < U$. It can easily be verified that the Cauchy net converges to x.

$(\Leftarrow)$ Let (L, U) be a Cauchy cut. Consider again $P = G^+$, equipped with the identity type as equality; see Theorem 5.5. Clearly, if $(\varepsilon, q) \in P$, then there are $u \in G$ and $u' \in G$ with

$$u \in L \,\&\, u' \in U \,\&\, u' < u + \varepsilon.$$

We thus find a choice function $\Phi : P \to G$ (remember what the equality on P is) such that for $\alpha = (\varepsilon, q) \in P$

$$\Phi(\alpha) \in L \,\&\, (\exists u' \in U) \,\&\, u' < \Phi(\alpha) + \varepsilon.$$

Pre-order P by $(\varepsilon, q) \sqsubseteq (\varepsilon', q')$ iff $\varepsilon' \leq \varepsilon$. We claim that $\Phi : P \to G$ is a Cauchy-net. For $\varepsilon > 0$ take $\varepsilon' > 0$ such that $0 < 2\varepsilon' < \varepsilon$. Let

$\alpha = (\varepsilon', q')$ where q' is some proof object for $\varepsilon' > 0$. Now if $\beta_1, \beta_2 \sqsupseteq \alpha$, where $\beta_i = (\varepsilon_i, q_i)$, we have $0 < 2\varepsilon_i \leq 2\varepsilon' < \varepsilon$ and

$$\Phi(\beta_i) \in L \,\&\, (\exists u_i \in U) \,\&\, u_i < \Phi(\beta_i) + \varepsilon_i \leq \Phi(\beta_i) + \varepsilon'.$$

for $i = 1, 2$. Let $\Delta = \Phi(\beta_1) - \Phi(\beta_2)$. Comparing Δ to $\varepsilon' < 2\varepsilon'$, we have $\varepsilon' < \Delta$ or $\Delta < 2\varepsilon'$. In the former case $\Phi(\beta_1) > \Phi(\beta_2) + \varepsilon'$, so $\Phi(\beta_1) > u_2$ which is impossible, since $u_2 \in U$ and $\Phi(\beta_1) \in L$. Thus $\Delta < 2\varepsilon'$. Similarly, one shows $-2\varepsilon' < \Delta$. Thus $-\varepsilon < \Delta < \varepsilon$.

Let x be a limit of Φ. We claim that $L < x < U$.

Let $u \in L$ and take $u < u' < u'' \in L$. Pick $\varepsilon > 0$ so that $2\varepsilon < u' - u, u'' - u'$. For this bound there is some α such that for all $\beta \sqsupseteq \alpha$

$$\Phi(\beta) - \varepsilon < x < \Phi(\beta) + \varepsilon.$$

Write $\alpha = (\varepsilon', q')$ and $\alpha_0 = (\varepsilon, q)$ and take $\beta = (\varepsilon'', q'') \sqsupseteq \alpha, \alpha_0$. Compare $y = \Phi(\beta) - \varepsilon$ to $u < u'$. We have $y < u'$ or $u < y$. If $y < u'$, then $y + 2\varepsilon < u' + (u'' - u') = u''$. But $\Phi(\beta) \in L$ with $v < \Phi(\beta) + \varepsilon''$ for some $v \in U$. Since $\varepsilon \geq \varepsilon''$, $y + 2\varepsilon = \Phi(\beta) + \varepsilon \in U$, but then also $u'' \in U$, which is a contradiction to the choice of u''. Hence $u < y$ is the only possibility, and $y < x$, so $u < x$.

Let $v \in U$. We are to show $x < v$. Take $v' < v$ with $v' \in U$ and then pick $\varepsilon > 0$ so that $2\varepsilon < v - v'$. Thus for some $\alpha = (\varepsilon', q')$, we have for any $\beta \sqsupseteq \alpha$

$$\Phi(\beta) - \varepsilon < x < \Phi(\beta) + \varepsilon \tag{6}$$

Let $\alpha_0 = (\varepsilon, q)$ where q is the proof object for $\varepsilon > 0$. Take now $\beta = (\varepsilon'', q'') \sqsupseteq \alpha, \alpha_0$. Then $\Phi(\beta) \in L$ and there is some $v'' \in U$ with $v'' < \Phi(\beta) + \varepsilon''$. Let $z = \Phi(\beta) + \varepsilon$. Then $v - \varepsilon < z$ or $z < v$. In the former case $v - 2\varepsilon < \Phi(\beta)$. Hence $v - 2\varepsilon \in L$ which by $2\varepsilon < v - v'$ yields $v' \in L$. This is impossible. The latter case $z < v$ must therefore hold. Then (6) gives $x < v$. $\Box$

A commutative ring with 1 is *local* if for any invertible $x+y$, x is invertible or y is invertible. A local ring A is *ordered* if there is a subset $P \subseteq A$ closed under addition and multiplication, containing 1, but not 0, and furthermore satisfying

(O1) x invertible iff $x \in P$ or $-x \in P$.

