Formalizing Results on Directed Sets in Isabelle/HOL (Proof Pearl)

Akihisa Yamada
National Institute of Advanced Industrial Science and Technology, Tokyo, Japan

Jérémy Dubut
National Institute of Advanced Industrial Science and Technology, Tokyo, Japan

Abstract

Directed sets are of fundamental interest in domain theory and topology. In this paper, we formalize some results on directed sets in Isabelle/HOL, most notably: under the axiom of choice, a poset has a supremum for every directed set if and only if it does so for every chain; and a function between such posets preserves suprema of directed sets if and only if it preserves suprema of chains. The known pen-and-paper proofs of these results crucially use uncountable transfinite sequences, which are not directly implementable in Isabelle/HOL. We show how to emulate such proofs by utilizing Isabelle/HOL's ordinal and cardinal library. Thanks to the formalization, we relax some conditions for the above results.

2012 ACM Subject Classification Theory of computation → Automated reasoning; Theory of computation → Denotational semantics

Keywords and phrases Directed Sets, Completeness, Scott Continuous Functions, Ordinals, Isabelle/HOL

Digital Object Identifier 10.4230/LIPIcs.ITP.2023.34

Funding This work was supported by JST, CREST Grant Number JPMJCR22M1, Japan.

1 Introduction

A *directed set* is a set D equipped with a binary relation $\sqsubseteq$ such that any finite subset $X \subseteq D$ has an upper bound in D with respect to $\sqsubseteq$. The property is often equivalently stated that D is non-empty and any two elements $x, y \in D$ have a bound in D, assuming that $\sqsubseteq$ is transitive (as in posets).

Directed sets find uses in various fields of mathematics and computer science. In topology (see for example the textbook [8]), directed sets are used to generalize the set of natural numbers: sequences $\mathbb{N} \to A$ are generalized to *nets* $D \to A$, where D is an arbitrary directed set. For example, the usual result on metric spaces that continuous functions are precisely functions that preserve limits of sequences can be generalized in general topological spaces as: the continuous functions are precisely functions that preserve limits of nets. In domain theory [1], key ingredients are *directed-complete posets*, where every directed subset has a supremum in the poset, and *Scott-continuous functions* between posets, that is, functions that preserve suprema of directed sets. Thanks to their fixed-point properties (which we have formalized in Isabelle/HOL in a previous work [6]), directed-complete posets naturally appear in denotational semantics of languages with loops or fixed-point operators (see for example Scott domains [13, 15]). Directed sets also appear in reachability and coverability analyses of transition systems through the notion of ideals, that is, downward-closed directed sets. They allow effective representations of objects, making forward and backward analysis of well-structured transition systems – such as Petri nets – possible (see e.g., [7]).

Apparently milder generalizations of natural numbers are chains (totally ordered sets) or even well-ordered sets. In the mathematics literature, the following results are known (assuming the axiom of choice):

▶ **Theorem 1** ([5]). *A poset is directed-complete if (and only if) it has a supremum for every non-empty well-ordered subset.*

▶ **Theorem 2** ([10]). *Let f be a function between posets, each of which has a supremum for every non-empty chain. If f preserves suprema of non-empty chains, then it is Scott-continuous.*

The pen-and-paper proofs of these results use induction on cardinality, where the finite case is merely the base case. The core of the proof is a technical result called Iwamura's Lemma [9], where the countable case is merely an easy case, and the main part heavily uses transfinite sequences indexed by uncountable ordinals.

In this paper, we formalize these results in the proof assistant Isabelle/HOL [11]. We extensively use the existing library for ordinals and cardinals in Isabelle/HOL [4], but we needed some delicate work in emulating the pen-and-paper proofs. In Isabelle/HOL, or any proof assistant based on higher-order logic (HOL), it is not possible to have a datatype for arbitrarily large ordinals; hence, it is not possible to directly formalize transfinite sequences. We show how to emulate transfinite sequences using the ordinal and cardinal library [4]. As far as the authors know, our work is the first to mechanize the proof of Theorems 1 and 2, as well as Iwamura's Lemma. We prove the two theorems for quasi-ordered sets, relaxing antisymmetry, and strengthen Theorem 2 so that chains are replaced by well-ordered sets and conditions on the codomain are completely dropped.

Related Work

Systems based on Zermelo-Fraenkel set theory, such as Mizar [2, 3] and Isabelle/ZF [12], have more direct support for ordinals and cardinals and should pose less challenge in mechanizing the above results. Nevertheless, a part of our contribution is in demonstrating that the power of (Isabelle/)HOL is strong enough to deal with uncountable transfinite sequences.

Except for the extra care for transfinite sequences, our proof of Iwamura's Lemma is largely based on the original proof from [9]. Markowsky presented a proof of Theorem 1 using Iwamura's Lemma [10, Corollary 1]. While he took a minimal-counterexample approach, we take a more constructive approach to build a well-ordered set of suprema. This construction was crucial to be reused in the proof of Theorem 2, which Markowsky claimed without a proof [10]. Another proof of Theorem 1 can be found in [5], without using Iwamura's Lemma, but still crucially using transfinite sequences.

Outline

The paper is organized as follows. In Section 2, we recall some basic concepts of order theory, ordinals, and cardinals, as well as their prior formalizations [4, 6]. In Section 3, we tackle the main formalization work of Iwamura's Lemma. The axiom of choice plays two crucial roles in the proof: first to obtain a well-ordering of a given set, and then to pick an upper bound for every finite subset. Finally, we use induction on directed sets – enabled by Iwamura's Lemma – to prove the equivalence between directed-completeness and well-completeness (Section 4), and the equivalence between Scott-continuity and preservation of suprema of chains (Section 5).

