RAIRO-Theor. Inf. Appl. 49 (2015) 1–22
DOI: 10.1051/ita/2014024

Available online at:
www.rairo-ita.org

ONE QUANTIFIER ALTERNATION IN FIRST-ORDER LOGIC WITH MODULAR PREDICATES *

Manfred Kufleitner[1] and Tobias Walter[1]

Abstract. Adding modular predicates yields a generalization of first-order logic FO over words. The expressive power of FO[<, MOD] with order comparison $x < y$ and predicates for $x \equiv i \bmod n$ has been investigated by Barrington *et al.* The study of FO[<, MOD]-fragments was initiated by Chaubard *et al.* More recently, Dartois and Paperman showed that definability in the two-variable fragment $\mathrm{FO}^2[<, \mathrm{MOD}]$ is decidable. In this paper we continue this line of work. We give an effective algebraic characterization of the word languages in $\Sigma_2[<, \mathrm{MOD}]$. The fragment Σ_2 consists of first-order formulas in prenex normal form with two blocks of quantifiers starting with an existential block. In addition we show that $\Delta_2[<, \mathrm{MOD}]$, the largest subclass of $\Sigma_2[<, \mathrm{MOD}]$ which is closed under negation, has the same expressive power as two-variable logic $\mathrm{FO}^2[<, \mathrm{MOD}]$. This generalizes the result $\mathrm{FO}^2[<] = \Delta_2[<]$ of Thérien and Wilke to modular predicates. As a byproduct, we obtain another decidable characterization of $\mathrm{FO}^2[<, \mathrm{MOD}]$.

Mathematics Subject Classification. 68Q70, 03D05, 20M35, 68Q45.

1. Introduction

A famous result of McNaughton and Papert says that a language L is definable in first-order logic FO[<] if and only if L is star-free [15]. By a theorem of Schützenberger, L is star-free if and only if its syntactic monoid is aperiodic [20].

Keywords and phrases. Finite monoid, syntactic homomorphism, logical fragment, first-order logic, modular predicate.

* *The first author was supported by the German Research Foundation (DFG) under grant DI 435/5-1.*

[1] University of Stuttgart, FMI, Germany. {kufleitner,walter}@fmi.uni-stuttgart.de

Article published by EDP Sciences

Therefore, since the syntactic monoid is effectively computable and since aperiodicity of finite monoids is decidable, one can verify whether or not a given regular language is definable in FO[<]. Not every regular language is definable in first-order logic FO[<]. In particular, one cannot express group properties such as the words of even length. Verifying whether the length is even corresponds to counting modulo 2. One can think of several ways of adding modular counting modalities to first-order logic. The two most common options are *modular quantifiers* and *modular predicates*. Modular quantifiers yield the logic $\mathrm{FO} + \mathrm{MOD}[<]$, and Straubing, Thérien and Thomas have shown that definability in $\mathrm{FO} + \mathrm{MOD}[<]$ is decidable [28], see also [9] for a more general setting. The expressive power of first-order logic $\mathrm{FO}[<, \mathrm{MOD}]$ with modular predicates was investigated by Barrington, Compton, Straubing and Thérien [2]. They gave an effective characterization of the $\mathrm{FO}[<, \mathrm{MOD}]$-definable languages.

There are several reasons for the study of fragments of first-order logic. With respect to many computational aspects such as the inclusion problem or the satisfiability problem, first-order logic is non-elementary [22]. On the other hand, for many interesting properties, one does not require the full expressive power of FO[<]. For example, when considering the two-variable fragment $\mathrm{FO}^2[<]$, then satisfiability is in NP [33]. From a very general point of view, the study of fragments also helps with the understanding of all regular languages since they often reveal important characteristics of regular languages (which can be present or absent). For example, one such property is the existence of non-trivial groups in the syntactic monoid. In addition, fragments give rise to a descriptive complexity theory inside the regular languages: The easier the formalism for defining a given language L, the easier is L. In the investigation of a fragment $\mathcal{F}$ several questions arise:

1. How can one decide whether a given regular language is definable in $\mathcal{F}$? For example, L is definable in FO[<] if and only if its syntactic monoid is aperiodic.
2. Which languages are definable in $\mathcal{F}$? For example, FO[<] defines precisely the star-free languages.
3. Which other fragment defines the same languages as $\mathcal{F}$? For example, three variables are sufficient for defining any FO[<]-language [10], *i.e.*, FO[<] and $\mathrm{FO}^3[<]$ have the same expressive power.
4. Which closure properties do the $\mathcal{F}$-definable languages have? For example, the FO[<]-definable languages are closed under inverse homomorphisms.
5. What is the complexity of the decision and computation problems for $\mathcal{F}$?

In this paper, we are mainly interested in the first three questions. The fourth question can frequently be answered by a result of Lauser and the first author [13]. Usually logical fragments are defined by restricting some resources in a formula. Typical resources are the number of variables, the quantifier depth, the alternation depth, or the possible atomic predicates. Inside FO[<], for every fixed quantifier depth and every fixed alphabet one can only define a finite number of languages. Therefore, all of the above questions become trivial in this case. Let Σ_n be the set of all first-order formulas in prenex normal form with at most n blocks of quantifiers

TABLE 1. Definability in logical fragments.

Signature	Σ_1	$\mathbb{B}\Sigma_1$	Σ_2	FO^2	FO^2 *vs.* Δ_2	FO
$[<]$	decidable [17]	decidable [21]	decidable [1,18]	decidable [31]	equivalent [31]	decidable [15,20]
$[<, \mathrm{MOD}]$	decidable [4]	decidable [4]	decidable new result	decidable [6]	equivalent new result	decidable [2]

such that the first block is existential, let Π_n be the negations of Σ_n-formulas, and let $\mathbb{B}\Sigma_n$ be the Boolean closure of Σ_n. The fragments Σ_n and $\mathbb{B}\Sigma_n$ define the (quantifier) alternation hierarchy. Over the signature $[<]$, the answer to the second question in case of the alternation hierarchy reveals a surprising connection: A language is definable in $\mathbb{B}\Sigma_n[<]$ if and only if it is on the n^{th} level of the Straubing–Thérien hierarchy [32]. The Straubing–Thérien hierarchy is an infinite hierarchy exhausting the star-free languages [23, 30], and it is tightly connected to the dot-depth hierarchy [24]. The fragments $\Sigma_n[<]$ correspond to the so-called half levels of the Straubing–Thérien hierarchy [18]. Decidability criteria are known only for the very first levels of the alternation hierarchy, *i.e.*, for $\Sigma_1[<]$, for $\mathbb{B}\Sigma_1[<]$ and for $\Sigma_2[<]$, [17,18,21]. Decidability of $\mathbb{B}\Sigma_2[<]$ is one of the major open problems in algebraic automata theory.

When restricting the number of variables, then, by Kamp's Theorem [10], using (and reusing) only three variables has the same expressive power as full first-order logic; this fact is often written as $\mathrm{FO}^3[<] = \mathrm{FO}[<]$. On the other hand, two variables are strictly less powerful. For instance, $(ab)^*$ is definable using three variables but it is not definable in $\mathrm{FO}^2[<]$, the two-variable fragment of $\mathrm{FO}[<]$. Thérien and Wilke have shown that definability in $\mathrm{FO}^2[<]$ is decidable and that $\mathrm{FO}^2[<]$ and $\Delta_2[<]$ have the same expressive power [31]. As usual, a language $L \subseteq A^*$ is definable in $\Delta_2[<]$ if both L and $A^* \setminus L$ are definable in $\Sigma_2[<]$. This is sometimes written as $\Delta_2[<] = \Sigma_2[<] \cap \Pi_2[<]$. In particular, $\Delta_2[<]$ is the largest subclass of $\Sigma_2[<]$ which is closed under complement.

The investigation of fragments over the signature $[<, \mathrm{MOD}]$ with modular predicates was initiated by Chaubard *et al.* [4]. They gave effective algebraic characterizations of $\Sigma_1[<, \mathrm{MOD}]$- and $\mathbb{B}\Sigma_1[<, \mathrm{MOD}]$-definability. Dartois and Paperman [6] showed that it is decidable whether or not a given regular language is definable in $\mathrm{FO}^2[<, \mathrm{MOD}]$. In addition, Dartois and Paperman described the languages definable in $\mathrm{FO}^2[<, \mathrm{MOD}]$. In this paper, we consider the fragment $\Sigma_2[<, \mathrm{MOD}]$. Our first main result is a decidable algebraic characterization of $\Sigma_2[<, \mathrm{MOD}]$. As a second result, we show that $\mathrm{FO}^2[<, \mathrm{MOD}]$ and $\Delta_2[<, \mathrm{MOD}]$ have the same expressive power. This leads to another decidable characterization of $\mathrm{FO}^2[<, \mathrm{MOD}]$. As a byproduct, we give a refinement of Dartois and Paperman's language characterization of $\mathrm{FO}^2[<, \mathrm{MOD}]$. Our proof technique for $\mathrm{FO}^2[<, \mathrm{MOD}]$ is different from the one by Dartois and Paperman. It relies on Mal'cev products with definite and reverse definite semigroups. One cannot expect to obtain decidability results for fragments with modular predicates if there is no such result without modular

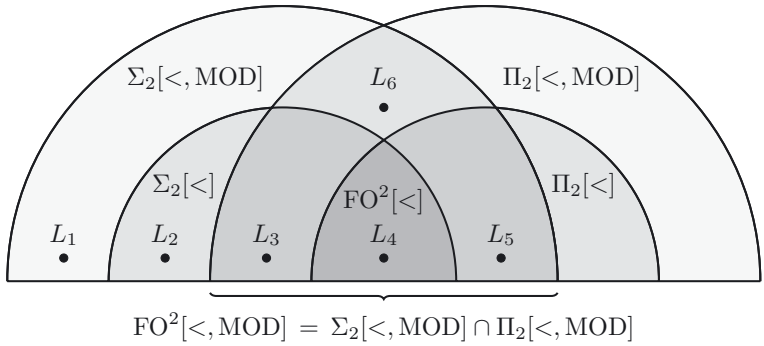
predicates. In this sense, our characterizations complete the picture for the major "small" fragments in the presence of modular predicates, see Table 1.

Naïvely, one could expect that modular predicates can only help with expressing group properties, but this is not true. The following example shows that modular predicates increase the expressive power also within the star-free languages.

