Basic Research in Computer Science

Temporal Logic with Cyclic Counting and the Degree of Aperiodicity of Finite Automata

Zoltán Ésik
Masami Ito

BRICS Report Series **RS-01-53**

ISSN 0909-0878 **December 2001**

See back inner page for a list of recent BRICS Report Series publications.
Copies may be obtained by contacting:

BRICS
Department of Computer Science
University of Aarhus
Ny Munkegade, building 540
DK–8000 Aarhus C
Denmark
Telephone: +45 8942 3360
Telefax: +45 8942 3255
Internet: BRICS@brics.dk

BRICS publications are in general accessible through the World Wide Web and anonymous FTP through these URLs:

`http://www.brics.dk`
`ftp://ftp.brics.dk`
This document in subdirectory `RS/01/53/`

Temporal Logic with Cyclic Counting and the Degree of Aperiodicity of Finite Automata

Z. Ésik*
Dept. of Computer Science
University of Szeged
Szeged, Hungary
esik@inf.u-szeged.hu

M. Ito†
Dept. of Mathematics
Kyoto Sangyo University
Kyoto, Japan
ito@ksuvx0.kyoto-su.ac.jp

December, 2001

Abstract

We define the degree of aperiodicity of finite automata and show that for every set M of positive integers, the class $\mathbf{QA}_M$ of finite automata whose degree of aperiodicity belongs to the division ideal generated by M is closed with respect to direct products, disjoint unions, subautomata, homomorphic images and renamings. These closure conditions define q-varieties of finite automata. We show that q-varieties are in a one-to-one correspondence with literal varieties of regular languages. We also characterize $\mathbf{QA}_M$ as the cascade product of a variety of counters with the variety of aperiodic (or counter-free) automata. We then use the notion of degree of aperiodicity to characterize the expressive power of first-order logic and temporal logic with cyclic counting with respect to any given set M of moduli. It follows that when M is finite, then it is decidable whether a regular language is definable in first-order or temporal logic with cyclic counting with respect to moduli in M.

*The results of this paper were obtained during the first author's visit at the Faculty of Science at the Kyoto Sangyo University and at the Department of Computer Science at the University of Aalborg. The first author was partially supported by Grant-in-Aid 10044098, Japan Society for the Promotion of Science, by BRICS (Basic Research in Computer Science), and by grant no. T30511 from the National Foundation of Hungary for Scientific Research.

†Partially supported by Grant-in-Aid 10044098, Japan Society for the Promotion of Science.

1 Introduction

The richness of the theory of regular languages is due to the many different characterizations of (subclasses of) regular languages. By the theorem of Büchi and Elgot, a language is regular iff it is definable in monadic second-order logic over words [2, 5] involving the predicate $<$ and a predicate corresponding to each letter of the alphabet. Moreover, by classic results of Schützenberger [13] and Mc Naughton and Papert [10], a language is star-free iff it is definable in first-order logic iff it is accepted by an aperiodic (or counter-free) finite automaton. Thus, it is decidable for a regular language whether or not it is definable in first-order logic, or has a star-free expression. Moreover, by a classic result of Kamp [9] and Gabbay et al. [7], the logic **LTL** of Linear (Propositional) Temporal Logic over words has the same expressive power as first-order logic.

The above results have been extended in several directions involving, in addition to words, also ω-words, trees and other structures, see [17, 18] for overviews. In order to increase the expressive power of first-order logic on words, two kinds of cyclic counting have been studied: the extension of first-order logic with numerical predicates $C^r_m(x)$ that holds for a position x in a word iff x is congruent to r modulo m, see [1, 15], and the extension with modular quantifiers, cf. [16, 15]. In this paper our concern is the first type of counting. In [1], Barrington, Compton, Straubing and Therien gave a decidable characterization of the languages definable in first-order logic with counting with respect to the predicates $C^r_m(x)$, where the modulus m ranges over all positive integers and r is any nonnegative integer $< m$. However, this characterization does not answer the question that, given a finite set M of moduli, what languages are definable by using only predicates involving moduli in M. Our aim in this paper is to provide an analysis of the above mentioned result of Barrington, Compton, Straubing and Therien that will allow to answer the previous question. Moreover, we also study an extension of temporal logic yielding the same expressive power.

We define the degree of aperiodicity of finite automata and show that for every set M of positive integers, the class $\mathbf{QA}_M$ of automata whose degree of aperiodicity belongs to the division ideal generated by M is closed with respect to direct products, disjoint unions, subautomata, homomorphic images and renamings. These closure conditions define q-varieties. We show that q-varieties are in a one-to-one correspondence with literal varieties of regular languages. We also characterize $\mathbf{QA}_M$ as the cascade product of a variety of counters with the variety of aperiodic (or counter-free) automata. We then use the notion of degree of aperiodicity to characterize the expressive power of first-order logic and temporal logic with cyclic counting with respect to any given set M of moduli. When M is finite, this characterization is effective.

The paper is organized as follows. In Section 2 we define literal varieties of regular languages, q-varieties of finite automata, and establish an Eilenberg-type correspondence between them. In Section 3, we recall the notion of cascade

product of finite automata together with a few basic facts regarding regular languages accepted by cascade products. We also define cascade products $\mathbf{V} \star \mathbf{W}$ of q-varieties. Then, in Section 4, we study q-varieties of finite automata of the form $\mathbf{C}_M \star \mathbf{V}$, where M is a given subset of the positive integers and $\mathbf{C}_M$ is the q-variety generated by all counters whose length belongs to M. Then, in Section 5, we define the degree of aperiodicity of finite automata and show that for every set M as above, the finite automata whose degree of aperiodicity belongs to the division ideal generated by M form a q-variety $\mathbf{QA}_M$ which is the cascade product of $\mathbf{C}_M$ with the q-variety of aperiodic (counter-free) automata. Moreover, we show that the degree of aperiodicity of a finite automaton is computable. We also show that a language can be recognized by an automaton in $\mathbf{QA}_M$ iff it can be constructed from the finite languages and the languages consisting of all words over the underlying alphabet whose length is a multiple of some integer in M by the boolean operations and concatenation. Then, in Section 6 we prove that the very same condition characterizes the languages definable in first-order logic with cyclic counting with respect to moduli in M. When M is empty or M is the set of all positive integers, these results correspond to those of Schützenberger [13], Mc Naughton and Papert [10], and Barrington et al. [1] mentioned above. In Section 7, we provide several extensions of propositional temporal logic with cyclic counting and show that all these are equivalent. Moreover, we show that temporal logic with cyclic counting with respect to any given set M of moduli has the same expressive power as first-order logic with counting with respect to moduli in M. When M is empty, this fact corresponds to the result of Kamp [9] and Gabbay et al. [7]. Section 8 contains a summary of the results obtained and outlines some future results.

2 An Eilenberg correspondence

A *finite alphabet*, or just alphabet, for short, is any finite nonempty set whose elements are called *letters*. When Σ is an alphabet, we let Σ^* denote the free monoid of *words* over Σ including the *empty word* ϵ equipped with the operation of *concatenation* as product. For any word $u = a_0 \dots a_{n-1}$, where the a_i are letters, we call the integer n the length of u and denote it by $|u|$. We let Σ^n denote the set of all words in Σ^* of length n. The *prefix order* $\leq$ on words is defined by $u \leq v$ iff there is a word z with $uz = v$, i.e., when u is a prefix of v. Suppose that h is a (monoid) homomorphism $\Sigma^* \to \Delta^*$, where Σ, Δ are finite alphabets. We call h *nonerasing* if $ah \neq \epsilon$ holds for all $a \in \Sigma$. Moreover, we call h a *literal homomorphism* if $ah \in \Delta$ holds for all $a \in \Sigma$.

A *language* (over Σ) is any subset of Σ^*. Languages over Σ are equipped with several operations including the boolean operations $\cup$, $\cap$ and ^{c} (complement), product (or concatenation), Kleene star (*), left and right quotients, homomorphisms, inverse homomorphisms, etc. These are defined in the standard way. When $L \subseteq \Sigma^*$ and $u \in \Sigma^*$, we let $u^{-1}L$ and Lu^{-1} denote the left and right

quotients of L with respect to u, respectively:

$$\begin{aligned} u^{-1}L &= \{v \in \Sigma^* : uv \in L\} \\ Lu^{-1} &= \{v \in \Sigma^* : vu \in L\}. \end{aligned}$$

We will sometimes identify a word w with the singleton set $\{w\}$ and write w^* for the Kleene star $\{w\}^*$ of the language $\{w\}$.

Recall that a language $L \subseteq \Sigma^*$ is called *regular* if it can be constructed from the finite subsets of Σ^* by the regular operations of union, product and Kleene star. It is well-known that the class of regular languages is closed with respect to all of the operations mentioned above. Moreover, by Kleene's classic theorem, the regular languages are exactly those languages that can be recognized by finite automata.

In this paper, by a *finite automaton*, or just automaton, we mean a system $Q = (Q, \Sigma, \cdot)$ consisting of a finite nonempty set Q of *states*, a finite *input alphabet* Σ and a right *action* of Σ on Q, i.e., a function $\cdot : Q \times \Sigma \to Q$, which is extended to an action of Σ^* on Q in the usual way. Below we will usually write just qu for $q \cdot u$, for all $q \in Q$ and $u \in \Sigma^*$. The function $q \mapsto qu$ is called the *function induced by* u, denoted u^Q. When we want to emphasize that the input alphabet of an automaton is some alphabet Σ, we call it a Σ-*automaton*. Suppose that $L \subseteq \Sigma^*$ and that $Q = (Q, \Sigma, \cdot)$ is a Σ-automaton. We say that L *is recognizable in* Q, or that L *can be recognized by* Q, if there is a state $q_0 \in Q$, the *initial state*, and a set $F \subseteq Q$ of *final states* such that $L = \{u \in \Sigma^* : q_0 u \in F\}$. Moreover, a language is called *recognizable* if it can be recognized by some finite automaton. The aforementioned theorem of Kleene equates the recognizable languages with the regular languages.

Recall [4, 11] that a *stream (or class)* $\mathcal{V}$ *of regular languages* is a nonempty collection $\Sigma^*\mathcal{V}$ of regular languages over Σ, for each finite alphabet Σ. Streams of regular languages are ordered by set inclusion: we write $\mathcal{V} \subseteq \mathcal{V}'$ if $\Sigma^*\mathcal{V} \subseteq \Sigma^*\mathcal{V}'$, for all finite alphabets Σ.

Definition 2.1 *A* literal variety (of languages)*, or l-variety, for short, is a stream* $\mathcal{V}$ *of regular languages closed with respect to the boolean operations, left and right quotients and inverse literal homomorphisms. Thus, if* $L_1, L_2 \in \Sigma^*\mathcal{V}$ *and* $a \in \Sigma$*, then* $L_1 \cup L_2$*,* $L_1 \cap L_2$*,* L_1^c*,* $a^{-1}L_1$ *and* $L_1 a^{-1}$ *are all in* $\Sigma^*\mathcal{V}$*. Moreover, if* h *is a literal homomorphism* $\Delta^* \to \Sigma^*$*, so that* $\Delta h \subseteq \Sigma$*, then* $L_1 h^{-1} \in \Delta^*\mathcal{V}$*.*

A $*$-variety ($+$-variety) of languages *is a literal variety which is closed with respect to all (nonerasing) inverse homomorphisms.*

Example 2.2 It is clear that l-varieties form a complete lattice, in fact, an algebraic lattice. The largest l-variety contains, for each Σ, all the regular languages in Σ^*, and the smallest only the empty language and the language

Σ^*. When $\{\mathcal{V}_i : i \in I\}$ is a directed set of l-varieties, the least upper bound $\mathcal{V} = \bigvee_{i\in I} \mathcal{V}_i$ is just the union $\bigcup_{i\in I} \mathcal{V}_i$, so that $\Sigma^*\mathcal{V} = \bigcup_{i\in I} \Sigma^*\mathcal{V}_i$, for each Σ.

EXAMPLE 2.3 Of course, every $*$-variety or $+$-variety is a literal variety. For each Σ, let $\Sigma^*\mathcal{L}$ consist of all regular languages L in Σ^* such that for all words $u, v \in \Sigma^*$, if $u \in L$ and $|u| = |v|$, then $v \in L$. Then $\mathcal{L}$ is a literal variety which is not a $+$-variety or a $*$-variety.

The l-varieties contained in $\mathcal{L}$ correspond to those boolean algebras of regular languages over the one-letter alphabet closed with respect to quotients. We give some examples of such varieties.

Suppose that $d \geq 1$ is an integer. The l-variety $\mathcal{C}_d$ is that generated by the one-letter regular language $(a^d)^*$, considered as a subset of a^*. It is not hard to see that each language in $\Sigma^*\mathcal{C}_d$ is a finite union of languages of the form $(\Sigma^d)^*\Sigma^i$, where i is an integer in $[d] = \{0, 1, \ldots, d-1\}$.

