MATHEMATICAL PROBLEMS IN COMPUTATION THEORY
BANACH CENTER PUBLICATIONS, VOLUME 21
PWN - POLISH SCIENTIFIC PUBLISHERS
WARSAW 1988

SAFETY- AND LIVENESS-PROPERTIES IN PROPOSITIONAL TEMPORAL LOGIC: CHARACTERIZATIONS AND DECIDABILITY

WOLFGANG THOMAS

Lehrstuhl für Informatik II, RWTH Aachen, Bundesrepublik Deutschland

Characterizations of propositional temporal logic (PTL) in model theory, formal language theory and semigroup theory are reviewed. It is shown that suitable restrictions of these results yield characterizations of safety- and liveness-properties expressed in PTL. As a consequence one obtains that it can be decided effectively whether a given PTL-formula represents such a property.

Introduction

In recent years several systems of temporal logic have been applied successfully in the construction and analysis of parallel programs or hardware (see e.g. [4], [14], [17]); at the same time, the mathematical investigation of temporal logics has gained considerable interest. The present paper is concerned with the most basic system in this context: *propositional temporal logic* of linear time ("PTL"), proposed in [23] and [12] as a formalism for the specification and verification of programs. We deal here with language theoretical aspects of PTL, and the aim of the paper is twofold: First we collect in a uniform framework several results which until now are somewhat scattered over the literature but which provide interesting and useful connections between temporal logic, formal language theory, and semigroup theory. Secondly, it is shown how these connections can be applied to clarify the role of safety- and liveness-properties in propositional temporal logic. Following a recent suggestion of [11], we consider these properties as represented by certain PTL-formulas in which the usual future operators are supplemented by operators for the past. We obtain characterization of safety- and liveness-properties which in particular imply that it can be decided effectively whether a given PTL-formula represents such a property or not.

The connection between PTL and formal language theory depends on the fact that PTL-formulas express properties of "execution sequences" of programs (i.e., sequences over some appropriate state space). If the state space is finite (as can be assumed in most practical applications), then a set of execution sequences can be considered as an ω-language in the usual sense of formal language theory. It turned out that the sequence sets which are definable in PTL constitute a fundamental class of ω-languages that has many characterizations and appealing mathematical properties.

Characterizations of PTL-definability have been found in several areas:

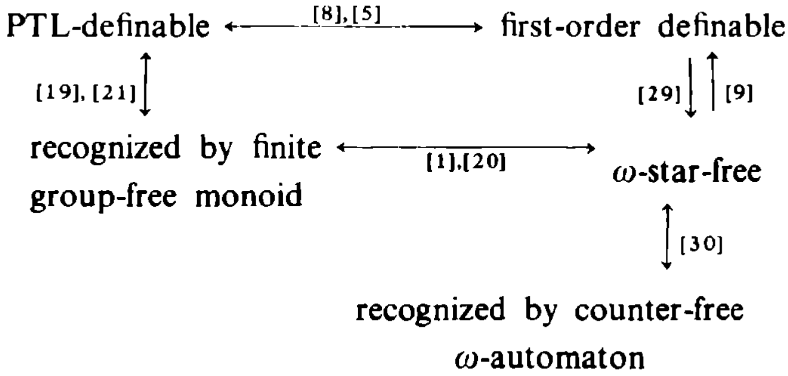
– in model theory, by first-order definability over the ordering of the natural numbers,

– in formal language theory, in terms of ω-star-free sequence sets,

– in automata theory, by counter-free ω-automata,

– in semigroup theory, in terms of group-free monoids.

The following diagram summarizes the connections between the definability notions of sets of ω-sequences and points to literature covering the equivalence proofs:



These equivalences not only show the mathematical relevance of propositional temporal logic, but (as illustrated in the present paper) make it also possible to apply the powerful methods of automata theory in the study of linear time temporal logic. At the present time, however, there seem to be only few references in which further applications of this kind appear (e.g., [28], [21]).

The paper is organized as follows: In Section 1 we present the definitions that are needed to formulate the first two equivalences in the list above (involving PTL, first-order logic, and ω-star-free ω-languages). Section 2 introduces safety- and liveness-properties and shows how the characterizations of full PTL can be specialized to capture these more restricted cases. In Section 3 we prove the mentioned decidability results. As a preparation, we give a simple proof of the characterization of ω-star-free ω-languages in terms of group-free monoids; this proof avoids semigroup-theoretical constructions like the Schützenberger product of monoids (appearing in [20]) and might make the results more easily accessible for readers not acquainted with semigroup theory.

1. PTL and ω-star-free ω-languages

Let Σ be a finite alphabet. The *PTL-formulas over* Σ are built up from the propositional variables p_a (for $a \in \Sigma$) using the boolean connectives $\neg$, $\wedge$, $\vee$, $\rightarrow$, $\leftrightarrow$, the unary temporal operators $\bigcirc$ (*next*), $\Diamond$ (*eventually*), $\Box$ (*always*), the binary temporal operator U (*until*), and brackets. Examples of PTL-formulas over $\Sigma = \{a, b\}$ are

$$\varphi_1 = \Box \Diamond (p_a \wedge \bigcirc p_b),$$
$$\varphi_2 = \neg \Diamond (p_a \wedge \bigcirc (\neg p_b \,\mathrm{U}\, p_a)).$$

