Proving Boolean Combinations of Deterministic Properties

Bowen Alpern
Fred B. Schneider†
87-819

March 1987

Department of Computer Science
Cornell University
Ithaca, New York 14853-7501

†Supported, in part, by NSF grant DCR-8320274 and Office of Naval Research contract N00014-86-K-0092.
Proving Boolean Combinations of Deterministic Properties

Bowen Alpern
Watson Research Center
Box 218
Yorktown Heights, NY 10598

Fred B. Schneider*
Department of Computer Science
Cornell University
Ithaca, NY 14853

Abstract This paper gives a method for proving that a program satisfies a temporal property that has been specified in terms of Buchi automata. The method permits extraction of proof obligations for a property formulated as the Boolean combination of properties, each of which is specified by a deterministic Buchi automaton, directly from the individual automata. The proof obligations can be formulated as Hoare triples. The method is proved sound and relatively complete. A simple example illustrates application of the method.

1. Introduction

Over the past 20 years, there has been increasing interest in ways to deduce properties of program behavior from the program text itself. One technique that is attracting attention is based on specifying a temporal property $P$ with a Buchi automata that accepts every sequence of program states satisfying $P$.\(^1\) Proof obligations are then extracted from this automaton. These obligations are generalizations of the invariant and variant function used to prove partial correctness and termination of a while loop. They define verification conditions that must hold for any program satisfying $P$. Since the verification conditions themselves are formulated as Hoare triples [Hoare 69], all reasoning can be done in first-order predicate logic, and temporal logic is not required.

Extraction of proof obligations from Buchi automata was first proposed in [Alpern & Schneider 85] for deterministic properties—those properties that can be specified by deterministic Buchi automata. Subsequently, [Manna & Pnueli 87] generalized the approach to handle properties that can be specified by non-deterministic Buchi automata.\(^2\) Both [Alpern & Schneider 85] and [Manna & Pnueli 87] treat a property as a monolithic entity. Doing so has some practical disadvantages. First, the Buchi automaton specifying a property that is the Boolean combination of simpler properties can be exponentially bigger than the combined size of the automata specifying its components [Sistla et al 86]. Since the amount of work required to prove correctness is linear in the size of the automata specifying the property being proved, working with the combined automata can be impractical. Second, combining properties requires complex automata constructions and simplifying properties requires automata transformations, both of which are error prone processes. By contrast, when, for example, temporal logic is used to specify properties, logical connectives permit properties to be combined and the laws of logic allow properties to be simplified.

This paper shows how to avoid these disadvantages by giving a way that proof obligations for a property formulated as the Boolean combination of deterministic properties can be extracted directly from the automata specifying those components. The method also unifies the approaches in [Alpern & Schneider 85] and [Manna & Pnueli 87]. The method of [Alpern & Schneider 85] extracts obligations for $P$ from a deterministic Buchi automata that accepts $P$; the method of [Manna & Pnueli 87] is equivalent to extracting obligations for $\neg P$ from a Buchi automata that accepts $P$.

In our new approach, a property is presented as a conjunction of clauses, each of which is proved separately and is formulated as the disjunction of deterministic properties and negations of deterministic properties. To prove that a program satisfies a clause, three proof instruments must be exhibited. An invariant handles the safety aspects of the proof; a variant function handles the liveness aspects; and a candidate function, arbitrates among the automata specifying the disjuncts of a clause to ensure that any program execution will be accepted by at least one automata representing a deterministic property or rejected by at least one automata representing the negation of a deterministic property. The three instruments define verification conditions, which can be formulated as Hoare triples.

In section 2, a simple concurrent programming language and its semantics is defined. Section 3 reviews Buchi automata for specifying properties. Proof instruments for a single clause are discussed in section 4; sound-
ness and completeness proofs are also given there. The
method is illustrated in section 5 by proving that assuming
weak fairness, Peterson’s protocol for mutual exclusion
[Peterson 81] satisfies a non-starvation property. Section 6
relates our approach to other techniques for proving pro-

properties of concurrent programs.

2. Programs

A program \( \pi \) is specified by a predicate \( Init_\pi \) de-
scribing possible initial states and a set of atomic actions \( A_\pi \).
An execution of \( \pi \) is modeled by an infinite sequence of
program states, called a history, in which the first state
satisfies \( Init_\pi \) and every subsequent state results from ex-
cuting an element of \( A_\pi \) in the preceding state. In a con-
current or distributed program, a history is the sequence of
states that results from interleaving the atomic actions of
processes as they are executed.

An atomic action \( \alpha \) defines a set of pairs of program
states. Execution of \( \alpha \) is enabled in a state \( s \), denoted
\( enabled(\alpha, s) \), provided \( (3 t: (s, t) \in \alpha) \). The state-

\( \langle b \rightarrow S \rangle \)

specifies an atomic action containing those elements \( (s, t) \)
such that \( b \) holds on \( s \) and \( t \) is the state produced by ex-
executing \( S \) starting in state \( s \).

