Searching for Invariants using Temporal Resolution*

James Brotherston[1], Anatoli Degtyarev[2], Michael Fisher[2], and Alexei Lisitsa[2]

[1] Division of Informatics, University of Edinburgh, Edinburgh EH1 1HN, U.K.
jjb@dai.ed.ac.uk
[2] Department of Computer Science, University of Liverpool, Liverpool L69 7ZF, U.K.
{A.Degtyarev,M.Fisher,A.Lisitsa}@csc.liv.ac.uk

Abstract. In this paper, we show how the clausal temporal resolution technique developed for temporal logic provides an effective method for searching for invariants, and so is suitable for mechanising of the wide class of temporal problems. We demonstrate that this scheme of searching for invariants can be also applied to a class of multi-predicate induction problems represented by mutually recursive definitions. Completeness of the approach, examples of the application of the scheme, and overview of the implementation are described.

1 Introduction

The identification of invariants within complex, often inductive, system descriptions, is a vital component within the area of program verification. However, identifying such invariants is often particularly complex. We are here concerned with finding invariants in a class of multi-predicate recursive definitions by translation of the problem to first-order temporal logic followed by application of a clausal temporal resolution method. It has been known for some time that first-order temporal logic over the Natural numbers (FOLTL, in short) is incomplete [Sza86]; that is, there exists no finitistic inference system which is sound and complete for this logic or, equivalently, the set of valid formulae of the logic is not recursively enumerable. The complete Gentzen-like proof systems for FOLTL contain the ω-type infinitary rule of inference [Kaw87]:

$$\frac{\Gamma \to \Delta, \psi; \quad \Gamma \to \Delta, \bigcirc\psi; \quad \dots \quad \Gamma \to \Delta, \bigcirc^n\psi; \quad \dots}{\Gamma \to \Delta, \Box\psi} \ (\to \Box_\omega)$$

However in some cases (in particular, in the propositional case [Pae88]), instead of the ω-type rule $(\to \Box_\omega)$ the following finitary rule can be used:

$$\frac{\Gamma \to \Delta, I; \qquad I \to \bigcirc I; \qquad I \to \psi}{\Gamma \to \Delta, \Box\psi} \ (\to \Box)$$

This rule corresponds to the induction axiom within temporal logic: $\psi \wedge \Box(\psi \supset \bigcirc\psi) \Rightarrow \Box\psi$. The formula I is called an *invariant* formula and has a close relation with invariant formulae in the logic of programs and dynamic logics. Even in the propositional case, the search for such invariants can be very expensive. It is quite a usual situation (e.g.

* Work supported by EPSRC grants GR/M46624, GR/M46631 and GR/R45367.

in Hoare logic for the partial correctness of *while*-programs) that the invariant has to be stronger than the desired conclusion suggests.

To illustrate the difficulties in searching for invariants let us consider an example. The sequent $P(c)$, $\Box\forall x(P(x) \supset \bigcirc P(f(x)) \rightarrow \Box\exists y P(y)$ can be proved using as an invariant the formula $I = \Box(\exists x P(x) \supset \bigcirc\exists x P(f(x))) \wedge \exists x P(x)$. At the same time the most plausible conjecture is that there is no invariant for the sequent $P(c), \forall x(P(x) \supset P(f(x))$, $\Box\forall x(P(f(x)) \supset \bigcirc P(x)) \rightarrow \Box\exists y P(y)$. In both these cases our arguments are heuristic since both sequents lie outside of any known complete fragment of FOLTL.

Recently, the interesting *monodic* fragment of first-order temporal logic has been investigated [HWZ00], which has a quite transparent (and intuitive) syntactic definition and a finite Hilbert-like inference system [WZ01]. In [DF01] a clausal temporal resolution procedure has been developed covering a special subclass of the monodic fragment, namely the subclass of *ground eventuality* monodic problems. In this paper we apply the clausal resolution method in order to give a sound and complete scheme for searching for invariants for sequents of the form $SP \rightarrow \Box\psi$ where SP is a monodic *temporal specification* and ψ is a ground first-order formula.

There is some similarity between linear temporal logic over the Natural numbers and Peano arithmetic. The induction axiom of Peano arithmentic $\varphi(0) \wedge \forall n(\varphi(n) \supset \varphi(s(n)) \Rightarrow \forall n\varphi(n)$ corresponds to the induction axiom within temporal logic, and there is a complete and consistent Gentzen-like proof system for Peano arithmentic where the induction axiom is replaced by an ω-type inference rule $(\rightarrow \forall_{\omega})$ similar to $(\rightarrow \Box_{\omega})$. Because of that we will refer to the temporal problem $SP \rightarrow \Box\psi$ mentioned above as a *(ground) induction problem* (taking into account that a formula ψ under $\Box$ is ground).

An important aspect of this paper is that we particularly consider a class of induction problems over the Natural numbers with *mutually recursive* predicate definitions. Such recursion is difficult for many systems to work with effectively, often leading to quite complex and non-trivial induction schemes (see, for example, [BS00] where the use of mutually recursive definitions has been investigated and several *heuristic* multi-predicate induction schemes have been worked out in order to make implementations of such definitions useful). If such a problem with mutually recursive definitions is translated into a monodic ground induction problem than we can automate its proof, using our invariant scheme. This aspect is demonstrated in examples.

Structure of the paper. We split our presentation into two main parts: the first essentially concerns propositional temporal logic; the second targets a fragment of monodic first-order temporal logic [HWZ00, DF01]. While the propositional part is clearly included within the first-order part, we have chosen to introduce this separately in order to give the reader a simpler introduction to the techniques involved. Thus, in §3, we consider this propositional temporal fragment, providing formal justification and a simple example. Then, in §4, we consider first-order monodic ground induction problems, providing both completeness arguments and examples, and, in §5, outline the current state of implementation. Finally, in §6, we provide concluding remarks.

2 Preliminaries

We consider the first-order temporal logic over the Natural numbers $TL(\mathbb{N})$ in a first-order temporal language $\mathcal{TL}$. The language $\mathcal{TL}$ is constructed in the standard way (see i.e. [Fis97, HWZ00]) from a classical (non-temporal) first-order language $\mathcal{L}$ and a set of future-time temporal operators '$\Diamond$' (*sometime*), '$\Box$' (*always*), '$\bigcirc$' (*in the next moment*). Here, $\mathcal{L}$ does not contain equality or functional symbols. Formulae of $\mathcal{L}$ without free variables are called ground formulae. The symbol $\vdash$ denotes derivability in first-order classical logic.

Formulae in $\mathcal{TL}$ are interpreted in *first-order temporal structures* of the form $\mathfrak{M} = \langle D, I \rangle$, where D is a non-empty set, the *domain* of $\mathfrak{M}$, and I is a function associating with every moment of time $n \in \mathbb{N}$ an interpretation of predicate and constant symbols of $\mathcal{L}$ over D. First-order (nontemporal) structures corresponding to each point of time n will be denoted by $\mathfrak{M}_n = \langle D, I_n \rangle$ where $I_n = I(n)$. Intuitively, the interpretations of $\mathcal{TL}$-formulae are sequences of *worlds* such as $\mathfrak{M}_0, \mathfrak{M}_1, \ldots, \mathfrak{M}_n \ldots$. An *assignment* in D is a function $\mathfrak{a}$ from the set $\mathcal{L}_v$ of individual variables of $\mathcal{L}$ to D. We require that (individual) variables and constants of $\mathcal{TL}$ are *rigid*, that is neither assignments nor interpretations of constants depend on worlds.

The *truth-relation* $\mathfrak{M}_n \models^{\mathfrak{a}} \varphi$ (or simply $n \models^{\mathfrak{a}} \varphi$, if $\mathfrak{M}$ is understood) in the structure $\mathfrak{M}$ for the assignment $\mathfrak{a}$ is defined inductively in usual way under the following semantics of temporal operators:

$$
\begin{array}{lll}
n \models^{\mathfrak{a}} \bigcirc\varphi & \text{iff} & n+1 \models^{\mathfrak{a}} \varphi; \\
n \models^{\mathfrak{a}} \Diamond\varphi & \text{iff} & \text{there exists a } m \geq n \text{ such that } m \models^{\mathfrak{a}} \varphi; \\
n \models^{\mathfrak{a}} \Box\varphi & \text{iff} & m \models^{\mathfrak{a}} \varphi \text{ for all } m \geq n.
\end{array}
$$

A formula φ is said to be *satisfiable* if there is a first-order structure $\mathfrak{M}$ and an assignment $\mathfrak{a}$ such that $\mathfrak{M}_0 \models^{\mathfrak{a}} \varphi$. If $\mathfrak{M}_0 \models^{\mathfrak{a}} \varphi$ for every structure $\mathfrak{M}$ and for all assignments, then φ is said to be *valid*. Note that formulae here are interpreted in the initial world $\mathfrak{M}_0$; that is an alternative but equivalent definition to the one used in [HWZ00].

We will begin by considering an invariant scheme over formulae corresponding to propositional temporal logic. In that case any temporal structure is represented only by the interpretation function I.

