COVERING AND SEPARATION FOR LOGICAL FRAGMENTS WITH MODULAR PREDICATES

THOMAS PLACE[1,4], VARUN RAMANATHAN[1,2,3], AND PASCAL WEIL[1,3]

[1]Univ. Bordeaux, CNRS, Bordeaux INP, LaBRI, UMR 5800, F-33400, Talence, France

[2]Chennai Mathematical Institute, Chennai, India

[3]CNRS, ReLaX, UMI 2000, Chennai, India

[4]Institut Universitaire de France
e-mail address: thomas.place@labri.fr, varun.ramanathan@u-bordeaux.fr, pascal.weil@labri.fr

ABSTRACT. For every class $\mathscr{C}$ of word languages, one may associate a decision problem called $\mathscr{C}$-separation. Given two regular languages, it asks whether there exists a third language in $\mathscr{C}$ containing the first language while being disjoint from the second one. Usually, finding an algorithm deciding $\mathscr{C}$-separation yields a deep insight on $\mathscr{C}$.

We consider classes defined by fragments of first-order logic. Given such a fragment, one may often build a larger class by adding more predicates to its signature. In the paper, we investigate the operation of enriching signatures with *modular predicates*. Our main theorem is a generic transfer result for this construction. Informally, we show that when a logical fragment is equipped with a signature containing the successor predicate, separation for the stronger logic enriched with modular predicates reduces to separation for the original logic. This result actually applies to a more general decision problem, called the covering problem.

1. INTRODUCTION

Context. Logic is a powerful tool for the specification of the behavior of systems, which is classically modeled by formal languages of words, trees and other discrete structures. Monadic second-order (MSO), first-order (FO) and their fragments play a prominent role in this context, especially in the case of languages of finite words (starting with the work of Büchi, see [Str94] for a general overview). An important set of problems deals with characterizing the expressive power of particular logics. Given a logic $\mathscr{F}$, one would want a decision procedure for the $\mathscr{F}$-*membership problem*: given a regular language L, decide whether L is definable by a sentence of $\mathscr{F}$ (i.e. whether L belongs to the class of languages

associated to $\mathscr{F}$). In practice, obtaining such an algorithm requires a deep understanding of $\mathscr{F}$: one needs to understand all the properties that can be expressed with $\mathscr{F}$.

Membership is known to be decidable for many fragments. The most celebrated result of this kind is the decidability of $\mathsf{FO}(<)$-membership (first-order logic equipped the linear ordering) which is due to Schützenberger, McNaughton and Papert [Sch65, MP71]. Another well-known example is the solution of Thérien and Wilke [TW98] for the two-variable fragment of first-order logic ($\mathsf{FO}^2(<)$). However, membership remains open for several natural fragments. A famous open question is to obtain membership algorithms for every level in the quantifier alternation hierarchy of first-order logic, which classifies it into levels $\Sigma_n(<)$ and $\mathscr{B}\Sigma_n(<)$. This problem has been investigated for years, starting with the theorem of Simon [Sim75] which states that $\mathscr{B}\Sigma_1(<)$-membership is decidable. However, despite all these efforts, progress has been slow and decidability is only known for $n \leq 4$ in the case of $\Sigma_n(<)$ and for $n \leq 2$ in the case of $\mathscr{B}\Sigma_n(<)$ [PW97, PZ14a, Pla15, Pla18] (we refer the reader to [Pin17, PZ15b, PZ17b] for detailed surveys on the problem). A key point is that the latest results on this question (for $\Sigma_3(<)$, $\mathscr{B}\Sigma_2(<)$ and $\Sigma_4(<)$) involve considering new decision problems generalizing membership: *separation* and *covering*.

For a fixed fragment $\mathscr{F}$, the $\mathscr{F}$-*separation problem* takes *two* input regular languages and asks whether there exists a third language, definable in $\mathscr{F}$, containing the first language and disjoint from the second one. Covering [PZ18, PZ16a] is even more general: it takes two different objects as input: a regular language L and a finite set of regular languages $\mathbf{L}$. It asks whether there exists an $\mathscr{F}$-cover $\mathbf{K}$ of L (*i.e.*, a finite set of languages definable in $\mathscr{F}$ whose union contains L) such that no language $K \in \mathbf{K}$ meets every language in $\mathbf{L}$. Separation corresponds to the special case of covering when the set $\mathbf{L}$ is a singleton. Membership is the particular case of separation where the input languages are of the form L and $A^* \setminus L$. The investigation of these two problems has been particularly fruitful. While obtaining an algorithm for separation or covering is usually more difficult than for membership, it is also more rewarding with respect to the insight one gets on the logical fragment investigated. Furthermore, solutions for these two problems are often more robust than those for membership. A striking example is a transfer theorem of [PZ14a] which can be applied to the quantifier alternation hierarchy: for every $n \geq 1$, $\Sigma_{n+1}(<)$-membership can be effectively reduced to $\Sigma_n(<)$-separation.

Separation is known to be decidable, for instance, for $\mathscr{B}\Sigma_1(<)$ (Place, van Rooijen, Zeitoun [PvRZ13] and, independently, Czerwinski, Martens and Masopust [CMM13]). The problem of separation was actually studied earlier, under a different guise: Almeida [Alm99] showed, if $\mathscr{V}$ is a variety of languages and $\mathbf{V}$ is the corresponding pseudovariety of monoids (in Eilenberg's correspondence, see [Pin86]), that the $\mathscr{V}$-covering problem and the problem of computing $\mathbf{V}$-*pointlikes* (a notion with deep roots in algebra and topology which we will not need to discuss here) reduce to each other in a natural fashion. It follows that earlier work of Henckell [Hen88] (see also [HRS10, vGS18a, vGS18b]) on aperiodic pointlikes shows that $\mathsf{FO}(<)$-separation and covering are decidable. For a a fully language-theoretic proof of this result, see Place and Zeitoun [PZ16b].

In the paper, we investigate the separation and covering problems for several families of logical fragments, built from weaker fragments using a generic operation: *enrichment by modular predicates*. This operation was first introduced by Barrington *et al.* [BCST92] in their study of circuit complexity. It is a natural extension also in the following sense: the first standard examples of regular languages that are not in $\mathsf{FO}(<)$ are those that involve modulo counting (*e.g.*, the set of words of even length). *Modular predicates* introduce just

that capability: for every natural number $d \geq 1$ and every $i < d$, a unary predicate is available, which selects the positions in a word that are congruent to i modulo d. Adding these predicates to a fragment of $\mathsf{FO}(<)$ allows the concise specification of languages that are not $\mathsf{FO}(<)$-definable (it strictly increases the expressive power of the logic), while remaining within MSO-definability, and hence within the realm of regular languages.

Before we give an overview of the state of the art, let us comment on our method, or rather on the point of view we adopted in this paper. Specialists of the domain are well aware that this sort of problems, linking automata theory and logical specifications, can be approached from different angles. One of those is to rely heavily on algebraic models (following, say, [Eil76, Pin86, Str94]). Here we choose instead to remain as close as possible to purely language-theoretic arguments as in, *e.g.*, [PZ17b, PZ18]. This way, we gain a little generality and we avoid introducing sophisticated machinery. One side-effect is that we are led to translating certain ideas that were already present in the framework of logic or algebra, under the restrictions imposed by that framework (and we explicitly mention these situations). Our main objective in opting for this approach is to, hopefully, make the paper more accessible to a wider audience.

State of the art. Currently, no results are known for the separation and covering problems associated to fragments enriched with modular predicates. However, earlier results considered the status of membership when a fragment of $\mathsf{FO}(<)$ is enriched with modular predicates: Barrington et al. showed that $\mathsf{FO}(<, \mathbf{MOD})$-membership is decidable [BCST92] (see also [Str94]). Chaubard et al. [CPS06] show the same result for the extensions of $\Sigma_1(<)$ and $\mathscr{B}\Sigma_1(<)$: $\Sigma_1(<, \mathbf{MOD})$ and $\mathscr{B}\Sigma_1(<, \mathbf{MOD})$. Kufleitner and Walter [KW15] show the decidability of membership for $\Sigma_2(<, \mathbf{MOD})$. Finally, Dartois and Paperman show that the extension of $\mathsf{FO}^2(<)$ with modular predicates ($\mathsf{FO}^2(<, \mathbf{MOD})$) has decidable membership as well [DP13]. In [DP15b], they extend their result to a wider range of logical fragments enriched with modular predicates (see also the unpublished [DP15a]).

Unfortunately, each of these decidability results is proved using a specific argument which deals directly with a particular fragment enriched with modular predicates. There are many fragments of first-order logic. Consequently, it would be preferable to avoid an approach which considers each of them independently. Instead, we would like to have a *generic transfer theorem* which, given a fragment $\mathscr{F}$, lifts a solution of the decision problems for $\mathscr{F}$ to the stronger variant of $\mathscr{F}$ enriched with modular predicates.

It turns out that such a transfer theorem is already known for another natural operation on fragments of first-order logic: enrichment by the local predicates (the successor binary relation "+1" and the min and max unary predicates). In [PZ15a, PZ17a], Place and Zeitoun showed that separation and covering are decidable for the following logical fragments enriched with the local predicates: $\mathsf{FO}^2(<, +1)$, $\Sigma_1(<, +1)$, $\mathscr{B}\Sigma_1(<, +1)$, $\Sigma_2(<, +1)$, $\mathscr{B}\Sigma_2(<, +1)$ and $\Sigma_3(<, +1)$ (the enrichment of $\mathsf{FO}(<)$ is omitted as its expressive power is not increased). A key point is that all these results rely on the same generic reduction which is obtained by translating the problem to a language theoretic statement. Translating ideas from Straubing's seminal paper [Str85] on algebraic methods to solve the membership problem when local predicates are added to a fragment into a purely language-theoretic setting, Place and Zeitoun investigate an operation on classes of languages, namely $\mathscr{C} \mapsto \mathscr{C} \circ \mathsf{SU}$ (see Section 4 for definitions). It satisfies the two following properties:

(1) In most cases, if $\mathscr{F}$ is a fragment of first-order logic, the enrichment of $\mathscr{F}$ with local predicates corresponds to the class $\mathscr{F} \circ \mathsf{SU}$. In [PZ18], this is proved for two-variable first-order logic ($\mathsf{FO}^2(<)$) and levels in the alternation hierarchy ($\Sigma_n(<)$ and $\mathscr{B}\Sigma_n(<)$).

(2) The main theorem of [PZ18] states that the separation and covering problems are decidable on $\mathscr{C} \circ \mathsf{SU}$ if they are on $\mathscr{C}$. This result highlights the robustness of separation and covering: such a theorem fails for membership.

The decidability results for the extended fragments that we mentioned above are then obtained from already established results for the separation and covering problems associated to $\mathsf{FO}^2(<)$, $\Sigma_1(<)$, $\mathscr{B}\Sigma_1(<)$, $\Sigma_2(<)$, $\mathscr{B}\Sigma_2(<)$ and $\Sigma_3(<)$ (see [PZ14b, CMM13, PZ18, Pla18]).

Contribution. Our results apply to enrichment by modular predicates and follow the same scheme, with an interesting twist. We investigate an operation on classes of languages whose origins can be found implicitly or explicitly in [BCST92, CPS06], written $\mathscr{C} \mapsto \mathscr{C} \circ \mathsf{MOD}$ (again, see Section 4 for definitions). Then we show two properties which are similar to those of $\mathscr{C} \circ \mathsf{SU}$.

(1) If $\mathscr{C}$ is the class corresponding to a fragment $\mathscr{F}$ of first-order logic satisfying some mild hypotheses, then $\mathscr{C} \circ \mathsf{MOD}$ corresponds to the extension of $\mathscr{F}$ by modular predicates. Let us point out that this result is generic, which makes it stronger, and much simpler to establish than the corresponding result for $\mathscr{C} \circ \mathsf{SU}$ (which requires a separate proof for each fragment).