Rather than enumerating the atomic actions of a pro-
gram directly, it is frequently convenient to annotate a
program with control points that delimit its atomic actions.
We will denote control points by marking and numbering
them. For example, program fragment of process \( \pi \)

\[ \langle \begin{array}{c}
(3 s: \langle \begin{array}{c}
(3 t: (s, t) \in \alpha) \end{array} \rangle \langle b \rightarrow S \rangle \end{array} \rangle \]

defines a single atomic action

\( \langle if \, pc_\alpha = 3 \rightarrow pc_\alpha := 4; S \rangle \)

where \( pc_\alpha \) simulates the program counter.

All histories are assumed to be infinite. One way to
achieve this is by including in \( A_\pi \) an atomic action that
has no effect on the program state and is enabled when no
other atomic action is. Thus, terminating executions are
extended to infinite histories by repeating the final state.

An example program \( MEP \) is shown in Figure 2.1. It
is a solution to the two-process critical section problem
described in [Peterson 81]. Based on the control point
annotations, we obtain set of atomic actions \( A_{MEP} \) of
Figure 2.2. In those atomic actions, variable \( pc_a \) simulates
the program counter for process \( A \) and variable \( pc_b \) simu-
lates the program counter for process \( B \). Finally, we have

\[ \text{Init}_{MEP}: pc_a = 1 \land pc_b = 1 \]

because when execution is begun, both processes start at
the the beginning of their loops.

3. Specifying Properties using Buchi Automata

A Buchi automaton is a finite state machine that
accepts infinite sequences. Since a property of a program
can be viewed as defining a set of infinite sequences of pro-
gram states, a Buchi automaton \( m \) can be used to specify
the property containing exactly those sequences accepted
by \( m \). Mechanical procedures exist to translate linear-time
first-order temporal formulas into Buchi automata where
state transitions are defined in terms of first-order program
state predicates [Wolper et al 83] [Alpern 86]. Moreover,
Buchi automata have natural diagrammatic representations
and this is sometimes convenient.

\[ A_{MEP}: \text{cobegin} \]

\[ \begin{array}{c}
(1) \text{nca} := true; \\
(2) \text{active}_a := true;
(3) \text{turn} := B;
(4) \text{do active}_b \land \text{turn} = B \rightarrow (5) \text{skip} \\
\end{array} \]

\[ \text{od} \]

\[ // \text{do true} \rightarrow (1) \text{nca} ; \\
(2) \text{active}_b := true; \\
(3) \text{turn} := A; \\
(4) \text{do active}_a \land \text{turn} = A \rightarrow (5) \text{skip} \\
\text{od} \]

\[ \text{od} \]

\[ \text{coend} \]

Figure 2.1. Peterson’s Mutual Exclusion Protocol

\[ A_{MEP} = \{ \alpha_1 \land (if \, pc_a = 1 \rightarrow pc_a := 2; nca \land \textbf{fl}), \alpha_2 \land (if \, pc_a = 2 \rightarrow pc_a := 3, true \land \textbf{fl}), \alpha_3 \land (if \, pc_a = 3 \rightarrow pc_a := 4, B \land \textbf{fl}), \alpha_4 \land (pc_a = 4 \land active_b \land \text{turn} = B \rightarrow pc_a := 5 \land \textbf{fl}), \alpha_5 \land (pc_a = 4 \land active_b \land \text{turn} = B \rightarrow pc_a := 5 \land \textbf{fl}), \alpha_6 \land (pc_a = 5 \rightarrow pc_a := 6 \land \textbf{fl}), \alpha_7 \land (pc_a = 6 \rightarrow pc_a := 7, \textbf{fl}), \alpha_8 \land (pc_a = 7 \rightarrow pc_a := 1, false \land \textbf{fl}), \alpha_9 \land (pc_a = 1 \rightarrow pc_a := 2; nca \land \textbf{fl}), \alpha_{10} \land (pc_a = 2 \rightarrow pc_a := 3, true \land \textbf{fl}), \alpha_{11} \land (pc_a = 3 \rightarrow pc_a := 4, A \land \textbf{fl}), \alpha_{12} \land (pc_a = 4 \land active_b \land \text{turn} = A \rightarrow pc_a := 5 \land \textbf{fl}), \alpha_{13} \land (pc_a = 5 \rightarrow pc_a := 6 \land \textbf{fl}), \alpha_{14} \land (pc_a = 6 \rightarrow pc_a := 7, \textbf{fl}), \alpha_{15} \land (pc_a = 7 \rightarrow pc_a := 1, false \land \textbf{fl}) \} \]

Figure 2.1. Atomic Actions \( A_{MEP} \)

Figure 3.1 is an example of a Buchi automaton \( m_{sr} \).
It accepts an infinite sequence in which after a finite prefix
each state satisfies the program state predicate \( P \). In
temporal logic, this property is given by \( \diamond P \). Automaton \( m_{sr} \)
contains three \textit{automaton states} labeled \( q_0, q_1, \) and \( q_2 \). The
\textit{start} state, \( q_0 \), is denoted by an edge with no origin, and
\textit{accepting state}, \( q_1 \), is denoted by two concentric circles.
A Buchi automaton accepts a sequence \( \sigma \) if and only if it
enters an accepting state infinitely often while reading \( \sigma \).
Notice, there is no way in \( m_{sr} \) to get from \( q_3 \) to an
accepting state. Such states are called \textit{dead states}. If an
automaton is in a dead state, it cannot accept its input.
Edges between automaton states are labeled by program-state predicates that are called transition predicates and define transitions between automaton states. If a program state satisfies the transition predicate on an edge then that edge is defined for that program state. For example, because there is an edge labeled \( P \) from \( q_0 \) to \( q_1 \) in \( m_{\omega} \), whenever \( m_{\omega} \) is in \( q_0 \) and the next symbol read is a program state satisfying \( P \), then a transition to \( q_1 \) can be made. We adopt the convention that there be an edge defined from each automaton state for each input symbol.