Suppose that M is a subset of the set Nat of positive integers. Then let $\mathcal{C}_M$ denote the smallest l-variety containing all of the $\mathcal{C}_m$ with $m \in M$. It is clear that $\mathcal{C}_M$ is the union of those $\mathcal{C}_d$ where d is contained in the *division ideal* $(M]$ generated by M. (Of course, $(M]$ consists of all divisors of least common multiples of finite families of elements of M.) Thus, $\mathcal{C}_M \subseteq \mathcal{C}_{M'}$ iff $(M] \subseteq (M']$. We write $\mathcal{C}$ for $\mathcal{C}_{\mathsf{Nat}}$.

Further examples of literal varieties that are not $*$-varieties or $+$-varieties will be given later.

REMARK 2.4 *The $*$-varieties defined above are the same as the $*$-varieties of Eilenberg [4], see also [11]. However, Eilenberg's $+$-varieties [4] are streams of regular languages containing only* nonempty *words closed with respect to the boolean operations, left and right quotients, and nonerasing inverse homomorphisms. If $\mathcal{V}$ is a $+$-variety as defined in Definition 2.1, and if $\Sigma^+\mathcal{W} = \Sigma^*\mathcal{V} \cap \Sigma^+$, for each Σ, where Σ^+ denotes the free semigroup of all nonempty words over Σ, then $\mathcal{W}$ is an Eilenberg $+$-variety. This mapping $\mathcal{V} \mapsto \mathcal{W}$ is surjective but not injective.*

Suppose that $\mathcal{W}$ is an Eilenberg $+$-variety. For each alphabet Σ, define

$$\Sigma^*\mathcal{V} \quad = \quad \{L, L \cup \epsilon : L \in \Sigma^+\mathcal{W}\}.$$

Then $\mathcal{V}$ is a $+$-variety, as defined in Definition 2.1, which is mapped to $\mathcal{W}$. If for some Σ, there is a finite nonempty set in $\Sigma^+\mathcal{W}$, then this is in fact the unique $+$-variety mapped to $\mathcal{W}$. However, if $\Sigma^*\mathcal{V} = \{\emptyset, \Sigma^*\}$ and $\Sigma^*\mathcal{V}' = \{\emptyset, \epsilon, \Sigma^+, \Sigma^*\}$, for each alphabet Σ, then the same Eilenberg $+$-variety $\mathcal{W}$ corresponds to both $\mathcal{V}$ and $\mathcal{V}'$:

$$\Sigma^+\mathcal{W} \quad = \quad \{\emptyset, \Sigma^+\},$$

for each Σ.

A *stream (or class)* $\mathbf{V}$ *of finite automata* is a nonempty collection $\Sigma\mathbf{V}$ of finite Σ-automata, for each finite alphabet Σ. Streams of finite automata are ordered by set inclusion in the same way as streams of regular languages.

The notions of *subautomaton* and *quotient* (or *homomorphic image*) of an automaton are defined as usual. When $Q = (Q, \Sigma, \cdot)$ and $Q' = (Q', \Sigma, \cdot)$ are automata with the same set of input letters, the *direct product* $Q \times Q' = (Q \times Q', \Sigma, \cdot)$ is equipped with the pointwise action, so that $(q, q') \cdot a = (qa, q'a)$, for all $q \in Q$, $q' \in Q'$ and $a \in \Sigma$. The *disjoint sum* (or *disjoint union*) of Q and Q' is also defined in the standard way. It is the automaton $Q \oplus Q' = (Q \times \{0\} \cup Q \times \{1\}, \Sigma, \cdot)$, where $(q, 0)a = (qa, 0)$ and $(q', 1)a = (q'a, 1)$, for all $q \in Q$ and $q' \in Q'$. Suppose now that $Q = (Q, \Sigma, \cdot)$ and $Q' = (Q', \Delta, \cdot)$, where Σ and Δ are any alphabets. We say that Q can be constructed from Q' by *renaming*, or that Q is a renaming of Q', if $Q = Q'$ and there is a function $h : \Sigma \to \Delta$ such that $qa = q(ah)$, for all $q \in Q$ and $a \in \Sigma$.

DEFINITION 2.5 *A* q-variety of finite automata *is any stream of finite automata closed with respect to the operations of taking subautomata, quotients, direct products, disjoint sums and renamings.*

We use the prefix to distinguish q-varieties from varieties (or pseudo-varieties) that are nonempty classes of automata with the same input alphabet closed with respect to the operations of taking subautomata, quotients, and direct products, and to express that q-varieties are also closed with respect to the *quasi-direct product* [8].

Since a q-variety $\mathbf{V}$ is nonempty and closed with respect to subautomata, quotients, direct product and renaming, closure under disjoint sum is clearly equivalent to the requirement that the two-element *discrete automaton* with a single input letter belongs to $\mathbf{V}$. (A Σ-automaton is called discrete if it is a disjoint sum of trivial, i.e., one-state Σ-automata.)

A $*$*-variety (+-variety) of finite automata* is a q-variety that is also closed with respect to the operation $Q \mapsto Q^*$ ($Q \mapsto Q^+$). Here, the operation $Q \mapsto Q^*$ is defined as follows. Let $Q = (Q, \Sigma, \cdot)$, say, and let $M(Q)$ denote the *monoid of* Q. Thus, the elements of $M(Q)$ are the functions $u^Q : Q \to Q$ induced by the words $u \in \Sigma^*$, and the product operation in $M(Q)$ is function composition written left-to-right. Now Q^* is $(Q, M(Q), \cdot)$, where for each $q \in Q$ and $u \in \Sigma^*$, $q \cdot u^Q$ is just $qu = q \cdot u$, the image of q under u^Q. The automaton Q^+ is defined in the same way except that its alphabet is $S(Q) = \{u^Q : u \in \Sigma^+\}$, the *semigroup of* Q.

REMARK 2.6 *It is clear that* $*$*-varieties of finite automata correspond in a bijective manner to varieties of finite monoids as defined in [4, 11]. Given a* $*$*-variety* $\mathbf{V}$ *of finite automata, the corresponding variety of finite monoids consists of all monoids that are isomorphic to the monoid of some automaton in* $\mathbf{V}$.

However, a similar function mapping +-varieties of finite automata to varieties of finite monoids is only surjective, but not injective. See also Remark 2.4.

EXAMPLE 2.7 The set of all q-varieties equipped with set inclusion is an algebraic lattice. The largest q-variety contains, for each Σ, all Σ-automata, and the smallest one only the discrete Σ-automata. When $\{\mathbf{V}_i : i \in I\}$ is a directed set of q-varieties, the least upper bound $\bigvee_{i\in I} \mathbf{V}_i$ is just the union $\bigcup_{i\in I} \mathbf{V}_i$.

EXAMPLE 2.8 For each Σ, the q-variety $\mathbf{L}$ consists of all *autonomous* Σ-automata, i.e., all the automata $Q = (Q, \Sigma, \cdot)$ such that $qa = qb$, for all $q \in Q$ and $a, b \in \Sigma$.

Given an integer $d \geq 1$, the q-variety $\mathbf{C}_d$ has, as its members in $\Sigma\mathbf{C}_d$, all the Σ-automata that are disjoint sums of Σ-*counters* of length a divisor of d. A Σ-counter is an automaton $(Q, \Sigma, \cdot)$ such that each letter in Σ induces the *same* cyclic permutation $Q \to Q$. The length of the counter is $|Q|$, the number of states in Q. Note that $\mathbf{C}_d$ is contained in $\mathbf{L}$.

When M is a set of positive integers, then we define $\mathbf{C}_M = \bigvee_{m\in M} \mathbf{C}_m$, so that $\mathbf{C}_M$ is the least q-variety containing all of the $\mathbf{C}_m$ with $m \in M$. Note that $\mathbf{C}_M$ is just the union of the $\mathbf{C}_d$ with d any integer in $(M]$. Thus, $\mathbf{C}_M \subseteq \mathbf{C}_{M'}$ iff $(M] \subseteq (M']$. We denote $\mathbf{C}_{\mathsf{Nat}}$ by $\mathbf{C}$.

Suppose that $\mathbf{V}$ is a q-variety. The corresponding stream $\mathcal{V}$ of regular languages contains those languages in $\Sigma^*\mathcal{V}$ that can be recognized by an automaton in $\Sigma\mathbf{V}$ (by a suitable initial state and a set of final states). Thus, a language $L \subseteq \Sigma^*$ belongs to $\Sigma^*\mathcal{V}$ if and only if there is an automaton $Q = (Q, \Sigma, \cdot)$ in $\mathbf{V}$, a state $q_0 \in Q$ and a set $F \subseteq Q$ such that the language recognized by Q with initial state q_0 and final states F is L. Alternatively, a (regular) language $L \subseteq \Sigma^*$ belongs to $\Sigma^*\mathcal{V}$ if and only if the *minimal* automaton recognizing L is in $\Sigma\mathbf{V}$.

The following variant of Eilenberg's variety theorem [4, 11] follows by standard arguments.

THEOREM 2.9 *The correspondence $\mathbf{V} \mapsto \mathcal{V}$ is an order isomorphism from the lattice of q-varieties of finite automata onto the lattice of l-varieties of regular languages. The same correspondence establishes an order isomorphism between $*$-varieties ($+$-varieties) of finite automata and $*$-varieties ($+$-varieties) of regular languages.*

Proof. We briefly sketch the proof of the first statement. If L is in $\Sigma^*\mathcal{V}$, then L is accepted by an automaton in $\mathbf{V}$ by a suitable initial state and a set of final states. By taking the same initial state and the complement of the set of final states, the same automaton accepts L^c. It is also known that any quotient of L can be accepted by the same automaton with suitable initial and final states. Closure with respect to set union follows from the fact that the union

of languages accepted by Q_1 and Q_2 can be accepted by the direct product of Q_1 and Q_2. It is clear that $\mathbf{V}_1 \subseteq \mathbf{V}_2$ implies $\mathcal{V}_1 \subseteq \mathcal{V}_2$. Suppose now that $\mathcal{V}_1 \subseteq \mathcal{V}_2$. Assume that $Q = (Q, \Sigma, \cdot) \in \mathbf{V}_1$ is generated by a single state q_0, so that each state $q \in Q$ is of the form $q_0 u$, for some $u \in \Sigma^*$. For each state $q \in Q$, let L_q denote the language accepted by Q with initial state q_0 and single final state q. Since $L_q \in \mathcal{V}_1$ and $\mathcal{V}_1 \subseteq \mathcal{V}_2$, there exists an automaton $Q_q \in \mathbf{V}_2$ accepting L_q with some initial state i_q and some set of final states F_q. Now the direct product of the Q_q contains a subautomaton that can be mapped homomorphically onto Q: take those tuples of the direct product accessible by a word from that tuple whose components are the respective initial states i_q. It follows that each state $s = (s_q)_{q \in Q}$ has a unique component s_q with $s_q \in F_q$, and that the map taking s to this component s_q is a homomorphism onto Q. Since $\mathbf{V}_2$ is closed with respect to direct product, subautomata and homomorphic images, it follows that Q is in $\mathbf{V}_2$. If $Q \in \mathcal{V}_1$ is not generated by a single state, then Q is a quotient of the disjoint sum of its (maximal) one-generated subautomata. Since q-varieties are closed with respect to disjoint sum, it follows by the above argument that $Q \in \mathbf{V}_2$. Finally, the fact that the assignment $\mathbf{V} \mapsto \mathcal{V}$ is surjective can be seen as follows. Given an l-variety $\mathcal{V}$, consider the stream $\mathbf{V}$ of automata that only accept languages in $\mathcal{V}$, so that $Q = (Q, \Sigma, \cdot) \in \mathbf{V}$ iff for each $q_0 \in Q$ and $F \subseteq Q$ it holds that the language accepted by Q with initial state q_0 and set of final states F is in $\mathcal{V}$. Then $\mathbf{V}$ is a q-variety mapped to $\mathcal{V}$. Indeed, the closure properties of $\mathcal{V}$ guarantee that $\mathbf{V}$ is a q-variety. Moreover, every language $L \in \Sigma^*\mathcal{V}$ can be accepted by an automaton in $\mathbf{V}$, namely the minimal automaton Q_L corresponding to L, since any language accepted by this automaton is a boolean combination of quotients of L. ■

EXAMPLE 2.10 The l-variety corresponding to $\mathbf{L}$ is the variety $\mathcal{L}$ defined in Example 2.3. For each M, the l-variety corresponding to $\mathbf{C}_M$ is $\mathcal{C}_M$.

