Two-variable first order logic with modular predicates over words*

Luc Dartois[1] and Charles Paperman[1]

1 LIAFA, Université Paris-Diderot and CNRS,
Case 7014, 75205 Paris Cedex 13, France
luc.dartois,charles.paperman@liafa.univ-paris-diderot.fr

Abstract

We consider first order formulae over the signature consisting of the symbols of the alphabet, the symbol $<$ (interpreted as a linear order) and the set MOD of modular numerical predicates. We study the expressive power of $\mathbf{FO}^2[<, \mathrm{MOD}]$, the two-variable first order logic over this signature, interpreted over finite words. We give an algebraic characterization of the corresponding regular languages in terms of their syntactic morphisms and we also give simple unambiguous regular expressions for them. It follows that one can decide whether a given regular language is captured by $\mathbf{FO}^2[<, \mathrm{MOD}]$. Our proofs rely on a combination of arguments from semigroup theory (stamps), model theory (Ehrenfeucht-Fraïssé games) and combinatorics.

1998 ACM Subject Classification F.4.3 Formal Languages

Keywords and phrases First order logic, automata theory, semigroup, modular predicates

Digital Object Identifier 10.4230/LIPIcs.STACS.2013.329

Following the pioneering work of Büchi [3], McNaughton and Papert [11] and Thomas [21], the study of the expressive power of fragments of first order logic has grown up to an important topic of automata theory. Part of the main results for finite words are summarized in the table below. They are concerned with the signature $[<]$ (the "sequential calculus" first considered by Büchi) and $[<, \mathrm{MOD}]$, where MOD stands for the set of modular predicates. The fragments of interest include $\mathbf{\Sigma}_1$, the set of existential formulae, its Boolean closure $\mathcal{B}\mathbf{\Sigma}_1$, the set $\mathbf{FO}$ of first order formulae and its restriction $\mathbf{FO}^2$ to two-variable formulae. As shown in the table below, all the corresponding fragments are already known to be decidable except for the class $\mathbf{FO}^2[<, \mathrm{MOD}]$, which is the topic of this paper.

	$\mathbf{\Sigma_1}$	$\mathcal{B}\mathbf{\Sigma}_1$	$\mathbf{FO}^2$	$\mathbf{FO}$
$[<]$	Decidable [12, 21]	Decidable [17, 21]	Decidable [20]	Decidable [11, 15]
$[<, \mathrm{MOD}]$	Decidable [4]	Decidable [4]	Decidable **New result**	Decidable [18, 2]

We also give an algebraic characterization of $\mathbf{FO}^2[<, \mathrm{MOD}]$ (Theorem 6), a description of the corresponding languages as unambiguous regular expressions (Proposition 31) and

* The authors are supported by the project ANR 2010 BLAN 0202 02 FREC, the second author is supported by Fondation CFM.

30th Symposium on Theoretical Aspects of Computer Science (STACS'13).
Editors: Natacha Portier and Thomas Wilke; pp. 329–340

Leibniz International Proceedings in Informatics
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany


an equivalent definition in terms of a suitable variant of temporal logic (Proposition 30). Our algebraic characterization $\mathbf{QDA} = \mathbf{FO}^2[<, \mathrm{MOD}]$ can be viewed as an extension of two known results (a) $\mathbf{QA} = \mathbf{FO}[<, \mathrm{MOD}]$ proved in [2, 18] and (b) $\mathbf{DA} = \mathbf{FO}^2[<]$ proved in [5, 20]. However, it is not easy to extend the proofs of these equalities to our case. For instance, the proof of (a) makes use of the successor relation, which is not expressible in $\mathbf{FO}^2[<]$. Therefore our proof is closer to the proof of (b) but some technical difficulties still have to be worked out (See Section 5).

1 Preliminaries

1.1 Words and logic

Let A be a finite alphabet. We denote by A^* the set of all finite words over A and 1 the empty word. Given a word $u = a_0 \cdots a_{n-1}$ of length n, we denote by $\alpha(u)$ the set of letters of A occurring in u. We associate to u the *relational structure* $M_u = \{[0, n-1], \sigma\}$, where $[i, j]$ is the set of integers between i and j and σ is the truth table of the predicates over u. Basic examples of predicates are the binary predicate $<$, which is the usual order on integers, and $(\mathbf{a})_{a \in A}$ that are disjoint monadic predicates marking the positions of the letters over the structure. For instance, if $u = aabbab$, then $\mathbf{a} = \{0, 1, 4\}$ and $\mathbf{b} = \{2, 3, 5\}$. We also consider the modular predicate MOD_i^d, which holds at all positions equal to i modulo d, and the 0-ary predicate D_i^d which is true if the word has length equals to i modulo d. For $u = aabbab$, we have $MOD_0^2 = \{0, 2, 4\}$, and D_1^3 is *false* whereas D_0^3 is *true*. We denote by MOD the set of these *modular* predicates.

First order formulae are interpreted on words in the usual way (see [18]). For instance the formula $\exists x\ \exists y\ \exists z\ a(x) \wedge b(y) \wedge a(z) \wedge x < y \wedge y < z$ defines the language $A^*aA^*bA^*aA^*$.

In this article, we focus on the first order formulae containing only two different variables. The subsequent logic is denoted by $\mathbf{FO}^2[<]$. For instance the two-variable formula $\exists x\ \exists y\ a(x) \wedge b(y) \wedge x < y \wedge (\exists x \wedge a(x) \wedge y < x)$ also defines the language $A^*aA^*bA^*aA^*$ of the previous example. The first order logic with the order predicate can be enriched with modular predicates. We denote by $\mathbf{FO}[<, \mathrm{MOD}]$ (resp. $\mathbf{FO}^2[<, \mathrm{MOD}]$) the logic built with the same atomic propositions that $\mathbf{FO}[<]$ (resp. $\mathbf{FO}^2[<]$) except that we allow the modular predicates. For instance the formula $\exists x\ \exists y\ \exists z\ a(x) \wedge MOD_0^2(x) \wedge b(y) \wedge a(z) \wedge x < y \wedge y < z$ defines the language $(A^2)^*aA^*bA^*aA^*$.

