THE GLOBAL TIME ASSUMPTION AND SEMANTICS FOR CONCURRENT SYSTEMS
(Extended Abstract)

by

Shāi Ben-David
Technical Report #471
November 1987
THE GLOBAL TIME ASSUMPTION AND SEMANTICS
FOR CONCURRENT SYSTEMS

(Extended Abstract)

Revised version, January 1988

Shai Ben-David
Computer Science Department
Technion - Israel Institute of Technology
Haifa 32000, Israel

ABSTRACT

A common approach to dealing with distributed systems is to describe it in a Global Time or an Interleaving setting. Such a description allows one to think about such systems in terms of the more familiar sequential model. However, many researchers feel that significant properties of the systems may be lost through such modeling.

Lamport offers a formal axiomatic approach, but his, and other approaches that do not assume the existence of global time of atomic operations, result in non-intuitive and complicated correctness proofs.

The first contribution of this paper is the presentation of a new way of modeling such systems. The new approach combines the intuitive appeal of the global time model with the generality of Lamport's formal treatment. It provides a framework that allows easy translation of informal arguments to rigorous proofs.

Another contribution of this work is that we characterize a wide class of problems for which it is proven that the existence of a global time can be assumed without losing any generality. The much discussed problems of Concurrent Reading While Writing and the Mutual exclusion problems fall into this class. This enables axiomatic correctness proofs like those in [4,5] to be easily simplified. On the other hand, protocols conceived in a global time framework like those of [3,6,8,9] become more general.

* This work was carried out while the author was a visitor at, and supported by the University of Toronto, Computer Science Department.
INTRODUCTION

Concurrency in distributed systems seems to be difficult to reason about directly. A common solution to such a problem is to model the complicated system via a more familiar one. In this case the Interleaving Model allows one to think of distributed systems in terms of the simpler sequential model.

The interleaving model approach views a system as if it is executed by a single processor, and views each operation as if it is made up of finitely many atomic steps. In such a model the processor executes the atomic steps of all the processes of the systems in some sequential order.

Such modeling is very convenient to work with (for analysis of protocols, etc.). It is only natural to worry about the cost of such a simplification.

There seems to be an agreement that for the purposes of analyzing the lower levels of communication mechanisms, like the implementation of atomic registers, those simple models become inadequate. It is also recognized that intuitive arguments are not a sufficiently sound basis for such investigations.

There is a different approach to such issues -- the development of formal theories. Lately, this direction is taken by an increasing number of researchers. We use Lamport's work as a basis for this paper.

In a series of papers Lamport has presented a very elegant abstract formalism for distributed systems with concurrency. On top of offering a clear mathematical tool for analyzing such systems, Lamport's framework allows one to work without assuming the existence of either global time or atomic operations.

One major drawback in Lamport's and other axiomatic approaches is the lack of a natural formal semantics to support the deductive systems. Lamport in [5] explains it by basically claiming that any such semantics will fall short of the full generality of the theory. Others, Peterson and Burns, for an example, feel that any formal model "will add little but complexity to our discussion" [7].

As a result, to apply Lamport's theory one has to derive axiomatic proofs without having a model to serve as an intuitive guideline. The other difficulty with Lamport's theory is that, in order to achieve greater generality, it leaves out the assumption of global time (and also of the existence of atomic operations). These demands result in complicating many proofs, some simple protocols are thus doomed to carrying with them long technical correctness proofs.

We offer remedies to both of the above mentioned problems. We work in an axiomatic system that is essentially Lamport's (we add one axiom to his, the axiom $A_\ast$, but this axiom is implicit in his theory, as it is valid in his formal system executions). We present a formal semantics that enjoys the following properties:

1. It has a clear intuitive meaning.
2. It provably captures the full generality of Lamport's axiomatic theory.
3. It supplies a (mathematical) proof that in many "cases" (communication mechanisms, protocols, types of specifications) correctness proof for the interleaving model apply to the more general models -- to every model satisfying Lamport's axioms.

After giving a precise definition of the semantics we prove that for every formal model satisfying the axioms there is an isomorphic model in the class of our models.

Our semantics is based on First Order Modal Logic. A model is basically a collection of possible global time interpretations of a system execution. As the models are made up of global time interpretations, many properties of such interpretations can be lifted up to the general model. For a wide class of problems (that can
be syntactically characterized), our models "collapse" to the simple Interleaving (or Real Line) models.