Example 1.1. The following six languages are all star-free (even though the given expressions for L_1 and L_5 are using non-trivial star-operations):

$$\begin{aligned} L_1 &= \left(\{a,b\}^2\right)^* \{aa,bb\}\{a,b\}^* & L_4 &= \{a,b\}^* \{ab,ba\}\{a,b\}^* \\ L_2 &= \{a,b\}^* aa \{a,b\}^* & L_5 &= (bc)^* \\ L_3 &= \{a,b\}^* \{aa,bb\}\{a,b\}^* & L_6 &= L_3 \cup L_5. \end{aligned}$$

The definability of these languages in the fragments Σ_2, Π_2 and FO^2 either with or without modular predicates is depicted in the following diagram:



Examples for the remaining two regions can be obtained by complementation of L_1 and L_2. Next, we give formulas φ_i and φ_i' for the languages L_i which justify membership in the respective fragments. We write $\lambda(x)$ for the label of position x. For better readability we define the following macros. Let $\mathrm{suc}(x,y) := x < y \wedge (\forall z\colon z \le x \vee y \le z)$ resemble the successor predicate, the formulas $a(\min) := \forall z\colon \lambda(z) = a \vee (\exists x\colon x < z)$ and $a(\max) := \forall z\colon \lambda(z) = a \vee (\exists x\colon z < x)$ state that the first (resp. last) position in a non-empty word is labeled by a, and for letters a, b we set:

$$\begin{aligned} \varphi_{ab}(x,y) &:= x < y \wedge \lambda(x) = a \wedge \lambda(y) = b \\ \psi_{ab}(x,y) &:= \mathrm{suc}(x,y) \wedge \lambda(x) = a \wedge \lambda(y) = b. \end{aligned}$$

The formula $\varphi_{ab}(x,y)$ says that x is an a-position, y is a b-position, and x is smaller than y. The formula $\psi_{ab}(x,y)$ additionally claims that $y = x+1$. We set:

$$\begin{aligned}
\varphi_1 &:= \exists x \exists y\colon x \equiv 1 \bmod 2 \wedge \big(\psi_{aa}(x,y) \vee \psi_{bb}(x,y)\big) && \in \Sigma_2[<,\mathrm{MOD}]\\
\varphi_2 &:= \exists x \exists y\colon \psi_{aa}(x,y) && \in \Sigma_2[<]\\
\varphi_3 &:= \exists x \exists y\colon \psi_{aa}(x,y) \vee \psi_{bb}(x,y) && \in \Sigma_2[<]\\
\varphi_3' &:= \exists x \exists y\colon x \equiv 1 \bmod 2 \wedge y \equiv 0 \bmod 2 \wedge \lambda(x) = \lambda(y) && \in \Pi_2[<,\mathrm{MOD}]\\
\varphi_4 &:= \exists x \exists y\colon \lambda(x) = a \wedge \lambda(y) = b && \in \mathrm{FO}^2[<]\\
\varphi_5 &:= b(\min) \wedge c(\max) \wedge \forall x \forall y\colon \mathrm{suc}(x,y) \to \big(\varphi_{bc}(x,y) \vee \varphi_{cb}(x,y)\big) && \in \Pi_2[<]\\
\varphi_5' &:= \mathrm{LEN}_0^2 \wedge \forall x\colon \lambda(x) \in \{b,c\} \wedge \big(x \equiv 1 \bmod 2 \leftrightarrow \lambda(x) = b\big) && \in \Sigma_2[<,\mathrm{MOD}].
\end{aligned}$$

Note that $\varphi_3', \varphi_5' \in \mathrm{FO}^2[<,\mathrm{MOD}]$. The formulas for L_6 are just the disjunctions of those for L_3 and L_5. One can show that some language L_i is not definable in some of the above fragments by using the effective algebebraic characterizations of the fragments.

Finally, we remark that the two-variable fragment of first-order logic with modular quantifiers $(\mathrm{FO}{+}\mathrm{MOD})^2[<]$ was characterized by Straubing and Thérien [27], but there is no immediate connection between the decidability results for the fragments $(\mathrm{FO}{+}\mathrm{MOD})^2[<]$ and $\mathrm{FO}^2[<,\mathrm{MOD}]$ since $\mathrm{FO}^2[<,\mathrm{MOD}]$ is not closed under arbitrary inverse homomorphisms. In general, the study of fragments with modular predicates requires so-called $\mathcal{C}$-varieties where $\mathcal{C}$ is the class of length-multiplying homomorphisms, see [8, 13, 26].

2. Preliminaries

Words. Let A be a finite alphabet. Elements of A are *letters*. We denote by A^* the set of all words over A and by A^+ the set of all non-empty words over A. The empty word is ε. Let $w = w_1w_2w_3$ be a factorization, then w_1 is a *prefix*, w_2 a *factor* and w_3 a *suffix* of w. A *language* L is a subset of A^*. Let $|w|$ denote the *length* of a word w and let $w[i]$ be the letter at position $1 \le i \le |w|$, *i.e.*, we have $w = w[1] \cdot w[2] \dots w[|w|]$. The *alphabet* of w is the subset $\alpha(w) = \{w[i] \mid 1 \le i \le |w|\}$ of A. Let

$$T_n(A) = A \times \{1,\dots,n\}.$$

For $w \in A^*$ we define the word $\tau_{j,n}(w) \in T_n(A)^*$ augmented with some additional information by

$$\tau_{j,n}(w) = (w[1], 1 + j \bmod n) \dots (w[|w|], |w| + j \bmod n)$$

and we set $\tau_n(w) = \tau_{0,n}(w)$. One can think of j as an offset when counting the positions modulo n. Words in $T_n(A)^*$ of the form $\tau_{j,n}(w)$ are *well-formed*. For example, $\tau_{1,3}(acbabc) = (a,2)(c,3)(b,1)(a,2)(b,3)(c,1)$ is well-formed. Note that by $i \bmod n$ we denote the unique integer $k \in \{1,\dots,n\}$ satisfying $k \equiv i \bmod n$.

First-order logic with modular predicates. We consider first-order logic FO interpreted over positions of words. The atomic formulas are

$$\top,\ \bot,\ \lambda(x) = a,\ x = y,\ x < y,\ \mathrm{MOD}_i^n(x),\ \mathrm{LEN}_i^n\,.$$

The semantics of $\top$ is *true*, $\bot$ means *false*, $\lambda(x) = a$ states that the position x is labeled by a, $x = y$ means x and y are identical, $x < y$ says that the position x is smaller than the position y, $\mathrm{MOD}_i^n(x)$ holds, if the position x is congruent to i modulo n, and the 0-ary predicate LEN_i^n is true if the length of the word model is congruent to i modulo n. Formulas can be composed by the Boolean connectives and by existential and universal quantifiers. For better readability, we introduce the following macros: We write $x \equiv i \bmod n$ for $\mathrm{MOD}_i^n(x)$, we write $x + j \equiv y \bmod n$ for $\bigwedge_{i=1}^n \big(\mathrm{MOD}_i^n(x) \leftrightarrow \mathrm{MOD}_{i+j}^n(y)\big)$, and for $B \subseteq A$ we use the shortcut $\lambda(x) \in B$ for $\bigvee_{b\in B} \lambda(x) = b$. We consider the negation-free FO fragment $\Sigma_2[<, \mathrm{MOD}]$ of all formulas without an existential quantifier in the scope of a universal quantifier. Over non-empty words, a formula is in $\Sigma_2[<, \mathrm{MOD}]$ if there exists an equivalent formula in prenex normal form having two blocks of quantifiers, starting with a block of existential quantifiers. The fragment $\Pi_2[<, \mathrm{MOD}]$ contains all negation-free formulas without a universal quantifier in the scope of an existential quantifier. A formula is in $\Pi_2[<, \mathrm{MOD}]$ if and only if it is equivalent to the negation of a formula in $\Sigma_2[<, \mathrm{MOD}]$. By $\mathrm{FO}^2[<, \mathrm{MOD}]$ we denote the first-order formulas which use only two variables (say x and y). We write $\mathrm{FO}^2[<, \mathrm{MOD}^n]$ for the formulas in $\mathrm{FO}^2[<, \mathrm{MOD}]$ which use the same modulus n for all modular predicates. For any class of formulas $\mathcal{F}[<, \mathrm{MOD}]$ we write $\mathcal{F}[<]$ for the formulas in $\mathcal{F}[<, \mathrm{MOD}]$ which neither use predicates MOD_i^n nor LEN_i^n. A *sentence* is a formula without free variables. For a sentence φ we write $u \models \varphi$ if φ satisfies u. The language defined by a sentence φ is $L(\varphi) = \{u \in A^* \mid u \models \varphi\}$. Let $\mathcal{F}$ be a subset of FO. A language L is *definable* in $\mathcal{F}$ if there exists a sentence φ in $\mathcal{F}$ such that $L = L(\varphi)$. We say that a language is definable in $\Delta_2[<, \mathrm{MOD}]$ if it is definable in both $\Sigma_2[<, \mathrm{MOD}]$ and $\Pi_2[<, \mathrm{MOD}]$. This is often written as $\Delta_2[<, \mathrm{MOD}] = \Sigma_2[<, \mathrm{MOD}] \cap \Pi_2[<, \mathrm{MOD}]$.

Monoids. Let M be a finite monoid. We assume that every finite monoid is equipped with a partial order $\leq$ which is compatible with multiplication, *i.e.*, $x \leq y$ implies $pxq \leq pyq$ for all $p, q \in M$. Note that equality always yields such a partial order. Therefore, ordered monoids generalize the notation of arbitrary monoids. An element $e \in M$ is *idempotent* if $e^2 = e$. There exists an integer $\omega \geq 1$ (depending on M) such that x^ω is idempotent for every element $x \in M$. A *stability index* of a homomorphism $h : A^* \to M$ is a positive integer s such that $h(A^s) = h(A^{2s})$. Such numbers exist since $h(A)$ generates an idempotent element in the power monoid $\mathcal{P}(M)$ endowed with the multiplication $XY = \{xy \mid x \in X, y \in Y\}$ for $X, Y \subseteq M$. We note that *the* stability index is usually defined as the smallest such number. As all our results hold for every stability index, we refrain from this restriction. The monoid $S = h((A^s)^*) = h(\{\varepsilon\} \cup A^s)$ is called the *stable monoid* of h. Note that S does not dependent on the stability index s. For this purpose, let s' be another stability index; then $h(A^s) = h(A^{ss'}) = h(A^{s'})$.

3. Homomorphisms and recognition

A homomorphism $h : A^* \to M$ to an ordered monoid M *recognizes* a language L if $L = h^{-1}(\downarrow h(L))$. As usual $\downarrow D = \{x \in M \mid \exists y \in D\colon x \leq y\}$ for $D \subseteq M$. Similarly, we say that L is *recognizable* by a monoid M if there exists a homomorphism $h : A^* \to M$ which recognizes L. A language L is regular if and only if it is recognizable by a finite monoid, see *e.g.* [16]. The *syntactic preorder* $\leq_L$ of a language $L \subseteq A^*$ is defined by $u \leq_L v$ if for all $p, q \in A^*$ the following implication holds:

$$pvq \in L \;\Rightarrow\; puq \in L\,.$$

We set $u \equiv_L v$ if both $u \leq_L v$ and $v \leq_L u$. The relation $\equiv_L$ is called the *syntactic congruence* of L, and the quotient $\mathrm{Synt}(L) = A^*/\equiv_L$ is the *syntactic monoid*. The syntactic preorder induces a partial order on $\mathrm{Synt}(L)$ such that the syntactic homomorphism

$$\begin{aligned} h_L : A^* &\to \mathrm{Synt}(L) \\ u &\mapsto \{v \in A^* \mid u \equiv_L v\} \end{aligned}$$

recognizes the language L. The syntactic monoid $\mathrm{Synt}(L)$ is the unique minimal monoid which recognizes L, see *e.g.* [16]. From any reasonable representation of a regular language L (such as nondeterministic finite automata or sentences in monadic second-order logic) one can effectively compute its syntactic homomorphism h_L.