Note that if required by context, we will specify the alphabet, denoting it between parentheses. For instance $\mathbf{FO}[<](B^*)$ denotes the set of the languages of B^* definable by a formula of $\mathbf{FO}[<]$.

1.2 Algebraic notions

We recall in this section the algebraic notions used in this paper.

1.2.1 Semigroups and recognizable languages

We refer to [13] for the standard definitions of semigroup theory. A *semigroup* is a set equipped with a binary associative operation, which we will denote multiplicatively. A *monoid* is a semigroup with a neutral element 1. Given a semigroup S, we denote by S^1 either S if S is already a monoid or the monoid obtained by adding a neutral element 1 to S otherwise. Recall that a monoid M *divides* another monoid N if M is a quotient of a submonoid of N. This defines a partial order on finite monoids.

A *stamp* is a surjective monoid morphism from A^* onto a finite monoid. A language L is *recognized* by a finite monoid M if there exists a stamp $\varphi : A^* \to M$ and a subset P of M such that $L = \varphi^{-1}(P)$. A language is *recognizable* if it is recognized by a finite monoid. Kleene's theorem states that the set of recognizable languages is exactly the set of rational (or regular) languages. The syntactic congruence of a regular language L of A^* is the equivalence relation $\equiv_L$ defined as follow:

$$u \equiv_L v \text{ if and only if for all } w, w' \in A^*, wuw' \in L \Leftrightarrow wvw' \in L.$$

The monoid $A^*/\equiv_L$ is the *syntactic monoid* of L and the morphism $\varphi : A^* \to A^*/\equiv_L$ is the *syntactic stamp*.

1.2.2 Stability index, stable semigroup, stable automaton

For a stamp $\varphi : A^* \to M$, the set $\varphi(A)$ is an element of the powerset monoid of M. As such it has an idempotent power. The *stability index* of a stamp is the least positive integer s such that $\varphi(A^s) = \varphi(A^{2s})$. This set is therefore a semigroup called the *stable semigroup* of φ. Stable semigroups are strongly related to *stable automata*, defined as follows. Let $\mathcal{A} = (Q, A, \cdot)$ be a deterministic automaton and let k be a positive integer. The *k-automaton* of $\mathcal{A}$ is the deterministic automaton $\mathcal{A}_k = (Q, A^k, \cdot^k)$ where $q \cdot^k (a_1 a_2 \cdots a_k) = (\cdots (q \cdot a_1) \cdot a_2) \cdots) \cdot a_k)$. Note that if M is the transition monoid of $\mathcal{A}$, and M_k the transition monoid of $\mathcal{A}_k$, then M_k is the submonoid of M generated by the image elements of words of length k in M.

▶ **Definition 1.** Let $\mathcal{A} = (Q, B, \cdot)$ be a deterministic automaton. We say that $\mathcal{A}$ is *stable* if for any two-letter word, there exists a letter that has the same action over the set Q, and conversely for any letter of B, there exists a word of B^2 that has the same action over Q.

As shown in the next proposition, this definition is a compatible translation of the stable semigroup for an automaton.

▶ **Proposition 2.** *Let $\mathcal{A}$ be a deterministic automaton. Then, there is an integer k such that the associated k-automaton is stable.*

The least k which satisfies this proposition is called the *stability index* of the automaton. It is equal to the stability index of the associated stamp.

1.2.3 Stamps and varieties

A (pseudo) variety of (finite) monoids is a class of monoids closed under division and finite products. According to Eilenberg [6], a *variety of languages* $\mathcal{V}$ is a class of languages closed under finite union, intersection and complementation, and closed under inverse of monoid morphism. This means that, for any monoid morphism $\varphi : A^* \to B^*$, $X \in \mathcal{V}(B^*)$ implies $\varphi^{-1}(X) \in \mathcal{V}(A^*)$. Furthermore Eilenberg [6] proved that there is a one-to-one correspondence between varieties of monoids and varieties of languages.
The class of languages $\mathbf{FO}^2[<, \mathrm{MOD}]$ is not closed under inverse morphisms, and the Eilenberg's varieties theory does not apply. Still, this class is closed under inverse of length-multiplying morphisms (shortened as *lm*-morphisms), and an algebraic characterization can be obtained by considering a more general framework : the theory of $\mathcal{C}$-varieties independently introduced by Esik and Ito [7] and Straubing [19] and developed by Pin and Straubing [14].

Let us now recall the notion of variety of stamps. A morphism $\alpha : A^* \to B^*$ is *length-multiplying* if there exists an integer n such that for any letter a of A, $\varphi(a)$ is a word of B^n. Given two stamps $\varphi : A^* \to M$ and $\psi : A^* \to N$, the product stamp is the stamp $\eta : A^* \to M \times N$ defined by $\eta(a) = (\varphi(a), \psi(a))$. A stamp $\varphi : A^* \to M$ lm-divides another stamp $\psi : B^* \to N$ if and only if there exists a pair (α, β) such that α is a lm-morphism from A^* to B^*, $\beta : N \to M$ is a partial onto monoid morphism and $\varphi = \beta \circ \psi \circ \alpha$. The couple (α, β) is called an lm-division.
Then a lm-variety of stamps is a class of stamps containing the trivial stamp and closed under lm-division and finite product. Note that if $\mathbf{V}$ is a variety of monoids, then the class of all stamps whose image is a monoid in $\mathbf{V}$ forms a lm-variety of stamps, also denoted $\mathbf{V}$. Moreover, given a lm-variety of stamps $\mathbf{V}$, the class $\mathcal{V}$ of all languages recognized by a stamp in $\mathbf{V}$ is a lm-variety of languages. The correspondence $\mathbf{V} \to \mathcal{V}$ is one-to-one and onto [19]. These notions are very useful to decide membership problems for regular languages. Let us recall a few examples.

▶ **Example 3.** A monoid M is *aperiodic* if there exists an integer n such that for any $x \in M$, $x^n = x^{n+1}$. It has been proved by Schützenberger [15] and McNaughton and Papert [11] that the class of aperiodic monoids forms a variety called $\mathbf{A}$ and the corresponding variety of languages is exactly the first-order definable languages, with the order and letter predicates.

