Generalized Newman's Lemma for Discrete and Continuous Systems

Ievgen Ivanov ✉
Taras Shevchenko National University of Kyiv, Ukraine

Abstract

We propose a generalization of Newman's lemma which gives a criterion of confluence for a wide class of not-necessarily-terminating abstract rewriting systems. We show that ordinary Newman's lemma for terminating systems can be considered as a corollary of this criterion. We describe a formalization of the proposed generalized Newman's lemma in Isabelle proof assistant using HOL logic.

2012 ACM Subject Classification Theory of computation → Equational logic and rewriting; Theory of computation → Logic and verification; Theory of computation → Timed and hybrid models

Keywords and phrases abstract rewriting system, confluence, discrete-continuous systems, proof assistant, formal proof

Digital Object Identifier 10.4230/LIPIcs.FSCD.2023.9

Supplementary Material *Text*: `https://doi.org/10.5281/zenodo.7855691` [14]

1 Introduction

Newman's lemma [20, 10, 15, 2, 17] is a mathematical result that is well-known in computer science community and that is usually associated with analysis of discrete structures and the principle of well-founded[1], or, dually, Noetherian induction. However, Noetherian induction has a generalization to Raoult's open induction principle [24] which can be considered as an interesting example of unification of proof principles important for analysis of discrete and continuous structures. More specifically, both the Noetherian induction principle for proving properties of elements of a Noetherian poset and a variant of a real induction principle [4] for proving properties of real numbers in a bounded closed interval can be interpreted as applications of the open induction principle. Moreover, it is known [23] that real induction is relevant to analysis of continuous-time dynamical systems defined using ordinary differential equations.

Taking into account the above mentioned remarks, it is natural to consider the question of whether Newman's lemma can be generalized in such a way that its generalization can be applied to a range of discrete, continuous, and discrete-continuous dynamical models (e.g. [8]). Note that discrete-continuous (hybrid) models become increasingly important for computer science with the spread of such concepts as cyber-physical systems [3], Internet of Things, etc., and although mathematical systems theory and control theory study a variety of models and properties (e.g. reachability, stability, controllability, etc.) that have certain correspondences with computation-related notions considered in computer science, the task of combining modeling and reasoning approaches from different fields remains non-trivial.

[1] For example, as of the time of writing, the article on Newman's lemma in English Wikipedia [21] mentions: "*Today, this is seen as a purely combinatorial result based on well-foundedness due to a proof of Gérard Huet in 1980.*"

And to simplify this task one can search for such generalizations of important results from one field (e.g. computer science) that they begin to directly overlap with another field (e.g. control theory) and vice versa.

In literature one can find confluence conditions that can be considered as generalizations of Newman's lemma for certain classes of abstract rewriting systems (ARS) [26, 5, 6, 7]. A notable example is Van Oostrom's theorem [26, Theorem 3.7] and its corollary that any Decreasing Church-Rosser (DCR) ARS is confluent. However, most of such conditions are linked in some way to auxiliary well-foundness, countability, and/or cofinality assumptions that are more relevant to analysis of discrete models of computation or discrete-continuous dynamical models with limited nondeterminism.

In this paper we propose a different approach to the mentioned question which makes use of a topology on the preordered set $(X, \to^*)$ associated with an ARS $(X, \to)$ in a way reminiscent to how it is used in Raoult's open induction principle, where $\to^*$ denotes the reflexive transitive closure of a reduction relation $\to$. Using this approach we obtain a generalized Newman's lemma (Theorem 28 in Section 3) which gives a necessary and sufficient condition of confluence for the class of ARS $(X, \to)$ such that $(X, \to^*)$ is a strictly inductive [18] preordered set (i.e. a preordered set where every nonempty chain has a least upper bound). Ordinary Newman's lemma for terminating systems can be considered as a corollary of the proposed criterion (Corollary 29 from Theorem 28).

As a proof of the main result we give a machine-checked formal proof of a formalized statement of generalized Newman's lemma in Isabelle proof assistant using HOL logic [11, 22, 27] in supplementary material [14] for this paper. Note that this proof is not based on direct application of either Noetherian or open induction, however, Noetherian induction and a suitably adapted open induction principle can be used to characterize classes of ARS for which the ordinary and generalized Newman's lemmas can be used as confluence criteria (Propositions 7 and 14 in Section 2).

Isabelle is a generic proof assistant software with a small logical core that provides a meta-logic in which several object logics are encoded. Supported object logics include, in particular, higher-order logic (HOL) and Zermelo-Fraenkel set theory (ZF). They can be used to formalize statements and proofs from pure mathematics, but they also have applications in the domain of formal specification and verification of systems and software. A user can introduce new definitions and formulate statements (lemmas, theorems) using special formal notation. In simple cases, a proof of a valid statement can be obtained automatically by calling automated theorem provers, but in most non-trivial cases a user needs to guide the system using a proof script or a structured proof text, so that a complete formal proof can be constructed automatically from such a script/text.

Note that there exist other formalizations of ARS-related notions and results in Isabelle, e.g. [25, 1, 29], however, our formalization does not depend on them. Our formalization depends only on standard theories included in Isabelle distribution.

2 Preliminaries

Below we give definitions of the notions which we need to formulate and discuss the main result. Definitions and propositions given in this section and Theorem 28 in Section 3 (main result) are formulated using ordinary mathematical notation. Propositions 7-27 are accompanied by non-formalized proof sketches which explain main proof ideas. Such formulations and proof sketches are intended to simplify understanding of the main result and omit low-level details of our Isabelle formalization. A reader can assume that a background theory for understanding them is ZFC, however, our Isabelle formalization is based on HOL.

Formalized versions of Definitions 1-24 and statements of Propositions 7-27 and Theorem 28 for proof assistant software, as well as complete formal proof texts are given in [14] (supplementary material for this paper). Formal proofs can be checked automatically using Isabelle 2022 software [11].

2.1 Abstract rewriting systems

Let us recall several standard notions that appear in literature on rewriting systems (e.g. [15, 2, 17]). Note that we assume that the axiom of choice holds.

We will denote logical negation, disjunction, conjunction, and implication as $\neg$, $\vee$, $\wedge$, and $\Rightarrow$ respectively.

▶ **Definition 1.** *An abstract rewriting system (ARS) is a pair $(X, \to)$, where X is a set and $\to$ is a binary relation on X (called reduction).*

Note that some authors define an ARS to be a pair of a set and an indexed family of reduction relations $(\to_i)_{i\in I}$. We do not use this approach in this paper and instead restrict attention to ARS with a single reduction relation $\to$. Also, we allow X to be empty.

Let $(X, \to)$ be an ARS. Denote as $\to^+$ the transitive closure of $\to$, and denote as $\to^*$ the reflexive transitive closure of $\to$.