EXAMPLE 2.11 We call a finite automaton $Q = (Q, \Sigma, \cdot)$ *nilpotent* if there is an integer n such that $qu = qv$ holds for all words $u, v \in \Sigma^*$ of length $\geq n$. (Note that the usual definition of nilpotent automata [8] requires that $qu = q'v$ hold for all states q, q' and words $u, v \in \Sigma^*$ of length at least n.) Nilpotent automata form a $+$-variety denoted $\mathbf{N}$. The corresponding $+$-variety $\mathcal{N}$ of languages contains in $\Sigma^*\mathcal{N}$, for each alphabet Σ, all finite and cofinite languages in Σ^*.

EXAMPLE 2.12 A finite automaton $Q = (Q, \Sigma, \cdot)$ is called *definite* if there exits some $n \geq 0$ such that for all $q \in Q$ and $u, v \in \Sigma^*$, if the suffixes of u and v of length at most n agree, then $qu = qv$. (Again, the usual definition of definite automata [8] requires more.) For example, any *shift register* $(\Sigma^n, \Sigma, \cdot)$ with $u \cdot a$ being the length n suffix of ua, for each $u \in \Sigma^n$ and $a \in A$, is definite.

Definite automata form a $+$-variety $\mathbf{D}$ with corresponding $+$-variety of languages denoted $\mathcal{D}$. We call $\mathcal{D}$ the $+$-variety of definite languages. For each Σ and

$L \subseteq \Sigma^*$, we have $L \in \Sigma^*$ iff there is an integer $n \geq 0$ such that for all words $u, v \in \Sigma^*$ such that u and v have the same suffixes of length at most n, it holds that $u \in L$ iff $v \in L$. (See [4].)

EXAMPLE 2.13 A finite automaton Q is called *aperiodic*, or *counter-free* [4], if $M(Q)$ (or $S(Q)$) contains only trivial subgroups. Aperiodic automata form a $*$-variety $\mathbf{A}$ with corresponding language variety $\mathcal{A}$. We have that $\mathbf{N} \subset \mathbf{D} \subset \mathbf{A}$ and $\mathcal{N} \subset \mathcal{D} \subset \mathcal{A}$.

3 Cascade product

We call a function $\tau : \Sigma^* \to \Delta^*$ *sequential* if τ preserves prefixes, i.e., for all words u and v in Σ^*, if $u \leq v$ in the prefix order then $\tau(u) \leq \tau(v)$. It then follows that for each word $u \in \Sigma^*$ there is a (unique) function, in fact a sequential function $\tau_u : \Sigma^* \to \Delta^*$ with $\tau(uv) = \tau(u)\tau_u(v)$. If in addition τ preserves the length of the words, then we call τ a *literal sequential function*.

Sequential functions are known to be the functions inducible by sequential transducers, and literal sequential functions by Mealy automata [8], which are a restricted type of transducers. The (literal) sequential functions $\tau : \Sigma^* \to \Delta^*$ that can be induced by finite transducers obey the condition that the functions τ_u, $u \in \Sigma^*$ form a finite set. Such (literal) sequential functions are said to be of *finite state*. Note that any (literal) homomorphism is a finite state (literal) sequential function.

Suppose that $Q = (Q, \Sigma, \cdot)$ is a finite automaton. A *Mealy automaton* [8] over Q is the extension of Q by an output alphabet Δ and an output function $\mu : Q \times \Sigma \to \Delta$. We let $Q(\Delta, \mu)$ denote this extension. Clearly, each state $q \in Q$ may be used to induce a finite state literal sequential function $\mu_q : \Sigma^* \to \Delta^*$ defined by $\mu_q(\epsilon) = \epsilon$ and $\mu_q(ua) = \mu_q(u)\mu(qu, a)$. We use Mealy automata extensions to define *cascade products*.

Suppose that $Q = (Q, \Sigma, \cdot)$ and $R = (R, \Delta, \cdot)$ are finite automata and suppose that we are given a Mealy automaton extension $Q(\Delta, \mu)$. Then the cascade product of Q with R determined by μ is defined to be the automaton $Q \times_\mu R = (Q \times R, \Sigma, \cdot)$, where $(q, r) \cdot a = (qa, r\mu(q, a)) = (qa, r\mu_q(a))$, for all $q \in Q$ and $r \in R$. Note that it follows by induction that $(q, r) \cdot u = (qu, r\mu_q(u))$, for all $u \in \Sigma^*$.

The semigroup theoretic concepts corresponding to the cascade product are the *semi-direct product* and the *wreath product*, cf. [4, 11]. The following fundamental fact is an adaptation of Straubing's "wreath product principle" [3] to the cascade product.

PROPOSITION 3.1 *A language is recognized by a cascade product $Q \times_\mu R$ with*

initial state (q_0, r_0) *iff it is a finite union of languages of the form* $K \cap \mu_{q_0}^{-1}(L)$, *where* K *is a language recognized by* Q *with initial state* q_0 *and* L *is a language recognized by* R *with initial state* r_0.

The cascade product may be extended to q-varieties.

DEFINITION 3.2 *Suppose that* $\mathbf{V}$ *and* $\mathbf{W}$ *are q-varieties. The q-variety* $\mathbf{V} \star \mathbf{W}$ *is that generated by all cascade products* $Q \times_\mu R$ *with* Q *an automaton in* $\Sigma\mathbf{V}$, R *an automaton in* $\Delta\mathbf{W}$, *and* $Q(\Delta, \mu)$ *a Mealy automaton extension of* Q.

It is immediate to prove that when both $\mathbf{V}$ and $\mathbf{W}$ are $+$-varieties ($*$-varieties, respectively), then so is $\mathbf{V} \star \mathbf{W}$.

The l-variety corresponding to $\mathbf{V} \star \mathbf{W}$ has the following description. The result is an adaptation of a similar characterization of languages recognizable by semigroups in the wreath product of two semigroup varieties, see [11].

THEOREM 3.3 *Suppose that* $\mathbf{V}$ *and* $\mathbf{W}$ *are q-varieties with corresponding l-varieties* $\mathcal{V}$ *and* $\mathcal{W}$. *Then for each* Σ, *the l-variety* $\mathcal{V} \star \mathcal{W}$ *corresponding to* $\mathbf{V} \star \mathbf{W}$ *contains exactly those languages in* Σ^* *that are finite unions of languages of the form* $K \cap \mu^{-1}(L)$, *where* $K \in \Sigma^*\mathcal{V}$, $L \in \Delta^*\mathcal{W}$ *and where* $\mu : \Sigma^* \to \Delta^*$ *is a sequential function induced by some state of a Mealy automaton extension of an automaton in* $\mathbf{V}$.

We may as well require that the same finite state literal sequential function μ appears in all terms of the finite union. Theorem 3.3 relies on on Proposition 3.1 and the following fact.

THEOREM 3.4 *For any q-varieties* $\mathbf{V}$ *and* $\mathbf{W}$ *and any* Σ, *an automaton* Q *is in* $\Sigma(\mathbf{V} \star \mathbf{W})$ *iff* Q *is a quotient of a subautomaton of a cascade product* $R \times_\mu S$, *where* $R \in \Sigma\mathbf{V}$ *and* $S \in \Delta\mathbf{W}$ *such that and* $R(\Delta, \mu)$ *is a Mealy automaton extension of* R.

Proof. Let $\mathbf{K}$ denote the stream determined by those automata Q that can be constructed as quotients of subautomata of cascade products of automata $R \in \mathbf{V}$ and $S \in \mathbf{W}$. It is clear that $\mathbf{K} \subseteq \mathbf{V} \star \mathbf{W}$. Also, $\mathbf{K}$ is easily shown to be closed with respect to subautomata, quotients, direct products and renaming. Moreover, $\mathbf{K}$ clearly contains all discrete automata. Hence, $\mathbf{K}$ is closed with respect to disjoint sum. It follows that $\mathbf{V} \star \mathbf{W} \subseteq \mathbf{K}$. ■

We say that a q-variety $\mathbf{V}$ is *closed with respect to the cascade product* if for any cascade product $Q \times_\mu R$ with $Q, R \in \mathbf{V}$, it holds that $Q \times_\mu R \in \mathbf{V}$. For example, $\mathbf{N}, \mathbf{D}, \mathbf{A}$ are all closed with respect to the cascade product, cf. [4]. Moreover, for any set M of positive integers, $\mathbf{C}_M$ is closed with respect to the cascade product, as is *any* q-variety of autonomous automata.

We omit the straightforward proofs of the following facts.

PROPOSITION 3.5 *Any q-variety contained in* $\mathbf{L}$ *is closed with respect to the cascade product. If* $\mathbf{V}$ *and* $\mathbf{W}$ *are q-varieties such that* $\mathbf{V}$ *is contained in* $\mathbf{L}$ *and* $\mathbf{W}$ *is closed with respect to the cascade product, then* $\mathbf{V} \star \mathbf{W}$ *is also closed with respect to the cascade product.*

PROPOSITION 3.6 *Suppose that* $\{\mathbf{V}_i : i \in I\}$ *is a directed set of q-varieties and* $\mathbf{V} = \bigcup_{i \in I} \mathbf{V}_i$*. Then for any q-variety* $\mathbf{W}$*, we have* $\mathbf{V} \star \mathbf{W} = \bigcup_{i \in I} \mathbf{V}_i \star \mathbf{W}$*. Suppose that* $\mathcal{V}_i$ *denotes the l-variety corresponding to* $\mathbf{V}_i$*, for each* $i \in I$*, and suppose that* $\mathcal{V}$ *denotes the l-variety corresponding to* $\mathbf{V}$*. Then for any l-variety* $\mathcal{W}$*, it holds that* $\mathcal{V} \star \mathcal{W} = \bigcup_{i \in I} (\mathcal{V}_i \star \mathcal{W})$*.*

Thus, the $\star$ operation is continuous in its first argument. In a similar way, it is continuous in its second argument.

As an immediate application of Proposition 3.6 we have that

$$\mathbf{C}_M \star \mathbf{V} \quad = \quad \bigcup_{d \in (M]} \mathbf{C}_d \star \mathbf{V}$$

and

$$\mathcal{C}_M \star \mathcal{V} \quad = \quad \bigcup_{d \in (M]} \mathcal{C}_d \star \mathcal{V},$$

for all q-varieties $\mathbf{V}$ and l-varieties $\mathcal{V}$, and for all $M \subseteq \mathsf{Nat}$.

4 Varieties $\mathbf{C}_M \star \mathbf{V}$

In this section, we study q-varieties of the form $\mathbf{C}_d \star \mathbf{V}$ and $\mathbf{C}_M \star \mathbf{V}$, and the corresponding l-varieties $\mathcal{C}_d \star \mathcal{V}$ and $\mathcal{C}_M \star \mathcal{V}$.

DEFINITION 4.1 *For any automaton* $Q = (Q, \Sigma, \cdot)$ *and integer* $d > 0$*, let* $Q^{(d)}$ *denote the automaton* $(Q, \Sigma^{(d)}, \cdot)$*, where* $\Sigma^{(d)}$ *consists of all* letters $\langle u \rangle$*, where* u *is any word of length* d *in* Σ^**, i.e., any element of* Σ^d*, and where*

$$q \cdot \langle u \rangle \quad = \quad qu,$$

for all $q \in Q$ *and* $u \in \Sigma^d$*.*

Thus, $Q^{(d)}$ arises from Q by letting the words in Σ^* of length d be the input letters. For each $u \in \Sigma^d$, the function induced by $\langle u \rangle$ in $Q^{(d)}$ is the same as the function induced by u in the automaton Q. Besides $Q^{(d)}$, we will also use

the automaton $Q_1^{(d)}$, which is the extension of $Q^{(d)}$ by a letter a_0 inducing the identity function $Q \to Q$. Thus, $Q_1^{(d)} = (Q, \Sigma^{(d)} \cup \{a_0\}, \cdot)$, where $q \cdot a_0 = q$, for all $q \in Q$, and where for all $q \in Q$ and $u \in \Sigma^d$, $q \cdot \langle u \rangle$ is defined as above. Note that the monoids $M(Q^{(d)})$ and $M(Q_1^{(d)})$ are both isomorphic to the submonoid $M_d(Q)$ of the monoid $M(Q)$ of automaton Q consisting of all functions $Q \to Q$ induced by those words in Σ^* whose length is a multiple of d.

PROPOSITION 4.2 *Each automaton Q is a homomorphic image of a cascade product of an automaton which is a direct product of a counter of length d with a shift register, and the automaton $Q_1^{(d)}$.*

Proof. Suppose that $Q = (Q, \Sigma, \cdot)$, so that $Q_1^{(d)}$ is $(Q, \Sigma^{(d)} \cup \{a_0\}, \cdot)$ defined above.