3 Propositional invariant scheme

We are here interested in a proof search method (an invariant scheme) for problems which are represented in the form $SP \models \Box\psi$, where ψ is a propositional formula (without temporal operators) and SP is a temporal specification defined below. In what follows we will not distinguish between a finite set of formulae $\mathcal{X}$ and the conjunction $\bigwedge \mathcal{X}$ of formulae within it.

Definition 1 (propositional temporal specification). *A propositional* temporal specification *SP is a triple* $< \mathcal{U}, \mathcal{S}, \mathcal{T} >$ *where*

– $\mathcal{U}$ *is the set of* universal formulae*, that is propositional formulae which are valid in every state* $n \in \mathbb{N}$ *(ensured in temporal logic by the '* $\Box$*').*
– $\mathcal{S}$ *is the set of* initial formulae*, that is propositional formulae which are true only in the initial state* $0 \in \mathbb{N}$*.*
– $\mathcal{T}$ *is the set of* step formulae *(sometimes termed* temporal or step rules*), that is a set of the formulae of the form* $p \Rightarrow \bigcirc r$ *which are true in every state* $n \in \mathbb{N}$*. Here* p *is a proposition symbol (atom),* r *is propositional formula, and* $\Rightarrow$ *is a substitute for implication. Without loss of generality we suppose that there are no two different temporal step rules with the same left-hand sides.*
– *The formula* $\Box\mathcal{U} \wedge \mathcal{S} \wedge \Box\mathcal{T}$ *is called a formula image of SP. When we refer to validity, satisfiability, logical consequences and such like of a temporal specification we mean its formula image.*

The intuitive meaning of a temporal specification $SP = < \mathcal{U}, \mathcal{S}, \mathcal{T} >$ is that a temporal interpretation I satisfies SP if $I \models \Box\mathcal{U} \wedge \mathcal{S} \wedge \Box\mathcal{T}$. Two temporal specifications, SP_1 and SP_2, are said to be equivalent if $I \models SP_1$ if, and only if, $I \models SP_2$ for any temporal interpretation I.

We will prove $SP \models \Box\psi$ using an invariant rule slightly different from that given earlier:

$$\frac{SP \to \psi \wedge I \qquad I \to \bigcirc I \qquad I \to \bigcirc\psi}{SP \to \Box\psi}\ (\to \Box) \tag{1}$$

Our scheme for searching for an invariant formula I starts with transferring SP into so-called reduced temporal specification.After that an analogue of the temporal resolution rule [DF00, DFK02] is applied. At both stages we work with some generalisations of step rules, namely with *merged step rules based on* $\mathcal{T}$ [FDP01] of the form

$$\bigwedge_{i=1}^{n} p_i \Rightarrow \bigcirc \bigwedge_{i=1}^{n} r_i$$

where $(p_i \Rightarrow \bigcirc r_i) \in \mathcal{T}$ for all $1 \le i \le n$, and $n \ge 0$. If $n = 0$ the degenerate merged rule **true** $\Rightarrow \bigcirc$**true** is produced. Clearly, that every merged step rule based on $\mathcal{T}$ is a logical consequence of $\mathcal{T}$.

Definition 2 (ψ-favourable set of merged rules). *A set of merged step rules* $\mathcal{G} = \{A_1 \Rightarrow \bigcirc B_1, \ldots, A_m \Rightarrow \bigcirc B_m\}$ *is called* ψ-favourable with respect to $\mathcal{U}$ *for some propositional formula* ψ*, if the following conditions are satisfied:*

1. $\mathcal{U} \wedge B_j \vdash \psi$ *for all* $1 \le j \le m$*;* *2.* $\mathcal{U} \wedge B_j \vdash \bigvee_{i=1}^{m} A_i$ *for all* $1 \le j \le m$*.*

It is easy to see that if a set $\mathcal{G} = \{A_1 \Rightarrow \bigcirc B_1, \ldots, A_m \Rightarrow \bigcirc B_m\}$ is ψ-favourable with respect to $\mathcal{U}$ then $\Box\mathcal{G} \wedge \Box\mathcal{U} \models (\bigvee_{i=1}^{m} A_i \supset \bigcirc \Box\psi)$. The formula $\Box\mathcal{G} \wedge \Box\mathcal{U} \wedge \bigvee_{i=1}^{m} A_i$ can be taken as a invariant formula for solving the problem $SP \models \Box\psi$ under the condition that $\mathcal{S} \wedge \mathcal{U} \vdash (\psi \wedge \bigvee_{i=1}^{m} A_i)$.

Theorem 1 (correctness of the invariant scheme). *Let $SP =< \mathcal{U},\mathcal{S},\mathcal{T} >$ be a temporal specification, ψ be a propositional formula, and there exists a ψ-favourable set of merged rules $\mathcal{G} = \{A_1 \Rightarrow \bigcirc B_1,\ldots,A_m \Rightarrow \bigcirc B_m\}$ based on $\mathcal{T}$ such that $\mathcal{S} \wedge \mathcal{U} \vdash (\psi \wedge \bigvee_{i=1}^{m} A_i)$. Then $SP \models \Box\psi$.*

Proof Let us take as an invariant I in (1) the formula $\Box\mathcal{G} \wedge \Box\mathcal{U} \wedge \bigvee_{i=1}^{m} A_i$. Now we must prove that every sequent in the premise of this inference becomes valid after such substitution:

- $\models SP \to \psi \wedge I$ in accordance with the condition of the theorem that $\mathcal{S} \wedge \mathcal{U} \vdash (\psi \wedge \bigvee_{i=1}^{m} A_i)$ and taking into account that $\mathcal{T} \models \mathcal{G}$;
- $\models I \to \bigcirc I$ because $\Box\mathcal{G} \wedge \Box\mathcal{U} \wedge \bigvee_{i=1}^{m} A_i$ implies $\Box\mathcal{G} \wedge \Box\mathcal{U} \wedge \bigcirc \bigvee_{i=1}^{m} B_i$, and $\Box\mathcal{G} \wedge \Box\mathcal{U} \wedge \bigcirc \bigvee_{i=1}^{m} B_i$ implies $\Box\mathcal{G} \wedge \Box\mathcal{U} \wedge \bigcirc \bigvee_{i=1}^{m} A_i$ in accordance with ψ-*favourability* of $\mathcal{G}$, and $\Box\mathcal{G} \wedge \Box\mathcal{U} \wedge \bigcirc \bigvee_{i=1}^{m} A_i$ implies $\bigcirc(\Box\mathcal{G} \wedge \Box\mathcal{U} \wedge \bigvee_{i=1}^{m} A_i)$;
- $\models I \to \bigcirc\psi$ because $\Box\mathcal{G} \wedge \Box\mathcal{U} \wedge \bigvee_{i=1}^{m} A_i$ implies $\Box\mathcal{G} \wedge \Box\mathcal{U} \wedge \bigvee_{i=1}^{m} \bigcirc B_i$, and $\Box\mathcal{G} \wedge \Box\mathcal{U} \wedge \bigvee_{i=1}^{m} \bigcirc B_i$ implies $\bigcirc\psi$ in accordance with ψ-*favourability* of $\mathcal{G}$. ❑

What remains is to construct ψ-favourable sets of merged rules.

Definition 3 (reduced temporal specification). *A temporal specification $SP = < \mathcal{U},\mathcal{S}, \mathcal{T} >$ is said to be reduced if, for any merged rule $A \Rightarrow \bigcirc B$ based on $\mathcal{T}$, the following condition is satisfied: if $\mathcal{U} \wedge B \vdash \bot$ then $\mathcal{U} \wedge A \vdash \bot$.*

The sense of reducing is explained further in Lemma 5 and Corollary 1. Every temporal specification SP is transformed into an equivalent reduced temporal specification, SP', using the following lemma:

Lemma 1. *Let $SP =< \mathcal{U},\mathcal{S},\mathcal{T} >$ be a temporal specification, and $\{A \Rightarrow \bigcirc B\}$ be a merged rule based on $\mathcal{T}$ such that $\mathcal{U} \wedge B \vdash \bot$. Then the specification $SP' = < \mathcal{U} \cup \{\neg A\},\mathcal{S},\mathcal{T} >$ is equivalent to SP.*

The first-order version of this lemma, Lemma 6, is proved in §4.
It is clear that, due to finiteness of the set of merged rules, every temporal specification becomes reduced after a finite number of the steps defined in the previous lemma.

Theorem 2 (completeness of the invariant scheme). *Let $SP =< \mathcal{U},\mathcal{S},\mathcal{T} >$ be a reduced temporal specification and ψ be a propositional formula. If $\Box\psi$ is a (temporal) logical consequence of SP, i.e $SP \models \Box\psi$, then there exists a set of merged rules $\{A_1 \Rightarrow \bigcirc B_1,\ldots,A_m \Rightarrow \bigcirc B_m\}$ based on $\mathcal{T}$ such that this set is ψ-favourable w.r.t. $\mathcal{U}$ and $\mathcal{S} \wedge \mathcal{U} \vdash \psi \wedge (\bigvee_{j=1}^{m} A_i)$.*

In §4 the completeness of a first-order version of the invariant scheme will be proved, such that Theorem 2 will be a partial case of it.