▶ **Definition 2.** *Let $x \in X$. Then*

(1) *x is reducible, if there exists $x' \in X$ such that $x \to x'$*
(2) *x is irreducible, if x is not reducible*
(3) *$x' \in X$ is a normal form of x, if $x \to^* x'$ and x' is irreducible.*

▶ **Definition 3.** *An ARS $(X, \to)$ is*

(1) *(weakly) normalizing, if for each $x \in X$ there exists $x' \in X$ such that x' is a normal form of x*
(2) *terminating (or, alternatively, strongly normalizing), if there is no infinite reduction sequence $x_1 \to x_2 \to \ldots$ ($x_i \in X$).*

▶ **Definition 4.** *An ARS $(X, \to)$ is*

(1) *confluent, if*

$$\forall a, b, c \in X \ (a \to^* b \wedge a \to^* c \Rightarrow \exists d \in X \ (b \to^* d \wedge c \to^* d))$$

(2) *locally confluent, if*

$$\forall a, b, c \in X \ (a \to b \wedge a \to c \Rightarrow \exists d \in X \ (b \to^* d \wedge c \to^* d)).$$

2.2 Noetherian induction

It is known that the condition that an ARS $(X, \to)$ is terminating can be characterized in terms of soundness of a variant of Noetherian induction principle which can be used to show that a given property $P(x)$ holds for all $x \in X$.

We will use a variant of Noetherian induction principle similar to the one given in [17, paragraph 1.3.15], but will reformulate it in extensional form by assuming that the mentioned property $P(x)$ is represented as $x \in S$, where S is a set.

▶ **Definition 5.** *S is a Noetherian-inductive subset in ARS $(X, \to)$, if $S \subseteq X$ and*

$$\forall x \in X \ ((\forall y \in X \ (x \to^+ y \Rightarrow y \in S)) \Rightarrow x \in S).$$

▶ **Definition 6.** *$(X, \to)$ has sound Noetherian induction principle, if for every $S \subseteq X$, if S is a Noetherian-inductive subset in ARS $(X, \to)$, then $S = X$.*

▶ **Proposition 7.** *For any ARS $(X, \to)$ the following conditions are equivalent:*
1. *$(X, \to)$ is terminating*
2. *$(X, \to)$ has sound Noetherian induction principle.*

Proof sketch. Similar to the proof of [17, Theorem 1.3.16]. ◀

2.3 Strictly inductive ARS

Let $(X, \leq)$ be a preordered set (so $\leq$ is a reflexive and transitive binary relation on X).

▶ **Definition 8.** *Let $A \subseteq X$ and $x \in X$. Then x is*
(1) *an upper bound of A, if $\forall a \in A\ a \leq x$*
(2) *a least element of A, if $x \in A \wedge \forall a \in A\ x \leq a$*
(3) *a least upper bound of A, if x is a least element of the set of all upper bounds of A.*

▶ **Definition 9.** *A subset $A \subseteq X$ is*
(1) *a chain (in $(X, \leq)$), if $\forall x, y \in A\ (x \leq y \vee y \leq x)$*
(2) *closed (in $(X, \leq)$), if for every nonempty chain C in $(X, \leq)$, if C has a least upper bound $x \in X$ and $C \subseteq A$, then $x \in A$*
(3) *open (in $(X, \leq)$), if $X \backslash A$ is closed in $(X, \leq)$*
(4) *relatively open in B w.r.t. preorder relation $\leq$, where $B \subseteq X$ is a superset of A, if A is open in $(B, \leq \cap (B \times B))$.*

▶ Remark. A Scott-open subset in a poset is open in the above mentioned sense, but the converse may not hold. More information on topologies on ordered sets can be found in [9].

Some examples that illustrate Definition 9 are given below.

If $X = [0, 1]$, where $[0, 1]$ denotes the real unit interval, and $\leq$ is the standard order on real numbers restricted to X, then
- every subset of X is a chain
- the set $\{1\}$ is closed: every nonempty chain in $\{1\}$ contains only 1, so its supremum is 1, and $1 \in \{1\}$
- the set $\{1\}$ is *not* open: the element $1 \in \{1\}$ can be approached from below using a nonempty chain of elements outside $\{1\}$, e.g. 0.9, 0.99, 0.999, ...
- the set $(0, 1)$ is open: no number in $(0, 1)$ can be approached from below using a nonempty chain that has no elements in $(0, 1)$.

If X is the set of all finite strings in the alphabet $\{0, 1\}$ (e.g. $01010 \in X$), and $s \leq s'$ if and only if s is a prefix of s' (e.g. $01 \leq 010$, but $01 \not\leq 110$), then
- the set $\{0, 00\}$ is a chain
- the set $\{0, 1\}$ is *not* a chain: the elements 0, 1 are incomparable
- the set $\{1\}$ is closed and open.

▶ **Definition 10.** *A preordered set $(X, \leq)$ is strictly inductive, if every nonempty chain in $(X, \leq)$ has a least upper bound (i.e. for every nonempty chain C there exists $x \in X$ such that x is a least upper bound of C).*

The term "strictly inductive" is adapted from [18]. Note that a dcpo is a strictly inductive preordered set.

▶ **Definition 11.** *An ARS $(X, \to)$ is*

(1) *strictly inductive, if $(X, \to^*)$, considered as a preordered set, is strictly inductive*

(2) *acyclic [7], if for each $x, y \in X$, if $x \to^+ y$, then $x \neq y$.*

▶ Remark. In some literature, e.g. [15], an *inductive* ARS is defined as an ARS where for every reduction sequence $x_1 \to x_2 \to \ldots$ there exists $x \in X$ such that $x_n \to^* x$ for all n. In general, this condition is weaker than the condition that $(X, \to^*)$ is a strictly inductive preordered set, so our terminology is consistent with such literature: a strictly inductive ARS is inductive in the mentioned sense, but the converse may not hold.

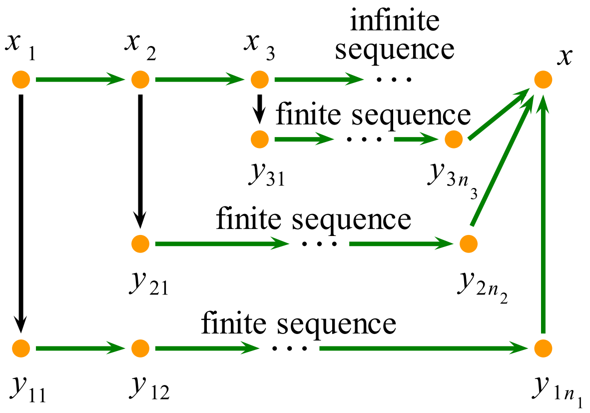

Figure 1 Illustration of the notion of an *inductive* ARS: for every reduction sequence $x_1 \to x_2 \to \ldots$ there exists $x \in X$ such that $x_n \to^* x$ for all n. Such an element x is an upper bound of $\{x_1, x_2, \ldots\}$ in the preordered set $(X, \to^*)$. The notion of a *strictly indutive* ARS further requires that $\{x_1, x_2, \ldots\}$ has a least upper bound, and, moreover, every nonempty chain in $(X, \leq)$ has a least upper bound.

▶ **Example 12.** Let $(X, \to) = ([0, 1], < \cap ([0, 1] \times [0, 1]))$, where $[0, 1]$ is the real unit interval and $<$ is the standard strict order on real numbers. Then $(X, \to)$ is a strictly inductive ARS. Moreover, $(X, \to)$ is acyclic.