(2) We show that, for every class $\mathscr{C}$ of the form $\mathscr{C} = \mathscr{D} \circ \mathsf{SU}$, the separation and covering problems are decidable on $\mathscr{C} \circ \mathsf{MOD}$ if they are on $\mathscr{C}$. This result is weaker than that for $\mathscr{C} \circ \mathsf{SU}$: it does not apply to all classes, only those of the form $\mathscr{D} \circ \mathsf{SU}$.

Consequently, our results complement those of Place and Zeitoun [PZ16b, PZ17a] in a natural way. Combining the two theorems yield that for every class $\mathscr{C}$, the separation and covering problems are decidable on $(\mathscr{C} \circ \mathsf{SU}) \circ \mathsf{MOD}$ if they are on $\mathscr{C}$.

Going back to the logical point of view, this shows that for most fragments $\mathscr{F}$, enriching $\mathscr{F}$ with the local and modular predicates simultaneously preserves the decidability of separation and covering. In the paper, we use this result to show that separation and covering are decidable for several fragments: $\mathsf{FO}(<, \mathbf{MOD})$, $\mathsf{FO}^2(<, +1, \mathbf{MOD})$, $\Sigma_n(<, +1, \mathbf{MOD})$ for $n = 1, 2, 3$ and $\mathscr{B}\Sigma_n(<, +1, \mathbf{MOD})$ for $n = 1, 2$.

Plan of the paper. The paper is organized as follows. Classes of languages and the membership, separation and covering problems are introduced in Section 2. Fragments of first-order logic, and the notion of enrichment of a fragment by the adjunction of new predicates (typically: the local and the modular predicates) is introduced in Section 3. The enrichment operation on classes of languages, namely the operation $\mathscr{C}, \mathscr{D} \mapsto \mathscr{C} \circ \mathscr{D}$, is studied in Section 4. We also discuss in that section the language-theoretic impact of enriching a logical fragment with local and, especially, modular predicates. We formulate our main theorem in Section 5: it reduces the covering and separation problems in a class of the form $(\mathscr{C} \circ \mathsf{SU}) \circ \mathsf{MOD}$ to the same problem in $\mathscr{C} \circ \mathsf{SU}$.

The proof of Theorem 5.1 is given in two parts: in Section 6, we translate the problem to another language theoretic problem (in terms of the operation of block abstraction, introduced here), which turns out to be easier to handle. The proof of the theorem itself is given in Section 7.

2. Preliminaries

In this section, we introduce classes of languages and the decision problems that we shall consider.

2.1. **Classes of languages.** An *alphabet* is a finite non-empty set of symbols that we call *letters*. Given an alphabet A, we denote by A^* the set of all finite sequences (known as *words*) of letters in A, including the empty word denoted by ε. Given a word $w \in A^*$ we write $|w| \in \mathbb{N}$ for the length of w. The set of non-empty words is written A^+ ($A^+ = A^* \setminus \{\varepsilon\}$). A subset of A^* is called a *language*.

A *class of languages* $\mathscr{C}$ is a correspondence $A \mapsto \mathscr{C}(A)$, defined for all alphabets A, where $\mathscr{C}(A)$ is a set of languages over A. All classes considered in the paper are included in the class of regular languages, this will be implicitly assumed from now on. These are the languages which are accepted by a nondeterministic finite automaton (see e.g. [Koz97]). Here, we shall work with the classical monoid-theoretic characterizations, which we now recall.

Recall that a *semigroup* S is a set equipped with an associative binary operation (called the *product*) and a *monoid* is a semigroup M that has an identity element (which we denote by 1_M). If A is an alphabet, then A^* is a monoid under word concatenation and A^+ is a semigroup under the same operation.

A morphism $\eta\colon A^* \to M$, into a finite monoid, is said to recognize a language $L \subseteq A^*$ if $L = \eta^{-1}(X)$ for some subset X of M, that is, if $L = \eta^{-1}(\eta(L))$. It is well-known that a language is regular if and only if it is recognized by a morphism into a finite monoid [Pin86].

2.2. **Closure properties.** In the paper, we only work with classes of languages satisfying robust closure properties that we describe below.

Boolean operations. A class $\mathscr{C}$ of languages is a *lattice* when $\mathscr{C}(A)$ is closed under finite unions and intersections for every alphabet A: that is, $\emptyset, A^* \in \mathscr{C}(A)$ and for every $L_1, L_2 \in \mathscr{C}(A)$, we have $L_1 \cup L_2 \in \mathscr{C}(A)$ and $L_1 \cap L_2 \in \mathscr{C}(A)$. A *Boolean algebra* is a lattice $\mathscr{C}$ that is additionally closed under complement: for every alphabet A and every $L \in \mathscr{C}(A)$, we have $A^* \setminus L \in \mathscr{C}(A)$.

Quotients. Recall that if L is a language in A^* and $u \in A^*$, then the *left* and *right quotients* $u^{-1}L$ and Lu^{-1} are defined as follows

$$u^{-1}L = \{v \in A^* \mid uv \in L\} \quad \text{and} \quad Lu^{-1} = \{v \in A^* \mid vu \in L\}.$$

We say that a class $\mathscr{C}$ is *quotient-closed* when it is closed under taking (left and right) quotients by words of A^*.

Inverse morphisms. A class $\mathscr{C}$ is *closed under inverse morphisms* when, for all alphabets A, B, morphism $\alpha\colon A^* \to B^*$ and language $L \in \mathscr{C}(B)$, we have $\alpha^{-1}(L) \in \mathscr{C}(A)$.

We shall also consider a weaker variant of this closure property, namely *closure under inverse length increasing morphisms*. A morphism α as above is *length increasing* when $|\alpha(w)| \geq |w|$ for every $w \in A^*$. A class $\mathscr{C}$ is closed under inverse length increasing morphisms when for every such morphism and every language $L \in \mathscr{C}(B)$, we have $\alpha^{-1}(L) \in \mathscr{C}(A)$. Observe that by definition, any class $\mathscr{C}$ which is closed under inverse morphisms is also closed under inverse length increasing morphisms.

Remark 2.1. The morphism α is length increasing if and only if $\alpha(a) \neq \varepsilon$ for any $a \in A$. Such morphisms are also called *non-erasing*. $\qquad\square$

Varieties. We call *positive variety* (resp. *variety*) a quotienting lattice (resp. quotienting Boolean algebra) which is closed under inverse morphisms. Similarly, we call *positive* **li**-*variety* (resp **li**-*variety*) a quotienting lattice (resp. quotienting Boolean algebra) which is closed under inverse length increasing morphisms.

2.3. **Decision problems.** Our main objective in this paper is to investigate two decision problems: separation and covering. Both problems are parametrized by an arbitrary class of languages $\mathscr{C}$. We start with the definition of separation.

Given two languages L_1, L_2 over some alphabet A, we say that a language $K \subseteq A^*$ *separates L_1 from L_2* if $L_1 \subseteq K$ and $L_2 \cap K = \emptyset$. Furthermore, given a class $\mathscr{C}$, we say that L_1 is $\mathscr{C}$*-separable from* L_2 if there exists $K \in \mathscr{C}(A)$ which separates L_1 from L_2.

Given a class of languages $\mathscr{C}$, the $\mathscr{C}$*-separation problem* takes as input two regular languages L_1 and L_2 and asks whether L_1 is $\mathscr{C}$-separable from L_2.

Remark 2.2. Note that when $\mathscr{C}$ is not closed under complement, this definition is not symmetric: it could happen that L_1 is $\mathscr{C}$-separable from L_2 while L_2 is not $\mathscr{C}$-separable from L_1. $\qquad\square$

The covering problem is a generalization of separation that was originally defined in [PZ18, PZ16a]. As pointed out in the introduction, in the particular case of varieties of regular languages, the covering problem is a translation of the more algebraic problem of the computation of pointlikes [Alm99].

Given a language L in A^*, a *cover of L* is a finite set of languages $\mathbf{K}$ in A^* such that $L \subseteq \bigcup_{K \in \mathbf{K}} K$. For a given class $\mathscr{C}$, a $\mathscr{C}$*-cover* of L is a cover $\mathbf{K}$ of L such that every $K \in \mathbf{K}$ belongs to $\mathscr{C}$. Additionally, given a finite multiset[1] of languages $\mathbf{L}$, we say that a finite set of languages $\mathbf{K}$ is *separating for* $\mathbf{L}$ if for any $K \in \mathbf{K}$, there exists $L \in \mathbf{L}$ such that $K \cap L = \emptyset$ (that is: no language in $\mathbf{K}$ intersects every language in $\mathbf{L}$).

Now consider a class $\mathscr{C}$. Given a language L_1 and a finite multiset of languages $\mathbf{L}_2$, we say that the pair $(L_1, \mathbf{L}_2)$ is $\mathscr{C}$*-coverable* if there exists a $\mathscr{C}$-cover of L_1 which is separating for $\mathbf{L}_2$. The $\mathscr{C}$*-covering problem* takes as input a regular language L_1 and a finite multiset of regular languages $\mathbf{L}_2$, and it asks whether $(L_1, \mathbf{L}_2)$ is $\mathscr{C}$-coverable.

We complete this definition by showing why covering generalizes separation, at least when the class $\mathscr{C}$ is a lattice.

Fact 2.3. *Let $\mathscr{C}$ be a lattice and L_1, L_2 two languages. Then L_1 is $\mathscr{C}$-separable from L_2, if and only if $(L_1, \{L_2\})$ is $\mathscr{C}$-coverable.*

Proof. Assume that L_1 is $\mathscr{C}$-separable from L_2 and let $K \in \mathscr{C}$ be a separator. It is immediate that $\mathbf{K} = \{K\}$ is a separating $\mathscr{C}$-cover for $(L_1, \{L_2\})$. Conversely, assume that $(L_1, \{L_2\})$ is $\mathscr{C}$-coverable and let $\mathbf{K}$ be the separating $\mathscr{C}$-cover. The union K of the languages in $\mathbf{K}$ is in $\mathscr{C}$ since $\mathscr{C}$ is a lattice, and $L_1 \subseteq K$ by definition of a cover. Moreover, no language in $\mathbf{K}$ intersects L_2 since $\mathbf{K}$ was separating for $\{L_2\}$, that is, $L_2 \cap K = \emptyset$. Therefore $K \in \mathscr{C}$ separates L_1 from L_2. $\qquad\square$

---

[1]We speak of multiset here in order to allow $\mathbf{L}$ to have several copies of the same language. This is natural as the input for the covering problem is given by monoid morphisms recognizing the languages in $\mathbf{L}$, and it may happen that several distinct recognizers define the same language. This is harmless in practice.

3. Logic and modular predicates

We introduce here the formal definition of fragments of first-order logic and the classes of languages they define.

3.1. First-order logic.

Let us fix an alphabet A. Any word $w \in A^*$ may be viewed as a logical structure whose domain is the set of positions $\{0, \ldots, |w| - 1\}$ in w. In first-order logic, one can quantify over these positions and use a pre-determined signature of predicates.

More precisely: a *predicate* is a symbol P together with an integer $k \in \mathbb{N}$ called the *arity* of P. Moreover, whenever we consider a predicate P of arity k, we shall assume that an *interpretation* of P is fixed: for every word $w \in A^*$, P is interpreted as a k-ary relation over the set of positions of w. A *signature* (over the alphabet A) is a (possibly infinite) set of predicate symbols $\boldsymbol{S} = \{P_1, \ldots, P_\ell, \ldots\}$, all interpreted over words in A^*. Given such a signature $\boldsymbol{S}$, we write $\mathsf{FO}[\boldsymbol{S}]$ for the set of all first-order formulas over $\boldsymbol{S}$. As usual, we call sentence a formula with no free variable.