The formalization is available in the development version of the Archive of Formal Proofs as entry `Directed_Sets`, consisting of 726 lines of Isabelle code in total. The work also involves refactoring of our previous AFP entry `Complete_Non_Orders`[1] for reformulating continuity, completeness, well-foundedness and directed sets. The most changes are found in the new files `Continuity.thy` and `Directedness.thy` (427 lines).

2 Preliminaries

We assume some familiarity with Isabelle/HOL and use its notations also in mathematical formulas in the paper. We refer interested readers to the textbook [11] for more detail. Logical implication is denoted by $\Longrightarrow$ or $\longrightarrow$. We use *meta-equality* $\equiv$ to introduce definitions and abbreviations. By $X :: \textit{'a set}$ we denote a set X whose elements are of type $\textit{'a}$, and $R :: \textit{'a} \Rightarrow \textit{'a} \Rightarrow \textit{bool}$ is a binary predicate defined over $\textit{'a}$. Type annotations "$::$ _" are omitted unless necessary. The application of a function f to an element x is written $f\ x$, and the image of a set X under f is f ‘ X. The power set of X is denoted by $\textit{Pow}\ X$.

2.1 Binary Relations

In our previous Isabelle/HOL formalization on binary relations [6], some notations and properties of relations are defined as *locales*. Another approach is to use Isabelle's *type class* mechanism, which fixes a relation $\le$ for each type so that one do not have to specify the relation of concern as a parameter. The drawback of the class-based approach is that one must use this relation $\le$, which is too restrictive in the current development where we want to use *some* well-ordering of a given set.

To illustrate the use of locales, we revisit some definitions we need for the current paper. By *related set* we mean a set A with a binary relation (predicate) *less_eq* defined on A, denoted by infix symbol $\sqsubseteq$. In Isabelle:

```
locale related_set =
  fixes A :: 'a set and less_eq :: 'a ⇒ 'a ⇒ bool (infix ⊑ 50)
```

Then *reflexivity* and *transitivity* are defined as locales by making corresponding assumptions as follows:

```
locale reflexive = related_set + assumes x ∈ A ⟹ x ⊑ x
```

```
locale transitive = related_set +
  assumes x ⊑ y ⟹ y ⊑ z ⟹ x ∈ A ⟹ y ∈ A ⟹ z ∈ A ⟹ x ⊑ z
```

Then *quasi-ordered sets* are defined as the combination of reflexivity and transitivity:

```
locale quasi_ordered_set = reflexive + transitive
```

In this paper, we may use terminologies assuming that the right side of $\sqsubseteq$ is "greater", and use $\sqsupseteq$ to denote the dual of $\sqsubseteq$, though the notation is not always available in the actual Isabelle code. An (upper) *bound* of a set X is formalized by

```
definition bound X (⊑) b ≡ ∀x ∈ X. x ⊑ b for r (infix ⊑ 50)
```

[1] `https://www.isa-afp.org/entries/Complete_Non_Orders.html`

Dually, *bound* X $(\sqsupseteq)$ b specifies a lower bound. A *greatest (extreme)* element in X is a bound which is also in X:

definition *extreme* X $(\sqsubseteq)$ $e \equiv e \in X \wedge (\forall x \in X.\ x \sqsubseteq e)$ **for** r (**infix** $\sqsubseteq$ *50*)

Dually, *extreme* X $(\sqsupseteq)$ e specifies a least element. The following generalization of well-ordered sets frequently appears in this paper:

locale *well_related_set* = *related_set* +
  assumes $X \subseteq A \Longrightarrow X \neq \{\} \Longrightarrow \exists e.$ *extreme* X $(\sqsupseteq)$ e

that is, a set A together with a relation $\sqsubseteq$ such that every non-empty subset of A has a least element for $\sqsubseteq$. It can be also rephrased as the well-foundedness of the negation of $\sqsubseteq$. A well-related set is necessarily reflexive, which can be formalized by a sublocale statement:

sublocale *well_related_set* $\subseteq$ *reflexive*...

A *well-ordered* set is a well-related set where $\sqsubseteq$ is also antisymmetric (or equivalently a total order). A *pre-well-ordered* set is a well-related set which is also a quasi-order.

2.2 Ordinals and Cardinality Library

Here we briefly recap the ordinal and cardinality library [4] of Isabelle/HOL.

The library chooses the *set-oriented* formulation of relations: type *'a rel* is a shorthand for (*'a* × *'a*) *set*, and proposition $(x,y) \in R$ denotes that x and y are in relation R :: *'a rel*.

An *order embedding* of a relation $(A, \sqsubseteq)$ into $(B, \trianglelefteq)$ is a function $f : A \to B$ such that $x \sqsubseteq y \iff f\ x \trianglelefteq f\ y$. The polymorphic relation $\leq o$ :: *'a rel* ⇒ *'b rel* ⇒ *bool* over binary relations is defined by $R \leq o\ S$ if and only if there is an order embedding from R to S. Two relations R :: *'a rel* and S :: *'b rel* are *order isomorphic*, $R =o\ S$, if $R \leq o\ S$ and $S \leq o\ R$.

One of the important results from the ordinal library is that $<o$, the asymmetric part of $\leq o$ (defined by $x <o\ y \equiv x \leq o\ y \wedge \neg\ y \leq o\ x$), seen as a relation over the same type, is well-founded. In fact, $\leq o$ forms a pre-well-order.