In order to define Buchi automata formally, the following notation will be useful. For any sequence \( \sigma = s_0 s_1 \ldots \),

\[
\begin{align*}
\sigma[i] &= s_i, \\
\sigma[i:] &= s_0 s_1 \ldots s_{i-1}, \\
\sigma[i..] &= s_i s_{i+1} \ldots, \\
|\sigma| &= \text{the length of } \sigma \text{ (if } \sigma \text{ is infinite)}, \\
INF(\sigma) &= \{ i | \sigma \text{ appears infinitely often in } \sigma \}.
\end{align*}
\]

A Buchi automaton \( m \) for a property of a program \( \pi \) is a five-tuple \((S, Q, Q_0, A, \delta)\), where

- \( S \) is the (countable) set of program states of \( \pi \),
- \( Q \) is the (finite) set of automaton states of \( m \),
- \( Q_0 \subseteq Q \) is the set of start states of \( m \),
- \( A \subseteq Q \) is the set of accepting states of \( m \),
- \( \delta \subseteq (Q \times S) \rightarrow 2^Q \) is the transition function of \( m \).

Transition predicate \( T_\pi \) associated with the edge from automaton state \( q_i \) to \( q_j \), holds for a program state \( x \) if and only if \( q_j \in \delta(q_i, x) \). (Although \( S \) may be infinite, we only consider properties for which the transition predicates have finite description as a first-order formula involving program variables.) Transition function \( \delta \) can be extended to handle finite sequences of program states in the usual way:

\[
\delta'(q, \sigma) = \begin{cases} 
(q) & \text{if } |\sigma| = 0 \\
(\delta' \circ \epsilon : q'' \rightarrow \delta'(q, \sigma[..|\sigma| - 1])); & \text{if } 0 < |\sigma| < \omega
\end{cases}
\]

A sequence of automaton states that \( m \) might occupy while reading \( \sigma \) is called a run. Thus, \( \rho \) is a run of \( m \) on \( \sigma \) if and only if

\[
\rho[0] \in Q_0 \text{ and } (\forall i: 0 < i < |\sigma| : \rho[i] \in \delta(\rho[i - 1], s_0(i - 1))).
\]

A Buchi automaton \( m \) accepts a sequence \( \sigma \) if and only if there is a run \( \rho \) of \( m \) on \( \sigma \) for which \( INF(\rho) \cap A \neq \emptyset \).

Notice in \( m_{\omega} \) (Figure 3.1) that two transitions are possible from \( q_0 \) for a program state satisfying \( P \), because any program state that satisfies \( P \) also satisfies \( true \). When there is more than one start state or more than one transition is possible from some automaton state for a given input symbol, the automaton is non-deterministic; otherwise, it is deterministic. Thus, \( m_{\omega} \) is non-deterministic. However, \( L(m_{\omega}) \) the language accepted by \( m_{\omega} \) is the negation of the deterministic property \( \Box \neg P \) accepted by \( m_{\omega} \) of Figure 3.2.

4. Proof Instruments from Buchi Automata

Let property \( P \) be the conjunction of clauses \( P_1, P_2, \ldots, P_n \). To prove that a program \( \pi \) satisfies \( P \), we prove separately that \( \pi \) satisfies each of the clauses. Thus, it suffices to derive proof instruments for a single clause \( P_i \) of the form

\[
P_i \lor \ldots \lor P_i \lor \neg P_i \lor \neg P_{i+1} \lor \ldots \lor \neg P_{k+n},
\]

where each \( D_k \) is specified by \( m_k \), a deterministic Buchi automaton. Any property that can be specified by a non-deterministic Buchi automaton can be put in this form [Eilenberg '74]. We call \( m_1 \) through \( m_n \) the positive automata of \( P \), and \( m_k+1 \) through \( m_{k+n} \) the negative automata.

Let \( m_k \) be defined by \((S_k, Q_k, Q_0, A_k, \delta_k)\).