A PTL-formula is interpreted either over a finite nonempty sequence $\alpha = \alpha(0)\alpha(1)\ldots\alpha(n-1)$ $(n \geqslant 1)$ or over an infinite sequence $\alpha = \alpha(0)\alpha(1)\ldots$ with $\alpha(i) \in \Sigma$. The length of α, denoted by $|\alpha|$, is thus either a positive natural number or ω. The satisfaction relation $\models$ between pairs (α, i) (where $0 \leqslant i < |\alpha|$) and PTL-formulas φ is defined inductively as follows:

$$(\alpha, i) \models p_a \quad \text{iff} \quad \alpha(i) = a,$$
$$(\alpha, i) \models \neg\varphi \quad \text{iff} \quad \text{not } (\alpha, i) \models \varphi,$$

similarly for the other boolean connectives,

$$(\alpha, i) \models \bigcirc\varphi \quad \text{iff} \quad i+1 < |\alpha| \text{ and } (\alpha, i+1) \models \varphi,$$
$$(\alpha, i) \models \Diamond\varphi \quad \text{iff} \quad \text{for some } j \text{ with } i \leqslant j < |\alpha|\text{: } (\alpha, j) \models \varphi,$$
$$(\alpha, i) \models \Box\varphi \quad \text{iff} \quad \text{for all } j \text{ with } i \leqslant j < |\alpha|\text{: } (\alpha, j) \models \varphi,$$
$$(\alpha, i) \models \varphi \,\mathrm{U}\, \psi \quad \text{iff} \quad \text{for some } j \text{ with } i \leqslant j < |\alpha| \text{ we have: } (\alpha, j) \models \psi \text{ and for all } k \text{ with } i \leqslant k < j,\ (\alpha, k) \models \varphi.$$

A PTL-formula φ defines a set $K(\varphi)$ of finite sequences and a set $L(\varphi)$ of infinite sequences:

$$K(\varphi) := \{\alpha \in \Sigma^{+} \mid (\alpha, 0) \models \varphi\},$$
$$L(\varphi) := \{\alpha \in \Sigma^{\omega} \mid (\alpha, 0) \models \varphi\}.$$

EXAMPLE. Considering the PTL-formulas φ_1 and φ_2 from above, we have, for $\alpha \in \Sigma^\omega$,

$\alpha \in L(\varphi_1)$ iff α contains infinitely many segments ab,

$\alpha \in L(\varphi_2)$ iff between any two a's in α there is some b (i.e., there is no occurrence of an a such that up to the following a there is no b).

Note that by the semantics of the next-operator (*strong next*) we have $K(\varphi_1) = \emptyset$.

Remark. Usually, the semantics of PTL is introduced in a slightly more general form: Instead of Σ, a (finite or infinite) set S of states is considered, and a map τ from the set of propositional variables into 2^S is given, stipulating for any variable p those states in which p is assumed true. Restricting to finitely many propositional variables only (which is sufficient for any concrete applications), τ induces a finite partition of S (where two states s, s' belong to the same class provided for any propositional variable p we have $s \in \tau(p)$ iff $s' \in \tau(p)$). Hence our terminology is no essential restriction of the usual definitions, on the other hand it simplifies the transition to other frameworks like automata or formal languages.

Let us turn to characterizations of PTL-definable sequence sets. For a model theoretic description we view a sequence $\alpha = \alpha(0) \ldots \alpha(n-1)$, resp. $\alpha = a(0)a(1)a(2)\ldots$, over Σ as a finite, resp. infinite linear ordering with additional unary predicates. The domain of the ordering is the set $\{0, \ldots, n-1\}$, resp. ω, ordered in the usual way by $<$ and equipped for any $a \in \Sigma$ with a unary predicate P_a containing the numbers i with $\alpha(i) = a$. A sentence φ in the corresponding first-order language (with nonlogical symbols $<$ and P_a for $a \in \Sigma$) defines again a set $K(\varphi)$ of finite sequences and a set $L(\varphi)$ of infinite sequences (namely those sequences which satisfy φ under the indicated standard interpretation). For example, the sentences

$$\psi_1 = \forall x \exists y (x < y \wedge P_a y \wedge \exists z (z = \mathrm{succ}(y) \wedge P_b z)),$$

$$\psi_2 = \forall x \forall y (x < y \wedge P_a x \wedge P_a y \rightarrow \exists z (x < z \wedge z < y \wedge P_b z))$$

(where $z = \mathrm{succ}(y)$ abbreviates $y < z \wedge \neg\exists z' (y < z' \wedge z' < z)$) define the same sets of ω-sequences as the PTL-formulas φ_1 and φ_2 above. Call a set $K \subset \Sigma^+$ (resp. $L \subset \Sigma^\omega$) *first-order definable* if for some sentence φ of the first-order language appropriate for Σ, we have $K = K(\varphi)$ (resp. $L = L(\varphi)$). Clearly, PTL-formulas can be translated into first-order sentences by formalizing the semantics of the temporal operators in the first-order language over the structure $(\omega, <)$. The fact that also a converse translation is possible is much less obvious.

1.1. THEOREM ([8], [5]). (a) *A language $K \subset \Sigma^+$ is* PTL-*definable iff K is first-order definable.*

(b) *An ω-language $L \subset \Sigma^\omega$ is* PTL-*definable iff L is first-order definable.*

As a consequence one notes that PTL-definable sequence sets are *regular* (either regular sets of finite words or ω-regular sets of ω-sequences), since by Büchi's characterization results [2], [3] a set of sequences is regular (resp. ω-regular) iff it is defined in the monadic second-order extension of the first-order language considered above. Conversely, however, not every (ω-) regular sequence set is first-order definable: For example, as observed by Ladner in [9], the property of sequences which requires that between any two letters a an even number of letters b occurs is not expressible in the first-order language. This was also shown in [32] and taken there as a motivation to set up an extended temporal logic ETL in which precisely the ω-regular ω-languages are definable (see also [33]).

For sets of *finite* words, it has been known since the early seventies that first-order definability can be characterized elegantly in terms of "star-free" languages. A set $K \subset \Sigma^*$ is called *star-free* if it is in the closure of the finite word-sets under concatenation and boolean operations. A comprehensive treatment of star-free languages is given in the monograph [16]. In [9] an extension of the above definition to ω-languages was suggested: A set $L \subset \Sigma^\omega$ is called *ω-star-free* if it belongs to the closure of the empty set of ω-sequences over Σ under boolean operations and concatenation with star-free sets of finite words on the left.