A *positive variety* of finite monoids is a class of finite monoids $\mathbf{V}$ such that $\mathbf{V}$ is closed under direct products, submonoids, and monotone homomorphic images. A *full variety* of finite monoids is a positive variety $\mathbf{V}$ such that $(M, \leq) \in \mathbf{V}$ if and only if $(M, \geq) \in \mathbf{V}$. The order $\geq$ on M is the dual order of $\leq$. Note that $(M, =)$ is a submonoid of the direct product of $(M, \leq)$ and $(M, \geq)$. A monoid M is *aperiodic* if $x^\omega = x^{\omega+1}$ for all $x \in M$. The class of aperiodic monoids is denoted by $\mathbf{A}$. For a monoid M and an idempotent $e \in M$ let M_e be the submonoid of M generated by $\{a \in M \mid e \in MaM\}$. A monoid M is in $\mathbf{DA}$ if $eM_ee = e$ for all idempotents $e \in M$, *i.e.*, if $ese = e$ for all $s \in M_e$; see [7, 29] for further characterizations of $\mathbf{DA}$. A monoid M is in $[\![\, x^\omega y x^\omega \leq x^\omega \,]\!]\, ⓜ\, \mathbf{J_1}$ if $eM_ee \leq e$ for all idempotents $e \in M$, *i.e.*, if $ese \leq e$ for all $s \in M_e$. Usually, one uses relational morphisms for defining Mal'cev products $\mathbf{W}\, ⓜ\, \mathbf{V}$, but in this particular case the current definition is equivalent, *cf.* [7, 18]. We have

$$\mathbf{DA} \subseteq [\![\, x^\omega y x^\omega \leq x^\omega \,]\!]\, ⓜ\, \mathbf{J_1} \subseteq \mathbf{A},$$

and membership in each of the classes is decidable. The classes $\mathbf{A}$ and $\mathbf{DA}$ form full varieties whereas $[\![\, x^\omega y x^\omega \leq x^\omega \,]\!]\, ⓜ\, \mathbf{J_1}$ is a positive variety but not a full variety.

As pointed out by Straubing [25], for $A = \{a, b\}$ the syntactic monoids of $L_1 = \{u \in A^* \mid |u| \equiv 0 \bmod 2\}$ and $L_2 = \{u \in A^* \mid |u|_a \equiv 0 \bmod 2\}$ are both isomorphic to the cyclic group of order 2. Here, $|u|_a$ denotes the number of occurrences of the letter a in u. Since L_1 is definable in first-order logic with modular predicates

(using the sentence LEN_0^2) whereas L_2 is not definable in this logic, the structure of the syntactic monoid cannot be used as a characterization of definability in logical fragments with modular predicates. Instead, we rely on properties of the syntactic homomorphism. Let $\mathbf{V}$ be a variety of finite monoids. A surjective homomorphism $h : A^* \to M$ is in $\mathbf{QV}$ if the stable monoid of h is in $\mathbf{V}$. If membership in $\mathbf{V}$ is decidable, then, since the stable monoid is effectively computable, membership in $\mathbf{QV}$ is decidable. A language is definable in first-order logic with modular predicates if and only if its syntactic homomorphism is in $\mathbf{QA}$, *cf.* [25]. Note that in the above example, the stable monoid of L_1 is the trivial monoid whereas the stable monoid of L_2 is the cyclic group of order two.

Next, we define the class $\mathbf{V} * \mathbf{MOD}$. This is usually done in terms of semidirect products of $\mathbf{V}$ with cyclic groups [3], see also [4]. In this paper we rely on an equivalent approach using a condition on homomorphisms, see Appendix A for a proof of the equivalence. The class $\mathbf{V} * \mathbf{MOD}$ consists of all surjective homomorphisms $h : A^* \to M$ such that there exists an integer $n > 0$ and a homomorphism $g : T_n(A)^* \to N$ with $N \in \mathbf{V}$ satisfying

$$g\big(\tau_n(u)\big) \leq g\big(\tau_n(v)\big) \;\Rightarrow\; h(u) \leq h(v)$$

for all $u, v \in A^*$ with $|u| \equiv |v| \bmod n$. If $\mathbf{V}$ is a full variety, then this means that the image $h(u)$ of the word $u \in A^*$ is uniquely determined by the pair $\big(|u| \bmod n,\, g(\tau_n(u))\big)$. Recall that $T_n(A) = A \times \{1, \ldots, n\}$ and $\tau_n(u)$ is the decoration of the word u with positional information modulo n. Counting starts at offset $j + 1$ when using the notation $\tau_{j,n}(u)$.

Lemma 3.1. *Let $\mathbf{V}$ be a positive variety and let $h : A^* \to M$ be a homomorphism. Suppose there exists an integer $n > 0$ and a homomorphism $g : T_n(A)^* \to N$ with $N \in \mathbf{V}$ such that for all $u, v \in A^*$ with $|u| \equiv |v| \bmod n$ the following implication holds:*

$$\text{If } g\big(\tau_{j,n}(u)\big) \leq g\big(\tau_{j,n}(v)\big) \text{ for all integers } j, \text{ then } h(u) \leq h(v).$$

Then h is in $\mathbf{V} * \mathbf{MOD}$.

Proof. It suffices to consider integers $j \in \{0, \ldots, n-1\}$. Let $g_j : T_n(A)^* \to N$ be the homomorphism induced by $g_j(a, i) = g(a, i + j \bmod n)$ and let $g' : T_n(A)^* \to \prod_{j=0}^{n-1} N$ be defined by $g'(w) = \big(g_0(w), \ldots, g_{n-1}(w)\big)$. Since we have

$$g'(\tau_n(u)) = \big(g(\tau_{0,n}(u)), \ldots, g(\tau_{n-1,n}(u))\big),$$

this completes the proof. □

A construction which forms the basis of our characterizations of $\Sigma_2[<, \mathrm{MOD}]$ and $\mathrm{FO}^2[<, \mathrm{MOD}]$ is the monoid $M_e^{(s)}$. Let $h : A^* \to M$ be a homomorphism with stability index s. The submonoid $M_e^{(s)}$ of M consists of images of words $a_1 \ldots a_k$ under h such that $k \equiv 0 \bmod s$ and for every letter $a_i \in A$ there exist words p_i, q_i with $|p_i| \equiv i - 1 \bmod s$, $|q_i| \equiv -i \bmod s$ and $h(p_i a_i q_i) = e$. We note that, by definition of the stability index, it suffices to consider words p_i, q_i of length less than $2s$. Therefore, $M_e^{(s)}$ is effectively computable.

4. The fragment Σ_2 with modular predicates

In this section we give an effective algebraic characterization of the first-order fragment $\Sigma_2[<, \mathrm{MOD}]$ with modular predicates. Without modular predicates, a language L is definable in $\Sigma_2[<]$ if and only if its syntactic monoid is in $[\![\, x^\omega y x^\omega \leq x^\omega \,]\!]\, @\, \mathbf{J_1}$, see *e.g.* [7]. We show that a similar result holds, involving submonoids of the form $M_e^{(s)}$ instead of M_e.

Theorem 4.1. *Let $h_L : A^* \to M$ be the syntactic homomorphism of $L \subseteq A^*$ and let $s \geq 1$ satisfy $h_L(A^s) = h_L(A^{2s})$. Then the following conditions are equivalent:*

1. *L is definable in $\Sigma_2[<, \mathrm{MOD}]$.*
2. *L is recognized by a homomorphism in $\big([\![\, x^\omega y x^\omega \leq x^\omega \,]\!]\, @\, \mathbf{J_1}\big) * \mathbf{MOD}$.*
3. *h_L satisfies $eM_e^{(s)}e \leq e$ for all idempotents e in M.*

We give the proof of Theorem 4.1 in the remainder of this section. We say that a subset $\mathcal{F}$ of FO forms a *fragment* if $\mathcal{F}$ is closed under conjunctions and disjunctions and if every atomic formula can be replaced by an arbitrary Boolean combination of atomic formulas. We write $\mathcal{F}[<, \mathrm{MOD}]$ if arbitrary atomic formulas are allowed whereas $\mathcal{F}[<]$ indicates that only non-modular atomic formulas are considered. In particular, for every fragment $\mathcal{F}[<]$ we write $\mathcal{F}[<, \mathrm{MOD}]$ for the fragment generated by $\mathcal{F}[<]$ when additionally allowing modular predicates. This notion of fragment is slightly more general than the one introduced in [13]. A fragment $\mathcal{F}[<]$ corresponds to a variety $\mathbf{V}$ if for every language L the following two properties are equivalent: (1) L is definable in $\mathcal{F}$, and (2) its syntactic monoid $\mathrm{Synt}(L)$ is in $\mathbf{V}$.

Proposition 4.2. *Let $L \subseteq A^*$ and suppose that the fragment $\mathcal{F}[<]$ corresponds to the variety $\mathbf{V}$. Then the syntactic homomorphism h_L of L is in $\mathbf{V} * \mathbf{MOD}$ if and only if L is a $\mathcal{F}[<, \mathrm{MOD}]$-definable language.*

Proof. Let φ be a sentence in $\mathcal{F}[<, \mathrm{MOD}]$ which defines L. We can assume that there is a single integer $n > 0$ such that all modular predicates in φ are using the modulus n. Let $j \in \{1, \ldots, n\}$. We replace every occurrence of the atomic predicate $\lambda(x) = a$ in φ by $\lambda(x) \in \{a\} \times \{1, \ldots, n\}$. Similarly, we substitute predicates of the form $x \equiv i \bmod n$ by $\lambda(x) \in A \times \{i\}$. Further we replace LEN_i^n by $\top$ if $i = j$ and by $\bot$ otherwise. The resulting $\mathcal{F}[<]$-sentence φ'_j defines a language $K_j \subseteq T_n(A)^*$. In particular, the syntactic monoid of K_j is in $\mathbf{V}$. Let g_j be the syntactic homomorphism of K_j and let $g = \prod_{j=1}^n g_j$ be the homomorphism defined by $g(u) = (g_1(u), \ldots, g_n(u))$. Consider words $u, v \in A^*$ with $|u| \equiv |v| \bmod n$ and $g\big(\tau_{i,n}(u)\big) \leq g\big(\tau_{i,n}(v)\big)$ for all integers i. Suppose $pvq \models \varphi$ and let $j \equiv |pvq| \bmod n$. Then by construction of φ'_j we have $\tau_n(pvq) \models \varphi'_j$. Since

$$\begin{aligned} g\big(\tau_n(puq)\big) &= g\big(\tau_n(p)\tau_{|p|,n}(u)\tau_{|pu|,n}(q)\big) \\ &\leq g\big(\tau_n(p)\tau_{|p|,n}(v)\tau_{|pu|,n}(q)\big) = g\big(\tau_n(pvq)\big), \end{aligned}$$

we conclude $\tau_n(puq) \models \varphi'_j$. Again by construction of φ'_j we see that $puq \models \varphi$. This shows $h_L(u) \leq h_L(v)$. By Lemma 3.1 we conclude $h_L \in \mathbf{V} * \mathbf{MOD}$.

