Centrum voor Wiskunde en Informatica
Centre for Mathematics and Computer Science

E. Kranakis, K.N. Oikonomou

Fixpoint representations of characteristic sets of linear-time temporal formulas (Extended abstract)

Computer Science/Department of Algorithmics & Architecture Report CS-R8754 November

Centrum voor Wiskunde en Informatica
Amsterdam

The Centre for Mathematics and Computer Science is a research institute of the Stichting Mathematisch Centrum, which was founded on February 11, 1946, as a nonprofit institution aiming at the promotion of mathematics, computer science, and their applications. It is sponsored by the Dutch Government through the Netherlands Organization for the Advancement of Pure Research (Z.W.O.).

bqF31,bqF41

Copyright © Stichting Mathematisch Centrum, Amsterdam

FIXPOINT REPRESENTATIONS OF CHARACTERISTIC SETS OF LINEAR-TIME TEMPORAL FORMULAS

Evangelos Kranakis
Center for Mathematics and Computer Science
Kruislaan 413, 1098 SJ Amsterdam, The Netherlands
(eva@cwi.nl)

Kostas N. Oikonomou
AT&T Bell Laboratories, Holmdel, 07733 NJ, USA
(allegra!houdi!ko)

ABSTRACT

We present an algebraic-axiomatic method for computing existential and universal characteristic sets of linear-time temporal logic formulas on directed graphs. The set of all nodes v of a given graph (model) such that all (respectively, some) infinite walks starting from v satisfy a formula ϕ is called the universal (respectively, existential) characteristic set of ϕ. We reduce the computation of the characteristic set to finding the least or greatest fixpoint of a system of set equations. Our method is sufficient to handle the following subsets of the logic $L(\Box, \Diamond, \bigcirc, \wedge, \vee, \sim)$: formulas in which the temporal connective $\Diamond$ applies only to boolean sub-formulas, formulas in which $\Box$ does not occur, and formulas that express general fairness properties of concurrent systems, such as impartiality, justice, and fairness. The representations of the characteristic sets obtained are model-independent, in the sense that the same representation holds for all graphs, and regardless of whether or not they are finite or infinite.

1980 Mathematics Subject Classification: 68N05, 68N15
CR Categories: F.3.1, F.4.1
Keywords and Phrases: temporal logic, fixpoint, set-transformer, temporal functional equation, walk, universal and existential characteristic set.
Note: This paper is submitted for publication elsewhere.

Report CS-R8754
Centre for Mathematics and Computer Science
P.O. Box 4079, 1009 AB Amsterdam, The Netherlands

1. INTRODUCTION

As is nicely explained in [La], temporal logic has proven to be useful in the formal specification and analysis of programs. A basic question in formal program verification is: given a program P —which may be deterministic or non-deterministic, sequential or parallel— do all, or some, of its execution sequences satisfy a temporal formula ϕ? Assume that the set of execution sequences of P can be represented as the set of walks in a directed graph G, whose vertices correspond to the states of P [1]. To answer the question posed above, one then needs to check if every, or some, walks in G are models of (satisfy) the formula ϕ; thus the problem is sometimes called *model-checking*. If P is finite-state, G is finite, and the model-checking problem has been shown in [CES] to be solvable in polynomial time for formulas of *branching*-time temporal logic, but, as shown in [SC], it is PSPACE-complete for formulas of propositional *linear*-time temporal logic (PTL). An algorithm to determine whether all walks in $G = (V, E)$ satisfy a PTL formula ϕ has been given in [LP], and runs in worst-case time polynomial in $|E|$ and exponential in the length of ϕ. This algorithm, as well as similar ones for more general temporal logics (see [ES] and [VW]), is based on the connection between linear-time temporal logic and the theory of finite automata accepting infinite strings. The basic idea is that the *tableau* for the formula $\sim\phi$ can be turned into a non-deterministic finite automaton $\mathcal{A}(\sim\phi)$ which accepts only the infinite strings that are models of $\sim\phi$. Then one tries to check if there is an infinite walk in G accepted by $\mathcal{A}(\sim\phi)$; if there is no such walk, then ϕ is satisfied on all walks of G, otherwise it isn't.

Here we propose an approach to the model-checking problem with an *axiomatic* and *algebraic*, rather than a model-theoretic, flavor. More precisely, we are interested in determining the *characteristic sets* of ϕ on G. The *universal* characteristic set $\mathsf{C}_u(\phi;G)$ of ϕ on G contains the vertices of G which are such that all walks beginning at them satisfy ϕ. The *existential* characteristic set $\mathsf{C}_e(\phi;G)$ consists of the vertices from which there is a walk satisfying ϕ. Our approach to finding these sets can be summarized as follows. First we derive from ϕ a *temporal functional equation* (tfe) such that ϕ *is either its least or greatest solution*

1. For concurrent programs, some model of parallel execution (e.g. interleaving) must be used in forming G.

(an extremal solution); the tfe for ϕ *can be thought of as an inductive definition of* ϕ. *Then we translate* the tfe into a *set* equation for the characteristic set of ϕ. The required set is guaranteed to be an extremal solution of the equation, which has the form $C = f(C)$, where f is a *monotonic set transformer* defined on V. Our set can then be computed *inductively*, as the least or greatest *fixpoint* of this transformer [2]. It is not difficult to see that characteristic sets *can* be defined inductively [3], but the problem lies in finding such a definition from which the sets are easily computable. This is exactly the issue addressed here.

Given a formula ϕ in the logic $L(\bigcirc, \diamond, \Box, \vee, \wedge, \sim)$ (with some restrictions mentioned below), whose atomic subformulas are $\alpha_1,..., \alpha_s$, we show how to construct a set transformer $f_\phi(X_1,..., X_s)$ by composing certain elementary set transformers (section 2.3), such that for all graphs G,

$$C_u(\phi; G) = f_\phi(C_u(\alpha_1; G),..., C_u(\alpha_s; G)).$$

A similar *dual* result holds for existential characteristic sets. Obtaining the tfe for ϕ is the difficult step in this procedure, because only tfe's of a restricted form are translatable into set equations on an arbitrary G; in particular, it is difficult to ''universally'' translate disjunctions of formulas, and to ''existentially'' translate conjunctions. At its present state, our method is sufficient to handle formulas of the following types:

1. Formulas in which the temporal connective $\diamond$ applies only to boolean sub-formulas, but there is no restriction on the occurrences of $\bigcirc$ and $\Box$ (theorem 6.1).

2. Formulas in which the temporal connective $\Box$ does not occur at all, but there is no restriction on the occurrences of $\bigcirc$ and $\diamond$ (theorem 6.2).

3. General ''fairness formulas'', i.e. formulas that can express properties of parallel programs such as impartiality (every process is executed infinitely often during the computation), justice (every

---

2. The idea of interpreting temporal operators as fixpoints of predicate transformers originally appeared in [EC], and in a much clearer form in [Sif] and [QS].

3. A very condensed argument runs as follows. Taking the definition of $C_u(\phi;G)$ given in section 2.2 as an example, the predicate $w \in W_v \supset w \models \phi$ can be shown to be arithmetical over the natural numbers $\mathbf{N}$. Hence, by adding a universal 2nd order quantifier $(\forall w)$, we obtain a set in Π^1_1. We know from [Mo], sec. 1B-1D, that every Π^1_1 set over $\mathbf{N}$, and in fact only such sets, can be defined inductively by a recursive operator.

process enabled almost everywhere is executed infinitely often), fairness (every process enabled infinitely often is executed infinitely often), etc. (theorems 7.1 and 7.2).

The graph G may be specified either by an explicit list of vertices and edges, or it may be defined by a set of predicates from which its edges can be generated. Sometimes the "symbolic" description by predicates can be much smaller than an explicit one, and if G is infinite, it is the only possible finite description. Our approach is suited to computing characteristic sets symbolically [4], so, laying convergence questions aside, we can compute characteristic sets on *infinite*, as well as on finite graphs. It is not clear whether it is possible to do this with the automata-based approach. Moreover, the representations we obtain are *model independent*, i.e. the same representation holds for all graphs, and irrespectively of whether they are finite or infinite. In contrast, the representations of [LP] and [EL] hold only for finite graphs, and also depend on the particular G under consideration. To illustrate the difference note that the concept of a *strong component* of a graph is indispensable in the automata-based approach, since it is used to define what it means for a finite automaton to accept an infinite string. However, we show in section 7 how to compute the set $\mathsf{C}_u(\Diamond\Box a; G)$ for an arbitrary G *without* any reference to its strong components.

Much of the interest of our results lies in the *temporal theorems* listed in section 5. We use these theorems to transform a tfe into a simpler, more easily translatable form. The theorems also provide algebraic insight into the meaning of PTL formulas, which the automata-theoretic method does not. In dealing with the logic $L(\mathsf{O}, \Diamond, \wedge, \vee)$, we also show that it is often advantageous for the purposes of translation, to transform a future PTL formula into an equivalent *past* PTL formula; we believe that this exposes a novel aspect of the past in linear-time temporal logic.

The results presented in this paper are not sufficient to handle all formulas in the logic $L(\mathsf{O}, \Diamond, \Box, \wedge, \vee, \sim)$, or formulas involving the "until" and "precedes" operators U and P, so our method is not as general as the tableaux-and-automata one. However, our results cover a useful subset of linear-time PTL, and they appear to be extensible.

---

4. Similar work has been done in [Cou] and [Sif].

2. DEFINITIONS

2.1 Well-Founded Formulas and Semantics

Let Ω be a possibly infinite set of atomic propositions. The (well-founded) formulas of linear time temporal logic are built up from the set Ω of atomic formulas using the usual propositional connectives $\wedge, \vee, \sim$, as well as the temporal connectives $\bigcirc, \Diamond, \Box, \mathsf{U}, \mathsf{P}$. Those well-founded formulas which are built up from the atomic formulas in Ω using only the propositional connectives $\wedge, \vee, \sim$ are called *boolean formulas.*

Let $G = (V, E)$ be a finite or infinite directed graph, with vertices V and edges E, and such that every vertex has at least one outgoing edge (possibly a loop)[5]. An *interpretation* mapping $I : V \to 2^{\Omega}$ associates with each node $v \in V$ a set $I(v) \subseteq \Omega$ of atomic propositions which are true at node v. A walk w in G is an infinite sequence $w_0,\ldots,w_n,\ldots$ of nodes of G such that $E(w_n, w_{n+1})$, for all $n \geq 0$. For any walk w let $w^{(n)}$ be the "suffix" walk obtained from w by omitting the first n nodes $w_0,\ldots,w_{n-1}$.