To formulate proof instruments for \( \pi \) and \( P_i \), define a joint state \( x \) to be an element of \( JS(P_i, \pi) \) the joint state space, \( Q_1 \times \cdots \times Q_n \times S_{\pi} \). Let \( x^{(k)} \) denote the \( k \)th element of a joint state \( x \) and set \( x^{(k+1)} \) abbreviate \( x^{(k+1)} \). A joint state \( x \) is positive, denoted \( pos(x) \), iff for some positive automata \( m_i \), \( x^{(i)} \in A_i \). Thus, \( x \) is positive if one of \( m_1 \) through \( m_n \) is in an accepting state. The set of negative automata that are in an accepting state in a joint state \( x \) is \( neg(x) = \{ k | 0 < k \leq k \wedge x^{(k)} \notin A_k \} \). For a sequence \( \sigma \) of joint states, define \( \rho^{(k)} \) to be the projection of \( \rho \) onto its \( k \)th element; i.e. \( \rho^{(k)} = \rho[0]^{(k)} \rho[1]^{(k)} \cdots \). A sequence of joint states \( \rho \) is a joint history of \( \pi \) and \( P \) iff \( \rho^{(k)} \) is a history of \( \pi \) and for all \( 1 \leq k \leq n \), \( \rho^{(k)} \) is a run of \( m_k \) on \( \rho^{(k)} \).

A program \( \pi \) satisfies the property specified by a clause \( P_i \) iff each history \( \sigma \) of \( \pi \) is either accepted by one of the positive automata—and therefore satisfies one of the properties \( D_1 \) through \( D_n \)—or is rejected by one of the negative automata—and therefore satisfies one of \( \neg D_{n+1} \) through \( \neg D_{n+n} \). Thus, \( \pi \) satisfies \( P_i \) iff for every history \( \sigma \) there is a joint history \( \rho \) such that \( \sigma = \rho^{(k)} \) and either (i) there is a positive automata \( m_k \), such that \( INF(\rho^{(k)}) \cap A_k \neq \emptyset \) or (ii) there is a negative automata \( m_k \), such that \( INF(\rho^{(k)}) \cap A_k = \emptyset \).

To prove that \( \pi \) satisfies the property specified by a clause \( P_i \), three proof instruments must be exhibited:

- an invariant \( I \subseteq JS(P_i, \pi) \),
- a candidate function \( u : JS(P_i, \pi) \rightarrow 2^{[1^{n+1} n^+}] \),
- a variant function \( v : JS(P_i, \pi) \rightarrow W \), where \( W \) is a well-founded set.

The invariant relates program states in a history to automaton states occupied while reading that history. The candidate function identifies negative automata that might never again enter an accepting state. And, the variant function bounds the number of times that the candidate function can become empty before one of the positive automata enters an accepting state.

If the invariant, candidate function, and variant function satisfy the following obligations, then \( \pi \) will satisfy \( P_i \). In these obligations, \( x \) and \( x' \) denote elements of \( JS(P_i, \pi) \).
The first two obligations ensure that $I$ holds throughout any joint history.

O1: If $x_0 = \rho[0]$ for some joint history of $\pi$ and $P_i$, then $x \in I$.

O2: If $x \in I$ and $(x(\pi), x'(\pi)) \in \alpha$ then $x' \in I$.

O1 constitutes the base case and O2 an induction step for an argument that execution of each atomic action produces a joint state in $I$. Choosing an invariant $I$ permits unreachable joint states to be ignored in the obligations that follow.

The next obligation requires that a variant function $u$ increase only in or immediately after processing a joint state in which a positive automata is in an accepting state.

O3: If $x \in I$ and $(x(\pi), x'(\pi)) \in \alpha$ then

\[ Pos(x) \lor Pos(x') \lor u(x) < u(x') \lor \emptyset \subseteq u(x') \subseteq u(x). \]

Thus, O3 ensures that either (i) some positive automaton enters an accepting state infinitely often (and the history is accepted) or (ii) after some point $u$ never increases and no positive automaton subsequently enters an accepting state.

Since the range of $u$ is a well-founded set, if $u$ never increases then eventually its value must become constant. The next obligation implies that under these circumstances, throughout the rest of the history, the candidate function is a non-empty set and contains the index of some negative automaton $m_k$.

O4: If $x \in I$ and $(x(\pi), x'(\pi)) \in \alpha$ then

\[ Pos(x) \lor Pos(x') \lor u(x) < u(x') \lor \emptyset \subseteq u(x') \subseteq u(x). \]

The final obligation ensures that a negative automata that enters an accepting state cannot be a candidate unless a positive state is entered or the variant function decreases. Thus, if no positive state is entered and the variant function does not decrease then $m_k$ does not enter an accepting state for the remainder of the history, hence it rejects the history.

O5: If $x \in I$ and $(x(\pi), x'(\pi)) \in \alpha$ then

\[ Pos(x) \lor Pos(x') \lor neg(x') \cap u(x') = \emptyset. \]

Since $m_k$ rejects the history, the history satisfies $\neg D_k$ and therefore satisfies $P_i$.

We can now prove:

Soundness Theorem: If there are proof instruments $I$, $v$, and $u$ that satisfy obligations O1 through O5 then $\pi$ satisfies $P_i$.