1.2. THEOREM (a) ([16]). *A language $K \subset \Sigma^+$ is first-order definable iff it is star-free.*
(b) ([9], [29]). *An ω-language $L \subset \Sigma^\omega$ is first-order definable iff it is ω-star-free.*

As an illustration for (b) we present ω-star-free representations of the ω-languages $L(\varphi_1)$ and $L(\varphi_2)$ considered above as examples:

$$L(\varphi_1) = \sim(\Sigma^* \cdot \sim(\Sigma^* \cdot a \cdot b \cdot \Sigma^\omega)),$$
$$L(\varphi_2) = \sim(\Sigma^* \cdot a \cdot (\Sigma - b)^* \cdot a \cdot \Sigma^\omega).$$

(Note that $\Sigma^\omega = \sim\emptyset$ and that $(\Sigma - b)^* = \Sigma^* - (\Sigma^* \cdot b \cdot \Sigma^*)$.)

Referring to some given alphabet Σ, we denote in the sequel by REG (resp. SF) the class of regular (resp. star-free) languages over Σ, and by ω-REG (resp. ω-SF) the class of ω-regular (resp. ω-star-free) ω-languages over Σ.

The simple inductive structure of the classes of star-free and ω-star-free sets can provide, via the characterization results above, a valuable tool in investigations concerning PTL. An example is Theorem 3.4 below. The ω-star-free sequence sets also consitute a natural intermediate step in the difficult proof that first-order definability implies PTL-definability. Indeed, the normal form for first-order formulas called "special formulas" in [5] is very similar to ω-star-free representations of sequence sets.

2. Safety- and liveness-properties

In many practical applications, the specification of parallel programs involves only temporal formulas of a special form: For instance, the specification may just require that for the resulting execution sequences a certain condition on states should hold at any time, or that such a condition should hold again and again. Properties of execution sequences of this kind are called safety- and liveness-properties, respectively. Papers [12], [13], [18] show by several examples how these properties arise naturally in specifications, and they present elegant methods for their verification.

Recently, [11] proposed a general and precise definition of the notions "safety-property" and "liveness-property". For this purpose, the PTL-formalism is extended by the unary past operators $\otimes$ (*strong previous*), $\langle + \rangle$ (*sometime in the past*) $[\times]$ (*always in the past*), and the binary operator S (*since*). Their semantics is defined (for a sequence α and $0 \leqslant i < |\alpha|$) by the clauses

$$
\begin{array}{lll}
(\alpha, i) \models \otimes\varphi & \text{iff} & i > 0 \text{ and } (\alpha, i-1) \models \varphi, \\
(\alpha, i) \models \langle + \rangle\varphi & \text{iff} & \text{for some } j \text{ with } 0 \leqslant j \leqslant i\text{: } (\alpha, j) \models \varphi, \\
(\alpha, i) \models [\times]\varphi & \text{iff} & \text{for all } j \text{ with } 0 \leqslant j \leqslant i\text{: } (\alpha, j) \models \varphi, \\
(\alpha, i) \models \varphi \mathrm{S} \psi & \text{iff} & \text{for some } j \text{ with } 0 \leqslant j \leqslant i\text{: } (\alpha, j) \models \psi \\
 & & \quad \text{and for all } k \text{ with } j < k \leqslant i, (\alpha, k) \models \varphi.
\end{array}
$$

Since the semantics of these operators can be described in the first-order language over $(\omega, <)$ in the same way as for the "future operators" $\bigcirc$, $\Diamond$, $\Box$ and U, it follows that in the extended system, denoted here by PTL^+, no more properties can be expressed than in the original system PTL. A PTL^+-formula is called a *past formula* if all temporal operators occurring in it are past operators. Dualizing the case of the PTL-formulas, such a past formula φ defines a language $K_p(\varphi)$ of finite words by setting

$$K_p(\varphi) = \{\alpha \in \Sigma^+ \mid \alpha = \alpha(0) \ldots \alpha(n-1),\ (\alpha, n-1) \models \varphi\}.$$

By the symmetry between $\bigcirc$, $\Diamond$, $\Box$, U and $\otimes$, $\langle + \rangle$, $[\times]$, S it is obvious that a set $K \subset \Sigma^+$ is defined in this sense by a past formula iff K is PTL-definable. Let us now say that a PTL- (or PTL^+-) formula *represents a safety-property* (resp. *eventuality-property*, *liveness-property*) if φ is equivalent over all ω-sequences to a formula $\Box\psi$ (resp. $\Diamond\varphi$, $\Box\Diamond\psi$), where ψ is a past formula. (It is easy to give corresponding definitions for the extended temporal logic ETL of [32], [33] instead of PTL. We do not pursue this case in further detail here; it turns out that the characterization results below extend in a straightforward way to ETL, referring to monadic second-order logic instead of first-order logic and to regular languages instead of star-free languages.)

It should be noted that one finds several variants of the notions "safety-property" and "liveness-property" in the literature. In [11], for example, liveness-properties are defined not only in terms of formulas $\Box\Diamond\psi$ with past formula ψ, but also in terms of formulas $\Diamond\psi$ (i.e., eventuality formulas) and formulas $\Diamond\Box\psi$; even any positive boolean combination of such formulas is allowed. As will be clear from Theorem 2.6 below, this proposal means that *any* PTL-formula not defining a safety-property will represent a liveness property. Thus we are led to restrict liveness formulas to the form which is most typical in applications (namely, $\Box\Diamond\psi$). As a more special definition of safety and liveness properties we mention that of [18]: There safety-properties are represented by formulas $\varphi \to \Box\psi$ and liveness-properties by formulas $\Box(\varphi \to \Diamond\varphi)$; in both cases φ and ψ are "immediate assertions", i.e., formulas without temporal operators. Still a different approach is taken by Sistla in [27]; there φ represents a safety-property if $(\alpha, 0) \models \varphi$ is equivalent to the condition that any prefix u of α can be extended by some β with $(u\beta, 0) \models \varphi$; and φ represents a liveness-property if for any finite u there is an extension β such that $(u\beta, 0) \models \varphi$. For safety-properties this definition is equivalent to our definition, but for liveness-properties a notion results that is incomparable to the one introduced above. Sistla characterizes safety and liveness properties in his sense syntactically by fragments of PTL; this allows then to set up axiom systems which yield effective enumerations of the PTL-formulas representing such safety, resp. liveness properties.