The implications of these results are twofold:
For those who prefer a semantic reasoning, not only that we offer a rigorous semantics, but in the above mentioned cases the familiar Interleaving (or Real Line) models are proved to be a sound enough basis.
For those who choose axiomatic reasoning, we show that in those cases an extra axiom—the Global-Time-Axiom can be added to the set of axioms without losing generality.

1. A SHORT REVIEW OF LAMPORT'S FORMAL THEORY

This is a minimal outline of Lamport's theory, the reader is encouraged to consult [4, 5], for an elaborate presentation and discussion. Lamport bases his formal theory on two abstract relations over operation executions. For operation executions A, B, A → B stands for "A precedes B" and A ---> B for "A can causally affect B".

A System Execution is a triple <E, →, ---> > where E is a set of operation executions and →, ---> are binary relations over E. Lamport offers the following axioms:

A1: → is an irreflexive transitive relation.
A2: If A → B then A ---> B and B /→ A.
A3: (A → B and B ---> C) or (A ---> B and B → C) implies A ---> C.
A4: If A → B ---> C → D then A → D.
A5: For every A, {B : A /→ B} is finite. (This is assuming all events are terminating.)

An intuition for these axioms can be gained by considering the following model for it.

Let S be a partially ordered set and let E be a collection of non-empty subsets of S. For A, B, in E, define A → B iff ∀x ∈ A ∀y ∈ B (x < y) (in the sense of S), and A ---> B iff ∃x ∈ A ∃y ∈ B (x < y).

A straightforward checking shows that such models satisfy axioms A1, A2, A3, A4, and also the following axiom:

A4*: If A ---> B ---> C ---> D then A ---> D.

This last axiom was suggested by Abraham in [1] where a completeness theorem is proved for the above mentioned class of models with respect to {A1, A2, A3, A4, A4*}.

An important class of models is obtained when S is a linear (= total) ordering. In such a case the system satisfies an additional axiom—the Global Time Axiom: For all A, B, A ---> B or B → A.

On top of these axioms there are the communication axioms that specify the communication mechanism of a system. Lamport's idea is to express them in terms of the abstract arrows → and --->. We refer the reader to [5] for these.

* We were later informed that this result was obtained by Anger independently.
2. BASIC DEFINITIONS

1) We adopt Lamport's definition of a System Execution. Usually, we shall assume that Lamport's axioms $A_1 \ldots A_5$ hold in such a system.

2) For $I, J$, nonempty intervals of some linear order $<$
   
   $I \ll J$ if $\forall x \forall y (x \in I, y \in J \text{ imply } x < y)$
   
   $I \bigcirc J$ if $\exists x \exists y (x \in I, y \in J \text{ and } x < y)$.

3) A Global Time model is a system execution $(E, \rightarrow, \longrightarrow)$ such that $E$ is a set of closed non-empty intervals of a linear order and the system relations '$\rightarrow$', '$\longrightarrow$', are '$\emptyset$' and '$\ll$' respectively.

4) A function $f$ from a set $E$ to a set of nonempty intervals of some order $<$, is an embedding of $(E, \rightarrow, \longrightarrow)$ iff for every $A,B \in E$, if $A \rightarrow B$ then $f(A) \ll f(B)$ and if $A \longrightarrow B$ then $f(A) \bigcirc f(B)$.

Throughout this paper the underlying ordered set is the Real Line and $<$ is its usual order. All the results apply to any other linear ordering containing a copy of the rational numbers.

3. THE MODAL REAL EMBEDDING'S (MRE) MODELS

An MRE model is a modal system. It is made up of a collection of worlds, each such world $w$, determines its own satisfaction relation $|=_.$ The truth of a formula with the modal operator given world, depends upon the truth function in other worlds in the system.

The language we use is first order logic over two binary predicates '$\ll$', '$\emptyset$', augmented by the modal operator '$\Box$'.

The worlds in our model system have a fixed domain $E$ (conceived as the set of events of the distributed system we are modeling), so $\forall$ and $\exists$ range over $E$ in every world $w$.