Let C_d denote the counter of length d whose input alphabet is Σ and whose states are the integers in $[d]$, so that $i \cdot a = i + 1 \bmod d$, for all $i \in [d]$ and $a \in \Sigma$. Let D_{d-1} denote the shift register of length $d-1$ over Σ. Thus the states of D_{d-1} are the words in Σ^{d-1}, and the transition is defined so that for each $u \in \Sigma^{d-1}$ and $a \in \Sigma$, state $u \cdot a$ is the suffix of ua of length $d-1$. Define

$$\mu : ([d] \times \Sigma^{d-1}) \times \Sigma \quad \to \quad \Sigma^{(d)} \cup \{a_0\}$$

by

$$\mu((i,u),a) \quad = \quad \begin{cases} a_0 & \text{if } i \neq d-1 \\ \langle ua \rangle & \text{otherwise.} \end{cases}$$

We thus obtain the cascade product $Q' = (C_d \times D_{d-1}) \times_\mu Q_1^{(d)}$. We claim that there is a surjective homomorphism $h : Q' \to Q$. Indeed, for each state $((i,u),q)$ of Q', define

$$((i,u),q)h \quad = \quad qv,$$

where v denotes the suffix of u of length i. In particular, $((0,u),q)h = q$, for all $u \in \Sigma^{d-1}$ and $q \in Q$, so that h is surjective. We show that h is a homomorphism. Assume that $((i,u),q)$ is a state of Q' and $a \in \Sigma$. If $i \neq d-1$ then

$$\begin{aligned} ((i,u),q)ah &= ((i+1,u'a),q)h \\ &= qva \\ &= (((i,u),q)h)a, \end{aligned}$$

where v denotes the suffix of u of length i and u' the suffix of u of length $d-1$. When $i = d-1$, we have

$$\begin{aligned} ((d-1,u),q)ah &= ((0,u'a),qua)h \\ &= qua \\ &= (((d-1,u),q)h)a, \end{aligned}$$

where u' is the same as above. ■

REMARK 4.3 *The same argument proves the following stronger version of Proposition 4.2. Suppose that R is a subautomaton of $Q_1^{(d)}$ such that for each $q \in Q$ there exists a state $r \in R$ and a word $u \in \Sigma^*$ with $|u| < d$ such that $ru = q$ holds in Q. Then automaton Q is a homomorphic image of a cascade product of an automaton which is the direct product of a counter of length d with a shiftregister, and the automaton R. Indeed, if we replace $Q_1^{(d)}$ with R in the above proof, the same argument works. The assumption that each q be of the form ru with $r \in R$ and $|u| < d$ is needed to show that h is surjective.*

Recall that $\mathbf{D}$ denotes the $+$-variety of definite automata and that $\mathcal{D}$ denotes the corresponding $+$-variety of definite languages. Note that for any $*$-variety $\mathbf{V}$ of automata and for any automaton Q and $d \geq 1$, we have $Q^{(d)} \in \mathbf{V}$ iff $Q_1^{(d)} \in \mathbf{V}$.

COROLLARY 4.4 *Suppose that $\mathbf{V}$ is a q-variety such that $\mathbf{D} \star \mathbf{V} \subseteq \mathbf{V}$. Then for any integer $d \geq 1$ and automaton Q, if $Q_1^{(d)} \in \mathbf{V}$ then $Q \in \mathbf{C}_d \star \mathbf{V}$.*

We now want to prove a certain converse of the above result.

PROPOSITION 4.5 *Suppose that $\mathbf{V}$ is a $*$-variety of automata and $d \geq 1$. If $Q \in \mathbf{C}_d \star \mathbf{V}$, then $Q^{(d)}$, and thus $Q_1^{(d)}$, is in $\mathbf{V}$.*

Proof. First assume that Q is 1-generated, i.e., there exists a state q_0 in Q such that each state is accessible from q_0 by an input word. If $Q \in \mathbf{C}_d \star \mathbf{V}$ then, by Theorem 3.4, Q is a quotient of a subautomaton R' of a cascade product of an automaton C in $\mathbf{C}_d$ and an automaton R in $\mathbf{V}$. Since Q is 1-generated, without loss of generality we may assume that so is R'. But in that case C may be chosen to be 1-generated as well, so that C is a counter in $\mathbf{C}_d$ and is thus a quotient of a counter of length d. We conclude that Q is a homomorphic image, with respect to a homomorphism h, of a subautomaton $R' = (R', \Sigma, \cdot)$ of a cascade product $C_d \times_\mu R$, where $C_d = ([d], \Sigma, \cdot)$ is the counter of length d with $ia = i + 1 \bmod d$, for all $i \in [d]$ and $a \in \Sigma$, and $R = (R, \Delta, \cdot)$ is an automaton in $\mathbf{V}$. For each $i \in [d]$, let R_i denote the set of all states $r \in R$ such that $(i, r) \in R'$. It is clear that $R_i \neq \emptyset$. Moreover, let $h_i : R_i \to Q$ be defined by $r \mapsto h((i, r))$, for all $r \in R_i$. We turn each R_i into an automaton $R_i = (R_i, \Sigma^{(d)}, \cdot)$ with input letters in the set $\Sigma^{(d)}$. For each $r \in R_i$ and $u \in \Sigma^d$, let $r \cdot \langle u \rangle = r\mu_i(u)$, the image of r with respect to the word which is the image of u with respect to the sequential function induced by state i of the Mealy extension $C_d(\Delta, \mu)$. Since $\mathbf{V}$ is a $*$-variety and $R \in \mathbf{V}$, it follows that each R_i is in $\mathbf{V}$. Indeed, R_i can be constructed from R^* by renaming and taking subautomata. Also, each h_i is a homomorphism $R_i \to Q^{(d)}$, and since h is surjective, each state in Q appears as the image of some state in $\bigcup_{i \in [d]} R_i$. Thus, the disjoint sum of the R_i can be mapped homomorphically onto $Q^{(d)}$, proving that $Q^{(d)}$ is in $\mathbf{V}$ (since $\mathbf{V}$ is closed with respect to disjoint sum).

In the general case, Q is a quotient of the disjoint sum of its 1-generated subautomata $Q_1, \ldots, Q_n$. If $Q \in \mathbf{C}_d \star \mathbf{V}$ then each Q_i belongs to $\mathbf{C}_d \star \mathbf{V}$. Thus, by the above argument, we have $Q_i^{(d)} \in \mathbf{V}$, for each i. Since $\mathbf{V}$ is closed with respect to disjoint sum, it follows that the disjoint sum of the $Q_i^{(d)}$ is also in $\mathbf{V}$. But $Q^{(d)}$ is a quotient of this disjoint sum, so that $Q^{(d)} \in \mathbf{V}$. ■

Call a q-variety $\mathbf{V}$ *decidable* if there is an algorithm to decide for any given automaton Q whether or not Q belongs to $\mathbf{V}$. Similarly, call an l-variety $\mathcal{V}$ decidable if there is an algorithm to decide whether or not a regular language (given by an automaton or a regular expression) belongs to $\mathcal{V}$. From Corollary 4.4 and Proposition 4.5 we have:

THEOREM 4.6 *For any $*$-variety $\mathbf{V}$ of automata with $\mathbf{D} \star \mathbf{V} \subseteq \mathbf{V}$, and for any $d \geq 1$ and automaton Q, we have that $Q \in \mathbf{C}_d \star \mathbf{V}$ iff $Q^{(d)} \in \mathbf{V}$. Thus, if $\mathbf{V}$ is decidable, then so is $\mathbf{C}_d \star \mathbf{V}$.*

A first characterization of the languages in the variety $\mathcal{C}_d \star \mathcal{V}$, where $\mathcal{V}$ is any l-variety of languages, may be obtained from the wreath product principle. Let Σ denote an alphabet and consider the Σ-counter $C_d = ([d], \Sigma, \cdot)$ with $i \cdot a = i + 1 \bmod d$, for all $i \in [d]$ and $a \in \Sigma$. Consider the alphabet $[d] \times \Sigma$ and the identity function $\pi_d : [d] \times \Sigma \to [d] \times \Sigma$. Let σ_d denote the literal sequential function induced by the Mealy extension $C_d([d] \times \Sigma, \pi_d)$ in state 0. Then any literal sequential function $\sigma : \Sigma^* \to \Delta^*$ induced by a state of a Mealy extension of an automaton in $\mathbf{C}_d$ can be factorized as the composite of σ_d with a literal homomorphism $\tau : ([d] \times \Sigma)^* \to \Delta^*$. Thus, by the wreath product principle we get:

PROPOSITION 4.7 *A language $L \subseteq \Sigma^*$ belongs to $\mathcal{C}_d \star \mathcal{V}$ iff L can be written as*

$$L \quad = \quad \bigcup_{i \in [d]} (\Sigma^d)\Sigma^i \cap \sigma_d^{-1}(K_i),$$

for some languages $K_i \in ([d] \times \Sigma)^* \mathcal{V}$, $i \in [d]$.

When $\mathcal{V}$ corresponds to a $*$-variety $\mathbf{V}$ with $\mathbf{D} \star \mathbf{V} \subseteq \mathbf{V}$, we can use Theorem 4.6 to derive an alternative characterization of the languages in $\mathcal{C}_d \star \mathcal{V}$.

Suppose that $L \subseteq \Sigma^*$ and $d \geq 1$. We define

$$L^{(d)} \quad = \quad \{\langle u_0 \rangle \ldots \langle u_{k-1} \rangle : u_0 \ldots u_{k-1} \in L,\ u_i \in \Sigma^d,\ i \in [k]\},$$

so that $L^{(d)} \subseteq (\Sigma^{(d)})^*$. Moreover, for each $u \in \Sigma^*$ with $|u| < d$, we define $L^{(d,u)} = (Lu^{-1})^{(d)}$. Thus, $L^{(d)}$ and each $L^{(d,u)}$ is a language in $(\Sigma^{(d)})^*$, moreover, $L^{(d)} = L^{(d,\epsilon)}$.

THEOREM 4.8 *Suppose that* $\mathbf{V}$ *is a* $*$*-variety of automata with* $\mathbf{D} \star \mathbf{V} \subseteq \mathbf{V}$*, and suppose that* $\mathcal{V}$ *denotes the language variety corresponding to* $\mathbf{V}$*. Then for any integer* $d \geq 1$ *and language* $L \subseteq \Sigma^*$*, if* $L \in \mathcal{C}_d \star \mathcal{V}$ *then* $L^{(d,u)} \in \mathcal{V}$*, for all* $u \in \Sigma^*$ *with* $|u| < d$*. Moreover, if* $L^{(d,u)} \in \mathcal{V}$*, for all* $u \in \Sigma^*$ *with* $|u| < d$*, and if* $\mathcal{V}$ *is closed with respect to right (or left) concatenation with letters, then* $L \in \mathcal{C}_d \star \mathcal{V}$*.*

Proof. Suppose first that $L \subseteq \Sigma^*$ is in $\Sigma^*(\mathcal{C}_d \star \mathcal{V})$. Then L can be recognized by an automaton Q in $\mathbf{C}_d \star \mathbf{V}$. By Theorem 4.6 we have that $Q^{(d)} \in \mathbf{V}$. But each of the languages $L^{(d,u)}$, where $u \in \Sigma^*$ with $|u| < d$ can be recognized by $Q^{(d)}$. For if L is recognized by $Q = (Q, \Sigma, \cdot)$ with initial state q_0 and final states F, then $L^{(d,u)}$ is recognized by $Q^{(d)}$ with initial state q_0 and final states $F_u = \{q \in Q : qu \in F\}$. Thus, each $L^{(d,u)}$ belongs to $\mathcal{V}$.

Suppose now that each $L^{(d,u)}$ belongs to $\mathcal{V}$, for any $u \in \Sigma^*$ with $|u| < d$, so that each $L^{(d,u)}$ can be recognized by some automaton Q_u in $\Sigma^{(d)}\mathbf{V}$. For each u, let $R_u = Q_u \times (\cup_{k \in [d]} \Sigma^k)$. We turn R_u into a Σ-automaton $(R_u, \Sigma, \cdot)$ by defining, for each $(q, v) \in R_u$ and $a \in \Sigma$,

$$(q, v) \cdot a \quad = \quad \begin{cases} (q, va) & \text{if } |v| < d - 1 \\ q\langle va \rangle & \text{otherwise.} \end{cases}$$

Let $Q'_u = (q, \epsilon)$, $q \in Q_u$. Then Q'_u determines a subautomaton of $R_u^{(d)}$ which is isomorphic to Q_u. Moreover, $(q, v) = (q, \epsilon)v$, for each $(q, v) \in R_u$. Thus, by Remark 4.3 and the assumption $\mathbf{D} \star \mathbf{V} \subseteq \mathbf{V}$, it follows that R_u belongs to $\mathbf{C}_d \star \mathbf{V}$. Now for every u, the language $L_u = (Lu^{-1}) \cap (\Sigma^d)^*$ can be recognized by R_u, so that $L_u \in \mathcal{C}_d \star \mathcal{V}$. Since $L = \bigcup_{u \in \Sigma^*,\ |u| < d} L_u u$, it follows now that L is in $\mathcal{C}_d \star \mathcal{V}$. ■

COROLLARY 4.9 *Under the assumption of Theorem 4.8, if* $\mathcal{V}$ *is decidable, then so is* $\mathcal{C}_d \star \mathcal{V}$*.*

Proof. This follows either from Theorem 4.8 or from Theorem 4.6. ■

COROLLARY 4.10 *Suppose that* $M \subseteq \mathsf{Nat}$ *and* $\mathbf{V}$ *is a q-variety with corresponding l-variety* $\mathcal{V}$*. Suppose that* $\mathbf{D} \star \mathbf{V} \subseteq \mathbf{V}$ *and that* $\mathcal{V}$ *is closed with respect to right concatenation by letters. An automaton* Q *is in* $\mathbf{C}_M \star \mathbf{V}$ *iff there is some* $d \in (M]$ *with* $Q^{(d)} \in \mathbf{V}$*. Moreover, a language* $L \subseteq \Sigma^*$ *is in* $\mathcal{C}_M \star \mathcal{V}$ *iff there is some* $d \in (M]$ *such that* $L^{(d,u)} \in \mathcal{V}$ *for each* $u \in \Sigma^*$ *with* $|u| < d$*.*

5 Degree of aperiodicity

Following [1, 15], we call an automaton $Q = (Q, \Sigma, \cdot)$ *quasi-aperiodic* if for each n, $M(Q)$ (or $S(Q)$) contains no nontrivial group *all of whose members can be*

induced by length n words. Thus, for any given n, the set of functions u^Q, where u is any word in Σ^n of length n, does not contain a nontrivial group. (In the terminology of [6], Q is quasi-aperiodic if no nontrivial group divides $M(Q)$ in "equal lengths".)