Note that φ represents a safety-property iff $\neg\varphi$ represents an eventuality-property. In the context of language theory, eventuality-properties arise more naturally. Thus in the sequel we will often refer to eventuality-properties and not primarily to safety-properties.

Using the results of Section 1, one obtains a characterization of these properties in first-order logic. It is convenient for this purpose to consider the notion of a "bounded formula" (as in [29], [30]): Call a first-order formula $\psi(x)$ with one free variable x *bounded* if all quantifiers in ψ are relativized to the elements $\leqslant x$, i.e., all quantifiers are of the form $\exists z(z \leqslant x \wedge \ldots)$ or $\forall z(z \leqslant x \to \ldots)$. Then from Theorem 1.1 we infer

2.1. PROPOSITION. *A PTL-formula φ represents an eventuality-property (resp. safety-property, liveness-property) iff φ is equivalent over all ω-sequences to a first-order formula of the form $\exists x\psi(x)$ (resp. $\forall x\psi(x)$, $\forall y \exists x(y < x \wedge \psi(x))$), where $\psi(x)$ is bounded.*

Note that it is easy to write the example formula $\varphi_1 = \Box\Diamond(p_a \wedge \bigcirc p_b)$ of Section 1 in the form $\forall y \exists x(y < x \wedge \psi(x))$, and $\varphi_2 = \neg\Diamond(p_a \wedge \bigcirc(\neg p_b \mathrm{U} p_a))$ in the form $\forall x \psi(x)$, where $\psi(x)$ is bounded. Hence φ_1 represents a liveness-property and φ_2 represents a safety-property.

A characterization in language theoretical terms uses two operations that transform a set $K \subset \Sigma^+$ of finite words into a set of ω-words:

$$\mathrm{ext}\, K = \{\alpha \in \Sigma^\omega \mid \text{some initial segment of } \alpha \text{ is in } K \text{ ("}\alpha\text{ extends a word in } K\text{")}\},$$

$$\lim K = \{\alpha \in \Sigma^\omega \mid \text{infinitely many initial segments of } \alpha \text{ are in } K \text{ ("}\alpha\text{ is a limit of words in } K\text{")}\}$$

Given the alphabet Σ, let ext(REG) and ext(SF) denote the classes of ω-languages of the form ext K with $K \subset \Sigma^+$ regular, resp. star-free. Similarly we define lim(REG) and lim(SF). Then we have, by Theorem 1.2.

2.2. PROPOSITION. *A* PTL-*formula* φ *represents an eventuality-property (resp. liveness-property) iff* $L(\varphi) \in \mathrm{ext(SF)}$ *(resp.* $L(\varphi) \in \mathrm{lim(SF)}$*).*

It is interesting to note that the classes ext(REG) and lim (REG) have been investigated by Landweber [10] in an automata theoretic context. The objective of this work was to compare different acceptance modes of deterministic ω-automata: Given an ω-automaton $\mathcal{A} = (\Sigma, Q, q_0, \delta, F)$ with state set Q, initial state q_0, transition function δ: $Q \times \Sigma \to Q$ (extended in the natural way to δ: $Q \times \Sigma^* \to Q$), and a set F of final states, Landweber defined, for a sequence $\alpha \in \Sigma^\omega$:

$$\mathcal{A} \text{ 1-accepts } \alpha \quad \text{iff} \quad \delta(q_0, \alpha(0)\ldots\alpha(n-1)) \in F \quad \text{for some } n,$$

$$\mathcal{A} \text{ 2-accepts } \alpha \quad \text{iff} \quad \delta(q_0, \alpha(0)\ldots\alpha(n-1)) \in F \quad \text{for infinitely many } n.$$

An ω-language $L \subset \Sigma^\omega$ is called 1- (resp. 2-) *definable* if for some finite automaton $\mathcal{A}$,

$$\alpha \in L \quad \text{iff} \quad \mathcal{A} \text{ 1- (resp. 2-) accepts } \alpha.$$

Recall that L is ω-regular iff it is definable by a *non*deterministic finite automaton using 2-acceptance (*Büchi automaton*). From the above definitions we have immediately

2.3. *Remark.* $L \in \mathrm{ext(REG)}$ iff L is 1-definable; $L \in \mathrm{lim(REG)}$ iff L is 2-definable.

The main result of [10] can now be stated as follows (referring to an alphabet with at least two letters):

2.4. THEOREM ([10]). (a) ext(REG) $\subsetneqq$ lim(REG) $\subsetneqq$ ω-REG.

(b) *For* ω*-languages in* ω-REG *(given e.g. by Büchi automata) membership in* ext(REG) *and in* lim(REG) *is decidable.*

The ω-languages needed to prove (a), i.e., $\lim(\text{REG})-\text{ext}(\text{REG}) \neq \emptyset$ and $(\omega\text{-REG})-\lim(\text{REG}) \neq \emptyset$, can simply be taken as the set of ω-sequences having infinitely many, resp. only finitely many letters a. Since these sets clearly belong to lim(SF), resp. ω-SF, we have

2.5. COROLLARY. $\text{ext}(\text{SF}) \subsetneqq \lim(\text{SF}) \subsetneqq \omega\text{-SF}$.

In the following section it will be seen that also part (b) of Theorem 2.4 extends to the case of star-free sets.