For the converse let $h_L \in \mathbf{V} * \mathbf{MOD}$. Then there exists an integer $n > 0$ and a homomorphism $g : T_n(A)^* \to N$ with $N \in \mathbf{V}$ such that $g(\tau_n(u)) \leq g(\tau_n(v))$ implies $h(u) \leq h(v)$ for all $u, v \in A^*$ with $|u| \equiv |v| \bmod n$. For every $i \in \{1, \ldots, n\}$ we define

$$K_i = g^{-1}\Big(\downarrow g\big(\{\tau_n(v) \mid v \in L,\ |v| \equiv i \bmod n\}\big)\Big).$$

Since $N \in \mathbf{V}$ and since $\mathbf{V}$ corresponds to $\mathcal{F}[<]$, there exist formulas $\varphi'_i \in \mathcal{F}[<]$ with $K_i = L(\varphi'_i)$. For every formula φ'_i we construct $\varphi_i \in \mathcal{F}[<, \mathrm{MOD}]$ by replacing every atomic proposition $\lambda(x) = (a, j)$ by $\lambda(x) = a \wedge x \equiv j \bmod n$. We set $\varphi = \bigvee_i \big(\varphi_i \wedge \mathrm{LEN}_i^n\big)$. It remains to show $L = L(\varphi)$. Consider $u \in A^*$ with $|u| \equiv i \bmod n$. Then

$$\begin{aligned} u \in L(\varphi) &\Leftrightarrow u \in L(\varphi_i) \\ &\Leftrightarrow \tau_n(u) \in L(\varphi'_i) = K_i \\ &\Leftrightarrow \exists v \in L\colon g\big(\tau_n(u)\big) \leq g\big(\tau_n(v)\big) \text{ and } |v| \equiv i \bmod n \\ &\Leftrightarrow u \in L. \end{aligned}$$

This shows $L = L(\varphi)$ and thus L is $\mathcal{F}[<, \mathrm{MOD}]$-definable. □

Proposition 4.2 shows that the first two conditions in Theorem 4.1 are equivalent. The characterization in terms of $\big(\llbracket\, x^\omega y x^\omega \leq x^\omega \,\rrbracket\, \textcircled{m}\, \mathbf{J_1}\big) * \mathbf{MOD}$ involves some integer n such that positions are counted modulo n. In particular, this characterization of $\Sigma_2[<, \mathrm{MOD}]$ does not immediately yield decidability. Roughly speaking, the following lemma implies that counting modulo any stability index is sufficient.

Lemma 4.3. *Let $L \subseteq A^*$ be recognizable in $\big(\llbracket\, x^\omega y x^\omega \leq x^\omega \,\rrbracket\, \textcircled{m}\, \mathbf{J_1}\big) * \mathbf{MOD}$. Let $h_L : A^* \to M$ be the syntactic homomorphism of $L \subseteq A^*$ and suppose $h_L(A^s) = h_L(A^{2s})$. Then h_L satisfies $eM_e^{(s)}e \leq e$ for all idempotents e.*

Proof. Let $h' : A^* \to M'$ be a homomorphism in $\big(\llbracket\, x^\omega y x^\omega \leq x^\omega \,\rrbracket\, \textcircled{m}\, \mathbf{J_1}\big) * \mathbf{MOD}$ which recognizes L. Then there exists an integer n and a homomorphism $g : T_n(A)^* \to N$ with $N \in \llbracket\, x^\omega y x^\omega \leq x^\omega \,\rrbracket\, \textcircled{m}\, \mathbf{J_1}$ such that for all $u, v \in A^*$ with $|u| \equiv |v| \bmod n$ the following implication holds:

$$g\big(\tau_n(u)\big) \leq g\big(\tau_n(v)\big) \ \Rightarrow\ h'(u) \leq h'(v).$$

If n is a divisor of m, then the homomorphism $\pi : T_m(A)^* \to T_n(A)^*$ induced by the mapping $\pi(a, i \bmod m) = (a, i \bmod n)$ satisfies $\pi(\tau_m(u)) = \tau_n(u)$. Therefore, we can assume that s is a divisor of n and that x^n is idempotent for all $x \in N$. Let $e \in h_L(A^s)$ be idempotent. Consider $a_1 \ldots a_k \in \big(A^s\big)^*$ such that for every letter $a_i \in A$ there exist words p_i and q_i with $|p_i| \equiv i - 1 \bmod s$, $|q_i| \equiv -i \bmod s$ and $h_L(p_i a_i q_i) = e$. Choose $v \in A^s$ such that $h_L(v) = e$. Let $u_i = v^{j_i} p_i a_i q_i v^{j'_i}$ for some integers j_i, j'_i such that $\big|v^{j_i} p_i\big| \equiv i - 1 \bmod n$ and $\big|q_i v^{j'_i}\big| \equiv -i \bmod n$. We set $u = (u_1 \ldots u_k v^n)^n$. Note that $h_L(u) = e$ and that $g(\tau_n(u)) = f$ is

idempotent. Choose $0 \leq j < n$ with $k + j\,|v| \equiv 0 \bmod n$. By construction of u, we have $\alpha\big(\tau_n(a_1 \dots a_k v^j)\big) \subseteq \alpha\big(\tau_n(u)\big)$ and thus $g\big(\tau_n(a_1 \dots a_k v^j)\big) \in N_f$. Since $N \in [\![\, x^\omega y x^\omega \leq x^\omega \,]\!]\, \mathcal{M}\, \mathbf{J_1}$, we have

$$g\big(\tau_n(u\, a_1 \dots a_k v^j u)\big) = g\big(\tau_n(u)\tau_n(a_1 \dots a_k v^j)\tau_n(u)\big) \in fN_f f \leq f = g(\tau_n(u))\,.$$

It follows $h'(u\, a_1 \dots a_k v^j u) \leq h'(u)$. Suppose $puq \in L$ for some words $p, q \in A^*$. Then $pua_1 \dots a_k v^j uq \in L$ since h' recognizes L. This shows

$$e\, h_L(a_1 \dots a_k)\, e = h_L(u\, a_1 \dots a_k v^j u) \leq h_L(u) = e\,.$$

Since all elements in $M_e^{(s)}$ are of the form $h_L(a_1 \dots a_k)$ with $a_1 \dots a_k$ as above, the syntactic homomorphism h_L satisfies $eM_e^{(s)}e \leq e$ for all $e^2 = e$. □

Lemma 4.4. *Let $h : A^* \to M$ be a homomorphism with stability index s such that $eM_e^{(s)}e \leq e$ for all $e^2 = e$. Then $h \in \big([\![\, x^\omega y x^\omega \leq x^\omega \,]\!]\, \mathcal{M}\, \mathbf{J_1}\big) * \mathbf{MOD}$.*

Proof. Let $\pi : T_s(A)^* \to A^*$ be the canonical projection. We say that a letter $(a, i) \in T_s(A)$ has *offset* i. We define a string rewriting system $\Longrightarrow$ over the alphabet $T_s(A)$ as follows. We set $v \Longrightarrow u$ for $u, v \in T_s(A)^+$ if one of the following conditions is satisfied:

1. u is not well-formed or
2. both u and v are well-formed, start and end with the same offset and we have $h(\pi(u)) \leq h(\pi(v))$.

Note that $v \Longrightarrow u$ implies $pvq \Longrightarrow puq$. Moreover, $\Longrightarrow$ is reflexive and transitive. If $v \Longrightarrow u$ with u well-formed, then v is also well-formed. Let $u \sim v$ if both $u \Longrightarrow v$ and $v \Longrightarrow u$. The relation $\sim$ forms a congruence on $T_s(A)^*$. Every $\sim$-class either contains only well-formed words or it contains only non-well-formed words. Moreover, there is only one class of non-well-formed words. Every class of nonempty well-formed words is uniquely determined by the offset of the first letter, the offset of the last letter, and the image under $h \circ \pi$. Therefore, the index of $\sim$ is at most $s^2\,|M| + 2$; note that the empty word has its own class. If u is well-formed, then $h(\pi(u)) = h(\pi(v))$ for all words v with $u \sim v$. In particular, the image $h(\pi([u]))$ of a well-formed $\sim$-class $[u]$ is well-defined. Let $N = T_s(A)^*/\!\sim$. The relation $\Longrightarrow$ induces a partial order relation $\preceq$ on N, *i.e.*, we set $[u] \preceq [v]$ if $v \Longrightarrow u$. By $g : T_s(A)^* \to N$ we denote the natural projection.

Let $f \in N$ be idempotent and let $y \in N_f$. We want to show $fyf \preceq f$. If fyf is not well-formed, then $fyf \preceq f$ by the first type of rules in the definition of $\Longrightarrow$. Hence we may assume that fyf is a class of well-formed words. Since $f^2 = f$, the length of all words in $g^{-1}(f)$ is divisible by s. Let $e = h(\pi(f))$ and $x = h(\pi(y))$. The element $e \in M$ is idempotent and we have $x \in M_e^{(s)}$. To see the latter property, suppose $g(b_1 \dots b_k) = y$ for $b_i \in T_s(A)$. Since all words in $g^{-1}(fyf)$ are well-formed, we have $k \equiv 0 \bmod s$ and $b_1 \dots b_k$ starts and ends with the same offsets as the words in $g^{-1}(f)$. Let $p_i, q_i \in T_s(A)^*$ with $g(p_i b_i q_i) = f$. Since $p_i b_i q_i$ is well-formed, we have $|p_i| \equiv i - 1 \bmod s$ and $|q_i| \equiv -i \bmod s$. Applying the homomorphism π yields

$x = h(\pi(b_1 \dots b_k)) \in M_e^{(s)}$. It follows $exe \leq e$. By definition of $\Longrightarrow$ we conclude $v \Longrightarrow u$ for all $v \in g^{-1}(f)$ and all $u \in g^{-1}(fyf)$. This shows $fyf \preceq f$ as desired. Hence $N \in [\![\, x^\omega y x^\omega \leq x^\omega \,]\!]\, \mathcal{M}\, \mathbf{J_1}$.

We finally show that $g(\tau_s(u)) \preceq g(\tau_s(v))$ implies $h(u) \leq h(v)$ for all $u, v \in A^*$ with $|u| \equiv |v| \bmod s$. To this end, we need to prove that $\tau_s(v) \Longrightarrow \tau_s(u)$ implies $h(u) \leq h(v)$. However, by definition, this holds since $\tau_s(u)$ is well-formed. □

The proof technique used in Lemma 4.4 is quite general, it works as soon as the (ordered) syntactic monoid is available for recognizing the non-wellformed words. We can now combine the results in this section to obtain a proof of Theorem 4.1.

Proof of Theorem 4.1. The first-order fragment $\Sigma_2[<]$ corresponds to the positive variety $[\![\, x^\omega y x^\omega \leq x^\omega \,]\!]\, \mathcal{M}\, \mathbf{J_1}$, see *e.g.* [7]. Therefore, the equivalence of "1" and "2" follows by Proposition 4.2. The implications from "2" to "3" is Lemmas 4.3, and 4.4 shows that "3" implies "2". □

Theorem 4.1 and its dual version for $\Pi_2[<, \mathrm{MOD}]$ immediately lead to the following effective characterization of $\Delta_2[<, \mathrm{MOD}]$-definable languages.

