On Induction for Diamond-Free Directed Complete Partial Orders

Ievgen Ivanov

Taras Shevchenko National University of Kyiv
ivanov.eugen@gmail.com

Abstract. A formulation of an induction principle for diamond-free directed complete partial orders is proposed. This principle may be useful for specification and verification of non-discrete systems using interactive proof assistant software.

Keywords: Formal methods, partial order, real induction, open induction.

1 Introduction

Inductive proofs and recursive definitions are very useful tools in software specification and verification. In particular, they are frequently used in formalizations of algorithms in proof assistants such as Isabelle and Coq. This leads to a question of whether certain analogous proof methods and corresponding definition methods may be useful in the case of specification and verification of cyber-physical systems, in particular, using proof assistants. Since in this case one is expected to deal with formalization of properties which involve continuous variables, investigation of generalized inductive proof methods and recursive definitions which use a continuous parameter is relevant.

Proof principles that allow one to prove a property of real numbers by an argument that is in some sense similar to mathematical induction may be called real or continuous induction principles [1–3]. An overview, literature references and applications related to this topic can be found in [1, 2].

Recently, real induction was used in differential equation invariance axiomatization [4, 5] which extends a logic (differential dynamic logic [4]) intended for verification of hybrid systems (which may be used as mathematical models of behaviors of cyber-physical systems).

The real induction principle referenced in [4] is given in [2, Theorem 2]. It states that a subset $S \subseteq [a, b]$ ($a < b$ are real numbers) is inductive if and only if $S = [a, b]$. Here a subset $S \subseteq [a, b]$ is called inductive, if it satisfies the following properties [2]: (1) $a \in S$; (2) if $a \leq x < b$, then $x \in S$ implies $[x, y] \subseteq S$ for some $y > x$; (3) if $a < x \leq b$ and $[a, x) \subseteq S$, then $x \in S$.

A more general theorem which characterizes Dedekind-complete total orders is also given in [2].

A discussion of a question about generalization of a slightly different theorem for total orders to an induction principle for partial orders and a formulation of an induction principle for complete lattices can be found at [6].

However, in formal methods and verification, some posets of interest do not form lattices. One example is the set of partial trajectories of a *nondeterministic* (possibly hybrid) dynamical system, defined on time intervals of the forms $[0, t)$, $[0, t]$, ordered by the extension relation ($s_1 \leq s_2$, if s_2 extends s_1), where diverging trajectories (incomparable elements) have no joins.

But in this example and in some other, a poset of interest belongs to the class of diamond-free posets, i.e. posets such that there is no tuple (a, b, c, d) in which $a \leq b \leq d$, $a \leq c \leq d$, and b, c are incomparable.

In this paper we will argue that Raoult's open induction principle [7] can be used to obtain an induction principle for diamond-free directed complete partial orders (dcpos) which extends the real induction principle.

2 Preliminaries

Let $(X, \leq)$ be a subset and $A \subseteq X$ be a subset. We will use the following notation:

- $<$ is the strict order which corresponds to $\leq$;
- $[a, b]$ is the set $\{x \in X \mid a \leq x \wedge x \leq b\}$;
- $[a, b)$ is the set $\{x \in X \mid a \leq x \wedge x < b\}$;
- $x = \sup_{\leq} A$ denotes that x is the least upper bound of A in $(X, \leq)$.

We will assume that the axiom of choice holds.

3 Main Result

Firstly, let us consider the following auxiliary statement.

Theorem 1 (Converse open induction principle). *Let $(X, \leq)$ be a poset.*

Assume that X is the only directed open subset $S \subseteq X$ which satisfies the following condition:

(1) for each $x \in X$, if $\forall y \in X(x < y \Rightarrow y \in S)$ holds, then $x \in S$.

Then $(X, \leq)$ is a dcpo.

Proof. Suppose that $(X, \leq)$ is not directed complete (so $(X, \leq)$ is not chain complete). Then there exists a nonempty $\leq$-chain $C \subseteq X$ which has no supremum in $(X, \leq)$. Let C' be the directed closure of C. Let $S = X \backslash C'$. Let us show that S satisfies the condition (1).