Conceptually, an ordinal can be seen as the equivalence class of well-orderings which are order isomorphic to each other. In Isabelle/HOL, or in any other HOL-based systems, it is not possible to have a set collecting well-orderings of different types. It is hence not possible to have a type for general ordinals in Isabelle/HOL. Instead, any well-ordering of any type is used to represent an ordinal in [4].

The *cardinality* of a set X is the least ordinal that is bijective with X. In Isabelle/HOL, $|X|$ :: *'a rel* is defined as *one of the* well-orderings on X :: *'a set* which are least with respect to $\leq o$; there are well-orderings on X thanks to the well-order theorem (which is in turn due to the axiom of choice), and there are least ones since $\leq o$ is a pre-well-order.

3 Iwamura's Lemma

The main idea for proving Theorem 1 is, given a directed set D, to construct a well-ordered set whose supremum (which exists by assumption) is also a supremum for D. The difficulty is that the usual methods to construct a well-ordered set, such as Zorn's lemma, fail to achieve this goal. The crucial idea brought by Markowsky [10, Corollary 1] is that this well-ordered set can be obtained by a transfinite induction on the cardinality of the directed set, using Iwamura's Lemma [9]. Concretely, Iwamura's Lemma states the following:

▶ **Theorem 3.** *Let $(A, \sqsubseteq)$ be a reflexive directed set. If A is infinite, then there exists a transfinite sequence $\{I_\alpha\}_{\alpha<|A|}$ of subsets of A that satisfies the following four conditions:*

- *directedness: I_α is directed for all $\alpha < |A|$,*
- *cardinality: $|I_\alpha| < |A|$ for all $\alpha < |A|$,*
- *monotonicity: $I_\alpha \subseteq I_\beta$ whenever $\alpha \leq \beta < |A|$, and*
- *range: $\bigcup_{\alpha<|A|} I_\alpha = A$.*

Note that, if we drop directedness, then the statement is equivalent to the well-ordering theorem. The main point of Iwamura's Lemma is that one can extend any subset of a directed set into a directed one without changing the cardinality.

As in the original statement, $\sqsubseteq$ need not be transitive. Hence, directedness is formalized as follows:

```
definition directed_set A (⊑) ≡ ∀X ⊆ A. finite X ⟶ (∃b ∈ A. bound X (⊑) b)
  for less_eq (infix ⊑ 50)
```

As the proof involves a number of (inductive) definitions, we build a **locale** for collecting those definitions and lemmas.

```
locale Iwamura_proof = related_set +
  assumes dir: directed_set A (⊑)
begin
```

Inside this locale, a related set $(A, \sqsubseteq)$ is fixed and assumed to be directed. The proof starts with declaring, using the axiom of choice, a function f that chooses a bound $f\ X \in A$ for every finite subset $X \subseteq A$. This function can be formalized using the *SOME* construction:

```
definition f where f X ≡ SOME x. x ∈ A ∧ bound X (⊑) x
```

In Isabelle, *SOME* $x.\ \phi\ x$ takes *some* value x that satisfies the condition $\phi\ x$, if such a value exists; otherwise it takes an unspecified value. As we assume that any finite subset $X \subseteq A$ has an upper bound in A, we can prove that f satisfies the following specification:

```
lemma assumes X ⊆ A and finite X
  shows f X ∈ A and bound X (⊑) (f X) ...
```

After obtaining this f, the proof constructs $\{I_\alpha\}_{\alpha<|A|}$ depending crucially on whether A is countably or uncountably infinite.

3.1 Uncountable Case

We start with the core case, where A is uncountable. The original proof goes as follows: Thanks to the well-order theorem, one can have a sequence $\{A_\alpha\}_{\alpha<|A|}$ of subsets of A that satisfies the following three conditions:

- cardinality: $|A_\alpha| < |A|$ for every $\alpha < |A|$,
- monotonicity: $A_\alpha \subseteq A_\beta$ whenever $\alpha \leq \beta < |A|$, and
- range: $A = \bigcup_{\alpha<|A|} A_\alpha$.

Then it is shown that any subset of A, in particular A_α, can be monotonically extended to a directed one I_α, such that $|I_\alpha| \leq |A_\alpha| \cdot \aleph_0$. Since $|A_\alpha| < |A|$ and $|A|$ is uncountable, it follows that $|I_\alpha| < |A|$.

In order to formalize the above argument in Isabelle/HOL, one of the challenges is that we do not have a datatype for ordinals (that works for arbitrary types of A), and thus one cannot formalize transfinite sequences as functions from ordinals.

3.1.1 Formalizing Transfinite Sequences

As we cannot formalize transfinite sequences directly, we take the following approach: We just use A as the index set, and instead of the ordering on ordinals, we take the well-order $(\preceq_A)$ that is chosen by the cardinality library to denote $|A|$, as follows:

definition ... **where** $(\preceq_A)\ x\ y \equiv (x,y) \in |A|$

Recall that $|A|$ is defined as *one of the* well-orders on A which are least with respect to $\leq o$, in a set-oriented formulation of relations. We also introduce infix notations for $\preceq_A$ and its asymmetric part $\prec_A$ as follows:

abbreviation ... **where** $x \preceq_A\ y \equiv (\preceq_A)\ x\ y$
abbreviation ... **where** $x \prec_A\ y \equiv \mathit{asympartp}\ (\preceq_A)\ x\ y$

Now we show that $A_\prec : A \rightarrow \mathit{Pow}\ A$ serves the purpose of $\{A_\alpha\}_{\alpha<|A|}$ above, where

definition ... **where** $A_\prec\ a \equiv \{x \in A.\ x \prec_A\ a\}$

First, we prove the counterpart of the cardinality condition $|A_\alpha| < |A|$.

lemma *Pre_card*: **assumes** $a \in A$ **shows** $|A_\prec\ a| <o\ |A|$

Proof. On pen and paper, one would first well-order A as $\{a_\alpha\}_{\alpha<|A|}$ and chose $A_\alpha = \{a_\beta\}_{\beta<\alpha}$; then $|A_\alpha| < |A|$ would look obvious. Note that there is an implicit use of the fact that $|A|$ is least; otherwise $\alpha < |A|$ and $|\{a_\beta\}_{\beta<\alpha}| = |A|$ is possible.