(O2) if $x \notin P$ and $-x \notin P$, then $x = 0$.

The actual order, defined by $x < y$ iff $y - x \in P$, is clearly transitive. Note that $<$ is a pseudo-order on A. To check co-transitivity, assume $x < y$. Let z be arbitrary. Hence $y - x \in P$ and $y - x = (y - z) + (z - x)$, so $y - z$ or $z - x$ is invertible. If $y - z$ is invertible, then by (O1) we have either $y < z$, and so $x < z$, or $z < y$. Similarly, $z - x$ invertible implies $z < x < y$ or $x < z$.

Ordered local rings A are also known as *ordered Heyting fields*; see [11]. It is easy to see that the additive part G is a pseudo-ordered group which is divisible and non-trivial. Thus $\tilde{G}$ is Cauchy-complete and we may define multiplication in the standard way. For $x, y \in \tilde{G}$, let $x_\alpha, y_\alpha \in G$ be sequences indexed by $\alpha \in P$ converging to x and y respectively. Multiplication is defined in G so we let $z_\alpha = x_\alpha y_\alpha$ for $\alpha \in P$. The standard proof that this is a Cauchy net can now be used. Write $\tilde{A}$ for $\tilde{G}$ extended with the multiplication operation.

Theorem 6.2 *If A is an ordered local ring, then $\tilde{A}$ is a Cauchy complete, ordered local ring.*

Proof. The algebraic laws are easy to check directly using the Cauchy nets. We consider the existence of inverses. Suppose that $x > 0$ and that $x_\alpha \to x$ where $\alpha \in P$ and $x_\alpha \in A$. Then there exists a $\delta > 0$ in A and $\gamma \in P$ so that for all $\alpha \sqsupseteq \gamma$: $x_\alpha > \delta$. Now form a new index set

$$P_\gamma = (\Sigma \alpha \in P)\alpha \sqsupseteq \gamma$$

thus consisting of all (α, q) where q is a proof object for $\alpha \sqsupseteq \gamma$. The pre-order is given by

$$(\alpha, q) \sqsubseteq (\beta, r) \Longleftrightarrow \alpha \sqsubseteq \beta.$$

The fundamental sequence for the inverse is then $\Phi : P_\gamma \to A$ given by $\Phi(\alpha, q) = x_\alpha^{-1}$. For $\varepsilon > 0$, let $\gamma_1 \sqsupseteq \gamma$ be such that

$$-\delta^2\varepsilon < x_\beta - x_\alpha < \delta^2\varepsilon$$

for all indices $\alpha, \beta \sqsupseteq \gamma_1$. For such indices also

$$-\varepsilon < \frac{1}{x_\alpha} - \frac{1}{x_\beta} < \varepsilon.$$

So Φ is a Cauchy net on P_γ. $\square$

Example 6.3 Let $A = \mathbb{Q}(t)$ be the field of rational functions in one indeterminate. Every such function can be written uniquely as $\alpha(t) = f(t)/g(t)$ where $g(t)$ is a monic polynomial, with no common factor with the polynomial $f(t)$. For $f(t) \neq 0$, declare $\alpha(t)$ to be positive (negative) if the sign of the leading coefficient of $f(t)$ is positive (negative). In this field t is thus larger than any rational number. Thus we obtain a standard example of a discrete non-archimedean ordered field. In the Cauchy completion $\tilde{A}$ of A, the sequence $x_n = 2^{-n}$ is not Cauchy. For if $\varepsilon = t^{-1}$, the difference $|x_m - x_n|$ is larger than ε whenever $m \neq n$. On the other hand, if a_n is any sequence of rational numbers then, the sequence

$$y_m = \sum_{n=0}^{m} a_n t^{-n}$$

is Cauchy.