Given a graph G and interpretation I, $(G, I, w) \models \phi$ will mean that the walk w in G *satisfies* formula ϕ under interpretation I. We will normally use the briefer notation $w \models \phi$, in which G and I are implicit. The satisfaction relation $\models$ is defined inductively as follows:

$$w \models \alpha \quad \Leftrightarrow \quad \alpha \in I(w_0), \ \alpha \in \Omega \tag{S1}$$

$$w \models \phi \wedge \psi \quad \Leftrightarrow \quad w \models \phi \wedge w \models \psi \tag{S2}$$

$$w \models \phi \vee \psi \quad \Leftrightarrow \quad w \models \phi \vee w \models \psi \tag{S3}$$

$$w \models \sim\phi \quad \Leftrightarrow \quad \text{not } w \models \phi \tag{S4}$$

$$w \models \bigcirc\phi \quad \Leftrightarrow \quad w^{(1)} \models \phi \tag{S5}$$

$$w \models \Box\phi \quad \Leftrightarrow \quad \forall n\,(w^{(n)} \models \phi) \tag{S6}$$

$$w \models \Diamond\phi \quad \Leftrightarrow \quad \exists n\,(w^{(n)} \models \phi) \tag{S7}$$

$$w \models \phi \mathsf{U} \psi \quad \Leftrightarrow \quad \exists n\,(w^{(n)} \models \psi \wedge \forall m < n\,(w^{(m)} \models \phi)) \tag{S8}$$

$$w \models \phi \mathsf{P} \psi \quad \Leftrightarrow \quad \forall n\,(w^{(n)} \models \psi \supset \exists m < n\,(w^{(m)}) \models \phi)) \tag{S9}$$

It follows that the operators $\Diamond$ and $\Box$ are duals, and so are U and P. We will denote the fact that for all

5. It is no essential restriction that we assume that every node of the graph has outdegree at least 1. It would amount to the same thing if we were to add a loop to every node of the original graph with outdegree 0.

walks w in G, $(G; w) \models \phi$ by $G \models \phi$; also, we will denote the fact that for all graphs G, $G \models \phi$ by $\models \phi$. When the graph G is easily understood, we will write $w \models \phi$ instead of $(G; w) \models \phi$.

2.2 Characteristic Sets

Let $G = (V, E)$ be a directed graph as above and let $I : V \to 2^{\alpha}$ be an interpretation. For any $v \in V$, let W_v be the set of all walks of G beginning at node v. To any formula ϕ correspond *universal* and *existential characteristic sets* of vertices:

$$\mathsf{C}_u(\phi) = \{v \in V \mid \forall w (w \in W_v \supset w \models \phi)\},$$
$$\mathsf{C}_e(\phi) = \{v \in V \mid \exists w (w \in W_v \wedge w \models \phi)\}.$$

A vertex belongs to $\mathsf{C}_u(\phi)$ iff all walks beginning at it satisfy ϕ; it belongs to $\mathsf{C}_e(\phi)$ iff there is a walk from it that satisfies ϕ (note the relationship with branching-time semantics). Although the underlying graph G does not appear in these definitions, the characteristic sets are really defined with respect to a particular G; a more complete notation, which we will use occasionally, is $\mathsf{C}_u(\phi;G)$ and $\mathsf{C}_e(\phi;G)$. We will denote the fact that all walks in G satisfy ϕ by $G \models \phi$. Clearly, this is equivalent to $\mathsf{C}_u(\phi;G) = V$. The characteristic sets of atomic formulas are particularly simple: if α is atomic, then

$$\mathsf{C}_u(\alpha) = \mathsf{C}_e(\alpha) = \{v \in V : \alpha \in I(v)\}$$

Example 2.1: More generally, let α be a *boolean* (i.e., free from temporal connectives) formula. Write α in conjunctive normal form $\alpha \equiv (\alpha_{1,1} \vee \cdots \vee \alpha_{1,k_1}) \wedge \cdots \wedge (\alpha_{r,1} \vee \cdots \vee \alpha_{r,k_r})$, where the $\alpha_{i,j}$ are either atomic or negated atomic. Then it is clear that

$$\mathsf{C}_u(\alpha) = \mathsf{C}_e(\alpha) = (\mathsf{C}_u(\alpha_{1,1}) \cup \cdots \cup \mathsf{C}_u(\alpha_{1,k_1})) \cap \cdots \cap (\mathsf{C}_u(\alpha_{r,1}) \cup \cdots \cup \mathsf{C}_u(\alpha_{r,k_r})).$$

2.3 Basic Set Transformers

Given any graph $G = (V, E)$ we define the basic set transformers $post^G$, $\forall post^G$, pre^G, $\exists pre^G$ as follows. For any set A of vertices of G,

$$post^G(A) = \{v \in V : \exists u\ (E(u,v) \wedge u \in A)\},$$
$$\forall post^G(A) = \{v \in V : \forall u\ (E(u,v) \supset u \in A)\},$$
$$pre^G(A) = \{v \in V : \forall u\ (E(v,u) \supset u \in A)\},$$
$$\exists pre^G(A) = \{v \in V : \exists u\ (E(v,u) \wedge u \in A)\}.$$

Thus, given a graph G, the set $post(A)$ contains all vertices that have a predecessor in A; $\forall post(A)$ contains the vertices all of whose predecessors are in A. The set $pre(A)$ consists of the vertices all of whose successors are in A, while $\exists pre(A)$ consists of the vertices one of whose successors is in A [6]. For simplicity, we will from now on omit the superscript G from the above notations.

3. THE PAST

In this paper we only consider the "future fragment" of linear-time temporal logic. However, by introducing the basic past operators $\ominus$ and $\odot$ (strong and weak "previous" [7]) into our *derivations* only, some of them are greatly facilitated. It is important to note that "past" formulas, i.e. involving $\ominus$ or $\odot$ in our case, are interpreted *only on suffixes of walks*, and not on walks themselves. The semantics of $\ominus$ and $\odot$ are:

$$\begin{aligned} w^{(n)} \models \ominus\phi &\quad \Leftrightarrow \quad n > 0 \wedge w^{(n-1)} \models \phi, \\ w^{(n)} \models \odot\phi &\quad \Leftrightarrow \quad n > 0 \supset w^{(n-1)} \models \phi, \end{aligned} \tag{3.1}$$

ϕ being any temporal formula. $\ominus$ and $\odot$ are duals and are related by

$$\begin{aligned} &\models \sim\ominus\phi \equiv \odot\sim\phi \\ &\models \phi \equiv \bigcirc\ominus\phi \equiv \bigcirc\odot\phi. \end{aligned} \tag{3.2}$$

$\ominus$ and $\odot$ distribute over $\wedge$ and $\vee$, just like $\bigcirc$ does [8].

To define the characteristic sets of past formulas we need to generalize the definitions given in §2 as follows. If ϕ is *any* formula in the logic $L(\bigcirc, \ominus, \odot, \Diamond, \Box, \wedge, \vee, \sim)$, its existential and universal characteristic sets on a graph G are defined by

---

6. *pre* and *post* have been introduced in [Sif]. Note however that our *pre* corresponds to his $pr\bar{e} \wedge pre$.
7. Our $\ominus$ and $\odot$ correspond to the $\ominus$ and $\odot$ of [LPZ].
8. These properties may be violated if one tries to interpret $\ominus$ or $\odot$ on a walk.

$$\begin{aligned} C_e(\phi) &= \{v \mid \exists w\,(\exists m\,(w^{(m)} \in W_v \wedge w^{(m)} \models \phi))\} \\ C_u(\phi) &= \{v \mid \forall w\,(\forall m\,(w^{(m)} \in W_v \supset w^{(m)} \models \phi))\}. \end{aligned} \tag{3.3}$$

For example, the first definition says that v belongs to the existential characteristic set of ϕ iff there is a walk w in G with a suffix which begins at v and which (suffix) satisfies ϕ. If ϕ is a future formula, we can take the suffix to be $w^{(0)}$ [9].

4. TEMPORAL FUNCTIONAL EQUATIONS, TRANSLATION RULES, AND SET EQUATIONS

4.1 Temporal Functional Equations

A *temporal functional equation (tfe)* for the (unknown) formula ϕ is a temporal formula f in which ϕ occurs as a subformula. We will say that a formula σ is a *solution* of the tfe $f(\phi)$ iff $\models f(\sigma)$, i.e. iff the substitution of σ for ϕ in f results in a *valid* formula. If σ is a solution of $f(\phi)$, then any formula equivalent to σ is also a solution. For example, $\phi \supset \Diamond\psi$, with ψ assumed known, is a temporal functional equation for ϕ. The formulas ψ, $\bigcirc\psi$, $\Diamond\psi$, $\Box\psi$, and $\Diamond\Box\psi$ are all solutions of this tfe. Temporal functional equations have *extremal* solutions:

- ω is the *greatest* solution of the tfe $F(\phi)$ iff for any other solution χ of $F(\phi)$ we have $\models \chi \supset \omega$
- ω is the *least* solution of the tfe $F(\phi)$ iff for any other solution χ of $F(\phi)$ we have $\models \omega \supset \chi$

The least solution of our example tfe is $\perp$, the identically false formula.

The following four theorems show that the basic temporal formulas $\Box\psi$, $\Diamond\psi$, $\chi U\psi$, and $\chi P\psi$ *are the extremal solutions of certain basic tfe's.*

Theorem A: The greatest solution of the tfe $\phi \equiv \psi \wedge \bigcirc\phi$ is $\Box\psi$.

Theorem E: The least solution of the tfe $\phi \equiv \psi \vee \bigcirc\phi$ is $\Diamond\psi$.

---

9. The reader should be aware of the fact that according to our definitions, $C_u(\ominus\alpha;G) = \varnothing$ for any model G. To avoid this, we only consider C_u's of past formulas that contain only $\ominus$ (see rules T_5, T_6, and the proof of theorem 6.2). By the duality (3.2a), the same remark applies to the existential characteristic set $C_e(\ominus\alpha;G)$ $(= V$ for any $G)$.

Theorem U: The least solution of the tfe $\phi \equiv \psi \vee (\chi \wedge \bigcirc\phi)$ is $\chi U \psi$.

Theorem P: The greatest solution of the tfe $\phi \equiv \psi \wedge (\chi \vee \bigcirc\phi)$ is $\chi P \sim\psi$.

Note that Theorems U and P subsume Theorems E and A respectively. The theorems are best proved by the semantics of sec. 2.1 (see, e.g. [Oik]).

4.2 Translation Rules

The following *translation rules* allow us to transform a relation between temporal formulas to a relation between their characteristic sets.

T_0: $G \models (\phi \equiv \psi) \Rightarrow C_u(\phi;G) = C_u(\psi;G)$ and $C_e(\phi;G) = C_e(\psi;G)$

T_1: $C_u(\phi \wedge \psi) = C_u(\phi) \cap C_u(\psi)$
$C_e(a \wedge \psi) = C_e(a) \cap C_e(\psi)$, if a is boolean

T_2: $C_u(\sim\phi) = \neg C_e(\phi)$

T_3: $C_e(\phi \vee \psi) = C_e(\phi) \cup C_e(\psi)$
$C_u(a \vee \psi) = C_u(a) \cup C_u(\psi)$, if a is boolean

T_4: $C_u(\bigcirc\phi) = pre(C_u(\phi))$
$C_e(\bigcirc\phi) = \exists pre(C_e(\phi))$

Call π a *strong* (respectively, *weak*) *past* formula if the only temporal connective occurring in it is $\ominus$ (respectively $\odot$). Call ϕ a *future* formula if none of the past temporal connectives $\ominus$, $\odot$ occur in it. The following rules hold only when π is past formula and ϕ a future formula:

T_5: $C_u(\ominus\pi) = \forall post(C_u(\pi))$, π is a weak past formula
$C_e(\ominus\pi) = post(C_e(\pi))$, π is a strong past formula

T_6: $C_u(\pi \vee \phi) = C_u(\pi) \cup C_u(\phi)$, π is a weak past formula
$C_e(\pi \wedge \phi) = C_e(\pi) \cap C_e(\phi)$, π is a strong past formula

Using these rules, we can sometimes translate a temporal functional equation for a formula ϕ into a set equation for its (universal or existential) characteristic set.