Corollary 4.5. *Let $h_L : A^* \to M$ be the syntactic homomorphism of $L \subseteq A^*$ and let $s \geq 1$ satisfy $h_L(A^s) = h_L(A^{2s})$. Then the following conditions are equivalent:*

1. *L is definable in $\Delta_2[<, \mathrm{MOD}]$.*
2. *h_L satisfies $eM_e^{(s)}e = e$ for all idempotents e in M.*

Proof. The language L is $\Delta_2[<, \mathrm{MOD}]$-definable if, and only if, it is definable in both $\Sigma_2[<, \mathrm{MOD}]$ and $\Pi_2[<, \mathrm{MOD}]$ if, and only if, $eM_e^{(s)}e \leq e$ and $e \leq eM_e^{(s)}e$ for all idempotents $e \in M$ if, and only if, $eM_e^{(s)}e = e$ for all idempotents e. □

5. The fragment FO^2 with modular predicates

Dartois and Paperman have shown that a language is definable in two-variable first-order logic $\mathrm{FO}^2[<, \mathrm{MOD}]$ with modular predicates if and only if its syntactic homomorphism is in **QDA** [6], thereby showing that it is decidable whether or not a given language is definable in $\mathrm{FO}^2[<, \mathrm{MOD}]$. The main result of this section establishes a new effective algebraic characterization of $\mathrm{FO}^2[<, \mathrm{MOD}]$. Since this characterization is the same as the one for $\Delta_2[<, \mathrm{MOD}]$ in Corollary 4.5, this immediately implies that $\mathrm{FO}^2[<, \mathrm{MOD}]$ and $\Delta_2[<, \mathrm{MOD}]$ have the same expressive power. This extends the result of Thérien and Wilke that $\mathrm{FO}^2[<]$ and $\Delta_2[<]$ without modular predicates define the same languages [31].

The equivalence of $\mathrm{FO}^2[<, \mathrm{MOD}]$ and $\Delta_2[<, \mathrm{MOD}]$ does not immediately follow from Proposition 4.2 and the Thérien-Wilke result for two reasons. First, formally Δ_2 is not a fragment. A typical example which illustrates this problem is the language $L = A^*abA^*$ defined by the following $\Sigma_2[<]$-sentence:

$$\varphi := \exists x \exists y \forall z \colon x < y \wedge \lambda(x) = a \wedge \lambda(y) = b \wedge (z \leq x \vee y \leq z).$$

If $A = \{a, b\}$, then L is definable in $\Pi_2[<]$; and if $A = \{a, b, c\}$, then L is not definable in $\Pi_2[<]$. Therefore, saying whether the sentence φ is in $\Delta_2[<]$ is not well-defined. Second, the operation $\mathbf{V} \mapsto \mathbf{V} * \mathbf{MOD}$ is not compatible with intersection, see Example 5.11 below. Therefore, applying Proposition 4.2 to Σ_2 and Π_2 separately does immediately yield a characterization of Δ_2.

Dartois and Paperman proved that the languages in $\mathrm{FO}^2[<, \mathrm{MOD}]$ are exactly the so-called unambiguous modular polynomials. As a byproduct, we refine this result by showing that modular determinism and co-determinism can be used as the sole reason of unambiguity. The proof of our result relies on different techniques than the one by Dartois and Paperman. This new language characterization in terms of modular deterministic and co-deterministic products can be seen as an extension of a corresponding result without modular predicates [14]. Let $L, K \subseteq A^*$ and $a \in A$. The product LaK is *deterministic* if every word in LaK has a unique prefix in La. Symmetrically the product LaK is *co-deterministic* if every word in LaK has a unique suffix in aK. We further introduce a special kind of (co-)deterministic products. The product LaK is *n-modularly deterministic* if all words in L have the same length i modulo n and $(a, i+1) \notin \alpha(\tau_n(L))$, *i.e.*, the letter a in the product LaK is the first occurrence at a position congruent $i+1$ modulo n. A product is *modularly deterministic* if it is n-modularly deterministic for some integer $n \geq 1$.

Modularly co-deterministic and *n-modularly co-deterministic products* are defined symmetrically. It is easy to see that modularly (co-)deterministic products are indeed (co-)deterministic.

Theorem 5.1. *Let $h_L : A^* \to M$ be the syntactic homomorphism of $L \subseteq A^*$ and let $s \geq 1$ satisfy $h_L(A^s) = h_L(A^{2s})$. Then the following conditions are equivalent:*

1. *L is definable in $\mathrm{FO}^2[<, \mathrm{MOD}]$.*
2. *L is recognized by a homomorphism in $\mathbf{DA} * \mathbf{MOD}$.*
3. *h_L satisfies $eM_e^{(s)}e = e$ for all idempotents e in M.*
4. *L is expressible from languages of the form $(A_1 \dots A_s)^*$ for $A_i \subseteq A$ using disjoint unions and s-modularly deterministic and co-deterministic products.*

For the proof of Theorem 5.1 we need additional techniques. First, we define Green's relations which are a classical tool in semigroup theory. Let M be a monoid and let $x, y \in M$. We set $x \leq_{\mathcal{R}} y$ if $xM \subseteq yM$, and we set $x \leq_{\mathcal{L}} y$ if $Mx \subseteq My$. We define similar notions using the stable monoid. Let $h : A^* \to M$ be a homomorphism with stable monoid S. Then we set

$$\begin{aligned} x \leq_{\mathcal{J}^{(s)}} y &\Leftrightarrow SxS \subseteq SyS, \\ x \leq_{\mathcal{R}^{(s)}} y &\Leftrightarrow xS \subseteq yS, \\ x \leq_{\mathcal{L}^{(s)}} y &\Leftrightarrow Sx \subseteq Sy. \end{aligned}$$

Let $\mathcal{G} \in \{\mathcal{J}^{(s)}, \mathcal{R}, \mathcal{R}^{(s)}, \mathcal{L}, \mathcal{L}^{(s)}\}$. Then we set $x \mathcal{G} y$ if both $x \leq_{\mathcal{G}} y$ and $y \leq_{\mathcal{G}} x$. We write $x <_{\mathcal{G}} y$ if $x \leq_{\mathcal{G}} y$ but not $x \mathcal{G} y$. A monoid is *$\mathcal{G}$-trivial* if every $\mathcal{G}$-class contains only one element. It is easy to see that $\leq_{\mathcal{G}}$ is a preorder and $\mathcal{G}$

is an equivalence relation. The relations $\mathcal{R}^{(s)}$ and $\mathcal{L}^{(s)}$ have a similar purpose as the relations $\mathcal{R}_{st}$ and $\mathcal{L}_{st}$ introduced in [6], yet they are not the same. If h is the syntactic homomorphism of the language $(A^2)^*$, then $\mathcal{R}^{(s)}$ and $\mathcal{L}^{(s)}$ are the identity relation (since $S = \{1\}$) whereas $\mathcal{R}_{st}$ and $\mathcal{L}_{st}$ are universal.

Lemma 5.2. *Let $h : A^* \to M$ be a surjective homomorphism with stability index s. If $xh(u)\ \mathcal{R}\ x$ for $u \in (A^s)^*$, then $xh(u)\ \mathcal{R}^{(s)}\ x$. If $h(u)x\ \mathcal{L}\ x$ for $u \in (A^s)^*$, then $h(u)x\ \mathcal{L}^{(s)}\ x$.*

Proof. By left-right symmetry, it suffices to prove the first statement. Let $v \in A^*$ such that $xh(uv) = x$. Let $v' = v(uv)^{s-1}$. Then $v' \in (A^s)^*$ and $xh(uv') = x$. This shows $x \leq_{\mathcal{R}^{(s)}} xh(u)$. □

A typical application of Lemma 5.2 is in the case of $xe\ \mathcal{R}\ x$ or $ex\ \mathcal{L}\ x$ for some idempotent $e \in M$ since then we have $e \in S = h\big((A^s)^*\big)$.

Lemma 5.3. *Let $h : A^* \to M$ be a homomorphism such that $eM_e^{(s)}e = e$ for all idempotents $e \in M$. Then $x\ \mathcal{J}^{(s)}\ e^2 = e$ implies $x^2 = x$.*

Proof. Let S be the stable monoid of h. Consider $u, v \in S$ such that $x = uev$. Since $x\ \mathcal{J}^{(s)}\ e$, there exist $u', v' \in S$ such that $e = u'uevv'$. This shows $u, v \in M_e^{(s)}$. It follows $x^2 = u(evue)v = uev = x$. □

Lemma 5.4. *Let $h : A^* \to M$ be a surjective homomorphism with stability index s, let $\pi : M \to N$ be a surjective homomorphism, and let $g = \pi \circ h : A^* \to N$. Then s is also a stability index of g; and if $eM_e^{(s)}e = e$ for all idempotents $e \in M$, then we have $fN_f^{(s)}f = f$ for all idempotents $f \in N$.*

Proof. We have $g(A^s) = \pi(h(A^s)) = \pi(h(A^{2s})) = g(A^{2s})$. Suppose $eM_e^{(s)}e = e$ for all idempotents $e \in M$. Let $f \in N$ be idempotent and consider a word $a_1 \dots a_k \in A^*$ with $k \equiv 0 \bmod s$ such that there exist $p_i, q_i \in A^*$ with $|p_i| \equiv i - 1 \bmod s$, $|q_i| \equiv -i$ and $g(p_i a_i q_i) = f$. With $u_i = p_i a_i q_i$ we define $u = (u_1 \dots u_k)^n$ for some $n \geq 1$ such that $h(u) = e$ is idempotent. By considering factorizations of u we can choose words $p_i', q_i' \in A^*$ with $|p_i'| \equiv i - 1 \bmod s$, $|q_i'| \equiv -i$ and $h(p_i' a_i q_i') = h(u) = e$. Therefore $h(ua_1 \dots a_k u) = eh(a_1 \dots a_k)e = e = h(u)$. It follows $fg(a_1 \dots a_k)f = \pi(h(ua_1 \dots a_k u)) = \pi(h(u)) = f$ which completes the proof. □

The next lemma is an analogue of a basic property of Green's relations. An $\mathcal{R}^{(s)}$-class is *regular* if it contains an idempotent element.

Lemma 5.5. *Let $h : A^* \to M$ be a homomorphism and let every regular $\mathcal{R}^{(s)}$-class of M be trivial. Then M is $\mathcal{R}^{(s)}$-trivial.*

Proof. Let S be the stable monoid of h and let $x\ \mathcal{R}^{(s)}\ y$. Then there exist $u, v \in S$ such that $xu = y$ and $yv = x$. Since $(uv)^\omega\ \mathcal{R}^{(s)}\ (uv)^\omega u$ is within a regular $\mathcal{R}^{(s)}$-class, we have $(uv)^\omega = (uv)^\omega u$. Hence we conclude $x = yv = xuv = x(uv)^\omega = x(uv)^\omega u = xu = y$. □

Let M be a monoid. For $x, y \in M$ we set $x \sim_K y$ if for every idempotent $e \in M$ we have either $ex = ey$ or $ex, ey <_{\mathcal{R}} e$. Symmetrically, we set $x \sim_D y$ if for every idempotent $e \in M$ we have either $xe = ye$ or $xe, ye <_{\mathcal{L}} e$. The relations $\sim_K$ and $\sim_D$ form congruences [11]. We define Mal'cev products of the semigroup varieties $\mathbf{K}$ and $\mathbf{D}$ and classes of homomorphisms $\mathbf{V}$. A surjective homomorphism $h : A^* \to M$ onto a finite monoid M is in $\mathbf{K} \circledcirc{m} \mathbf{V}$ if $\pi_K \circ h : A^* \to M/\!\sim_K$ is in $\mathbf{V}$. Here, $\pi_K : M \to M/\!\sim_K$ is the natural projection. The definition of $\mathbf{D} \circledcirc{m} \mathbf{V}$ is similar using $\sim_D$. The definition of Mal'cev products usually relies on relational morphisms, but the current approach is equivalent [11]. Let $\mathbf{W}_2$ be the class of homomorphisms $A^* \to M$ onto $\mathcal{R}^{(s)}$-trivial monoids, let $\mathbf{V}_2$ be the class of homomorphisms $A^* \to M$ onto $\mathcal{L}^{(s)}$-trivial monoids, and let $\mathbf{V}_{m+1} = \mathbf{D} \circledcirc{m} \mathbf{W}_m$ and $\mathbf{W}_{m+1} = \mathbf{K} \circledcirc{m} \mathbf{V}_m$ for $m \geq 2$. The definition starts with index $m = 2$ in order to match the corresponding levels of the Trotter-Weil hierarchy, *cf.* [12].