▶ **Example 4.** Let $\mathbf{DA}$ be the variety of monoids satisfying the equation $(xy)^\omega = (xy)^\omega x (xy)^\omega$ where ω is the idempotent power of the monoid. Alternatively $\mathbf{DA}$ is the variety of monoids whose regular $\mathcal{D}$-classes are aperiodic semigroups. The corresponding variety of languages $\mathcal{DA}$ is the class of $\mathbf{FO}^2[<]$-definable languages [20] or equivalently the unambiguous star-free languages [16].

▶ **Example 5.** Given a variety $\mathbf{V}$, the set of all stamps whose stable semigroup is in $\mathbf{V}$ forms a lm-variety of stamps denoted by $\mathbf{QV}$. A language L has its syntactic stamp in $\mathbf{QV}$ if and only if there is an automaton $\mathcal{A}$ recognizing L and a positive integer k such that the k-automaton of $\mathcal{A}$ has its transition monoid in $\mathbf{V}$. Straubing proved in [18] that a language is definable in $\mathbf{FO}[<, \mathrm{MOD}]$ if and only if its syntactic stamp belongs to the lm-variety of stamps $\mathbf{QA}$. We always denote by $\mathcal{QV}$ the lm-variety of languages associated to $\mathbf{QV}$.

2 Main result

Our main result extends the algebraic characterization of $\mathbf{FO}^2[<]$-definable languages by Thérien and Wilke [20] to $\mathbf{FO}^2[<, \mathrm{MOD}]$-definable languages. The next theorem states that the languages definable in $\mathbf{FO}^2[<, \mathrm{MOD}]$ are exactly the languages whose syntactic stamp is in $\mathbf{QDA}$.

▶ **Theorem 6.** $\mathbf{FO}^2[<, \mathrm{MOD}] = \mathbf{QDA}$

Given a regular language (given by a regular expression or by some finite automaton), one can effectively compute the stable semigroup of its syntactic stamp. Since membership in $\mathbf{DA}$ is decidable we get the following corollary.

▶ **Corollary 7.** *Given a regular language L, one can decide whether L is $\mathbf{FO}^2[<, \mathrm{MOD}]$-definable.*

In Section 3 we will give intuition of the power of the modular predicates. The first inclusion $\mathbf{FO}^2[<, \mathrm{MOD}] \subseteq \mathbf{QDA}$ will be proved in Section 4, using general arguments on automata and logic. The second inclusion is proved in Section 5, using Ehrenfeucht-Fraïssé games and algebraic tools. We will extend our main result to several other characterizations in Section 6.

3 $\mathbf{FO}^2[<]$ over an enriched alphabet

Given an integer $d > 1$, let us denote by $\mathbf{FO}^2[<, \mathrm{MOD}_d]$ the fragment of $\mathbf{FO}^2[<, \mathrm{MOD}]$ restricted to congruences modulo d. For a given language, this restriction does not lead to any loss of generality.

▶ **Lemma 8.** *Let L be a language of $\mathbf{FO}^2[<, \mathrm{MOD}]$. Then there exists an integer d such that L is in $\mathbf{FO}^2[<, \mathrm{MOD}_d]$.*

We now fix a positive integer d.

▶ **Definition 9** (Enriched alphabet)**.** Let A be an alphabet. We call the set $A_d = A \times (\mathbb{Z}/d\mathbb{Z})$ the *enriched alphabet* of A, and we denote by $\pi : A_d^* \to A^*$ the projection defined by $\pi(a, i) = a$ for each $(a, i) \in A_d$.

For example, the word $(a, 2)(b, 1)(b, 2)(a, 0)$ is an enriched word of *abba* for $d = 3$. We say that *abba* is the *underlying word* of $(a, 2)(b, 1)(b, 2)(a, 0)$.

▶ **Definition 10** (Well-formed words)**.** A word $(a_0, i_0)(a_1, i_1) \cdots (a_n, i_n)$ of A_d is *well-formed* if for $0 \leqslant j \leqslant n$, $i_j \equiv j \bmod d$. We denote by K the set of all well-formed words of A_d^*.

▶ **Definition 11.** For a word $u = a_0 a_1 \cdots a_n \in A^*$, the word $\overline{u} = (a_0, 0)(a_1, 1) \cdots (a_i, i \bmod d) \cdots (a_n, n \bmod d)$ is called the *well-formed word attached* to u.

▶ Remark. On well-formed structures, the projection π is a one-to-one application.

The enriched word $(a, 0)(b, 1)(b, 2)(a, 0)$ is a well-formed word for $d = 3$. Thanks to the previous remark, it is the unique well-formed word having the word *abba* as underlying word.

▶ Remark. The operation $u \to \overline{u}$ is not a morphism. Indeed, if $|u| \not\equiv 0 \bmod d$ then $\overline{uv} \neq \overline{u}\,\overline{v}$. Thus we define the *$k$-shift operation*, denoted by $\overline{u}^k$, which maps the word $u = u_0 \cdots u_n$ to the enriched word $(u_0, k \bmod d)(u_1, k + 1 \bmod d) \cdots (u_n, n + k \bmod d)$. Note that, if $|u| \equiv k \bmod d$, then $\overline{uv} = \overline{u}\,\overline{v}^k$.

▶ **Proposition 12.** *Let d be a positive integer. Then*

$$\mathbf{FO}^2[<, \mathrm{MOD}_d](A^*) = \pi(\mathbf{FO}^2[<](A_d^*) \cap K).$$

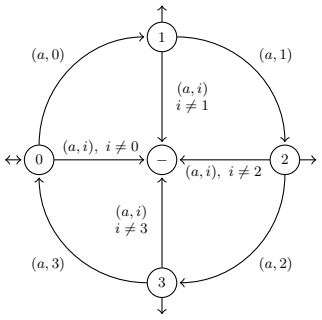
The proof relies on a syntactic transformation of the formulae. We replace MOD_i^d by a conjunction of enriched letters predicates. This can be done in the opposite direction as well, as we consider only well-formed words.