Example 4.1: If α is boolean, then the tfe $\phi \equiv \alpha \vee \bigcirc\phi$, can be translated by rule T_3 into $\Phi = A \cup pre(\Phi)$, where the capital letter A represents the universal characteristic set of the boolean formula α.

However, if α were a general temporal formula, this translation cannot be performed. The importance of introducing the past into our derivations is that given a ''future'' tfe involving $\bigcirc$, untranslatable by rules T_0 to T_5, it is sometimes possible to find a *related* tfe, involving $\ominus$ or $\ominus$, which *is* translatable by virtue of rule T_6.

Example 4.2: Although $\phi \equiv (\bigcirc\bigcirc a \wedge b) \vee \bigcirc\phi$ is untranslatable, the closely related tfe $\phi \equiv (\ominus\ominus b \wedge a) \vee \bigcirc\phi$ is translatable into $\Phi = (A \cap \forall post^2(B)) \cup pre(\Phi)$.

4.3 Set Transformers and Set Equations

Given a finite or infinite set V, a unary set transformer on V is a function mapping subsets of V into other subsets of V, i.e. $2^V \rightarrow 2^V$. We will also consider n-ary set transformers on V, i.e. mappings $(2^V)^n \rightarrow 2^V$ (see for example the statements of theorems 6.1, 6.2, etc.).

4.3.1 Operations on Set Transformers

Besides using $\cup$ and $\cap$ for the union and intersection of sets, we will also use them to denote analogous operations on set transformers. If f and g are set transformers,

$$(f \cup g)(A) = f(A) \cup g(A) \quad \text{and} \quad (f \cap g)(A) = f(A) \cap g(A)$$

Composition $\cdot$ and *dualization* $\dagger$ are defined by

$$(f \cdot g)(A) = f(g(A)) \quad \text{and} \quad f^{\dagger}(A) = \neg f(\neg A)$$

f^k denotes f composed with itself k times. Note that pre and $\exists pre$ are duals, and so are $post$ and $\forall post$.

If I is the identity set transformer, we define

$$f^*(A) = (I \cup f \cup f^2 \cup \cdots)(A) = \bigcup_{k=0}^{\infty} f^k(A)$$

$$f^\times(A) = (I \cap f \cap f^2 \cap \cdots)(A) = \bigcap_{k=0}^{\infty} f^k(A)$$

A set transformer f is called *monotonic* if it preserves the ordering $\subseteq$ on V, that is, if for any A, B, $A \subseteq B \Rightarrow f(A) \subseteq f(B)$. f is *$\cup$–distributive* if $f(A \cup B) = f(A) \cup f(B)$, and *$\cap$–distributive* if $f(A \cap B) = f(A) \cap f(B)$. f will be called *$\cup$–continuous* if it is "infinitely $\cup$-distributive", i.e. if for any infinite increasing sequence of sets $A_0 \subseteq A_1 \subseteq \cdots$

$$f(\bigcup_{i=0}^{\infty} A_i) = \bigcup_{i=0}^{\infty} f(A_i),$$

and *$\cap$–continuous* if for any infinite decreasing sequence $A_0 \supseteq A_1 \supseteq \cdots$

$$f(\bigcap_{i=0}^{\infty} A_i) = \bigcap_{i=0}^{\infty} f(A_i)$$

Note that any monotonic set transformer defined on a *finite* lattice is also continuous.

4.3.2 Properties of the Operations

The operations $\cup, \cap, \cdot, \dagger, {}^*, {}^\times$ have the following properties:

- $(f \cap g)^\dagger = f^\dagger \cup g^\dagger$; $(f \cup g)^\dagger = f^\dagger \cap g^\dagger$; $(f \cdot g)^\dagger = f^\dagger \cdot g^\dagger$
- f is monotonic $\Leftrightarrow$ $f^\dagger$ is monotonic
- f is $\cup$- ($\cap$-) continuous $\Leftrightarrow$ $f^\dagger$ is $\cap$- ($\cup$-) continuous
- $\cup$, $\cap$, and $\cdot$ preserve both $\cup$- and $\cap$-continuity
- $(f^*)^\dagger = (f^\dagger)^\times$, and $(f^\times)^\dagger = (f^\dagger)^*$
- * preserves monotonicity and $\cup$-distributivity and continuity
- $^\times$ preserves monotonicity and $\cap$-distributivity and continuity
- A *constant* set transformer $\mathbf{C}$ is both $\cup$- and $\cap$- distributive [10]

---

10. Constant set transformers, denoted here by a bold letter, map any subset of V to the set corresponding to their name. E.g. $\mathbf{C}(X) = C$, for any $X \subseteq V$.

- If f is $\cup$-distributive, $C \cap f$ is also $\cup$-distributive
- If f is $\cap$-distributive, $C \cup f$ is also $\cap$-distributive
- If f is $\cup$-continuous and $f(\varnothing) = \varnothing$, then $(C \cup f)^*(\varnothing) = f^*(C)$
- If f is $\cap$-continuous and $f(V) = V$, then $(C \cap f)^\times(V) = f^\times(C)$

4.3.3 Continuity and Fixpoints

The set Φ is a *fixpoint* of the set transformer f if $f(\Phi) = \Phi$. A fundamental theorem of Tarski ([Tar]) says that every *monotonic* set transformer defined on a complete lattice (2^V with $\subseteq$, $\cup$ and $\cup$, in our case) has a set of fixpoints, which themselves form a complete lattice. Φ is the *least* fixpoint of f if it is contained in every other fixpoint of f, and it is the *greatest* fixpoint of f if it contains every other fixpoint. Let A be a subset of V. Least and greatest fixpoints of dual set transformers are related by ([Sif], Prop. 7):

Theorem FD:

Φ is the least fixpoint of f containing A $\Leftrightarrow$ $\neg\Phi$ is the greatest fixpoint of $f^\dagger$ contained in $\neg A$.

If a set transformer is also *continuous* in addition to being monotonic, then its extremal fixpoints can be conveniently computed as follows: [11]

Theorem F1: If f is $\cup$-continuous and A is s.t. $A \subseteq f(A)$, then $f^*(A)$ is the least fixpoint of f containing A.

Theorem F2: If f is $\cap$-continuous and A is s.t. $A \supseteq f(A)$, then $f^\times(A)$ is the greatest fixpoint of f contained in A.

In the first case, the fixpoint is found when the increasing sequence $A \subseteq f(A) \subseteq f^2(A) \subseteq \cdots$ stabilizes. In the second case, the fixpoint is found when the decreasing sequence $A \supseteq f(A) \supseteq f^2(A) \supseteq \cdots$ stabilizes. In both cases, stabilization will occur within a finite time if the set V is finite, but this may or may not happen if V is infinite. Also recall that if V is finite, theorems F1

11. The next two theorems appear in [Sif], Proposition 6.

and F2 apply regardless of continuity.

It is easy to show (see [Sif]) that *pre* is monotonic, $\cap$-distributive, and $\cap$-continuous. Also *post* is monotonic, $\cup$-distributive, and $\cup$-continuous. If the graph G is *finitely-branching*, then *pre* is also $\cup$-continuous and *post* is $\cap$-continuous ([Sif]).

4.3.4 Extremal Solutions of Set Equations

Suppose that we are trying to find $\mathsf{C}_u(\phi;G)$, and we know that ϕ is the least or greatest solution of a certain tfe $\phi \equiv f(\phi)$. Also suppose that by using the rules of §4.2 this tfe is translated into a set equation for $\mathsf{C}_u(\phi;G)$ or $\mathsf{C}_e(\phi;G)$ of the form $\Phi = F(\Phi)$, where F is a set transformer on V. It is easy to show that the translation from tfe's to set equations is "monotonic", in the sense that

Lemma M: If $\models \chi \supset \psi$, then for any model G,

$$\mathsf{C}_u(\chi;G) \subseteq \mathsf{C}_u(\psi;G) \qquad \text{and} \qquad \mathsf{C}_e(\chi;G) \subseteq \mathsf{C}_e(\psi;G)$$ [12]

However, we would like to have the translation guarantee even more, that is *preserve* the extremality of solutions. Given Lemma M, one way to do this is to show that in addition, there is a 1-1 correspondence between the set of solutions of the tfe $\phi \equiv f(\phi)$ and the set of solutions of its translation $\Phi \equiv F(\Phi)$. This correspondence exists if for every $v \in V$ there is an atomic proposition $at(v)$ which is true exactly at node v. This condition is quite reasonable, and eliminates the necessity for proofs such as that of Lemma 4.1 below, the proof following Lemma 7.1 in sec. 7, etc. Nevertheless, we will not require this condition in order to obtain the most general results possible.

To find extremal solutions of set equations, we note that

- If F is $\cup$-continuous, the *least* solution of the equation $X = F(X)$ is $F^*(\varnothing)$
- If F is $\cap$-continuous, the *greatest* solution of the equation $X = F(X)$ is $F^{\times}(V)$

Three simple results that will be used repeatedly in the sequel are included in the lemma below.

---

12. Neither of these two inclusions implies $G \models \chi \supset \psi$.

Lemma 4.1: For any formula ϕ and any boolean formula α,

$$C_u(\Box\phi) = pre^{\times}(C_u(\phi)) \tag{4.1}$$

$$C_u(\langle\rangle\alpha) = (A \cup pre)^*(\varnothing) \tag{4.2}$$

$$C_u(\alpha P\phi) = (A \cup pre)^{\times}(C_u(\sim\phi)) \tag{4.3}$$

Here A is the constant set transformer (sec. 4.3.2) corresponding to $A = C_u(\alpha)$.

Proof: (4.1) follows immediately from the semantics of $\Box$ and the definition of $^{\times}$. To see (4.2), notice that $\langle\rangle\alpha$ is the least fixpoint of the tfe $\phi \equiv \alpha \vee \bigcirc\phi$ (theorem E of sec. 4.1). Hence, $C = C_u(\langle\rangle\alpha)$ satisfies the set equation $X = A \cup pre(X)$. Thus, it is clear that if F is the least fixpoint of this set equation then $F \subseteq C$. It remains to show that $C \subseteq F$. Indeed, let $v = v_0 \notin F$. Then there exists a v_1 such that $E(v_0, v_1)$ and $v_0 \notin A$ and $v_1 \notin F$. Continue in this fashion to construct an infinite sequence $v_0, v_1, \ldots, v_k, \ldots$ such that for all k, $E(v_k, v_{k+1})$ and $v_k \notin A$ and $v_{k+1} \notin F$. Now, if $w = (v_0, v_1, \ldots, v_k, \ldots)$, then it is clear that $\neg(w \models \langle\rangle\alpha)$, which implies that $v \notin C$, as desired. This proves (4.2). The proof of (4.3) can be carried out along the same lines, using (S9) in sec. 2.1. Actually, (4.2) and (4.1) follow from (4.3).