▶ **Definition 13.** *An ARS $(X, \to)$ has sound open induction principle, if for every open $S \subseteq X$ in the preordered set $(X, \to^*)$, if S is a Noetherian-inductive subset in ARS $(X, \to)$, then $S = X$.*

▶ **Proposition 14.** *For any ARS $(X, \to)$ the following conditions are equivalent:*

1. *$(X, \to)$ is a strictly inductive and acyclic ARS*
2. *$(X, \to)$ has sound open induction principle.*

Proof sketch. A proof that Item 1 implies Item 2 is analogous to a proof of Raoult's theorem [24, Theorem 3.3]. A proof that Item 2 implies Item 1 consists of two parts.

- A proof that an ARS with sound open induction principle is strictly inductive is analogous to the proof of a converse open induction principle proposed in [13, Theorem 1].
- A proof that an ARS with sound open induction principle is acyclic can be performed by contradiction (by assuming that $x \to^+ x$ holds for some $x \in X$ and considering $S = X \backslash \{y \in X \mid y \to^* x\}$ in Definition 13). ◀

▶ **Proposition 15.** *Any terminating ARS is strictly inductive and acyclic.*

Proof sketch. Follows immediately from Propositions 7, 14 by noting that an ARS with sound Noetherian induction principle also has sound open induction principle (see Definitions 6 and 13). ◀

▶ **Proposition 16.** *If $(X, \to)$ is an ARS and X is finite, then $(X, \to)$ is strictly inductive.*

Proof sketch. Follows from Definition 10 by noting that a nonempty finite chain in a preordered set has a least upper bound. ◀

2.4 Quasi-normal forms

In contrast to terminating ARS, strictly inductive ARS are not necessarily weakly normalizing (e.g., the ARS ({0},{(0,0)}) is strictly inductive, but is not weakly normalizing). However, the following notions can be used to preserve a certain similarity between the studies of properties of terminating and strictly inductive ARS in the general case.

▶ **Definition 17.** *Let $(X, \to)$ be an ARS and $x, x' \in X$. Then*

(1) *x is quasi-irreducible, if for each $y \in X$, $x \to^* y$ implies $y \to^* x$*

(2) *x' is a quasi-normal form of x (or, shortly, x' is a QNF of x), if $x \to^* x'$ and x' is quasi-irreducible*

(3) *x, x' are QNF-equivalent, if*

$$\{y \in X \mid y \text{ is a QNF of } x\} = \{y \in X \mid y \text{ is a QNF of } x'\}.$$

▶ **Definition 18.** *An ARS $(X, \to)$ is*

(1) *quasi-normalizing, if for each $x \in X$ there exists $x' \in X$ such that x' is a quasi-normal form of x.*

(2) *openly quasi-normalizing, if $(X, \to)$ is quasi-normalizing and for each $x, x' \in X$ such that x' is a quasi-normal form of x, the set*

$$\{y \in X \mid x \to^* y \ \wedge \ y \text{ and } x' \text{ are QNF-equivalent }\}$$

is relatively open in $\{y \in X \mid x \to^* y\}$ w.r.t. preorder relation $\to^*$.

The quasi-normalization condition has an obvious analogy with the (weak) normalization condition. In the general case, open quasi-normalization condition is a stroger requirement, the importance of which for checking confluence will be shown below in Theorem 28 and Example 31 (in particular, the ARS given in Example 31 is strictly inductive and quasi-normalizing, but is neither openly quasi-normalizing, nor confluent, and in this example the lack of confluence is linked to the lack of open quasi-normalization).

▶ **Proposition 19.** *Any strictly inductive ARS is quasi-normalizing.*

Proof sketch. Follows from Zorn's lemma. ◀

▶ **Proposition 20.** *Let $(X, \to)$ be a terminating ARS. Then for any sets A, B such that $A \subseteq B \subseteq X$, A is relatively open in B w.r.t. preorder relation $\to^*$.*

Proof sketch. Follows from Definition 9 by noting that for a terminating $(X, \to)$, a nonempty chain C in $(X, \to^*)$ has a greatest element (i.e. $x \in C$ such that $\forall c \in C \ c \to^* x$). ◀

▶ **Proposition 21.** *Any terminating ARS is openly quasi-normalizing.*

Proof sketch. Follows immediately from Propositions 15, 19, 20 and Definition 18. ◀

Another simple sufficient condition which guarantees that an ARS is openly quasi-normalizing is given below.

▶ **Definition 22.** *An ARS $(X, \to)$ is finitely normalizing, if it is normalizing and the set of all irreducible elements in $(X, \to)$ is finite.*

▶ **Proposition 23.** *Any finitely normalizing ARS is openly quasi-normalizing.*

Proof sketch. Follows from Definition 18 by noting that for a finitely normalizing $(X, \to)$, the set

$$\{y \in X \mid x \to^* y \ \wedge\ y \text{ and } x' \text{ are QNF-equivalent }\}$$

can be expressed as a complement of a finite union of closed sets in $\{y \in X \mid x \to^* y\}$ considered as an induced preordered set (from $(X, \to^*)$). ◀

2.5 Quasi-local confluence

The notion of local confluence loses its usefulness when a reduction relation $\to$ is reflexive and transitive, because in this case the definitions of confluence and local confluence become trivially equivalent (and equivalent to the diamond property condition). In some of such and other situations related to non-terminating ARS, the notion of quasi-local confluence introduced below can be used as a replacement for local confluence.

▶ **Definition 24.** *An ARS $(X, \to)$ is quasi-locally confluent, if for each $a \in X$ there exists a subset $S \subseteq \{x \in X \mid a \to^+ x\}$ such that the following 2 conditions hold:*

1. *two-consistency condition:*

$$\forall b, c \in S\ \exists d \in X\ (b \to^* d \wedge c \to^* d)$$

2. *coinitiality condition:*

$$\forall x \in X\ (a \to^+ x \Rightarrow (x \to^* a) \vee (\exists b \in S\ b \to^* x \wedge \neg(b \to^* a))).$$

Intuitively, a set S in Definition 24 can be thought of as a substitute for the set of successors of a: $\{x \in X \mid a \to x\}$. The latter set actually satisfies the conditions 1 and 2 in the case of locally confluent acyclic ARS as Proposition 26 below states. Basically, the conditions 1 and 2 axiomatize some properties of the mentioned set to allow one to obtain useful generalizations of confluence criteria for wider classes of ARS.

The two-consistency condition is an adaptation of the following notion of a *2-consistent set* for preordered sets to ARS: a subset $A \subseteq X$ in a preordered set $(X, \leq)$ is 2-consistent, if for each $a_1, a_2 \in A$ there exists $x \in X$ such that $a_1 \leq x$ and $a_2 \leq x$ (when $A \neq \emptyset$ this is reminiscent to the notion of a directed set, however x is not required to belong to A). Thus the two-consistency condition expresses the requirement that S is a 2-consistent set in the preordered set $(X, \to^*)$.

The coinitiality condition is an adaptation of the notion of a *coinitial subset* for preordered sets to ARS: if $(X, \leq)$ is a preordered set and $A, B \subseteq X$, then A is a coinitial subset of B, if $A \subseteq B$ and for each $b \in B$ there exists $a \in A$ such that $a \leq b$. In particular, when a reduction relation $\to$ coincides with some strict partial order $<$ on X, the coinitiality condition together with the condition $S \subseteq \{x \in X \mid a \to^+ x\}$ expresses the requirement that S is a coinitial subset of $\{x \in X \mid a < x\}$ in the poset $(X, \leq)$, where $x \leq y \Leftrightarrow (x = y \vee x < y)$.