We recall (see [10]) that two words are separated by a formula of $\mathbf{FO}^2[<]$ with quantifier depth n if and only if Spoiler wins the n rounds Ehrenfeucht-Fraïssé game with two coloured pebbles. Thus one can state, in light of Proposition 12, the following assertion:

▶ **Proposition 13.** *Let u, v be words of A^*. Then there exists a formula of $\mathbf{FO}^2[<, \mathrm{MOD}_d]$ of quantifier depth n that separates them if, and only if, Spoiler wins the n rounds Ehrenfeucht-Fraïssé game for $\mathbf{FO}^2[<]$ over the well-formed pair $(\overline{u}, \overline{v})$.*

4 The inclusion $\mathbf{FO}^2[<, \mathrm{MOD}] \subseteq \mathbf{QDA}$

In this section, we prove one direction of the main theorem, using the enriched alphabet and the well-formed words. Let us first study the language K of well-formed words.



	0	1	2	3	–
$(a,0)$	1	–	–	–	–
$(a,1)$	–	2	–	–	–
$(a,2)$	–	–	3	–	–
$(a,3)$	–	–	–	0	–

Figure 1 Minimal automaton and transition monoid of K (for $d = 4$).

Consider the semigroup $B_d = (\mathbb{Z}/d\mathbb{Z} \times \mathbb{Z}/d\mathbb{Z}) \cup \{\perp\}$ where $\perp$ is a zero of B_d and for all (i, j) and (k, ℓ) in $\mathbb{Z}/d\mathbb{Z} \times \mathbb{Z}/d\mathbb{Z}$,

$$(i,j)(k,\ell) = \begin{cases} (i,\ell) & \text{if } j = k \\ \perp & \text{otherwise.} \end{cases}$$

The monoid B_d^1 is the transition monoid of the minimal automaton of K for $d \geqslant 2$. Let us denote by $\mathbf{J_1}$ the variety of idempotent and commutative monoids.

▶ **Proposition 14.** *The set of all well-formed words is recognized by a stamp in* $\mathbf{QJ_1}$.

▶ **Lemma 15.** *Let L be a language of $\mathcal{DA}(A_d^*)$. Then the language $L \cap K$ is in $\mathcal{QDA}(A_d^*)$.*

Proof. This comes from the fact that $L \in \mathcal{DA}(A_d^*) \subseteq \mathcal{QDA}(A_d^*)$, and $K \in \mathcal{QJ}_1(A_d^*) \subseteq \mathcal{QDA}(A_d^*)$. ◀

Now, we can use the previous result on well-formed words over modular predicates and prove the inclusion $\mathbf{FO}^2[<, \mathrm{MOD}] \subseteq \mathbf{QDA}$.

▶ **Theorem 16.** *The syntactic stamp of a* $\mathbf{FO}^2[<, \mathrm{MOD}]$*-definable language belongs to* $\mathbf{QDA}$.

As suggested by one the referees, this result can be proved by using Ehrenfeucht-Fraïssé games. The proof given below relies on finite automata and could easily be modified to recover the inclusion $\mathbf{FO}[<, \mathrm{MOD}] \subseteq \mathbf{QA}$ [18] and similar results for other fragments of logic.

Proof. Let L be a regular language definable in $\mathbf{FO}^2[<, \mathrm{MOD}](A^*)$. Then by Lemma 8, there exists an integer d such that L is defined in $\mathbf{FO}^2[<, \mathrm{MOD}_d](A^*)$. By Proposition 12, there exists a formula φ in $\mathbf{FO}^2[<](A_d^*)$ such that, $L = \pi(L')$ with $L' = L(\varphi) \cap K$. Since $\mathbf{FO}^2[<] = \mathbf{DA}$ (see [20]), and thanks to Lemma 15, the language L' is in $\mathcal{QDA}(A_d^*)$. Let $\mathcal{A}' = (Q, A_d, \cdot, i, F)$ be its minimal trim deterministic automaton. Since π is one-to-one, the automaton $\pi(\mathcal{A}')$, obtained by dropping the integer component on the transitions of $\mathcal{A}'$, recognizes L. As $\mathcal{A}'$ is trim and recognizes only well-formed words, the labels of all the outgoing edges from a given state have the same second component. For $0 \leqslant i < d$, let

$$Q_i = \{q \in Q \mid \text{ there exists } a \in A \text{ such that } q \cdot (a, i) \text{ is defined } \}$$

and let Q_E be the set of all states of fanout 0. Then Q is a disjoint union of the sets Q_i $(0 \leqslant i < d)$ and Q_E. Observing that a word of length k can only send a state of Q_i to

a state of $Q_{i+k \bmod d} \cup Q_E$, the transition function of the d-automaton $\mathcal{A}'_d$ is a subset of $\bigcup_{0 \leqslant i < d} \big(Q_i \times A_d^d \times (Q_i \cup Q_E)\big)$. Then each set Q_i induces a monoid M_i, which is a submonoid of the transition monoid of $\mathcal{A}'_d$. Now, going back to the projected d-automaton $\pi(\mathcal{A}')_d$, one can see that the action of a word $u \in A^d$ on the set Q_i is the action of the word $(u_0, i) \cdots (u_d, i-1)$ on Q_i in the automaton $\mathcal{A}'_d$, described in M_i.

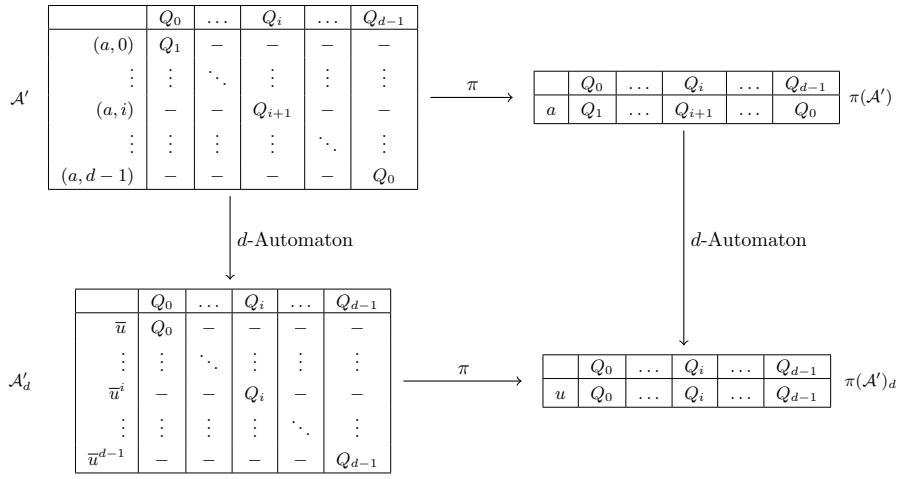


Figure 2 Transitions monoids.