It is clear that any aperiodic automaton is quasi-aperiodic. On the other hand, a counter of length > 1 is quasi-aperiodic, but not aperiodic. Let $\mathbf{QA}$ denote the stream of quasi-aperiodic automata. The following theorem is a rephrasing of a result due to Barrington, Compton, Straubing and Therien. In its original formulation, the theorem involved the wreath product instead of the cascade product.

THEOREM 5.1 (Barrington et al. [1]) $\mathbf{QA} = \mathbf{C} \star \mathbf{A}$. *Thus* $\mathbf{QA}$ *is a q-variety.*

It is a well-known consequence of the Krohn-Rhodes theorem [4, 15] that $\mathbf{A} \star \mathbf{A} \subseteq \mathbf{A}$, in fact equality holds. Thus, by Proposition 3.5, $\mathbf{QA}$ is also closed with respect to the cascade product. Moreover, since $\mathbf{D} \subseteq \mathbf{A}$, we have that $\mathbf{D} \star \mathbf{A} \subseteq \mathbf{A}$. Thus, by Theorem 4.6 we have:

COROLLARY 5.2 *For any* $d \geq 1$ *and automaton* Q*, we have* $Q \in \mathbf{C}_d \star \mathbf{A}$ *iff* $Q^{(d)} \in \mathbf{A}$.

COROLLARY 5.3 *An automaton* Q *is quasi-aperiodic iff there is some integer* $d \geq 1$ *such that* $Q^{(d)}$ *is aperiodic.*

Proof. If Q is quasi-aperiodic, then by Theorem 5.1, Q is in $\mathbf{C} \star \mathbf{A}$. But since $\mathbf{C}$ is the union of the $\mathbf{C}_n$ where n is any positive integer, it follows that Q is in $\mathbf{C}_d \star \mathbf{A}$, for some $d \geq 1$. Thus, by Corollary 5.2, $Q^{(d)}$ is in $\mathbf{A}$, so that $Q^{(d)}$ is aperiodic.

Assume now that $Q^{(d)}$ is aperiodic, for some $d \geq 1$. Then, by Corollary 5.2 and Theorem 5.1, Q is in $\mathbf{C}_d \star \mathbf{A} \subseteq \mathbf{QA}$. ■

REMARK 5.4 *Of course, it is possible to prove Corollary 5.3 without using Theorem 5.1 and Corollary 5.2. Assume that* $Q^{(d)}$ *is aperiodic for some* $d \geq 1$*. Then it cannot be the case that for some* n*, the set of all functions in* $M(Q)$ *that can be induced by the length* n *words contains a nontrivial group* G*, since otherwise each element of* G *would be induced by a word of length* dn*, so that* $Q^{(d)}$ *would not be aperiodic. The other direction can be verified by following the argument given in the proof of Theorem 5.10.*

PROPOSITION 5.5 *Suppose that* Q *is an automaton such that both* $Q^{(m)}$ *and* $Q^{(n)}$ *are aperiodic, where* $m, n \geq 1$*. If* m *and* n *are relative primes, then also* Q *is aperiodic.*

Proof. If Q is not aperiodic, then $M(Q)$ contains a cyclic subgroup $G = \{g_0, \ldots, g_{p-1}\}$ of prime order $p > 1$, where $g_0 = e$ denotes the unit. Unless $g_1^m = e$, it follows that each element of G can be induced by a word whose length is a multiple of m. (Indeed, if $g_1^m = g_i$, where $i \neq 0$, then g_i can be induced by a word whose length is a multiple of m. Since g_i is a generator element of G, the same holds for any other group element.) But since $Q^{(m)}$ is aperiodic, this is impossible. We conclude that $g_1^m = e$. In the same way, $g_1^n = e$. But then p divides both m and n, a contradiction. ■

COROLLARY 5.6 *Suppose that Q is an automaton such that both $Q^{(m)}$ and $Q^{(n)}$ are aperiodic. If d denotes the g.c.d. of m and n, then $Q^{(d)}$ is also aperiodic.*

COROLLARY 5.7 *An automaton Q is quasi-aperiodic iff there is a least integer $d \geq 1$ such that $Q^{(d)}$ is aperiodic. Moreover, for an integer $n \geq 1$ we have that $Q^{(n)}$ is aperiodic iff this integer d is a divisor of n.*

DEFINITION 5.8 *The* degree of aperiodicity*, or* aperiodicity degree *of an automaton Q is the least integer d such that $Q^{(d)}$ is aperiodic, if such an integer exists. Otherwise the degree of aperiodicity of Q is ∞.*

Thus, by Corollary 5.7, the aperiodicity degree of Q is finite iff Q is quasi-aperiodic.

For any set M of positive integers, we let $\mathbf{QA}_M$ denote the stream of automata whose aperiodicity degree is finite and belongs to $(M]$. In particular, $\mathbf{A} = \mathbf{QA}_{\{1\}} = \mathbf{QA}_\emptyset$ and $\mathbf{QA} = \mathbf{QA}_{\mathsf{Nat}}$. We also denote $\mathbf{QA}_d = \mathbf{QA}_{\{d\}}$, for each $d \geq 1$.

THEOREM 5.9 *Suppose that M is a set of positive integers. Then $\mathbf{QA}_M = \mathbf{C}_M \star \mathbf{A}$. Thus, $\mathbf{QA}_M$ is a q-variety closed with respect to the cascade product.*

Proof. Suppose that the aperiodicity degree d of automaton Q is finite and is contained in $(M]$. Then $Q^{(d)}$ is aperiodic so that $Q \in \mathbf{C}_d \star \mathbf{A}$, by Corollary 5.2. But $\mathbf{C}_d \subseteq \mathbf{C}_M$, so that $Q \in \mathbf{C}_M \star \mathbf{A}$.

Suppose now that $Q \in \mathbf{C}_M \star \mathbf{A}$. Then since $\mathbf{C}_M$ is the union of all varieties $\mathbf{C}_d$, where d belongs to $(M]$, it follows by Proposition 3.6 that $Q \in \mathbf{C}_d \star \mathbf{A}$, for some such d. Thus, by Corollary 5.2, $Q^{(d)}$ is aperiodic. But then the aperiodicity degree of Q divides d, so that it also belongs to $(M]$. ■

THEOREM 5.10 *There exists an algorithm to compute the aperiodicity degree of an automaton.*

Proof. Barrington, Compton, Straubing and Therien showed in [1] how to decide for an automaton whether or not it belongs to $\mathbf{QA}$. (See also [6].) Our result

follows by a slight modification of their argument. Given $Q = (Q, \Sigma, \cdot)$, successively compute the sets $M_{=1}(Q)$, $M_{=2}(Q), \ldots$ until a repetition occurs, i.e., until $M_{=m}(Q) = M_{=n}(Q)$, for some $m < n$. Here, we let $M_{=m}(Q)$ denote the set of all functions $Q \to Q$ induced by the words in Σ^m. Then also $M_{=m+r}(Q) = M_{=n+r}(Q)$, for all $r \geq 1$. In particular, we have $M_{=d}(Q) = M_{=d+n-m}(Q)$ for some $m \leq d < n$ such that $n-m$ divides d. Thus, $M_{=d}(Q) = M_{=2d}(Q)$, showing that $M_{=d}(Q)$ is a subsemigroup of $M(Q)$. In fact, $M_{=d}(Q)$ is the semigroup of all functions inducible by words whose length is a positive multiple of d. If Q is quasi-aperiodic, then this semigroup contains no nontrivial group by definition. It follows that $Q^{(d)}$ is aperiodic. Thus, to compute the aperiodicity degree of Q it suffices to find the least divisor d' of d such that $Q^{(d')}$ is aperiodic. On the other hand, if $M_{=d}$ does contain a nontrivial group, then Q is not quasi-aperiodic and thus its aperiodicity degree is ∞. ■

COROLLARY 5.11 *Suppose that it is decidable for an integer n whether n belongs to the division ideal generated by M. Then $\mathbf{QA}_M$ is decidable. In particular, if M is a recursive set and a division ideal, then $\mathbf{QA}_M$ is decidable.*

REMARK 5.12 *The opposite direction is immediate: if $\mathbf{QA}_M$ is decidable then $(M]$ is recursive.*

Since $\mathbf{QA}_M$ is a q-variety, there is a corresponding l-variety that we denote by $\mathcal{QA}_M$. We also denote $\mathcal{QA}_{\{d\}}$ by $\mathcal{QA}_d$. In particular, $\mathcal{QA}_{\{1\}} = \mathcal{QA}_1 = \mathcal{A}$ and $\mathcal{QA}_{\mathsf{Nat}} = \mathcal{QA}$, the l-variety corresponding to $\mathbf{QA}$. Since $\mathbf{QA}_M$ is the union of the $\mathbf{QA}_d$, where d is any element of the division ideal $(M]$ generated by M, also $\mathcal{QA}_M$ is the union of the $\mathcal{QA}_d$, where d is any member $(M]$. The languages belonging to $\mathcal{A}$ have been characterized by Schützenberger as the *star-free languages*.

THEOREM 5.13 (Schützenberger [13]) *A language $L \subseteq \Sigma^*$ belongs to $\mathcal{A}$ iff L can be constructed from the finite subsets of Σ^* by the operations of set union, complement and concatenation.*

A similar characterization of languages in $\mathcal{QA}$ was obtained in [1].

THEOREM 5.14 (Barrington, Compton, Straubing and Therien [1]) *A language $L \subseteq \Sigma^*$ belongs to $\mathcal{QA}$ iff L can be constructed from the finite languages in Σ^* and the languages $(\Sigma^d)^*$, $d \geq 1$, by the operations of union, complement and concatenation.*

In the rest of this section we prove a refinement of these results.

THEOREM 5.15 *Let M denote any subset of the set of positive integers. A language $L \subseteq \Sigma^*$ belongs to $\mathcal{QA}_M$ iff L can be constructed from the finite languages*

in Σ^* and the languages $(\Sigma^m)^*$, where $m \in M$, by the operations of union, complement and concatenation.

In our argument, we will make use of the following characterization of $\mathcal{QA}_d$, which is an immediate consequence of Theorem 4.8 and the fact that $\mathcal{A}$ is closed with respect to concatenation and contains the finite sets.

COROLLARY 5.16 *For any integer $d \geq 1$ and language $L \subseteq \Sigma^*$, if $L \in \mathcal{QA}_d$ then $L^{(d,u)} \in \mathcal{A}$, for all $u \in \Sigma^*$ with $|u| < d$. Moreover, if $L^{(d,u)} \in \mathcal{A}$, for all $u \in \Sigma^*$ with $|u| < d$, then $L \in \mathcal{QA}_d$.*

Proof of Theorem 5.15. First note that any language $(\Sigma^d)^*$, where d is any member of the division ideal generated by M can be constructed from the finite languages and the languages $(\Sigma^m)^*$, $m \in M$ by the operations of union, complement, and concatenation. This follows from the following two facts. If m_1 and m_2 are positive integers and m denotes their least common multiple (l.c.m.), then $(\Sigma^m)^* = (\Sigma^{m_1})^* \cap (\Sigma^{m_2})^*$. Moreover, if d is a divisor of m, then for some finite F, $(\Sigma^d)^* = (\Sigma^m)^* F$. Thus, since $\mathcal{QA}_M = \bigcup_{d \in (M]} \mathcal{QA}_d$, in the rest of the argument we may assume that M is itself a division ideal.