Proof: Let $\rho$ be a joint history of $\pi$ and $P_i$, $\rho[0] \in I$ by O1. By O2 and induction, $\rho[i] \in I$ for all $i \geq 0$. We must show that $\rho$ causes some positive automaton to be in an accepting state infinitely often or some negative automaton to be in an accepting state only finitely often. Assume that no positive automaton is in an accepting state infinitely often. Thus, there is an index $l_1$ such that $\rho[l_1]$ contains no positive states. By O3, the variant function is non-increasing on $\rho[l_1]$. Since its range is well-founded, there must be an index $l_2$ such that $l_1 \leq l_2$ and the variant function is constant on $\rho[l_2]$. By O4, there is a negated automaton $m_k$ such that $k \in u(\rho[l_2])$. Also by O4, for all $l_2 < j < k$, $k \in u(\rho[j])$. Therefore, by O5, $m_k$ does not enter an accepting state after $l_2$. This means that $m_k$ rejects $\rho$, so $\pi$ satisfies $P_i$.

We now show that our technique is relatively complete.

Completeness Theorem: If $\pi$ satisfies $P$ then there exist proof instruments $I$, $v$, and $u$ that satisfy obligations O1 through O5.

Proof: Form a directed graph where the nodes are the joint states appearing in joint histories and there is an edge from node $x$ to $y$ iff $y$ is not a positive accepting state and $x$ immediately precedes $y$ in some joint history. Define partial order $\succ$ on the nodes of this graph such that $x \succ y$ iff there is a path with non-zero length from $x$ to $y$ and somewhere on this path appears an accepting state for each negative automaton.

Partial order $\succ$ is well-founded, as is shown by the following proof by contradiction. If $\succ$ were not well-founded then there would be an infinite descending chain $x_1 \succ x_2 \ldots$. By construction of the graph, this implies the existence of a joint history that includes $x_1$. Let $\sigma_0$ be a prefix of such a joint history that ends with $x_1$. For each $x_i$ in the infinite descending chain, let $\sigma_i$ be the path from $x_i$ to $x_{i+1}$ that includes an accepting state for every negative automaton. Such a path exists by definition, because $x_i \succ x_{i+1}$. Finally, let $\sigma = \sigma_0 \sigma_1 \cdots$. Notice that $\sigma$ is a joint history, that $\sigma$ contains no positive accepting states after $\sigma_0$, and that there are infinitely many accepting states for each negative automaton in $\sigma$. Thus, $\sigma$ does not satisfy $P$. This is a contradiction, and we conclude that $\succ$ is well-founded.

Since $\succ$ is well-founded, the following recursive function is well defined:

\[ H(x) = \sup_{y \in \gamma} H(y) + 1. \]

$H$ is a function from the joint state space to the ordinals. If there is no $y$ such that $x \succ y$ then $H(x) = 0$ by definition of $\sup$, so the function is total. Notice that if $x \succ y$ then $H(x) > H(y)$. Moreover, if there is any path from $x$ to $y$ in the graph then $H(x) \geq H(y)$.

The variant function will be constructed using $H$ and the level $l(x)$ of a node $x$, defined as follows. Level $l(x) = i$ iff for any collection of $i$ and no more than $i$ negative automata, there exists some node $u$ with $H(u) = H(x)$ such that there is a path to $x$ and there is an accepting state for each automaton in the collection somewhere on the path. Note that by definition of $H$, the level of a node will be less than $n$.

The three proof instruments can now be defined. Choose $I$ to be the characteristic predicate for the set of joint states that appear in joint histories of $\pi$ and $P_i$. Choose $v(x)$ to be $H(x) + 1 - l(x)$. The range of $v$ with lexicographic ordering of pairs as the ordering relation is well-founded because the ordinals are. Finally, choose $u(x)$ to be the set of negative automata that do not have accepting states on any path from $u$ to $x$ for any $u \neq x$ such that $u(v) = v(x)$.

Proof obligations O1 and O2 follow immediately from the definition of $I$.

To see that O3 holds, notice that if neither $x$ nor $x'$ is positive then there is a path (of length 1) from $x$ to $x'$ in the graph. Thus, $H(x) = H(x')$. Suppose $H(x) = H(x')$. Since any path to $x$ can be extended to $x'$, $l(x') = l(x')$. Therefore, $v(x) = v(x')$.

To see that O4 holds, suppose that neither $x$ nor $x'$ is positive and that $v(x) = v(x')$. By construction of $u$, both $x$ and $x'$ must be at the same level. By the construction of $u$, $u(x') \subseteq u(x)$, since there is a path (of
length 1) from $x$ to $x'$. Also by construction of $u$, $u(x') \neq \emptyset$.

If there exists a node $w$ such that $\nu(w) = \nu(x')$ and there is a path from $w$ to $x'$ then $\neg \nu(x') \cap u(x') = \emptyset$ since $x'$ is (trivially) included on the path to $x'$. If there is no such $w$ then $\nu(x) > \nu(x')$. So, $O_5$ holds. This completes the proof.

Obligations $O_1$ through $O_5$ can be translated into verification conditions formulated as Hoare triples and first-order predicate logic formulas. A Hoare triple $(P) \alpha (Q)$ for an atomic action $\alpha$ asserts that a start state in a satisfying state $P$ terminates in a state satisfying $Q$. Thus, $(P) \alpha (Q)$ is valid iff $(\forall (s,t) : (s,t) \in \alpha \Rightarrow P(s) \Rightarrow Q((t)))$.