In the formalization, we derive this fact by connecting to the cardinality library. In fact, $A_\prec\ a$ corresponds precisely to *underS* $|A|$ a in terms of the library. Then lemma *card_of_underS* from the library easily concludes the lemma. ◀

Second, the monotonicity condition, $A_\alpha \subseteq A_\beta$ whenever $\alpha \leq \beta$, is easy:

lemma *Pre_mono*: $\mathit{monotone\_on}\ A\ (\preceq_A)\ (\subseteq)\ (A_\prec)$ ...

The final property we need is $\bigcup_{\alpha<|A|} A_\alpha = A$. This is not as easy as the previous two properties; note that it cannot hold for finite A. We first prove that if the well-ordering $(A, \preceq_A)$ has a greatest element, then A must be finite:

lemma *extreme_imp_finite*: **assumes** $\mathit{extreme}\ A\ (\preceq_A)\ e$ **shows** $\mathit{finite}\ A$

Proof. Since e is greatest in A, we have $A_\prec\ e = A - \{e\}$. On the other hand, $|A - \{e\}| =o\ |A|$ if A is infinite. This cannot happen due to Lemma *Pre_card*. ◀

This allows us to prove the desired property:

lemma *infinite_imp_Un_Pre*: **assumes** $\mathit{infinite}\ A$ **shows** $\bigcup(A_\prec\ `\ A) = A$

Proof. The inclusion $A_\prec\ `\ A \subseteq A$ is obvious. For the other direction, consider $a \in A$. Due to Lemma *extreme_imp_finite*, $a$ cannot be the greatest in $A$ with respect to $\preceq_A$. So there exists some $b \in A$ such that $a \prec_A b$. Hence $a \in A_\prec b \subseteq \bigcup(A_\prec\ `\ A)$. ◀

3.1.2 Expanding Infinite Sets into Directed Sets

Actually, the main part of the proof of Iwamura's Lemma is about monotonically expanding an infinite subset (in particular A_α) of A into a directed one, without changing the cardinality. To this end, Iwamura's original proof introduces a function $F : \mathit{Pow}\ A \to \mathit{Pow}\ A$ that expands a set with upper bounds of *all finite subsets*. This approach is different from Markowsky's reproof (based on [14]) which uses nested transfinite induction to extend a set one element after another.

definition F **where** $F\ X \equiv X \cup f\ `\ \mathit{Fpow}\ X$

Here, $\mathit{Fpow}\ X$ is an Isabelle/HOL notation for the set of finite subsets of X. Hence, for any finite subset Y of X, there is an upper bound $f\ Y$ in $F\ X$. We take the ω-iteration of the monotone function F, namely:

definition Flim (F^ω) **where** $F^\omega\ X \equiv \bigcup i.\ F^i\ X$

We prove that $\{F^\omega\ (A_\prec\ a)\}_{a \in A}$ serves the purpose of $\{I_\alpha\}_{\alpha<|A|}$ when A is uncountable.

Directedness condition is satisfied regardless of uncountability. More generally, $F^\omega\ X$ is directed for every $X \subseteq A$.

lemma *Flim_directed*: **assumes** $X \subseteq A$ **shows** $\mathit{directed\_set}\ (F^\omega\ X)\ (\sqsubseteq)$

Proof. Take an arbitrary finite subset $Y \subseteq F^\omega\ X$. Since Y is finite, we inductively obtain $i \in \mathbb{N}$ such that $Y \subseteq F^i\ X$, i.e., $Y \in \mathit{Fpow}\ (F^i\ X)$. Hence we find an upper bound $f\ Y \in F^{i+1}\ X \subseteq F^\omega\ X$. ◀

The cardinality condition holds when $|A|$ is uncountable. Using the cardinality library, (un)countability is stated using the term *natLeq*, which denotes the well-order $(\mathbb{N}, \leq)$, i.e., the ordinal ω or cardinality $\aleph_0$.

lemma *card_uncountable*:
assumes $a \in A$ **and** $\mathit{natLeq} <o |A|$ **shows** $|F^\omega\ (A_\prec\ a)| <o |A|$

Proof. Let $X = A_\prec\ a$. The proof proceeds by case distinction on whether X is finite or not. If X is finite, then every $F^i\ X$ is finite and thus $F^\omega\ X$ is at most countable. Note that $F^\omega\ X$ is not necessarily finite. Nevertheless, since A is assumed to be uncountable, we conclude $|F^\omega\ X| <o |A|$.

Now we show that if X is infinite, then $|F^\omega\ X| =o |X|$. This will conclude the claim as $|X| <o |A|$ due to Lemma *Pre_card*. First, we have $|F\ X| =o |X|$. This is easy using the library fact *card_of_Fpow_infinite*: $\mathit{infinite}\ X \Longrightarrow |\mathit{Fpow}\ X| =o |X|$. Then this property is carried over to $|F^i\ X| =o |X|$ for every $i \in \mathbb{N}$, proved by an easy induction.