We use the classical semantic of first-order formulas to interpret formulas of $\mathsf{FO}[\boldsymbol{S}]$ on a word $w \in A^*$. In particular, every $\mathsf{FO}[\boldsymbol{S}]$ sentence φ defines a language $L \subseteq A^*$. It contains all words $w \in A^*$ satisfying φ: $L = \{w \in A^* \mid w \models \varphi\}$.

Example 3.1. Assume that $A = \{a, b\}$ and consider the signature $\boldsymbol{S} = \{a, b, <\}$ where a (resp. b) is a unary predicate which selects positions labeled with the letter a (resp. b) and $<$ is a binary predicate interpreted as the (strict) linear order. Then the following is an $\mathsf{FO}[\boldsymbol{S}]$ sentence:
$$\exists x \exists y \; x < y \wedge a(x) \wedge b(x) \wedge \neg(\exists z \; x < z \wedge z < y).$$
It defines the language $A^* ab A^*$. □

In the paper, we shall consider signatures containing specific predicates. We present them now.

Label predicates. All the signatures that we consider include the label predicates. For each letter $a \in A$, the unary *label predicate* $a(x)$ is interpreted as the unary relation selecting all positions whose label is a. Observe that these predicates depend on the alphabet A that we are using. Abusing notation, we write A for the set of label predicates over alphabet A.

Linear order. Another predicate that is also always contained in our signatures is the binary predicate $<$ which is interpreted as the (strict) linear order over the positions.

Moreover, two natural sets of predicates are of particular interest for the paper: the local predicates and the modular predicates.

Local predicates. There are four local predicates. They are as follows:
- the binary predicate $+1$ interpreted as the successor relation between positions;
- the unary predicate min selecting the leftmost position in the word;
- the unary predicate max selecting the rightmost position in the word;
- the constant (0-ary) predicate ε which holds exactly when the word is empty.

Modular predicates. There are infinitely many modular predicates. For every natural number $d > 1$ and $0 \le i < d$,

- the unary predicate $\mathbf{MOD}_i^d$ selects the positions x that are congruent to i modulo d;
- the constant $\mathbf{D}_i^d$ holds when the length of the word is congruent to i modulo d.

We denote by $\mathbf{MOD}$ the (infinite) set of all modular predicates.

These are all the predicates that we shall consider. An important observation is that the order predicate $<$, the local and the modular predicates are examples of *structural* predicates (also known as *numerical* predicates, see [Str94]): a k-ary predicate P is structural if its interpretation is defined for every alphabet and is independent from the labels. More precisely, given two words w, w' (possibly over different alphabets) having the same length ℓ and k positions $i_1, \ldots, i_k \le \ell$, P satisfies the following property:

$$P(i_1, \ldots, i_k) \text{ holds in } w \quad \text{if and only if} \quad P(i_1, \ldots, i_k) \text{ holds in } w'.$$

We say that a signature $\boldsymbol{S}$ is *structural* if it contains only structural predicates.

3.2. **Fragments of first-order logic.** A *fragment* $\mathscr{F}$ of first-order logic consists in the specification of a (possibly finite) set $V_{\mathscr{F}}$ of variables and a correspondence $\mathscr{F} \colon \boldsymbol{S} \mapsto \mathscr{F}[\boldsymbol{S}]$ which associates with every signature $\boldsymbol{S}$ a set $\mathscr{F}[\boldsymbol{S}] \subseteq \mathsf{FO}[\boldsymbol{S}]$ of formulas over the signature $\boldsymbol{S}$ using only the variables in $V_{\mathscr{F}}$ and which satisfies the following properties:

- for every signature $\boldsymbol{S}$, every quantifier-free $\mathsf{FO}[\boldsymbol{S}]$-formula belongs to $\mathscr{F}[\boldsymbol{S}]$;
- $\mathscr{F}[\boldsymbol{S}]$ is closed under conjunction and disjunction;
- $\mathscr{F}$ is closed under quantifier-free substitution: if $\boldsymbol{S}, \boldsymbol{S}'$ are signatures and φ is a formula in $\mathscr{F}[\boldsymbol{S}]$, then $\mathscr{F}[\boldsymbol{S}']$ contains every formula φ' obtained by replacing each atomic formula in φ by a quantifier-free formula of $\mathscr{F}[\boldsymbol{S}']$.

Example 3.2. FO itself is a fragment of first-order logic, and so is FO^2, where $\mathsf{FO}^2[\boldsymbol{S}]$ is the set of formulas in $\mathsf{FO}[\boldsymbol{S}]$ which use at most two variable names.

The classes in the quantifier alternation hierarchy also provide interesting examples: given $n \ge 1$, a formula of $\mathsf{FO}[\boldsymbol{S}]$ is in $\Sigma_n[\boldsymbol{S}]$ (resp. $\Pi_n[\boldsymbol{S}]$) if its prenex normal form has $n - 1$ quantifier alternations (i.e. n blocks of quantifiers) and starts with an existential (resp. universal) quantifier, or if it has at most $n - 2$ quantifier alternations. For example, a sentence whose prenex normal form is

$$\exists x_1 \ \forall x_2 \ \forall x_3 \ \exists x_4 \ \forall x_5 \ \varphi(x_1, x_2, x_3, x_4, x_5) \quad \text{(with } \varphi \text{ quantifier-free)}$$

is Σ_4. Clearly, $\Sigma_{n+1}[\boldsymbol{S}]$ contains both $\Sigma_n[\boldsymbol{S}]$ and $\Pi_n[\boldsymbol{S}]$. Moreover, Σ_n and Π_n formulas are not closed under negation and it is standard to also consider $\mathscr{B}\Sigma_n$, namely the Boolean combinations of Σ_n formulas. □

A fragment $\mathscr{F}$ and a structural signature $\boldsymbol{S}$ determine a class of languages, denoted by $\mathscr{F}(\boldsymbol{S})$. For every alphabet A, $\mathscr{F}(\boldsymbol{S})(A)$ contains the languages $L \subseteq A^*$ which can be defined by a sentence of $\mathscr{F}[A, \boldsymbol{S}]$. That is, a sentence of $\mathscr{F}$ over the signature containing the label predicates over A and the structural predicates in $\boldsymbol{S}$ (whose interpretation is defined independently of the alphabet).

It is well known that the classes $\mathsf{FO}(<)$, $\mathsf{FO}^2(<)$, $\mathscr{B}\Sigma_n(<)$ are varieties, and that the classes $\Sigma_n(<)$ and $\Pi_n(<)$ are positive varieties. The latter form a strict hierarchy whose union is $\mathsf{FO}(<)$ [BK78].

Logical enrichment. In the paper, we are not interested in a particular class. Instead, we consider a generic operation that one may apply to logically defined classes. Let $\mathscr{F}$ be a fragment, $\boldsymbol{S}$ a structural signature and consider the class $\mathscr{F}(\boldsymbol{S})$. One may define a larger class by enriching $\boldsymbol{S}$ with additional predicates. We are mainly interested in enrichment by *modular predicates*. If $\mathscr{F}$ is a fragment and $\boldsymbol{S}$ is a structural signature, we write $\mathscr{F}(\boldsymbol{S}, \mathbf{MOD})$ for the class associated to $\mathscr{F}$ and the enriched structural signature $\boldsymbol{S} \cup \mathbf{MOD}$.

Our main objective is to investigate the separation and covering problems for classes of the form $\mathscr{F}(\boldsymbol{S}, \mathbf{MOD})$. Ideally, we would like to have a transfer theorem: a generic effective reduction from $\mathscr{F}(\boldsymbol{S}, \mathbf{MOD})$-covering to $\mathscr{F}(\boldsymbol{S})$-covering. Getting such a result remains an open problem. We obtain a slightly weaker one: while we do present such a reduction, it is only correct when the smaller class $\mathscr{F}(\boldsymbol{S})$ satisfies specific hypotheses. Informally, we require the original signature $\boldsymbol{S}$ to contain the set of local predicates ($+1$, min, max and ε).

This motivates us to introduce a notation for enrichment by local predicates. If $\mathscr{F}$ is a fragment of first-order logic and $\boldsymbol{S}$ a structural signature, we denote by $\mathscr{F}(\boldsymbol{S}, +1)$ the class of languages associated to $\mathscr{F}$ and the enriched structural signature $\boldsymbol{S} \cup \{+1, \mathsf{min}, \mathsf{max}, \varepsilon\}$.

Remark 3.3. By combining the two above operations, every fragment $\mathscr{F}$ and structural signature $\boldsymbol{S}$ yield four classes: $\mathscr{F}(\boldsymbol{S})$, $\mathscr{F}(\boldsymbol{S}, +1)$, $\mathscr{F}(\boldsymbol{S}, \mathbf{MOD})$ or $\mathscr{F}(\boldsymbol{S}, +1, \mathbf{MOD})$. These four classes are distinct in most cases. However, it may not be the case in specific situations. We shall encounter one important such situation in the paper: $\mathsf{FO}(<)$ and $\mathsf{FO}(<, +1)$ coincide (as well as $\mathsf{FO}(<, \mathbf{MOD})$ and $\mathsf{FO}(<, +1, \mathbf{MOD})$). This is because the local predicates are easily defined from the linear order when quantifications are unrestricted. For example, $x + 1 = y$ is expressed by the formula $x < y \wedge \neg\exists z\,(x < z \wedge z < y)$. $\qquad\square$

It was shown in [PZ15a, PZ17a] that under mild assumptions on $\mathscr{F}(\boldsymbol{S})$ (general enough to capture all relevant examples), $\mathscr{F}(\boldsymbol{S}, +1)$-covering can be effectively reduced to $\mathscr{F}(\boldsymbol{S})$-covering. Our main theorem (presented in Section 5) extends this result: under the same assumptions (on $\mathscr{F}(\boldsymbol{S})$), there is another effective reduction from $\mathscr{F}(\boldsymbol{S}, +1, \mathbf{MOD})$-covering to $\mathscr{F}(\boldsymbol{S}, +1)$-covering (and therefore to $\mathscr{F}(\boldsymbol{S})$-covering as well by transitivity). Combined with previously known results, this yields the decidability of covering for several classes of the form $\mathscr{F}(\boldsymbol{S}, +1, \mathbf{MOD})$.

Our approach is similar to that taken in [PZ17a]. We exploit the fact that the addition of local or modular predicates to a structural signature admits a nice language-theoretic characterization. This is discussed in Section 4. We then formulate our main theorem precisely in Section 5.

4. The enrichment operation for classes of languages

Let $\mathscr{C}$ and $\mathscr{D}$ be classes of languages. We define in Section 4.1 the *$\mathscr{D}$-enrichment of $\mathscr{C}$*, written $\mathscr{C} \circ \mathscr{D}$. Before we get to the precise definition, let us formulate two remarks.

Remark 4.1. Enrichment is the language theoretic counterpart of an algebraic operation defined between varieties of semigroups: the *wreath product*. In fact, we use the same notation as for the wreath product and our definition (taken from [PZ17a]) is based on Straubing's so-called wreath product principle [Str85]. Much of the literature on this topic is written from an algebraic point of view, including the connection with logic. The language theoretic approach adopted here allows us to bypass some general machinery which is not needed in this context. $\qquad\square$

Remark 4.2. Whereas we define enrichment for arbitrary classes $\mathscr{C}$ and $\mathscr{D}$, we will mainly be concerned with $\mathscr{D}$-enrichment when $\mathscr{D}$ is the class SU of suffix languages or the class MOD of modulo languages (defined below). If $\mathscr{C}$ is defined by a fragment of first-order logic and a structural signature, these language-theoretic operations correspond to adding local or modular predicates to the signature, see Section 4.3. The main result of the paper, Theorem 5.1, states that, for any positive variety $\mathscr{C}$, the covering problem associated to the class $(\mathscr{C} \circ \mathsf{SU}) \circ \mathsf{MOD}$ reduces to the same problem for the class $\mathscr{C} \circ \mathsf{SU}$. $\square$

4.1. **Enrichment of a class of languages.** We first define a technical notion of $\mathbf{P}$-tagging. Let A be an alphabet and $\mathbf{P}$ a finite partition of A^*. For each word $u \in A^*$, we denote by $[u]_{\mathbf{P}} \in \mathbf{P}$ the unique language in $\mathbf{P}$ which contains u. We use the finite set $\mathbf{P} \times A$ as an extended alphabet and define a canonical map $\tau_{\mathbf{P}} \colon A^* \to (\mathbf{P} \times A)^*$ as follows.