■

5. TEMPORAL EQUIVALENCES

The following temporal equivalences are fundamental to the whole paper: they express the formula on the left hand side in a form which is easier to translate into a set equation. However, the equivalences are also interesting in themselves, as temporal *theorems*.

$$\models \Box\phi \vee \Box\psi \equiv \Box(\phi \vee \Box\psi) \wedge \Box(\Box\psi \vee \phi)$$
$$\models \langle\rangle\phi \wedge \langle\rangle\psi \equiv \langle\rangle(\phi \wedge \langle\rangle\psi) \vee \langle\rangle(\langle\rangle\psi \wedge \phi) \tag{5.1}$$

$$\models \langle\rangle(\langle\rangle\phi \wedge \langle\rangle\psi) \equiv \langle\rangle\phi \wedge \langle\rangle\psi$$
$$\models \Box(\Box\phi \vee \Box\psi) \equiv \Box\phi \vee \Box\psi \tag{5.2}$$

$$\models \langle\rangle(\phi \wedge \langle\rangle\psi) \equiv \langle\rangle\phi \wedge \phi P(\sim\langle\rangle\psi) \tag{5.3}$$

For any $n \geq m \geq 0$, (5.4)

$$\models \bigcirc^m\phi \vee \bigcirc^{m+1}\phi \vee \cdots \vee \bigcirc^{n-1}\phi \vee \langle\rangle(\bigcirc^n\phi \wedge \langle\rangle\psi) \equiv \bigcirc^m\langle\rangle\phi \wedge \bigcirc^n\phi P(\sim\langle\rangle\psi)$$

$$\models \Diamond\phi \vee \Box\psi \equiv \phi P[\sim(\psi \vee \Diamond\phi)] \tag{5.5}$$

$$\models \Diamond\Box\phi \wedge \Diamond\Box\psi \equiv \Diamond\Box(\phi \wedge \psi)$$
$$\models \Box\Diamond\phi \vee \Box\Diamond\psi \equiv \Box\Diamond(\phi \vee \psi) \tag{5.6}$$

$$\models \Diamond(\Box\phi \wedge \Diamond\psi) \equiv \Diamond(\Box\phi \wedge \psi)$$
$$\models \Box(\Box\phi \wedge \Diamond\psi) \equiv \Box(\phi \wedge \Diamond\psi) \tag{5.7}$$

$$\models \Diamond\Box\Diamond\phi \equiv \Box\Diamond\phi$$
$$\models \Box\Diamond\Box\phi \equiv \Diamond\Box\phi \tag{5.8}$$

$$\models \Diamond\Box(\phi \vee \Box\psi) \equiv \Diamond\Box\phi \vee \Diamond\Box\psi$$
$$\models \Box\Diamond(\phi \wedge \Diamond\psi) \equiv \Box\Diamond\phi \wedge \Box\Diamond\psi \tag{5.9}$$

$$\models \Diamond\Box(\phi \vee \Diamond\psi) \equiv \Diamond\Box\phi \vee \Box\Diamond\psi$$
$$\models \Box\Diamond(\phi \wedge \Box\psi) \equiv \Box\Diamond\phi \wedge \Diamond\Box\psi \tag{5.10}$$

$$\models \Diamond\Box\phi \vee \Box\Diamond \equiv \Box(\Diamond\Box\phi \vee \Diamond\psi)$$
$$\models \Box\Diamond\phi \wedge \Diamond\Box\psi \equiv \Diamond(\Box\Diamond\phi \wedge \Box\psi) \tag{5.11}$$

One way to establish (5.1) to (5.11) is by semantics, i.e. by using (S1)-(S9) of sec. 2.1. For an axiomatic proof style, see [MP].

6. RESTRICTED VERSIONS OF THE LOGIC $L(\mathsf{O}, \Diamond, \Box, \wedge, \vee, \sim)$

In this and the next section we are interested in finding fixpoint representations of the characteristic sets $C_u(\phi; G)$, $C_e(\phi; G)$, of some formula ϕ. The first result, Theorem 6.1, concerns formulas in the logic $L(\mathsf{O}, \Diamond, \Box, \vee, \wedge, \sim)$ such that $\sim$ and $\Diamond$ (respectively $\Box$) apply only to boolean formulas. The second result, Theorem 6.2, deals with formulas in the logic $L(\mathsf{O}, \Diamond, \vee, \wedge, \sim)$ such that $\sim$ and $\Diamond$ (respectively $\Box$) apply only to boolean formulas. Theorems 6.1 and 6.2 provide fixpoint representations for both universal and existential characteristic sets.

Theorem 6.1:

Let ϕ be a formula in the logic $L(\mathsf{O}, \Diamond, \Box, \vee, \wedge, \sim)$ such that $\sim$ and $\Diamond$ (respectively $\Box$) apply only to

boolean subformulas of ϕ and suppose that the atomic propositions occurring in ϕ are $\alpha_1,\ldots,\alpha_s$. Then there exists a set transformer $f_\phi(X_1,\ldots,X_s)$ (respectively, $g_\phi(X_1,\ldots,X_s)$) constructed from the operators $\sim, \cup, \cap, pre, ^\times, ^*$ (respectively, $\sim, \cup, \cap, \exists pre, ^\times, ^*$) via composition such that for all graphs G,

$$C_u(\phi; G) = f_\phi(C_u(\alpha_1; G),\ldots, C_u(\alpha_s; G))$$

(respectively, $C_e(\phi;G) = g_\phi(C_e(\alpha_1; G),\ldots, C_e(\alpha_s; G))$.

Proof:

Only the result for universal characteristic sets will be proved: the result for the existential characteristic sets will then follow by duality. The proof is by induction on the number $\#(\phi)$ of connectives occurring in the formula ϕ. If ϕ is boolean, the result is trivial (see example 2.1). If ϕ is the conjunction of the formulas χ, ψ then by translation rule T_1 in §4.2, $C_u(\phi) = C_u(\chi) \cap C_u(\psi)$. If ϕ is of the form $\bigcirc\psi$ then by translation rule T_4, $C_u(\phi) = pre(C_u(\psi))$. If ϕ is of the form $\Box\psi$ then by (4.1) in §4.3.3,

$$C_u(\phi) = pre^\times(C_u(\psi)) = \bigcap_{n\geq 0} pre^n(C_u(\psi)).$$

If ϕ is of the form $\Diamond\alpha$, with α boolean, then by (4.2) in §4.3.3,

$$C_u(\phi) = (A \cup pre)^*(\varnothing) = \bigcup_{n\geq 0}(A \cup pre)^n(\varnothing).$$

If ϕ is of none of the above forms, then it must be a disjunction $\phi_1 \vee \cdots \vee \phi_n$, where $n > 1$ and none of the ϕ_i is itself a disjunction. If one of the ϕ_i, say ϕ_1, is boolean, then the result follows trivially from the induction hypothesis, since by rule T_3, $C_u(\phi) = C_u(\phi_1) \cup C_u(\phi_2 \vee \cdots \vee \phi_n)$. If one of the ϕ_i, say ϕ_1, is a conjunction $\psi \wedge \chi$, then the result is clear from the induction hypothesis, since ϕ itself would have to be equivalent to a conjunction of two formulas each of which has fewer connectives than ϕ.

Hence, we reduce to the case where none of the ϕ_i is boolean, or a conjunction, or a disjunction. Let $\phi_1,\ldots,\phi_m$ be the only ϕ_i that are of the form $\bigcirc\psi_i$. Then ϕ is equivalent to the formula

$$\bigcirc(\psi_1 \vee \cdots \vee \psi_m) \vee \phi_{m+1} \vee \cdots \vee \phi_n.$$

It is easy to see that if $m > 1$ then the number of connectives of this last formula is reduced by at least 1, so the result follows from the induction hypothesis. Consequently, for the rest of the proof we can assume that the formula ϕ has the form $\phi_1 \vee \cdots \vee \phi_n$, where each of the ϕ_i begins with a temporal connective,

at most one of which is $\bigcirc$. The following lemma will be found useful; it is proved by induction on n using the dual of (5.1b).

Lemma 6.1: For any $\theta_1,\ldots,\theta_n$,

$$\Box\theta_1 \vee \cdots \vee \Box\theta_n \quad \equiv \quad \bigwedge_{1\le i\le n} \Box(\theta_i \vee \bigvee_{j\neq i}\Box\theta_j)$$

Now we can distinguish the following cases.

Case 1: none of the ϕ_i begins with $\Diamond$.

If every ϕ_i is of the form $\Box\psi_i$ then Lemma 6.1 reduces ϕ to a conjunction of n formulas, on each of which (4.1) can be used. The result in each case is a formula to which the induction hypothesis applies. Otherwise, there is exactly one ϕ_i of the form $\bigcirc\psi_i$. Say, ϕ_1 is of the form $\bigcirc\psi_1$ and ϕ_i is of the form $\Box\psi_i$, for all $i > 1$. Then the result follows from Lemma 6.1 and the equivalence

$$\Box\chi \vee \bigcirc\psi \equiv (\chi \vee \bigcirc\psi) \wedge \bigcirc(\Box\chi \vee \psi),$$

where $\chi = \Box\phi_2 \vee \cdots \vee \Box\phi_n$.

Case 2: at least one of the ϕ_i begins with $\Diamond$.

Since $\Diamond\theta_1 \vee \Diamond\theta_2 \equiv \Diamond(\theta_1 \vee \theta_2)$, it can further be assumed that exactly one of the ϕ_i, say ϕ_1, is of the form $\Diamond\psi_1$. If none of the ϕ_i begins with $\bigcirc$ then ϕ is of the form $\Diamond\psi_1 \vee \Box\psi_2 \vee \cdots \vee \Box\psi_n$. Using Lemma 6.1 and the induction hypothesis it can be assumed, without loss of generality, that $n = 2$. Now, by (5.3) and (4.2), since the formula ψ_1 must be boolean,

$$C_u(\phi) = (C(\psi_1) \cup pre)^{\times} (C_u(\psi_2 \vee \Diamond\psi_1)).$$

The rest of the proof in this case follows from the induction hypothesis. If exactly one of the ϕ_i begins with $\bigcirc$, say ϕ_2 is of the form $\bigcirc\psi_2$, and none of the ϕ_i begins with $\Box$ then ϕ is of the form $\Diamond\psi_1 \vee \bigcirc\psi_2$, with ψ_1 boolean, so

$$\begin{aligned} C_u(\phi) &= C_u(\psi_1 \vee \bigcirc\Diamond\psi_1 \vee \bigcirc\psi_2) \\ &= C_u(\psi_1) \cup C_u(\bigcirc(\Diamond\psi_1 \vee \psi_2)) \\ &= C_u(\psi_1) \cup pre(C_u(\Diamond\psi_1 \vee \psi_2)). \end{aligned}$$

Otherwise, if all remaining ϕ_i begin with $\Box$ then ϕ is of the form $\Diamond\psi_1 \vee \bigcirc\psi_2 \vee \Box\psi_3 \vee \cdots \vee \Box\psi_n$.

