WHAT GOOD IS TEMPORAL LOGIC?
Leslie LAMPRECHT
Computer Science Laboratory, SRI International
Menlo Park, California 94025, USA

Invited Paper

Temporal logic is a formal system for specifying and reasoning about concurrent programs. The purpose of this paper is to explain why. It is primarily about my method for using temporal logic, but also discusses some other approaches.

Temporal logic is a branch of formal logic that is used in many ways. When advancing a new formalism, one usually argues that it is simple, natural and easy to use. Temporal logic is a rather simple extension of classical logic, and it does provide a natural way of describing the temporal behavior of a program. However, learning to use a new formalism is never easy because it requires learning to think in a new way. You probably found it hard at first to use the V and S of predicate calculus, only after changing your way of thinking did the formalism become simple and natural. Learning to reason about programs in terms of temporal logic is just as hard as learning to use V and S. Moreover, there are other formalisms that at first seem more natural than temporal logic; you would probably find them easier to learn.

If temporal logic is not simpler and more natural than other methods, why should we use it? Although there are many reasons why I like temporal logic, there is one that is paramount: temporal logic supports hierarchical specification and reasoning in a simple, natural way. Experience has shown that the best way to describe a complex system is through a hierarchy of levels of abstraction, starting from a high-level specification and ending with the implementation in some programming language. Each level adds a specification of the next lower level and an implementation of the next higher one. Temporal logic provides a single logical system for describing the program at any level of abstraction—from the highest-level specification through the programming-language implementation. A statement about the program at one level is a meaningful statement about any lower level. Thus, hierarchical design methods are supported directly, with no extra mechanism needed to link the different levels of description.

The remainder of this section explains in vague generalities how temporal logic differs from other approaches. Subsequent sections describe what temporal logic is, how it is used to specify programs, and how it supports hierarchical specification and verification.

1. INTRODUCTION

1.1. The Answer

The question posed in the title has a simple answer: temporal logic is a good method for specifying and reasoning about concurrent programs. The purpose of this paper is to explain why. It is primarily about my method for using temporal logic, but also discusses some other approaches.

Temporal logic is a branch of formal logic that is used in many ways. When advancing a new formalism, one usually argues that it is simple, natural and easy to use. Temporal logic is a rather simple extension of classical logic, and it does provide a natural way of describing the temporal behavior of a program. However, learning to use a new formalism is never easy because it requires learning to think in a new way. You probably found it hard at first to use the V and S of predicate calculus, only after changing your way of thinking did the formalism become simple and natural. Learning to reason about programs in terms of temporal logic is just as hard as learning to use V and S. Moreover, there are other formalisms that at first seem more natural than temporal logic; you would probably find them easier to learn.

If temporal logic is not simpler and more natural than other methods, why should we use it? Although there are many reasons why I like temporal logic, there is one that is paramount: temporal logic supports hierarchical specification and reasoning in a simple, natural way. Experience has shown that the best way to describe a complex system is through a hierarchy of levels of abstraction, starting from a high-level specification and ending with the implementation in some programming language. Each level adds a specification of the next lower level and an implementation of the next higher one. Temporal logic provides a single logical system for describing the program at any level of abstraction—from the highest-level specification through the programming-language implementation. A statement about the program at one level is a meaningful statement about any lower level. Thus, hierarchical design methods are supported directly, with no extra mechanism needed to link the different levels of description.

1.2. How Do You Say "Maybe" in Temporal Logic?

Natural languages are very expressive and very imprecise. You can express any property of a program in natural English—for example, you can say that it is race—-but it is hard to be sure that someone else will understand exactly what you mean. Formal languages are not very expressive, but they are precise. You can't say very much in a formal language, but what you can say is completely unambiguous.

A temporal logic is a formal language for expressing temporal properties. A number of different temporal logics have been studied by logicians and computer scientists [6], but there is one that I find useful for specifying and reasoning about concurrent programs. This temporal logic allows you to express two kinds of properties of a program.

- Safety properties, which assert that the program does not do something bad.
- Liveness properties, which assert that the program eventually does something good.

Partial correctness (the program does not produce the wrong answer), natural exclusion (two processes are not in their critical sections at the same time), and deadlock-freedom (the program does not reach a deadlocked state) are safety properties. Progress (the program eventually does terminate) and starvation-freedom (a process eventually receives service) are liveness properties.

Safety and liveness are not the only properties of a program that are of interest. For example, one might wish to know the program's probability of terminating or whether it is correct. However, I do not know of any practical method for reasoning about such properties. I do know how to reason about safety and liveness properties, and these are the only ones that I consider.

One type of property that is not of interest is the possibility that the program might do something. We want to specify not that the program might produce the right answer, but that it must do so. Because many formalisms cannot...
expresses linear properties, they have led people to consider such "possibility" properties instead. If you can't prove that the program must do something, proving that it might do is the next best thing. Since temporal logic can express linear, we do not need to talk about possibilities. In fact, the temporal logic I've cannot even express such properties; you can't say "maybe" in this temporal logic.

Temporal logic was developed to describe the order in which things must happen rather than the actual times at which they happen. To talk about real time, one can introduce the notion of a clock. Real-time properties of programs can then be expressed as safety properties. For example, the assertion "the program must respond to an input within ten milliseconds" can be expressed as "the clock cannot reach ten milliseconds after the time of the last input without an output being produced", which is a safety property. Linear properties, which state that something must eventually happen, follow from the physical nature of time—the ten milliseconds must eventually elapse. A somewhat different method of applying temporal logic to real-time programs was used in [2], where the number of program steps counted replaces real time.

1.3. Actions or Models?

There are two ways to specify a program:

- **Describe an abstract model that tells how the program should behave**.
- **State what properties the program should have**.