Thus the full action of the word u over Q is described in each M_i, and hence the transition monoid of $\pi(\mathcal{A}')_d$ is a submonoid of the product monoid $\prod_{i=0}^{d} M_i$ (full picture on Figure 2). Finally, as **DA** is a variety and $\mathcal{A}'_d$ has its transition monoid in **DA**, each submonoid M_i is also in **DA** and so is the transition monoid of $\pi(\mathcal{A}')_d$. We can conclude as L is recognized by an automaton whose d-automata has its transition monoid in **DA**. ◀

5 The inclusion QDA $\subseteq$ FO$^2[<, \mathrm{MOD}]$

We now come to the second part of the proof of Theorem 6. We first enrich the congruences defined in [20] to take the modular predicates into account.

5.1 Congruence and syntactic operations over FO$^2[<, \mathrm{MOD}]$

▶ **Definition 17.** Let $u \in A^*$ be a word, and let $a \in A$ be a letter of u. We call *left a-decomposition* of u the unique triple (u_0, a, u_1) such that $u = u_0 a u_1$ and u_0 does not contain any a. We define the *right decomposition* in a symmetrical way.

We recall the definition of the congruence $\equiv_n$ on A^* from [20].

▶ **Definition 18.** [20] Let $u, v \in A^*$ be words. Then we have $u \equiv_0 v$.
Moreover, $u \equiv_n v$ if and only if the following conditions hold:

1. $\alpha(u) = \alpha(v)$, the two words have the same alphabet,
2. For each a occurring in u, if (u_0, a, u_1) is the left a-decomposition of u and (v_0, a, v_1) that of v, then $u_0 \equiv_n v_0$ and $u_1 \equiv_{n-1} v_1$,
3. For each a occurring in u, if (u_0, a, u_1) is the right a-decomposition of u and (v_0, a, v_1) that of v, then $u_0 \equiv_{n-1} v_0$ and $u_1 \equiv_n v_1$.

The termination of these inductive definitions has to be verified. Let suppose that $u \equiv_n v$ for some words u and v and some positive integer n. Then, thanks to the first condition, the parameter $n+|\alpha(u)|$ is equal to $n+|\alpha(v)|$. For any left or right decomposition we decompose the words in two parts for which the parameter strictly decreases.

▶ **Proposition 19.** *[20] The relation $\equiv_n$is a congruence.*

This definition can be extended to the enriched alphabet and well-formed words as follows. We say that $u \equiv_n^d v$ if and only if $\overline{u} \equiv_n \overline{v}$.

▶ **Lemma 20.** *Let n, d be two positive integers, and u and v two words such that $u \equiv_n^d v$. Then the following statements hold:*

1. *if u is the empty word, then so is v,*
2. *$|u| \equiv |v| \bmod d$,*
3. *if $u = u_0au_1$, $v = v_0bv_1$ with $|u_0a| \equiv |v_0b| \bmod d$ and $|u_1| < d$, $|v_1| < d$, then $a = b$, $u_1 = v_1$ and $u_0 \equiv_{n-1}^d v_0$,*
4. *if $u = u_0au_1$, $v = v_0bv_1$ with $|u_0| < d$, $|v_0| < d$ and $|au_1| \equiv |bv_1| \bmod d$, then $a = b$, $u_0 = v_0$ and $u_1 \equiv_{n-1}^d v_1$,*
5. *for any word w, $uw \equiv_n^d vw$ and $wu \equiv_n^d wv$.*

▶ **Corollary 21.** *The relation $\equiv_n^d$ is a congruence on A^*.*

We will now connect our congruence to the logic $\mathbf{FO}^2[<, \mathrm{MOD}_d]$ through the Ehrenfeucht-Fraïssé games for $\mathbf{FO}^2[<](A_d^*)$ (cf. Proposition 13).

▶ **Theorem 22.** *Let $u, v \in A^*$ be words. If $u \not\equiv_n^d v$ then there is a formula of $\mathbf{FO}^2[<, \mathrm{MOD}_d]$ of quantifier depth at most $n + |\alpha(\overline{u})|$ that separates u from v.*

The proof makes use of Ehrenfeucht-Fraïssé games following the arguments of [20].

5.2 Congruence and algebraic operations over QDA

We now define a slightly modified version of the Green's preorders adapted to the stable semigroup. Let $h : A^* \to M$ be a stamp and let S be its stable semigroup. For any elements x and y in M let us write:

- $x \leqslant_{\mathcal{R}_{st}} y$ if and only if $xM \cap S \subseteq yM \cap S$
- $x \leqslant_{\mathcal{L}_{st}} y$ if and only if $Mx \cap S \subseteq My \cap S$
- $x \leqslant_{\mathcal{H}_{st}} y$ if and only if $x \leqslant_{\mathcal{R}_{st}} y$ and $x \leqslant_{\mathcal{L}_{st}} y$.

We also extend our definitions to modified versions of the Green's relations.

- $x \,\mathcal{R}_{st}\, y$ if and only if $x \leqslant_{\mathcal{R}_{st}} y$ and $y \leqslant_{\mathcal{R}_{st}} x$
- $x \,\mathcal{L}_{st}\, y$ if and only if $x \leqslant_{\mathcal{L}_{st}} y$ and $y \leqslant_{\mathcal{L}_{st}} x$
- $x \,\mathcal{H}_{st}\, y$ if and only if $x \leqslant_{\mathcal{H}_{st}} y$ and $y \leqslant_{\mathcal{H}_{st}} x$

We say that the stamp h is *length faithful* if $h^{-1}(S^1) = (A^d)^*$. This notion is shown to be necessary in the next lemma and does not involve a loss of generality, as shown in the proof of Corollary 29.