Using Lemma 6.1 it can be assumed without loss of generality that $n = 3$. Then

$$\begin{aligned} C_u(\phi) &= C_u(\Diamond\psi_1 \vee \bigcirc\psi_2 \vee \Box\psi_3) \\ &= C_u(\Diamond\psi_1 \vee \bigcirc\psi_2 \vee \psi_3) \cap C_u(\Diamond\psi_1 \vee \bigcirc\psi_2 \vee \bigcirc\Box\psi_3) \\ &= C_u(\Diamond\psi_1 \vee \bigcirc\psi_2 \vee \psi_3) \cap [C_u(\psi_1) \cup C_u(\Diamond\bigcirc\psi_1 \vee \bigcirc\psi_2 \vee \bigcirc\Box\psi_3)] \\ &= C_u(\Diamond\psi_1 \vee \bigcirc\psi_2 \vee \psi_3) \cap [C_u(\psi_1) \cup pre(C_u(\Diamond\psi_1 \vee \psi_2 \vee \Box\psi_3))]. \end{aligned}$$

Using the induction hypothesis, this completes the proof of the theorem.

■

Theorem 6.2:

Let ϕ be a formula in the logic $L(\Diamond, \bigcirc, \wedge, \vee, \sim)$, where the negation symbol $\sim$ applies only to boolean subformulas of ϕ and let the atomic propositions occurring in ϕ be $\alpha_1,\ldots,\alpha_s$. Then there exists a set transformer $f_\phi(X_1,\ldots,X_s)$ constructed from the operators $\sim, \cup, \cap, pre, \forall post, ^\times, ^*$ via composition, such that for all graphs G,

$$C_u(\phi; G) = f_\phi(C_u(\alpha_1; G),\ldots, C_u(\alpha_s; G)).$$

Proof:

As before the proof is by induction on the number of connectives (temporal or not) occurring in the formula ϕ. If ϕ is either boolean or of the form $\phi_1 \wedge \cdots \wedge \phi_n$ or of the form $\bigcirc\psi$ then the inductive hypothesis applies. It remains to consider the cases where ϕ is either of the form $\Diamond\psi$ or of the form $\phi_1 \vee \cdots \vee \phi_n$. For the rest of the proof the following two lemmas will be useful. The first one is simply the dual of Lemma 6.1, while the second is proved easily using the fact that $\bigcirc$ commutes with $\Diamond$ and is associative with $\wedge$ and $\vee$.

Lemma 6.2: For any $\theta_1, \ldots, \theta_n$,

$$\Diamond\theta_1 \wedge \cdots \wedge \Diamond\theta_n \quad \equiv \quad \bigvee_{1\le i\le n} \Diamond(\theta_i \wedge \bigwedge_{j\neq i} \Diamond\theta_j)$$

Lemma 6.3: Any $\phi \in L(\bigcirc, \Diamond, \wedge, \vee)$ can be put into a form in which $\bigcirc$ appears only in subformulas of the form $\bigcirc^m \alpha$, for some boolean α.

Now, as indicated above, we can consider two cases.

Case 1: $\phi : \Diamond\psi$, and ψ is not a disjunction.

If ψ is boolean then use Lemma 4.1 in §4.3.4. If ψ is $\Diamond\chi$, then use $\Diamond\psi \equiv \Diamond\chi$ to reduce the number of connectives of ϕ. If ψ is $\bigcirc\chi$, use the fact that $C_u(\phi) = pre(C_u(\Diamond\chi))$. In this way, we reduce to the case where ψ must be a conjunction $\psi_1 \wedge \cdots \wedge \psi_m$. No ψ_i can be a conjunction, and no ψ_i can be a disjunction either (then ψ would be a disjunction). Hence, some of the ψ_i must be boolean, some must begin with $\bigcirc$, and some must begin with $\Diamond$, i.e. ϕ is of the form

$$\phi \equiv \Diamond(\alpha \wedge \bigcirc^{n_1}\alpha_1 \wedge \cdots \wedge \bigcirc^{n_k}\alpha_k \wedge \Diamond\chi_1 \wedge \cdots \wedge \Diamond\chi_p),$$

where $\alpha, \alpha_1, \ldots, \alpha_k$ are boolean and $k, p \geq 0$. If $k = 0$ then the result follows by applying Lemma 6.2. Indeed,

$$\phi \equiv \Diamond(\alpha \wedge \Diamond\chi_1 \wedge \cdots \wedge \Diamond\chi_p)$$

and by Lemma 6.2, we know that there is a formula χ such that $\Diamond\chi_1 \wedge \cdots \wedge \Diamond\chi_p \equiv \Diamond\chi$. So by (5.3)

$$\phi \equiv \Diamond(\alpha \wedge \Diamond\chi) \equiv \Diamond\alpha \wedge \alpha P(\sim\Diamond\chi).$$

It follows from Lemma 4.1 that

$$C_u(\alpha P(\sim\Diamond\chi) = (A \cup pre)^{\times}(C_u(\Diamond\chi_1) \cap \cdots \cap C_u(\Diamond\chi_p))$$

If $k \geq 1$ and $p = 0$ then

$$\phi \equiv \Diamond(\alpha \wedge \bigcirc^{n_1}\alpha_1 \wedge \cdots \wedge \bigcirc^{n_k}\alpha_k),$$

and the C_u of the right hand side can be computed directly by Lemma A2 in the Appendix. Thus, we have reduced to the case where both $k, p \geq 1$, i.e. ϕ must have the form

$$\phi \equiv \Diamond(\alpha_0 \wedge \bigcirc^{n_1}\alpha_1 \wedge \cdots \wedge \bigcirc^{n_k}\alpha_k \wedge \Diamond\chi_1 \wedge \cdots \wedge \Diamond\chi_p) \equiv \text{ by Lemma 6.2}$$
$$\equiv \Diamond(\alpha_0 \wedge \bigcirc^{n_1}\alpha_1 \wedge \cdots \wedge \bigcirc^{n_k}\alpha_k \wedge \Diamond\theta),$$

where $\Diamond\theta \equiv \Diamond\chi_1 \wedge \cdots \wedge \Diamond\chi_p$, and from which α_0 may be missing. Applying (5.3) to this formula,

$$\phi \equiv \Diamond(\alpha_0 \wedge \bigcirc^{n_1}\alpha_1 \wedge \cdots \wedge \bigcirc^{n_k}\alpha_k) \wedge (\alpha_0 \wedge \bigcirc^{n_1}\alpha_1 \wedge \cdots \wedge \bigcirc^{n_k}\alpha_k)\mathsf{P}(\sim\Diamond\theta).$$

The eventuality formula can be immediately handled by Lemma A2. The precedence formula is more troublesome. First assume that $n_1 > n_2 > \cdots > n_k$. Then, by (3.2), the precedence formula is equivalent to

$$(\bigcirc^{n_1}(\ominus^{\nu_0}\alpha_0 \wedge \alpha_1 \wedge \ominus^{\nu_2}\alpha_2 \wedge \cdots \wedge \ominus^{\nu_k}\alpha_k))\mathsf{P}(\sim\Diamond\theta),$$

where $\nu_0 = n_1$ and for $i \geq 2$, $\nu_i = n_1 - n_i$. Setting $\pi = \ominus^{\nu_0}\alpha_0 \wedge \alpha_1 \wedge \ominus^{\nu_2}\alpha_2 \wedge \cdots \wedge \ominus^{\nu_k}\alpha_k$, and applying Lemma A3 to the result, we reduce to formulas of the form

$$\bigcirc^{n_1-1}\pi \vee \cdots \vee \bigcirc^{s+1}\pi \vee \bigcirc^{s}\pi,$$

for some s. Notice that $\pi\mathsf{P}\sim(\Diamond\theta \vee \bigcirc^{n_1-1}\pi \vee \cdots \vee \bigcirc\pi \vee \pi)$ is the greatest solution of the tfe

$$\phi \equiv (\pi \vee \bigcirc\pi \vee \cdots \vee \bigcirc^{n_1-1}\pi \vee \Diamond\theta) \wedge (\pi \vee \bigcirc\phi).$$

Now, since π is a past formula, $\pi \vee \bigcirc\phi$ is translatable by rule T_6. The set $\mathsf{C}_u(\pi)$ can be computed by the methods of Theorem 6.1, using $\ominus$ in place of $\bigcirc$ and translation rule T_5 in place of rule T_4. Hence, we reduce to formulas of the form

$$(\bigcirc^{s}\pi \vee \bigcirc^{s+1}\pi \vee \cdots \vee \bigcirc^{n_1-1}\pi) \vee \Diamond\chi, \tag{6.1}$$

where χ is any of the formulas χ_i above. After substituting for π, the (n_1-s)-term disjunction in ( ) can be written as a $(k+1)^{n_1-s}$-term conjunction of the form $\wedge\delta_i$, where each δ_i is a (n_1-s)-term disjunction. In this way (6.1) can be expressed as

$$(\Diamond\chi \vee \delta_1) \wedge \cdots \wedge (\Diamond\chi \vee \delta_{(k+1)^n}), \tag{6.2}$$

so we reduce to the consideration of a formula of the form

$$\Diamond\chi \vee \delta. \tag{6.3}$$

Example 6.1: Let the original formula ϕ be $\Diamond(\alpha_0 \wedge \bigcirc^5\alpha_1 \wedge \bigcirc^3\alpha_2 \wedge \bigcirc^2\alpha_3 \wedge \Diamond\chi)$. Then the part of (6.1) in ( ) is

$$(\ominus^5\alpha_0 \wedge \alpha_1 \wedge \ominus^2\alpha_2 \wedge \ominus^3\alpha_3) \vee (\ominus^4\alpha_0 \wedge \bigcirc\alpha_1 \wedge \ominus\alpha_2 \wedge \ominus^2\alpha_3) \vee$$
$$(\ominus^3\alpha_0 \wedge \bigcirc^2\alpha_1 \wedge \alpha_2 \wedge \ominus\alpha_3) \vee (\ominus^2\alpha_0 \wedge \bigcirc^3\alpha_1 \wedge \bigcirc\alpha_2 \wedge \alpha_3) \vee$$
$$(\ominus\alpha_0 \wedge \bigcirc^4\alpha_1 \wedge \bigcirc^2\alpha_2 \wedge \bigcirc\alpha_3)$$

and (6.2) has 4^5 terms (a large number!). A typical δ that may appear in (6.3) is

$$\ominus^5\alpha_0 \vee \bigcirc\alpha_1 \vee \ominus\alpha_3 \vee \bigcirc\alpha_2 \vee \bigcirc^2\alpha_2$$

We see from the example that the formula δ appearing in (6.3) generally consists of a past part $\delta^{(p)}$ and of a future part $\delta^{(f)}$. Applying translation rule T_6 to (6.3), we reduce to finding $C_u(\delta^{(p)})$ and $C_u(\delta^{(f)} \vee \Diamond\chi)$. The first of these sets can be computed just like $C_u(\pi)$ above, so we have finally reduced to computing the C_u of a formula of the form $\Diamond\chi \vee \delta^{(f)}$. From (6.1) and the definition of π it can be seen that the ''worst'' such formula, i.e. the one involving the $\delta^{(f)}$ with the greatest number of connectives, is

$$\Diamond\chi \vee \alpha_1 \vee \bigcirc\alpha_1 \vee \cdots \vee \bigcirc^{n_1-1}\alpha_1 \tag{6.4}$$

(consider also Example 6.1). If the number of connectives of this formula is less than $\#(\phi)$, the proof for this case is finished [13]. Otherwise, formulas of the type (6.4) fall under Case 2 below.