Example 1. Consider predicates *even* and *odd* defined over the Natural numbers, where the type of Natural numbers is constructed in the usual way by the constant 0 and the free constructor s (successor): $even(0) \wedge odd(s(0)), even(n) \supset even(s(s(n))), odd(n) \supset odd(s(s(n)))$. Suppose we wish to prove the following property: $\forall n(even(n) \vee odd(n))$.

To represent this problem in our propositional temporal logic format let us introduce two propositional symbols p and q intuitively meaning that $p^{I(n)} \approx even(n)$ and $q^{I(n)} \approx odd(n)$ in an intended temporal interpretation I, and two auxiliary propositional symbols p_1 and q_1. Then this interpretation is defined by a temporal specification SP with the following components:

$$\mathcal{U} = \emptyset, \quad \mathcal{S} = \left\{ \text{s1. } p \wedge q_1 \right\}, \quad \mathcal{T} = \left\{ \begin{array}{l} \text{t1. } q \Rightarrow \bigcirc q_1, \ \text{t2. } q_1 \Rightarrow \bigcirc q \\ \text{t3. } p \Rightarrow \bigcirc p_1, \text{t4. } p_1 \Rightarrow \bigcirc p \end{array} \right\}.$$

New symbols p_1 and q_1 have been introduced to rename formulae $\bigcirc p$ and $\bigcirc q$, correspondingly. Such renaming is required to obtain a standard representation of a temporal specification. The property to be checked is expressed by the formula $\Box(p \vee q)$. The specification SP is reduced and we can apply Theorem 1 immediately taking as a $(p \vee q)$-favourable (w.r.t. $\emptyset$) set of merged rules the pair $\{q \wedge p_1 \Rightarrow \bigcirc(q_1 \wedge p), p \wedge q_1 \Rightarrow \bigcirc(p_1 \wedge q)\}$. The premises of Theorem 1 are satisfied because of $(p \wedge q_1) \vdash (p \vee q)$ and $(p \wedge q_1) \vdash ((q \wedge p_1) \vee (p \wedge q_1))$. Therefore $SP \models \Box(p \vee q)$ and the formula $I = ((q \wedge p_1) \vee (p \wedge q_1)) \wedge \Box(((q \wedge p_1) \supset \bigcirc(q_1 \wedge p)) \wedge (p \wedge q_1 \supset \bigcirc(p_1 \wedge q)))$ is an invariant.

In the previous example we did not apply any reduction rule. The next example shows that reducing a specification can be necessary sometimes.

Example 2. Let this induction problem be defined by a temporal specification SP with the following components:

$$\mathcal{U} = \emptyset, \quad \mathcal{S} = \left\{ \text{s1. } p \right\}, \quad \mathcal{T} = \left\{ \text{t1. } q \Rightarrow \bigcirc p, \ \text{t2. } p \Rightarrow \bigcirc q, \ \text{t3. } r \Rightarrow \bigcirc \neg p \right\}.$$

Suppose we are interested whether $SP \models \Box(p \vee \neg r)$. The specification SP is not reduced because the right-hand sides of (t1) and (t3) contradict each other, and we cannot find any $(p \vee \neg r)$-favourable (w.r.t. $\emptyset$) set of merged rules satisfying the conditions of Theorem 1. So, according to Lemma 1, we derive a new universal formula $\neg q \vee \neg r$ and add it to $\mathcal{U}$. This new specification $SP' =< \{\text{u1. } \neg q \vee \neg r\}, \mathcal{S}, \mathcal{T} >$ is already reduced, and we can apply Theorem 1, taking as a set of merged rules $(p \vee \neg r)$-favourable w.r.t. $\{\neg q \vee \neg r\}$, the pair of the original step rules $\{q \Rightarrow \bigcirc p, \ p \Rightarrow \bigcirc q\}$. This pair becomes $(p \vee \neg r)$-favourable after extending $\mathcal{U}$ by $(\neg q \vee \neg r)$ because, in particular, $(q \wedge (\neg q \vee \neg r)) \vdash (p \vee \neg r)$. The premises of Theorem 1 are satisfied for the reason that $\mathcal{S} \vdash (p \vee r) \wedge (p \vee q)$. Therefore $SP' \models \Box(p \vee \neg r)$ and the formula $I = (p \vee q) \wedge \Box((p \supset \bigcirc q) \wedge (q \supset \bigcirc p)) \wedge \Box(\neg q \vee \neg r)$ is an invariant.

Notice that the induction problems in both considered examples cannot be resolved by straightforward application of usual (one-step) induction. First example can be tackled by two-step induction, but in general the task of finding an appropriate induction scheme is a work of art [Bun01].

4 First-order invariant scheme

We now consider a more complex invariant scheme corresponding to a fragment of first-order temporal logic. A first-order temporal specification is a triple $< \mathcal{U}, \mathcal{S}, \mathcal{T} >$ where $\mathcal{S}$ and $\mathcal{U}$ are the *universal part* and the *initial part*, respectively, given by finite sets of (nontemporal) first-order formulae, and $\mathcal{T}$ is the *temporal part* given by a finite set of *temporal step formulae*. All formulae are written in $\mathcal{L}$ extended by a set of (unary) predicate and propositional symbols. A temporal step formula has one of the following forms:

$$P(x) \Rightarrow \bigcirc R(x) \qquad \text{(\textit{predicate step formula})},$$
$$p \Rightarrow \bigcirc r \qquad \text{(\textit{propositional step formula})},$$

where P and p are unary (i.e. one-place) predicate symbol and propositional symbol, respectively, $R(x)$ and r are boolean expressions composed from one-place predicates and propositional symbols, respectively. Following [HWZ00] we restrict ourselves only to *monodic* temporal specifications, that is only one free variable is admitted under every temporal operator. Otherwise, the induction problem becomes not only undecidable but not even partially decidable. (Simulating Minsky mashines by formulae of two-variable monadic monodic first-order temporal logic with equality given in [DFL02] can be transformed into simulating them by non-monodic ground induction problems.) Without loss of generality we suppose that there are no two different temporal step rules with the same left-hand sides.

To define first-order merged step rules we introduce the notions of colour schemes and constant distributions [DF01]. Let $\mathcal{P} =< \mathcal{U}, \mathcal{S}, \mathcal{T} >$ be a temporal specification. Let C be the set of constants occurring in $\mathcal{P}$. Let $\mathcal{T}^{\mathbf{P}} = \{P_i(x) \Rightarrow \bigcirc R_i(x), \mid 1 \leq i \leq K\}$ and $\mathcal{T}^{\mathbf{p}} = \{p_j \Rightarrow \bigcirc r_j \mid 1 \leq j \leq k\}$ be the sets of all predicate step rules and all propositional step rules of $\mathcal{T}$, respectively. We suppose that $K \geq 0$ and $k \geq 0$; if $K = 0$ ($k = 0$) it means that the set $\mathcal{T}^{\mathbf{P}}$ ($\mathcal{T}^{\mathbf{p}}$) is empty.

Let $\{P_1, \ldots, P_K, P_{K+1} \ldots, P_M\}$, $0 \leq K \leq M$, and $\{p_1, \ldots, p_k, p_{k+1} \ldots, p_m\}$, $0 \leq k \leq m$, be sets of all (monadic) predicate symbols and propositional symbols, respectively, occurring in $\mathcal{T}$. Let Δ be the set of all mappings from $\{1, \ldots, M\}$ to $\{0,1\}$, and Θ be the set of all mappings from $\{1, \ldots, m\}$ to $\{0,1\}$. An element $\delta \in \Delta$ ($\theta \in \Theta$) is represented by the sequence $[\delta(1), \ldots, \delta(M)] \in \{0,1\}^M$ ($[\theta(1), \ldots, \theta(m)] \in \{0,1\}^m$). Let us call elements of Δ and Θ predicate and propositional *colours*, respectively. Let Γ be a subset of Δ, and θ be an element of Θ, and ρ be a map from C to Γ . A triple (Γ, θ, ρ) is called a *colour scheme*, and ρ is called a *constant distribution*.

Note 1. The notion of the colour scheme came, of course, from the well known method within the decidability proof for the monadic class in classical first-order logic (see, for example, [BGG97]). In our case Γ is the quotient domain (a subset of all possible equivalence classes of predicate values), θ is a propositional valuation, and ρ is a standard interpretation of constants in the domain Γ. We construct quotient structures based only on the predicates and propositions which occur in the temporal part of the specification, because only these symbols are really responsible for the satisfiability of temporal constraints. Besides, we have to consider so-called constant distributions because, unlike the classical case, we cannot eliminate constants replacing them by existentially bound variables – the monodicity property would be lost.