I will call the first approach constructive and the second axiomatic. Since one can describe an abstract model by stating its properties, there is no way to formalise this distinction. Nevertheless, it is useful to classify methods in this way. Perhaps the most elegant example of a constructive method is Milner's Calculus of Communicating Systems [15]. Temporal logic is an axiomatic method.

Hierarchical specification poses a problem for constructive methods. As an example, consider the specification of a queue. At a high level, the queue operations consist of adding an element to or removing one from the queue. A constructive specification uses a model in which these are the elementary operations. At the implementation level, each queue operation is performed by executing many program steps. The individual program steps are this level's elementary operations; they are the elementary operations in a constructive specification of the implementation. What does it mean for the program to correctly implement the specification? In the constructive approach, the answer requires a definition of what it means for a sequence of lower-level operations to correctly implement a single high-level operation. This may not be easy: since actions from other parts of the program may be executed concurrently with the actions that implement the queue operation, Section 1 explains how temporal logic specifications avoid this problem.

There is another problem facing constructive methods. They specify a program essentially by writing another, presumably simpler, program. However, concurrent programs that seem simple can exhibit quite unexpected behavior. How can we be sure that we understand the program if its specification says only this in helpful like some other program which we may not understand?

Axiomatic methods attempt to overcome this difficulty by stating directly what properties the program must have. They will succeed only if the properties are easy to understand. The challenge facing the axiomatic approach is therefore to express the required properties so that they are both precise and understandable.

1.4. Operations or States?

In an axiomatic specification, one expresses the properties that the program must have as assertions in some logical system. What should these assertions tell about? Two possibilities arise:

- What operations are performed by the program.
- How the state of the program changes.

At first, talking about operations seems the more natural approach. However, the work of Floyd and Hoare on sequential program verification demonstrated the benefits of thinking in terms of states rather than operations. Hence, methods were developed for state-based, axiomatic reasoning about concurrent programs [6], [17].

In the seven or eight years I have used axiomatic methods to reason about concurrent programs, the following has occurred over and over again. First, I find a proof in terms of the sequence of operations executed by the program. The proof seems natural, and there appears to be no nice way of expressing it in terms of assertions about states. However, I persevere, and out of two things happens: I either find an axiomatic proof that is simpler and more elegant than the operational one—a proof that sheds new light on why the program works—or else I discover an error in the proof and a corresponding bug in the algorithm. The latter happens quite often; it is easy to make a mistake when reasoning about the sequence of operations executed by a concurrent program.

I have had a similar experience specifying properties of programs. When describing a program informally, I tend to speak in terms of operations rather than states—i.e., in terms of verbs rather than nouns. Supposing that the program displays a number on the terminal seems more natural than saying that it changes the terminal's state. However, when I try to specify something more precisely, I find myself talking about states. Trying to say exactly what it means to display a number on a terminal, I tend to talk about the state of the screen.

This experience made me decide to try an axiomatic system for describing concurrent programs upon states rather than operations.
1.5. Why Temporal Logic?

Having decided upon a state-based axiomatic method, why should I use temporal logic? People have been specifying and reasoning about sequential programs for years using ordinary, acentual forms of logic. Why does the introduction of concurrency require the use of temporal reasoning?

To describe a sequential program, we need consider the state of the system at any two times: before the program is executed and afterward. The program can be considered as a function from an initial to a final state, so it can be specified in terms of input and output conditions. The simple before/after temporal reasoning that is used need not be made explicit.

This is not true for concurrent programs. For example, consider the following two program statements, where the angle brackets denote atomic operations. (An atomic operation of a concurrent program is one that is indivisible with respect to concurrently executed operations.)

\[
S_1: (x := x + 1)
\]

\[
S_2: \begin{cases} 
    \tau := \tau + 1; \\
    (x := x - y)
\end{cases}
\]

end

Statement \( S_1 \) and \( S_2 \) produce the same mapping from initial to final states. They satisfy exactly the same input and output conditions, so they are completely equivalent when used in a sequential program. However, consider the following concurrent program, where the concurrency indicates that its two clauses are to be executed concurrently.

\[
\text{concurrent} \quad (\tau := \tau + 1; \quad S_1 \text{ and } S_2)
\]

Substituting \( S_2 \) for \( S_1 \) yields a program that increments \( x \) by one, while substituting \( S_1 \) for \( S_2 \) yields a program that increments \( y \) by either one or eight—the latter possibility occurring if the execution of the two statements of \( S_1 \), \( S_2 \), or \( S_2 \) and \( S_3 \) produces identical input/output conditions, are not equivalent when they appear as part of a concurrent program.

This example shows that, when describing a concurrent program, we cannot restrict our attention to what is true before and after its execution; we must also consider what happens during its execution. To prove simple safety properties, one need consider only properties that are true at all times during the program's execution. Since "at all times" is also a simple temporal concept, one can reason about these safety properties with no explicit temporal methodology, as in [9] and [11]. However, the more complex temporal reasoning needed for liveliness properties cannot be left implicit; it must be explicitly described.

Purdy was the first to recognize the usefulness of temporal logic for reasoning about liveliness properties of concurrent programs [9]; although Purdy had earlier suggested applying temporal logic to program verification [1].

1.6. Isn't Temporal Logic Good For?

Like any formal system, temporal logic has its limitations. One limitation is obvious, but it will state it anyway: temporal logic will not make the specification and verification of concurrent programs easy. Designing a concurrent program is a difficult task; no formalism can make it easy. Why, then, use temporal logic? Why use a temporal logic precisely what the program should do and analyzing rigorously what it will do. This method can be applied with varying degrees of rigor, ranging from an informal specification that serves only to guide the designer, to a completely formal specification with a machine-willed correctness proof of the implementation. Rigorous reasoning in any formal system is difficult and time consuming, but it is the only way I know to eliminate the subtle timing-dependent errors that are endemic to concurrent programs.