Statements 2.4(a) and 2.5 suggest the question "how far" the classes lim(REG) and ω-REG (resp. lim(SF) and ω-SF) are apart. An answer is provided by McNaughton's fundamental theorem on determinization of Büchi automata for the regular case and by the normal form theorem of [30] for the star-free case:

2.6. THEOREM ([15], [30]. *An ω-language $L \in \omega$-REG (resp. $L \in \omega$-SF) can be represented in the form*

$$\bigcup_{i=1}^{n} (\lim K_i \cap \sim \lim K_i'),$$

where K_i, $K_i' \in \text{REG}$ (resp. K_i, $K_i' \in \text{SF}$) for $i = 1, \ldots, n$.

Translating this normal form back to temporal logic, we obtain in particular that any PTL-formula is equivalent (over all ω-sequences) to a boolean combination of PTL-formulas that represent liveness properties.

3. Decidability results

The aim of this section is to show that the classes ω-SF, lim(SF) and ext(SF) are decidable relative to ω-REG. For the proofs we rely on Schützenberger's Theorem [26] characterizing the star-free sets of *finite* words and some elementary facts on a syntactic congruence for ω-languages that appear in Arnold's paper [1].

Let us state these preliminaries more precisely. Given a language $K \subset \Sigma^*$, the *syntactic congruence* of K is defined by

$$x \sim_K y \quad \text{iff} \quad \text{for all } u, v \in \Sigma^* \ (uxv \in K \text{ iff } uyv \in K)$$

for $x, y \in \Sigma^*$. The syntactic monoid $M(K)$ is the structure $\Sigma^*/\sim_K$, where multiplication is defined by concatenation of representatives of the $\sim_K$-classes. If K is regular, then $M(K)$ is finite and can be constructed effectively from a description of K (say in terms of automata or regular expressions). A monoid M is called *group-free* (or *aperiodic*) if there is no set $G \subset M$ with at least two elements which forms a group under the multiplication of M. Note that for finite M this property is effectively decidable.

3.1. *Remark* ([16], p. 52–53). Let K be a regular language. Then the following are equivalent:

(1) $M(K)$ is group-free,

(2) $\exists n_0 \forall n \geqslant n_0 \ \forall g \in M(K)$: $g^n = g^{n+1}$,

(3) K is *noncounting*, i.e., $\exists n_0 \ \forall n \geqslant n_0 \forall x, y, z \in \Sigma^*$: $xy^n z \in K$ iff $xy^{n+1} z \in K$.

3.2. SCHÜTZENBERGER'S THEOREM ([26], [16], [22]). *A regular language $K \subset \Sigma^*$ is star-free iff $M(K)$ is group-free. (Hence for regular languages the property "star-free" is decidable.)*

Recently, Arnold [1] has suggested a modified congruence relation $\approx_L$ on Σ^* which refers to an ω-language L (instead of the language K above) and is appropriate for an extension Schützenberger's Theorem to sets of infinite words. Given $L \subset \Sigma^\omega$, define for $x, y \in \Sigma^*$

$$x \approx_L y \quad \text{iff} \quad \text{for all } u, v, w \in \Sigma^*:$$

$$(uxvw^\omega \in L \text{ iff } uyvw^\omega \in L) \text{ and } \big(u(vxw)^\omega \in L \text{ iff } u(vyw)^\omega \in L\big).$$

Remark. Note that the straightforward extension of $\sim_K$ would just require that $ux\alpha \in L$ iff $uy\alpha \in L$ for any $u \in \Sigma^*$, $\alpha \in \Sigma^\omega$. This congruence has been considered previously by [6] but is too coarse for the present purpose: For example it is not possible to distinguish whether some given word occurs infinitely often or only finitely often in an ω-word.

3.3. LEMMA ([1]). *If $L \subset \Sigma^\omega$ is ω-regular, then $\approx_L$ is a congruence relation on Σ^* of finite index having regular equivalence classes. Moreover, L is a union of sets of the form $K_0 \cdot K^\omega$, where K_0, K are equivalence classes of $\approx_L$.*

For $L \subset \Sigma^\omega$, the *syntactic monoid* $M(L)$ is the structure $\Sigma^*/\approx_L$. Now we can state the analogue of Theorem 3.2 for ω-languages:

3.4. THEOREM ([20]). *An ω-regular ω-language $L \subset \Sigma^\omega$ is ω-star-free iff $M(L)$ is group-free. (Hence for ω-regular ω-languages the property "ω-star-free" is decidable.)*

For our proof we need the following equivalences, obtained as Remark 3.1 above:

3.5. *Remark.* Let $L \subset \Sigma^\omega$ be ω-regular. Then the following are equivalent:

(1) $M(L)$ is group-free,

(2) $\exists n_0 \ \forall n \geqslant n_0 \ \forall g \in M(L)$, $g^n = g^{n+1}$,

(3) $\exists n_0 \ \forall n \geqslant n_0 \ \forall y, u, v, w \in \Sigma^*$:

$$(*) \quad \begin{aligned} &(uy^n vw^\omega \in L \quad \text{iff} \quad uy^{n+1} vw^\omega \in L) \quad \text{and} \\ &\big(u(vy^n w)^\omega \in L \quad \text{iff} \quad u(vy^{n+1} w)^\omega \in L\big). \end{aligned}$$

Proof of 3.4. For the direction from left to right we use induction over the construction of ω-star-free sequence sets. It suffices to verify condition (3) of

3.5. For $L = \emptyset$ this is clear; also if (3) holds for L it obviously holds for the complement $\sim L$. Assuming (*) for L_1 (with $n \geqslant n_1$) and for L_2 (similarly with $n \geqslant n_2$) then (*) holds for $L_1 \cup L_2$ provided $n \geqslant \max(n_1, n_2)$. Thus it remains to treat the concatenation step: Suppose $L \subset \Sigma^\omega$ is given s.t. (*) holds for $n \geqslant n_2$, and assume $K \subset \Sigma^\omega$ is star-free, i.e., we have n_1 with

(○) $$xy^n z \in K \quad \text{iff} \quad xy^{n+1} z \in K$$

for $n \geqslant n_1$. Set $n_0 = n_1 + 1 + n_2$; we claim that (*) holds for $K \cdot L$ if $n \geqslant n_0$.