Suppose first that $L \in \mathcal{QA}_M$. Since $\mathcal{QA}_M$ is the union of the $\mathcal{QA}_m$ with $m \in M$, there exists an integer $d \in M$ with $L \in \mathcal{QA}_d$. Thus, by Corollary 5.16, all the languages $L^{(d,u)}$, $u \in \Sigma^*$, $|u| < d$ are in $\mathcal{A}$. By Schützenberger's theorem, Theorem 5.13, it follows that each $L^{(d,u)}$ with $u \in \Sigma^*$, $|u| < d$ can be constructed from the finite languages in $(\Sigma^{(d)})^*$ by using the operations of union, complement and concatenation. Hence, each language $K_u = Lu^{-1} \cap (\Sigma^d)^*$, where $u \in \Sigma^*$ with $|u| < d$ can be constructed from the finite languages in Σ^* and the language $(\Sigma^d)^*$ by the operations of union, complement and concatenation. (Take complement relatively to $(\Sigma^d)^*$.) Since $L = \bigcup_{u \in \Sigma^*,\ |u| < d} K_u u$, the same holds for L.

Suppose now that L can be constructed from the finite subsets of Σ^* and the languages $(\Sigma^m)^*$, where $m \in M$ by the operations of union, complement and concatenation. Let d denote the l.c.m. of those integers m for which $(\Sigma^m)^*$ is used in the construction of L. If we can show that $L^{(d,v)}$ belongs to $\mathcal{A}$, for each $v \in \Sigma^*$ with $|v| < d$, then it follows by Corollary 5.16 that $L \in \mathcal{QA}_d$, and thus that $L \in \mathcal{QA}_M$. We will show that for each $u, v \in \Sigma^*$ with $|u|, |v| < d$, the language in $(\Sigma^{(d)})^*$

$$L^{(d,u,v)} \quad = \quad \{\langle x_0 \rangle \dots \langle x_{k-1} \rangle : k \geq 0,\ ux_0 \dots x_{k-1} v \in L\}$$

is in $\mathcal{A}$. Now this follows by a straightforward induction argument using Schützenberger's theorem, Theorem 5.13, and the following facts. Let $u, v \in \Sigma^*$ with $|u|, |v| < d$, and let $L, L_1, L_2 \subseteq \Sigma^*$.

1. If L is finite, then so is $L^{(d,u,v)}$.

2. $(L_1 \cup L_2)^{(d,u,v)} = L_1^{(d,u,v)} \cup L_2^{(d,u,v)}$.
3. $(L^c)^{(d,u,v)} = (L^{(d,u,v)})^c$.
4. If the length of each word in L_1 is at least $|u|$ and the length of each word in L_2 is at least $|v|$, then $(L_1L_2)^{(d,u,v)} = \bigcup_{|wz|=d} L_1^{(d,u,w)}\langle wz\rangle L_2^{(d,z,v)}$.
5. If the length of each word in L_1 is less than $|u|$ and the length of each word in L_2 is at least $|v|$, then $(L_1L_2)^{(d,u,v)} = \bigcup_{wz=u,\ w\in L_1} L_2^{(d,z,v)}$.
6. If the length of each word in L_1 is at least $|u|$ and the length of each word in L_2 is less than $|v|$, then $(L_1L_2)^{(d,u,v)} = \bigcup_{zw=v,\ w\in L_2} L_1^{(d,u,z)}$.
7. If the length of each word in L_1 is less than $|u|$ and the length of each word in L_2 is less than $|v|$, then $(L_1L_2)^{(d,u,v)}$ is finite. ■

COROLLARY 5.17 *Suppose that it is decidable for an integer whether it is contained in the division ideal generated by M. Then there exists an algorithm to decide for a regular language $L \subseteq \Sigma^*$ whether or not L can be constructed from the finite languages and the languages $(\Sigma^m)^*$ with $m \in M$ by the operations of union, complement and concatenation.*

REMARK 5.18 *The converse of the above corollary is immediate. If there exists an algorithm to decide for a regular language $L \subseteq \Sigma^*$ whether or not L can be constructed from the finite languages and the languages $(\Sigma^m)^*$ with $m \in M$ by the operations of union, complement and concatenation, then $(M]$ is a recursive set.*

6 First-order logic

The expressive power of first-order logic on words with a unary predicate corresponding to each letter of the alphabet and $<$ as the only numerical predicate was characterized by McNaughton and Papert [10]. We let $\mathbf{FO}[<]$ denote this logic. Thus, for any fixed alphabet Σ, the *atomic formulas* of $\mathbf{FO}[<]$ are the propositions $P_a(x)$ and $x < y$, where a is any letter of Σ and x and y are variables. *Formulas* can be constructed from the atomic formulas by the boolean connectives $\vee$ and $\neg$, denoting disjunction and negation, and existential quantification. The other boolean connectives and universal quantification can be introduced as abbreviations. *Free and bound variables* are defined as usual. We may assume that no variable is bound two or more times in a formula, or in a finite set of formulas, and that any free variable is different from any bound variable. Below we will denote *syntactic equality* by $\equiv$.

Suppose that φ is a formula with free variables in X, and suppose that $w \in \Sigma^*$ and $\lambda : X \to [|w|]$, i.e., λ maps variables in X to "positions" in w. We say that (w, λ) *satisfies* φ, denoted $(w, \lambda) \models \varphi$, if

- $\varphi \equiv P_a(x)$ and the letter in w at position x is a, or
- $\varphi \equiv x < y$ and $x\lambda < y\lambda$, or
- $\varphi \equiv \varphi_1 \vee \varphi_2$ and $(w, \lambda) \models \varphi_1$ or $(w, \lambda) \models \varphi_2$, or
- $\varphi \equiv \neg\psi$ and $(w, \lambda) \not\models \psi$, or
- $\varphi \equiv (\exists x)\psi$ and there exists a function $\lambda' : X \cup \{x\} \to [|w|]$ which agrees with λ on X such that $(w, \lambda') \models \psi$. (Here, by our conventions, we may assume without loss of generality that $x \notin X$.)

When X is empty, so that φ is a *sentence*, i.e., φ has no free variables, we just write $w \models \varphi$ and call $\{w \in \Sigma^* : w \models \varphi\}$ the *language defined by* φ. Moreover, we say that a language $L \subseteq \Sigma^*$ is *definable in* $\mathbf{FO}[<]$ if there is a sentence φ which defines L.

As before, we let $\mathbf{A}$ denote the $*$-variety of aperiodic automata, and let $\mathcal{A}$ denote the corresponding $*$-variety of languages.

THEOREM 6.1 (McNaughton and Papert [10]) *A language $L \subseteq \Sigma^*$ is definable in $\mathbf{FO}[<]$ iff $L \in \Sigma^*\mathcal{A}$.*

We refer the reader to [10], and in particular to [15], for detailed proofs of Theorem 6.1.

Subsequently, Barrington, Compton, Straubing and Therien [1] considered the extension of first-order logic by atomic propositions of the form $C_d^r(x)$, $d \geq 1$, $r \in [d]$ meaning that position x in the word satisfies $x \equiv r \bmod d$. Thus, using the above notations, $(w, \lambda) \models C_d^r(x)$ if and only if $x\lambda$ is congruent to r mod d. Since this logic is equivalent to the extension of $\mathbf{FO}[<]$ by all regular numerical predicates, see [14], we denote it by $\mathbf{FO}[\mathbf{R}]$. As before, let $\mathcal{QA}$ denote the l-variety corresponding to the q-variety $\mathbf{QA}$ of quasi-aperiodic automata.

THEOREM 6.2 (Barrington et al. [1]) *A language $L \subseteq \Sigma^*$ is definable in $\mathbf{FO}[\mathbf{R}]$ iff $L \in \Sigma^*\mathcal{QA}$.*

For an integer $d \geq 1$ let $\mathbf{FO}[d]$ denote the fragment of $\mathbf{FO}[\mathbf{R}]$ where only atomic propositions associated to the letters of the alphabet and propositions of the form $x < y$ and $C_d^r(x)$ are allowed. (It would be sufficient to allow only $x < y$ and $C_d^0(x)$.) Moreover, for a set M of the positive integers, let $\mathbf{FO}[M]$ denote the union of the $\mathbf{FO}[d]$ with $d \in M$. Thus, $\mathbf{FO}[\mathbf{R}] = \mathbf{FO}[\mathsf{Nat}]$ and $\mathbf{FO}[<] = \mathbf{FO}[\emptyset] = \mathbf{FO}[1]$.

Below we will write $x \leq y$ as abbreviation for $\neg(y < x)$, $x = y + 1$ for $x < y \wedge \neg(\exists z)(x < z \wedge z < y)$, $\mathsf{Last}(x)$ for $(\forall y)(y \leq x)$, True for $\varphi \vee \neg\varphi$, where φ is a fixed sentence, and False for $\neg\mathsf{True}$.

PROPOSITION 6.3 *A language $L \subseteq \Sigma^*$ is definable in* $\mathbf{FO}[M]$ *iff L is definable in* $\mathbf{FO}[(M]]$.

Proof. This follows by the following two observations.

1. If d is a divisor of m, say $dk = m$, then $C_d^0(x)$ can be expressed as $C_m^0(x) \vee C_m^d(x) \vee \ldots C_m^{d(k-1)}(x)$. Moreover, for every $r \in [d]$, $C_m^{r+1}(x)$ can be expressed by $(\exists y)(x = y + 1 \wedge C_m^r(y))$.
2. If $m_1, m_2 \geq 1$ and m denotes the l.c.m. of m_1 and m_2, then $C_m^0(x)$ can be expressed as $C_{m_1}^0(x) \wedge C_{m_2}^0(x)$. ■

By our previous results we can prove the following common extension of Theorems 6.1 and 6.2.

THEOREM 6.4 *Suppose that M is any set of the positive integers. Then a language $L \subseteq \Sigma^*$ is definable in* $\mathbf{FO}[M]$ *iff $L \in \Sigma^* \mathcal{QA}_M$.*

The proof of Theorem 6.4 will be completed at the end of the section.

PROPOSITION 6.5 *Suppose that $L \subseteq \Sigma^*$ and $d \geq 1$. If $L^{(d)}$ is definable in* $\mathbf{FO}[<]$, *then $L \cap (\Sigma^d)^*$ is definable in* $\mathbf{FO}[d]$.

Proof. First we prove that for all $\varphi \in \mathbf{FO}[<]$ with free variables in X there exists some $\varphi' \in \mathbf{FO}[d]$ with free variables in X such that for all $w \in (\Sigma^{(d)})^*$ and $\lambda : X \to [|w|]$,

$$(w, \lambda) \models \varphi \quad \textit{iff} \quad (wh, \kappa) \models \varphi',$$

where h denotes the homomorphism $(\Sigma^{(d)})^* \to \Sigma^*$ defined by $\langle u \rangle \mapsto u$, for all $u \in \Sigma^d$, and where $x\kappa = d(x\lambda)$, the product of the integers d and $x\lambda$, for all $x \in X$. We prove this claim by induction on the structure of φ.

- $\varphi \equiv P_{\langle u \rangle}(x)$, where $u = a_0 \ldots a_{d-1}$. Then, writing x_{d-1} for x, we define

$$\varphi' \quad \equiv \quad (\exists x_0) \ldots (\exists x_{d-2}) \left[\bigwedge_{j=0}^{d-2} x_{j+1} = x_j + 1 \wedge \bigwedge_{j=0}^{d-1} P_{a_j}(x_j) \right].$$

- $\varphi \equiv x < y$. Then $\varphi' \equiv x < y$.
- $\varphi \equiv \varphi_1 \vee \varphi_2$. Then $\varphi' \equiv \varphi_1' \vee \varphi_2'$.
- $\varphi \equiv \neg\varphi_1$. Then $\varphi' \equiv \neg\varphi_1'$.

- $\varphi \equiv \exists x \varphi_1$, Then $\varphi' \equiv (\exists x)(C_d^0(x) \wedge \varphi_1')$.