Our temporal logic also has less obvious limitations. Its expressiveness has been carefully limited so as to be adequate for its intended purpose: specifying and reasoning about a concurrent program. Its limited expressiveness is what makes temporal logic so good for this purpose because it prevents one from saying things that could get him into trouble. However, it means that our temporal logic is worthless for many other purposes. For example, it cannot express the statement that two programs are equivalent. This is because two programs are equivalent if they have the same set of possible behaviors, and our temporal logic cannot express the notion of possibilities.

In general, temporal logic is not good for comparing programs or describing sets of programs. When specifying and reasoning about a single program, the only relevant comparison between programs is that a lower-level version correctly implements a higher-level one. There is only one program that counts as the implementation running on the computer. It is this single program that one specifies and reasons about with temporal logic.

2. WHAT IS TEMPORAL LOGIC?

2.1. Is Temporal Logic Talking About?

Viewed formally, temporal logic consists of a language of formulas and a set of axioms and inference rules for deriving which formulas are theorems. However, a formal description does not tell us what temporal logic really is about. Just as Frege's axioms were meaningless without an understanding of the objects that underlie it.

We model a program as a set of (finite or infinite) behaviors of the form

\[
\phi = \phi_0 \lor \phi_1 \lor \phi_2 \lor \cdots
\]

where the \( \phi_i \) are states and the \( a_i \) are actions. For now, think of each behavior as a possible execution of some stage program written in a Pascal-like language with constructs...
for expressing concurrency. For the sake of euphony, I will refer to this Pascal-like language simply as "Pascal.

A state consists of a possible "snapshot" taken in the middle of an execution, containing all the information needed to resume execution right from that point. Thus, the state must describe the value of each program variable, the contents of the subroutine-calling stack, the value of each "program counter", etc. An action is a specific atomic action of the program—for example, the execution of some particular atomic assignment statement. The behavior of the model represents all possible executions of the program.

We think of the behavior
\[ a_* \downarrow q, a_2 \downarrow q, a_3 \downarrow q \ldots \]

as describing an execution that starts at some time \( \alpha \) in state \( a_\alpha \); is at state \( a_\alpha \) at some time, etc. Time \( \alpha \) is regarded as the present, all future times as the future.

Observe that we are modeling concurrency as the interleaving of atomic actions. Computer scientists often feel that something is lost by not considering concurrent programs in this way, and that one should instead see a partial ordering among the actions. However, so long as we are talking only about safety and fairness properties, there is no loss of generality in considering totally ordered sequences of actions. Our model includes all possible sequences, and a partial ordering is completely equivalent to the set of all total orderings consistent with it. The real assumption implicit in the model is the existence of atomic actions. Since the assumption is made in virtually all formal models of concurrency, I will not discuss it here. As you will see, temporal logic requires only that at some sufficiently low level—perhaps at the level of microcode—the program's execution be accurately described by a collection of atomic actions.

2.2. How Do You Speak Temporal Logic?

It would be appropriate here to define exactly what the formulas of temporal logic are, and how each formula is interpreted as a statement about the underlying model. However, rather than have you with formalism, I will describe the language of temporal logic informally. A more formal definition can be found in the appendix of [1].

In the temporal logic that I use, assertions are constructed from state predicates, action predicates, the usual logical operators, and the single temporal operator \( \square \). A state predicate is an assertion about a state, a typical example being:

\[ (x \geq 0) \quad \square \] (at or after program location \( \alpha \)),

which asserts that the state is one in which: (i) the value of the variable \( x \) is positive and (ii) the program counter indicates that control is at a certain location \( \alpha \). This assertion is true for some states and false for others.

An action predicate is an assertion about an action. The action predicates we need have the form:

this is an action of \( \alpha \),

where \( \alpha \) is some part of the program, such as a particular subroutine or while loop. Although needed to formalize the concepts, action predicates play a minor role in specifying and reasoning about a program. For simplicity, they will be largely ignored from now on.

Temporal relations are expressed with the operator \( \square \). The formula \( (\square (x \geq 0)) \) is interpreted to mean that \( x \) remains true at least as long as \( \alpha \) does. You can remember this by thinking of \( \square \) as a "temporal \( \geq \) operator, where \( A \triangleleft B \) means that the length of time for which \( A \) holds continuously is less than the length of time that \( B \) holds. Thus, \((x \geq 0) \triangleleft (x > 7)\) asserts that if \( x \) has the value 6 from time 0 through time 27, then the value of \( y \) is greater than 7 from time 0 through time 27. The \( \square \) operator is related to the usual until operator by \( A \equiv B \triangleleft \equiv A \).

An important type of temporal formula is one of the form \( \neg \square A \). It asserts that \( A \) remains true at least as long as true does—in other words, \( A \) remains true forever. This assertion is written \( \neg \square A \), and is read "negate-"temporal-"A". Another important type of formula has the form \( A \triangleleft \neg \square A \) and asserts that it is not the case that \( A \) always false—in other words, \( A \) must eventually become true. This assertion is written \( \neg \square A \) and read "eventually-true". While most speakers of English would say "that A does not always remain false" is equivalent to "A eventually becomes true", some computer scientists disagree. If you are one of them, see [10] for an explanation.

A temporal logic formula is interpreted as an assertion about a single behavior of the program. It may be true of some behavior and false of others. We say that the formula is satisfied by a program, or that it is true for the program, if it is true of every behavior of the program. A temporal logic specification consists of a collection of temporal formulas that the program must satisfy—i.e., formulas that must be true for every possible program behavior.