Let $w \in A^*$. If $w = \varepsilon$, then we let $\tau_{\mathbf{P}}(\varepsilon) = \varepsilon$. Otherwise, $w = a_1 \cdots a_n$ with $n \geq 1$ and $a_1, \ldots, a_n \in A$, and we let $\tau_{\mathbf{P}}(w) = b_1 \cdots b_n$ with

$$b_1 = ([\varepsilon]_{\mathbf{P}}, a_1) \in \mathbf{P} \times A \quad \text{and} \quad b_i = ([a_1 \cdots a_{i-1}]_{\mathbf{P}}, a_i) \in \mathbf{P} \times A \quad \text{for } 2 \leq i \leq n.$$

We call $\tau_{\mathbf{P}}(w)$ the $\mathbf{P}$-*tagging* of w. It can be viewed as a simple relabeling: each position i in w is given a new label encoding its original label in A and the unique language in $\mathbf{P}$ which contains the prefix ending at position $i - 1$.

Example 4.3. On alphabet $A = \{a, b\}$, consider the languages P_0, P_1, P_2, defined by $P_m = \{w \in A^* \mid |w| = m \mod 3\}$. Clearly, $\mathbf{P} = \{P_0, P_1, P_2\}$ is a partition of A^*. The $\mathbf{P}$-tagging of $w = babbbaaa$ is $\tau_{\mathbf{P}}(w) = (P_0, b)(P_1, a)(P_2, b)(P_0, b)(P_1, b)(P_2, a)(P_0, a)(P_1, a)$. $\square$

Remark 4.4. Note that the map $w \mapsto \tau_{\mathbf{P}}(w)$ is not a morphism, nor is it surjective in general. There are usually compatibility constraints between consecutive positions in $\tau_{\mathbf{P}}(w)$. This can be observed in Example 4.3. On the other hand, $\tau_{\mathbf{P}}$ is clearly injective. $\square$

The following fact is an immediate consequence of the definition.

Fact 4.5. *Let A be an alphabet and $\mathbf{P}$ a finite partition of A^*. Then for any $a \in A$ and $u \in A^*$, we have $\tau_{\mathbf{P}}(ua) = \tau_{\mathbf{P}}(u) \cdot ([u]_{\mathbf{P}}, a)$.*

We now explain how one may use taggings to build new languages from those contained in a fixed class. Consider an arbitrary class $\mathscr{C}$ and an alphabet A. Let $\mathbf{P}$ be a finite partition of A^*. We say that a language $L \subseteq A^*$ is $\mathbf{P}$-*liftable from $\mathscr{C}$* if there exist languages $L_P \in \mathscr{C}(\mathbf{P} \times A)$ for every $P \in \mathbf{P}$ such that

$$L = \bigcup_{P \in \mathbf{P}} \left(\tau_{\mathbf{P}}^{-1}(L_P) \cap P \right).$$

We may now define enrichment. Consider two classes of languages $\mathscr{C}$ and $\mathscr{D}$. If A is an alphabet, a *finite* partition of A^* into languages of $\mathscr{D}$ is called a $\mathscr{D}$-*partition of A^**. The $\mathscr{D}$-*enrichment of $\mathscr{C}$*, written $\mathscr{C} \circ \mathscr{D}$, is the class such that for every alphabet A, $(\mathscr{C} \circ \mathscr{D})(A)$ consists of the languages $L \subseteq A^*$ which are $\mathbf{P}$-liftable from $\mathscr{C}$, for some $\mathscr{D}$-partition $\mathbf{P}$ of A^*.

Before we investigate the properties of classes that are built with enrichment, let us present two technical lemmas. We shall use them to select appropriate $\mathscr{D}$-partitions for building languages in $\mathscr{C} \circ \mathscr{D}$.

Lemma 4.6. *Let $\mathscr{C}$ be a class closed under inverse length increasing morphism and A an alphabet. Let $\mathbf{P}$ and $\mathbf{Q}$ be finite partitions of A^* such that $\mathbf{P}$ refines $\mathbf{Q}$. Then every language $L \subseteq A^*$ which is $\mathbf{Q}$-liftable from $\mathscr{C}$ is also $\mathbf{P}$-liftable from $\mathscr{C}$.*

Proof. Let $L \subseteq A^*$ be $\mathbf{Q}$-liftable from $\mathscr{C}$. There are languages $L_Q \in \mathscr{C}(\mathbf{Q} \times A)$ for every $Q \in \mathbf{Q}$ such that

$$L = \bigcup_{Q \in \mathbf{Q}} \left(\tau_{\mathbf{Q}}^{-1}(L_Q) \cap Q \right).$$

Since $\mathbf{P}$ refines $\mathbf{Q}$, for every $P \in \mathbf{P}$, there exists a unique language $Q_P \in \mathbf{Q}$ such that $P \subseteq Q_P$. We use this to define a length increasing morphism $\alpha : (\mathbf{P} \times A)^* \to (\mathbf{Q} \times A)^*$. For every letter $(P, a) \in \mathbf{P} \times A$, we define $\alpha((P, a)) = (Q_P, a)$. It is now simple to verify from the definitions that

$$L = \bigcup_{P \in \mathbf{P}} \left(\tau_{\mathbf{P}}^{-1}(\alpha^{-1}(L_{Q_P})) \cap P \right).$$

Since $\mathscr{C}$ is closed under inverse length increasing morphism, it is immediate that for every $P \in \mathbf{P}$, we have $\alpha^{-1}(L_{Q_P}) \in \mathscr{C}(\mathbf{P} \times A)$. Therefore L is $\mathbf{P}$-liftable from $\mathscr{C}$, as desired.   □

The second lemma shows that we may always work with a $\mathscr{D}$-partition which satisfies some additional properties (provided that $\mathscr{D}$ is sufficiently robust). Recall that a finite partition $\mathbf{P}$ of A^* is a (finite index) *congruence* if $[u]_{\mathbf{P}}[v]_{\mathbf{P}}$ is contained in $[uv]_{\mathbf{P}}$ for every $u, v \in A^*$. In that case, the set $\mathbf{P}$ is a monoid for the operation $[u]_{\mathbf{P}} \bullet [v]_{\mathbf{P}} = [uv]_{\mathbf{P}}$ and the map $w \mapsto [w]_{\mathbf{P}}$ is a morphism from A^* to $\mathbf{P}$. We talk of a *$\mathscr{D}$-congruence* if $\mathbf{P}$ is a $\mathscr{D}$-partition and a finite index congruence.

Lemma 4.7. *Let $\mathscr{C}$ be a class closed under inverse length increasing morphism and $\mathscr{D}$ a quotienting Boolean algebra. Let A be an alphabet and $L \in (\mathscr{C} \circ \mathscr{D})(A)$. Then there exists a $\mathscr{D}$-congruence $\mathbf{P}$ of A^* such that L is $\mathbf{P}$-liftable from $\mathscr{C}$.*

Proof. By definition L is $\mathbf{Q}$-liftable from an arbitrary $\mathscr{D}$-partition $\mathbf{Q}$ of A^*. Thus, by Lemma 4.6, it suffices to show that there exists a $\mathscr{D}$-congruence $\mathbf{P}$ which refines $\mathbf{Q}$. Since $\mathbf{Q}$ is a finite set, it is folklore[2] (see e.g. [RW95, Prop. 1.3]) that one may construct a finite monoid M and a surjective morphism $\eta : A^* \to M$ satisfying the following properties.

- Every $Q \in \mathbf{Q}$ is recognized by η.
- Every language recognized by η is a Boolean combination of languages having the form $u^{-1} Q v^{-1}$ with $Q \in \mathbf{Q}$ and $u, v \in A^*$.

For every $s \in M$, let $P_s = \eta^{-1}(s)$. We let $\mathbf{P} = \{P_s \mid s \in M\}$. Clearly, $\mathbf{P}$ is a finite partition of A^* and a congruence. The first assertion implies that $\mathbf{P}$ refines $\mathbf{Q}$ and the second one that $\mathbf{P}$ is a $\mathscr{D}$-partition since $\mathscr{D}$ is a quotienting Boolean algebra.   □

4.2. **Closure properties of enrichment.** The definition of enrichment makes sense for any two classes $\mathscr{C}$ and $\mathscr{D}$. However, one needs a few hypotheses on $\mathscr{C}$ and $\mathscr{D}$ for it to be robust. The technical proposition below summarizes the closure properties we will need.

Proposition 4.8. *Let $\mathscr{C}$ be a positive $\mathbf{li}$-variety and $\mathscr{D}$ a $\mathbf{li}$-variety. Then $\mathscr{C} \circ \mathscr{D}$ is a positive $\mathbf{li}$-variety containing $\mathscr{C}$ and $\mathscr{D}$.*

---

[2]It is important here that all languages considered in the paper are regular.

Proof. We fix the positive **li**-variety $\mathscr{C}$ and the **li**-variety of regular languages $\mathscr{D}$ for the proof. There are several properties of $\mathscr{C} \circ \mathscr{D}$ to show.

Containment. We first prove that $\mathscr{C} \circ \mathscr{D}$ contains $\mathscr{C}$ and $\mathscr{D}$. Consider an alphabet A. We start with $\mathscr{D}$. Let $L \in \mathscr{D}(A)$. Since $\mathscr{D}$ is a Boolean algebra, $\mathbf{P} = \{L, A^* \setminus L\}$ is a $\mathscr{D}$-partition of A^*. Moreover $(\mathbf{P} \times A)^*$ and $\emptyset$ lie in the lattice $\mathscr{C}(\mathbf{P} \times A)$. The equality

$$L = \left(\tau_{\mathbf{P}}^{-1}((\mathbf{P} \times A)^*) \cap L\right) \cup \left(\tau_{\mathbf{P}}^{-1}(\emptyset) \cap (A^* \setminus L)\right)$$

then shows that $L \in (\mathscr{C} \circ \mathscr{D})(A)$. We turn to $\mathscr{C}$. Consider $L \in \mathscr{C}(A)$. Let $\mathbf{Q} = \{A^*\}$ which is clearly a $\mathscr{D}$-partition of A^*. Moreover consider the morphism $\alpha : (\mathbf{Q} \times A)^* \to A^*$ defined by $\alpha(A^*, a) = a$ for all $a \in A$. Since $\mathscr{C}$ is closed under inverse length increasing morphism, we have $\alpha^{-1}(L) \in \mathscr{C}(\mathbf{Q} \times A)$. It is now clear that

$$L = \tau_{\mathbf{Q}}^{-1}(\alpha^{-1}(L)) \cap A^*.$$

This yields as desired that $L \in (\mathscr{C} \circ \mathscr{D})(A)$.