The next lemma shows that a homomorphism $h : A^* \to M$ which satisfies $eM_e^{(s)}e = e$ is within this hierarchy.

Lemma 5.6. *Let $h : A^* \to M$ be a homomorphism satisfying $eM_e^{(s)}e = e$ for all idempotents e. Then $h \in \mathbf{W}_m \cap \mathbf{V}_m$ for some $m \geq 2$.*

Proof. We can assume that M is either not $\mathcal{R}^{(s)}$-trivial or not $\mathcal{L}^{(s)}$-trivial. By induction on the number of non-trivial $\mathcal{R}^{(s)}$- and $\mathcal{L}^{(s)}$-classes we show that after finitely many quotients with $\sim_K$ and $\sim_D$ we obtain a homomorphism in $\mathbf{W}_2 \cap \mathbf{V}_2$. This induction scheme relies on Lemma 5.4.

By left-right symmetry (and using Lemmas 5.3 and 5.5) we can assume that there exist two idempotents $f \neq g$ in M with $f \mathcal{R}^{(s)} g$. Moreover we can choose f and g such that all regular $\mathcal{L}^{(s)}$-classes which are $<_{\mathcal{J}^{(s)}}$-below f are trivial (note that this can be achieved either with $f \mathcal{R}^{(s)} g$ and $\mathcal{L}^{(s)}$-classes below f or with $f \mathcal{L}^{(s)} g$ and $\mathcal{R}^{(s)}$-classes below f, and the latter situation is left-right symmetric). From $f \mathcal{R}^{(s)} g$ we obtain $fg = g$ and $gf = f$.

We want to show $f \sim_D g$. Consider an idempotent $e \in M$. The proof of $f \sim_D g$ consists of two steps. First, we convince ourselves that $fe \mathcal{L} e$ if and only if $ge \mathcal{L} e$. Second, we verify that $fe \mathcal{L} e \mathcal{L} ge$ implies $fe = ge$.

If $fe \mathcal{L} e$, then $fe \mathcal{L}^{(s)} e$ by Lemma 5.2; therefore we have $f \in M_e^{(s)}$ and $e = efe = egfe$. This shows $g \in M_e^{(s)}$ and $ege = e$, *i.e.*, $ge \mathcal{L}^{(s)} e$. This completes the first step. For the second step, we can assume $fe \mathcal{L}^{(s)} e \mathcal{L}^{(s)} ge$ by Lemma 5.2. Since $fe \leq_{\mathcal{J}^{(s)}} f$, there are two possible cases: Either $fe <_{\mathcal{J}^{(s)}} f$ or $fe \mathcal{J}^{(s)} f$. If $fe <_{\mathcal{J}^{(s)}} f$, then, by the assumption on the $\mathcal{L}^{(s)}$-classes $<_{\mathcal{J}^{(s)}}$-below f, we have $fe = e$ and thus $fe = gfe = ge$. If $fe \mathcal{J}^{(s)} f$, then $e \in M_f^{(s)}$ and $fef = f$. This implies $ge = fge = fefge = fe$. In any case, we have $fe = ge$. □

The following lemma shows that certain information is never destroyed by the congruences $\sim_K$ and $\sim_D$. For example, if $h : A^* \to M$ can distinguish the length of a word modulo s, then so does $\pi_K \circ h : A^* \to M/\!\sim_K$. This property is used in the induction scheme of Proposition 5.8.

Lemma 5.7. *Let $h : A^* \to M$ be a homomorphism with stability index s such that $h(u) = h(v)$ implies $|u| \equiv |v| \bmod s$ for all $u, v \in A^*$, and $h(u') = h(v')$ implies $\alpha(\tau_s(u')) = \alpha(\tau_s(v'))$ for all $u', v' \in (A^s)^*$. Let $\pi : M \to M/{\sim_K}$ be the natural projection and let $g = \pi \circ h : A^* \to M/{\sim_K}$. Then $g(u) = g(v)$ implies $|u| \equiv |v| \bmod s$ for all $u, v \in A^*$, and $g(u') = g(v')$ implies $\alpha(\tau_s(u')) = \alpha(\tau_s(v'))$ for all $u', v' \in (A^s)^*$.*

Proof. Let x^n be idempotent for all $x \in M$. Let $u, v \in A^*$ with $g(u) = g(v)$. This means $h(u) \sim_K h(v)$. We have $h(u^{sn}u) \mathcal{R} h(u^{sn})$ and hence $h(u^{sn}u) = h(u^{sn}v)$. This implies $|u| \equiv |u^{sn}u| \equiv |u^{sn}v| \equiv |v| \bmod s$. Similarly, let $u', v' \in (A^s)^*$ with $h(u') \sim_K h(v')$. Then $h(u'^n u') \mathcal{R} h(u'^n)$ and thus $h(u'^n u') = h(u'^n v')$. This yields $\alpha(\tau_s(v')) \subseteq \alpha(\tau_s(u'^n v')) = \alpha(\tau_s(u'^n u')) = \alpha(\tau_s(u'))$. Symmetrically, we have $\alpha(\tau_s(u')) \subseteq \alpha(\tau_s(v'))$. □

Proposition 5.8. *Let $h : A^* \to M$ be a surjective homomorphism with stability index s satisfying the following three properties:*

- *$eM_e^{(s)}e = e$ for all idempotents $e \in M$,*
- *$h(u) = h(v)$ implies $|u| \equiv |v| \bmod s$ for all $u, v \in A^*$, and*
- *$h(u') = h(v')$ implies $\alpha(\tau_s(u')) = \alpha(\tau_s(v'))$ for all $u', v' \in (A^s)^*$.*

If $L \subseteq A^*$ is recognized by h, then L is expressible from the languages $(A_1 \dots A_s)^*$ for $A_i \subseteq A$ using disjoint unions and s-modularly deterministic and co-deterministic products.

Proof. Let $\pi : M \to N = M/{\sim_K}$ be the natural projection and let $g = \pi \circ h : A^* \to N$. By Lemma 5.6, the homomorphism h is in $\mathbf{W}_m$ for some m. If $m > 2$ then we can assume $h \notin \mathbf{V}_{m-1}$, since otherwise we proceed with a symmetric construction using s-modularly co-deterministic products. Therefore, in the case of $m > 2$, we can assume that all g-recognizable languages have the desired property. The homomorphism g satisfies the desired presumptions by Lemma 5.4 and Lemma 5.7.

By induction on $|\alpha(\tau_s(w))|$ we show that for every word w there exists a language L_w with $w \in L_w \subseteq h^{-1}h(w)$ with the desired property such that the number of products is bounded by a function depending on h and $\alpha(\tau_s(w))$, but neither on w nor on $|w|$. In particular, there are only finitely many such languages L_w. Moreover, we ensure $|v| \equiv |w| \bmod s$ and $L_v = L_w$ for all $v \in L_w$. In addition, if $m > 2$, then $v \in L_w$ implies $\alpha(\tau_s(v)) = \alpha(\tau_s(w))$. Note that $|\alpha(\tau_s(w))| = |\alpha(\tau_{j,s}(w))|$ for all integers j.

If $\alpha(\tau_s(w)) = \emptyset$, then $w = \varepsilon$ and we set $L_w = \{\varepsilon\}$. Let now $\alpha(\tau_s(w)) \neq \emptyset$ and consider the factorization $w = w_1 a_1 \dots w_k a_k w'$ with

$$\alpha\big(\tau_{|w_1 a_1 \dots w_{i-1} a_{i-1}|,s}(w_i)\big) \subsetneq \alpha\big(\tau_{|w_1 a_1 \dots w_{i-1} a_{i-1}|,s}(w_i a_i)\big) = \alpha\big(\tau_s(w)\big)$$

such that $k \leq |M|+1$ is minimal satisfying one (or both) of the following properties:

1. $\alpha(\tau_{|w_1 a_1 \dots w_k a_k|,s}(w')) \subsetneq \alpha(\tau_s(w))$.

2. There exists $u \in (A^s)^*$ with $\alpha(\tau_s(w)) \subseteq \alpha(\tau_{|w_1a_1\dots w_ka_k|,s}(u))$ such that $e = h(u)$ is idempotent and $h(w_1a_1 \dots w_ka_k) = h(w_1a_1 \dots w_ka_ku)$.

If property 1. holds, then we set

$$L_w = L_{w_1}a_1 \dots L_{w_k}a_kL_{w'}$$

and this yields $w \in L_w \subseteq h^{-1}h(w)$. If property 1. does not hold for all $k \leq |M|+1$, then we can consider the factorization $w = w_1a_1 \dots w_{|M|+1}a_{|M|+1}w''$. By the pigeonhole principle there exist $j < k \leq |M|+1$ such that $h(w_1a_1 \dots w_ja_j) = h(w_1a_1 \dots w_ka_k)$. In this case we set $u = (w_{j+1}a_j \dots w_ka_k)^{ns}$ for some integer n such that $h(u)$ is idempotent. Therefore, we can assume that property 2. holds and that property 1. does not hold. Write $w' = xy$ such that $|x| < s$ and $|y| \equiv 0 \bmod s$. If $m > 2$ then we set

$$L_w = L_{w_1}a_1 \dots L_{w_k}a_k\, x\, g^{-1}g(y).$$

By definition, we have $w \in L_w$. Let $v \in L_w$ and write $v = v_1a_1 \dots v_ka_kxv'$ with $v_i \in L_{w_i}$ and $h(v') \sim_K h(y)$. In particular, $h(v_i) = h(w_i)$. We choose some word z such that $\alpha(\tau_s(xyz)) \subseteq \alpha(\tau_s(u))$ and $|xyz| \equiv 0 \bmod s$, *i.e.*, we pad xy to an s-divisible length. Then we have $h(xyz) \in M_e^{(s)}$ and thus $eh(xyz)e = e$. We deduce $e\,h(xy)\,\mathcal{R}\,e$ and hence, by $h(xy) \sim_K h(xv')$, we have $e\,h(xy) = e\,h(xv')$. It follows

$$\begin{aligned} h(w) &= h(w_1a_1w_2a_2 \dots w_ka_kxy) \\ &= h(w_1a_1w_2a_2 \dots w_ka_k)eh(xy) \\ &= h(v_1a_1v_2a_2 \dots v_ka_k)eh(xv') = h(v)\,. \end{aligned}$$

This shows $L_w \subseteq h^{-1}h(w)$. The remaining case of the construction is $m = 2$ in the situation where property 2. holds and property 1. does not hold. Let

$$A_i = \{a \mid \exists p, q\colon w = paq \text{ and } |p| \equiv i-1 \bmod s\}$$

be the set of letters which appear in w at a position congruent modulo i and let $j \in \{1, \dots, s\}$ satisfy $j \equiv |w_1a_1 \dots w_ka_kx| \bmod s$. Then we set

$$L_w = L_{w_1}a_1 \dots L_{w_k}a_kx(A_{j+1} \dots A_sA_1 \dots A_j)^*.$$

Again, we trivially have $w \in L_w$. Let $v \in L_w$ and write $v = v_1a_1 \dots v_ka_kxv'$ with $v_i \in L_{w_i}$ and $v' \in (A_{j+1} \dots A_sA_1 \dots A_j)^*$. In particular, $h(v_i) = h(w_i)$. As before, we choose some word z such that $\alpha(\tau_s(xyz)) \subseteq \alpha(\tau_s(u))$ and $|xyz| \equiv 0 \bmod s$, *i.e.*, we pad xy to an s-divisible length. Then we have $h(xyz) \in M_e^{(s)}$ and thus $eh(xyz)e = e$. We deduce $eh(xy)\ \mathcal{R}\ eh(x)$. This implies $eh(xy)\ \mathcal{R}^{(s)}\ eh(x)$ by Lemma 5.2. Since M is $\mathcal{R}^{(s)}$-trivial, we conclude $eh(xy) = eh(x)$. A similar reasoning shows $eh(xv') = eh(x)$. As in the previous case, this yields $h(w) = h(v)$.