▶ **Proposition 25.** *Any confluent ARS is quasi-locally confluent.*

Proof sketch. Assume that an ARS $(X, \to)$ is confluent. Then it is straightforward to check that for any $a \in X$, the set $S = \{x \in X \mid a \to^* x \wedge \neg(x \to^* a)\}$ satisfies the conditions of Definition 24. So $(X, \to)$ is quasi-locally confluent. ◀

▶ **Proposition 26.** *Let $(X, \to)$ be a locally confluent acyclic ARS and $a \in X$. Then $S = \{x \in X \mid a \to x\}$ satisfies the conditions 1-2 of Definition 24.*

Proof sketch. A proof is straightforward and follows from the relevant definitions. ◀

▶ **Proposition 27.** *Any locally confluent acyclic ARS is quasi-locally confluent.*

Proof sketch. Follows immediately from Definition 24 and Proposition 26. ◀

3 Main Result

▶ **Theorem 28** (Generalized Newman's lemma)**.** *Let $(X, \to)$ be a strictly inductive ARS. Then $(X, \to)$ is confluent if and only if $(X, \to)$ is openly quasi-normalizing and quasi-locally confluent.*

Proof sketch.

"If" part. Assume that $(X, \to)$ is a strictly inductive, openly quasi-normalizing, and quasi-locally confluent ARS. Let us show that $(X, \to)$ is confluent.

Let $a \in X$. To show that for any b, c with $a \to^* b \wedge a \to^* c$ there exists $d \in X$ such that $b \to^* d \wedge c \to^* d$, it is sufficient to show that all maximal elements in $X' = \{x \in X \mid a \to^* x\}$, considered as an induced preordered subset of the preordered set $(X, \to^*)$, are equivalent w.r.t. the equivalence relation $\approx$, where $x \approx x'$ if and only if $x \to^* x' \wedge x' \to^* x$.

Consider any two such maximal elements $M, M' \in X'$ (they will also be maximal elements in the preordered set $(X, \to^*)$ and quasi-normal forms in ARS $(X, \to)$) and introduce an auxiliary preordered set $(X', \leq')$, where

$$x \leq' y \Leftrightarrow (x \to^* y \vee ((\exists x' \in X'\ x \to^* x' \wedge \neg(x' \to^* M)) \wedge M' \to^* y))).$$

Then for each $x \in X'$, $x \leq' M \vee x \leq' M'$ holds.

The main reason for introducing the preordered set $(X', \leq')$ is that it simplifies further analysis of relations between M and M' (note that $(X', \leq')$ does not have any elements incomparable with both M and M').

The preordered set $(X', \leq')$ can be shown to be strictly inductive using the assumption that the ARS $(X, \to)$ is openly quasi-normalizing.

The sets $\{x \in X' \mid x \leq' M\}$, $\{x \in X' \mid x \leq' M'\}$ are closed in $(X, \leq')$. Denote their intersection as D. Then D is closed in $(X', \leq')$, and is also nonempty since $(X', \leq')$ has a least element. Since $(X, \leq')$ is strictly inductive (implicitly using Zorn's lemma) one can conclude that there is some $\leq'$-maximal element $m \in D$.

As before, for any preordered set $(P, \leq)$ we call a subset $A \subseteq P$ 2-consistent, if for each $a_1, a_2 \in A$ there exists $x \in P$ such that $a_1 \leq x \wedge a_2 \leq x$. It is straightforward to show the following criterion of 2-consistency: a subset $A \subseteq P$ is 2-consistent if and only if for any down-closed sets $X_1, X_2 \subseteq P$ the condition $P = X_1 \cup X_2$ implies $A \subseteq X_1 \vee A \subseteq X_2$.

Using the assumption that the ARS $(X, \to)$ is quasi-locally confluent one can show that there is some coinitial subset N of $\{x \in X' \mid m \leq' x \wedge \neg x \leq' m\}$ which is 2-consistent in $(X', \leq')$. The above mentioned 2-consistency criterion implies that $N \subseteq \{y \in X' \mid y \leq' M\} \vee N \subseteq \{y \in X' \mid y \leq' M'\}$.

Suppose that M and M' are not comparable w.r.t. $\leq'$. Then using coinitiality of N, there exist $b \in N$ and $c \in N$ such that $b \leq' M$ and $c \leq' M'$. As we have mentioned above, $N \subseteq \{y \in X' \mid y \leq' M\} \vee N \subseteq \{y \in X' \mid y \leq' M'\}$.

If $N \subseteq \{y \in X' \mid y \leq' M\}$, then $c \leq' M$, whence $m \leq' c \wedge \neg c \leq' m$ and $c \in D$.

If $N \subseteq \{y \in X' \mid y \leq' M'\}$, then $b \leq' M'$, whence $m \leq' b \wedge \neg b \leq' m$ and $b \in D$.

In both cases we have a contradiction with $\leq'$-maximality of m in D. Thus M and M' are comparable w.r.t. $\leq'$, which implies that $M \approx M'$.

"Only if" part. Assume that an ARS $(X, \to)$ is strictly inductive and confluent ARS. Let us show that $(X, \to)$ is openly quasi-normalizing and quasi-locally confluent.

From Proposition 19 it follows that $(X, \to)$ is quasi-normalizing. Then it is straightforward to show that $(X, \to)$ is openly quasi-normalizing by noting that in the case of a confluent $(X, \to)$, for any $x \in X$ and for any $x', x'' \in X$ which are quasi-normal forms of x, $x' \to^* x'' \wedge x'' \to^* x'$ holds. Also, $(X, \to)$ is quasi-locally confluent by Proposition 25. ◀

The following statements can be considered as corollaries from Theorem 28.

▶ **Corollary 29.** *(Newman's lemma) Any locally confluent terminating ARS is confluent.*

Proof. Follows immediately from Theorem 28 and the following propositions from Section 2:

- any terminating ARS is strictly inductive and acyclic (Proposition 15)
- any terminating ARS is openly quasi-normalizing. (Proposition 21)
- any locally confluent acyclic ARS is quasi-locally confluent (Proposition 27).

Note that straightforward proofs of these propositions do not rely on the ordinary Newman's lemma itself. ◀

▶ **Corollary 30.** *Any locally confluent ARS which is strictly inductive, acyclic and finitely normalizing is confluent.*

Proof. Follows immediately from Theorem 28 and the following propositions from Section 2:

- any finitely normalizing ARS is openly quasi-normalizing (Proposition 23)
- any locally confluent acyclic ARS is quasi-locally confluent (Proposition 27). ◀

Note that in the general case, the open quasi-normalization condition cannot be omitted from the statement of Theorem 28 as the following example shows.

▶ **Example 31.** Consider an ARS $(P, \to)$, where $P = [0,1] \times [0,1]$ (where $[0,1]$ denotes the real unit interval) and the reduction relation $\to$ is defined as follows (where components of elements of P are denoted as x and t):

$$(x,t) \to (x',t') \text{ if and only if } (x \leq x' \ \wedge\ t < t' \ \wedge\ x' - x \leq t' - t).$$

It is straightforward to check that $(P, \to)$ is strictly inductive, quasi-locally confluent, but is *not* confluent. Then $(P, \to)$ is *not* openly quasi-normalizing by Theorem 28, however, $(P, \to)$ is quasi-normalizing by Proposition 19. Thus in this example one can link the lack of confluence to the lack of open quasi-normalization. The described ARS is illustrated in Figure 2.