Case 2: ϕ is $\phi_1 \vee \cdots \vee \phi_n$ and no ϕ_i is a disjunction.

If one of the ϕ_i, say ϕ_1, is boolean then $C_u(\phi_1 \vee \cdots \vee \phi_n) = C_u(\phi_1) \cup C_u(\phi_2 \vee \cdots \vee \phi_n)$, and the induction hypothesis applies. If no ϕ_i is boolean, but, say ϕ_1, is a conjunction $\phi_1 : \phi_{11} \wedge \phi_{12}$ then

$$C_u((\phi_{11} \wedge \phi_{12}) \vee \phi_2 \vee \cdots \vee \phi_n) = C_u(\phi_{11} \vee \phi_2 \vee \cdots \vee \phi_n) \cap C_u(\phi_{12} \vee \phi_2 \vee \cdots \vee \phi_n),$$

and the induction hypothesis applies again. If no ϕ_i is either boolean or a conjunction (or a disjunction) then all ϕ_i must begin either with $\bigcirc$ or with $\Diamond$. Hence we reduce to

$$\phi \equiv \bigcirc^{m_1}\alpha_1 \vee \cdots \vee \bigcirc^{m_k}\alpha_k \vee \Diamond\chi,$$

where χ is not a disjunction. If χ is boolean then

13. $\#(\phi) = (k+p)(\wedge) + (p+1)(\Diamond) + (n_1+\cdots+n_k)(\bigcirc)$, while $\#(6.4) = n_1(\vee) + 1(\Diamond) + (1/2)n_1(n_1-1)(\bigcirc)$.

$$C_u(\phi) = pre\,(C_u(\bigcirc^{m_1-1}\alpha_1 \vee \cdots \vee \bigcirc^{m_k-1}\alpha_k \vee \Diamond\chi)) \cup C_u(\chi)\,,$$

and so again we reduce the number of connectives. Hence, without loss of generality it can be assumed that χ is not boolean, but it is a conjunction $\chi_1 \wedge \cdots \wedge \chi_p$. If all χ_i begin with $\Diamond$, say $\chi_i = \Diamond\omega_i$, then by (5.2), $\Diamond\chi = \Diamond(\Diamond\omega_1 \wedge \cdots \wedge \Diamond\omega_p) \equiv \Diamond\omega_1 \wedge \cdots \wedge \Diamond\omega_p$. So

$$C_u(\phi) = \bigcap_{1\le i\le p} C_u(\bigcirc^{m_1}\alpha_1 \vee \cdots \vee \bigcirc^{m_k}\alpha_k \vee \Diamond\omega_i)\,,$$

If all χ_i begin with $\bigcirc$ then $\Diamond\chi = \bigcirc\Diamond(\omega_1 \wedge \cdots \wedge \omega_p)$ and hence

$$C_u(\phi) = pre\,(C_u(\bigcirc^{m_1-1}\alpha_1 \vee \cdots \vee \bigcirc^{m_k-1}\alpha_k \vee \Diamond(\omega_1 \wedge \cdots \wedge \omega_p))).$$

Thus we reduce to the case where some χ_i are boolean, some begin with $\bigcirc$, and some begin with $\Diamond$, i.e.

$$\phi \equiv \bigcirc^{m_1}\alpha_1 \vee \cdots \vee \bigcirc^{m_k}\alpha_k \vee \Diamond(\beta_0 \wedge \bigcirc^{n_1}\beta_1 \wedge \cdots \wedge \bigcirc^{n_l}\beta_l \wedge \Diamond\omega_1 \wedge \cdots \wedge \Diamond\omega_p)\,,$$

from which β_0 may be absent. The proof here will be by induction *on the number of* $\Diamond$*'s in the formula.* Also, we will consider only the special case $l = 1, p = 1$ (the general case $p \ge 1$ follows similarly by generalizing identity (5.4) as well as Lemma A3 to formulas $\bigcirc^n\beta P(\sim\Diamond\psi_1 \wedge \cdots \wedge \sim\Diamond\psi_p)$). Let $m_1 < m_2 < \cdots < m_k$, and set

$$\gamma : \alpha_1 \vee \bigcirc^{m_2-m_1}\alpha_2 \vee \cdots \vee \bigcirc^{m_k-m_1}\alpha_k$$

Then our formula can be abbreviated as

$$\phi \equiv \bigcirc^{m_1}\gamma \vee \Diamond(\bigcirc^n\beta \wedge \Diamond\omega) \tag{6.5}$$

Using the identity $\Diamond\psi \equiv \psi \vee \bigcirc\Diamond\psi$, we can write (6.5) as the conjunction of the following two formulas

$$\bigcirc^{m_1}\gamma \vee \Diamond\omega \vee \bigcirc\Diamond(\bigcirc^n\beta \wedge \Diamond\omega) \equiv \bigcirc^{m_1}\gamma \vee \Diamond\omega \tag{6.6}$$

$$\bigcirc(\bigcirc^{m_1-1}\gamma \vee \bigcirc^{n-1}\beta \vee \Diamond(\bigcirc^n\beta \wedge \Diamond\omega)). \tag{6.7}$$

(The simplification in formula (6.6) follows from the fact that the last two disjuncts are equivalent to simply $\Diamond\omega$). The induction hypothesis applies to formula (6.6), since it has fewer $\Diamond$'s than the original formula (6.5). Formula (6.7) is of the same form as (6.5). It is easily seen that by iterating m_1 times on it the above decomposition into a conjunction of two formulas, we arrive at a formula of the form

$$\gamma \vee \bigcirc^{\nu}\beta \vee \bigcirc^{\nu+1}\beta \vee \cdots \vee \bigcirc^{n-1}\beta \vee \Diamond(\bigcirc^{n}\beta \wedge \Diamond\omega)$$

for some $\nu \geq 0$. Now, setting $\gamma : \alpha_1 \vee \bigcirc^{m_2-m_1}\gamma'$, where γ' is appropriately chosen, we can continue decomposing as above. Eventually, after k such "decomposition phases", we succeed in eliminating all the α_i, and we reduce to a formula of the form

$$\bigcirc^{\nu}\beta \vee \bigcirc^{\nu+1}\beta \vee \cdots \vee \bigcirc^{n-1}\beta \vee \Diamond(\bigcirc^{n}\beta \wedge \Diamond\omega)$$

for some $\nu \geq 0$. Applying (5.4) to this, we obtain $\bigcirc^{\nu}\Diamond\beta \wedge \bigcirc^{n}\beta P(\sim\Diamond\omega)$. By Lemma A3, this last precedence formula reduces to

$$\beta P \sim(\Diamond\omega \vee \bigcirc^{n-1}\beta \vee \bigcirc^{n-2}\beta \vee \cdots \vee \bigcirc\beta \vee \beta),$$

which is the greatest solution of the tfe

$$\phi \equiv (\beta \vee \bigcirc\beta \vee \cdots \vee \bigcirc^{n-1}\beta \vee \Diamond\omega) \wedge (\beta \vee \bigcirc\phi).$$

The first conjunct on the right-hand side of this tfe is a formula with fewer $\Diamond$'s than (6.5), so the result of the theorem follows from (4.3) and the induction hypothesis.

■

7. CHARACTERISTIC SETS OF FAIRNESS FORMULAS

The general fairness formula

$$\bigvee_{i \in I} \bigwedge_{j \in J} (\Box\Diamond p_{ij} \supset \Box\Diamond q_{ij})$$

considered in [LP] and [EL], where the p_{ij}, q_{ij} are boolean, expresses an arbitrary boolean combination of facts of the form "if p_{ij} holds infinitely often, then q_{ij} holds infinitely often" (to be precise, the q_{ij} must really be "edge" propositions). To compute the universal characteristic set of such a formula it suffices to be able to find the C_u of a formula of the form

$$\Diamond\Box\phi_1 \vee \cdots \vee \Diamond\Box\phi_k \vee \Box\Diamond\psi_1 \vee \cdots \Box\Diamond\psi_l, \tag{7.1}$$

where it is possible that either $k = 0$ or $l = 0$. Since the construction of this characteristic set is complicated, we introduce the important ideas by first establishing a restricted theorem:

Theorem 7.1:

Let $\phi = \langle\rangle\Box\phi_1 \vee \cdots \vee \langle\rangle\Box\phi_k$ be a formula such that the only temporal connective in $\phi_1,\ldots, \phi_k$ is $\bigcirc$, and let $\alpha_1,\ldots, \alpha_s$ be the boolean formulas occurring in ϕ. Then there exists a monotonic set transformer $f_\phi(X_1,\ldots, X_s)$ constructed from the operators $\sim, \cup, \cap, pre, ^\times, ^*$ via composition such that for all graphs G,

$$C_u(\phi; G) = f_\phi(C_u(\alpha_1; G),\ldots, C_u(\alpha_s; G))$$

The following result is basic for the proof:

Lemma 7.1: For any ψ, the formula $\langle\rangle\Box\psi$ is the least fixpoint of the tfe

$$\phi \equiv \Box(\psi \vee \bigcirc^k\phi),$$

where $k \geq 1$ is arbitrary, but fixed.

This lemma is proved in the Appendix. To see its validity intuitively, take $k=1$ and note that its dual says that $\Box\langle\rangle a$ satisfies the tfe $\phi \equiv \langle\rangle(a \vee \bigcirc\phi)$. This is plausible, since $\Box\langle\rangle a$ has the "infinite expansion"

$$\langle\rangle(a \wedge \bigcirc\langle\rangle(a \wedge \bigcirc\langle\rangle(a \wedge \bigcirc\langle\rangle \cdots$$

Note 1:

The importance of Lemma 7.1 is that it gives us a way to compute the fundamental set $C_u(\langle\rangle\Box a)$ *without introducing the notion of the strong components of a graph*, i.e. in a truly model-independent manner. Contrast this with the approach of [LP] in which the concept of a strong component is essential.

Note 2:

Observe that when the lemma is used to compute e.g. $C_u(\langle\rangle\Box a)$, we want to find the least fixpoint of the $\cap$-continuous set transformer $pre^\times$, and the results of sec. 4.3.3 *do not apply*, unless the graph G is finite. Cousot ([Cou]) has done extensive work on the problem of computing extremal fixpoints of monotonic (non-continuous) set transformers.