Now, the following fact (*card_of_UNION_ordLeq_infinite*) is available in the library:

$$\mathit{infinite}\ B \Longrightarrow |I| \leq o\ |B| \Longrightarrow \forall i{\in}I.\ |A\ i| \leq o\ |B| \Longrightarrow |\bigcup (A\ `\ I)| \leq o\ |B|$$

Since X is infinite, we know $|\mathbb{N}| \leq o\ |X|$, and we have proved that $|F^i\ X| \leq o\ |X|$ for all $i \in \mathbb{N}$. Thus, by taking $I = \mathbb{N}$, $A\ i = F^i\ X$, and $B = X$, we conclude $|F^\omega\ X| \leq o\ |X| <o |A|$. Since $X \subseteq F^\omega\ X$, we also have $|F^\omega\ X| =o |X|$. ◀

Monotonicity is due to that of the building components:

lemma *mono_uncountable*: $\mathit{monotone\_on}\ D\ (\preceq_A)\ (\subseteq)\ (F^\omega \circ A_\prec)$

Proof. As $A_{\prec}$ is monotone (Lemma *Pre_mono*) and monotonicity is preserved by composition, it suffices to show that F^{ω} is monotone. It is easy to see that F is monotone. Then so is F^{i} for every $i \in \mathbb{N}$, as i-th fold of a monotone function is still monotone. Finally, we conclude the monotonicity of F^{ω} by the following more general statement:

lemma *Sup_funpow_mono*:
  fixes f :: $'a :: complete\_lattice \Rightarrow\ 'a$
  assumes $mono\ f$ **shows** $mono\ (\bigsqcup i.\ f^{i})$ ...

which is proved easily. ◀

Finally, for the range condition, the infiniteness of A is sufficient.

lemma *range_uncountable*: **assumes** $infinite\ A$ **shows** $\bigcup((F^{\omega} \circ A_{\prec})\ `\ A) = A$

Proof. The ($\subseteq$)-direction is obvious. For the ($\supseteq$)-direction, take $a \in A$. As A is infinite, by **lemma** *extreme_imp_finite*, we obtain $b \in A$ such that $a \in A_{\prec}\ b$. By definition, $X \subseteq F\ X$. By induction, $X \subseteq F^{\omega}\ X$. We conclude $a \in A_{\prec}\ b \subseteq F^{\omega}\ (A_{\prec}\ b) \subseteq \bigcup((F^{\omega} \circ A_{\prec})\ `\ A$. ◀

3.2 Countable Case

Next we consider the case where A is countably infinite. We make the assumption by making a subcontext within the locale *Iwamura_proof*:

context
  assumes *countable*: $|A| =o\ natLeq$
begin

The assumption above means that there exists an order-isomorphism between $(\mathbb{N}, \leq)$ and $(A, \preceq_A)$. In Isabelle/HOL, we can obtain the isomorphism as follows:

definition *seq* :: $nat \Rightarrow\ 'a$ **where** $seq \equiv SOME\ g.\ iso\ natLeq\ |A|\ g$

lemma *seq_iso*: $iso\ natLeq\ |A|\ seq$ ...

The definition of the predicate *iso* is given in the ordinal library. For our use, it suffices to know a few consequences of *seq_iso*. Most importantly, *seq* is bijective between $\mathbb{N}$ and A:

lemma *seq_bij_betw*: $bij\_betw\ seq\ UNIV\ A$

This means that A has been indexed by $\mathbb{N}$: $A = \{seq\ 0,\ seq\ 1,\ seq\ 2,\ \ldots\}$. We turn the sequence into a sequence of directed subsets of A: $Seq\ 0 \subseteq Seq\ 1 \subseteq Seq\ 2 \subseteq \ldots \subseteq A$.

fun *Seq* :: $nat \Rightarrow\ 'a\ set$ **where**
  $Seq\ 0 = \{f\ \{\}\}$
| $Seq\ (Suc\ n) = Seq\ n \cup \{seq\ n,\ f\ (Seq\ n \cup \{seq\ n\})\}$

As *Seq* is a plain inductive function, it is an easy exercise to formally prove that $\{Seq\ n\}_{n \in \mathbb{N}}$ satisfies the four requirements of Iwamura's Lemma. A more interesting formalization work is in combining with the uncountable case. In Section 3.1, we took $F^{\omega} \circ A_{\prec}$ as the candidate of I, which is of type $'a \Rightarrow\ 'a\ set$. On the other hand, *Seq* is of type $nat \Rightarrow\ 'a\ set$. To match the types, we use the inverse seq^{-1} :: $'a \Rightarrow nat$ ($inv\ seq$ in the standard Isabelle notation) of the isomorphism *seq*. We define the final I as follows:

definition I **where** $I \equiv$ ***if*** $|A| =o\ \mathit{natLeq}$ ***then*** $\mathit{Seq} \circ \mathit{seq}^{-1}$ ***else*** $F^{\omega} \circ A_{\prec}$

Now we close the locale *Iwamura_proof* and state the final result in the global scope.

theorem (**in** *reflexive*) *Iwamura*:
  assumes $\mathit{directed\_set}\ A\ (\sqsubseteq)$ **and** $\mathit{infinite}\ A$
  shows $\exists I.\ (\forall a \in A.\ \mathit{directed\_set}\ (I\ a)\ (\sqsubseteq) \wedge |I\ a| <o\ |A|\ ) \wedge$
    $\mathit{monotone\_on}\ A\ (\preceq_A)\ (\subseteq)\ I \wedge \bigcup(I`A) = A$

Proof. Inside the proof we reopen the proof locale:

  interpret *Iwamura_proof* ...