Formally an MRE model $M$ is a triple $<U,E,F>$ where $U$ is a set (the universe of the modal system), $E$ is another set (the set of events) and $F$ is a two place function $F : U \times E \rightarrow$ closed nonempty intervals.

The relations $\ll$, $\emptyset$, among the events of $E$ in the world $w$ are induced through $F(w, \_)$ by the relations between the closed intervals.

The satisfiability relation is defined inductively.

Case 1: $\phi$ atomic:

$|= A \ll B$ if $F(w,A) \ll F(w,B)$;

$|= A \emptyset B$ if $F(w,A) \emptyset F(w,B)$.

Case 2: $\phi$ is a 1st order composition of shorter formulas:

$|= \phi$ is defined just like $|= \phi$ in the usual 1st order logic.

Case 3: $\phi = \Box \psi$:

$|= \phi$ holds iff $|= \psi$ holds for all $w' \in U$. 
Note that for every \( w, w' \in U \), \( w \models \psi \) \iff \( w' \models \psi \). For such formulas we use the notation \( w \models \psi \), omitting the subscript \( w \).

### The L-Companion of an MRE Model

Given an MRE model \( M = \langle U, E, F \rangle \) we derive a System Execution \( L_M = \langle E, \rightarrow, \rightarrow \rightarrow \rangle \), called the L-companion of \( M \), by using the same set of events \( E \) and letting \( A \rightarrow B \) hold (in \( L_M \)) \iff \( \models (A \prec B) \) (in \( M \)), and \( A \rightarrow \rightarrow B \iff \models (A \preceq B) \).

In other words, \( A \rightarrow B \) holds if in every \( w \in U \), \( F(w, A) \prec F(w, B) \) and \( A \rightarrow \rightarrow B \) if for all \( w \)'s \( F(w, A) \preceq F(w, B) \).

### Proposition

Given any MRE model \( M \), its L-companion \( L_M \) satisfies Lamport Axioms \( A_1 \ldots A_4 \) and the extra axiom \( A_5^* \).

### 4. THE MAIN THEOREM

**Theorem:** For every System Execution \( L = \langle E, \rightarrow, \rightarrow \rightarrow \rangle \) that satisfies \( A_1 \ldots A_5 A_5^* \), there exists a MRE model \( M_L \) such that \( L_M = L \).

The proof is via the next Lemma.

**Main Lemma:**

1) For every System Execution \( \langle E, \rightarrow, \rightarrow \rightarrow \rangle \), that satisfies the axioms \( A_1 \ldots A_5 \) and every \( A, B \in E \) if \( A \neq B \) and \( B \nrightarrow A \) then there exist an embedding \( f : E \rightarrow \text{Real Intervals} \) such that \( f(A) \cap f(B) \neq \emptyset \).

2) For every System Execution \( \langle E, \rightarrow, \rightarrow \rightarrow \rangle \) that satisfies \( A_1 \ldots A_5 \) and \( A_5^* \), and for every \( A, B \in E \) such that \( A \nrightarrow \rightarrow B \) there exists an embedding \( f \), to Real Intervals, such that \( f(B) \ll f(A) \).

Note that in part 1) of the lemma, axiom \( A_5^* \) is not assumed.

**Proof of Lemma:**

1) Given a System Execution \( \langle L, \rightarrow, \rightarrow \rightarrow \rangle \) and \( A \in E \) define a rank \( r(A) = |\{ B : B \rightarrow \rightarrow \rightarrow A \}| \) (the number of \( B \)'s in this set).

**Claim:**

1) \( r(A) \) is a finite number (by ax. 5),
2) \( A \rightarrow B \) implies \( r(A) < r(B) \) (by ax. 1),
3) \( C \rightarrow \rightarrow B \) imply \( r(C) < r(B) \) (by ax. 4).

Let \( A, B \) be such that \( A \rightarrow B \) and \( B \rightarrow \rightarrow \rightarrow A \).

Let \( d = r(A) - r(B) \) (w.l.o.g. assume \( r(B) \leq r(A) \)).

Define a new rank \( r^* \) by

\[
 r^*(X) = \begin{cases} 
 r(X) + d + 1 & \text{if } B \rightarrow X \\
 r(X) & \text{otherwise}
\end{cases}
\]

It is easy to check that \( r^* \) satisfies (all 3 parts) of the above claim.