First, suppose we have $uy^n vw^\omega \in K \cdot L$ and hence an initial segment s_1 of this ω-word in K and the corresponding final part s_2 in L. Since $n \geqslant n_0 = n_1 + 1 + n_2$, we have $s_1 = uy^{n_1} u'$ for some u', or $s_2 = u'' y^{n_2} vw^\omega$ for some u''. In the first case we apply (○), and in the second we apply (*) to obtain $uy^{n_1+1} u' \in K$, resp. $u'' y^{n_2+1} vw^\omega \in L$. Hence $uy^{n+1} vw^\omega \in K \cdot L$ as desired. The step from $n+1$ back to n is similar.

Secondly, suppose $u(vy^n w)^\omega \in K \cdot L$; we have to verify $u(vy^{n+1} w)^\omega \in K \cdot L$. Let s_1, s_2 be the segments in K, resp. L as above such that $s_1 s_2 = u(vy^n w)^\omega$, say

$$s_1 = u(vy^n w)^k u', \qquad s_2 = u''(vy^n w)^\omega, \qquad u'u'' = vy^n w.$$

Since $n \geqslant n_1$ we can apply (○) k times to s_1 (for the different occurrences of the segements y^n) and obtain $u(vy^{n+1} w)^k u' \in K$. Moreover, by $n \geqslant n_2$ and (*) we have $u''(vy^{n+1} w)^\omega \in L$. Finally, by $n \geqslant n_1 + 1 + n_2$, we can add as before one y-segment either to u' or to u'', without leaving the set K, resp. L; so $u'u''$ can be replaced by $vy^{n+1} w$. Hence $u(vy^{n+1} w)^\omega \in K \cdot L$. Again the step from $n+1$ to n is analogous.

Let us now prove the converse direction of the theorem assuming that $M(L)$ is group-free. In the sequel, $[x]$ denotes the element of $M(L)$ (i.e., the $\approx_L$-class) that contains x. Note that for $\approx_L$-classes K_1, K_2, K, $K_1 \cdot K_2 \cap K \neq \emptyset$ implies $K_1 \cdot K_2 \subset K$. By 3.3, L is a finite union of sets $K_0 \cdot K^\omega$; where K_0, K are $\approx_L$-classes. We shall show that any of these sets $K_0 \cdot K^\omega$ is first-order definable (and hence, by 1.2, ω-star-free). First we see that any $\approx_L$-class C is noncounting since $M(L)$ is group-free: Indeed, we have $uv^n w \in C$ iff $uv^{n+1} w \in C$ for n large enough, since in $M(L)$ the equality $[v]^n = [v]^{n+1}$ holds (by 3.5(2)) and hence $[uv^n w] = [uv^{n+1} w]$. Thus any $\approx_L$-class is first-order definable by Theorems 1.2 and 3.2. Furthermore, when considering $K_0 \cdot K^\omega$ we may restrict to the case that $K \cdot K \subset K$ since $K_0 \cdot K^\omega = K_0 \cdot (K^n)^\omega$ and for n large enough we have $K^{n+1} \subset K^n$ (by the noncounting property) and hence $K^n \cdot K^n \subset K^n$. We claim that in this case ($K \cdot K \subset K$), for any $\alpha \in \Sigma^\omega$:

(+) $\alpha \in K_0 \cdot K^\omega$ iff

$$\exists k_0 \big(\alpha(0, k_0) \in K_0 \wedge \forall k \exists k', k'' > k \big(\alpha(k_0, k') \in K \wedge \alpha(k', k'') \in K\big)\big).$$

(Here $\alpha(i, j)$ indicates for $i < j$ the segment $\alpha(i)\ldots\alpha(j-1)$.) Since (+) is clearly first-order formalizable over $(\omega, <)$ assuming first-order definability of K_0 and K, it remains to show that the above equivalence holds. The direction from $\alpha \in K_0 \cdot K^\omega$ to (+) is obvious (by $K \cdot K \subset K$). For the converse, first note that the last conjunction implies $\alpha(k_0, k'') \in K$. We shall find a sequence $k_0, k_1, \ldots$ such that $\alpha(0, k_0) \in K_0$, and for each i

(1) $\alpha(k_0, k_1), \ldots, \alpha(k_{i-1}, k_i) \in K$,

(2) there is $l > k_i$ with $\alpha(k_0, l)$, $\alpha(k_i, l) \in K$.

Pick k_0 as guaranteed by (+). Then $\alpha(0, k_0) \in K_0$ and (2) is satisfied for k_0. Assume $k_0, \ldots, k_i$ have been found such that $\alpha(k_0, k_1), \ldots, \alpha(k_{i-1}, k_i) \in K$ and (2) holds for k_i. Choose l as in (2) and find $k', k'' > l$ as given by (+). Set $k_{i+1} = k'$ and use k'' to check that (2) is satisfied for k'. On the other hand we have $\alpha(k_i, k') \in K$: Namely, $\alpha(k_0, l)$ and $\alpha(k_i, l)$ are in the same $\approx_L$-class K and hence clearly $\alpha(k_0, n)$ and $\alpha(k_i, n)$ will be in the same $\approx_L$-class for any $n \geqslant l$ (since $\approx_L$ is a congruence). By $k' > l$ and $\alpha(k_0, k') \in K$ we thus have $\alpha(k_i, k') \in K$ as required.

Remark. It is a somewhat tedious task to transform the first-order formula (+) directly into an ω-star-free representation of $K_0 \cdot K^\omega$, assuming that K_0 and K are star-free. This would make it unnecessary to refer to Theorem 1.2 in the proof above.

In order to combine Landweber's Theorem 2.4 and the preceding Theorem 3.4 we show the following equalities:

3.5. Proposition. (a) $\text{ext}(\text{SF}) = \text{ext}(\text{REG}) \cap \omega\text{-SF}$,

(b) $\lim(\text{SF}) = \lim(\text{REG}) \cap \omega\text{-SF}$.