By this we obtain I defined above. We conclude by proving that I satisfies the requirements.

- $\mathit{directed\_set}\ (I\ a)\ (\sqsubseteq)$: The uncountable case is by *Flim_directed*. For the countable case, we show that $\mathit{Seq}\ n$ is directed for every $n \in \mathbb{N}$. Note that $\mathit{Seq}\ n$ can be written $X \cup \{f\ X\}$ for appropriate X. Then since $f\ X$ is an upper bound of X and $\sqsubseteq$ is reflexive, $f\ X$ serves as an upper bound of any (finite) subset of $X \cup \{f\ X\}$.
- $|I\ a| <o\ |A|$: The uncountable case is by *card_uncountable*. For countable case, we just prove that $\mathit{Seq}\ n$ is finite for any $n \in \mathbb{N}$, by easy induction.
- $\mathit{monotone\_on}\ A\ (\preceq_A)\ (\subseteq)\ I$: The uncountable case is by *mono_uncountable*. For the countable case, we need another consequence of lemma *seq_iso*:

  lemma *inv_seq_mono*: $\mathit{monotone\_on}\ A\ (\preceq_A)\ (\leq)\ (\mathit{seq}^{-1})$ ...

  We then combine with the monotonicity of *Seq*, which is easily proved by induction.
- $\bigcup(I\ `\ A) = A$: The uncountable case is by *range_uncountable*. For the countable case, we need to prove $\bigcup((\mathit{Seq} \circ \mathit{seq}^{-1})\ `\ A) = A$. The $(\subseteq)$-direction is obvious. For the other direction, take an arbitrary $a \in A$. We know $a = \mathit{seq}\ (\mathit{seq}^{-1}\ a) \in \mathit{Seq}\ n$ with $n = \mathit{Suc}\ (\mathit{seq}^{-1}\ a)$. On the other hand, $\mathit{seq}\ n \in A$. Hence $a \in \mathit{Seq}\ n = \mathit{Seq}\ (\mathit{seq}^{-1}\ (\mathit{seq}\ n)) \subseteq \bigcup(\mathit{Seq} \circ \mathit{seq}^{-1})\ `\ A$. ◀

4 Directed Completeness

Now we formalize Theorem 1: A quasi-ordered set has a supremum for every directed subset, if and only if it does so for every non-empty well-related subset. The statement is slightly generalized, so that the underlying order need not be antisymmetric.

The property that certain class of subsets have suprema is called *completeness*. We formalize completeness as follows:

definition ... **where**
  $\mathcal{C}\text{-}\mathit{complete}\ A\ (\sqsubseteq) \equiv \forall X \subseteq A.\ \mathcal{C}\ X\ (\sqsubseteq) \longrightarrow (\exists s.\ \mathit{extreme\_bound}\ A\ (\sqsubseteq)\ X\ s)$
  for *less_eq* (**infix** $\sqsubseteq$ *50*)

Using this notation, we can formalize Theorem 1 concisely as follows:

theorem (**in** *quasi_ordered_set*) *well_complete_iff_directed_complete*:
  $(\mathit{nonempty} \sqcap \mathit{well\_related\_set})\text{-}\mathit{complete}\ A\ (\sqsubseteq) \longleftrightarrow \mathit{directed\_set}\text{-}\mathit{complete}\ A\ (\sqsubseteq)$

where *nonempty* $A \equiv$ ***if*** $A = \{\}$ ***then*** $\bot$ ***else*** $\top$. For the ($\longleftarrow$)-direction we must prove that non-empty well-related sets are actually directed. Well-related sets clearly are *connex*, i.e., every two elements are comparable. Under transitivity this is sufficient for directedness, but we can actually prove a stronger statement without transitivity: every non-empty finite subset X of a well-related set A has a greatest element.

lemma (**in** *well_related_set*) *finite_sets_extremed*:
  assumes *finite* X **and** $X \neq \{\}$ **and** $X \subseteq A$
  shows *extremed* X $(\sqsubseteq)$

Proof. By induction on the number[2] of elements in the finite set X. As X is nonempty, by well-relatedness, it has a least element l. If $X - \{l\}$ is empty, then l is the greatest in $X = \{l\}$ by reflexivity. Otherwise, by induction hypothesis, $X - \{l\}$ has a greatest element e. As l is least in X and in particular $l \sqsubseteq e$, e is also greatest in X. ◀

For the ($\longrightarrow$)-direction, we prove the following elaborated statement:

lemma (**in** *quasi_ordered_set*) *directed_completeness_lemma*:
  assumes (*nonempty* $\sqcap$ *well_related_set*)*-complete* A $(\sqsubseteq)$
    and *directed_set* D $(\sqsubseteq)$ **and** $D \subseteq A$
  shows $\exists x.$ *extreme_bound* A $(\sqsubseteq)$ D x

Proof. We apply induction on the cardinality $|D|$ with respect to $<o$. To be more precise, we are given fresh D for which we must prove ϕ D, where ϕ X denotes

$$\mathit{directed\_set}\ X\ (\sqsubseteq) \Longrightarrow X \subseteq A \Longrightarrow \exists x.\ \mathit{extreme\_bound}\ A\ (\sqsubseteq)\ X\ x$$

assuming ϕ *D'* for any *D'* with $|D'| <o |D|$.