The field $\tilde{A}$ is not sup-complete, and not even real closed. Consider the set

$$S = \{b \in \tilde{A} : 0 < b \,\&\, b^2 < t\}.$$

It is easily seen to be upper located by considering elements

$$x = q(t) + r(t)/p(t) \tag{7}$$

where p, q, r are polynomials and the degree of r is less than that of p. Suppose that S has a supremum α. Using the continuity of multiplication one shows that $\alpha^2 = t$, $\alpha > 0$. By density one picks a positive $x \in A$ such that $x < \alpha < x + t^{-1}$. Thus $x^2 < t < x^2 + 2xt^{-1} + t^{-2}$. Considering x as in (7) on sees that this is impossible. We conclude that S has no supremum. The second part of the argument shows also that $\tilde{A}$ is not real closed.

7 Some type-theoretic constructions

To prove set-representability of located cuts, when $<$ is neither discrete, nor is part of some archimedean group, we use some more elaborate type-theoretic constructions.

7.1 Regular universes

We define a type-theoretic counterpart to regular sets (Aczel 1986). A *regular universe* is a pair (U, T) where U is a set and $T : U \to \mathrm{Set}$ is a family indexed by this set and which satisfies the closure axioms

$$\frac{a : U \qquad b : T(a) \to U}{\sigma(a, b) : U}, \qquad T(\sigma(a, b)) = \Sigma(T(a), (x)T(b(x))). \tag{8}$$

Notice this formal resemblance to a regular cardinal κ: If $|I| < \kappa$ and $\kappa_i < \kappa$ for each $i \in I$, then $\cup_{i \in I} \kappa_i < \kappa$. According to the Curry-Howard interpretation, U may also be regarded as a set of propositions which is closed under conjunction ($a \,\&\, b = \sigma(a, (x)b)$) and existential quantification over sets in U.

Let $B : A \to \mathrm{Set}$ be a family of sets indexed by $A : \mathrm{Set}$. This family is enclosed in (U, T) if there is a function ε so that

$$\frac{a : A}{\varepsilon(a) : U}, \qquad T(\varepsilon(a)) = B(a). \tag{9}$$

We say that a set X is *included* in (U, T) if $X = T(a)$ for some $a : U$. The minimal U, T defined by (8) and (9), and where σ and ε are constructors is the *canonical regular universe* enclosing B. Denote it by $(U(B), T(B))$. This universe could also be considered as the set of "enumerable" sets relative to the family B. Define the regular power set of X enclosing B as

$$\mathcal{R}(X) = \mathcal{R}_B(X) =_{\mathrm{def}} X \to U(B)$$

Remark 7.1 Universes corresponding to inaccessible cardinals are considered in (Martin-Löf 1984). Canonical universes over families have been studied in (Palmgren 1998).

7.2 Well-founded choices

We give a generalisation of the principle of dependent choice. The choices are indexed by well-founded trees instead of natural numbers.

Let I be a set and let B be a family of sets over I and take $W(I,B)$ to be the W-type specified by these data. It consists of well-founded, usually infinitely branching, trees. Denote by $\sup(i,f) : W(I,B)$ the tree formed from the subtrees $f(u) : W(I,B)$ $(u : B(i),\ i : I)$. There are natural recursion and induction principles associated with these trees (Martin-Löf 1984).

Theorem 7.2 (Well-founded Dependent Choice) *Let $W = W(I,B)$ for a family of sets B over the set I. Write $B_i = B(i)$ and $\sup_i h = \sup(i,h)$. 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 $g : B_i \to X$*

$$(\forall u : B_i)\, P(gu) \Rightarrow (\exists y : X)P(y) \wedge (\forall u : B_i)\, R_{i,u}(gu, y) \tag{10}$$

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

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

Proof. The proof is analogous to that for $\mathbb{N}$-dependent choice. We shall define by W-recursion a suitable function $q : W \to (\Sigma y : X)P(y)$. The details are as follows. Write $q = \langle q_1, q_2\rangle$. Assume that $t(i,g)$ is the proof object for (10). Suppose that for $i : I,\ h : B_i \to W,\ u : B_i$

$$(q_1 \circ h)(u) : X \qquad\qquad (q_2 \circ h)(u) : P((q_1 \circ h)(u)).$$

Let $g = q_1 \circ h$ and feed $k = q_2 \circ h$ to the proof-object $t(i,g)$. Thus writing $t = \langle t_1, \langle t_2, t_3\rangle\rangle$ we have by (10)

$$t_1(i, q_1 \circ h, q_2 \circ h) : X$$

$$t_2(i, q_1 \circ h, q_2 \circ h) : P(t_1(i, q_1 \circ h, q_2 \circ h))$$

$$t_3(i, q_1 \circ h, q_2 \circ h) : (\forall u : B_i)\, R_{i,u}((q_1 \circ h)(u), t_1(i, q_1 \circ h, q_2 \circ h)).$$