▶ **Lemma 23.** *Let $h : A^* \to M$ be a stamp and let S be its stable semigroup. If h is length faithful, then the restriction of $\leqslant_{\mathcal{R}_{st}}$ (resp. $\leqslant_{\mathcal{L}_{st}}$) to S is the usual Green relation $\leqslant_{\mathcal{R}}$ (resp. $\leqslant_{\mathcal{L}}$) over S.*

Proof. Let x be an element of S, and y an element of M such that xy is in S. Then, since h is length faithful, $h^{-1}(xy)$ is contained in $(A^d)^*$. Moreover, as x belongs to S, we also have $h^{-1}(x) \subseteq (A^d)^*$. Thus for any word u such that $h(u) = x$, and any word v such that $h(v) = y$, we have $|u| \equiv |uv| \equiv 0 \bmod d$, so $|v| \equiv 0 \bmod d$. Therefore y is an element of S. This proves that for any x in S, $xM \cap S = xS$, and consequently for any x, y in S, $x \leqslant_{\mathcal{R}_{st}} y$ if and only if $x \leqslant_{\mathcal{R}} y$ in the Green relation over S.
The result for the $\leqslant_{\mathcal{L}_{st}}$ relation is obtained with a symmetric proof. ◀

▶ **Corollary 24.** *Let $h : A^* \to M$ be a length faithful stamp of* **QDA**. *Then, the restriction of the $\mathcal{H}_{st}$-classes to S are trivial.*

We also define the *$\mathcal{R}_{st}$-decomposition* :

▶ **Definition 25.** Let u be a word and let $h : A^* \to M$ be a stamp. We call the $\mathcal{R}_{st}$-decomposition of u the tuple $(u_0, a_1, u_1, \ldots, a_s, u_s)$ such that $u = u_0a_1u_1 \cdots a_su_s$ and:

1. $|u_0a_1u_1 \cdots a_iu_i| \equiv 0 \bmod d$ for all $0 \leqslant i < s$
2. $h(u_0a_1u_1 \cdots u_{i-1}a_i) >_{\mathcal{R}_{st}} h(u_0 \cdots u_ia_{i+1})$
3. For every prefix v of u_i of length multiple of d, $h(u_0 \cdots u_{i-1}a_i)\, \mathcal{R}_{st}\, h(u_0 \cdots a_iv)$
4. For every prefix v and v' of u_0 of length multiple of d, $h(v)\, \mathcal{R}_{st}\, h(v')$

The positions occurring in the $\mathcal{R}_{st}$-decomposition are the first positions multiple of d after falling in the $\leqslant_{\mathcal{R}_{st}}$-order. The two next lemmas will link our congruence $\equiv_d^n$ to the $\mathcal{R}_{st}$-decomposition of the lm-morphisms of **QDA**.

▶ **Lemma 26.** *Let $h : A^* \to M$ be a length faithful stamp in* **QDA**, *let S be its stable semigroup. Let $u \in S$ and $a, x \in M$. If $ax \in S$, then $uax\, \mathcal{R}_{st}\, u$ implies $uaxa\, \mathcal{R}_{st}\, u$.*

Proof. The elements u and uax are $\mathcal{R}_{st}$-equivalent and h is length faithful. So thanks to Lemma 23 there is an element t of S such that $u = uaxt$. By iteration, we obtain $u = u(axt)^\omega$. But S belongs to **DA**, hence it satisfies the equation $(xy)^\omega x(xy)^\omega = (xy)^\omega$. Thus, $(axt)^\omega ax(axt)^\omega = (axt)^\omega$, then $u = u(axt)^\omega ax(axt)^\omega$. Shall we rewrite this last equation, we finally get $u = uaxa(xt(axt)^{\omega-1})$. And finally $u \in uaxaM \cap S$, proving that $u\, \mathcal{R}_{st}\, uaxa$. ◀

▶ **Corollary 27.** *Let $h : A^* \to M$ be a length faithful stamp in* **QDA** *and let u be a word. Then if $(u_0, a_1, u_1, \ldots, a_s, u_s)$ is the $\mathcal{R}_{st}$-decomposition of u then $(a_{i+1}, 0) \notin \alpha(\overline{a_iu_i})$ for $i < s$.*

Proof. Let $(u_0, a_1, u_1, \ldots, a_s, u_s)$ be the $\mathcal{R}_{st}$-decomposition of u. Suppose now that there exists i such that $(a_{i+1}, 0) \in \alpha(\overline{a_iu_i})$ for $i < s$. Then, thanks to the preceding Lemma, $h(a_iu_ia_{i+1})\, \mathcal{R}_{st}\, h(a_iu_i)$ which is in contradiction with the definition of the $\mathcal{R}_{st}$-decomposition of u. ◀

We now have all the tools to prove the following theorem.

▶ **Theorem 28.** *Let $h : A^* \to M$ be a length faithful stamp of* **QDA** *and let d be its stability index. Then there exists an integer n such that for every words u and v, $u \equiv_n^d v$ implies $h(u) = h(v)$.*

Proof. Thanks to Lemma 20, if two words are equivalent for the congruence $\equiv_{n+1}^d$, then their suffixes of length smaller than d are equal and the associated prefixes are equivalent for the congruence $\equiv_n^d$. Therefore it is sufficient to prove the result for words of length multiple of d.

Let u and v be two words of length multiple of d, and an integer $n > |\alpha(\overline{u})||S|$ such that $u \equiv_n^d v$. Let us prove by induction on $|\alpha(\overline{u})|$ that $h(u) = h(v)$. If $|\alpha(\overline{u})| = 0$, then $u = v = 1$.