If D is finite, then D has an upper bound of itself, i.e., a greatest element, which serves also as a supremum. So suppose that D is infinite. For this D, we apply Iwamura's Lemma and obtain I as follows.

  obtain I **where** *monotone_on* D $(\preceq_D)$ $(\subseteq)$ I
    and $\forall a \in D.\ |I\ a| <o |D|$
    and $\forall a \in D.$ *directed_set* $(I\ a)$ $(\sqsubseteq)$
    and $\bigcup (I\ `\ D) = D$ ...

For every $d \in D$, since $|I\ d| <o |D|$, induction hypothesis ensures that $I\ d$ has a supremum in A. Thus, using the axiom of choice, we obtain a function s that picks a supremum for $I\ d$. Note that as we do not assume that $\sqsubseteq$ is antisymmetric, suprema are not unique so the axiom of unique choice cannot be used.

  obtain s **where** $d \in D \Longrightarrow$ *extreme_bound* A $(\sqsubseteq)$ $(I\ d)$ $(s\ d)$ **for** d ...

Next we show that $(s\ `\ D, \sqsubseteq)$ is well-related. To this end, we formalized the following fact: monotone image of a well-related set is well-related.

  lemma (**in** *well_related_set*) *monotone_image_well_related*:
    fixes *leB* (**infix** $\trianglelefteq$ *50*)
    assumes *monotone_on* A $(\sqsubseteq)$ $(\trianglelefteq)$ f **shows** *well_related_set* $(f\ `\ A)$ $(\trianglelefteq)$ ...

[2] In Isabelle, *card* X is used to denote the number of elements in X, assuming that X is finite. In contrast, $|X|$ is the cardinality in more general sense.

So now we need that s is monotone from $(D, \preceq_D)$ to $(A, \sqsubseteq)$. This follows as I is monotone from $(D, \preceq_D)$ to $(Pow\ D, \subseteq)$, and taking suprema is monotone from $(Pow\ D, \subseteq)$ to $(A, \sqsubseteq)$. This concludes that $(s\ `\ D, \sqsubseteq)$ is well-related. Since $D$ is infinite and thus non-empty, thanks to the completeness assumption we obtain a supremum $x$ of $s\ `\ D$. We conclude by showing that x is also a supremum of D.

To show that x is a bound of D, consider an arbitrary $d \in D$. Since $D = \bigcup\ (I\ `\ D)$, we obtain $d' \in D$ such that $d \in I\ d'$. As $s\ d'$ is a supremum of $I\ d'$, we know $d \sqsubseteq s\ d'$. Since $s\ d' \in s\ `\ D$ and x is a supremum of $s\ `\ D$, we have $s\ d' \sqsubseteq x$. By transitivity we conclude $d \sqsubseteq x$.

Finally, let b be another bound of D. For any $d \in D$, since $I\ d \subseteq D$, b is a bound of $I\ d$. Since $s\ d$ is least among the bounds of $I\ d$, we have $s\ d \sqsubseteq b$. This shows that b is a bound of $s\ `\ D$. Since $x$ is least among the bounds of $s\ `\ D$, we conclude $x \sqsubseteq b$. ◀

5 Scott-Continuity

The previous inductive proof can be strengthened to prove and generalize Theorem 2: A function that preserves suprema of well-related subsets also preserves suprema of directed subsets, if the domain has a supremum for every nonempty well-related sets. Markowsky claimed Theorem 2 [10, Corollary 3], saying briefly that it follows from Iwamura's Lemma and transfinite induction. We did not find it that obvious (at least for mechanization), and by completing the proof, we could slightly generalize Markowsky's claim. Now it works for quasi-ordered domain, relaxing antisymmetry; the codomain need not be complete in any class, or even transitivity or reflexivity are not necessary; and chains are refined to well-related sets.

Functions that preserve a particular class of suprema are called *continuous*. We formalize the notion in Isabelle as follows:

```
definition ... where
  𝒞-continuous A (⊑) B (⊴) f ≡ f ` A ⊆ B ∧
   (∀X s. 𝒞 X (⊑) ⟶ X ≠ {} ⟶ X ⊆ A ⟶
     extreme_bound A (⊑) X s ⟶ extreme_bound B (⊴) (f ` X) (f s))
  for leA (infix ⊑ 50) and leB (infix ⊴ 50)
```

A useful fact about continuous functions, is that, under a mild condition on the class $\mathcal{C}$ – namely, all pairs of related elements are in the class – every $\mathcal{C}$-continuous function is monotone:

```
lemma (in reflexive) continuous_imp_monotone_on:
  assumes 𝒞-continuous A (⊑) B (⊴) f and ∀i ∈ A. ∀ j ∈ A. i ⊑ j ⟶ 𝒞 {i,j} (⊑)
  shows monotone_on A (⊑) (⊴) f ...
```

This is the case for *well_related_set*-continuous functions.

The Isabelle statement of Theorem 2 then becomes:

```
theorem (in quasi_ordered_set)
  assumes (nonempty ⊓ well_related_set)-complete A (⊑)
  shows well_related_set-continuous A (⊑) B (⊴) f ⟷ directed_set-continuous A (⊑) B
(⊴) f
```

As before, the $(\longleftarrow)$-direction is obvious. For the $(\longrightarrow)$-direction, our strategy is to prove that f preserves the suprema of every directed set, at the same time we construct the suprema in the previous section. Precisely, into the statement of **lemma** *directed_completeness_lemma* we add the following claim:

$$\textbf{and}\ \textit{well\_related\_set-continuous}\ A\ (\sqsubseteq)\ B\ (\trianglelefteq)\ f \Longrightarrow$$
$$D \neq \{\} \Longrightarrow \textit{extreme\_bound}\ A\ (\sqsubseteq)\ D\ x \Longrightarrow \textit{extreme\_bound}\ B\ (\trianglelefteq)\ (f\ `\ D)\ (f\ x)$$

Proof. The claim is proved simultaneously with the previous statement by induction on $|D|$. Our new goal is to show, given a supremum x of D in $(A, \sqsubseteq)$, that $f\,x$ is a supremum of $f\ `\ D$ in $(B, \trianglelefteq)$.