2.3. What Did You S... S... S... Say?

While the exact form of our temporal logic formula might not concern us here, they have one crucial property that must be discussed: they cannot detect "non-temporal". To see what this means, let \( \gamma \) be the behavior:

\[ a_0 \quad a_1 \quad a_2 \quad \ldots \]

and let \( \gamma \) be another behavior which is the same as \( \gamma \) except that some particular transition \( a_n \rightarrow a_n \) is replaced by the stuttering sequence:

\[ a_n \rightarrow a_n \rightarrow a_n \rightarrow a_n \rightarrow a_n \rightarrow a_n \]

No temporal-logic-formula can distinguish between \( \gamma \) and \( \gamma \). In other words, any formula in our temporal logic is true for the behavior \( \gamma \) if and only if it is true for \( \gamma \). This fact is easily proved from the formal semantics given in [1].

A little experimentation should also convince you that it is
impossible to construct an assertion from state predicates and the operator $\mathcal{O}$ that can distinguish between these two behaviors.

Not only can a temporal logic assertion not detect the addition of identical copies of a transition, but it cannot detect the replacement of a transition by a sequence of transitions if the state and action predicates from which it is constructed cannot distinguish between the original and action and the interleaved states and actions. More precisely, let $A$ be as above, but this time let $\sigma$ be the same as $\sigma'$ except with the transition $\tau_{c_{1}} \rightarrow \tau_{a_{1}}$ replaced by the sequence

$$\tau_{c_{1}} \rightarrow \tau_{c_{2}} \rightarrow \cdots \rightarrow \tau_{c_{n}} \rightarrow \tau_{a_{1}}.$$ 

Let $A$ be any temporal logic assertion such that none of the state predicates appearing in $A$ can distinguish between $\tau_{c_{1}}$ and the various $\tau_{c_{i}}$, and none of the action predicates appearing in $A$ can distinguish between $\tau_{a_{1}}$ and the various $\tau_{a_{i}}$. In other words, for every $j$, each state predicate appearing in $A$ is true for the state $\tau_{c_{j}}$ if and only if it is true for the state $\tau_{c_{j}}$, and similarly for each action predicate appearing in $A$. In this case, $A$ is true for $\sigma$ if and only if it is true for $\sigma'$.

When most computer scientists see that our temporal logic cannot detect muttering, they want to overcome this deficiency by making the logic expressive. Many of them have done this—usually by adding a next operator, where next $A$ means that $A$ is true after the next action. I have a definite reason for not adding a next operator or any other operator to increase the expressiveness of this temporal logic. We use an abstract logic instead of reasoning directly about the underlying model because the logic does not let us talk about important properties of the model. Proofs assume properties of such things as $\sigma = 0 \mod 7$ or $\tau_{0} \rightarrow \tau_{1}$ by printing no means of expressing. Using the next operator, one could write a specification for a store that includes the requirement "putting an element in the queue should result in exactly 10 steps." The number of steps in a Pascal implementation is not a meaningful concept when one gives an abstract, high level specification of a queue. It is just as irrelevant as the roundness of an integer, since it is a property of a specific representation of the operation, not the operation itself.

When one talks about the next state, one really means the next state in which a significant change occurs—where significant means visible at the level of detail of the specification. For example, in saying that an element is added to the queue in the next state, one means that the element will be added to the queue before certain other parts of the state change. This can be expressed in temporal logic without using the next operator. It takes a little time to get used to expressing properties in this way, without the next operator, but it is worth it. You will see that increasing the expressiveness of our temporal logic with a next operator would destroy the entire logical foundation for its use in hierarchical methods.

3. SPECIFICATIONS

3.1. What Good is a Specification?

A specification serves as a contract between the implementer of a program module and the user of that module. This contract has two features:

1. It allows the implementer to design the module, knowing that his only responsibility is to meet the requirements imposed by the specification.

2. It allows the user to write programs that call upon the module, knowing that he need worry only about the correctness of his programs, and can assume that the module will behave as specified.

How can one see that a specification method really serves these functions? How do we know that the specification tells the implementer and the user everything they need to know? In principle, we know that these functions are satisfied if:

1. The implementer can formally prove that his implementation satisfies the specification.

2. The user, given only the specification of the module, with no knowledge of how it is implemented, can formally prove the correctness of his programs that use the module.

Now even formidable specification is not attempted, the fact that a method purports this kind of logical reasoning ensures that it will produce precise, unambiguous specifications.

In an ideal world, a specification is written once, and the implementer and user need never talk to each other again. In practice, like any real contract, a specification must be renegotiated if the implementer or realizer finds that he has promised more than he can deliver, or if the user realizes that the specified module does not meet his needs. Contrasts are no less useful if they are renegotiated. I believe that whatever a system is "too complicated to be formally specified"—its sole specification being several hundred thousand lines of Pascal code—it is because the system evolved without the implementation of a paradigm, or there was no one to negotiate on behalf of the user.

3.2. An Example

The method I advocate for writing temporal logic specifications is described in detail in [11]. In this section, I will present a rough sketch of the way it works by considering a simple example. Other specification methods based upon temporal logic are discussed at the end of the section.

The example is a FIFO (First-In-First-Out) queue. There are two operations performed on the queue: FCUT, which inserts an element at the tail of the queue, and GET, which removes an element from the head of the queue. More precisely, PUT and GET are two abstractnesses that are called to perform these operations. They can be called concurrently by two different processes, but, for simplicity, I assume that each can be called by only one process at a time.
We must decide what GET should do if it finds the queue empty. In a sequential program, this is treated as an anomalous condition—for example, by returning a special error value. However, for a concurrent program, there is the additional possibility of waiting for another process to put something in the queue. This possibility is more interesting, since it occurs only for concurrent programs, so we choose it.