▶ Remark. A possible interpretation of the ARS $(P, \to)$ given in Example 31 in terms of physics (special relativity) is as follows. Consider x as space coordinate, t as time coordinate, P as a region of spacetime. The relation

$$t < t' \ \wedge\ |x' - x| \leq t' - t,$$

which can also be expressed as

$$(t'-t)>0 \ \wedge \ c^2(t'-t)^2-(x'-x)^2 \geq 0,$$

where $c=1$, is a strict causal precedence between events in (1+1) dimensional Minkowski spacetime[2], so a reduction $(x,t) \to (x',t')$ is a conjunction of this relation and a spatial direction condition $x \leq x'$, restricted to P.

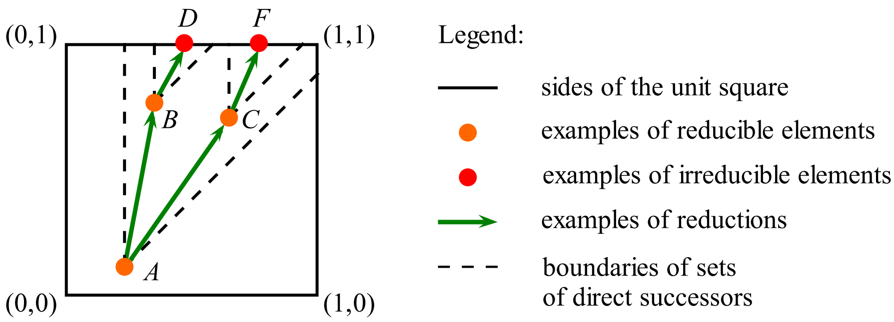

Figure 2 Illustration of the ARS $(P, \to)$ from Example 31. Horizontal axis is x, vertical axis is t.

▶ Remark. Using a slight generalization of a chain completion construction for posets given in [18], Theorem 28 may be indirectly applied to ARS which are not strictly inductive.

▶ **Example 32.** Consider an ARS $(X, \to)$, where $X=[0,1]\times[0,1]$ (where $[0,1]$ denotes a real interval) and $\to \subseteq X \times X$ is a relation such that for each $x, y, x', y' \in [0,1]$,

$(x,y) \to (x',y')$ if and only if $(x<x' \ \vee \ (x=x' \wedge y'<y \wedge (x<1 \vee y<1))) \wedge (x-y \leq x'-y') \wedge \ (x=y \Rightarrow x'=y') \wedge (x \leq y \Rightarrow x' \leq y')$.

The behavior of $\to$ is illustrated in Figure 3 below.

It is straightforward to check that this ARS is strictly inductive and acyclic and that $(1,0)$ and $(1,1)$ are the only irreducible elements. Then using Proposition 19 one can conclude that $(X, \to)$ is finitely normalizing, so from Proposition 23 and Theorem 28 it follows that for $(X, \to)$ confluence and quasi-local confluence conditions are equivalent. To show quasi-local confluence, for any point $a \in X$ it is sufficient to choose some set S (e.g. the set of $p \in X$ such that $a \to^+ p$ and $d(a,p) \in (0, \varepsilon)$ for a small positive number ε which may depend on a, where d is Euclidean distance) which satisfies the coinitiality condition from Definition 24 and make sure that it satisfies the two-consistency condition, i.e. pairs of elements in S can be joined using finite reduction sequences which are allowed to end outside S. Note that the given ARS $(X, \to)$ is indeed confluent.

▶ Remark. Further examples of ARS can be obtained from reachability relations on states of various (possibly nondeterministic) dynamical models. For example, consider a hybrid automaton [8] illustrated in Figure 4 that represents a simple model of motion of a bouncing ball. Note that it is usual to consider a simplified version of such an automaton with a single discrete state (Discrete state 1 in Figure 4), however, a model with a single discrete state is deterministic and has Zeno behavior [8] (semi-formally, performs infinitely many discrete

[2] Note that there exist known links [19] between this notion and models of distributed systems in the sense of computer science.

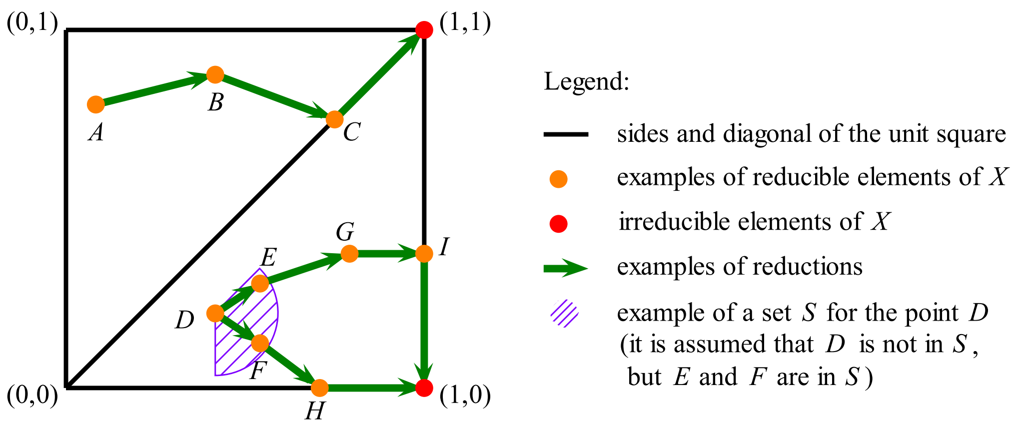

Figure 3 Illustration for Example 32. Elements of the ARS are points in the square $[0,1] \times [0,1]$. The reduction relation $\to$ is described in Example 32. Horizontal axis is x, vertical axis is y. Points above or on the diagonal shown in the figure have the point $(1,1)$ as a unique normal form. Points strictly below the diagonal shown in the figure have $(1,0)$ as a unique normal form. For this ARS quasi-local confluence implies confluence. Semi-formally, the quasi-local confluence condition for this (acyclic) ARS can be checked by making sure that for every point (x,y) (e.g. (x,y) is a point D) there exists a set S (e.g. intersection of $\{(x',y') \mid (x,y) \to^+ (x',y')\}$ and a neighborhood of D) such that any two points in S (e.g. points E, F) can be joined using some finite reduction sequences (e.g. $E \to G \to I \to (1,0)$ and $F \to H \to (1,0)$), and any point which is reachable from (x,y) using a nonempty finite reduction sequence can be reached from some element of S using a finite (possibly empty) reduction sequence. Such a set S is a generalization of the set of direct successors of an element and the mentioned conditions replace the local confluence condition.

transitions over a bounded interval of continuous time). Since one cannot expect such a model to adequately represent the behavior of a real object when very short time intervals and distances are involved, one can introduce a new discrete state [16] (Discrete state 2, stopped ball) and a nondeterministic transition between discrete states that represents an uncertain moment when the ball stops. This does not exclude Zeno executions, but allows one to acknowledge limitations of the model and of its ability to predict the behavior of a real object (there exist other ways to address Zeno behavior issue [8], however, we will not focus on them in this paper).