We now complete the proof of Proposition 6.5. Suppose that $L^{(d)}$ is defined by sentence φ in $\mathbf{FO}[<]$. Then $L \cap (\Sigma^d)^*$ is defined by $\varphi' \wedge (\forall x)(\mathsf{Last}(x) \rightarrow C_d^0(x))$. ■

COROLLARY 6.6 *Suppose that $L \subseteq \Sigma^*$ and $d \geq 1$. If $L^{(d,u)}$ is definable in $\mathbf{FO}[<]$ for all $u \in \Sigma^*$ with $|u| < d$, then L is definable in $\mathbf{FO}[d]$.*

Proof. For each $u \in \Sigma^*$ with $|u| < d$ we have that $L^{(d,u)} = (Lu^{-1})^{(d)}$. By Proposition 6.5, it follows that if $L^{(d,u)}$ is definable in $\mathbf{FO}[<]$, then $K_u = Lu^{-1} \cap (\Sigma^d)^*$ is definable in $\mathbf{FO}[d]$, for each $u \in \Sigma^*$, $|u| < d$. But then, using the formula $L = \bigcup_{u \in \Sigma^*,\ |u|<d} K_u u$, it follows easily that L is definable in $\mathbf{FO}[d]$. Indeed, if K_u is defined by φ_u, where $u = a_0 \ldots a_{n-1} \in \Sigma^*$ with $|u| = n < d$, then $K_u u$ is defined by the formula ψ_u

$$(\exists x_0) \ldots (\exists x_{n-1}) \left[\bigwedge_{i=0}^{n-2} x_{i+1} = x_i + 1 \wedge \bigwedge_{i=0}^{n-1} P_{a_i}(x_i) \wedge \mathsf{Last}(x_{n-1}) \wedge \varphi_u[< x_0] \right],$$

where $\varphi_u[< x_0]$ is the *relativization* of φ_u defined in the usual manner [15]. Finally, L is defined by $\bigvee_{u \in \Sigma^*,\ |u|<d} \psi_u$. ■

PROPOSITION 6.7 *If $L \subseteq \Sigma^*$ is definable in $\mathbf{FO}[d]$, then $L^{(d)}$ is definable in $\mathbf{FO}[<]$.*

Proof. We prove the following claim. For all φ in $\mathbf{FO}[d]$ with free variables in X and for all functions $\rho : X \rightarrow [d]$ there exists a formula $\varphi_\rho' \in \mathbf{FO}[<]$ with free variables in X such that for all words $w \in (\Sigma^{(d)})^*$ and functions $\lambda : X \rightarrow [|w|]$,

$$(w, \lambda) \models \varphi_\rho' \quad \textit{iff} \quad (wh, \kappa_\rho) \models \varphi,$$

where h denotes the homomorphism $(\Sigma^{(d)})^* \rightarrow \Sigma^*$ given by $\langle u \rangle \mapsto u$, for all $u \in \Sigma^d$, and where $x\kappa_\rho = (x\lambda)d + x\rho$, for all $x \in X$. We prove this claim by induction on the structure of φ.

- $\varphi \equiv P_a(x)$. Then φ_ρ' is the disjunction of all of the $P_{\langle u \rangle}(x)$ such that the letter of u on the $(x\rho)$th position is a.
- $\varphi \equiv x < y$. Then

$$\varphi_\rho' \quad \equiv \quad \begin{cases} x < y & \text{if } x\rho \geq y\rho \\ x \leq y & \text{if } x\rho < y\rho. \end{cases}$$

- $\varphi \equiv C_d^r(x)$. Then

$$\varphi'_\rho \quad \equiv \quad \begin{cases} \mathsf{True} & \text{if } x\rho = r \\ \mathsf{False} & \text{if } x\rho \neq r. \end{cases}$$

- $\varphi \equiv \varphi_1 \vee \varphi_2$. Then $\varphi'_\rho = (\varphi'_1)_\rho \vee (\varphi'_2)_\rho$.
- $\varphi \equiv \neg\psi$. Then $\varphi'_\rho = \neg\psi'_\rho$.
- $\varphi \equiv (\exists x)\psi$. Here we may assume that x is not in the set X. For each $i \in [d]$, let $\rho[x \mapsto i]$ denote that function $X \cup \{x\} \to [d]$ which agrees with ρ on X and such that $x\rho = i$. Then we define

$$\varphi'_\rho \quad \equiv \quad (\exists x) \bigvee_{i \in [d]} \psi'_{\rho[x \mapsto i]}.$$

We now complete the proof of Proposition 6.7. Suppose that $L \subseteq \Sigma^*$ is defined by the sentence φ in $\mathbf{FO}[d]$. Let φ' be the corresponding sentence of $\mathbf{FO}[<]$ defined above. Then for all $w \in (\Sigma^{(d)})^*$,

$$w \models \varphi' \quad \textit{iff} \quad wh \models \varphi.$$

(Note that ρ is the empty function.) Thus, φ' defines $L^{(d)}$. ■

COROLLARY 6.8 *If $L \subseteq \Sigma^*$ is definable in $\mathbf{FO}[d]$ then for each $u \in \Sigma^*$ with $|u| < d$, $L^{(d,u)}$ is definable in $\mathbf{FO}[<]$.*

Proof. Use the fact that $L^{(d,u)} = (Lu^{-1})^{(d)}$ and that if L is definable in $\mathbf{FO}[d]$, then so is Lu^{-1}. ■

We are now in the position to complete the proof of Theorem 6.4.

Proof of Theorem 6.4. By Corollaries 6.6 and 6.8, a language $L \subseteq \Sigma^*$ is definable in $\mathbf{FO}[d]$ iff $L^{(d,u)}$ is definable in $\mathbf{FO}[<]$, for each $u \in \Sigma^*$ with $|u| < d$. Thus, by the theorem of McNaughton and Papert, Theorem 6.1, and by Corollary 5.16, L is definable in $\mathbf{FO}[d]$ iff $L \in \mathcal{QA}_d$. Since a language is definable in $\mathbf{FO}[M]$ iff it is definable in $\mathbf{FO}[d]$, for some d in the division ideal generated by M, and since $\mathcal{QA}_M$ is the union of the $\mathcal{QA}_d$ where d is any integer in the division ideal generated by M, the result follows. ■

COROLLARY 6.9 *Suppose that membership in the division ideal generated by M is decidable. Then it is decidable for a regular language L whether or not L can be defined in $\mathbf{FO}[M]$.*

Again, the converse direction holds obviously.

7 Temporal logic

The language **LTL** of Linear (Propositional) Temporal Logic [12] over an alphabet Σ has, as atomic formulas (or atomic propositions), the propositional constants p_a associated with the letters $a \in \Sigma$. Formulas can be constructed from the atomic formulas by the boolean connectives $\vee$ and $\neg$, and the modalities X (next) and U (until). Other boolean connectives may be introduced as usual. Suppose that $u \in \Sigma^*$ and that φ is a formula. We say that u satisfies φ, denoted $u \models \varphi$, if

1. $\varphi \equiv p_a$ and $u = av$, for some $a \in \Sigma$ and $v \in \Sigma^*$, or
2. $\varphi \equiv \varphi_1 \vee \varphi_2$, for some φ_1 and φ_2, and $u \models \varphi_1$ or $u \models \varphi_2$, or
3. $\varphi \equiv \neg\psi$, for some formula ψ, and it is not the case that $u \models \psi$, or
4. $\varphi \equiv \varphi_1 U \varphi_2$, for some φ_1 and φ_2, and there exist $v, w \in \Sigma^*$ such that $u = vw$, $w \models \varphi_2$, moreover, $z \models \varphi_1$ for all suffixes z of u properly including w.

In this section we study the extension of **LTL** by counting. Suppose that $M \subseteq \mathsf{Nat}$. For an alphabet Σ, the atomic formulas of $\mathbf{LTL}[M]$ are those of **LTL** together with an additional propositional constant $\mathsf{lg}_{d,r}$, for each $d \in M$ and $r \in [d]$. Formulas are constructed from the atomic formulas as above, so that if φ and ψ are formulas, then so are $\varphi \vee \psi$, $\neg\varphi$, $X\varphi$ and $\varphi U \psi$. For all $d \in M$ and $r \in [d]$, we define $u \models \mathsf{lg}_{d,r}$ iff the length of u is congruent to r modulo d. The semantics of the other constructs of $\mathbf{LTL}[M]$ are defined as above. When M is the division ideal generated by d, we write just $\mathbf{LTL}[d]$ for $\mathbf{LTL}[M]$. Note that $\mathbf{LTL}[1]$ is just **LTL**, as is $\mathbf{LTL}[\emptyset]$.

We say that a language $L \subseteq \Sigma^*$ is definable in $\mathbf{LTL}[M]$ if there is a formula φ of $\mathbf{LTL}[M]$ (with propositional constants corresponding to the letters of Σ) such that $L = L_\varphi = \{u \in \Sigma^* : u \models \varphi\}$.

EXAMPLE 7.1 For any $m, n > 0$ and $u \in \Sigma^*$, we have that $u \models \mathsf{lg}_{m,0}$ and $u \models \mathsf{lg}_{n,0}$ iff $u \models \mathsf{lg}_{k,0}$, where k denotes the least common multiple of m and n. Moreover, $u \models \mathsf{lg}_{m,r}$, for $r \in [m]$, iff $u \models X^r \mathsf{lg}_{m,0}$, where X^r is $X \ldots X$ with X appearing r times. Also, if n divides m, then $u \models \mathsf{lg}_{n,0}$ iff $u \models \bigvee_{i \in [m/n]} \mathsf{lg}_{m,in}$.

By the above example, we have that $\mathbf{LTL}[M]$ is as exactly as expressive as $\mathbf{LTL}[(M]]$, i.e., a language is definable in $\mathbf{LTL}[M]$ iff it is definable in $\mathbf{LTL}[(M]]$. Moreover, when M is not empty, then a language is definable in $\mathbf{LTL}[M]$ iff it is definable in $\mathbf{LTL}[d]$, for some $d \in (M]$.

The logic $\mathbf{LTL}[M]$ allows for several counting versions of the until modality. For any formulas φ and ψ, and for any $d \in M$ and $r \in [d]$, define $\varphi U^{(d,0)} \psi$ to

be the formula

$$\bigvee_{i\in[d]} [\mathsf{lg}_{d,i} \wedge (\varphi U(\psi \wedge \mathsf{lg}_{d,i}))],$$

and define $\varphi U^{(d,r)}\psi$, $r > 0$ as

$$\varphi \wedge X\varphi \wedge \ldots \wedge X^{r-1}\varphi \wedge X^r(\varphi U^{(d,0)}\psi).$$

We then have $u \models \varphi U^{(d,r)}\psi$ iff u has a decomposition $u = vw$ such that $w \models \psi$, $|v|$ is congruent to r modulo d, moreover, for all x, z with $xz = u$ such that w is a proper suffix of z, it holds that $z \models \varphi$.

A second counting version of the until modality can now be defined as follows. For all φ, ψ and d, r as before, let $\varphi U_1^{(d,0)}\psi$ be the formula

$$\bigvee_{i\in[d]} [\mathsf{lg}_{d,i} \wedge (\neg\mathsf{lg}_{d,i} \vee \varphi)U^{(d,0)}\psi)].$$

Moreover, when $r > 0$, let $\varphi U_1^{(d,r)}\psi$ be the formula

$$\varphi \wedge X\varphi \wedge \ldots \wedge X^{r-1}\varphi \wedge X^r(\varphi U_1^{(d,0)}\psi).$$

We now have $u \models \varphi U^{(d,r)}\psi$, for u a word in Σ^*, iff u has a decomposition $u = vw$ such that $w \models \psi$, $|v|$ is congruent to r modulo d, moreover, for all x, z with $xz = u$ such that w is a proper suffix of z and $|x|$ is congruent to r modulo d, it holds that $z \models \varphi$.

A last version of until involves several formulas. Suppose, as before, that $d \in M$, and suppose that $\varphi_0, \ldots, \varphi_{d-1}, \psi$ are formulas of $\mathbf{LTL}[M]$. We define $(\varphi_0, \ldots, \varphi_{d-1})U_2^{(d,0)}\psi$ as the formula

$$\bigvee_{i\in[d]} [\mathsf{lg}_{d,i} \wedge ((\neg\mathsf{lg}_{d,i} \vee \varphi_i)U^{(d,0)}\psi)]$$

Thus, for all words $u \in \Sigma^*$, we have $u \models (\varphi_0, \ldots, \varphi_{d-1})U_2^{(d,0)}\psi$ iff u has a decomposition $u = vw$ such that $w \models \psi$, $|v|$ is congruent to r modulo 0, moreover, for all x, z and $i \in [d]$ with $xz = u$ such that w is a proper suffix of z and $|x|$ is congruent to i modulo d, it holds that $z \models \varphi_i$. The modalities $U^{(d,r)}$ with $r \in [d]$, $r \neq 0$, which have a similar semantics, can be introduced in the obvious way. Of course, the propositional constants $\mathsf{lg}_{d,r}$ can in turn be defined using either version of until.

REMARK 7.2 *The last version of until shows that the extension of* **LTL** *by counting fits in the framework of Wolper's extension of temporal logic by grammar (or finite automaton) operators, cf. [21, 20].*

We introduce several abbreviations. First, let $\mathsf{True} = p_a \vee \neg p_a$, where a is any letter in Σ, and let $\mathsf{False} = \neg\mathsf{True}$. Moreover, let End denote the formula $\bigwedge_{a\in\Sigma} \neg p_a$, so that for all $u \in \Sigma^*$, we have $u \models \mathsf{End}$ iff $u = \epsilon$. Finally, for any formula φ, let $\Diamond^{(d,r)}\varphi$ stand for $\mathsf{True}\, U^{(d,r)}\varphi$ and $\Box^{(d,r)}\varphi$ for $\neg\Diamond^{(d,r)}\neg\varphi$. The modalities $\Diamond$ and $\Box$ are defined as usual.