You should be very suspicious when someone uses a queue to illustrate a specification method. Many methods have queues built in as primitive concepts, sometimes implicitly in the form of sequences, so it is not surprising that they can very easily specify a queue. A good way to judge whether the example is biased is to compare the specifications of different kinds of queues: FIFO versus LIFO (Last-In-First-Out), unbounded versus bounded, waiting on a GET to an empty queue versus returning an error value, etc. If two programs that have very similar informal descriptions require very different specifications, then the method may be difficult to use in practice.

3.3 State Functions

We want to think about programs in terms of states, so a specification should be written in terms of states. The basic object mentioned in a specification is the state function, which is a function that assigns a value to any program state. In specifying a queue, there are many ways of choosing the state functions, but the different choices I might make all produce specifications that are easily shown to be equivalent. Here, I will use the following three state functions:

gens: The current contents of the queue.
past: When PUT is called, pasty equals the element to be inserted into the queue. After the element is put on the queue, pasty assumes a special value NULL. Thus, pasty serves to "remember" both the argument with which PUT is called and whether or not PUT has finished inserting an element into the queue.

prefix: The analogue of pasty for the GET operation. It equals NULL when GET is called, and equals the element removed by GET when queue is changed.

These descriptions of the state functions are not part of the specification; they are just comments to help you understand it. The specification simply declares queuer, pasty, and prefix to be state functions, and indicates what type of values they may assume. Formally, the specification has the form

there exist state functions queuer, pasty, ... such that 

Two other, less interesting, state functions are needed: in(PUT) and in(GET). These are boolean-valued state functions that are true when control is inside a call to the PUT and GET subroutines, respectively. They are thus functions of "program counter" values. A few other state functions are needed to specify how arguments and values are passed in calls to PUT and GET, but I will ignore them.

3.4 Specifying Safety Properties

Recall that an automatic specification consists of a list of properties, the so-called axioms, each of which must be satisfied by every possible behavior of the implementation. I will describe only the interesting axioms for the queue, omitting the initial conditions and some simple safety properties that describe the passing of arguments and values in subroutine calls. The complete specification, which is not very long, can be found in [1].

The only interesting safety property is one that describes how the three major state functions are allowed to change. There are two occasions on which queue can change:

(a) When PUT adds the current value of pasty to the end of the queue, setting pasty to NULL.

(b) When GET removes an element from the front of the queue, changing the value of prefix from NULL to that element.

These are also the only interesting changes that can occur to pasty and prefix. More precisely, (a) describes the only time pasty can change when control is in the PUT subroutine and (b) describes the only time prefix can change when control is in the GET subroutine.

This restriction on when these three state functions are allowed to change is expressed more formally as follows, where + denotes concatenation. (The notation of [1] has been changed a bit to make the property less compact and easier to read.)

allowed changes to pasty

\[ \text{put} \text{ when } \text{in}(\text{PUT}) \]

\[ \text{get} \text{ when } \text{in}(\text{GET}) \]

(a) in(\text{PUT}) \& (\text{past} + \text{new} \neq \text{NULL}) \Rightarrow

\[ \text{put(new + \text{prefix}) = \text{new}} \]

(b) in(\text{GET}) \& (\text{prefix} = \text{NULL}) \Rightarrow

\[ \text{get(prefix + \text{new}) = \text{new}} \]

This property states that for any transition \( a \leadsto b \) in the behavior

\[ a_0 \rightarrow a_1 \rightarrow a_2 \rightarrow \ldots \]

of one of the following holds:

- the value of the state function queuer is not the same in states \( a_0 \) and \( a_1 \) or
- the value of pasty is not the same in \( a_0 \) and \( a_1 \) and \( \text{in}(\text{PUT}) \) is true for state \( a_0 \), or
- the value of prefix is not the same in \( a_0 \) and \( a_1 \) and \( \text{in}(\text{GET}) \) is true for state \( a_1 \).

Thus the transition must be either of type (a) or type (b). It is a type (a) transition if the predicate \( \text{in}(\text{PUT}) \) is true for state \( a_0 \), pasty equals \( \text{NULL} \) in state \( a_0 \), and the value of queue in state \( a_0 \) equals the concatenation of its value in state \( a_0 \) with the value of pasty in state \( a_0 \). It is a type (b) transition if the-
values

them.

list of

an

at

time

long.

other

range.

to

the

out

of

null

occur

z

only

f

sub-

change

as

were

been

caster

predicate int(rget) A (preval = NULL) A queue not empty in state a., prevall not NULI in state a, and the value of queue is state a., equals the value of getrel-queue in state a.

To specify a LIFO queue, one requires that the new element be added at the head rather than at the tail of the queue, which is done by simply replacing queuep = queuep * queue in (a) with queuep = * queue. A queue of maximum length 23 is specified by adding the condition

\[
\text{length of queuep} < 23
\]

to the "preconditions" of (a). To allow the GET subroutine to return a special value EMPTY when the queue is empty, one just adds the following special transition.

(3) rget(queue) A (preval = NULL) A (return is empty) 

\[
\rightarrow \text{preval} = \text{EMPTY}
\]

Our allowed changes property states that queue changes atomically when no element is added to or removed from the queue by the PUT and GET operations. It looks just like a constructive specification which says that adding or removing a queue is a single atomic action. If this is so, how can the property be valid for a Pascal implementation in which the PUT subroutine requires 62 program steps to add an element to the queue?

Although the syntax of the allowed changes statement makes it look like a constructive specification, it is actually a temporal logic formula that can be expressed using only the temporal operator cf. Writing it as such a formula is not easy (the general method is given in [11]), but we never have to; we just rewrite directly about the allowed changes statement. Being a temporal logic formula, it cannot distinguish between the situations a....a, and the sequence of transitions

\[
\begin{align*}
\sigma_1, \sigma_2, \ldots, \sigma_{n-1}, \sigma_n
\end{align*}
\]

when the temporal function that appears to be empty, queue, putrel, getrel, int(put) and int(get) - have the same value for each state \(\sigma_i\), so they do for \(\sigma_n\).