Clearly this yields, by 2.4 and 3.4:

3.6. Corollary. *For ω-regular ω-languages, membership in* ext(SF) *and in* lim(SF) *is decidable. Hence for a* PTL- (*or* ETL-) *formula it can be decided effectively whether it represents a safety-, eventuality- or liveness-property.*

Proof of 3.5.([1]). It suffices to show the inclusions "$\supset$". For (a), assume that $L \subset \Sigma^\omega$ is ω-star-free and $L = K \cdot \Sigma^\omega$ for some regular $K \subset \Sigma^*$. Let

$$K_0 = \{y \in \Sigma^* \mid \text{all } \omega\text{-sequences with prefix } y \text{ have some prefix in } K\}.$$

We claim that $L = K_0 \cdot \Sigma^\omega$ and that K_0 is star-free (which proves $L \in \text{ext}(\text{SF})$). To prove $L = K_0 \cdot \Sigma^\omega$, note that $K \subset K_0$ and hence $L \subset K_0 \cdot \Sigma^\omega$. On the other hand, given $\alpha \in K_0 \cdot \Sigma^\omega$, by definition of K_0 some prefix of α belongs to K, i.e., $\alpha \in K \cdot \Sigma^\omega$. To prove that K_0 is star-free we show that K_0 is regular and satisfies the noncounting property of 3.1(3): First note that a finite automaton $\mathscr{A}$ recognizing K, say with initial state q_0, can be transformed

([1]) A preliminary version of this proof was obtained jointly with F. Rancke, cf. [25].

into a finite automaton recognizing K_0 by taking as final states all states q such that any infinite path from q_0 through q hits some final state of $\mathscr{A}$. Next we state two facts on K_0:

(1) $$y \in K_0 \Rightarrow \forall y', w \in \Sigma^*: yy'w^\omega \in K_0 \cdot \Sigma^\omega,$$

(2) $$y \notin K_0 \Rightarrow \exists y', w \in \Sigma^*: yy'w^\omega \notin K_0 \cdot \Sigma^\omega.$$

(1) is obvious from the definitions. For (2) assume that $y \notin K_0$, i.e., some sequence in $y \cdot \Sigma^\omega$ does not belong to $K \cdot \Sigma^\omega$. Then the ω-language $y \cdot \Sigma^\omega \cap \sim(K \cdot \Sigma^\omega)$ is nonempty, and since it is ω-regular it contains (by [3]) an ultimately periodic sequence. This sequence is of the form $yy'w^\omega$ as required. We now show (by contradiction) that K_0 is noncounting: Assume that for arbitrary large n there are $x, y, z \in \Sigma^*$ such that

(3) $$xy^n z \in K_0 \quad \text{and} \quad xy^{n+1} z \notin K_0.$$

Since L was assumed ω-star-free and hence satisfies the property of 3.5(3), we have for sufficiently large n, say with $n \geqslant n_0$, that for all $y, u, v, w \in \Sigma^*$

(4) $$uy^n vw^\omega \in L \quad \text{iff} \quad uy^{n+1} vw^\omega \in L.$$

Now pick some $n \geqslant n_0$ and x, y, z such that (3) holds. Since $xy^{n+1} z \notin K_0$ we find by (2) some y', w with $xy^{n+1} zy'w^\omega \notin K_0 \cdot \Sigma^\omega$ $(= L)$. Hence, by (4), we have $xy^n zy'w^\omega \notin K_0 \cdot \Sigma^\omega$; but this contradicts (3), in particular $xy^n z \in K_0$.

The proof of (b) is similar: Assume L is ω-star-free and $L = \lim K$ for some regular K. Let

$$K_0 = \{y \in K \mid \text{for some } \beta \in \Sigma^\omega,\ y\beta \in \lim K\}.$$

We claim that $\lim K_0 = \lim K$ and that K_0 is star-free. Since $K_0 \subset K$ we have $\lim K_0 \subset \lim K$. Conversely, given $\alpha \in \lim K$, we have that any α-prefix y in K has an extension β with $y\beta \in \lim K$ and thus belongs to K_0; this yields $\alpha \in \lim K_0$. Again it is easy to verify that K_0 is regular, by taking appropriate final states in a finite automaton recognizing K. It remains to show that K_0 is noncounting; here we use

(1) $$y \in K_0 \Rightarrow \exists y', w \in \Sigma^*: yy'w^\omega \in \lim K_0,$$

(2) $$y \notin K_0 \Rightarrow \forall y', w \in \Sigma^*: yy'w^\omega \notin \lim K_0.$$

Condition (2) is obvious; and (1) is satisfied since from $y \in K_0$ we have $y \cdot \Sigma^\omega \cap \lim K \neq \emptyset$ and thus obtain in this (ω-regular) set an ultimately periodic sequence $yy'w^\omega$. Assume now that for K_0 the noncounting condition of 3.1(3) is violated; then for arbitrary large n we may choose x, y, z with

$$xy^n z \in K_0 \quad \text{and} \quad xy^{n+1} z \notin K_0.$$

By (1) we find y' and w such that $xy^n zy'w^\omega \in \lim K_0$. However, applying (2) to $xy^{n+1} z$ we know that $xy^{n+1} zy'w^\omega \notin \lim K_0$ $(= L)$. But since L was assumed ω-star-free, the noncounting Property 3.5(3) is satisfied, i.e., for n large enough $xy^n zy'w^\omega \in L$ iff $xy^{n+1} zy'w^\omega \in L$. Thus we obtain the desired contradiction.

As a final remark we mention that a strong extension of Landweber's Theorem has been obtained by Wagner [31] (and recently reproved by Kamiński [7]): For any $n \geqslant 1$, consider the class $\mathscr{L}_n$ of ω-regular sequence sets L with a representation

$$L = \bigcup_{i=1}^{n} (\lim K_i \cap \sim \lim K_i') \qquad (K_i, K_i' \text{ regular})$$

as in the normal form Theorem 2.6.