For every colour scheme $\mathcal{C} = \langle \Gamma, \theta, \rho \rangle$ let us construct the formulae $\mathcal{F}_\mathcal{C}$, $\mathcal{A}_\mathcal{C}$, $\mathcal{B}_\mathcal{C}$ in the following way. In the beginning for every $\gamma \in \Gamma$ and for θ introduce the conjunctions:

$$F_\gamma(x) = \bigwedge_{\gamma(i)=1\&i\leq M} P_i(x) \wedge \bigwedge_{\gamma(i)=0\&i\leq M} \neg P_i(x), \qquad F_\theta = \bigwedge_{\theta(i)=1\&i\leq m} p_i \wedge \bigwedge_{\theta(i)=0\&i\leq m} \neg p_i,$$

$$A_\gamma(x) = \bigwedge_{\gamma(i)=1\&i\leq K} P_i(x), \qquad A_\theta = \bigwedge_{\theta(i)=1\&i\leq k} p_i,$$

$$B_\gamma(x) = \bigwedge_{\gamma(i)=1\&i\leq K} R_i(x), \qquad B_\theta = \bigwedge_{\theta(i)=1\&i\leq k} r_i.$$

Now $\mathcal{F}_\mathcal{C}$, $\mathcal{A}_\mathcal{C}$, $\mathcal{B}_\mathcal{C}$ are of the following forms

$$\mathcal{F}_\mathcal{C} = \bigwedge_{\gamma\in\Gamma} \exists x F_\gamma(x) \wedge F_\theta \wedge \bigwedge_{c\in C} F_{\rho(c)}(c) \wedge \forall x \bigvee_{\gamma\in\Gamma} F_\gamma(x),$$

$$\mathcal{A}_\mathcal{C} = \bigwedge_{\gamma\in\Gamma} \exists x A_\gamma(x) \wedge A_\theta \wedge \bigwedge_{c\in C} A_{\rho(c)}(c) \wedge \forall x \bigvee_{\gamma\in\Gamma} A_\gamma(x),$$

$$\mathcal{B}_\mathcal{C} = \bigwedge_{\gamma\in\Gamma} \exists x B_\gamma(x) \wedge B_\theta \wedge \bigwedge_{c\in C} B_{\rho(c)}(c) \wedge \forall x \bigvee_{\gamma\in\Gamma} B_\gamma(x).$$

We can consider the formula $\mathcal{F}_\mathcal{C}$ as a 'categorical' formula specification of a quotient structure given by a colour scheme. In turn, the formula $\mathcal{A}_\mathcal{C}$ represents the part of this specification which is 'responsible' just for 'transferring' temporal requirements from the current world (quotient structure) to its immediate successors.

Definition 4 (merged step rule). *Let SP be a first-order temporal specification, $\mathcal{C}$ is a colour scheme for SP. Then the clause $(\Box\forall)(\mathcal{A}_\mathcal{C} \Rightarrow \bigcirc\mathcal{B}_\mathcal{C})$ where $\mathcal{A}_\mathcal{C}$ and $\mathcal{B}_\mathcal{C}$ are defined as above is called a* merged step rule *for SP.*

Note that if both sets $\{i \mid i \leq K, \gamma \in \Gamma, \gamma(i) = 1\}$ and $\{i \mid i \leq k, \theta(i) = 1\}$ are empty the rule $(\mathcal{A}_\mathcal{C} \Rightarrow \bigcirc\mathcal{B}_\mathcal{C})$ degenerates to $(\textbf{true} \Rightarrow \bigcirc\textbf{true})$. If a conjunction $A_\gamma(x)$, $\gamma \in \Gamma$, is empty, that is its truth value is **true**, then the formula $\forall x \bigvee_{\gamma\in\Gamma} A_\gamma(x)$ $(\forall x \bigvee_{\gamma\in\Gamma} B_\gamma(x))$ disappears from $\mathcal{A}_\mathcal{C}$ $(\mathcal{B}_\mathcal{C})$. In the propositional case the rule $(\mathcal{A}_\mathcal{C} \Rightarrow \bigcirc\mathcal{B}_\mathcal{C})$ reduces to $(A_\theta \Rightarrow \bigcirc B_\theta)$ which corresponds to the definition of a propositional merged rule given earlier.

We now reproduce results relevant to the particular form of temporal specifications used in [DF01]. Similar to [FDP01] we represent possible interpretations of a temporal specification $< \mathcal{U}, \mathcal{S}, \mathcal{T} >$ via the *behaviour graph* for this specification.

Definition 5 (behaviour graph). *Given a specification $SP = < \mathcal{U}, \mathcal{S}, \mathcal{T} >$ we construct a finite directed graph G as follows. Every node of G is a colour scheme $\mathcal{C}$ for $\mathcal{T}$ such that the set $\mathcal{U} \cup \mathcal{F}_\mathcal{C}$ is satisfiable.*

For each node $\mathcal{C} = (\Gamma, \theta, \rho)$, we construct an edge in G to a node $\mathcal{C}' = (\Gamma', \theta', \rho')$, if $\mathcal{U} \wedge \mathcal{F}_{\mathcal{C}'} \wedge \mathcal{B}_\mathcal{C}$ is satisfiable. They are the only edges originating from $\mathcal{C}$.

A node $\mathcal{C}$ is designated as an initial node of G if $\mathcal{S} \wedge \mathcal{U} \wedge \mathcal{F}_\mathcal{C}$ is satisfiable.

The behaviour graph *H of SP is the full subgraph of G given by the set of all nodes reachable from the initial nodes.*

It is easy to see that there is the following relation between behaviour graphs of two temporal specifications when one of them is obtained by extending the universal part of another one.

Lemma 2. *Let $SP_1 = < \mathcal{U}_1, \mathcal{S}, \mathcal{T} >$ and $SP_2 = < \mathcal{U}_2, \mathcal{S}, \mathcal{T} >$ be two $\mathcal{TL}$ specifications such that $\mathcal{U}_1 \subseteq \mathcal{U}_2$. Then the behaviour graph H_2 of SP_2 is a subgraph of the behaviour graph H_1 of SP_1.*

Proof The graph H_2 is the full subgraph of H_1 given by the set of nodes whose interpretations satisfy $\mathcal{U}_2$ and which are reachable from the initial nodes of H_1 whose interpretations also satisfy $\mathcal{U}_2$. ❑

Definition 6 (suitable pairs). *Let $(\mathcal{C}, \mathcal{C}')$ where $\mathcal{C} = (\Gamma, \theta, \rho)$, $\mathcal{C}' = (\Gamma', \theta', \rho')$ be an (ordered) pair of colour schemes for $\mathcal{T}$. An ordered pair of predicate colours (γ, γ') where $\gamma \in \Gamma$, $\gamma' \in \Gamma'$ is called* suitable *if the formula $\mathcal{U} \wedge F_{\gamma'}(x) \wedge B_\gamma(x)$ is satisfiable. Similarly, the ordered pair of propositional colours (θ, θ') is suitable if $\mathcal{U} \wedge F_{\theta'} \wedge B_\theta$ is satisfiable. The ordered pair of constant distributions (ρ, ρ') is called suitable if, for every $c \in C$, the pair $(\rho(c), \rho'(c))$ is suitable.*

Let us note that the satisfiability of $F_{\gamma'}(x) \wedge B_\gamma(x)$ implies $F_{\gamma'}(x) \vdash B_\gamma(x)$ because the conjunction $F_{\gamma'}(x)$ contains a valuation at x of all predicates occurring in the expression $B_\gamma(x)$.

Lemma 3. *Let H be the behaviour graph of a specification $< \mathcal{U}, \mathcal{S}, \mathcal{T} >$ with an edge from a node $\mathcal{C} = (\Gamma, \theta, \rho)$ to a node $\mathcal{C}' = (\Gamma', \theta', \rho')$. Then*

- *for every $\gamma \in \Gamma$ there exists $\gamma' \in \Gamma'$ such that the pair (γ, γ') is suitable;*
- *for every $\gamma' \in \Gamma'$ there exists $\gamma \in \Gamma$ such that the pair (γ, γ') is suitable;*
- *the pair of propositional colours (θ, θ') is suitable;*
- *the pair of constant distributions (ρ, ρ') is suitable.*

Proof From the definition of a behaviour graph it follows that $\mathcal{U} \wedge \mathcal{F}_{\mathcal{C}'} \wedge \mathcal{B}_{\mathcal{C}}$ is satisfiable. Now to prove the first item it is enough to note that satisfiability of the expression $\mathcal{U} \wedge \mathcal{F}_{\mathcal{C}'} \wedge \mathcal{B}_{\mathcal{C}}$ implies satisfiability of $\mathcal{U} \wedge (\forall x \bigvee_{\gamma' \in \Gamma'} F_{\gamma'}(x)) \wedge \exists x B_\gamma(x)$. This, in turn, implies satisfiability of its logical consequence $\mathcal{U} \wedge \bigvee_{\gamma' \in \Gamma'} \exists x (F_{\gamma'}(x) \wedge B_\gamma(x))$. So, one of the members of this disjunction must be satisfiable. The second item follows from the satisfiability of $\mathcal{U} \wedge (\forall x \bigvee_{\gamma \in \Gamma} B_\gamma(x)) \wedge \exists x F_{\gamma'}(x)$. Other items are similar. ❑

Let H be the behaviour graph of a specification $< \mathcal{U}, \mathcal{S}, \mathcal{T} >$ and $\Pi = \mathcal{C}_0, \ldots, \mathcal{C}_n, \ldots$ be a path in H where $\mathcal{C}_i = (\Gamma_i, \theta_i, \rho_i)$. Let $\mathcal{G}_0 = \mathcal{S} \cup \{\mathcal{F}_{\mathcal{C}_o}\}$ and $\mathcal{G}_n = \mathcal{F}_{\mathcal{C}_n} \wedge \mathcal{B}_{\mathcal{C}_{n-1}}$ for $n \geq 1$. According to the definition of a behaviour graph the set $\mathcal{U} \cup \{\mathcal{G}_n\}$ is satisfiable for every $n \geq 0$. According to classical model theory, since the language $\mathcal{L}$ is countable and does not contain equality the following lemma holds.