Although the allowed changes property asserts that the state function queue must change atomically, it does not say anything about how many steps it takes for PUT subroutine to perform the operation. Remember that queue is not a program variable; it is a state function whose value is the function of the values of program variables, program counters, etc. Each of the PUT subroutine's 42 program steps may change variables and program counter values. However, the state function queue and prevall must be defined in such a way that they are changed by only one of those steps.

To prove the correctness of an implementation, one must define the state functions queue, prevall, and prevrel so they change atomically even if the program moves sound data around in small pieces. This may seem like magic, but it really isn't hard. You can see how it is done in [5], where those state functions are defined for an implementation in which the data are moved one bit at a time. The idea does not work so strange if we remember that all sequential methods for proving safety properties involve finding an invariant—a boolean state function whose value does not change during program execution. Instead of finding state functions that do not change at all, verifying the specification requires finding state functions that change only the way the allowed changes statement permits them to. In principle, these state functions can always be defined—in fact, there are usually many different ways of doing so. In practice, the appropriate definitions are just as hard to find as the invariants for proving safety properties. If the program is simple, or if the correctness is based upon subtle interactions among the program, proving its correctness will not be easy. No method will make it easy to prove the correctness of a complex concurrent program.

I have indicated how this method of specifying safety properties fulfills the first function of a specification: allowing one to prove the correctness of an implementation. How does it achieve the second function: allowing one to prove safety properties of programs that call the PUT and GET subroutines? Proving safety properties requires finding invariants. The invariants for programs that use PUT and GET will be functions not only of the program's variables and program counter values, but of the state functions queue, putrel and getrel as well. The allowed changes statement in the queue module's specification, which constrains how these state functions can change, will be used in the proof of invariants.

3.1. Liveness Properties

Safety properties state what the program may or may not do, not what it must do. The allowed changes statement specifies how state functions are allowed to change; it does not say that they must change. Liveness properties assert that the program must do something. Temporal logic was applied to programs especially for reasoning about liveness properties, so it is not surprising that it excels at specifying these properties. The liveness property we require of the GET subroutine is that if the queue is nonempty, then GET will eventually end. Letting \(\alpha\) (GET) be the state function that is true when the GET subroutine is in its exit point, the requirement is stated simply as

\[
\text{int(put) \ (queue not empty) } \supset \ \alpha \ \text{after GET.}
\]

(Remark that \(\alpha \) means that \(\alpha \) eventually becomes true.) The obvious liveness property for the PUT subroutine is that it is never terminate, stated simply as

\[
\text{int(put) } \supset \ \alpha \ \text{after PUT.}
\]

However, this specifies that there is always room in the queue for another element, so the queue must have an unbounded capacity. A more realistic specification would state that the queue must have room for at least 17 elements, so PUT will wait if it finds fewer than 17 elements on the queue. This is stated formally as

\[
\text{int(put) } \supset \ \text{length of queue } \leq 17 \supset \ \alpha \ \text{after PUT.}
\]
How one proves that an implementation satisfies these liveness properties is described in [14] and will not be discussed here. The same technique allows one to test the liveliness properties of the PUT and GET subroutines to deduce liveliness properties of programs that call them.

3.5. Other Temporal Logic Specification Methods

There has been considerable interest in using temporal logic to specify concurrent programs, and several methods have been proposed. Since these methods are all based upon temporal logic, they are in some sense formally equivalent. However, they are quite different in practice.

One method, described in [6] and [7], involves making temporal logic assertions about histories. Instead of using a state function, it uses its partial sequence of values with which PUT has been called and the sequence of values returned by GET. This approach is appealing for two reasons. First, it produces some very simple specifications. For example, when this method is used to specify a queue, the property that corresponds to our allowed changes statement is that the sequence of values returned by GET is a subsequence of the sequence of values with which PUT has been called. Second, talking about the sequence of inputs and outputs seems like a natural way to describe a subroutine.

However, these sequences of values are really behaviors disguised as state functions. I have already indicated that it is easy to make errors when reasoning informally in terms of behavior, so I am suspicious of formal methods based upon them. Moreover, the simplicity of the specifications is deceptive. While specifying a FIFO queue is simple, a specification of a LIFO queue in terms of history sequences is no simpler than the one described above. Methods based upon history sequences will work well for specifying FIFO queueing disciplines, but will not work as well with more complicated interactions. These methods may be appropriate in certain areas, such as communication protocols.

Another approach to temporal logic specification has been advocated by Schwartz and Mellis-Smith [21]. Their approach, which might be called a “more temporal” one, differs from the method I have advocated by replacing many of the state functions with temporal assertions. A more temporal specification of a queue might use the state function queue, but not put and get. Instead of asserting that queues can change by adding to it the value of putget, each a specification asserts that the value with which PUT was most recently called can be added to queue. The state function queue is replaced by the temporal construction “with which PUT was most recently called”.

While the state function queue seems natural, the state functions putget and get were rather contrived. Replacing them with temporal specifications is quite appealing. Unfortunately, the resulting temporal logic specification seems difficult to understand. I introduced the state functions putget and get to eliminate the complex temporal logic formulas that arise when they are not used. More recently, Schwartz, Mellis-Smith and Vogt have developed a new way of writing temporal logic specifications, called interval logic, that seems to yield more understandable specifications [22]. I have also been working on a method of eliminating explicit mention of state functions like putget and get by the use of temporal expressions, but, in my approach, these temporal expressions turn out to be state functions in disguise.