Union and intersection. We now prove that $\mathscr{C} \circ \mathscr{D}$ is a lattice. Consider an alphabet A. First we verify that $A^*, \emptyset \in \mathscr{C} \circ \mathscr{D}$. This follows from the observation that $\mathbf{P} = \{A^*\}$ always is a $\mathscr{D}$-partition and $L_{A^*} = A^*$ always sits in the lattice $\mathscr{C}$: then $A^* = \bigcup_{P \in \mathbf{P}} \tau_P^{-1}(L_P) \cap P$ is in $\mathscr{C} \circ \mathscr{D}$. The same holds for $\emptyset$ if we let $L_{A^*} = \emptyset$. Now let $K, L \in (\mathscr{C} \circ \mathscr{D})(A)$. We show that $K \cup L$ and $L \cap K$ belong to $(\mathscr{C} \circ \mathscr{D})(A)$ as well. By definition there exist $\mathscr{D}$-partitions $\mathbf{P}_K$ and $\mathbf{P}_L$ of A^* such that K and L are respectively $\mathbf{P}_K$-liftable and $\mathbf{P}_L$-liftable from $\mathscr{C}$. Since $\mathscr{D}$ is a Boolean algebra, it is immediate that we may construct a third $\mathscr{D}$-partition $\mathbf{P}$ of A^* which refines both $\mathbf{P}_K$ and $\mathbf{P}_L$. By Lemma 4.6, this implies that K and L are both $\mathbf{P}$-liftable from $\mathscr{C}$. Therefore there exist languages $K_P, L_P \in \mathscr{C}(\mathbf{P} \times A)$, for every $P \in \mathbf{P}$, such that

$$K = \bigcup_{P \in \mathbf{P}} \left(\tau_{\mathbf{P}}^{-1}(K_P) \cap P\right) \quad \text{and} \quad L = \bigcup_{P \in \mathbf{P}} \left(\tau_{\mathbf{P}}^{-1}(L_P) \cap P\right).$$

Since inverse images commute with Boolean operations, it follows that

$$K \cup L = \bigcup_{P \in \mathbf{P}} \left(\tau_{\mathbf{P}}^{-1}(K_P \cup L_P) \cap P\right) \quad \text{and} \quad K \cap L = \bigcup_{P \in \mathbf{P}} \left(\tau_{\mathbf{P}}^{-1}(K_P \cap L_P) \cap P\right).$$

Since $\mathscr{C}$ is a lattice, it is immediate that $K_P \cup L_P$ and $K_P \cap L_P$ belong to $\mathscr{C}(\mathbf{P} \times A)$ for every $P \in \mathbf{P}$. Consequently $K \cup L$ and $K \cap L$ are $\mathbf{P}$-liftable from $\mathscr{C}$ and belong to $(\mathscr{C} \circ \mathscr{D})(A)$.

We turn to quotients and inverse morphism. Let A, B be alphabets, $\alpha : B^* \to A^*$ a length increasing morphism and $u \in A^*$. Consider $L \in (\mathscr{C} \circ \mathscr{D})(A)$. We show that $u^{-1}L$ and Lu^{-1} belong to $(\mathscr{C} \circ \mathscr{D})(A)$ and $\alpha^{-1}(L)$ belongs to $(\mathscr{C} \circ \mathscr{D})(B)$. Let us start with an observation.

By hypothesis on $\mathscr{D}$ and Lemma 4.7, there exists a finite index $\mathscr{D}$-congruence $\mathbf{P}$ of A^* such that L is $\mathbf{P}$-liftable from $\mathscr{C}$. It follows that there exist languages $L_P \in \mathscr{C}(\mathbf{P} \times A)$ for every $P \in \mathbf{P}$ such that

$$L = \bigcup_{P \in \mathbf{P}} \left(\tau_{\mathbf{P}}^{-1}(L_P) \cap P\right).$$

Since $\mathbf{P}$ is a congruence, $\mathbf{P}$ is a monoid for an operation denoted by $\bullet$, such that the map $w \mapsto [w]_{\mathbf{P}}$ is a morphism. If $P \in \mathbf{P}$, we denote by λ_P the (length increasing) morphism from $(\mathbf{P} \times A)^*$ to itself given by $\lambda_P((Q, a)) = (P \bullet Q, a)$ for every $(Q, a) \in \mathbf{P} \times A$. One may verify from the definitions that for every $u, v \in A^*$, we have

$$\tau_{\mathbf{P}}(uv) = \tau_{\mathbf{P}}(u)\lambda_{[u]_{\mathbf{P}}}(\tau_{\mathbf{P}}(v)).$$

Right quotients. We first show that $Lu^{-1} \in (\mathscr{C} \circ \mathscr{D})(A)$. Let $P \in \mathbf{P}$ and $v \in P$. Then $v \in Lu^{-1}$ if and only if $vu \in L$, if and only if $\tau_{\mathbf{P}}(vu) \in L_Q$, where $Q = [vu]_{\mathbf{P}} = [v]_{\mathbf{P}} \bullet [u]_{\mathbf{P}} = P \bullet [u]_{\mathbf{P}}$. Since $\tau_{\mathbf{P}}(vu) = \tau_{\mathbf{P}}(v) \, \lambda_{[v]_{\mathbf{P}}}(\tau_{\mathbf{P}}(u)) = \tau_{\mathbf{P}}(v) \, \lambda_P(\tau_{\mathbf{P}}(u))$, we find that

$$Lu^{-1} \cap P = \{v \in A^* \mid \tau_{\mathbf{P}}(v) \in L_Q(\lambda_P(\tau_{\mathbf{P}}(u)))^{-1}\} \cap P.$$

Then if we let $M_P = L_{P \bullet [u]_{\mathbf{P}}}(\lambda_P(\tau_{\mathbf{P}}(u)))^{-1}$ for each $P \in \mathbf{P}$, we get

$$Lu^{-1} = \bigcup_{P \in \mathbf{P}} \left(\tau_{\mathbf{P}}^{-1}(M_P) \cap P \right).$$

Since $\mathscr{C}$ is quotient-closed, this establishes that $Lu^{-1} \in (\mathscr{C} \circ \mathscr{D})(A)$.

Left quotients. We turn to the proof that $u^{-1}L \in (\mathscr{C} \circ \mathscr{D})(A)$. Let $P \in \mathbf{P}$ and $v \in P$. Then $v \in u^{-1}L$ if and only if $uv \in L$, if and only if $\tau_{\mathbf{P}}(uv) \in L_{[u]_{\mathbf{P}} \bullet P}$, if and only if $\tau_{\mathbf{P}}(u)\lambda_{[u]_{\mathbf{P}}}(\tau_{\mathbf{P}}(v)) \in L_{[u]_{\mathbf{P}} \bullet P}$. Therefore, if we let $M_P = \lambda_{[u]_{\mathbf{P}}}^{-1}(\tau_{\mathbf{P}}(u))^{-1}(L_{[u]_{\mathbf{P}} \bullet P})$, we find that

$$u^{-1}L = \bigcup_{P \in \mathbf{P}} \left(\tau_{\mathbf{P}}^{-1}(M_P) \cap P \right).$$

Since $\mathscr{C}$ is quotient-closed and closed under length increasing morphisms, this establishes that $u^{-1}L \in (\mathscr{C} \circ \mathscr{D})(A)$, and concludes the proof for quotients.

Inverse length increasing morphisms. It remains to show that $\alpha^{-1}(L) \in (\mathscr{C} \circ \mathscr{D})(B)$. Consider the finite partition $\mathbf{Q}$ of B^* given by

$$\mathbf{Q} = \{\alpha^{-1}(P) \mid P \in \mathbf{P} \text{ and } \alpha^{-1}(P) \neq \emptyset\}.$$

Then $\mathbf{Q}$ is a $\mathscr{D}$-partition since $\mathbf{P}$ is one and $\mathscr{D}$ is closed under inverse length increasing morphisms.

We define a morphism $\beta \colon (\mathbf{Q} \times B)^* \to (\mathbf{P} \times A)^*$ as follows. Let (Q, b) be a letter in $\mathbf{Q} \times B$. By definition of $\mathbf{Q}$, $Q = \alpha^{-1}(P)$ for a uniquely determined $P \in \mathbf{P}$ and in particular, $P = [\alpha(u)]_{\mathbf{P}}$ for any $u \in Q$. Then we let

$$\beta((Q, b)) = \lambda_P(\tau_{\mathbf{P}}(\alpha(b))).$$

Clearly, this defines a morphism $\beta \colon (\mathbf{Q} \times B)^* \to (\mathbf{P} \times A)^*$. Moreover, it is length increasing since both λ_P and α are.

Fact 4.9. *The morphism β satisfies $\beta \circ \tau_{\mathbf{Q}} = \tau_{\mathbf{P}} \circ \alpha$.*

Proof. We verify that $\beta \circ \tau_{\mathbf{Q}}(w) = \tau_{\mathbf{P}} \circ \alpha(w)$ for every $w \in B^*$, by induction on the length of w. The result is trivial if $w = \varepsilon$ and we now assume that $|w| \geq 1$. Then $w = ub$ for some letter $b \in B$ and word $u \in B^*$. By Fact 4.5, $\tau_{\mathbf{Q}}(w) = \tau_{\mathbf{Q}}(u) \cdot ([u]_{\mathbf{Q}}, b)$ and it follows, by induction, that

$$\beta(\tau_{\mathbf{Q}}(w)) = \beta(\tau_{\mathbf{Q}}(u)) \, \beta(([u]_{\mathbf{Q}}, b)) = \tau_{\mathbf{P}}(\alpha(u)) \, \beta(([u]_{\mathbf{Q}}, b)).$$

By definition, $\beta(([u]_{\mathbf{Q}}, b)) = \lambda_P(\tau_{\mathbf{P}}(\alpha(b)))$, where $P = [\alpha(u)]_{\mathbf{P}}$. Therefore

$$\beta(\tau_{\mathbf{Q}}(w)) = \tau_{\mathbf{P}}(\alpha(u)) \, \lambda_{[\alpha(u)]_{\mathbf{P}}}(\tau_{\mathbf{P}}(\alpha(b))) = \tau_{\mathbf{P}}(\alpha(u)\alpha(b)) = \tau_{\mathbf{P}}(\alpha(ub)) = \tau_{\mathbf{P}}(\alpha(w)),$$

as desired. $\qquad\square$

Recall that we have languages $L_P \in \mathscr{C}(\mathbf{P} \times A)$ for every $P \in \mathbf{P}$ such that

$$L = \bigcup_{P \in \mathbf{P}} \left(\tau_{\mathbf{P}}^{-1}(L_P) \cap P \right).$$

Fact 4.9 shows that

$$\alpha^{-1}(L) = \bigcup_{P \in \mathbf{P}} \left(\alpha^{-1}(\tau_{\mathbf{P}}^{-1}(L_P)) \cap \alpha^{-1}(P) \right) = \bigcup_{P \in \mathbf{P}} \left(\tau_{\mathbf{Q}}^{-1}(\beta^{-1}(L_P)) \cap \alpha^{-1}(P) \right).$$

For each $Q \in \mathbf{Q}$, we note that $Q = \alpha^{-1}(P)$ for a uniquely defined $P \in \mathbf{P}$, and we let $H_Q = \beta^{-1}(L_P)$. Since $\mathscr{C}$ is closed under inverse (length increasing) morphisms, every H_Q lies in $\mathscr{C}(\mathbf{Q} \times B)$ and we have

$$\alpha^{-1}(L) = \bigcup_{Q \in \mathbf{Q}} (\tau_{\mathbf{Q}}^{-1}(H_Q) \cap Q),$$

showing directly that $\alpha^{-1}(L) \in (\mathscr{C} \circ \mathscr{D})(B)$. This concludes the proof of Proposition 4.8. $\square$

4.3. **Enrichment by modulo languages.** As mentioned in Remark 4.2, we are mainly interested in the special instances of $\mathscr{D}$-enrichment for two particular classes $\mathscr{D}$. This is because these operations are the language-theoretic counterparts of the logical enrichment operations with local and modular predicates that we introduced in Section 3.2.