Lemma 4. *Let κ be a cardinal, $\kappa \geq \aleph_0$. For every $n \geq 0$, if a set $\mathcal{U} \cup \{\mathcal{G}_n\}$ is satisfiable, then there exists an $\mathcal{L}$-model $\mathfrak{M}_n = \langle D, I_n \rangle$ of $\mathcal{U} \cup \{\mathcal{G}_n\}$ such that for every $\gamma \in \Gamma_n$ the set $D_{(n,\gamma)} = \{a \in D \mid \mathfrak{M}_n \models F_\gamma(a)\}$ is of cardinality κ.*

Definition 7 (run). *By a* run *in* Π *we mean a function from* $\mathbb{N}$ *to* $\bigcup_{i \in \mathbb{N}} \Gamma_i$ *such that for every* $n \in \mathbb{N}$*,* $r(n) \in \Gamma_n$ *and the pair* $(r(n), r(n+1))$ *is suitable.*

It follows from the definition of H that for every $c \in C$ the function r_c defined by $r_c(n) = \rho_n(c)$ is a run in Π.

Theorem 3. *Let* $< \mathcal{U}, \mathcal{S}, \mathcal{T} >$ *be a satisfiable temporal specification. Then there exists an infinite path* $\Pi = \mathcal{C}_0, \ldots, \mathcal{C}_n, \ldots$ *through the behaviour graph* H *for* $< \mathcal{U}, \mathcal{S}, \mathcal{T} >$ *where* $\mathcal{C}_0$ *is an initial node of* H*.*

A proof of this theorem is given in Appendix A.

Theorem 4. *Let* $\Pi = \mathcal{C}_0, \ldots, \mathcal{C}_n, \ldots$ *be an infinite path through the behaviour graph* H *for a temporal specification* $SP =< \mathcal{U}, \mathcal{S}, \mathcal{T} >$*,* $\mathcal{C}_0$ *is an initial node of* H*. Then there exists a model* $\mathfrak{M} = \langle D, I \rangle$ *of* SP*.*

A proof of this theorem is given in Appendix A.
So, all models of a specification $SP =< \mathcal{U}, \mathcal{S}, \mathcal{T} >$ are represented by infinite paths through the behaviour graph for SP. Moreover, it is clear that the following relation between an infinite path $\Pi = \mathcal{C}_0, \ldots, \mathcal{C}_n, \ldots$ through the behaviour graph H for SP and the set of models $\mathfrak{M} = \langle D, I \rangle$ defined by Theorems 4 holds: for every propositional symbol p and for every $n \in \mathbb{N}$ there exist a model $\mathfrak{M} = \langle D, I \rangle$ such that $\mathfrak{M}_n \models p$ if, and only if, the set $\mathcal{U} \cup \{F_{\mathcal{C}_n}, p\}$ is satisfiable. The same is true if we take instead of a propositional symbol p any ground formula.

Now we are interested in an invariant scheme for problems of the form $SP \models \Box\psi$, where $SP =< \mathcal{U}, \mathcal{S}, \mathcal{T} >$ is a monodic first-order temporal specification, and ψ is a ground formula. The first step, the same as in the propositional case, is to transform SP into an equivalent reduced specification.

We note that the definitions of ψ-*favourable sets of merged rules* and *reduced temporal specifications* carry over from the earlier propositional definitions.

Our interest in reduced specifications is caused by the following lemma.

Lemma 5. *Let* $SP =< \mathcal{U}, \mathcal{S}, \mathcal{T} >$ *be a reduced temporal specification and the behaviour graph* H *for* SP *be nonempty. Then all paths in* H *are infinite.*

Proof Suppose there is a path through H which is finite, that is there is a node $\mathcal{C}$ on this path which has no successors. In this case the set $\mathcal{U} \cup \{\mathcal{B}_\mathcal{C}\}$ is unsatisfiable. Indeed, suppose $\mathcal{U} \cup \{\mathcal{B}_\mathcal{C}\}$ is satisfiable, and $\langle D', I' \rangle$ is a model of $\mathcal{U} \cup \{\mathcal{B}_\mathcal{C}\}$. Then following the proof of Theorem 4 we can define a colour scheme $\mathcal{C}'$ such that $\langle D', I' \rangle \models \mathcal{F}_{\mathcal{C}'}$. Since $\mathcal{B}_\mathcal{C} \wedge \mathcal{F}_{\mathcal{C}'}$ is satisfiable there is an edge from the node $\mathcal{C}$ to the node $\mathcal{C}'$ in the contradiction with the choice of $\mathcal{C}$ as having no successors. So, $\mathcal{U} \cup \{\mathcal{B}_\mathcal{C}\}$ is unsatisfiable. Since the specification is reduced the set $\mathcal{U} \cup \{\mathcal{A}_\mathcal{C}\}$ also has to be unsatisfiable. However it contradicts the existence of $\mathcal{C}$. ❏

This lemma, together with Theorem 4, immediately implies the following.

Corollary 1. *A reduced temporal specification* $SP =< \mathcal{U}, \mathcal{S}, \mathcal{T} >$ *is satisfiable if, and only if, the set* $\mathcal{U} \cup \mathcal{S}$ *is satisfiable.*

Proof The behaviour graph H for SP is not empty because the set of its initial nodes is not empty. ❑

Every temporal specification SP_1 is transformed into an equivalent reduced temporal specification SP_2 using the following lemma (the first-order version of Lemma 1):

Lemma 6. *Let $SP_1 =< \mathcal{U}, \mathcal{S}, \mathcal{T} >$ be a temporal specification, and $\mathcal{A} \Rightarrow \bigcirc\mathcal{B}$ be a merged rule based on $\mathcal{T}$ such that $\mathcal{U} \wedge \mathcal{B} \vdash \perp$. Then the specification $SP_2 = < \mathcal{U} \cup \{\neg\mathcal{A}\}, \mathcal{S}, \mathcal{T} >$ is equivalent to SP_1.*

Proof It is obvious that every model of SP_2 is a model of SP_1. To prove the inverse inclusion suppose an interpretation, $\mathfrak{M} = \langle D, I \rangle$, is a model of SP_1. Then for every $n \in \mathbb{N}$ it holds that $\mathfrak{M}_n \models \neg\mathcal{A}$, otherwise it would be $\mathfrak{M}_{n+1} \models \mathcal{B}$ in contradiction with the condition $\mathcal{U} \wedge \mathcal{B}$ is unsatisfiable. So, $\mathfrak{M}$ is a model of SP_2. ❑

This lemma justifies the following inference rule over temporal specifications.

Definition 8 (reduction rule). *Let $SP =< \mathcal{U}, \mathcal{S}, \mathcal{T} >$ be a temporal specification, and $\mathbf{m}\mathcal{T}$ be the set of merged rules based on $\mathcal{T}$. Then the reduction inference rule has the following form*

$$\frac{< \mathcal{U}, \mathcal{S}, \mathcal{T} >}{< \mathcal{U} \cup \{\neg\mathcal{A}\}, \mathcal{S}, \mathcal{T} >}\ (red)$$

if there is a merged rule $(\mathcal{A} \Rightarrow \bigcirc\mathcal{B}) \in \mathbf{m}\mathcal{T}$ such that the set $\mathcal{U} \cup \{\mathcal{B}\}$ is unsatisfiable.

The saturation of $\mathcal{U}$ by the reduction rule terminates both in the first-order and in the propositional cases because the set of merged rules is always finite. Quite another matter is checking the condition whether $\mathcal{U} \cup \{\mathcal{B}\}$ is unsatisfiable. In general this problem can be undecidable. In order to avoid such situation we have to suppose that the universal part $\mathcal{U}$ of our specification belongs to an arbitrary decidable fragment of first-order logic (one-variable monadic formulae $\neg\mathcal{A}$ and $\mathcal{B}$ cannot affect the decidability). The same supposition relates to checking whether a set of merged rules is ψ-favourable.

The following two lemmas substantiate the invariant scheme which is required. Proofs of both lemmas are given in Appendix B.