An ω-language in class $\mathscr{L}_n$ is said to be of *Rabin index n* (reminding of Rabin's acceptance condition for automata on infinite trees [24]). In [31], Sections 5, 8, it is shown that these classes form a proper hierarchy ($\lim(\text{REG}) \subsetneqq \mathscr{L}_1 \subsetneqq \mathscr{L}_2 \ldots$), and that the Rabin index of an ω-language is effectively computable. A natural generalization of the present paper would consist in a "star-free version" of these results; in particular, we conjecture that for each $n \geqslant 1$ the star-free analogue of $\mathscr{L}_n$ coincides with the class $\mathscr{L}_n \cap \omega$-SF.

References

[1] A. Arnold, *A syntactic congruence for rational ω-languages*, Theor. Comput. Sci. 39 (1985), 333–335.

[2] J. R. Büchi, *Weak second-order arithmetic and finite automata*, Z. Math. Logik u. Grundlag Math. 6 (1960), 66–92.

[3] –, *On a decision method in restricted second-order arithmetic*, in: Proc. Int. Congr. Logic, Meth. and Phil. of Sci. 1960, Stanford Univ. Press, Stanford, Calif. 1962, 1–11.

[4] E. A. Emerson, E. M. Clarke, *Using branching time temporal logic to synthesize synchronization skeletons*, Sci. Comput. Progr. 2 (1982), 241–266.

[5] D. Gabbay, A. Pnueli, S. Shelah, J. Stavi, *On the temporal analysis of fairness*, 7th ACM Symp. on Principles of Progr. Languages (1980), 163–173.

[6] H. Jürgensen, G. Thierrin, *On ω-languages whose syntactic monoid is trivial*, Int. J. Comput. Inform. Syst. 12 (1983), 359–365.

[7] M. Kamiński, *A classification of ω-regular languages*, Theor. Comput. Sci. 36 (1985), 217–239.

[8] H. W. Kamp, *Tense logic and the theory of linear order*, Ph. D. Thesis, Univ. of California, Los Angeles 1968.

[9] R. E. Ladner, *Application of model-theoretic games to discrete linear orders and finite automata*, Inf. Contr. 33 (1977), 281–303.

[10] L. H. Landweber, *Decision problems of ω-automata*, Math. Syst. Theory 4 (1969), 376–384.

[11] O. Lichtenstein, A. Pnueli, L. Zuck, *The glory of the past*, Logics of Programs, Proceedings, Springer Lecture Notes in Comput. Sci. 193 (1985), 196–218.

[12] Z. Manna, A. Pnueli, *Verification of concurrent programs: the temporal framework*, in: *The Correctness Problem in Computer Science* (eds. R. S. Boyer, J. S. Moore), Int. Lect. Series in Comp. Sci., Academic Press, 1981.

[13] –, –, *Adequate proof principles for invariance and liveness properties of concurrent programs*, Science Comput. Progr. 4 (1984), 257–289.

[14] Z. Manna, P. Wolper, *Synthesis of communicating processes from temporal logic specifications*, ACM Trans. on Progr. Lang. 6 (1984), 68–93.

[15] R. McNaughton, *Testing and generating infinite sequences by a finite automaton*, Inf. Contr. 9 (1966), 521–530.

[16] –, S. Papert, *Counter-free Automata*, MIT-Press, Cambridge Mass. 1971.

[17] B. C. Moszkowski, *Reasoning about digital circuits*, Ph. D. Thesis, Stanford Univ. 1983.

[18] S. Owicki, L. Lamport, *Proving liveness properties of concurrent programs*, ACM TOPLAS 4 (1982), 445–495.

[19] R. Peikert, *ω-regular languages and propositional temporal logic*, Report No. 85–01, Mathematik, ETH Zürich 1985.

[20] D. Perrin, *Recent results on automata and infinite words*, in: Math. Found. of Comput. Sci. 1984, LNCS 176 (1984), 134–148.

[21] –, J. E. Pin, *On the expressive power of temporal logic*, Rep. 86–17, LITP, Univ. Paris VII, 1986.

[22] J. E. Pin, *Variétés de langages formels*, Masson 1984.

[23] A. Pnueli, *The temporal logic of programs*, Proc. 18th IEEE Symp. Found. of Comput. Sci. (Providence, R. I.) (1977), 46–57.

[24] M. O. Rabin, *Decidability of second-order theories and automata on infinite trees*, Trans. Amer. Math. Soc. 141 (1969), 1–35.

[25] F. Rancke, *Zählerfreie ω-Automaten*, Diplomarbeit, RWTH, Aachen 1985.

[26] M. P. Schützenberger, *On monoids having only trivial subgroups*, Inf. Contr. 8 (1965), 190–194.

[27] A. P. Sistla, *On characterization of safety and livieness properties*, Proc. 4th ACM Symp. on Principles of Distributed Computing (1985), 39–48.

[28] –, E. M. Clarke, N. Francez, A. R. Meyer, *Can message buffers be axiomatized in linear temporal logic?*, Inf. Contr. 63 (1984), 88–112.

[29] W. Thomas, *Star-free regular sets of ω-sequences*, ibidem 42 (1979), 148–156.

[30] –, *A combinatorial approach to the theory of ω-automata*, ibidem 48 (1981), 261–283.

[31] K. Wagner, *On ω-regular sets*, ibidem 43 (1979), 123–177.

[32] P. Wolper, *Temporal logic can be more expressive*, ibidem 56 (1983), 72–99.

[33] –, M. Y. Vardi, A. P. Sistla, *Reasoning about infinite computation paths*, Proc. 24th IEEE Symp. on Found. of Comput. Sci. (1983), 185–194.

Presented to the semester
Mathematical Problems in Computation Theory
September 16–December 14, 1985