Consider the result to be true up to the rank $k-1$ and let u be such that $|\alpha(\overline{u})| = k$. We write $(u_0, a_1, u_1, \ldots, a_\ell, u_\ell)$ the $\mathcal{R}_{st}$-decomposition of u. One can remark that $\ell \leqslant |S|$, as each a_i makes the word go down in the $\mathcal{R}_{st}$-classes, whose number is bounded by the size of S. Using the preceding corollary, $(u_i, a_{i+1}, u_{i+1} \cdots u_\ell)$ is a left decomposition of $x_i = u_i \cdots u_\ell$ for $i < \ell$. As $u \equiv_n^d v$, there also exists a decomposition $(v_0, a_1, \ldots, a_\ell, v_\ell)$ of v such that $a_i u_i \equiv_{n-i}^d a_i v_i$ where $(a_{i+1}, 0) \notin \alpha(\overline{a_i u_i})$ and hence $|\alpha(\overline{a_i u_i})| \leqslant |\alpha(\overline{u})| - 1$. As $i < \ell$, we have $n - i \geqslant (k-1)|S| \geqslant |\alpha(\overline{a_i u_i})||S|$. Using the induction hypothesis, for $i < \ell$, $h(a_i u_i) = h(a_i v_i)$. And hence $h(u)\,\mathcal{R}_{st}\,h(u_1 \cdots a_\ell) = h(v_1 \cdots a_\ell) \geqslant_{\mathcal{R}_{st}} h(v)$. Symmetrically, we obtain that $h(v) \geqslant_{\mathcal{R}_{st}} h(u)$ and thus $h(u)\,\mathcal{R}_{st}\,h(v)$. Using the left/right symmetry, we also get that $h(v)\,\mathcal{L}_{st}\,h(u)$ and hence $h(v)\,\mathcal{H}_{st}\,h(u)$. By Corollary 24, the $\mathcal{H}_{st}$-classes are trivial in **QDA** over words of length multiple of d and hence $h(u) = h(v)$. ◀

▶ **Corollary 29.** $\mathbf{QDA} \subseteq \mathbf{FO}^2[<, \mathrm{MOD}]$

Proof. Let $\eta : A^* \to M$ be the syntactic stamp of L and S be the stable semigroup of η. Assume that η is in **QDA**. We claim that the morphism $h : A^* \to M \times \mathbb{Z}/d\mathbb{Z}$ defined, for all words u, by $h(u) = (\eta(u), |u| \bmod d)$ is length faithful. Indeed, the stable semigroup of h is equal to $S \times \{0\}$ and $h^{-1}(S \times \{0\}) = (A^d)^*$.

By Theorem 28, there exists an integer n such that the congruence $\equiv_n^d$ is thinner than the congruence induced by h which is itself thinner than the syntactic congruence of L. Therefore L is a finite union of $\equiv_n^d$- classes, each of them being, according to Theorem 22, definable by a formula of $\mathbf{FO}^2[<, \mathrm{MOD}_d]$ of quantifier-depth at most $n + |A|^d$. ◀

6 Other characterizations

Several other characterizations of **DA** are known (see [5] for a survey). For example, consider the fragment $\mathbf{TL}[X_a, Y_a]$ of the *linear temporal logic* defined inductively as follow:

$$\varphi \;\equiv\; \top \mid \varphi \wedge \varphi \mid \varphi \vee \varphi \mid \neg\varphi \mid X_a\varphi \mid Y_a\varphi.$$

The unary operator X_a stands for ne**X**t a, and Y_a stands for **Y**esterday a. For a word u and one of its positions x, we have $(u, x) \models X_a\varphi$ if φ is true at the next a after x. We say that the word u satisfies $X_a\varphi$ if $(u, -1) \models X_a\varphi$. Symmetrically, we say that u satisfies $Y_a\varphi$ if $(u, |u|) \models Y_a\varphi$. It is a well known fact that the fragment $\mathbf{TL}[X_a, Y_a]$ has the same expressiveness power as the variety **DA**. Therefore, it is natural to look at $\mathbf{TL}[X_a^{r \bmod d}, Y_a^{r \bmod d}]$, where each predicate $X_a^{r \bmod d}$ is defined as follows. For a word u and one of its position x, we have $(u, x) \models X_a^{r \bmod d}\varphi$ if φ is true at the next a whose position is equal to r modulo d. As in Proposition 12 we can transfer a modular information from the predicates to the letters by changing the size of the alphabet.

▶ **Proposition 30.** *Let d be a non-zero integer. Then,*

$$\mathbf{TL}[X_a^{r \bmod d}, Y_a^{r \bmod d}](A^*) = \pi(\mathbf{TL}[X_{(a, r \bmod d)}, Y_{(a, r \bmod d)}](A_d^*) \cap K).$$

In [16], Schützenberger defined the *monomials* as the set of languages of the form $B_0^* a_1 B_1^* \cdots a_n B_n^*$, with $a_i \in A$ and $B_i \subseteq A$. A monomial L is said to be *unambiguous* if for every word u in L, there exists only one decomposition $u = u_0 a_1 u_1 \cdots a_n u_n$ with $\alpha(u_i) \subseteq B_i$. Finally, Schützenberger proved in [16] that a language is in **DA** if and only if it is a disjoint

union of unambiguous monomials. We now give a similar definition adapted to the modular predicates. We define the *modular monomials* as the languages of the form

$$(A_0^0 \cdots A_{d-1}^0)^* a_1 (A_0^1 \cdots A_{d-1}^1)^* \cdots a_n (A_0^n \cdots A_{d-1}^n)^*$$

with d an integer, $A_k^i \subseteq A$ and $a_i \in A$.

▶ **Proposition 31.** *A language L is in $\mathcal{QDA}(A^*)$ if and only if L is a disjoint union of unambiguous modular monomials.*

Proof. We know by Theorem 6 and Proposition 12 that a language L is in $\mathcal{QDA}(A^*)$ if and only if there exists an integer d such that L is the projection of a set of well-formed words of a language L' in $\mathcal{DA}(A_d^*)$. Then L' is a disjoint union of unambiguous monomials. As the projection over well-formed words preserves disjoint union, it suffices to show that each unambiguous monomial projects into a disjoint union of modular monomials. Let $B_0^* b_1 B_1^* \cdots b_n B_n^*$ be an enriched unambiguous monomial with $b_i = (a_i, r_i)$. Then the projection of its well-formed words is the rational expression

$$(A_0^0 \cdots A_{d-1}^0)^* A_0^0 \cdots A_{r_1}^0 a_1 (A_{i+1}^1 \cdots A_i^1)^* A_{i+1}^1 \cdots A_{r_2}^1 a_2 \cdots$$

with $A_j^i = \{a \mid (a, j) \in B_i\}$, which can be rewritten as a disjoint union of unambiguous modular monomials. ◀

7 Conclusion

Our main results can now be summarized in a single statement, a consequence of Propositions 12, 30, 31 and Theorem 6.