We begin with the class MOD (*modulo languages*). We first define it and then show that MOD-enrichment corresponds exactly to enriching signatures with modular predicates. For every alphabet A, MOD(A) consists of the finite Boolean combinations of languages of the form $\{w \in A^* \mid |w| = m \mod d\}$, with $m, d \in \mathbb{N}$ and $m < d$. The following is immediately verified.

Proposition 4.10. *The class* MOD *is a quotienting Boolean algebra.*

Remark 4.11. MOD is not closed inverse morphisms, nor even under inverse length increasing morphisms. Indeed, let $A = \{a, b\}$ and consider the language $L = \{w \in A^* \mid |w| = 0 \mod 2\} \in$ MOD. Let $\alpha \colon A^* \to A^*$ be the morphism defined by $\alpha(a) = aa$ and $\alpha(b) = b$. One may verify that $\alpha^{-1}(L) = \{w \in A^* \mid 2|w|_a + |w|_b = 0 \mod 2\}$ (here $|w|_a$ denotes the number of copies of the letter "a" occurring in w), a language outside MOD. It is known that MOD is closed under a weaker variant of inverse morphisms: inverse length multiplying morphisms (we shall not need this property). A morphism $\alpha \colon A^* \to B^*$ is *length multiplying* when there exists $k \geq 1$ depending only on α such that for every $w \in A^*$, we have $|\alpha(w)| = k|w|$. $\square$

We complete this definition with the following lemma. It states an elementary, yet useful property of MOD.

Lemma 4.12. *Let A be an alphabet and $L \in$ MOD(A). There exists a natural number $k \geq 1$ such that for every $w, w' \in A^*$, if $|w|$ and $|w'|$ are congruent modulo k, then $w \in L$ if and only if $w' \in L$.*

Proof. By definition, L is a Boolean combination of languages of the form $\{w \in A^* \mid |w| = m \mod d\}$ for some $m, d \in \mathbb{N}$. It suffices to let k be the least common multiple of these d. $\square$

We now connect MOD-enrichment with the logical operation of enriching signatures with modular predicates. For every fragment $\mathscr{F}$ and every structural signature $\boldsymbol{S}$, the equality $\mathscr{F}(\boldsymbol{S}) \circ \mathsf{MOD} = \mathscr{F}(\boldsymbol{S}, \mathbf{MOD})$ holds. This result is essentially folklore. However, the proofs available in the literature only apply to specific fragments and signatures. For example, a proof that $\mathscr{B}\Sigma_1(<, \mathbf{MOD}) = \mathscr{B}\Sigma_1(<) \circ \mathsf{MOD}$ is available in [CPS06]. Here, we properly establish the generic correspondence.

Theorem 4.13. *Let $\mathscr{F}$ be a fragment of first-order logic and let $\boldsymbol{S}$ be a structural signature. Then $\mathscr{F}(\boldsymbol{S}) \circ \mathsf{MOD} = \mathscr{F}(\boldsymbol{S}, \mathbf{MOD})$.*

Proof. The two directions in the proof are handled separately.

From $\mathscr{F}(\boldsymbol{S}) \circ \mathsf{MOD}$ to $\mathscr{F}(\boldsymbol{S}, \mathbf{MOD})$. Let L be a language in $(\mathscr{F}(\boldsymbol{S}) \circ \mathsf{MOD})(A)$. By definition, there exists a MOD-partition $\mathbf{P}$ of A^* and a language $L_P \subseteq (\mathbf{P} \times A)^*$ in $\mathscr{F}(\boldsymbol{S})$ for every $P \in \mathbf{P}$ such that
$$L = \bigcup_{P \in \mathbf{P}} \left(\tau_{\mathbf{P}}^{-1}(L_P) \cap P \right).$$
We want to show that $L \in \mathscr{F}(\boldsymbol{S}, \mathbf{MOD})(A)$. Since $\mathscr{F}$ is a fragment of first-order logic, it is closed under conjunctions and disjunctions, and it suffices to prove that for each $P \in \mathbf{P}$, both P and $\tau_{\mathbf{P}}^{-1}(L_P)$ are defined by $\mathscr{F}[A, \boldsymbol{S}, \mathbf{MOD}]$ sentences. The argument is based on the following lemma which is immediate from the definition of $\mathsf{MOD}(A)$ and $\mathbf{MOD}$.

Lemma 4.14. *For any language $Q \in \mathsf{MOD}(A)$, the following properties holds:*
(1) *Q is defined by a quantifier-free sentence ψ_Q of $\mathscr{F}[\mathbf{MOD}]$.*
(2) *There exists a quantifier-free formula $\xi_Q(x)$ in $\mathscr{F}[\mathbf{MOD}]$ with one free variable such that for any $w = a_0 \cdots a_n \in A^*$ and any position x in w, $w \models \xi_Q(x)$ if and only if $a_0 \cdots a_{x-1} \in Q$.*

Consider $P \in \mathbf{P}$. Since $\mathbf{P}$ is a MOD-partition, Lemma 4.14 (1) shows that P is defined by the sentence ψ_P in $\mathscr{F}[\mathbf{MOD}]$, which is contained in $\mathscr{F}[A, \boldsymbol{S}, \mathbf{MOD}]$.

Now consider the language $\tau_{\mathbf{P}}^{-1}(L_P) \subseteq A^*$. By definition, $L_P \subseteq (\mathbf{P} \times A)^*$ is defined by a sentence φ_P in $\mathscr{F}[\mathbf{P} \times A, \boldsymbol{S}]$. We build an $F[A, \boldsymbol{S}, \mathbf{MOD}]$-sentence $\hat{\varphi}_P$ defining $\tau_{\mathbf{P}}^{-1}(L_P)$ by applying quantifier-free substitutions to φ_P.

Note that the sentence φ_P contains two kinds of atomic formulas: those involving label predicates, of the form $(Q, a)(x)$ for some $(Q, a) \in \mathbf{P} \times A$, and those involving structural predicates in $\boldsymbol{S}$. The sentence $\hat{\varphi}_P$ is obtained from φ_P by replacing each atomic sub-formula $(Q, a)(x)$ in φ_P ($(Q, a) \in \mathbf{P} \times A$) by the quantifier-free $\mathscr{F}[A, \mathbf{MOD}]$-formula:

$$\xi_Q(x) \wedge a(x) \quad \text{where } \xi_Q(x) \text{ is as given by Lemma 4.14 (2).}$$

Then $\hat{\varphi}_P$ belongs to $\mathscr{F}[A, \boldsymbol{S}, \mathbf{MOD}]$ since every fragment is closed under quantifier-free substitutions. Moreover, one can verify directly from the definition of $\tau_{\mathbf{P}} \colon A^* \to (\mathbf{P} \times A)^*$ that $\hat{\varphi}_P$ defines $\tau_{\mathbf{P}}^{-1}(L_P)$. This concludes the proof that L is defined by a sentence in $\mathscr{F}(\boldsymbol{S}, \mathbf{MOD})$.

From $\mathscr{F}(\boldsymbol{S}, \mathbf{MOD})$ to $\mathscr{F}(\boldsymbol{S}) \circ \mathsf{MOD}$. We now want to show that a language L in $\mathscr{F}(\boldsymbol{S}, \mathbf{MOD})$ lies in $\mathscr{F}(\boldsymbol{S}) \circ \mathsf{MOD}$. First, we define an appropriate MOD-partition $\mathbf{P}$ of A^*.

Let φ be a sentence of $\mathscr{F}[A, \boldsymbol{S}, \mathbf{MOD}]$ defining L and let p be the least common multiple of the integers $d \geq 1$ such that φ contains a modular predicate of the form $\mathbf{MOD}_j^d(x)$ or

$\mathbf{D}_j^d$ for some $j < d$ (p is well-defined since φ contains finitely many predicates; we let $p = 1$ if φ contains no modular predicate). For every $i < p$, we define

$$P_i = \{w \in A^* \mid |w| = i \mod p\} \in \mathsf{MOD}$$

and we let $\mathbf{P} = \{P_i \mid i < p\}$. Clearly $\mathbf{P}$ is a MOD-partition of A^* and the following fact holds.

Fact 4.15. *For any predicate* $\mathbf{MOD}_j^d(x)$ *occurring in* φ*, there exists a quantifier-free formula* $\zeta_j^d(x)$ *of* $\mathscr{F}[\mathbf{P} \times A, \boldsymbol{S}]$ *such that for any* $w \in A^*$ *and any position* $x \geq 0$ *in* w*, we have*

$$w \models \mathbf{MOD}_j^d(x) \quad \text{if and only if} \quad \tau_{\mathbf{P}}(w) \models \zeta_j^d(x).$$

Proof. We let

$$\zeta_j^d(x) = \bigvee_{a \in A} \left(\bigvee_{\{i < p \mid j = i \mod d\}} (P_i, a)(x) \right).$$

The result follows since p is a multiple of d. $\qquad\square$

Next we exhibit languages $L_P \subseteq (\mathbf{P} \times A)^*$ for every $P \in \mathbf{P}$, all in $\mathscr{F}(\boldsymbol{S})$ and such that

$$L = \bigcup_{P \in \mathbf{P}} \left(P \cap \tau_{\mathbf{P}}^{-1}(L_P) \right),$$

and for that purpose, we rely on the following lemma.

Lemma 4.16. *For any* $P \in \mathbf{P}$*, there exists a sentence* ψ_P *of* $\mathscr{F}[\mathbf{P} \times A, \boldsymbol{S}]$ *such that for any* $w \in P$*, the following equivalence holds:*

$$w \models \varphi \quad \text{if and only if} \quad \tau_{\mathbf{P}}(w) \models \psi_P.$$

Let us assume for a moment that Lemma 4.16 holds. Then, for each $P \in \mathbf{P}$, we let L_P be the language in $(\mathbf{P} \times A)^*$ defined by the sentence ψ_P provided by Lemma 4.16. By definition, $L_P \in \mathscr{F}(\boldsymbol{S})$, and the equality

$$L = \bigcup_{P \in \mathbf{P}} \left(P \cap \tau_{\mathbf{P}}^{-1}(L_P) \right)$$

follows immediately from the lemma. We finish with the proof of Lemma 4.16.

Proof of Lemma 4.16. By definition $P = P_i$ for some $i < p$ (i.e. P is the language of all words whose length is congruent to i modulo p). We build ψ_P from φ in $\mathscr{F}[A, \boldsymbol{S}, \mathbf{MOD}]$ by replacing each atomic sub-formula by a quantifier-free $\mathscr{F}[\mathbf{P} \times A, \boldsymbol{S}]$ formula as follows:

- the atomic formula $a(x)$ ($a \in A$) is replaced by

$$\bigvee_{Q \in \mathbf{P}} (Q, a)(x);$$

- an atomic formula involving the structural predicates in $\boldsymbol{S}$ remains unchanged;
- the atomic formula $\mathbf{MOD}_j^d(x)$ (with $j < d$) is replaced by the formula $\zeta_j^d(x)$ given by Fact 4.15;
- the atomic formula $\mathbf{D}_j^d$ (with $j < d$) is replaced by $\top$ if i and j are congruent modulo d and $\bot$ otherwise.

Since $P = P_i = \{w \in A^* \mid |w| = i \mod p\}$ and p is a multiple of d, if $j < p$, then either every word in P satisfies $\mathbf{D}_j^d$ (exactly when i and j are congruent modulo d) or no word in P does. It is now straightforward to verify that ψ_P satisfies the desired property: for any $w \in P$, $w \models \varphi$ if and only if $\tau_{\mathbf{P}}(w) \models \psi_P$. $\square$

This concludes the proof of Theorem 4.13. $\square$

4.4. **Enrichment by suffix languages.** We now consider enrichment of logical signatures by local predicates. In most cases, it corresponds to SU-enrichment where SU denotes the class of suffix languages, defined below.