Lemma 7. *Let $SP =< \mathcal{U}, \mathcal{S}, \mathcal{T} >$ be a reduced temporal specification and ψ be a ground formula. If $\Box\psi$ is a (temporal) logical consequence of SP, that is $SP \models \Box\psi$, then $\mathcal{S} \cup \mathcal{U} \vdash \psi$.*

Lemma 8. *Let $SP =< \mathcal{U}, \mathcal{S}, \mathcal{T} >$ be a reduced temporal specification and ψ be a ground formula. If $\Box\psi$ is a (temporal) logical consequence of SP, that is $SP \models \Box\psi$, then there exists a set of merged rules $\mathcal{G} = \{\mathcal{A}_1 \Rightarrow \bigcirc\mathcal{B}_1, \ldots, \mathcal{A}_m \Rightarrow \bigcirc\mathcal{B}_m\}$ based on $\mathcal{T}$ such that $\mathcal{G}$ is ψ-favourable w.r.t. $\mathcal{U}$ and $\mathcal{S} \cup \mathcal{U} \vdash \bigvee_{j=1}^{m} \mathcal{A}_i$.*

Theorem 5 (correctness and completeness of the invariant scheme). *Let $SP =< \mathcal{U}, \mathcal{S}, \mathcal{T} >$ be a reduced temporal specification and ψ be a ground formula. Then $\Box\psi$ is a (temporal) logical consequence of SP, that is $SP \models \Box\psi$, if, and only if, $\mathcal{S} \cup \mathcal{U} \vdash \psi$ and there exists a set of merged rules $\mathcal{G} = \{\mathcal{A}_1 \Rightarrow \bigcirc\mathcal{B}_1, \ldots, \mathcal{A}_m \Rightarrow \bigcirc\mathcal{B}_m\}$ based on $\mathcal{T}$ such that $\mathcal{G}$ is ψ-favourable w.r.t. $\mathcal{U}$ and $\mathcal{S} \cup \mathcal{U} \vdash \bigvee_{j=1}^{m} A_i$.*

Proof Completeness is ensured by Lemmas 7 and 8. Correctness is carried from the earlier propositional Theorem 1. ❑

Note 2. The notion of a merged step rule given in Definition 4 and used through all this section seems to be quite involved. However we can note that every such rule is composed from a set of *simplified* merged rules of the form

$$\Box\forall x((P_{i_1}(x) \vee \ldots \vee P_{i_l}(x)) \Rightarrow \bigcirc \forall x(R_{i_1}(x) \vee \ldots \vee R_{i_l}(x)))$$
$$\Box\exists x((P_{j_1}(x) \wedge \ldots \wedge P_{j_m}(x)) \Rightarrow \bigcirc \exists x(R_{j_1}(x) \wedge \ldots \wedge R_{j_m}(x)))$$

for $1 \leq i_1 < \ldots i_l \leq K$, $1 \leq j_1 < \ldots j_l \leq K$ plus the rules of the form $\Box(P_1(c) \Rightarrow \bigcirc R_1(c))$ for every constant c occurring in the given *SP*, $1 \leq i \leq K$. Now we can replace merged rules of Definition 4 (let us call these rules as *canonical* merged step rules) by simplified merged step rules. The only difference related to using simplified merged step rules in inferences concerns the reduction rule (Definition 8), namely instead of a merged step rule we have to take a set of simplified merged step rules. Then we can consider applying canonical merged step rules as a special strategy of using simplified merged step rules.

Example 3. We here give a simple example of multi-predicate mutually recursive definitions, which can be described as follows. Consider the delivery of particular foodstuffs at different moments in time. Here, the predicates $deliver\_wood(b,t)$, $deliver\_eggs(b,t)$ and $deliver\_flour(b,t)$ represent the delivery by 'b' of item wood, eggs or flour, at time 't'. Now, we can specify the problem as follows. First, the initial condition:

1. $\exists x.\ deliver\_wood(x,0)$

Now for the dynamic properties of delivery:

2. $\forall x.\ \forall y.\ deliver\_eggs(x,y) \ \Rightarrow\ deliver\_flour(x,s(y)) \ \vee\ deliver\_wood(x,s(y))$
3. $\forall x.\ \forall y.\ deliver\_wood(x,y) \ \Rightarrow\ deliver\_eggs(x,s(y))$
4. $\forall x.\ \forall y.\ deliver\_flour(x,y) \ \Rightarrow\ deliver\_eggs(x,s(y))$

Note 3. The intuitive meanings of these are that if x delivers eggs then x delivers flour or wood in the next moment, and if x delivers wood or flour then x delivers eggs in the next moment.

Finally, we wish to be able to prove

$$\forall n.\ \exists x.\ \begin{pmatrix} (deliver\_eggs(x,n) \ \wedge\ deliver\_flour(x,s(n))) \ \vee \\ (deliver\_eggs(x,n) \ \wedge\ deliver\_wood(x,s(n))) \ \vee \\ deliver\_eggs(x,s(n)) \end{pmatrix}$$

from all of the above.

To achieve this, we first translate the formulae to temporal logic, giving a specification $< \mathcal{U}, \mathcal{S}, \mathcal{T} >$ where the initial part $\mathcal{S}$ consists of the single formula

s1. $\exists x.\ deliver\_wood(x)$

the universal part $\mathcal{U}$ is empty, and the temporal part $\mathcal{T}$ is the following

t1. $deliver\_eggs(x) \Rightarrow \bigcirc(deliver\_flour(x) \vee deliver\_wood(x))$
t2. $deliver\_wood(x) \Rightarrow \bigcirc deliver\_eggs(x)$
t3. $deliver\_flour(x) \Rightarrow \bigcirc deliver\_eggs(x)$

In renaming the above conclusion to a standard from, we introduce three new predicate symbols, so that the conclusion becomes

$$\Box\, \exists x. \big((deliver\_eggs(x) \wedge \neg B(x)) \vee (deliver\_eggs(x) \wedge \neg C(x)) \vee \neg A(x) \big)$$

or after equivalent transformations it becomes $\Box\psi$ where

$$\psi = \exists x\ (deliver\_eggs(x) \wedge (\neg B(x) \vee \neg C(x)) \vee \exists x \neg A(x).$$

We also add three new rules to the temporal part defining the new predicate symbols

t4. $B(x) \Rightarrow \bigcirc\neg deliver\_flour(x)$
t5. $C(x) \Rightarrow \bigcirc\neg deliver\_wood(x)$
t6. $A(x) \Rightarrow \bigcirc\neg deliver\_eggs(x)$

Now, we consecutively apply the reduction inference rule to merged rules

m1. $\exists x(deliver\_eggs(x) \wedge B(x) \wedge C(x)) \Rightarrow \bigcirc\exists x \begin{pmatrix} (deliver\_flour(x) \vee deliver\_wood(x)) \\ \wedge\, (\neg deliver\_flour(x) \wedge \neg deliver\_wood(x)) \end{pmatrix}$
m2. $\exists x(deliver\_wood(x) \wedge A(x)) \Rightarrow \bigcirc\exists x(deliver\_eggs(x) \wedge \neg deliver\_eggs(x))$
m3. $\exists x(deliver\_flour(x) \wedge A(x)) \Rightarrow \bigcirc\exists x(deliver\_eggs(x) \wedge \neg deliver\_eggs(x))$

deriving the following universal rules, respectively,

u1. $\forall x.\ deliver\_eggs(x) \supset (\neg B(x) \vee \neg C(x))$
u2. $\forall x.\ deliver\_wood(x) \supset \neg A(x)$
u3. $\forall x.\ deliver\_flour(x) \supset \neg A(x)$

The following set of merged rules is ψ-favourable with respect to $\mathcal{U}$ extended by u1,u2,u3:

m4. $\exists x\ deliver\_eggs(x) \Rightarrow \bigcirc\exists x\ (deliver\_flour(x) \vee deliver\_wood(x))$
m5. $\exists x\ deliver\_wood(x) \Rightarrow \bigcirc\exists x\ deliver\_eggs(x)$
m6. $\exists x\ deliver\_flour(x) \Rightarrow \bigcirc\exists x\ deliver\_eggs(x)$

Establishing $\mathcal{S} \cup \mathcal{U} \vdash \psi \wedge \exists x\ (deliver\_eggs(x) \vee deliver\_wood(x) \vee deliver\_flour(x))$ is quite straitforward. So, all the conditions of Theorem 5 are satisfied.

5 Implementation.

The method described in this paper has been implemented as a part of a prototype prover for temporal specifications in the λ*Clam* envinronment [RSG98]. λ*Clam* is a proof planning [Bun88] system, implemented in Teyjus λProlog, a higher-order typed logic programming language. A proof plan is a representation of a proof at some level of abstraction (usually above the level of basic inference rules, but not necessarily so). In λ*Clam* a proof plan is generated from a goal by the application of planning operators called *proof methods*. Atomic methods are suitable for the implementation of basic proof rules, or automated proof procedures, while compound methods are used to build more complex proof strategies (or heuristics) from atomic methods.

Our system works with arithmetical translations of temporal formulae. For first-order (non-temporal) proving called within the prover an atomic method *proof_tableau* re-implementing the simple, but convenient LeanTap tableaux prover [BP95] in λProlog, is used. The kernel of the system is an atomic method *mutual_induction*, implementing an invariant scheme more general than one discussed above and applicable not only to monodic specifications. Given a set of formulae, *mutual_induction* first separates it into the sets of step rules and the universal and start parts. Then, to ensure the completeness for the case of monodic specifications, three sub-methods are applied.