The recursive step is now taken by defining

$$q(\sup_i h) = \langle t_1(i, q_1 \circ h, q_2 \circ h), t_2(i, q_1 \circ h, q_2 \circ h)\rangle.$$

Let $f : W \to X$ be q_1. Thus for $v = \sup_i h$ we have

$$P(f(v)),$$

$$(\forall u : B_i)\, R_{i,u}(f(h(u)), f(\sup_i h)),$$

which was to be proven. □

8 Set-representability: general case

Theorem 8.1 *For any $S \in \mathbf{DO}$ its completion $\bar{S}$ can be represented by a set.*

Proof. Let $<$ be the order on S. By the propositions-as-types principle $(x < y)$ is the type of proof-objects for $x < y$. Form the W-type

$$W = (W(x,y) \in S \times S)\,(x < y).$$

Assume now that V is a regular universe that includes W, S, $T = \{1,2\}$ and encloses the relations $=_T$, $=_S$ and $<_S$. Let $\mathcal{R}(S)$ be the regular power set based on this universe. Denote by S^* the subset of $\bar{S}$ consisting of (L,U) such that $L = L'$ and $U = U'$ (extensionally) for some $L', U' \in \mathcal{R}(S)$. We claim that S^* is the same as $\bar{S}$.

Let $(L,U) \in \bar{S}$. Suppose that $x_0 \in L$ and $y_0 \in U$. We use well-founded dependent choice to construct the required (L', U'). We need to define the two predicates P and R. Let (A,B) vary over pairs in $\mathcal{R}(S) \times \mathcal{R}(S)$:

> $P(A,B)$ means $L_{x_0} \subseteq A \subseteq L$, $U_{y_0} \subseteq B \subseteq U$ and that (A,B) is a cut (not necessarily located)
>
> $R_{(x,y),p}((A,B),(A',B'))$ means $A \subseteq A'$, $B \subseteq B'$ and that
>
> $$L_x \subseteq A' \text{ or } U_y \subseteq B'.$$
>
> Here p is a proof-object for $(x < y)$.

We verify the prerequisites for the choice principle: Let $x, y \in S$ and suppose that $g = \langle g_1, g_2 \rangle : (x < y) \to \mathcal{R}(S) \times \mathcal{R}(S)$ is such that $P(g(p))$ for each $p : (x < y)$. Form the subsets

$$C = L_{x_0} \cup \bigcup_{p:(x<y)} g_1(p), \quad D = U_{y_0} \cup \bigcup_{p:(x<y)} g_2(p).$$

Furthermore, by the openness properties (L2) and (U2) we have

$$(\forall p : (x < y))\, \exists z\, \exists n\, [x < z \,\&\, z \in L \,\&\, n = 1 \text{ or } z < y \,\&\, z \in U \,\&\, n = 2].$$

Ordinary type-theoretic choice gives $h = \langle h_1, h_2 \rangle : (x < y) \to S \times \{1,2\}$ such that for all $p : (x < y)$

$$h_1(p) \in L \,\&\, x < h_1(p) \,\&\, h_2(p) = 1 \text{ or } h_1(p) \in U \,\&\, h_1(p) < y \,\&\, h_2(p) = 2.$$

Then put

$$C' = C \cup \bigcup_{p:(x<y)} \bigcup_{q:(h_2(p)=1)} L_{h_1(p)}$$

and

$$D' = D \cup \bigcup_{p:(x<y)} \bigcup_{q:(h_2(p)=2)} U_{h_1(p)}$$

Now a union of lower (upper) cuts becomes a lower (upper) cut. Clearly $L_{x_0} \subseteq C' \subseteq L$ and $U_{y_0} \subseteq D' \subseteq U$. Thus $P(C', D')$ holds. Moreover, for $p : (x < y)$, $g_1(p) \subseteq C \subseteq C'$ and $g_2(p) \subseteq D \subseteq D'$. Then $h_2(p)$ can take one of the values 1 or 2. If it is 1, then $L_x \subseteq L_{h_1(p)} \subseteq C'$. In case it is 2, then $U_y \subseteq U_{h_1(p)} \subseteq D'$.