Note 3:

Lemma 7.1 points out that a given formula ϕ may be the extremal solution of more than one tfe.

Proof of Theorem 7.1:

First we show how to compute $C_u(\langle\rangle\Box\psi)$, when ψ uses only the connectives $\sim, \vee, \wedge, \bigcirc$. Using identity (5.6) we can assume without loss of generality that ψ is of the form

$$\beta_0 \vee \bigcirc^{n_1}\beta_1 \vee \bigcirc^{n_2}\beta_2 \cdots \vee \bigcirc^{n_r}\beta_r \,, \tag{7.2}$$

where $\beta_0,...,\beta_r$ are boolean and $0 < n_1 < \cdots < n_r$. By Lemma 7.1, $\langle\rangle\Box\psi$ is the least fixpoint of $\phi \equiv \Box(\psi \vee \bigcirc^{n_k}\phi)$.

Example: Let ψ be the formula $\beta_0 \vee \bigcirc^2\beta_1 \vee \bigcirc^3\beta_2$. Writing this as $\beta_0 \vee \bigcirc^2(\beta_1 \vee \bigcirc\beta_2)$, we see that $\langle\rangle\Box\psi$ is the least fixpoint of the translatable tfe

$$\phi \equiv \Box(\beta_0 \vee \bigcirc^2(\beta_1 \vee \bigcirc(\beta_2 \vee \phi)))$$

It follows that the set $\Psi = C_u(\langle\rangle\Box\psi)$ satisfies the set equation

$$X = pre^{\times}(B_0 \cup pre^2(B_1 \cup pre(B_2 \cup X)))$$

Let F be the least fixpoint of this equation. It remains to show that $F = \Psi$. Since Φ satisfies the equation it must be that $F \subseteq \Psi$. Conversely, let $v \notin F = pre^{\times}(B_0 \cup pre^2(B_1 \cup pre(B_2 \cup F)))$. Then there exists a sequence $v_1,...,v_{n_1}$ such that $v_{n_1-3} \notin B_0$, $v_{n_1-1} \notin B_1$, $v_{n_1} \notin B_2, F$. Next, repeat the same procedure with $v = v_{n_1}$ to find a sequence $v_{n_1+1},...,v_{n_2}$ such that $v_{n_2-3} \notin B_0$, $v_{n_2-1} \notin B_1$, $v_{n_2} \notin B_2, F$. Let $w = (v, v_1, ..., v_n, ...)$ be the infinite walk thus obtained. It is obvious from the construction of w that $w \models \sim\langle\rangle\Box\psi$. Hence, $v \notin C_u(\langle\rangle\Box\psi) = \Psi$. This implies that $\Psi \subseteq F$, as desired.

To complete the proof of the theorem, we now extend Lemma 7.1 to

Lemma 7.2:

Let $k_1, ..., k_{n-1}$ be arbitrary integers ≥ 0, and let $k_n \geq 1$. For any $\phi_1, ..., \phi_n$, the formula $\langle\rangle\Box\phi_1 \vee \cdots \vee \langle\rangle\Box\phi_n$ is the greatest solution of the tfe

$$\phi \equiv \Box(\phi_1 \vee \bigcirc^{k_1}\Box(\phi_2 \vee \bigcirc^{k_2}\Box(\cdots \vee \bigcirc^{k_{n-1}}\Box(\phi_n \vee \bigcirc^{k_n}\phi)...)$$

Again, the dual of this lemma is more easily understood. For simplicity, set $k_1, ..., k_{n-1}$ to 0, and let $k_n = 1$. Then the dual lemma says that the formula $\Box\langle\rangle\phi_1 \vee \cdots \vee \Box\langle\rangle\phi_n$ satisfies the tfe

$$\phi \equiv \langle\rangle(\phi_1 \wedge \langle\rangle(\phi_2 \wedge \langle\rangle(\cdots \wedge \langle\rangle(\phi_n \wedge \bigcirc\phi)\cdots)$$

To see the truth of this, let $\phi_1, ..., \phi_n$ occur infinitely often on an infinite sequence σ. Then σ contains a subsequence σ' on which $\phi_1, ..., \phi_n$ occur infinitely often *in this order*. Clearly, the converse is also true.

Now assume that each ϕ_i has the form (7.2). To use Lemma 7.2, select n_i to be the *largest* exponent occurring in ϕ_i, and then proceed by "factoring" the ϕ_i as in the example given above. This completes the proof of Theorem 7.1.

■

The next theorem will make it possible to handle any formula of type (7.1):

Theorem 7.2:

Let $\phi = \Diamond\Box\phi_1 \vee \cdots \vee \Diamond\Box\phi_k \vee \Box\Diamond\beta_1 \vee \cdots \Box\Diamond\beta_l$, be a formula in the logic $L(\bigcirc, \Diamond, \Box, \vee, \wedge, \sim)$ such that the only temporal connective in $\phi_1,..., \phi_k$ is $\bigcirc$, and the formulas $\beta_1,..., \beta_l$ are boolean. If the atomic propositions occurring in ϕ are $\alpha_1,..., \alpha_s$, there exists a monotonic set transformer $f_\phi(X_1,..., X_s)$ constructed from the operators $\sim, \cup, \cap, pre, post, ^\times, ^*$ via composition such that for all graphs G,

$$C_u(\phi; G) = f_\phi(C_u(\alpha_1; G),..., C_u(\alpha_s; G))$$

Proof of Theorem 7.2:

The proof consists in extending the ideas introduced in establishing Theorem 7.1. Using identity (5.6b) in sec. 5, we can assume without loss of generality that l=1. Hence, we only have to consider formulas of the form

$$\Diamond\Box\phi_1 \vee \cdots \vee \Diamond\Box\phi_k \vee \Box\Diamond\beta$$

Next, it follows from (5.11a) that

$$\models \Diamond\Box\phi_1 \vee \cdots \vee \Diamond\Box\phi_k \vee \Box\Diamond\beta \equiv \Box\Diamond(\Box\phi_1 \vee \cdots \vee \Box\phi_k \vee \beta),$$

so we reduce to finding the universal characteristic sets of formulas of the form

$$\Diamond\Box\alpha_1 \vee \cdots \vee \Diamond\Box\alpha_k \vee \Diamond\beta, \tag{7.3}$$

where β is boolean. Now we will extend Lemma 7.2 to handle a formula of this type. The important feature

of the extension is the introduction of the "until" operator U.

Things are much clearer if we work with the dual of (7.3). We will also use the abbreviation

$$\bigcirc^{0,k} b \ : \ b \wedge \bigcirc b \wedge \cdots \wedge \bigcirc^k b$$

Lemma 7.3:

The formula $\Box\Diamond\phi_1 \wedge \cdots \wedge \Box\Diamond\phi_n \wedge \Box b$ is the least solution of the tfe

$$\phi \equiv b \,\mathsf{U}(\phi_1 \wedge \bigcirc^{0,k_1-1} b \wedge \bigcirc^{k_1}(b \,\mathsf{U}(\phi_2 \wedge \bigcirc^{k_2-1} b \wedge \bigcirc^{k_2}(b \,\mathsf{U}(\phi_3 \cdots \\ b \,\mathsf{U}(\phi_n \wedge \bigcirc^{0,k_n-1} b \wedge \bigcirc^{k_n}\phi) \cdots),$$

where $k_1, \ldots, k_n$ are arbitrary but fixed integers ≥ 0, and $k_1 \geq 1$.

The justification of this lemma is entirely analogous to that of Lemma 7.2. As in the case of Lemma 7.2, k_i should be set to the "degree" of ϕ_i, i.e. n_r in the form (7.2). After the ϕ_i are "factored" just as for Lemma 7.2, the tfe of the lemma becomes e-translatable. This completes the proof of theorem 7.2.

■

8. CONCLUSION

We conclude with the following remarks:

1. We have presented an inductive, model-independent representation for the characteristic sets of some linear-time temporal formulas ϕ. The automaton $\mathcal{A}(\phi)$ is a model-independent representation of ϕ, but *not* of its characteristic set.

2. Many of the manipulations that we perform on formulas in order to put them into a translatable form are similar to the rules for *generating the tableaux* (or *closure*) for a formula: see e.g. [ES].

3. It is interesting to compare the time required to compute characteristic sets by our method and by the automaton-based method. As a an example, it is apparent from Lemma 6.2 that the complexity of finding $\mathsf{C}_e(\Diamond a_1 \wedge \cdots \wedge \Diamond a_n)$ is factorial by our method, while it is known ([SC]) to be just exponential by the automaton method. On the other hand, the complexity of $\mathcal{A}(\sim\phi)$ for the formulas of Lemmas 7.1 and 7.2 may be exponential in n, while the systems of fixpoint equations given in the

Lemmas are parallelizable, hence performable in sub-exponential time.

4. It is possible to compute characteristic sets in a symbolic manner by our methods. This may lead to substantial time savings when the model (graph) is finite, and it is the only way to go when the model is infinite but has a finite description. Examples of such computations can be found in [Sif], so we have not given any here. However, as [Sif] points out, the stumbling, though not insurmountable, block in this attractive scheme is the difficulty of manipulating predicates symbolically.

5. Although our results are not sufficient to handle all formulas in the logic $L(\bigcirc, \Diamond, \Box, \wedge, \vee, \sim)$, or formulas involving the "until" and "precedes" operators U and P, they appear to be extensible ([Oik]).

APPENDIX

Lemma A1: The formula $\Diamond(a \wedge \bigcirc^n \chi)$ is the first component of the least solution of the following system of $2^{n-1} = m$ tfe's

$$\begin{aligned}
\phi_1 &\equiv (a \vee \bigcirc\phi_1) \wedge \bigcirc\phi_2 \\
\phi_2 &\equiv (a \vee \bigcirc\phi_3) \wedge \bigcirc\phi_4 \\
\phi_3 &\equiv (a \vee \bigcirc\phi_5) \wedge \bigcirc\phi_6 \\
&\cdots \\
\phi_{m/2} &\equiv (a \vee \bigcirc\phi_{m-1}) \wedge \bigcirc\phi_m \\
\phi_{m/2+1} &\equiv (a \vee \bigcirc(\chi \vee \phi_1)) \wedge \bigcirc(\chi \vee \phi_2) \\
\phi_{m/2+2} &\equiv (a \vee \bigcirc(\chi \vee \phi_3)) \wedge \bigcirc(\chi \vee \phi_4) \\
&\cdots \\
\phi_m &\equiv (a \vee \bigcirc(\chi \vee \phi_{m-1})) \wedge \bigcirc(\chi \vee \phi_m).
\end{aligned} \tag{A1}$$

That is, if the least solution of the system is $(\sigma_1, \ldots, \sigma_m)$, then $\sigma_1 : \Diamond(a \wedge \bigcirc^n \chi)$.