With the resulting hybrid model one associate an ARS $(X, \to)$ such that $X = [0, +\infty) \times \mathbb{R}$ (continuous state space) and $(y_1, v_1) \to (y_2, v_2)$, if (y_2, v_2) can be reached from (y_1, v_1)

- either via continuous evolution within one discrete state (see Figure 6),
- or as a result of a single transition between discrete states (from Discrete state 1 to Discrete state 1 or 2).

Often, important properties of the reachability relation (bounds on reachable sets, etc.) can be determined from a model without explicitly solving the equations that determine evolution of state in time (e.g. ordinary differential equations associated with discrete states). In particular, methods related to real induction can be used to prove bounds on reachable sets [23]. In this example such methods are not required, because the model is very simple, however, it is still possible to determine that (y_2, v_2) reachable from (y_1, v_1) via continuous evolution within Discrete state 1 satisfies $\frac{1}{2}v_2^2 - \frac{1}{2}v_1^2 = g(y_1 - y_2)$ using energy conservation considerations (without solving differential equations explicitly). The obtained properties of the reduction $\to$ can be used in confluence analysis. Note that the described ARS is confluent since the final position and velocity of the ball are both zero.

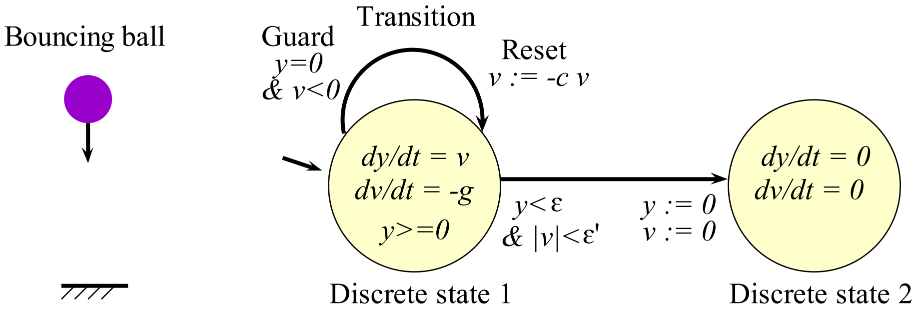

Figure 4 Illustration of a simple bouncing ball hybrid automaton with 2 discrete states. Here t is time, y is a vertical position, v is a vertical velocity, g is the gravity constant, c is a restitution coefficient, $\varepsilon, \varepsilon'$ are positive constants.

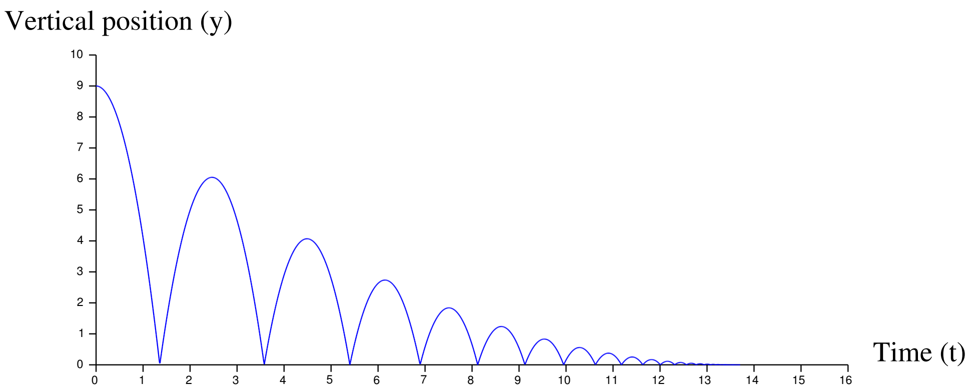

Figure 5 An example of an execution of the hybrid model illustrated in Figure 4.

4 Isabelle Formalization

Below we give formalized versions of definitions from Section 2 that are needed to formulate Theorem 28 and a formalized version of the statement of Theorem 28 (main result). Other formal definitions, Propositions 7-27, and formal proof texts for Theorem 28 and Propositions 7-27 are included in [14] (supplementary material for this paper).

The notions of an ARS and a confluent ARS are formalized as follows.

```
— Definition 1: (X,σ) is an abstract rewriting system (ARS) with a single reduction relation
— σ represents a reduction relation (->) as a predicate
— this formal definition enforces the types of X and σ and the condition -> ⊆ X×X
definition is_ars :: "'a set ⇒ ('a ⇒ 'a ⇒ bool) ⇒ bool"
("_,_ is ARS")
  where "X,σ is ARS ≡ (∀ x y. σ x y ⟶ x ∈ X ∧ y ∈ X)"

— Definition 4(1): (X,σ) is a confluent ARS
definition is_confl_ars ("_,_ is CONFLUENT ARS")
  where "X,σ is CONFLUENT ARS ≡ (X,σ is ARS) ∧
      (∀a∈X. ∀b∈X. ∀c∈X. (σ^** a b ∧ σ^** a c ⟶
                                    (∃d∈X. σ^** b d ∧ σ^** c d)))"
```

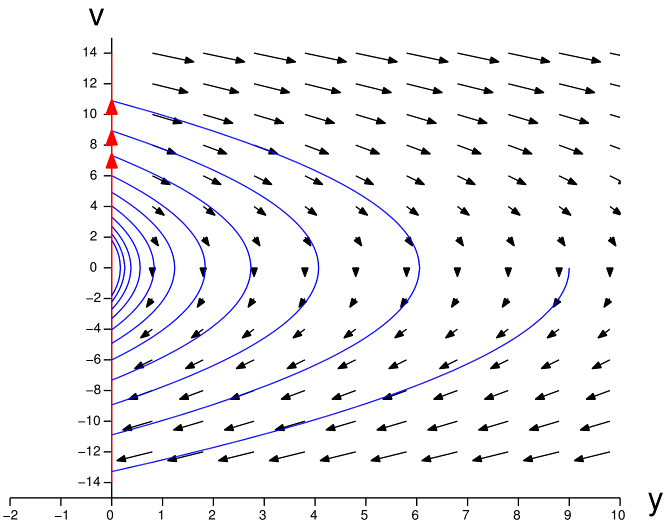

Figure 6 Continuous state space and example trajectories for the hybrid model illustrated in Figure 4 (transitions between Discrete states 1 and 2 are not illustrated).