Remark 4.17. There is a significant difference with what happened for MOD-enrichment and modular predicates. The correspondence stated in Theorem 4.13 is *generic*. This is not the case here. It is true that in almost all relevant cases, the equality $\mathscr{F}(\boldsymbol{S}) \circ \mathsf{SU} = \mathscr{F}(\boldsymbol{S}, +1)$ holds. However, this is not a generic theorem and there are counter-examples. For example, consider $\mathsf{FO}(\emptyset)$ (i.e. the structural signature is empty and only the label predicates are available). It turns out that the class $\mathsf{FO}(+1)$ is strictly larger than $\mathsf{FO}(\emptyset) \circ \mathsf{SU}$.

In practice, establishing the equality $\mathscr{F}(\boldsymbol{S}) \circ \mathsf{SU} = \mathscr{F}(\boldsymbol{S}, +1)$ requires a proof that is specific to $\mathscr{F}(\boldsymbol{S})$, and often technical and tedious. Fortunately, this has already been achieved for the classes that we consider in the paper. $\square$

Let us first define SU. For every alphabet A, $\mathsf{SU}(A)$ consists of the finite Boolean combinations of languages of the form A^*w, for some $w \in A^*$. These languages are sometimes called *definite*, see *e.g.*, [Eil76, Str85]. Again, the following is folklore and elementary.

Proposition 4.18. *The class* SU *is an* **li**-*variety.*

We consider a natural stratification $(\mathsf{SU}_k)_k$ within SU: for every $k \in \mathbb{N}$ and every alphabet A, we let $\mathsf{SU}_k(A)$ be the set of Boolean combinations of languages of the form A^*w, where $w \in A^*$ and $|w| \le k$. Note that every $\mathsf{SU}_k(A)$ is finite. Each stratum SU_k is an **li**-variety. Moreover, for every alphabet A, we have

$$\mathsf{SU}_k(A) \subseteq \mathsf{SU}_{k+1}(A) \text{ for every } k \in \mathbb{N} \qquad \text{and} \qquad \bigcup_{k \in \mathbb{N}} \mathsf{SU}_k(A) = \mathsf{SU}(A).$$

Given an alphabet A and an integer $k \in \mathbb{N}$, the equivalence relation $\sim_k$ on A^* is defined as follows if $w, w' \in A^*$, we let $w \sim_k w'$ if and only if the following condition holds:

$$\text{For every language } L \in \mathsf{SU}_k(A), \quad w \in L \Leftrightarrow w' \in L.$$

In other words, $w \sim_k w'$ if and only if $w = w'$ or $|w|, |w'| \ge k$ and w and w' have the same length k suffix. Note that $\sim_k$ has finite index since SU_k is finite. Since every stratum SU_k is a Boolean algebra, the following lemma is immediate.

Lemma 4.19. *Let* $k \in \mathbb{N}$. *For every alphabet* A, *the languages in* $\mathsf{SU}_k(A)$ *are exactly the unions of* $\sim_k$-*classes.*

As announced, it is known that for important fragments of first-order, SU-enrichment corresponds the logical operation of enrichment by local predicates. This goes back to Straubing [Str85] for the quantifier alternation hierarchies, and to Thérien and Wilke [TW98] for FO^2. Place and Zeitoun reformulated these results in terms of language class enrichment in [PZ17a, Prop. 5.2 and 6.2].

Theorem 4.20. *Let $\mathscr{F}$ be one of the following fragments of first-order logic: FO^2, Σ_n, $\mathscr{B}\Sigma_n$ ($n \geq 1$). Then $\mathscr{F}(<) \circ \mathsf{SU} = \mathscr{F}(<,+1)$.*

Another useful result is that applying SU-enrichment to $\mathsf{FO}(<)$ does not build a larger class. This not surprising: as we explained in Remark 3.3, the classes $\mathsf{FO}(<)$ and $\mathsf{FO}(<,+1)$ coincide. We prove this in the following proposition.

Proposition 4.21. *We have $\mathsf{FO}(<) \circ \mathsf{SU} = \mathsf{FO}(<)$.*

Proof. Since $\mathsf{FO}(<)$ is a variety, it is immediate from Proposition 4.8 that $\mathsf{FO}(<)$ is contained in $\mathsf{FO}(<) \circ \mathsf{SU}$. We now verify the converse inclusion. Let A be an alphabet and consider $L \in (\mathsf{FO}(<) \circ \mathsf{SU})(A)$. We show that $L \in \mathsf{FO}(<)$. By definition, there exists an SU-partition $\mathbf{P}$ of A^* such that L is $\mathbf{P}$-liftable from $\mathsf{FO}(<)$. Thus, we have languages $L_P \in \mathsf{FO}(<)(\mathbf{P} \times A)$ for every $P \in \mathbf{P}$ such that

$$L = \bigcup_{P \in \mathbf{P}} \tau_{\mathbf{P}}^{-1}(L_P) \cap P.$$

Since $\mathsf{FO}(<)$ is closed under union and intersection, it suffices to show that for each P in $\mathbf{P}$, both P and $\tau_{\mathbf{P}}^{-1}(L_P)$ are in $\mathsf{FO}(<)$. We use the following fact.

Fact 4.22. *For every $K \in \mathsf{SU}(A)$, one may build the following $\mathsf{FO}[A,<]$ formulas:*
- *a sentence φ_K which defines K;*
- *a formula $\psi_K(x)$ with one free variable x such that, for every word $u \in A^*$ and every position i in u, $u \models \psi_K(i)$ if and only if the prefix of u ending at position $i-1$ belongs to K.*

Proof. By definition a language $K \in \mathsf{SU}(A)$ is a Boolean combination of languages having the form A^*w for some $w \in A^*$. Hence, since one may freely use Boolean connectives in first-order formulas, it suffices to consider the case when K itself is of this form, $K = A^*w$. Let $a_1, \ldots, a_n \in A$ such that $w = a_1 \cdots a_n$. Recall that we may also freely use the successor predicate in $\mathsf{FO}[A,<]$ formulas since $x+1 = y$ is equivalent to $x < y \wedge \neg (\exists z\ x < z \wedge z < y)$. We may use max as well, as $\mathsf{max}(x)$ is equivalent to $\neg(\exists y\ x < y)$. We define φ_K as the following sentence:

$$\exists x_1 \cdots \exists x_n \quad \mathsf{max}(x_n) \wedge \left(\bigwedge_{1 \leq i \leq n} a_i(x_i) \right) \wedge \left(\bigwedge_{1 \leq i \leq n-1} x_i + 1 = x_{i+1} \right).$$

Furthermore, we define $\psi_K(x)$ as the following formula:

$$\exists x_1 \cdots \exists x_n \quad (x_n + 1 = x) \wedge \left(\bigwedge_{1 \leq i \leq n} a_i(x_i) \right) \wedge \left(\bigwedge_{1 \leq i \leq n-1} x_i + 1 = x_{i+1} \right).$$

One may verify that these formulas have the expected semantics. This concludes the proof of Fact 4.22. □

We may now finish the proof. Consider $P \in \mathbf{P}$. Since $\mathbf{P}$ is an SU-partition, we have $P \in \mathsf{SU}$ and it is immediate that $P \in \mathsf{FO}(<)$: it is defined by sentence φ_P given by Fact 4.22. It remains to show that $\tau_{\mathbf{P}}^{-1}(L_P) \in \mathsf{FO}(<)$. By hypothesis, $L_P \in \mathsf{FO}(<)(\mathbf{P} \times A)$. Thus, it is defined by a sentence ζ of $\mathsf{FO}[\mathbf{P} \times A, <]$. It is immediate, from the definition

of $\tau_{\mathbf{P}}$, that $\tau_{\mathbf{P}}^{-1}(L_P)$ is defined by the formula ζ' of $\mathsf{FO}[A, <]$ obtained by replacing every occurrence of an atomic formula $(Q, a)(x)$ in ζ by the formula

$$\psi_Q(x) \wedge a(x) \quad \text{where } \psi_Q(x) \text{ is the formula given by Fact 4.22.}$$

This implies that $\tau_{\mathbf{P}}^{-1}(L_P) \in \mathsf{FO}(<)$, finishing the proof.   □

5. Main theorem

We are now ready to present our main theorem. As announced, it states a generic reduction for the covering problem which applies to classes of the form $(\mathscr{C} \circ \mathsf{SU}) \circ \mathsf{MOD}$ where $\mathscr{C}$ is a positive variety.

Theorem 5.1. *Let $\mathscr{C}$ be a positive variety. The covering (resp. separation) problem for $(\mathscr{C} \circ \mathsf{SU}) \circ \mathsf{MOD}$ can be effectively reduced to the same problem for $\mathscr{C} \circ \mathsf{SU}$.*

Theorem 5.1 can be combined with another reduction theorem for classes of the form $\mathscr{C} \circ \mathsf{SU}$ ([PZ15a] and [PZ17a, Thm 4.12], see also [Ste01] for an algebraic statement relating to the Boolean algebra case): for any positive variety $\mathscr{C}$, the covering problem for $\mathscr{C} \circ \mathsf{SU}$ can be effectively reduced to the same problem for $\mathscr{C}$. When combining these theorems, we obtain the following corollary.

Corollary 5.2. *Let $\mathscr{C}$ be a positive variety. The covering (resp. separation) problem for $(\mathscr{C} \circ \mathsf{SU}) \circ \mathsf{MOD}$ can be effectively reduced to the same problem for $\mathscr{C}$.*

The remaining sections of the paper are devoted to the proof of Theorem 5.1. It is organized as follows. First we show (Theorem 6.6) that, for classes of the form $\mathscr{C} \circ \mathsf{SU}$, MOD-enrichment can be reformulated as yet another operation called block abstraction, written $\mathscr{D} \mapsto [\![\mathscr{D}]\!]$, which is much simpler to handle. Next we show (in Section 7) that for any class $\mathscr{D}$ closed under inverse length increasing morphisms, the $[\![\mathscr{D}]\!]$-covering problem reduces to the $\mathscr{D}$-covering problem. The combination of these two properties establishes Theorem 5.1: for any positive variety $\mathscr{C}$, Proposition 4.8 ensures that $\mathscr{C} \circ \mathsf{SU}$ is closed under inverse length increasing morphisms, and hence the covering problem for $(\mathscr{C} \circ \mathsf{SU}) \circ \mathsf{MOD}$ reduces to the same problem for $\mathscr{C} \circ \mathsf{SU}$.

However, before we start this proof, we discuss applications of Theorem 5.1 and Corollary 5.2: combining them with previously known results yields decidability results for new fragments.

5.1. Full first-order logic.

Let us start with FO itself. We showed in Proposition 4.21 that $\mathsf{FO}(<)$ is stabilized by SU-enrichment: $\mathsf{FO}(<) = \mathsf{FO}(<) \circ \mathsf{SU}$. Moreover, Theorem 4.13 shows that $\mathsf{FO}(<, \mathbf{MOD}) = \mathsf{FO}(<) \circ \mathsf{MOD}$ and, since $\mathsf{FO}(<)$ is a variety, we may instantiate Theorem 5.1 to obtain an effective reduction from $\mathsf{FO}(<, \mathbf{MOD})$-covering to $\mathsf{FO}(<)$-covering.

Finally, $\mathsf{FO}(<)$-covering is known to be decidable (see, *e.g.*, [PZ16b]). Altogether, we get the following corollary.