1. A sub-method for the saturation of the universal part (reduction) given a (not necessarily reduced) specification, applies the reduction rule (see Definition 8) until the specification becomes reduced and the universal part saturated. Simple optimization, based on the fact that any superset of an inconsistent set of formulae is itself inconsistent, is also used.
2. Given a reduced specification, SP, a further sub-method generates all merged rules based on SP (using the representation given in Note 2) and collects only those, whose right-hand side together with the universal part of SP implies the desired conclusion.
3. Given a set, M, of merged rules, generated by the previous method, the sub-method for the loop search iterates over subsets of M and generates subgoals, i.e. first-order formulae to prove, for checking the side conditions (ψ-favourability and initial condition).

Initial experiments have indicated the viability of our approach. The system is capable of proving all the examples mentioned in this paper, together with some (more complex) non-monodic examples.

6 Conclusion

We have shown that the clausal resolution technique developed for temporal logic provides us with a method for searching for invariant formulae, and is particularly suitable for proving ground "always" conclusions of monodic temporal specifications. We have demonstrated that this method can also be applied to the mechanization of multi-predicate induction problems over the Natural numbers with mutually recursive definitions via translating them into temporal logic.

We have established the correctness of such an approach and have given several, necessarily simplified, examples. Part of our future work concerns the extension of this technique to temporal logics over more complex inductively generated structures of time, in particular lists and trees, and the development of corresponding (complete) invariant schemes. Other aspects of future work concern extending the scope of the temporal resolution method and developing more complex invariant schemes within the first-order temporal logic, in particular for the monodic non-ground induction problems and for the numerous induction problems (ground, but non-monodic) considered by Pliuskevicius [Pli00, DFLP02].

As to the implementation, further work is to develop optimizations for the proof search procedure in the monodic case together with strategies/ heuristics applicable to non-monodic specifications.

References

[BGG97] E. Börger, E. Grädel, and Yu. Gurevich. *The Classical Decision Problem*. Springer, 1997.

[BP95] B. Beckert and J. Posegga. leanT^AP: Lean, Tableau-based Deduction. *Journal of Automated Reasoning*, Vol. 15, No. 3, pages 339-358, 1995.

[BS00] R. J. Boulton and K. Slind. Automatic derivation and application of induction schemes for mutually recursive functions. In *Proc. of CL 2000*, volume 1861 of *LNAI*, 2000.

[Bun88] A. Bundy. The use of explicit plans to guide inductive proofs. In *Proc. of 9th International Conference on Automated Deduction* Springer-Verlag, 1988.

[Bun01] A. Bundy. The Automation Of Proof By Mathematical Induction. In A. Robinson and A. Voronkov, editors, *Handbook of Automated Reasoning*, volume 1, pages 845–912. Elsevier Science and MIT Press, 2001.

[DF00] A. Degtyarev and M. Fisher. Propositional temporal resolution revised. In *Proc. of 7th UK Workshop on Automated Reasoning (ARW'00)*. London, U.K., June 2000.

[DF01] A. Degtyarev and M. Fisher. Towards first-order temporal resolution. In *Proccedings of KI-2001*, volume 2174 of *LNAI*, 2001.

[DFL02] A. Degtyarev, M. Fisher and A. Lisitsa. Equality and monodic first-order temporal logic . *Studia Logica*, Vol.72, No.2, 2002.

[DFK02] A. Degtyarev, M. Fisher and B. Konev. Simplified clausal resolution procedure for propositional linear-time temporal logic. To appear in *Proc. of TABLEAUX'02*, 2002.

[DFLP02] A. Degtyarev, M. Fisher, A.Lisitsa and R. Pliuskevicius. Simple decision procedures for non-monodic decidable fragments of FOLTL. In preparation, 2002.

[FDP01] M. Fisher, C. Dixon, and M. Peim. Clausal temporal resolution. *ACM Transactions on Computation Logic*, 2(1), January 2001.

[Fis97] M. Fisher. A normal form for temporal logics and its applications in theorem-proving and execution. *Journal of Logic and Computation*, 7(4), 1997.

[HWZ00] I. Hodkinson, F. Wolter, and M. Zakharyaschev. Fragments of first-order temporal logics. *Annals of Pure and Applied logic*, 106:85–134, 2000.

[Kaw87] H. Kawai. Sequential Calculus for a First Order Infinitary Temporal Logic. *Zeitschrift für Mathematische Logic and Grundlagen der Mathematik*, 33:423-432, 1987.

[Pae88] B. Paech. Gentzen Systems for Propositional Temporal Logics. *Proccedings of CSL'88*, volume 385 of *LNCS*, p.240–253. Springer Verlag, 1988.

[PG86] D. Plaisted and S. Greenbaum. A structure-preserving clause form transformation. *Journal of Symbolic Computation*, 2(3):293–304, September 1986.

[Pli00] R. Pliuskevicius. A decidable deductive procedure for a restricted FTL. In *Proc. of 7th UK Workshop on Automated Reasoning (ARW'00)*. London, U.K., June 2000.

[RSG98] J. Richardson, A. Smaill, and I. Green. System description: proof planning in higher-order logic with lambdaclam. In *Proc. of CADE'15*, volume 1421 of LNAI, 1998.

[Sza86] A. Szalas. Concerning the semantic consequence relation in first-order temporal logic. *Theoretical Computer Science*, 47:329–334, 1986.

[WZ01] F. Wolter and M. Zakharyaschev. Axiomatizing the monodic fragment of first-order temporal logic. To appear in *Annals of Pure and Applied logic.*, 2001.

Appendix A: Proofs of Theorems 3 and 4

Theorem 3. Let $< \mathcal{U}, \mathcal{S}, \mathcal{T} >$ be a satisfiable temporal specification. Then there exists an infinite path $\Pi = \mathcal{C}_0, \ldots, \mathcal{C}_n, \ldots$ through the behaviour graph H for $< \mathcal{U}, \mathcal{S}, \mathcal{T} >$ where $\mathcal{C}_0$ is an initial node of H.

Proof Let $\mathfrak{M} = \langle D, I \rangle$ be a model of $< \mathcal{U}, \mathcal{S}, \mathcal{T} >$. Let us define for every $n \in \mathbb{N}$ the node $(\mathcal{C})$, $\mathcal{C} = (\Gamma_n, \theta_n, \rho_n)$, as follows. For every $a \in D$ let $\gamma_{(n,a)}$ be a map from $\{1, \ldots, M\}$ to $\{0, 1\}$, and let θ_n be a map from $\{1, \ldots, m\}$ to $\{0, 1\}$ such that

$$\gamma_{(n,a)}(i) \rightleftharpoons \begin{cases} 1, & \text{if } \mathfrak{M}_n \models P_i(a), \\ 0, & \text{if } \mathfrak{M}_n \not\models P_i(a) \end{cases} \qquad \theta_n(j) \rightleftharpoons \begin{cases} 1, & \text{if } \mathfrak{M}_n \models p_j, \\ 0, & \text{if } \mathfrak{M}_n \not\models p_j \end{cases}$$

for every $1 \leq i \leq M$ and $1 \leq j \leq m$.

Now we define $\Gamma_n \rightleftharpoons \{\gamma_{(n,a)} \mid a \in D\}$, and $\rho_n(c) \rightleftharpoons \gamma_{(n, c^{I(n)})}$ for every $c \in C$. (Recall that, in accordance with our semantics, all constants are "rigid", that is $c^{I(u)} = c^{I(v)}$ for every $u, v \in \mathbb{N}$.) According to the construction $(\Gamma_n, \theta_n, \rho_n)$ given above we can conclude that the sequence $(\mathcal{C}_0), \ldots, (\mathcal{C}_n), \ldots$ where $\mathcal{C}_n = (\Gamma_n, \theta_n, \rho_n)$, $n \in \mathbb{N}$, is a path through H. ❑

Theorem 4. Let $\Pi = \mathcal{C}_0, \ldots, \mathcal{C}_n, \ldots$ be an infinite path through the behaviour graph H for a temporal specification $SP = < \mathcal{U}, \mathcal{S}, \mathcal{T} >$, $\mathcal{C}_0$ is an initial node of H. Then there exists a model $\mathfrak{M} = \langle D, I \rangle$ of SP.

Proof Following [HWZ00] take a cardinal $\kappa \geq \aleph_0$ exceeding the cardinality of the set $\mathfrak{R}$ of all runs in Π. Let us define a domain $D = \{\langle r, \xi \rangle \mid r \in \mathfrak{R}, \xi < \kappa\}$. So, for every $n \in \mathbb{N}$ it follows that $D = \bigcup_{\gamma \in \Gamma_n} D_{(n,\gamma)}$ where $D_{(n,\gamma)} = \{\langle r, \xi \rangle \in D \mid r(n) = \gamma\}$ and $\mid D_{(n,\gamma)} \mid = \kappa$. Hence by Lemma 4, for every $n \in \mathbb{N}$ there exists an $\mathcal{L}$-structure $\mathfrak{M}_n = \langle D, I_n \rangle$ satisfying $\mathcal{U} \cup \{\mathcal{G}_n\}$ such that $D_{(n,\gamma)} = \{\langle r, \xi \rangle \in D \mid \mathfrak{M}_n \models F_\gamma(\langle r, \xi \rangle)\}$ for every $\gamma \in \Gamma_n$. Moreover, we can suppose that $c^{I_n} = \langle r_c, 0 \rangle$ for every constant c in $\mathcal{L}$. A first-order temporal model that we sought is $\mathfrak{M} = \langle D, I \rangle$ where $I(n) = I_n$ for all $n \in \mathbb{N}$. To be convinced of that let us show validity of an arbitrary step rule $\Box(P_i(x) \Rightarrow \bigcirc R_i(x))$ in $\mathfrak{M}$. Namely, let us show that, for every $n \geq 0$ and for every $\langle r, \xi \rangle \in D$, if $\mathfrak{M}_n \models P_i(\langle r, \xi \rangle)$, then $\mathfrak{M}_{n+1} \models R_i(\langle r, \xi \rangle)$.