Formalizations of basic preorder-related notions are given below.

```
— Definition 8(1): x is an upper bound of A (in preordered set (X,ϱ))
— ϱ represents a preorder relation ≤ as a predicate
— assumptions: A ⊆ X and ϱ is reflexive and transitive
abbreviation is_upperbound ::
      "'a ⇒ 'a set ⇒ 'a set ⇒ ('a ⇒ 'a ⇒ bool) ⇒ bool"
      ("_ is anUPPER BOUND of _ in _,_")
where
  "x is anUPPER BOUND of A in X,ϱ ≡ x∈X ∧ (∀a∈A. ϱ a x)"

— Definition 8(2): x is a least element of A (in preordered set (X,ϱ))
— assumptions: A ⊆ X and ϱ is reflexive and transitive
abbreviation is_leastelem ::
      "'a ⇒ 'a set ⇒ 'a set ⇒ ('a ⇒ 'a ⇒ bool) ⇒ bool"
("_ is LEAST of _ in _,_")
where
  "x is LEAST of A in X,ϱ ≡ x∈A ∧ (∀a∈A. ϱ x a)"

— Definition 8(3): x is a least upper bound of A (in preordered set (X,ϱ))
— assumptions: A ⊆ X and ϱ is reflexive and transitive
definition is_lub ("_ is l.u.b. of _ in _,_")
where
  "x is l.u.b. of A in X,ϱ ≡ (x is LEAST of
      {u. u is anUPPER BOUND of A in X,ϱ} in X,ϱ)"

— Definition 9(1): A is a chain (in preordered set (X,ϱ))
— assumptions: ϱ is reflexive and transitive
definition is_achain ("_ is aCHAIN in _,_")
```

```
  where "A is aCHAIN in X,ϱ ≡ A⊆X ∧ (∀x∈A. ∀y∈A. ϱ x y ∨ ϱ y x)"
```

```
— Definition 9(2): A is a closed subset (in preordered set (X,ϱ))
— assumptions: ϱ is reflexive and transitive
definition is_cclosedset ("_ is CLOSED SUBSET in _,_")
where
  "A is CLOSED SUBSET in X,ϱ ≡ A ⊆ X ∧
      (∀ C x. (C is aCHAIN in X,ϱ) ∧ C ≠ {} ∧
      (x is l.u.b. of C in X,ϱ) ∧ C ⊆ A ⟶ x ∈ A)"
```

```
— Definition 9(3): A is an open subset (in preordered set (X,ϱ))
— assumptions: ϱ is reflexive and transitive
definition is_copenset ("_ is OPEN SUBSET in _,_")
where
  "A is OPEN SUBSET in X,ϱ ≡ A ⊆ X ∧ ((X-A) is CLOSED SUBSET in X,ϱ)"
```

```
— Definition 9(4): A is relatively open in B w.r.t. preorder ϱ
— assumptions: ϱ is reflexive and transitive
definition is_relopenset ("_ is REL.OPEN SUBSET in _ wrt _")
where
  "A is REL.OPEN SUBSET in B wrt ϱ ≡
      A is OPEN SUBSET in B,(λ x y. ϱ x y ∧ x ∈ B ∧ y ∈ B)"
```

```
— Definition 10: (X,ϱ) is a strictly inductive preordered set
— ϱ represents a preorder relation ≤ as a predicate
— this formal definition enforces that ≤ is reflexive and transitive
— but does not enforce that ≤ ⊆ X×X
definition is_siprset ("_,_ is S.I.PREORDERED")
where
  "X,ϱ is S.I.PREORDERED ≡
    (∀x∈X. ϱ x x) ∧
     (∀x∈X. ∀y∈X. ∀z∈X. ϱ x y ∧ ϱ y z ⟶ ϱ x z) ∧
     (∀C. (C is aCHAIN in X,ϱ) ∧ C ≠ {} ⟶ (∃x. (x is l.u.b. of C in X,ϱ)))"
```

```
— Definition 11(1): (X,σ) is a strictly inductive ARS
— Note that σ^** includes a diagonal relation which may relate
— elements which do not belong to X, but which are of the same type as members of X.
— However, existence of such elements is not significant for this formal definition.
definition is_si_ars ("_,_ is S.I.ARS")
  where "X,σ is S.I.ARS ≡ (X,σ is ARS) ∧ (X,(σ^**) is S.I.PREORDERED)"
```

The notions related to quasi-normal forms are formalized as follows.

```
— Definition 17(1): x is quasi-irreducible in (X,σ)
— assumptions: (X,σ) is ARS and x ∈ X
abbreviation is_qirreduc :: "'a ⇒ 'a set ⇒ ('a ⇒ 'a ⇒ bool) ⇒ bool"
("_ is Q.IRREDUCIBLE in _,_")
  where "x is Q.IRREDUCIBLE in X,σ ≡ ∀y∈X. σ^** x y ⟶ σ^** y x"
```

```
— Definition 17(2): x' is a quasi-normal form of x in (X,σ)
— assumptions: (X,σ) is ARS and x ∈ X
definition is_qnform  ("_ is Q.N.F. of _ in _,_")
  where "x' is Q.N.F. of x in X,σ ≡
        x'∈X ∧ σ^** x x' ∧ (x' is Q.IRREDUCIBLE in X,σ)"
```

```
— Definition 17(3): x,x' are quasi-equivalent in (X,σ)
— assumptions: (X,σ) is ARS and x ∈ X and x' ∈ X
definition are_qequiv  ("_,_ are QNF-EQUIVALENT in _,_")
  where "x,x' are QNF-EQUIVALENT in X,σ ≡
          {y∈X. y is Q.N.F. of x in X,σ} = {y∈X. y is Q.N.F. of x' in X,σ}"

— Definition 18(1): (X,σ) is a quasi-normalizing ARS
definition is_qn_ars  ("_,_ is Q.N.ARS")
  where "X,σ is Q.N.ARS ≡ (X,σ is ARS) ∧
          (∀x∈X. ∃x'∈X. (x' is Q.N.F. of x in X,σ))"

— Definition 18(2): (X,σ) is an openly quasi-normalizing ARS
definition is_oqn_ars  ("_,_ is O.Q.N.ARS")
  where "X,σ is O.Q.N.ARS ≡ (X,σ is Q.N.ARS) ∧
          (∀x∈X. ∀x'∈X. (x' is Q.N.F. of x in X,σ) ⟶
            ({y∈X. σ^** x y ∧ (y,x' are QNF-EQUIVALENT in X,σ)}
              is REL.OPEN SUBSET in {y∈X. σ^** x y} wrt (σ^**)))"
```

Quasi-local confluence is formalized as follows.

```
— A set S satisfies the two-consistency condition in ARS (X,σ)
— assumptions: (X,σ) is ARS and S ⊆ X
definition sat_two_consist_cond ("_ sat.2-CONSISTENCY in _,_")
where
  "S sat.2-CONSISTENCY in X,σ ≡ (∀b∈S. ∀c∈S. ∃d∈X. σ^** b d ∧ σ^** c d)"

— A set S satisfies the coinitiality condition in ARS (X,σ) w.r.t. element a
— assumptions: X,σ is ARS and S ⊆ X and a ∈ X
definition sat_coinit_cond ("_ sat.COINITIALITY in _,_ wrt _")
where
  "S sat.COINITIALITY in X,σ wrt a ≡
     (∀x∈X. σ^++ a x ⟶ ((σ^** x a) ∨ (∃b∈S. σ^** b x ∧ ¬ (σ^** b a))))"

— Definition 24: (X,σ) is a quasi-locally confluent ARS
definition is_qlconfl_ars  ("_,_ is Q.L.CONFLUENT ARS")
  where "X,σ is Q.L.CONFLUENT ARS ≡ (X,σ is ARS) ∧
        (∀a∈X. ∃ S ⊆ {x∈X. σ^++ a x}.
        (S sat.2-CONSISTENCY in X,σ) ∧ (S sat.COINITIALITY in X,σ wrt a))"
```