Note that as \( B \nrightarrow A \) and \( B \nrightarrow B \) \( r^*(A) = r(A) \) and \( r^*(B) = r(B) \).

We define an embedding \( f^* \) from \( \langle E, \rightarrow, \rightarrow \rightarrow \rangle \) to real intervals by a sequence of approximations \( \langle f^i : i \in N \rangle \) defined inductively:

Let \( \langle X_i : i \in N \rangle \) be an inumeration of \( E \) (we assume \( E \) is countable) such that \( r^*(X_i) \leq r^*(X_j) \) whenever \( i < j \). The domain of \( f^i \) is \( \{ X_j : j \leq i \} \) and for \( X \in \text{Dom} (f^i) \), \( f^{i+1}(X) \geq f^i(X) \) and both share the same
minimal point. Assume \( f^i \) is defined, let \( f^{i+1}(X_{i+1}) \) be any one -- point interval \([r,x]\) such that \( r > \text{Sup}(\text{Range}(f^i)) \). For \( Y \in \text{Dom} f^i \) let \( f^{i+1}(Y) = f^i(Y) \) if \( X_{i+1} \notightarrow Y \). If \( X_{i+1} \rightarrow Y \) let \( f^{i+1}(Y) \) be the interval \([\min f^i(Y), x]\). Note that \( f^i(X_i) \neq f^i(X_i) \) only if \( X_j \rightarrow X_i \) by axiom 5 this happens for only a finite number of \( j \)'s. Let \( f^* \) be the union of all the \( f^i \)'s \( (f^*(X) = f^i(X) \) where \( i = \max(j: X_j \rightarrow X_i, \forall X_j = X_i) \). Let \( f^* \) be \( f^* \) with one modification: \( f^*(B) \) is extended to be the minimal interval containing \( f^*(B) \) and intersecting \( f^*(A) \). It is straightforward to check that \( f^* \) is as needed (use the claim).

2) To prove part 2, a similar construction is used. This time the definition of the rank is different.

We define \( A \ominus B \) if \( \exists C \) such that \( A \rightarrow C \rightarrow B \) or if \( A \rightarrow B \). Using axiom \( A_3 \) one shows that \( \ominus \) is an irreflexive transitive relation.

Let \( r(X) \) be the number of \( Y \)'s such that \( Y \ominus X \). The claim from Part 1 of the proof still holds when \( r \) is replaced by \( r \).

Given \( A, B \) such that \( A \notightarrow B \) note that if \( r(A) > r(B) \) then the construction of Part 1 works. If \( r(A) \leq r(B) \) let \( d = 1(X: A X) \) and \( r^*(X) = r(X) + d + 1 \) if \( X = A \) or \( A X \) and \( r^*(X) = r(X) \) otherwise. Using \( r^* \) (instead of \( r \)) repeat the construction of \( f^* \) from the proof of Part 1.

Remark: The Main Lemma and consequently the Main Theorem hold just as well without assuming \( A_3 \) holds in \( L \). To prove this we apply the completeness result of [1].

A Completeness Theorem The class of MRE models is sound and complete for the set of axioms \( \{ A_1 \cdots A_4, A_5 \} \).

Proof: The soundness follows from the Proposition at the end of section 3 above. To get completeness it suffices to show that every consistent extension \( S \) of these axioms has an MRE model. As \( \{ A_1 \cdots A_4, A_5 \} \) are all expressible as first order formulas, one can apply Godel's completeness theorem to get an abstract model for \( S \). Now apply the Main Theorem with the Remark above, to get an isomorphic MRE model.

Extensions: Note that the same proof shows that a similar completeness theorem holds for every 1st order theory extending \( \{ A_1 \cdots A_4, A_5 \} \).

5. APPLICATIONS

In this section we show how the Main Theorem can be applied to prove that for a wide class of problems the global time assumption can be assumed without losing any generality. Equivalently, it is shown that for such problems, the simplest model -- the Global Time Model, is a sound enough basis for the analysis of distributed systems. A similar result holds for working in an Interleaving Model framework, but for the sake of clarity we concentrate on global time.