Note that all products are s-modularly deterministic. Moreover, in any case if $v \in L_w$, then v admits an equivalent factorization as w; and this yields $L_v = L_w$.

In the case of property 1, this immediately follows by induction whereas the second case also relies on the fact that g preserves the alphabetic information for words of length divisible by s. The prefix $L_{w_1}a_1$ of L_w ensures that the alphabet $\alpha(\tau_s(v))$ is never too small for any word $v \in L_w$. This shows that the union $\bigcup_{w\in L} L_w$ is disjoint and finite, and it coincides with L. □

Lemma 5.9. *Let $L \subseteq A^*$ be expressible in the closure of languages $(A_1 \dots A_n)^*$ for $A_i \subseteq A$ under finite union and modularly (co-)deterministic products. Then L is definable in* $\mathrm{FO}^2[<, \mathrm{MOD}]$.

Proof. The proof is by induction on the expression for $L \subseteq A^*$. The language $(A_1 \dots A_n)^*$ is defined by $\mathrm{LEN}_0^n \wedge \forall x : \bigwedge_{i=1}^n (x \equiv i \bmod n \to x \in A_i)$. Thus consider a modularly deterministic product LaK such that the letter $a \in A$ is at position $i \bmod n$ and there is no such a at a position j with $j \equiv i \bmod n$ in any word of L. We may assume, by using multiples of n, that L and K are expressible as $\mathrm{FO}^2[<, \mathrm{MOD}^n]$-formulas. Let

$$\varrho(y) = \exists x\colon (y < x) \wedge (\forall y\colon \lambda(x) = a \wedge x \equiv i \bmod n \\ \wedge (\lambda(y) = a \wedge y \equiv i \bmod n \to x \leq y)).$$

Then $\varrho(y)$ is used to check if y is left of the position of a. We can relativize L and K using the formula ϱ. Let φ be an $\mathrm{FO}^2[<, \mathrm{MOD}^n]$ formula with $L(\varphi) = L$. We inductively define $\varphi_{<a,i}$ which is true on the deterministic factorization $w = uav$ if φ is true on u. Let

$$(\exists y : \tilde{\varphi})_{<a,i} = \exists y(\varrho(y) \wedge \tilde{\varphi}_{<a,i}) \qquad (\forall y : \tilde{\varphi})_{<a,i} = \forall y(\varrho(y) \to \tilde{\varphi}_{<a,i})$$
$$(\lambda(y) = a)_{<a,i} = \lambda(y) = a \qquad (\mathrm{MOD}_j^n(y))_{<a,i} = \mathrm{MOD}_j^n(y)$$
$$(\hat{\varphi} \wedge \tilde{\varphi})_{<a,i} = \hat{\varphi}_{<a,i} \wedge \tilde{\varphi}_{<a,i} \qquad (\neg\tilde{\varphi})_{<a,i} = \neg\tilde{\varphi}_{<a,i}.$$

Symmetrically we can define $\psi_{>a,i}$ for a formula ψ with $L(\psi) = K$, however we have to change the offset $(\mathrm{MOD}_j^n(y))_{>a,i} = \mathrm{MOD}_{j+i}^n(y)$. The product LaK is now defined by the $\mathrm{FO}^2[<, \mathrm{MOD}^n]$-formula $\exists x\colon (\lambda(x) = a \wedge x \equiv i \bmod s) \wedge \varphi_{<a,i} \wedge \psi_{>a,i}$. □

We can now give a proof of the main result for $\mathrm{FO}^2[<, \mathrm{MOD}]$.

Proof of Theorem 5.1. Since $\mathrm{FO}^2[<]$ corresponds to **DA**, the equivalence of "5.1" and "5.1" follows by Proposition 4.2. "5.1" implies "5.1": As $\mathrm{FO}^2[<]$ and $\Delta_2[<]$ have the same expressive power over finite words, by Lemma 4.3 the syntactic homomorphism h_L satisfies $eM_e^{(s)}e \leq e$ as well as $eM_e^{(s)}e \geq e$. "5.1" implies "5.1": Let $N = (2^A)^s \times (\mathbb{Z}/s\mathbb{Z})$ be the monoid with the following multiplication $(A_1, \dots, A_s, i)\cdot(B_1, \dots, B_s, j) = (A_1 \cup B_{1+i \bmod s}, \dots, A_s \cup B_{s+i \bmod s}, i+j \bmod s)$. Let $\beta : A^* \to N$ be induced by $\beta(a) = (\{a\}, \emptyset, \dots, \emptyset, 1)$. Then $h : A^* \to \mathrm{Synt}(L) \times N$, $u \mapsto (h_L(u), \beta(u))$ satisfies the premise of Proposition 5.8. Therefore, L is of the desired form. "5.1" implies "5.1" follows from Lemma 5.9. □

The following corollary is a consequence of Corollary 4.5 and Theorem 5.1.

Corollary 5.10. *Let $L \subseteq A^*$. Then L is definable in* $\mathrm{FO}^2[<, \mathrm{MOD}]$ *if and only if it is definable in* $\Delta_2[<, \mathrm{MOD}]$.

We note that Corollary 5.10 does not immediately follow from the fact that $\mathrm{FO}^2[<]$ and $\Delta_2[<]$ define the same languages over finite words since, in general, we have $(\mathbf{V} * \mathbf{MOD}) \cap (\mathbf{W} * \mathbf{MOD}) \neq (\mathbf{V} \cap \mathbf{W}) * \mathbf{MOD}$ for varieties $\mathbf{V}$ and $\mathbf{W}$. The following example is due to Dartois and Paperman [5].

Example 5.11. Let $\mathbf{R}$ be the full variety of $\mathcal{R}$-trivial monoids, and let $\mathbf{L}$ be the full variety of $\mathcal{L}$-trivial monoids. The syntactic homomorphism h_L of the language $L = (aa)^*(bb)^*$ is in both $\mathbf{R} * \mathbf{MOD}$ and $\mathbf{L} * \mathbf{MOD}$ but not in $(\mathbf{R} \cap \mathbf{L}) * \mathbf{MOD}$. Furthermore, the stable monoid of h_L is in $\mathbf{R} \cap \mathbf{L}$, *i.e.*, the $\mathcal{J}$-trivial monoids $\mathbf{J} = \mathbf{R} \cap \mathbf{L}$ satisfy $\mathbf{J} * \mathbf{MOD} \neq \mathbf{QJ}$.

Conclusion

In Proposition 4.2 we have shown that the algebra operation $\mathbf{V} \mapsto \mathbf{V} * \mathbf{MOD}$ corresponds to adding modular predicates to a given logical fragment. Unfortunately, this does not immediately help with decidability. In Theorem 4.1 we show that a language $L \subseteq A^*$ is $\Sigma_2[<, \mathrm{MOD}]$-definable if and only if its syntactic homomorphism $h_L : A^* \to M$ satisfies $eM_e^{(s)}e \leq e$ for all idempotents e in M. Since the latter property is decidable, one can effectively determine whether or not a given language is $\Sigma_2[<, \mathrm{MOD}]$-definable. An important intermediate step in proving this decidability result is a characterization of the form $\mathbf{V} * \mathbf{MOD}$.

The characterization of the fragment $\Sigma_2[<, \mathrm{MOD}]$ in Theorem 4.1 immediately leads to an algebraic counterpart of $\Delta_2[<, \mathrm{MOD}]$. By definition, $\Delta_2[<, \mathrm{MOD}]$ is the largest subclass of the $\Sigma_2[<, \mathrm{MOD}]$-definable languages which is closed under complementation. We use this characterization of $\Delta_2[<, \mathrm{MOD}]$ for showing that the two-variable fragment $\mathrm{FO}^2[<, \mathrm{MOD}]$ has the same expressive power. Our proof yields two by-products. First, we characterize the $\mathrm{FO}^2[<, \mathrm{MOD}]$-definable languages in terms of modularly deterministic and co-deterministic products which generalizes a result of Dartois and Paperman. The second by-product is another proof for the decidablity of $\mathrm{FO}^2[<, \mathrm{MOD}]$; this was first shown by Dartois and Paperman [6] using the characterization $\mathbf{QDA}$, *i.e.*, a language is $\mathrm{FO}^2[<, \mathrm{MOD}]$-definable if and only if its stable monoid is in $\mathbf{DA}$. For $\Sigma_2[<, \mathrm{MOD}]$ it is still open whether definability only depends on its stable monoid.

A. Appendix: Semidirect products

In this appendix, we give an approach to the semidirect product $\mathbf{V} * \mathbf{MOD}$ where $\mathbf{V}$ is an arbitrary positive variety of finite monoids and $\mathbf{MOD}$ is some particular class of homomorphisms. Below, we show that the usual definition of $\mathbf{V} * \mathbf{MOD}$ and the definition used in this paper are equivalent. This can be seen as a variant of the so-called *wreath product principle*. An instance of $\mathbf{V} * \mathbf{MOD}$ with $\mathbf{V}$

being a positive variety was already studied by Chaubard, Pin, and Straubing [4], but the proof of the wreath product principle given in [4] is only stated for full varieties $\mathbf{V}$. Pin and Weil studied semidirect products $\mathbf{V} * \mathbf{W}$ of varieties $\mathbf{V}$ and $\mathbf{W}$ such that $\mathbf{V}$ is a positive variety [19]. On the other hand, semidirect products $\mathbf{V} * \mathbf{W}$ with $\mathbf{W}$ being a class of homomorphism were introduced by Chaubard, Pin, and Straubing [3], see also [8]. The case $\mathbf{V} * \mathbf{W}$ where $\mathbf{V}$ is a positive variety and where $\mathbf{W}$ is a class of homomorphisms can therefore be seen as a conjunction of [3, 19]. We restrict ourselves to the case $\mathbf{W} = \mathbf{MOD}$.