To reformulate $O_1$ through $O_5$ in terms of Hoare triples, we define slight variations of the three proof instruments. Define $PJS(P)$ the projection of $JS(P)$ with respect to program states as $PJS(P) = Q_1 \times \cdots \times Q_{p+n}$. Elements of $PJS(P)$ are called projected joint states. The projected joint state in which every automaton is in its start state is called the projected joint start state. A projected joint state $y$ is considered positive if it is the projection of a positive state. (Similarly, if $y$ is a projection of joint state $x$ then define $\neg \nu(y) = \neg \nu(x)$.) We now define projections of the three proof instruments with respect to projected joint states. For an invariant $I$, $I_y$ is the projection of $I$ with respect to a projected joint state $y$; i.e., $I_y = \{ s \in S_y : y \times s \in I \}$. For a variant function $u_y$, projection $u_y$ is a function from $S_y$ to $S_y$ such that $u(y, s) = u(y, s)$ for $s \in S_y$. And, for a candidate function $u$, define $u_y$ such that $u(y, s) = u_y(s)$ for $s \in S_y$.

Finally, we define a projected joint state transition predicate $T_{xy}$ to be a predicate that holds for any program state causing a transition from a projected joint state $y$ to a projected joint state $z$. $T_{xy}$ can be formed by taking the conjunction for all $m_i$ of the transition predicates labeling the edge from $y^{(s)}$ to $z^{(t)}$. $T_{xy}$ is the projected joint state transition predicate from the joint start state to $z$.

Verifying each of the following formulas implies that $O_1$ through $O_5$ hold. The first verification condition implies $O_1$.

**VC1:** $(\nu(y) \land T_{xy}) = I_x$

The next implies $O_2$ through $O_5$.

**VC2:** For all projected joint states $y$ and $z$ and atomic actions $\alpha \in A_y$:
(i) If $y$ or $z$ is positive then $(I_y) \alpha (T_{xy} \Rightarrow I_z)$.
(ii) Otherwise,
\[ (I_y \land u_y = V \land u_u = U) \alpha (T_{xy} \Rightarrow (I_z \land \left( u_z = V \land \neg \nu(z) \lor u_z = U \lor \neg \nu(z) \right)) \]

$O_2$ is implied by $T_{xy} \Rightarrow I_x$ in the postcondition of VC2(ii) and VC2(iii). To see that $O_3$, $O_4$, and $O_5$ follow from VC1 and VC2, choose $x = (y, s)$ and $x' = (z, s')$. It follows immediately from $O_2$ that $x' \in t$. We conclude that $s'$ satisfies $T_{xy}$ directly from the definition of $T_{xy}$. If $y$ or $z$ is positive, then $O_3$, $O_4$, and $O_5$ are trivially satisfied. Suppose neither $y$ nor $z$ is positive and let $u(x) = V$ and $u(z) = U$. From the postcondition of VC2(ii), it follows that either $u(x') < V$ or $u(x') = V$. Thus, $O_3$ holds. If $u(x') < V$ does not hold then, from the postcondition of VC2(ii), $\emptyset \cup u(x') \subseteq U$ and $u(x') \cap u(x') \subseteq U - \neg \nu(x')$. Thus, $O_4$ and $O_5$ hold.

Conversely, assume $O_1$ through $O_5$ hold. VC1 follows from O1. From O2 we get
\[ \{ I_y \land u_y = V \land u_u = U \} \alpha (T_{xy} \Rightarrow \left( u_z = V \lor u_y = U \right)) \]
Thus, VC2(ii) holds. Assume that neither $y$ nor $z$ is positive. From O3 we get
\[ \{ I_y \land u_y = V \land u_u = U \} \alpha (T_{xy} \Rightarrow \left( u_z = V \lor u_y = U \right)) \]
From O4 we get
\[ \{ I_y \land u_y = V \land u_u = U \} \alpha (T_{xy} \Rightarrow \left( u_z = V \lor u_y = U \right)) \]
Finally, from O5 we get
\[ \{ I_y \land u_y = V \land u_u = U \} \alpha (T_{xy} \Rightarrow \left( u_z = V \lor u_y = U \right)) \]
Together, these four Hoare triples imply VC2(ii).

We have shown that obligations $O_1$ through $O_5$ are equivalent to verification conditions VC1 and VC2. If the underlying first-order predicate logic is expressive enough to capture the preconditions and postconditions of the Hoare triples of VC2 then the verification conditions can be expressed in this logic. Since Hoare Logic is semantically complete relative to the completeness of the underlying first-order predicate logic (Apt 81), our proof technique is complete relative to the semantic and expressive completeness of this logic.