Let $x \in X$. Assume that $\forall y \in X(x < y \Rightarrow y \in S)$ holds. Suppose that $x \notin S$. Then $x \in C'$. The set $\{\sup_{\leq} C'' \mid C'' \subseteq C, C'' \neq \emptyset,$ and C'' has a supremum$\}$ is directed closed. Then $x = \sup_{\leq} C''$ for some nonempty $\leq$-chain $C'' \subseteq C$. Let us show that C and C'' are cofinal. Let $c \in C$. Suppose that for each $c'' \in C''$, $c < c''$ does not hold. Since $C'' \subseteq C$, each element of C'' is comparable with c. Then c is an upper bound of C''. Then $x \leq c$. The relation $x < c$ cannot hold,

because it implies $c \in S = X \backslash C'$, but $c \in C \subseteq C'$. Hence $x = c \in C$. Then each $y \in C$ such that $x < y$ belongs to S. This implies that x is the largest element of C. Then $x = \sup_{\leq} C$. This contradicts the assumption that C has no supremum. Thus there exists $c'' \in C''$ such that $c < c''$ holds. Since $c \in C$ is arbitrary, we conclude that C and C'' are cofinal. Then $x = \sup_{\leq} C$ and we get a contradiction with the assumption that C has no supremum. Thus $x \in S$.

Then S satisfies the condition (1). Note that S is directed open. Then $S = X$. Then $C' = \emptyset$ and we get a contradiction with the fact that C is nonempty.

Thus $(X, \leq)$ is directed complete. □

Theorem 2 (Induction principle for diamond-free dcpos).

Let $(X, \leq)$ be a diamond-free poset. Then $(X, \leq)$ is directed complete if and only if the only subset $S \subseteq X$ which satisfies the conditions (1)-(2) is X:

(1) for each $x \in X$, if $\forall y \in X(x < y \Rightarrow y \in S)$ holds, then $x \in S$;

(2) for each $x \in X$ and $z \in S$ such that $x < z$ and $\sup_{\leq}[x, z) = z$, there exists $y \in [x, z)$ such that $[y, z) \subseteq S$.

Proof. "If". Assume that X is the only subset of X which satisfies (1)-(2).

Let us show that each directed open set S satisfies the condition (2). Let $S \subseteq X$ be a directed open set, and $x \in X$ and $z \in S$ be such that $x < z$ and $\sup_{\leq}[x, z) = z$. Suppose that for each $y \in [x, z)$ we have $[y, z) \backslash S \neq \emptyset$. Then the sets $[x, z)$ and $[x, z) \backslash S$ are cofinal. Denote $C = [x, z) \backslash S$. Then $\sup_{\leq} C = z \in S$. Moreover, C is a $\leq$-chain, since $[x, z) \backslash S \subseteq [x, z]$ and $(X, \leq)$ is diamond-free. Since S is directed open, $C \cap S \neq \emptyset$. We have a contradiction with the definition $C = [x, z) \backslash S$. Thus there exists $y \in [x, z)$ such that $[y, z) \subseteq S$.

Thus X is the only directed open subset of X which satisfies the condition (1). Then $(X, \leq)$ is a dcpo by Theorem 1.

"Only if". Assume that $(X, \leq)$ is a diamond-free dcpo. Obviously, $S = X$ satisfies 1-2. Let $S \subseteq X$ be a set which satisfies 1-2. Let us show that $S = X$.

Firstly, let us show that S is a directed open set.

Let C be a nonempty $\leq$-chain such that $\sup_{\leq} C = z \in S$.

Let us show that $C \cap S \neq \emptyset$. Without loss of generality, assume that $z \notin C$. Let x be some element of C. Note that $x < z$.

Let $C_1 = \{y \in C \mid x \leq y\}$. Then C_1 is a nonempty $\leq$-chain. Moreover, C and C_1 are cofinal, so $\sup_{\leq} C_1 = z$. Since $z \notin C$, we have $C_1 \subseteq [x, z)$.