EXAMPLE 7.3 Let $\Sigma = \{a, b\}$. If φ is the formula $\Diamond^{(2,0)}\mathsf{End}$, then L_φ, the language defined by φ is $(\Sigma^2)^*$. Moreover, if $\psi \equiv p_a U^{(2,0)}(\Box p_b)$, then L_ψ is the language $(a^2)^*b^*$.

In his thesis [9], Kamp proved that temporal logic with past and future modalities is *expressively complete* in the sense that it can express every first-order property of words. Subsequently, it has been shown in [7] that future (or past) modalities alone suffice. An algebraic proof of this result, based on the Krohn-Rhodes decomposition theorem for finite semigroups and automata [4, 15], was later given by Cohen, Perrin and Pin in [3]. However, the simplest proof to date is the one found by Th. Wilke, cf. [19].

THEOREM 7.4 (Kamp [9], Gabbay et al. [7]) *A language $L \subseteq \Sigma^*$ is definable in* **LTL** *iff L is definable in* $\mathbf{FO}[<]$.

Hence, L is definable in **LTL** iff L is in $\mathcal{A}$. Our aim is to prove the following counting version of Kamp's theorem.

THEOREM 7.5 *Suppose that M is a division ideal. Then a language $L \subseteq \Sigma^*$ is definable in* $\mathbf{LTL}[M]$ *iff L is definable in* $\mathbf{FO}[M]$.

In our proof of Theorem 7.5, we will use:

PROPOSITION 7.6 *Suppose that $L \subseteq \Sigma^*$, $d \geq 1$ and $v \in \Sigma^*$ with $|v| < d$. If $L^{(d,v)}$ is definable in* **LTL**, *then $L \cap (\Sigma^d)^* v$ is definable in* $\mathbf{LTL}[d]$.

Proof. First we show that for every formula φ of **LTL** there is a formula φ' of $\mathbf{LTL}[d]$ such that for all words $w \in (\Sigma^{(d)})^*$ it holds that $w \models \varphi$ iff $(wh)v \models \varphi'$, where h denotes the homomorphism $(\Sigma^{(d)})^* \to \Sigma^*$ defined by $\langle w\rangle \mapsto w$, all $w \in \Sigma^d$. We construct φ' by induction.

- $\varphi \equiv p_{\langle u\rangle}$, where $u = a_0 \dots a_{d-1}$. Then

$$\varphi' \quad \equiv \quad p_{a_0} \wedge X p_{a_1} \wedge \dots \wedge X^{d-1} p_{a_{d-1}},$$

  where $X^n\varphi$ is $X \dots X\varphi$ with X appearing n times.

- $\varphi \equiv \varphi_1 \vee \varphi_2$. Then $\varphi' \equiv \varphi_1' \vee \varphi_2'$.
- $\varphi \equiv \neg\psi$. Then $\varphi' \equiv \neg\psi'$.
- $\varphi \equiv X\psi$. Then $\varphi' \equiv X^d\psi'$.
- $\varphi \equiv \varphi_1 U \varphi_2$. Then $\varphi' \equiv \varphi_1' U_1^{(d,0)} \varphi_2'$.

Suppose now that $L^{(d,v)}$ is defined by φ. Then the formula

$$\varphi' \wedge \langle\rangle^{(d,0)}(p_{a_0} \wedge Xp_{a_1} \wedge \ldots \wedge X^{i-1}p_{a_{i-1}} \wedge X^i\mathsf{End})$$

defines $L \cap (\Sigma^d)^* v$, where $v = a_0 \ldots a_{i-1}$ and φ' denotes the formula constructed above. ■

COROLLARY 7.7 *Suppose that $L \subseteq \Sigma^*$ and $d \geq 1$. If $L^{(d,u)}$ is definable in* **LTL**, *for each $u \in \Sigma^*$ with $u \in \Sigma^*$, $|u| < d$, then L is definable in* **LTL**$[d]$.

We are now ready to prove Theorem 7.5.

Proof of Theorem 7.5. It is well-known that temporal logic can be embedded in first order logic: any language definable in **LTL** is definable in **FO**$[<]$. The proof goes by formula induction, essentially by formalizing the definition of the semantics of **LTL**. It is easy to show in the same way that any language definable in **LTL**$[M]$ is definable in **FO**$[M]$.

Suppose now that L is definable in **FO**$[M]$. Then L is definable in **FO**$[d]$, for some $d \in M$. Thus, by Corollary 6.8, $L^{(d,u)}$ is definable in **FO**$[<]$, for each $u \in \Sigma^*$ with $|u| < d$. Thus, by Theorem 7.4 and Corollary 7.7, L is definable in **LTL**$[d]$, hence in **LTL**$[M]$. ■

8 Summary and future results

Our main results can be summarized in a single statement that establishes the equivalence between four descriptions of the same class of languages.

COROLLARY 8.1 *Suppose that M is a set of the positive integers. The following conditions are equivalent for a language $L \subseteq \Sigma^*$:*

1. *L can be constructed from the finite subsets of Σ^* and the languages $(\Sigma^m)^*$, where $m \in M$, by the Boolean operations and concatenation.*
2. *L can be defined by a formula of* **LTL**$[M]$.
3. *L can be defined by a formula of* **FO**$[M]$.

4. *L can be accepted by a finite automaton whose degree of aperiodicity belongs to $(M]$ (or equivalently, the minimal automaton accepting L is finite with aperiodicity degree contained in $(M]$).*

As mentioned above, this result is a common extension of those obtained in [1, 7, 9, 10, 13]. In fact, we have shown that Corollary 8.1 is easily derivable from the classical results of Schützenberger [13], McNaughton and Papert [10], Kamp [9] and Gabbay et al. [7], using Corollary 4.10, which is in turn based on Theorem 4.8 and Theorem 4.6. (Of course, it is possible to prove Corollary 4.10 without using Theorem 4.6.)

Some of the implications of Corollary 8.1 are quite obvious. It is clear that the second condition implies the third as does the first. The fact that the second condition implies the first can be proved by generalizing an argument from [3] which concerns the case when M is empty. That the third condition implies the fourth can also be shown directly using Ehrenfeucht-Fraisse games, following the usual argument establishing the fact that any language definable in **FO** has an aperiodic syntactic monoid. In the classical case, i.e., when $M = \emptyset$, there are two different direct arguments in the literature establishing that the last condition implies the second. The first argument is based on (a weak form of) the Krohn-Rhodes decomposition theorem, and can be found in [3]. A more elementary argument is given in [19]. Both arguments can be generalized to any given set M of moduli.

Theorem 4.8 and Theorem 4.6 are also very useful in the characterization of the expressive power of other variants of first-order and temporal logic. Various fragments of **LTL** have been studied in [3] and [19]. In a forthcoming paper, we will characterize the expressive power of the extension of most of these fragments by counting. In [15, 16], the expressive power of first-order logic with modular quantifiers with respect to any given set of moduli has been characterized, as well as the expressive power of first-order logic with modular quantifiers and the predicates $C_m^r(x)$, where m is any positive integer and $r \in [m]$. Using Theorem 4.8 and Theorem 4.6, we can give a characterization of the expressive power of the extension of first-order logic with any collection of modular quantifiers and any collection of predicates $C_m^r(x)$. A further natural research topic is to extend these results to ω-languages.

9 Acknowledgments

The first author would like to thank the members of the Department of Mathematics of Kyoto Sangyo University and the members of the DSS group of the Department of Computer Science of Aalborg University for their hospitality.

References

[1] D. A. M. Barrington, K. Compton, H. Straubing and D. Therien, Regular languages in NC^1, *J. Comput. Sys. Sci.,* 44(1992), 478–499.

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

[3] J. Cohen, D. Perrin and J.-E. Pin, On the expressive power of temporal logic, *J. Comp. Sys. Sci.,* 46(1993), 271–294.

[4] S. Eilenberg, *Automata, Languages and Machines*, v. A and B., Academic Press, 1974 and 1976.

[5] C. C. Elgot, Decision problems of finite automata design and related arithmetics. *Trans. Amer. Math. Soc.*, 98(1961), 21–51.

[6] Z. Ésik, Results on homomorphic representation of automata by α_0-products, *Theoret. Comp. Sci.*, 87(1991), 229-249.

[7] D. M. Gabbay, A. Pnueli, S. Shelah and J. Stavi, On the temporal analysis of fairness, in: proc. *12th ACM Symp. Principles of Programming Languages*, Las Vegas, 1980, 163–173.

[8] F. Gécseg and I. Peák, *Algebraic Theory of Automata*, Akadémiai Kiadó, Budapest, 1972.

[9] J. A. Kamp, *Tense Logic and the Theory of Linear Order*, Ph. D. Thesis, UCLA, 1968.

[10] R. McNaughton and S. Papert, *Counter-Free Automata*, MIT Press, 1971.

[11] J.-E. Pin, *Varieties of Formal Languages*, North Oxford Academic, 1986.

[12] A. Pnueli, The temporal logic of programs, in: proc. *18th IEEE Symp. Foundations of Computer Science*, Providence, RI, 1977, 46–57.

[13] M. P. Schützenberger, On finite monoids having only trivial subgroups, *Inform. Comp.*, 8(1965), 190–194.

[14] H. Straubing, Constant-depth periodic circuits, *Int. J. Algebra and Computation*, 1(1991), 45–88.

[15] H. Straubing, *Finite Automata, Formal Logic and Circuit Complexity*, Birkhauser, 1994.

[16] H. Straubing, D. Therien and W. Thomas, Regular languages defined with generalized quantifiers, *Information and computation*, 118(1995), 289–301.

[17] W. Thomas, Automata on infinite objects, in: *Handbook of Theoretical Computer Science*, Vol. B, Elsevier, Amsterdam, 1990, 133–191.

[18] W. Thomas, Languages, automata, and logic, in: *Handbook of Formal Language Theory*, Vol. III, (G. Rozenberg, A. Salomaa, Eds.), Springer-Verlag, New York, 1997, 389-455.

[19] Th. Wilke, Classifying discrete temporal properties, in: proc. *STACS 99*, Trier, 1999, LNCS 1563, Springer, 1999, 32–46.

[20] M. Y. Vardi and P. Wolper, Reasoning about infinite computation, *Information and Computation*, 115(1994), 1–37.

[21] P. Wolper, Temporal logic can be more expressive, *Information and Control*, 56(1983), 72–99.

Recent BRICS Report Series Publications

RS-01-53 **Zoltán Ésik and Masami Ito.** ***Temporal Logic with Cyclic Counting and the Degree of Aperiodicity of Finite Automata*****. December 2001. 31 pp.**

RS-01-52 **Jens Groth.** ***Extracting Witnesses from Proofs of Knowledge in the Random Oracle Model*****. December 2001. 23 pp.**

RS-01-51 **Ulrich Kohlenbach.** ***On Weak Markov's Principle*****. December 2001. 10 pp.**

RS-01-50 **Jiří Srba.** ***Note on the Tableau Technique for Commutative Transition Systems*****. December 2001. To appear in the proceedings of FOSSACS '02.**

RS-01-49 **Olivier Danvy and Lasse R. Nielsen.** ***A First-Order One-Pass CPS Transformation*****. 2001. Extended version of a paper to appear in the proceedings of FOSSACS '02.**

RS-01-48 **Mogens Nielsen and Frank D. Valencia.** ***Temporal Concurrent Constraint Programming: Applications and Behavior*****. December 2001. 36 pp.**

RS-01-47 **Jesper Buus Nielsen.** ***Non-Committing Encryption is Too Easy in the Random Oracle Model*****. December 2001. 20 pp.**

RS-01-46 **Lars Kristiansen.** ***The Implicit Computational Complexity of Imperative Programming Languages*****. November 2001. 46 pp.**

RS-01-45 **Ivan B. Damgård and Gudmund Skovbjerg Frandsen.** ***An Extended Quadratic Frobenius Primality Test with Average Case Error Estimates*****. November 2001. 43 pp.**

RS-01-44 **M. Oliver Möller, Harald Rueß, and Maria Sorea.** ***Predicate Abstraction for Dense Real-Time Systems*****. November 2001. 27 pp.**

RS-01-43 **Ivan B. Damgård and Jesper Buus Nielsen.** ***From Known-Plaintext Security to Chosen-Plaintext Security*****. November 2001. 18 pp.**

RS-01-42 **Zoltán Ésik and Werner Kuich.** ***Rationally Additive Semirings*****. November 2001. 11 pp.**

RS-01-41 **Ivan B. Damgård and Jesper Buus Nielsen.** ***Perfect Hiding and Perfect Binding Universally Composable Commitment Schemes with Constant Expansion Factor*****. October 2001. 43 pp.**