The statement of the main result is formalized as follows.

```
theorem thm_28:
— Theorem 28 (main result, generalized Newman's lemma)
fixes X σ
assumes "X,σ is S.I.ARS"
shows "(X,σ is CONFLUENT ARS) = ((X,σ is O.Q.N.ARS) ∧ (X,σ is Q.L.CONFLUENT ARS))"
```

5 Discussion

From a practical perspective, usual confluence criteria for ARS associated with discrete models of computation can be used in software tools that allow a user to make sure that an output of a nondeterministic program does not depend on its execution path. Program nondeterminism is frequently caused by concurrent mode of execution, so such tools can aid automated testing or formal verification of concurrent and distributed software. Similar reasons of nondeterminism exist for models of cyber-physical systems (CPS), however, for such models other sources of nondeterminism may also have significant role, e.g. abstractions and approximations used in dynamical models of physical components of a system can lead to non-uniqueness of solutions of state evolution equations [16]. Thus the reasons of development of confluence checkers for models of CPS can be generally analogous to the reasons of development of such checkers for discrete models of computation. Practical implementation of an automated confluence checker for models of CPS is out of scope of this paper, however, we consider this an important problem which requires further work, and the results obtained in this paper can be used to approach it.

One may question whether the notion of an ARS is adequate for modeling CPS. In our opinion, ARS can be used as an auxiliary model of dynamics for such systems, assuming that a reduction relation or its transitive closure represents a reachability relation on states of a primary dynamical model of a CPS (e.g. described as a hybrid dynamical system, etc.). This type of auxiliary model is most useful when a primary model satisfies a nondeterministic version of Markovian property [28, 12] (an adaptation of the respective notion known from the theory of stochastic processes to nondeterministic dynamical systems without any associated probability measures), which, informally speaking, generalizes (to non-discrete-time cases) the following condition which obviously holds for ARS: the set of possible reduction sequences which begin at a given element x does not depend on how x has been reached. When such a (generalized) property holds for a primary model, a correspondence between various properties of interest of an auxiliary model/ARS (like confluence) and of a primary model becomes particularly simple. Note that many types of (non-discrete-time) models relevant for CPS domain can be represented using nondeterministic dynamical systems which have Markovian property in the mentioned sense [12].

6 Conclusion

We have proposed a criterion of confluence for the class of abstract rewriting systems $(X, \to)$ such that $(X, \to^*)$ is a strictly inductive preordered set, where $\to^*$ is the reflexive transitive closure of the reduction relation $\to$. Ordinary Newman's lemma for terminating abstract rewriting systems can be considered as a corollary of this criterion. However, this criterion can also be applied to a wide class of non-terminating abstract rewriting systems.

We have described a formalization of this criterion in Isabelle proof assistant using HOL logic and have discussed its potential applications.

References

1 An Isabelle/HOL Formalization of Rewriting for Certified Tool Assertions. `http://cl-informatik.uibk.ac.at/isafor/`.

2 Franz Baader and Tobias Nipkow. *Term rewriting and all that.* Cambridge university press, 1999.

3 Radhakisan Baheti and Helen Gill. Cyber-physical systems. *The impact of control technology*, 12(1):161–166, 2011.

4 Pete L. Clark. The instructor's guide to real induction. *Mathematics Magazine*, 92(2):136–150, 2019.

5 Patrick Dehornoy and Vincent van Oostrom. Z, proving confluence by monotonic single-step upperbound functions. *Logical Models of Reasoning and Computation (LMRC-08)*, page 85, 2008.

6. Jörg Endrullis, Jan Willem Klop, and Roy Overbeek. Decreasing diagrams with two labels are complete for confluence of countable systems. In *3rd International Conference on Formal Structures for Computation and Deduction (FSCD 2018)*. Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik, 2018.
7. Jörg Endrullis, Jan Willem Klop, and Roy Overbeek. Decreasing diagrams for confluence and commutation. *Logical Methods in Computer Science*, 16, 2020.
8. Rafal Goebel, Ricardo G Sanfelice, and Andrew R Teel. Hybrid dynamical systems. *IEEE control systems magazine*, 29(2):28–93, 2009.
9. Jean Goubault-Larrecq. *Non-Hausdorff topology and domain theory: Selected topics in point-set topology*, volume 22. Cambridge University Press, 2013.
10. Gérard Huet. Confluent reductions: Abstract properties and applications to term rewriting systems. *Journal of the ACM*, 27(4):797–821, 1980.
11. Isabelle proof assistant. `http://isabelle.in.tum.de`. [Online].
12. Ievgen Ivanov. On representations of abstract systems with partial inputs and outputs. In T.V. Gopal, M. Agrawal, A. Li, and S.B. Cooper, editors, *Theory and Applications of Models of Computation*, volume 8402 of *Lecture Notes in Computer Science*, pages 104–123. Springer, 2014.
13. Ievgen Ivanov. On induction for diamond-free directed complete partial orders. In *CEUR-WS.org*, volume 2732, pages 70–73, 2020.
14. Ievgen Ivanov. Formalization of Generalized Newman's Lemma (supplementary material for this paper). `https://doi.org/10.5281/zenodo.7855691`, 2023. [Online].
15. Jan Willem Klop. *Term rewriting systems.* Centrum voor Wiskunde en Informatica, 1990.
16. Edward A. Lee. Fundamental limits of cyber-physical systems modeling. *ACM Transactions on Cyber-Physical Systems*, 1(1), 2016.
17. Philippe Malbos. Lectures on algebraic rewriting. `http://hal.archives-ouvertes.fr/hal-02461874`, 2019.
18. George Markowsky. Chain-complete posets and directed sets with applications. *Algebra universalis*, 6(1):53–68, 1976.
19. F. Mattern. On the relativistic structure of logical time in distributed systems. *Parallel and Distributed Algorithms*, 1992.
20. Maxwell Herman Alexander Newman. On theories with a combinatorial definition of "equivalence". *Annals of mathematics*, pages 223–243, 1942.
21. Newman's lemma — Wikipedia, the free encyclopedia. `http://en.wikipedia.org/Newman_lemma`. [Online].
22. Tobias Nipkow, Markus Wenzel, and Lawrence C Paulson. *Isabelle/HOL: a proof assistant for higher-order logic*. Springer, 2002.
23. André Platzer and Yong Kiam Tan. Differential equation axiomatization: The impressive power of differential ghosts. In *Proceedings of the 33rd Annual ACM/IEEE Symposium on Logic in Computer Science*, pages 819–828, 2018.
24. Jean-Claude Raoult. Proving open properties by induction. *Information processing letters*, 29(1):19–23, 1988.
25. Christian Sternagel and Rene Thiemann. Abstract rewriting. *Archive of Formal Proofs*, June 2010.
26. Vincent van Oostrom. Confluence by decreasing diagrams. *Theoretical computer science*, 126(2):259–280, 1994.
27. Freek Wiedijk. *The seventeen provers of the world: Foreword by Dana S. Scott*, volume 3600. Springer, 2006.
28. J. C. Willems. Paradigms and puzzles in the theory of dynamical systems. *IEEE Transactions on Automatic Control*, 36(3):259–294, 1991.
29. Harald Zankl. Decreasing diagrams. *Archive of Formal Proofs*, 2013.