Suppose $r(n) = \gamma \in \Gamma_n$ and $r(n+1) = \gamma' \in \Gamma_{n+1}$, where (γ, γ') is a suitable pair in accordance with the definition af a run. It follows that $\langle r, \xi \rangle \in D_{(n,\gamma)}$ and $\langle r, \xi \rangle \in D_{(n+1,\gamma')}$, in other words $\mathfrak{M}_n \models F_\gamma(\langle r, \xi \rangle)$ and $\mathfrak{M}_(n+1) \models F_{\gamma'}(\langle r, \xi \rangle)$. Since $\mathfrak{M}_n \models P_i(\langle r, \xi \rangle)$ it holds $\gamma(i) = 1$. It follows that $R_i(x)$ is a conjunctive member of $B_\gamma(x)$. Since the pair (γ, γ') is suitable it follows that the conjunction $F_{\gamma'}(x) \wedge B_\gamma(x)$ is satisfiable, and moreover $F_{\gamma'}(x) \vdash B_\gamma(x)$. Together with $\mathfrak{M}_{n+1} \models F_{\gamma'}(\langle r, \xi \rangle)$ this implies that $\mathfrak{M}_{n+1} \models R_i(\langle r, \xi \rangle)$. ❑

Appendix B: Proofs of Lemmas 7 and 8

Lemma 7. Let $SP = < \mathcal{U}, \mathcal{S}, \mathcal{T} >$ be a reduced temporal specification and ψ be a ground formula. If $\Box\psi$ is a (temporal) logical consequence of SP, that is $SP \models \Box\psi$, then $\mathcal{S} \cup \mathcal{U} \vdash \psi$.

Proof Let us suppose that $\mathcal{S} \cup \mathcal{U} \not\vdash \psi$, that is the set $\mathcal{S} \cup \mathcal{U} \cup \{\neg\psi\}$ is satisfiable. Then there exists a first-order structure $\langle D', I' \rangle$ which is a model of $\mathcal{U} \cup \mathcal{S} \cup \{\neg\psi\}$. Hence, a colour scheme $\mathcal{C}'$ can be constructed such that $\langle D', I' \rangle \models \mathcal{F}_{\mathcal{C}'}$, and therefore $\mathcal{U} \cup \mathcal{S} \cup \{\neg\psi, \mathcal{F}_{\mathcal{C}'}\}$ is satisfiable. Since by the construction the node $\mathcal{C}'$ is an initial node of the behaviour graph H, and all paths of H are infinite we conclude that there exists a model $\mathfrak{M} = \langle D, I \rangle$ of SP such that $\mathfrak{M}_0 \models \neg\psi$. It contradicts the premise $SP \models \Box\psi$. So, our supposition is refuted. ❑

Lemma 8. Let $SP = < \mathcal{U}, \mathcal{S}, \mathcal{T} >$ be a reduced temporal specification and ψ be a ground formula. If $\Box\psi$ is a (temporal) logical consequence of SP, that is $SP \models \Box\psi$, then there exists a set of merged rules $\mathcal{G} = \{\mathcal{A}_1 \Rightarrow \bigcirc\mathcal{B}_1, \ldots, \mathcal{A}_m \Rightarrow \bigcirc\mathcal{B}_m\}$ based on $\mathcal{T}$ such that $\mathcal{G}$ is ψ-favourable w.r.t. $\mathcal{U}$ and $\mathcal{S} \cup \mathcal{U} \vdash \bigvee\limits_{j=1}^{m} \mathcal{A}_i$.

Proof If a given specification is unsatisfiable, then the lemma is obviously true with the empty set of merged rules. Now let us suppose that the set $\{\mathcal{U} \cup \mathcal{S}\}$ is satisfiable.

Let us remind that there exists only a finite number of different colour schemes for SP, that is H is a finite graph. Let $\mathcal{M} = \{\mathcal{C}_1, \ldots, \mathcal{C}_m\}$ be the set of all nodes of H, and $\mathcal{F}_{\mathcal{C}_1}, \ldots, \mathcal{F}_{\mathcal{C}_m}$ be formula specifications of $\mathcal{C}_1, \ldots, \mathcal{C}_m$, and $\mathcal{A}_1 \Rightarrow \bigcirc\mathcal{B}_1, \ldots, \mathcal{A}_m \Rightarrow \bigcirc\mathcal{B}_m$ be the merged rules induced by $\mathcal{F}_{\mathcal{C}_1}, \ldots, \mathcal{F}_{\mathcal{C}_m}$, respectively. Let us prove now that the set $\mathcal{G} = \{\mathcal{A}_1 \Rightarrow \bigcirc\mathcal{B}_1, \ldots, \mathcal{A}_m \Rightarrow \bigcirc\mathcal{B}_m\}$ is a required set of merged rules.

1. Let us take an arbitrary rule $\mathcal{A}_j \Rightarrow \bigcirc\mathcal{B}_j$ and a corresponding colour scheme (or node) $\mathcal{C}_j$, $j \in \{1, \ldots, m\}$.
   (a) Let us show that $\mathcal{B}_j \wedge \mathcal{U} \vdash \psi$, that is the set $\mathcal{U} \cup \{\mathcal{B}_j, \neg\psi\}$ is unsatisfiable. Suppose that $\mathcal{U} \cup \{\mathcal{B}_j, \neg\psi\}$ is satisfiable. This supposition leads to the contradiction in the same way as in the proof of the previous lemma. It is enough to note that the set of possible successors of $\mathcal{C}_j$ is determined by the formula $\mathcal{U} \wedge \mathcal{B}_j$.
   (b) Let $\mathcal{C}_{j_1}, \ldots, \mathcal{C}_{j_k}, k \geq 1$, be the set of all successors of $\mathcal{C}_j$. Let $\mathcal{F}_{\mathcal{C}_{j_l}}$ be the formula specification of $\mathcal{C}_{j_l}$, for all $1 \leq l \leq k$, and $\mathcal{A}_{j_l} \Rightarrow \bigcirc\mathcal{B}_{j_l}$ is the merged rule induced by $\mathcal{F}_{\mathcal{C}_{j_l}}$. We assert that $\mathcal{U} \wedge \mathcal{B}_j \vdash \bigvee\limits_{l=1}^{k} \mathcal{A}_{j_l}$, that is the set $\mathcal{U} \cup \{\mathcal{B}_j, \neg\mathcal{A}_{j_1}, \ldots, \neg\mathcal{A}_{j_k}\}$ is unsatisfiable. Let as suppose, in an opposite way, that this set is satisfiable, and a structure $\langle D', I' \rangle$ is a model of $\mathcal{U} \cup \{\mathcal{B}_j, \neg\mathcal{A}_{j_1}, \ldots, \neg\mathcal{A}_{j_k}\}$. Let $\mathcal{C}'$ be a colour scheme of $\langle D', I' \rangle$, that is $\langle D', I' \rangle \models \mathcal{F}_{\mathcal{C}'}$ and $\mathcal{F}_{\mathcal{C}'}$ is consistent with $\{\neg\mathcal{A}_{j_1}, \ldots, \neg\mathcal{A}_{j_k}\}$. By the construction the node $\mathcal{C}'$ is a successor of $\mathcal{C}_j$, therefore there is $l \in \{1, \ldots, k\}$ such that $\mathcal{F}_{\mathcal{C}'} \models \mathcal{A}_{j_l}$. However it contradicts the consistency of $\mathcal{F}_{\mathcal{C}'}$ and $\bigwedge\limits_{l=1}^{k} \neg\mathcal{A}_{j_l}$. So, $\mathcal{U} \wedge \mathcal{B}_j \vdash \bigvee\limits_{l=1}^{k} \mathcal{A}_{j_l}$ and, hence $\mathcal{U} \wedge \mathcal{B}_j \vdash \bigvee\limits_{i=1}^{m} \mathcal{A}_i$.

   From (a) and (b) we conclude that $\mathcal{G}$ is ψ-favourable w.r.t. $\mathcal{U}$.
2. In order to show that $\mathcal{S} \cup \mathcal{U} \vdash \bigvee\limits_{j=1}^{m} A_i$ we follow the arguments given in 1.(b) taking as $\mathcal{C}_j$ an arbitrary initial node of H. ❑