Let $y \in [x, z)$. Since $\sup_{\leq} C_1 = z$, y is not an upper bound of C_1. Then exists $c \in C_1$ such that $c \leq y$ does not hold. Note that c and y are not incomparable, since $c, y \in [x, z]$ and $(X, \leq)$ is diamond-free. Then $y < c$.

Since y is arbitrary, C_1 and $[x, z)$ are cofinal. Then $\sup_{\leq}[x, z) = z$.

Then from the condition (2) it follows that there exists $y \in [x, z)$ such that $[y, z] \subseteq S$. Since $x \leq y < z$ and $\sup_{\leq} C = z$, there exists $c \in C \cap [x, z]$ such that $c \leq y$ does not hold. Note that c and y are not incomparable, because $c, y \in [x, z]$ and $(X, \leq)$ is diamond-free. Then $y < c$, so $c \in [y, z] \subseteq S$ and $C \cap S \neq \emptyset$.

Since C is arbitrary, this implies that S is a directed open set in $(X, \leq)$. From the condition (1) it follows that S is the set of elements which satisfy an inductive property in the sense of [7, Proposition 1.2].

Then $S = X$ by the open induction principle [7]. □

4 Discussion

Similarly to the case of the real induction principle, the conditions (1)-(2) of Theorem 2 can be formulated as a first-order formula in a signature that has symbols for the predicate of membership in S, the relation $\leq$, and equality.

The condition (1) states that the predicate $P(x) \Leftrightarrow x \in S$ defines an inductive property in the terminology of [7] (which should not be confused with the notion of an inductive subset from [2]). It also corresponds to the formulation of Noetherian induction schema.

The condition (2) is analogous, but somewhat weaker than the formulation of the condition [6, (POI2')] for the opposite order relation ($\leq^{-1}$).

Theorem 2 is applicable to total orders (which are diamond-free). In the special case when X is the real interval $[0, 1]$ and $\leq$ is a restriction of the order, opposite to the standard order on real numbers, $(X, \leq)$ is directed complete and the "only if" part of the statement of the theorem reduces to the statement that $[0, 1]$ is the only subset $S \subseteq [0, 1]$ which satisfies (1)-(2), where (1)-(2) are equivalent to statement that S is an inductive subset of $[0, 1]$ in terms of [2].

Theorem 2 can also be applied to sets of partial trajectories of nondeterministic continuous-time dynamical systems, defined on time intervals of the form $[0, t)$, $[0, t]$, ordered by the extension relation ($s_1 \leq s_2$, if s_2 extends s_1), or the opposite of this relation (with the dual completeness requirement), assuming that a partial trajectory cannot extend two incomparable partial trajectories (since their domains are $\subseteq$-comparable).

5 Conclusions

We have proposed an induction principle for diamond-free directed complete partial orders. It can be considered as an extension of the real induction principle for a real interval.

References

1. Clark, P.: The Instructor's Guide to Real Induction. Mathematics Magazine 92, 136–150 (2019)
2. Clark, P.: The Instructor's Guide to Real Induction (2012) Available at: http://arxiv.org/abs/1208.0973
3. Kalantari, I.: Induction over the Continuum. In: M. Friend, N.B. Goethe and V.S. Harizanov (eds.), Induction, Algorithmic Learning Theory, and Philosophy, 145–154, Springer (2007)
4. Platzer, A., Yong Kiam Tan: Differential Equation Axiomatization: The Impressive Power of Differential Ghosts. In: Proc. of LICS'18, pp. 819–828 (2018)
5. Platzer, A., Yong Kiam Tan: Differential Equation Invariance Axiomatization (2019) Available at: http://arxiv.org/abs/1905.13429
6. A principle of mathematical induction for partially ordered sets with infima. – Web page: https://mathoverflow.net/questions/38238
7. Raoult J.-C.: Proving open properties by induction. Information Processing Letters 29, 19-23 (1988)