By monotonicity, $f\,x$ is a bound of $f\ `\ D$, so we show that it is least of such. Recall that, in the previous section, a supremum of $D$ is obtained as a supremum of a well-related set $C$, where $C$ is a singleton set in the finite case, and is $s\ `\ D$ in the infinite case. Note that, as we do not assume antisymmetry, this supremum is not necessarily the supremum x we are given. Nevertheless, we know that x is also a supremum of C, thanks to the transitivity of $(A, \sqsubseteq)$. As f preserves suprema of well-related sets, we also know that $f\,x$ is a supremum of $f\ `\ C$ in $(B, \trianglelefteq)$. Hence, by showing that any bound $b$ of $f\ `\ D$ is also a bound of $f\ `\ C$, we can show $f\,x \trianglelefteq b$ and conclude the proof.

The finite case is obvious as $C \subseteq D$. Consider the infinite case: $C = s\ `\ D$. We know that $b$ is a bound of $f\ `\ I\ d$ for every $d \in D$, as $D = \bigcup\ (I\ `\ D)$. Recall that, in the previous section, $s\ d$ is an inductively obtained supremum of $I\ d$. With $|I\ d| <o\ |D|$, by induction hypothesis we know that $f\ (s\ d)$ is a supremum of $f\ `\ I\ d$. In particular $f\ (s\ d) \trianglelefteq b$, concluding that b is a bound of $f\ `\ s\ `\ D = f\ `\ C$. ◀

6 Conclusion

In this paper, we formalized some results for directed sets: Iwamura's Lemma to enable induction arguments on them; Cohn's theorem stating the equivalence between directed-completeness and well-completeness; and Markowski's corollary on Scott-continuity being equivalent to the preservation of suprema of well-related chains. The proofs involved some non-trivial formalization work on transfinite sequences that has been enabled by a careful management of locales and contexts, and Isabelle/HOL's libraries on cardinals and ordinals.

References

1 Samson Abramsky and Achim Jung. *Domain Theory*. Number III in Handbook of Logic in Computer Science. Oxford University Press, 1994.

2 Grzegorz Bancerek. The ordinal numbers. *Journal of Formalized Mathematics*, 1, 1989.

3 Grzegorz Bancerek and Piotr Rudnicki. A compendium of continuous lattices in MIZAR. *J. Autom. Reason.*, 29(3-4):189–224, 2002. doi:10.1023/A:1021966832558.

4 Jasmin Christian Blanchette, Andrei Popescu, and Dmitriy Traytel. Cardinals in Isabelle/HOL. In Gerwin Klein and Ruben Gamboa, editors, *Interactive Theorem Proving - 5th International Conference, ITP 2014, Held as Part of the Vienna Summer of Logic, VSL 2014, Vienna, Austria, July 14-17, 2014. Proceedings*, volume 8558 of *Lecture Notes in Computer Science*, pages 111–127. Springer, 2014. doi:10.1007/978-3-319-08970-6_8.

5 Paul M. Cohn. *Universal Algebra*. Harper & Row, 1965.

6 Jérémy Dubut and Akihisa Yamada. Fixed point theorems for non-transitive relations. *Log. Methods Comput. Sci.*, 18(1), 2022. doi:10.46298/lmcs-18(1:30)2022.

7 Alain Finkel and Jean Goubault-Larrecq. Forward Analysis for WSTS, Part I: Completions. In Susanne Albers and Jean-Yves Marion, editors, *26th International Symposium on Theoretical Aspects of Computer Science*, volume 3 of *Leibniz International Proceedings in Informatics*

(LIPIcs), pages 433–444, Dagstuhl, Germany, 2009. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik. doi:10.4230/LIPIcs.STACS.2009.1844.

8 Jean Goubault-Larrecq. *Non-Hausdorff Topology and Domain Theory: Selected Topics in Point-Set Topology*, volume 22 of *New Mathematical Monographs*. Cambridge University Press, 2013. doi:10.1017/CBO9781139524438.

9 Tsurane Iwamura. A lemma on directed sets. *Zenkoku Shijo Sugaku Danwakai*, 262:107–111, 1944. in Japanese.

10 George Markowsky. Chain-complete posets and directed sets with applications. *Algebra Universalis*, 6:53–68, 1976.

11 Tobias Nipkow, Markus Wenzel, and Lawrence C. Paulson. *Isabelle/HOL – A Proof Assistant for Higher-Order Logic*, volume 2283 of *LNCS*. Springer, 2002. doi:10.1007/3-540-45949-9.

12 Lawrence C. Paulson and Krzysztof Grabczewski. Mechanizing set theory. *J. Autom. Reason.*, 17(3):291–323, 1996. doi:10.1007/BF00283132.

13 Dana Scott. Outline of a Mathematical Theory of Computation. Technical Report PRG02, OUCL, 1970.

14 Lev Anatol'evich Skornyakov. *Complemented modular lattices and regular rings*. Oliver & Boyd, 1964.

15 Glynn Winskel. *The Formal Semantics of Programming Languages: An Introduction*. Foundations of Computing. The MIT Press, 1993.