**5. Example: Proving Non-Starvation Assuming Fairness**

In addition to mutual exclusion, a solution to the critical section problem should ensure that processes attempting entry to critical sections actually do enter eventually. A process of $M$ (Figure 2.1) is said to starve if it tries to enter its critical section but never succeeds. To formalize this, let $p_A (p_B) = b$ be a variable containing the value of the program counter for process $A (B)$. Process $A$ of $M$ should eventually enter $c_{A}$ whenever

\[ \text{TRY}_A : p_A = 4 \land p_B = 5 \]

holds, and similarly process $B$ should eventually enter $c_{B}$ whenever

\[ \text{TRY}_B : p_A = 4 \land p_B = 5 \]

holds. The Non-Starvation Property $NS_M$ asserts that neither process starves. This can be formalized in temporal logic as

\[ NS_M : (\square \rightarrow \text{TRY}_A) \land (\square \rightarrow \text{TRY}_B) \]

It is easy to see that $M$ does not satisfy $NS_M$ for histories in which one or the other process is not given sufficient opportunity to execute. A fairness assumption asserts that an atomic action that is enabled "often enough" will be executed eventually. Let $F_{A}$ be a fairness assumption for atomic action $A$. A fairness assumption for a program $\pi$ is the conjunction of fairness assumptions—one for each atomic action in $\pi$. Thus, $F_M$ the fairness assumption for $M$ is defined by

See [Francez 86] for various types of fairness assumptions.
To show that MEP satisfies NS\textsubscript{MEP} for all histories satisfying \( F_{\text{MEP}} \), we must prove that MEP satisfies \( F_{\text{MEP}} \Rightarrow NS_{\text{MEP}} \). Putting this property into conjunctive normal form, we get

\[
F_{\text{NS}_{\text{MEP}}} : \bigwedge_{a \in A_{\text{MEP}}} \left( \bigvee_{a} \neg F_a \lor \Box \neg TRY_A \right) \land \left( \bigvee_{a} \neg F_a \lor \Box \neg TRY_B \right)
\]

Each of the two clauses (conjuncts) in \( F_{\text{NS}_{\text{MEP}}} \) is proved separately. However, since the two clauses are symmetric, only the first one is proved here; the proof of the second is similar.

As a fairness assumption for atomic actions, we choose weak fairness, which asserts that an atomic action that becomes enabled is eventually executed. This is expressed in temporal logic as

\[
WF_a : \Box \neg \text{Before}_a,
\]

where \( \text{Before}_a(s) \) is the predicate \( (\exists t : (s, t)\in a) \). Thus, the first conjunct of \( F_{\text{NS}_{\text{MEP}}} \) property to be proven is

\[
F_{\text{NS}_{\text{MEP}}} : \bigwedge_{a \in A_{\text{MEP}}} \left( \bigvee_{a} \neg WF_a \lor \Box \neg TRY_A \right)
\]

This clause contains seventeen disjuncts because \( |A_{\text{MEP}}| = 16 \); all but one of these disjuncts is negated. Each disjunct is of the form \( \Box \neg \tau \), so the Buchi automaton specification for each literal is \( m_{\sigma} \) of Figure 3.2.

To prove that \( F_{\text{NS}_{\text{MEP}}} \) holds we use the following proof instruments.

\[
I = JS(F_{\text{NS}_{\text{MEP}}}, MEP)
\]

where

\[
u = \begin{cases}
0 & \neg TRY_A \\
2 & (4 - \text{pc}_A) \mod 7 & TRY_A \land \neg TRY_B \land \neg \tau = A \\
7 & \text{pc}_A & TRY_A \land \neg TRY_B \land \neg \tau = B
\end{cases}
\]

where \( \text{enbl}(a) \) holds in any program state \( s \) where atomic action \( a \) is enabled (i.e., \( enabled(a, s) \)).

Rather than checking that verification conditions VC1 and VC2 hold, we argue (informally) that obligations O1–O5 are satisfied by this choice of proof instruments.

Clearly, O1 and O2 are satisfied by the choice of invariant, since the invariant rules out no joint state.

O3 follows from the construction of the variant function, as follows. When \( \neg TRY_A, \nu = 0 \), but an automaton for a positive disjunct is in an accepting state, so O3 is satisfied in that case. If \( TRY_A \land \neg TRY_B \land \neg \tau = A \), then \( \nu \) is the number of atomic actions that \( A \) must execute before entering \( \text{enbl} \). Since \( \tau = A \), subsequent execution by \( B \) does not alter this value. If \( TRY_A \land \neg TRY_B \), then \( \nu \) includes the number of atomic actions \( B \) must execute to establish the previous case \( (TRY_A \land TRY_B \land \neg \tau = A) \).

Clearly, execution by \( A \) does not alter this value. Finally, when \( TRY_A \land TRY_B \land \neg \tau = B \), then \( \nu \) is the maximum value of \( \nu \) in the preceding case \( (TRY_A \land \neg TRY_B) \) plus the number of atomic actions that \( B \) must execute to make \( TRY_A \land \neg TRY_B \) hold.

O4 follows from the construction of the candidate function, which always contains the index of the automaton corresponding the fairness assumption for the atomic action that will reduce \( \nu \).

O5 holds because \( m_{\sigma} \) for an enabled atomic action is not in an accepting state.

Note that this proof is an instance of the method of helpful directions for weak fairness [Frances 86]. Each process corresponds to a direction. Execution of an enabled atomic action in the helpful direction decreases the variant function. Execution of an enabled atomic action in some other direction does not increase the variant function nor does it disable a helpful atomic action. Thus, when \( TRY_A \land TRY_B \land \neg \tau = A \), the helpful direction is process \( A \); when \( TRY_A \land \neg TRY_B \) or \( TRY_A \land TRY_B \land \neg \tau = B \), the helpful direction is process \( B \). The weak fairness assumption guarantees that the variant function decreases eventually.