The basic idea is as follows. Assume a statement \( \phi \) holds in every Global Time Model of a given system. By way of contradiction let \( L = \langle E, \rightarrow, 
\rightarrow, \rightarrow \rangle \) be a System Execution in which \( \phi \) fails. Apply the Main Theorem to get an MRE model \( M = \langle E, U, F \rangle \), isomorphic to \( L \). By the isomorphism \( \phi \) should fail in \( M \). But, \( M \) is made up of Global Time Models of the underlying system, the models defined by \( F \). As we assume that \( \phi \) is valid for such models, \( w \models \phi \) for every \( w \in U \), so \( M \models \square \phi \). Loosely speaking this implies that \( \phi \) holds in \( L \).

(Note that if \( \phi \) is an atomic formula, say \( A \Theta B \), than \( M \models \square \phi \) is equivalent to \( L \models A \rightarrow B \).

In order to turn this argument into a proof one has to be careful. First of all the language of \( L \) uses arrows \( \rightarrow, \rightarrow, \rightarrow \), where the language of \( M \) uses \( \Theta \) and \( \ll \). This is not a real problem, one solves it by the straightforward translation between these symbols. A more serious problem is that for certain \( \phi \)'s this scheme
won't work. For an example, let $\phi$ be $(A \rightarrow B$ or $B \rightarrow A)$, now $\Box (A \otimes B$ or $B \otimes A)$ does not imply $(\Box (A \otimes B$) or $\Box (B \otimes A)$), in such a case it maybe that for every $w \in U$, $|=\phi$ but yet $L$ does not satisfy $(A \rightarrow B$ or $B \rightarrow A$).

We shall briefly present some classes of properties for which the above argument does work. Full proofs are postponed to the full version of this paper.

Definition:

1) For a 1st order formula $\phi$ let $\phi^*$ be the modal logic formula obtained by replacing each relation symbol $R$ in $\phi$ by $\Box R$.

   For an example: $(\forall x \forall y (Rxy) \rightarrow T(x))^* = \forall x \forall y (\Box R (xy) \rightarrow \Box T(x))$.

2) We call $\phi$ distributed if $1 \models (\Box \phi \rightarrow \phi^*)$.

   ($S_5$ is the axiom system for first order modal logic for models based upon complete graphs with a fixed domain for all its worlds. Recall that MRIIs are such models.)

3) $\phi$ is transferable if $1 \models (\phi^* \rightarrow \Box \phi)$.

Lemma: Every universal closure of a $\{\rightarrow, \wedge\}$ combination of atomic formulas is distributed.

Proof: By induction on the construction of the formula using the Main Theorem, the distributivity of the modal $\Box$ over the connectives $\rightarrow$ and $\wedge$ and the Barkan formula ($\Box \forall x \phi \rightarrow \forall x \Box \phi$).

Examples:

(a) The following are distributive properties:

   FIFO: $\forall A \forall B$ (if $A \rightarrow B$ then $A' \rightarrow B'$).

   Atomicity: $\forall A \forall B$ (If $A \rightarrow B$ then $A \rightarrow B$).

   (Lamport defines atomicity as $\forall A \forall B$ ($\neg (A \rightarrow B) \wedge (B \rightarrow A)$)), but we feel that our formulation is the one closer to the meaning of the concept. This is also the formulation used by other researchers -- Peterson and Burns [5] when translated to the $\rightarrow$ --- $\rightarrow$ languages).

(b) Lamport's register axioms $B_3 B_5$ of [4] are all transferable, in particular so are the properties of being safe and regular and Lamport's notion of atomicity.

Definition:

1) Two system executions are history-equivalent if they have the same set of processes and the history of each process is the same in both.

2) A protocol is distributed if it implies the same next operation possibilities for history-equivalent execution (for each of the processes).

3) A property $\phi$ is internal if whenever $L_1, L_2$, are history equivalent then $L_1 \models \phi$ iff $L_2 \models \phi$.

Theorem: For a transferable $\phi$ and a distributive or internal $\psi$,

1) If in every global time system $\phi$ implies $\psi$ then this is the case in every system execution (provided it satisfies $A_1 \cdots A_4 A_5$).