Example: The formula $\Diamond(a \wedge \bigcirc^3 b)$ can be reduced to the (translatable) system

$$\begin{aligned}
\phi_1 &\equiv (a \vee \bigcirc\phi_1) \wedge \bigcirc\phi_2 \\
\phi_2 &\equiv (a \vee \bigcirc\phi_3) \wedge \bigcirc\phi_4 \\
\phi_3 &\equiv (a \vee \bigcirc(b \vee \phi_1)) \wedge \bigcirc(b \vee \phi_2) \\
\phi_4 &\equiv (a \vee \bigcirc(b \vee \phi_3)) \wedge \bigcirc(b \vee \phi_4).
\end{aligned}$$

It can be seen that ϕ_3 is actually not necessary. Generally, in the system of Lemma A1, only $\phi_1, \ldots, \phi_{m/2}$, and ϕ_m are essential. However, keeping all of the equations results in simpler forms.

Proof of Lemma A1:

The equations are derived as follows: writing formula $\Diamond(a \wedge \bigcirc^n \chi)$ as $\Diamond(a \wedge \bigcirc(\bigcirc^{n-1}\chi))$, we know from Theorem E in §3.1 that this formula is the least solution of the tfe $\phi_1 \equiv (a \vee \bigcirc\phi_1) \wedge \bigcirc(\bigcirc^{n-1}\chi \vee \phi_1)$. Now set $\phi_2 = \bigcirc^{n-1}\chi \vee \phi_1$; then the first equation of system (A1) follows:

$$\phi_1 \equiv (a \vee \bigcirc\phi_1) \wedge \bigcirc\phi_2$$

Using the right-hand side of this in the definition of ϕ_2, we find that

$$\begin{aligned}\phi_2 &\equiv \bigcirc^{n-1}\chi \vee ((a \vee \bigcirc\phi_1) \wedge \bigcirc\phi_2) \\ &\equiv (a \vee \bigcirc(\phi_1 \vee \bigcirc^{n-2}\chi)) \wedge \bigcirc(\phi_2 \vee \bigcirc^{n-2}\chi)\end{aligned}$$

Defining $\phi_3 = \phi_1 \vee \bigcirc^{n-2}\chi$ and $\phi_4 = \phi_2 \vee \bigcirc^{n-2}\chi$, the second equation of system (A1) follows. The rest of the equations are derived similarly, noting that in general $\phi_2, \ldots, \phi_m$ are defined by

$$\phi_{2^j+i} = \phi_i \vee \bigcirc^{n-j-1}\chi,$$

for $j = 0, 1, \ldots, n-2$, and $i = 1, 2, \ldots, 2^j$.

To show that $\Diamond(a \wedge \bigcirc^n\chi)$ is the first component of the least solution of system (A1), it is not necessary to use the expanded form (A1) of the system, which is suitable for translation. The proof is much simpler using the unexpanded form

$$\begin{aligned}\phi_1 &\equiv (a \vee \bigcirc\phi_1) \wedge \bigcirc\phi_2 \\ \phi_2 &\equiv \phi_1 \vee \bigcirc^{n-1}\chi \\ &\cdots \\ \phi_{m/2} &\equiv \phi_{m/4} \vee \bigcirc^2\chi \\ \phi_{m/2+1} &\equiv \phi_1 \vee \bigcirc\chi \\ &\cdots \\ \phi_m &\equiv \phi_{m/2} \vee \bigcirc\chi\end{aligned}$$

Substituting the second equation of this system into the first, we obtain $\phi_1 \equiv (a \wedge \bigcirc^n\chi) \vee \bigcirc\phi_1$.

When system (A1) is small, a more illustrative proof can be given. For $n = 2$ we have the system

$$\begin{aligned}\phi_1 &\equiv (a \vee \bigcirc\phi_1) \wedge \bigcirc\phi_2 \\ \phi_2 &\equiv (a \vee \bigcirc(\chi \vee \phi_1)) \wedge \bigcirc(\chi \vee \phi_2).\end{aligned}$$

The least solution (fixpoint) of this system is obtained by the iterative scheme

$$\begin{aligned}\phi_1^{(0)} &\equiv \bot, \quad \phi_2^{(0)} \equiv \bot \\ \phi_1^{(k)} &\equiv f_1(\phi_1^{(k-1)}, \phi_2^{(k-1)}) \\ \phi_2^{(k)} &\equiv f_2(\phi_1^{(k-1)}, \phi_2^{(k-1)}).\end{aligned}$$

If $\varepsilon : a \wedge \bigcirc^2\chi$, it can be seen that $\phi_1^{(k)} \equiv \varepsilon \vee \bigcirc\varepsilon \vee \cdots \vee \bigcirc^{k-2}\varepsilon, \phi_2^{(k)} \equiv \phi_1^{(k)} \vee \bigcirc\chi$.

■

Lemma A2: The formula $\Diamond(a \wedge \bigcirc^{n_1}a_1 \wedge \bigcirc^{n_2}a_2 \wedge \cdots \wedge \bigcirc^{n_k}a_k)$ where $n_1 > \cdots > n_k > 0$, is the first component of the least solution of a translatable system of 2^{n_1-1} tfe's. The system is identical to that

of Lemma A1, with the substitution

$$O(\chi \vee \phi_j) = O(a_1 \vee \phi_j) \wedge ((\ominus^{\nu_2-1} a_2 \wedge \cdots \wedge \ominus^{\nu_k-1} a_k) \vee \phi_j)$$

where $\nu_i = n_1 - n_i$.

Proof:

The given formula can be put into the form $\Diamond(a \wedge O^{n_1}\chi)$, where $\chi = a_1 \wedge \ominus^{\nu_2-1} a_2 \wedge \cdots \wedge \ominus^{\nu_k-1} a_k$ and $\nu_i = n_1 - n_i$. It is then easily found that for any ϕ_j, $j = 1, \ldots, 2^{n_1-1}$, $O(\chi \vee \phi_j)$ can be written as in the statement of the lemma. Note that $\nu_2 - 1 \geq 0$, while $\nu_3 - 1 > 0, \ldots, \nu_k - 1 > 0$. The formula

$$(a_1 \wedge \ominus^{\nu_2-1} a_2 \wedge \cdots \wedge \ominus^{\nu_k-1} a_k) \vee \phi_j$$

is translatable by rule T_6.

■

Lemma A3: For all n,

$$\models O^n \psi P \sim \omega \equiv \psi P \sim (\omega \vee O^{n-1}\psi \vee O^{n-2}\psi \vee \cdots \vee O\psi \vee \psi),$$

where ψ may be a past formula.

Proof:

Use repeatedly the fact that

$$\models O\chi_1 P \chi_2 \equiv \chi_1 P(\sim\chi_1 \wedge \chi_2)$$

■

Proof of Lemma 7.1:

It is more convenient to work with the dual version of the theorem, which states that $\Box\Diamond\psi$ is the greatest solution of the tfe

$$\phi \equiv \Diamond(\psi \wedge O^k \phi) \qquad \text{(A2)}$$

First it must be shown that $\Box\Diamond\psi$ satisfies this tfe. This is left as an exercise to the reader. We will show that $\Box\Diamond\psi$ is the greatest solution. Let χ be another solution of (A2). We will show that $\models \chi \supset \Box\Diamond\psi$.

To do this, we use the following principle: for any formulas p ,ω, and for any fixed $k \geq 1$,

$$\models p \wedge \Box(p \supset \omega \wedge \bigcirc^k p) \supset \Box\Diamond\omega \qquad (\dagger)$$

Note that ($\dagger$) is just a temporal formulation of a proof by induction on p that ω is true infinitely often. For k=1, ($\dagger$) takes the more familiar form $\models p \wedge \Box(p \supset \omega \wedge \bigcirc p) \supset \Box\omega$. Thus, with χ in place of p and $\Diamond\psi$ in place of ω, it suffices to establish that

$$\models \Box(\chi \supset \Diamond\psi \wedge \bigcirc^k \chi), \qquad (*)$$

To prove ($*$), note that since χ is a solution of (A2), we have

$$\models \chi \supset \Diamond(\psi \wedge \bigcirc^k \chi) \supset \Diamond\psi \wedge \bigcirc^k \Diamond\chi \qquad (**)$$

However, any solution σ of (A2) has the property $\models \sigma \equiv \Diamond\sigma$; to see this, use the $\Diamond\Diamond$-insertion rule on (A2). Substituting χ for $\Diamond\chi$ in ($**$), and using the $\Box$-insertion rule, we obtain ($*$).

■

REFERENCES

[CES] E. M. Clarke, E. A. Emerson, A.P. Sistla, "Automatic Verification of Finite-State Concurrent Systems Using Temporal Logic Specifications", 10th Annual ACM Symposium on Principles of Programming Languages, 1983.

[Cou] P. Cousot, "Systematic Design of Program Analysis Frameworks", 6th ACM Symposium on Principles of Programming Languages, 1979.

[EC] E. A. Emerson, E. M. Clarke, "Characterizing Correctness Properties of Parallel Programs Using Fixpoints", 7th Int'l Colloquium on Automata, Languages, and Programming, Springer Verlag, LNCS #85, 1981.

[EL] E. A. Emerson, C. L. Lei, "Modalities for Model Checking: Branching Time Strikes Back", 12th ACM Symposium on Principles of Programming Languages, 1985.

[ES] E. A. Emerson, A. P. Sistla, "Deciding Branching-Time Logic", 16th Symposium on Theory of Computing, 1984.

[La] L. Lamport, "What Good is Temporal Logic", IFIP 1983, R. E. A. Mason (ed.), pp. 657-668.

[LP] O. Lichtenstein, A. Pnueli, "Checking that Finite-State Concurrent Programs Satisfy their Linear Specification", 12th ACM Symposium on Principles of Programming Languages, 1985.

[LPZ] O. Lichtenstein, A. Pnueli, L. Zuck, "The Glory of the Past", in Logic of Programs, Springer Verlag LNCS Vol. 193, 1985.

[Mo] Y. N. Moschovakis, "Elementary Induction on Abstract Structures", North-Holland, 1974.

[MP] Z. Manna, A. Pnueli, "Verification of Sequential Programs: Temporal Axiomatization", Stanford University report STAN-CS-81-877, September 1981.

[Oik] K. N. Oikonomou, "The Set-Transformer/Fixpoint Approach to Checking the Truth of Linear-Time Temporal Logic Formulas on Directed Graphs, I", unpublished manuscript, 1984.

[QS] J. P. Queille, J. Sifakis, "Fairness and Related Properties in Transition Systems - A Temporal Logic to Deal with Fairness", Acta Informatica 19, 1983.

[SC] A. P. Sistla, E. M. Clarke, "The Complexity of Propositional Linear Temporal Logics", JACM, July 1985.

[Sif] J. Sifakis, "A Unified Approach for Studying the Properties of Transition Systems", Theoretical Computer Science 18, 1982.

[Tar] A. Tarski, "A Lattice-Theoretical Fixpoint Theorem and its Applications", Pacific J. Math., 5, 1955.

[VW] M. Vardi, P. Wolper, "Automata-Theoretic Techniques for Modal Logics of Programs", 16th Symposium on Theory of Computing, 1984.