4. HIERARCHY

4.1. The Hierarchy of Specifications

People have finite capacities; they can keep only so much in their minds at once. For a system to be understandable, it should have a high level specification simple enough so understood in its entirety. However, the thousands of lines of code in its implementation cannot be comprehended all at once. Therefore, the system’s description must be structured so it can be read in small pieces. This is done with a hierarchy of specifications. At each level of the hierarchy, the system is described as a number of interacting modules, where a module is a collection of related procedures.

As an example, consider a system for sending messages from computer S to computer R. A message is sent by calling a PUT subroutine in computer S, and is received by calling a GET subroutine in computer R. At the highest level, the system is described as a queue—sending is viewed as putting a message on the queue, and receiving is viewed as taking one of the queue. The entire system is regarded as a single atomic at this level. At the next lower level of the hierarchy, I will call the protocol level, the message-passing system is described in terms of three modules:

• A transmission model that performs the actual transfer of messages from computer S to computer R. Its implementation consists of code in both computers plus the actual transmission line.

• A sender module in computer S that accepts calls to PUT and calls the transmission module to send the messages to computer R.

• A receiver module in computer R that accepts calls to GET and in turn calls the transmission module to receive the messages coming from S.

At the level below the protocol level, each of these three modules is described as a set of interacting modules. For example, the sender module might consist of two concurrently active modules: one that handles calls to GET and puts messages on an internal queue, and another that takes messages from the queue and passes them to the transmission module. The process of hierarchical refinement continues down to a level whose modules are implemented directly in Pascal.

The high-level specification describes the message-passing system in terms of state functions like queue and putget. The three modules of the protocol level are specified in terms of other state functions, perhaps including the following:

1. A PUT function that sends a message to the receiver.
2. A GET function that receives a message from the sender.
3. A send function that sends a message to the receiver.
4. A receive function that receives a message from the sender.
5. A message function that represents a message.
6. A protocol function that represents the protocol level.
apenser: a queue of messages that have been given to the sender module by calls to PUT, but have not yet been seen by the receiver.

disperse: a queue of messages received by the receiver module, but not yet fetched by calls to GET.

map: the message currently in transit, or NULL if there is none.

What does it mean for the protocol-level specification to be a refinement of the high-level specification? Recall that the high-level specification has the form

there exist state functions qruer, patry, ... such that Aq, ..., An, where the Aq are temporal logic formulas. The protocol-level specification likewise has the form

there exist state functions qruer, map, ... such that B1, ..., Bn, where the Bj are also temporal logic formulas. For the protocol-level specification to be a correct refinement of the high-level specification, the existence of state functions qruer, map, ... satisfying properties B1, ..., Bn must imply the existence of state functions qruer, patry, ... satisfying properties A1, ..., An. How do we prove that this is the case?

To prove the existence of qruer, ..., we must define them in terms of map, qruer, map, ... For example, we might define qruer to be the concatenation of

- qruer
- map if it is not NULL
- qruer.

When we substitute for qruer, patry, ..., their definitions in terms of map, qruer, map, ..., the assertions Aq of the high-level specification become assertions Aq of the state functions of the protocol-level specification. The protocol-level specification is a correct refinement of the high-level specification if these assertions Aq are true—more precisely, if they follow from the truth of properties B1, ..., Bn. An example of how this is done is found in [11], where the protocol-level specification describes the alternating-bit protocol.

In summary, to prove that a lower level specification B: there exist state functions B1, ..., Bn such that B1, ..., Bn

is a correct refinement of a higher level specification A: there exist state functions f1, ..., fn such that A1, ..., An, we must find expressions fi(B1, ..., Bn) such that each formula Aq obtained from Aq by performing the substitutions

I = fi(B1, ..., Bn)

follows logically from the axioms B1, ..., Bn.

Now consider a still lower-level specification C: there exist state functions h1, ..., hn such that C1, ..., Cp

We prove it to be a correct refinement of specification B by finding substitutions

I = G(h1, ..., hn)

which yield formulas B1, ..., Bn that can be proved from C1, ..., Cp. It follows that the formulas Aq obtained from the Aq by the substitutions

I = f(G(h1, ..., hn), ..., G(hn, ..., hn))

can be proved from B1, ..., Bn, which in turn can be proved from C1, ..., Cp. Hence, if specification B is a correct refinement of specification A and specification C is a correct refinement of specification B, then specification C is, as expected, also a correct refinement of specification A. This means that if each refinement is correct, then proving that the program correctly implements the lowest level specification shows that it correctly implements every specification in the hierarchy.

The definitions of what it means for a hierarchical refinement to be correct makes sense because both the higher- and lower-level specifications are assertions about the same Pascal model. The mapping between levels of the hierarchy is a mapping between state functions; higher-level state functions are defined in terms of lower-level ones. Refining a specification means giving a more detailed description of the program state—a simple, well-understood concept. This is in contrast to the behavioral approach, in which refinement requires that actions be decomposed into sequences of simpler actions—a much more complicated concept.

4.2. The Hierarchy of Programming Languages

I have interpreted the temporal logic formulas in a specification as assertions about a Pascal implementation, and have indicated how one can prove that a Pascal program correctly implements the specification. However, computers don't execute Pascal programs; they execute machine language programs. It would be nice to prove not only that the Pascal program correctly implements the specification, but that a machine program correctly implements the Pascal program.

The Pascal program was described by a model consisting of sequences of atomic actions—i.e., a behavioral model. In it, the execution of an atomic statement such as

{x = x + 1}

is a single atomic action. However, in a machine language version of the program, executing this statement could take 42 program steps (most of them performing the synchronization needed to guarantee atomicity). What does it mean for these 42 machine language steps to implement a single Pascal action? Do we need behavioral methods to couple the Pascal view to the machine language view?