The method of helpful directions is a special case for proving properties that assume weak fairness of the technique developed in this paper. To see this observe that the candidate function identifies the helpful directions. The stipulation that execution of a helpful atomic action decrease the variant function guarantees O5. The stipulation that a non-helpful atomic action not increase the variant function guarantees O3. And, the stipulation that a non-helpful atomic action leave a helpful one enabled guarantees O4.

6. Discussion

Formulated in the terminology of this paper, our previous method ([Alpern & Schneider 85]) for extracting proof obligations from a deterministic Buchi automaton requires the program prove to exhibit an invariant \( I \) and a variant function \( \nu \) satisfying:

\[
\begin{align*}
\text{AS1:} & \quad \text{if } x \text{ is the first state of a joint history then } x \in I. \\
\text{AS2:} & \quad \text{if } x \in I \text{ and } (x') \in \alpha \text{ then } x' \in I. \\
\text{AS3:} & \quad \text{if } x \in I \text{ and } (x') \in \alpha \\
& \text{then } Pos(x) \lor Pos(x') \lor \nu(x') < \nu(x).
\end{align*}
\]

AS1 and AS2 are obligations O1 and O2 of the approach outlined in Section 4. Consider the remaining obligations (O3 through O5) of that approach. A deterministic property is a single clause that consists of a single, non-negated property, so there are no negative automata. Thus, \( \nu(x) = \emptyset \) for every joint state \( x \) and O5 is trivially satisfied because its final disjunct is. Moreover, the final disjunct of O4 must be false. AS3 and O4 are therefore equivalent, and each implies O3. Thus, the two techniques yield essentially the same proof obligations when applied to a deterministic property.

The method in [Alpern & Schneider 85] is unsatisfactory for properties specified by non-deterministic Buchi automata. To use it to prove that a program \( \pi \) satisfies such a property \( P \), a deterministic property \( D \) that is contained in \( P \) is found. Proof obligations are then extracted from the deterministic Buchi automata for \( D \). If a (finite-
state) program $\pi$ satisfies $P$, an appropriate $D$ always exists but may be big and difficult to find. Furthermore, the proof obligations for a non-deterministic property now depend on the program as well as on the Buchi automata for the property to be proved. The approach of Section 4 does not suffer from these difficulties. Since every property that can be specified using a non-deterministic Buchi automaton can be specified as a Boolean combination of deterministic properties [Eilenberg 74] and we can now handle such Boolean combinations, our new technique is general enough to prove non-deterministic as well as deterministic properties.

In [Manna & Pnueli 87], a different technique is given for obtaining proof obligations for non-deterministic properties. The approach is based upon a V-automaton for a property. Simplifying slightly, a V-automaton is a Buchi automaton that accepts its input iff every run on that input eventually is restricted to accepting states. Using the parlance of Section 4, to show that every history of a program will be accepted by a V-automaton $M$, one must exhibit an invariant $I$ that satisfies obligations O1 and O2 and a variant function $v$ satisfying:

\[ \text{MP1: If } x \in I, (x^0, x^1) \in \alpha, \text{ and } x^{(1)} \text{ is an accepting state of } M \text{ then } v(x') \leq v(x). \]

\[ \text{MP2: If } x \in I, (x^0, x^1) \in \alpha, \text{ and } x^{(1)} \text{ is a non-accepting state of } M \text{ then } v(x') < v(x). \]

The V-automaton for a property is isomorphic to the Buchi automaton for the negation of that property. This suggests there might be a connection between the proof obligations that are obtained from a V-automaton for the negation of a deterministic property and the proof obligations we obtain for a clause with a single negated property. And, there is. Since there are no positive joint states with a single negated property, O3 implies MP1, and MP1 and MP2 imply O3. O5 requires that the candidate function be empty whenever the Buchi automaton (V-automaton) enters an accepting (non-accepting) state. Thus, we can choose the candidate function such that O4 and MP2 are equivalent—define $u$ to be empty whenever the Buchi automata is in an accepting state and to be [1] when it is not. Therefore, the two techniques yield the same proof obligations for a property whose negation is deterministic.

The key insight underlying the approach of [Manna & Pnueli 87] is that proof obligations for the negation of a property can be extracted directly from a Buchi automaton for the property—whether or not this automaton is deterministic. Given a property specified by a Buchi automata, to extract proof obligations using the approach of [Manna & Pnueli 87], the Buchi automata for the negation of the property is constructed. With the technique presented in this paper, the property is decomposed into a Boolean combination of properties where the non-negated terms must be specified by deterministic Buchi automata. Depending on the property, one or the other approach may be easier.

An added advantage of the Boolean decomposition approach is that parts of the proof may be reusable since other properties might be constructed from these parts.

Acknowledgments

Discussions with Starvos Cosmadakis and Sheryl Brady were helpful, especially in formulating the completeness proof.

References