▶ **Theorem 32.** *Let L be a regular language. Then, the following assertions are equivalent:*

- *L has its syntactic stamp in* **QDA**,
- *L is definable in* $\mathbf{FO}^2[<, \mathrm{MOD}]$,
- *L is definable in* $\mathbf{TL}[X_a^{r \bmod d}, Y_a^{r \bmod d}]$,
- *L is a disjoint union of unambiguous modular monomials.*

Our results are an instance of a more general problem: given a fragment **F** of **FO**, what is the expressive power of $\mathbf{F}[<, \mathrm{MOD}]$. In particular, if $\mathbf{F}[<]$ has an algebraic characterization, is there also a natural algebraic description of $\mathbf{F}[<, \mathrm{MOD}]$? Further if $\mathbf{F}[<]$ is decidable, does it imply that $\mathbf{F}[<, \mathrm{MOD}]$ is also decidable?
These questions are related to non-trivial questions of semigroup theory [1]. There is some hope that, for some sufficiently well-behaved fragment, $\mathbf{F}[<]$ corresponds to some variety of monoids **V** and that $\mathbf{F}[<, \mathrm{MOD}]$ corresponds to the semidirect product $\mathbf{V} * \mathbf{MOD}$ where **MOD** denotes the variety of all stamps onto a cyclic group. This is the case for instance for the fragment $\mathbf{\Sigma}_1$ and $\mathcal{B}\mathbf{\Sigma}_1$, as shown in [4]. The decidability of $\mathbf{V} * \mathbf{MOD}$ (given that of **V**) leads to another series of problems. When $\mathbf{V} * \mathbf{MOD}$ is equal to **QV** the decidability follows immediately but this is not always the case. For instance, $\mathcal{B}\mathbf{\Sigma}_1[<]$ corresponds to the variety **J** but $\mathcal{B}\mathbf{\Sigma}_1[<, \mathrm{MOD}]$ does not correspond to **QJ** and more sophisticated tools using derived categories have to be used [22]. Another possible route would be to follow a model theoretic approach as in [8, 9].
Acknowledgements We would like to thank the anonymous referees for very useful suggestions and Olivier Carton and Jean-Éric Pin for their helpful advice.

References

1 J. Almeida, Hyperdecidable pseudovarieties and the calculation of semidirect products, *Internat. J. Algebra Comput.* **9**,3-4 (1999), 241–261.

2 D. A. M. Barrington, K. Compton, H. Straubing and D. Thérien, Regular languages in NC^1, *J. Comput. System Sci.* **44**,3 (1992), 478–499.

3 J. R. Büchi, Weak second-order arithmetic and finite automata, *Z. Math. Logik Grundlagen Math.* **6** (1960), 66–92.

4 L. Chaubard, J.-É. Pin and H. Straubing, First order formulas with modular predicates, in *21st Annual IEEE Symposium on Logic in Computer Science (LICS 2006)*, pp. 211–220, IEEE, 2006.

5 V. Diekert, P. Gastin and M. Kufleitner, A survey on small fragments of first-order logic over finite words, *Internat. J. Found. Comput. Sci.* **19**,3 (2008), 513–548.

6 S. Eilenberg, *Automata, languages, and machines. Vol. B*, Academic Press [Harcourt Brace Jovanovich Publishers], New York, 1976. With two chapters by Bret Tilson, Pure and Applied Mathematics, Vol. 59.

7 Z. Ésik and M. Ito, Temporal logic with cyclic counting and the degree of aperiodicity of finite automata, *Acta Cybernet.* **16**,1 (2003), 1–28.

8 C. Glasser and H. Schmitz, The Boolean structure of dot-depth one, *J. Autom. Lang. Comb.* **6**,4 (2001), 437–452. 2nd Workshop on Descriptional Complexity of Automata, Grammars and Related Structures (London, ON, 2000).

9 C. Glasser, H. Schmitz and V. Selivanov, Efficient algorithms for membership in Boolean hierarchies of regular languages, in *STACS 2008*, pp. 337–348, *LIPIcs. Leibniz Int. Proc. Inform.* vol. 1, Schloss Dagstuhl. Leibniz-Zent. Inform., Wadern, 2008.

10 N. Immerman, Upper and lower bounds for first order expressibility, *J. Comput. System Sci.* **25**,1 (1982), 76–98.

11 R. McNaughton and S. Papert, *Counter-free automata*, The M.I.T. Press, Cambridge, Mass.-London, 1971.

12 D. Perrin and J.-É. Pin, First-order logic and star-free sets, *J. Comput. System Sci.* **32**,3 (1986), 393–406.

13 J.-É. Pin, Syntactic semigroups, in *Handbook of formal languages, Vol. 1*, pp. 679–746, Springer, Berlin, 1997.

14 J.-É. Pin and H. Straubing, Some results on $\mathcal{C}$-varieties, *Theor. Inform. Appl.* **39**,1 (2005), 239–262.

15 M. P. Schützenberger, On finite monoids having only trivial subgroups, *Information and Control* **8** (1965), 190–194.

16 M. P. Schützenberger, Sur le produit de concaténation non ambigu, *Semigroup Forum* **13**,1 (1976/77), 47–75.

17 I. Simon, Piecewise testable events, in *Automata theory and formal languages (Second GI Conf., Kaiserslautern, 1975)*, pp. 214–222., *Lect. Notes Comp. Sci.* vol. 33, Springer, Berlin, 1975.

18 H. Straubing, *Finite automata, formal logic, and circuit complexity*, Birkhäuser Boston Inc., Boston, MA, 1994.

19 H. Straubing, On logical descriptions of regular languages, in *LATIN 2002: Theoretical informatics*, pp. 528–538, *Lect. Notes Comp. Sci.* vol. 2286, Springer, Berlin, 2002.

20 D. Thérien and T. Wilke, Over words, two variables are as powerful as one quantifier alternation, in *STOC '98 (Dallas, TX)*, pp. 234–240, ACM, New York, 1999.

21 W. Thomas, Classifying regular events in symbolic logic, *J. Comput. System Sci.* **25**,3 (1982), 360–376.

22 B. Tilson, Categories as algebra: an essential ingredient in the theory of monoids, *J. Pure Appl. Algebra* **48**,1-2 (1987), 83–198.