Thus we have established

$$R_{(x,y),p}(g(p), (C', D')),$$

for any $p : (x < y)$, so Theorem 7.2 is applicable. It gives us $f : W \to \mathcal{R}(S) \times \mathcal{R}(S)$ such that

$$(\forall u \in W)\, P(fu)$$

and

$$(\forall x, y \in S)(\forall g : (x < y) \to W)(\forall p : (x < y))\, R_{(x,y),p}(f(g(p)), f(\sup_{(x,y)} g)).$$

Write $f = \langle f_1, f_2 \rangle$. Let

$$L^* = \bigcup_{u:W} f_1(u) \qquad\qquad U^* = \bigcup_{u:W} f_2(u).$$

Each of these belong to $\mathcal{R}(S)$ since W belongs to the universe V. We have clearly $L^* \subseteq L$ and $U^* \subseteq U$ and that (L^*, U^*) is a cut. We show that indeed $L \subseteq L^*$ ($U \subseteq U^*$ follows by a similar argument). Let $x \in L$. By (L2) we may pick two more elements in L such that $x < x' < x''$. Since $x_0 < y_0$, the type $(y_0 < x_0)$ must be empty, and so there is some $w_0 \in W$. Let $g : (x' < x'') \to W$ be a function which is constant w_0. Take $w_1 = \sup_{(x',x'')} g$. For $p : (x' < x'')$ we have

$$R_{(x',x''),p}(f(g(p)), f(w_1)),$$

but this entails $L_{x'} \subseteq f_1(w_1)$ or $U_{x''} \subseteq f_2(w_1)$. Suppose that the latter is the case: $U_{x''} \subseteq f_2(w_1) \subseteq U^*$. Take $x''' \in L$ with $x'' < x'''$, and thereby $x''' \in U^* \subseteq U$, which is impossible. Hence we must have $L_{x'} \subseteq f_1(w_1)$, and so $x \in f_1(w_1) \subseteq L^*$. This proves $L \subseteq L^*$ and indeed $L = L^*$. The proof of $U = U^*$ is similar. □

References

[1] P. Aczel (1986). The type-theoretic interpretation of constructive set theory: inductive definitions. In: R.B. Marcus *et al.* (eds.), *Logic, Methodology and Philosophy of Science VII,* North-Holland, Amsterdam.

[2] P. Aczel and M. Rathjen (2001). *Notes on Constructive Set Theory.* Institut Mittag-Leffler Preprint.

[3] E. Bishop and D.S. Bridges (1985). *Constructive Analysis.* Springer.

[4] H.G. Dales and W.H. Woodin (1996). *Super-Real Fields.* Oxford University Press.

[5] P.T. Johnstone (1982). *Stone Spaces.* Cambridge University Press.

[6] A. Joyal and G.E. Reyes (1986). Separably real closed fields. *Journal of Pure and Applied Algebra* 43(1986), 271 – 279.

[7] H. Lombardi and M.-F. Roy (1991). Elementary constructive theory of ordered fields. In: T. Mora and C. Traverso (eds.) *Effective Methods in Algebraic Geometry.* Birkhäuser.

[8] P. Martin-Löf (1984). *Intuitionistic Type Theory.* Bibliopolis, Naples.

[9] S. Mac Lane and I. Moerdijk (1992). *Sheaves in Geometry and Logic.* Springer.

[10] H.M. Mac Neille (1937). Partially ordered sets. *Transactions of the American Mathematical Society,* vol. 42, 416 – 460.

[11] M. Mines, F. Richman and W. Ruitenburg (1988). *A Course in Constructive Algebra,* Springer.

[12] S. Negri (1999). Sequent calculus proof theory of intuitionistic apartness and order relations. *Archive for Mathematical Logic* 38(1999), 521 – 547.

[13] E. Palmgren (1998). On universes in type theory. In: G. Sambin and J. Smith (eds.) *Twenty-Five Years of Constructive Type Theory.* Oxford Logic Guides, Oxford University Press, pp. 191 – 204.

[14] E. Palmgren (2002). An intuitionistic axiomatisation of real closed fields. *Mathematical Logic Quarterly* 48(2002), 297 – 299.

[15] F. Richman (1997). Generalized real numbers in constructive mathematics. *Indagationes Mathematicae* N.S 9(4).

[16] D.S. Scott (1969). On completing ordered fields. In: (W.A.J. Luxemburg ed.) *Applications of model theory to algebra, analysis and probability,* Holt, Reinhart and Winston, New York.

[17] S.G. Simpson (1999). *Subsystems of Second Order Arithmetic.* Springer.

[18] H. Weyl (1994). *The Continuum. A Critical Examination of the Foundations of Analysis.* Dover Publications.

Erik Palmgren
Department of Mathematics, Uppsala University
PO Box 480, SE-751 06 Uppsala, Sweden
E-mail: palmgren@math.uu.se
WWW: www.math.uu.se/~palmgren