Of course, the answer is no. Just as putting an element on a queue can be an atomic action in the high-level specification and be implemented by 42 Pascal operations, so can the execution of an assignment statement. However, at the
Pascal level and be implemented by 42 machine language instructions. Although we have been thinking of Pascal corrections as our underlying model, we can just as well let the underlying model consist of execution sequences of a machine language program. In this model, a state consists of an assignment of values to all machine registers and memory locations, while an action is the execution of a single machine language instruction.

With this underlying model, the Pascal program can be viewed as a specification of a machine language program. Just like prose in our high-level specification, the variable $x$ is a state function in the Pascal program specification—a function of the values of registers and memory locations. Even though incrementing $x$ may require several machine language instructions (for example, it might be a multiple precision integer that occupies more than one memory location), the state function $x$ can be defined in such a way that its value changes atomically.

This sounds good in principle, but how does it really work? When we write a temporal logic specification, we are writing temporal logic formulas, or sentences like the allowed changes statement that can be translated directly into temporal logic formulas. It is no clear how one translates a Pascal program into a temporal logic specification of a machine language program.

A semantics for a programming language is a way of assigning a meaning to every legal program in the language. In a temporal logic semantics, the meaning of the program is a temporal logic specification, which is a collection of temporal logic axioms. To give a temporal logic semantics for Pascal, one must define a method for translating from Pascal statements to temporal logic axioms. For example, an atomic assignment statement

$$
i := x = n + 1$$

might yield the safety axiom

$$\text{allowed changes to } x \text{ while } i(n)$$

$$i(n) \implies (\text{new } x = x + 1) \land \text{affirm}(\text{new } x).$$

Defining how one translates from any arbitrary statement in a complex programming language into temporal logic formulas is a difficult task that has not been attempted. It has been done for some simple constructs in an idealized language, but this work has not yet appeared.

Machine language versions of Pascal programs are usually produced by a compiler. Instead of verifying each machine language program individually, one wants to show that the compiler is correct. A temporal logic semantics for Pascal defines what it means for the compiler to be correct—namely, that the machine language program it produces is always a correct implementation of the Pascal program it is given. However, there is still a big step from this to proving the correctness of a real compiler.

Of course, the hierarchy need not stop with the machine language program. We can just as well choose a register transfer model in which the atomic actions are the setting of individual registers inside the computer. The machine language program can then be viewed as a higher-level specification of a register transfer "program." Proving the correctness of the register transfer implementation of a machine language program involves proving that the computer correctly implements its machine-language description. This is the first step in hardware verification: proving the correctness of the register-transfer-level design.

One can proceed further into the hierarchy of descriptions of the computer. Since our model of temporal logic involves discrete events, it would appear that we must stop at the level of physical electronics, where a flip-flop contains a continuous range of voltage levels instead of a binary value. However, the temporal logic operator $\Diamond$ is meaningful even when time is continuous; our temporal logic does not rule out such an underlying model. (This is a further advantage of expressing the next operator.) The refinement process can continue until we reach a level where quantum effects appear. Because a quantum-mechanical state is a superposition of the states that temporal logic formulas talk about [9], I have no idea how one could use temporal logic at the quantum level.

Several researchers have investigated the use of temporal logic for specifying and verifying hardware [7,8,9]. An unusual method is proposed in [7] that, while not expressed in temporal logic, is compatible with our method. It seems clear that the design of VLSI circuits could benefit greatly from the hierarchical approach made possible by temporal logic.

5. SOME CONCLUDING REMARKS

I have not yet used the word "distributed." How one specifies and reasons about a system is independent of whether or not it is distributed. Although they may require different implementation techniques and different programming languages, distributed and nondistributed systems can be described in the same logical framework. It is shown in [10] that no special methods are needed to reason about distributed systems. You have just seen that one high-level specification describes both a distributed message-passing system and a shared memory system; only its implementations differ.

One important aspect of specification was ignored in the example. The actions of PUT and GET were specified in terms of certain operations on the data structure—for example, the concatenation operation $\star$. The question of how these operations are specified was not considered. A complete specification method must permit the precise definition of arbitrary data structures and the operations on them. Fortunately, a large body of research has been devoted to this topic—e.g., research on "abstract data types" and "algebraic specification" [9]. The goal of this work has been to specify programs, which is possible in the sequential case where programs can be described by the relation
between their input and output, so they can be specified purely in terms of operations on data structures. Concurrent programs cannot be specified in this way, which is why temporal logic was introduced. However, these algebraic methods can specify operations on the values assigned by state functions, while temporal logic specifies how the state functions change.

Concurrent systems are inherently complex and are often plagued by timing-dependent synchronization errors that are impossible to find by conventional testing methods. Thus, in many systems are due to such synchronization errors. Reasons, formal reasoning is the best way to eliminate them. Computers are much better than people at formal reasoning, so a formal correctness proof should be checked by a computer. The temporal logic reasoning I have described can be formalized and used as the basis for a mechanical verification system.

Mechanical verification is now feasible for small systems [14], but is expensive. Further development of verification systems is needed before they can be applied to larger concurrent programs. Fortunately, temporal logic is useful without mechanical verification. Writing a formal specification can be helpful even with no attempt at verification because it forces one to understand precisely what the system is supposed to do. Informal reasoning—the kind that mathematicians have been using for centuries—can catch some errors.

ACKNOWLEDGEMENTS

I wish to thank the following people for their helpful comments on an earlier draft of this paper: Edgar Dijkstra, Bret Halpern, C.A.R. Hoare, Cees Jan Koomen, Gerard LeLann, J. Mars, Ben Moskovitch, Fred Schneider, Richard Schwartz, and Michel Sztuff.

REFERENCES