We introduce semidirect products in terms of wreath products. Let N and K be monoids such that N is ordered. Then the *wreath product* $N \wr K$ is the set $N^K \times K$ with the composition

$$(f_1, k_1)(f_2, k_2) = (f, k_1 k_2) \quad \text{with} \quad f(k) = f_1(k) f_2(k k_1).$$

The order on $N \wr K$ is defined by

$$(f_1, k_1) \leq (f_2, k_2) \quad \text{if} \quad k_1 = k_2 \text{ and } f_1(k) \leq f_2(k) \text{ for all } k \in K.$$

Let $\mathbf{V}$ be a class of finite ordered monoids and let $\mathbf{W}$ be a class of homomorphisms of the form $h : A^* \to K$, so-called *stamps*. A surjective homomorphism $h : A^* \to M$ belongs to the *semidirect product* $\mathbf{V} * \mathbf{W}$ if there exists a homomorphism $\hat{h} : A^* \to N \wr K$ such that

- $N \in \mathbf{V}$,
- $\pi_2 \circ \hat{h} : A^* \to K$ is a homomorphism in $\mathbf{W}$; and
- the following implication holds for all $u, v \in A^*$:

$$\hat{h}(u) \leq \hat{h}(v) \;\Rightarrow\; h(u) \leq h(v).$$

Here, π_i denotes the projection to the i-th component. Let $\mathbf{MOD}$ be the class of all homomorphism $h : A^* \to \mathbb{Z}/n\mathbb{Z}$ such that $h(a) = h(b)$ for all letters $a, b \in A$. As usual, $\mathbb{Z}/n\mathbb{Z}$ denotes the cyclic group of order n, implemented using addition modulo n.

Proposition A.1. *Let $\mathbf{V}$ be a positive variety of finite monoids and let $h : A^* \to M$ be a homomorphism onto a finite ordered monoid M. We have $h \in \mathbf{V} * \mathbf{MOD}$ if and only if there exists an integer $n > 0$ and a homomorphism $g : T_n(A)^* \to N$ with $N \in \mathbf{V}$ satisfying*

$$g\big(\tau_n(u)\big) \leq g\big(\tau_n(v)\big) \;\Rightarrow\; h(u) \leq h(v)$$

for all $u, v \in A^*$ with $|u| \equiv |v| \bmod n$.

Proof. For the implication from left to right let $\hat{h} : A^* \to N \wr (\mathbb{Z}/n\mathbb{Z})$ be a homomorphism with $N \in \mathbf{V}$ and $\pi_2 \circ \hat{h}(a) = d$ for all $a \in A$, and suppose that $\hat{h}(u) \leq \hat{h}(v)$ implies $h(u) \leq h(v)$ for all $u, v \in A^*$. Let $\hat{h}(a) = (f_a, d)$ for $f_a \in N^{\mathbb{Z}/n\mathbb{Z}}$. For a function $f \in N^{\mathbb{Z}/n\mathbb{Z}}$ and $i \in \mathbb{Z}/n\mathbb{Z}$ we define $i \cdot f \in N^{\mathbb{Z}/n\mathbb{Z}}$ by

$$(i \cdot f)(k) = f(k + i).$$

Using this notation we define $g : T_n(A)^* \to N^{\mathbb{Z}/n\mathbb{Z}}$ by $g(a,i) = (i-1)d \cdot f_a$ for $(a,i) \in T_n(A)$. The composition in $N^{\mathbb{Z}/n\mathbb{Z}}$ is the componentwise composition of N; we have $N^{\mathbb{Z}/n\mathbb{Z}} \in \mathbf{V}$ since $\mathbf{V}$ is closed under direct products. For every word $u = a_1 \dots a_k$ with $a_i \in A$, the definition of the wreath product and the definition of g yields

$$\pi_1 \circ \hat{h}(u) = f_{a_1}\big(d \cdot f_{a_2}\big)\big(2d \cdot f_{a_3}\big) \dots \big((k-1)d \cdot f_{a_k}\big) = g\big(\tau_n(u)\big).$$

Consider words $u, v \in A^*$ with $|u| \equiv |v| \bmod n$ and $g\big(\tau_n(u)\big) \leq g\big(\tau_n(v)\big)$. Then

$$\hat{h}(u) = \big(g(\tau_n(u)),\, d\,|u| \bmod n\big) \leq \big(g(\tau_n(v)),\, d\,|v| \bmod n\big) = \hat{h}(v)$$

and thus $h(u) \leq h(v)$.

For the implication from right to left let n, N, and g be as in the statement of the proposition. For every letter $a \in A$ we define $f_a \in N^{\mathbb{Z}/n\mathbb{Z}}$ by $f_a(k) = g(a, k+1)$. This yields the homomorphism $\hat{h} : A^* \to N \wr (\mathbb{Z}/n\mathbb{Z})$ with

$$\hat{h}(a) = (f_a, 1).$$

As before, for a function $f \in N^{\mathbb{Z}/n\mathbb{Z}}$ and $i \in \mathbb{Z}/n\mathbb{Z}$ we define $i \cdot f \in N^{\mathbb{Z}/n\mathbb{Z}}$ by $(i \cdot f)(k) = f(k+i)$. Consider a word $u = a_1 \dots a_k$ with $a_i \in A$. Then $\hat{h}(u) = (f, |u| \bmod n)$ with

$$f = f_{a_1}(1 \cdot f_{a_2})(2 \cdot f_{a_3}) \dots \big((k-1) \cdot f_{a_k}\big).$$

By definition of the functions f_{a_i} we have $f(0) = g(\tau_n(u))$. Therefore, for all words $u, v \in A^*$, if $\hat{h}(u) \leq \hat{h}(v)$, then $|u| \equiv |v| \bmod n$ and $g(\tau_n(u)) \leq g(\tau_n(v))$, and thus $h(u) \leq h(v)$. □

Acknowledgements. We thank Luc Dartois, Alexander Lauser, and Charles Paperman for several fruitful discussions on modular predicates, we thank Volker Diekert for discussions on the proof of Lemma 5.6, and we are grateful to the anonymous referees for numerous suggestions which helped to improve the presentation of this paper.

References

[1] M. Arfi, Opérations polynomiales et hiérarchies de concaténation. *Theor. Comput. Sci.* **91** (1991) 71–84.
[2] D.A.M. Barrington, K.J. Compton, H. Straubing and D. Thérien, Regular languages in NC^1. *J. Comput. Syst. Sci.* **44** (1992) 478–499.
[3] L. Chaubard, J.-É. Pin and H. Straubing, Actions, wreath products of $\mathcal{C}$-varieties and concatenation product. *Theor. Comput. Sci.* **356** (2006) 73–89.
[4] L. Chaubard, J.-É. Pin and H. Straubing, First order formulas with modular predicates. In *Proc. of LICS 2006.* IEEE Computer Society (2006) 211–220.
[5] L. Dartois and C. Paperman, Personal communication (2013).
[6] L. Dartois and C. Paperman, Two-variable first order logic with modular predicates over words, in *Proc. of STACS 2013,* vol. 20 of *LIPIcs.* Dagstuhl Publishing (2013) 329–340.
[7] V. Diekert, P. Gastin and M. Kufleitner, A survey on small fragments of first-order logic over finite words. *Int. J. Found. Comput. Sci.* **19** (2008) 513–548.
[8] Z. Ésik and M. Ito, Temporal logic with counting and the degree of aperiodicity of finite automata. *Acta Cybernetica* **16** (2003) 1–28.

[9] Z. Ésik and K.G. Larsen, Regular languages definable by Lindström quantifiers. *RAIRO: ITA* **37** (2003) 179–241.
[10] J.A.W. Kamp, *Tense Logic and the Theory of Linear Order*. Ph.D. thesis, University of California (1968).
[11] K. Krohn, J.L. Rhodes and B. Tilson, Homomorphisms and semilocal theory. In Chapter 8 of *Algebraic Theory of Machines, Languages, and Semigroups*. Academic Press (1968) 191–231.
[12] M. Kufleitner and A. Lauser, The join levels of the Trotter-Weil hierarchy are decidable. In *Proc. of MFCS 2012*, vol. 7464. *Lect. Notes Comput. Sci.* Springer (2012) 603–614.
[13] M. Kufleitner and A. Lauser, Lattices of logical fragments over words. In *Proc. of ICALP 2012*, vol. 7392. *Lect. Notes Comput. Sci.* Springer (2012) 275–286.
[14] M. Kufleitner and P. Weil, On logical hierarchies within FO^2-definable languages. *Logical Methods Comput. Sci.* **8** (2012).
[15] R. McNaughton and S. Papert, Counter-Free Automata. The MIT Press, Cambridge, Mass. (1971).
[16] J.-É. Pin, Varieties of Formal Languages. North Oxford Academic, London (1986).
[17] J.-É. Pin, A variety theorem without complementation, in *Russian Math. (Iz. VUZ)* **39** (1995) 80–90.
[18] J.-É. Pin and P. Weil. Polynomial closure and unambiguous product. *Theory Comput. Syst.* **30** (1997) 383–422.
[19] J.-É. Pin and P. Weil, Semidirect products of ordered semigroups. *Commun. Algebra* **30** (2002) 149–169.
[20] M. P. Schützenberger, On finite monoids having only trivial subgroups. *Inf. Control* **8** (1965) 190–194.
[21] I. Simon, Piecewise testable events, in *2nd GI Conf. of Autom. Theor. Form. Lang.*, vol. 33. *Lect. Notes Comput. Sci.* Springer (1975) 214–222.
[22] L.J. Stockmeyer, *The complexity of decision problems in automata theory and logic*. Ph.D. thesis, TR 133, M.I.T., Cambridge (1974).
[23] H. Straubing, A generalization of the Schützenberger product of finite monoids. *Theor. Comput. Sci.* **13** (1981) 137–150.
[24] H. Straubing, Finite semigroup varieties of the form $\mathbf{V} * \mathbf{D}$. *J. Pure Appl. Algebra* **36** (1985) 53–94.
[25] H. Straubing, Finite Automata, Formal Logic, and Circuit Complexity. Birkhäuser, Boston, Basel and Berlin (1994).
[26] H. Straubing, On logical descriptions of regular languages, in *Proc. of LATIN 2002*, vol. 2286. *Lect. Notes Comput. Sci.* Springer (2002) 528–538.
[27] H. Straubing and D. Thérien, Regular languages defined by generalized first-order formulas with a bounded number of bound variables. *Theory Comput. Syst.* **36** (2003) 29–69.
[28] H. Straubing, D. Thérien and W. Thomas, Regular languages defined with generalized quantifiers. *Inf. Comput.* **118** (1995) 289–301.
[29] P. Tesson and D. Thérien, Diamonds are forever: The variety DA. In *Proc. of Semigroups, Algorithms, Automata and Languages 2001*. World Scientific (2002) 475–500.
[30] D. Thérien, Classification of finite monoids: The language approach. *Theor. Comput. Sci.* **14** (1981) 195–208.
[31] D. Thérien and Th. Wilke, Over words, two variables are as powerful as one quantifier alternation. In *Proc. of STOC 1998*. ACM Press (1998) 234–240.
[32] W. Thomas, Classifying regular events in symbolic logic. *J. Comput. Syst. Sci.* **25** (1982) 360–376.
[33] Ph. Weis, *Expressiveness and succinctness of first-order logic on finite words*. Ph.D. thesis, University of Massachusetts Amherst (2011).

Communicated by P. Weil.
Received October 17, 2013. Accepted June 18, 2014.