2) If $P$ is a distributed protocol and $P$ guarantees $\psi$ in every global time model of $\phi$ then $P$ guarantees $\psi$ in every system execution (as above).
Proof: By way of contradiction assume \( L = <E, \rightarrow, \ldots > \) is a system execution of \( P \) that satisfies \( \phi \) but \( \psi \) fails there. We assume that in \( L \) the operation executions of each processor are linearly ordered by \( \rightarrow \). Let \( M \) be an MRE model isomorphic to \( L \). Each world in \( M \) is history-equivalent to \( L \), so \( P \) behaves there as it does in \( L \). As \( \phi \) is transferable it is satisfied by every world in \( M \). This contradicts the distributivity of \( \psi \), as \( \psi \) fails in \( L \).

Corollaries: If a protocol guarantees atomicity of (implemented) registers, or FIFO, or any other distributed property in a global time framework then it does so in every model.

Proof: Practically all protocols considered for distributed systems are distributed. The communication mechanism usually assumed for these problems are transferable and the above mentioned properties are distributed properties.

Mutual Exclusion: The Mutual Exclusion \( \forall A \forall B (A \rightarrow B \lor B \rightarrow A) \) is clearly not distributive property. Just the same as the above corollary holds for it. This is because by Part 1 of the Main Lemma, if such a formula fails in \( L \), it fails in some \( w \).

Syntactic Applications

In all the cases described above, the formal deductive calculus can be strengthened by adding the Global Time Axiom. As this axiom is not a consequence of the usual Lamport set of axioms, it does add deductive power to the formal theory. Just the same, for statements that fall in the categories described above, if they are provable in the extended system they are consequences of the usual one. Such a 'strengthening' gives the prover extra flexibility. As an example of such an application one can quite easily use the Global Time Axiom to get a shorter proof to the main technical theorem of [4,11]—theorem 2 of section 3 there.

To conclude this section, here are two corollaries of the main theorem that have a different nature.

Claim:

1) A system execution is isomorphic to a global time execution iff it satisfies: for all \( A, B \), \( A \rightarrow B \) or \( B \rightarrow A \).

2) A system execution is isomorphic to an atomic one, (= an execution in which each operation is made up of finitely many atomic sub-operations) iff it satisfies \( A^{\#} \).

The first part is stated by Lamport in [5] without a proof. Here it easily follows from the Main Theorem. The proof of the second part combines the techniques of this paper with the completeness theorem of [1].

5. DISCUSSION

We have presented a class of models for executions of distributed systems. This class is general enough to model concurrency (\( A \rightarrow B \) and \( B \rightarrow A \)) even without the use of a global clock or atomic operations. We have shown that it captures the full generality of Lamport's theory. The mere existence of such a semantic is important. It is very common in this area to see "semantic" correctness "proofs" that are carried out in some undefined intuitive model that the writer believes everybody knows. It shouldn't be wonder that faults are discovered in protocols that were " proven" correct in such a manner. On the other hand, without a sound semantics it is not so clear what is meant by the 'validity' of a statement that has a formal proof.

As mentioned in section 2 above, this is not the first formal semantics for Lamport's System Executions, there exists the partial order semantics, but that semantics has no intuitive appeal and was never meant to serve as a basis for analysing systems and protocols.
Our models do have an intuitive content. One can view an MRE model as a collection of possible recordings of a fixed run of a system, recordings done by different participating processes. The main theorem implies that a basic statement holds in the real system execution iff it holds in every such interpretation.

Another possible interpretation of MRE models is obtained by assuming that a real global clock does exist (though the processes are not aware of it). Now an MRE model can be viewed as a collection of different runs of the system under a given protocol. The system's rules and the protocol are defined through the formal relations of the associated System Execution.

What seems to be the most interesting feature of our semantics, is that it provides a proof that, for many (even 'most') of the issues that are currently discussed in this area of distributed computation theory, the simplest semantics -- the Interleaving Model, is a sound basis for analysis. It follows that for these issues the Global Time Axiom can be added to Lamport's axioms without losing any generality.

Acknowledgement

I wish to thank the theory group of the Dept. of Computer Science of Toronto University for their warm hospitality and the stimulating environment they provided me. I feel special gratitude towards Mike Luby and Al Borodin for many insightful discussions regarding this work.

This work was inspired by the work of Abraham and Magidor [2]. They introduced the idea of embedding a Lamport system in a Real Line and (implicitly) proved part 2 of our main Lemma (using a different proof technique).
REFERENCES