Corollary 5.3. *The covering problem for $\mathsf{FO}(<, \mathbf{MOD})$ is decidable.*

5.2. **Two-variable first-order logic.** We now consider FO^2. As stated in Theorem 4.20, we have $\mathsf{FO}^2(<,+1) = \mathsf{FO}^2(<) \circ \mathsf{SU}$. When combined with Theorem 4.13, this yields $\mathsf{FO}^2(<,+1,\mathbf{MOD}) = (\mathsf{FO}^2(<) \circ \mathsf{SU}) \circ \mathsf{MOD}$. Since $\mathsf{FO}^2(<)$ is a variety, Corollary 5.2 gives an effective reduction from $\mathsf{FO}^2(<,+1,\mathbf{MOD})$-covering to $\mathsf{FO}^2(<)$-covering.

It was shown in [PZ16a, PZ18] that $\mathsf{FO}^2(<)$-covering is decidable (see also [PvRZ13] for a proof restricted to $\mathsf{FO}^2(<)$-separation). We obtain the following corollary.

Corollary 5.4. *The covering problem for* $\mathsf{FO}^2(<,+1,\mathbf{MOD})$ *is decidable.*

5.3. **Quantifier alternation hierarchy.** Finally, we consider the quantifier alternation hierarchy of first-order logic. We may combine Theorems 4.20 and 4.13 to obtain that for every $n \geq 1$,

$$\Sigma_n(<,+1,\mathbf{MOD}) = (\Sigma_n(<) \circ \mathsf{SU}) \circ \mathsf{MOD} \text{ and } \mathscr{B}\Sigma_n(<,+1,\mathbf{MOD}) = (\mathscr{B}\Sigma_n(<) \circ \mathsf{SU}) \circ \mathsf{MOD}.$$

Since $\Sigma_n(<)$ and $\mathscr{B}\Sigma_n(<)$ are respectively a positive variety and a variety, Corollary 5.2 shows that $\Sigma_n(<,+1,\mathbf{MOD})$-covering (resp. $\mathscr{B}\Sigma_n(<,+1,\mathbf{MOD})$-covering) is effectively reducible to $\Sigma_n(<)$-covering (resp. $\mathscr{B}\Sigma_n(<)$-covering).

It is shown in [PZ14b, Pla15, Pla18] that $\Sigma_1(<)$-, $\Sigma_2(<)$- and $\Sigma_3(<)$-covering are decidable. Moreover, $\mathscr{B}\Sigma_1(<)$- and $\mathscr{B}\Sigma_2(<)$-covering are proved to be decidable in [PZ17c] (there also exists many proofs for the decidability of $\mathscr{B}\Sigma_1(<)$-separation, see [PvRZ13, CMM13]). Altogether, we get the following corollary.

Corollary 5.5. *The covering problem for the levels* $\Sigma_1(<,+1,\mathbf{MOD})$, $\mathscr{B}\Sigma_1(<,+1,\mathbf{MOD})$, $\Sigma_2(<,+1,\mathbf{MOD})$, $\mathscr{B}\Sigma_2(<,+1,\mathbf{MOD})$ *and* $\Sigma_3(<,+1,\mathbf{MOD})$ *is decidable.*

6. BLOCK ABSTRACTION

In this section, we introduce the operation $\mathscr{C} \mapsto [\![\mathscr{C}]\!]$ of *block abstraction*, defined on classes of languages. While less standard than enrichment, this operation is a key ingredient of this paper because of its connection with MOD-enrichment: the two operations coincide for classes of the form $\mathscr{C} \circ \mathsf{SU}$ where $\mathscr{C}$ is a positive variety.

6.1. **Definition of block abstraction.** Let $d \geq 1$ be an integer and A an alphabet. Recall that A^d denotes the set of words with length d. We let $A^{<d} = \bigcup_{0<c<d} A^c$ and $A_d = A^{<d} \cup A^d$. Our intent is to use A_d as an alphabet and form words in $(A_d)^*$. This can be misleading since a letter $w \in A_d$ is also a word in A^*. To avoid confusion, we adopt the following convention: when $w \in A_d$ is used as a letter of the alphabet A_d, we denote it by (w).

We define a map $\mu_d \colon A^* \to A_d^*$ as follows. If $w \in A^*$ has length ℓ, we consider the Euclidean division of ℓ by d: $\ell = dq + r$, with $q, r \in \mathbb{N}$ and $0 \leq r < d$. Then w admits a decomposition $w = w_1 \cdots w_{q+1}$ where $|w_i| = d$ for $1 \leq i \leq q$ and $|w_{q+1}| = r$, and we let

$$\mu_d(w) = \begin{cases} (w_1) \cdots (w_q) & \text{if } w_{q+1} = \varepsilon \text{ (i.e. } r = 0), \\ (w_1) \cdots (w_q)(w_{q+1}) & \text{if } w_{q+1} \neq \varepsilon \text{ (i.e. } r \neq 0). \end{cases}$$

Remark 6.1. The map $\mu_d \colon A^* \to A_d^*$ is not a morphism and it is not surjective: all letters in $\mu_d(w)$, except possibly the last one, are in A^d. However, μ_d is clearly injective. □

We also note the following elementary fact.

Fact 6.2. *Let $d \geq 1$ and $u, v \in A^*$. If the length of u is a multiple of d, then $\mu_d(uv) = \mu_d(u) \cdot \mu_d(v)$.*

Let $\mathscr{C}$ be a class of languages. For any natural number $d \geq 1$, we let $[\![\mathscr{C}]\!]_d$ be the class such that, for any alphabet A, $[\![\mathscr{C}]\!]_d(A)$ consists of the languages L of the form

$$L = \mu_d^{-1}(K) \quad \text{for some language } K \in \mathscr{C}(A_d).$$

The *block abstraction* of $\mathscr{C}$ is defined as the union of the classes $[\![\mathscr{C}]\!]_d$ for $d \geq 1$. More precisely, for any alphabet A, we let

$$[\![\mathscr{C}]\!](A) = \bigcup_{d \geq 1} [\![\mathscr{C}]\!]_d(A).$$

We record a few simple properties of the block abstraction operation.

Lemma 6.3. *Let $\mathscr{C}$ be a class of languages closed under inverse length increasing morphisms. Let $d, n \geq 1$ such that n is a multiple of d. Then $[\![\mathscr{C}]\!]_d \subseteq [\![\mathscr{C}]\!]_n$.*

Proof. If $L \in [\![\mathscr{C}]\!]_d$, then $L = \mu_d^{-1}(K)$ for some language $K \in \mathscr{C}(A_d)$. Now let $\eta \colon A_n^* \to A_d^*$ be the length increasing morphism which maps each letter $(w) \in A_n$ to $\mu_d(w)$. Note in particular that $\mu_d = \eta \circ \mu_n$ (this is where we use the fact that n is a multiple of d). By our hypothesis on $\mathscr{C}$, the language $H = \eta^{-1}(K)$ belongs to $\mathscr{C}(A_n)$ and we have

$$L = \mu_d^{-1}(K) = \mu_n^{-1}(\eta^{-1}(K)) = \mu_n^{-1}(H),$$

which concludes the proof. $\qquad\square$

Corollary 6.4. *Let $\mathscr{C}$ be a class closed under inverse length increasing morphisms and let $L_1, \ldots, L_m$ ($m \geq 1$) be languages in $[\![\mathscr{C}]\!]$. There exists $d \geq 1$ such that $L_1, \ldots, L_m \in [\![\mathscr{C}]\!]_d$.*

Proof. By definition, each L_i ($1 \leq i \leq m$) lies in $[\![\mathscr{C}]\!]_{d_i}$ for some $d_i \geq 1$, and Lemma 6.3 then shows that $L_1, \ldots, L_m \in [\![\mathscr{C}]\!]_d$ where d is the least common multiplier of the d_i. $\quad\square$

This in turn shows that block abstraction preserves closure under Boolean operations.

Corollary 6.5. *If $\mathscr{C}$ is a lattice closed under inverse length increasing morphisms, then its block abstraction $[\![\mathscr{C}]\!]$ is a lattice.*

Proof. Let A be an alphabet. It is immediate that $\emptyset$ and A^* are elements of $[\![\mathscr{C}]\!](A)$. Now let $L_1, L_2 \in [\![\mathscr{C}]\!](A)$. By Corollary 6.4, there exists $d \geq 1$ such that $L_1, L_2 \in [\![\mathscr{C}]\!]_d(A)$, so that $L_1 = \mu_d^{-1}(K_1)$ and $L_2 = \mu_d^{-1}(K_2)$ for some $K_1, K_2 \in \mathscr{C}(A_d)$. Therefore $L_1 \cup L_2 = \mu_d^{-1}(K_1 \cup K_2)$ and $L_1 \cap L_2 = \mu_d^{-1}(K_1 \cap K_2)$, which concludes the proof since $L_1 \cup L_2$ and $L_1 \cap L_2$ both belong to $[\![\mathscr{C}]\!]$. $\quad\square$

We now turn to the main theorem of the section.

Theorem 6.6. *If $\mathscr{C}$ is a positive variety, then $(\mathscr{C} \circ \mathsf{SU}) \circ \mathsf{MOD} = [\![\mathscr{C} \circ \mathsf{SU}]\!]$.*

The rest of this section is devoted to the proof of Theorem 6.6. We fix a positive variety $\mathscr{C}$ and an alphabet A, and we prove separately that $((\mathscr{C} \circ \mathsf{SU}) \circ \mathsf{MOD})(A) \subseteq [\![\mathscr{C} \circ \mathsf{SU}]\!](A)$ and $[\![\mathscr{C} \circ \mathsf{SU}]\!](A) \subseteq ((\mathscr{C} \circ \mathsf{SU}) \circ \mathsf{MOD})(A)$.

6.2. **From modulo enrichment to block abstraction.** We start with the containment $(\mathscr{C} \circ \mathsf{SU}) \circ \mathsf{MOD} \subseteq [\![\mathscr{C} \circ \mathsf{SU}]\!]$. We actually prove the following stronger result.

Proposition 6.7. *If $\mathscr{D}$ is a lattice closed under inverse length increasing morphisms and containing SU, then $\mathscr{D} \circ \mathsf{MOD} \subseteq [\![\mathscr{D}]\!]$.*

With reference to Theorem 6.6, we note that if $\mathscr{C}$ is a positive variety, then $\mathscr{D} = \mathscr{C} \circ \mathsf{SU}$ satisfies the hypothesis of Proposition 6.7, see Proposition 4.8.

Let us now prove Proposition 6.7: let $\mathscr{D}$ be a lattice closed under inverse length increasing morphisms and containing SU, and let $L \in (\mathscr{D} \circ \mathsf{MOD})(A)$. Then there exists a MOD-partition $\mathbf{P}$ of A^* and languages $L_P \in \mathscr{D}(\mathbf{P} \times A)$ for every $P \in \mathbf{P}$ such that

$$L = \bigcup_{P \in \mathbf{P}} \left(\tau_{\mathbf{P}}^{-1}(L_P) \cap P \right).$$

Recall that $[\![\mathscr{D}]\!]$ is a lattice by Corollary 6.5. To show that $L \in [\![\mathscr{D}]\!](A)$, we only need to show that, for every $P \in \mathbf{P}$, both P and $\tau_{\mathbf{P}}^{-1}(L_P)$ belong to $[\![\mathscr{D}]\!](A)$.

The proof that $P \in [\![\mathscr{D}]\!](A)$ is handled by the following lemma.

Lemma 6.8. *If $\mathscr{D}$ is a lattice closed under inverse length increasing morphisms and containing SU, then $\mathsf{MOD} \subseteq [\![\mathscr{D}]\!]$.*

Proof. Let $P \in \mathsf{MOD}(A)$. In view of Lemma 4.12, there exists a natural number $d \geq 1$ such that P is a finite union of languages of the form $P_{m,d} = \{w \in A^* \mid |w| = m \mod d\}$, with $0 \leq m < d$. Since $[\![\mathscr{D}]\!]$ is a lattice, we only need to show that every $P_{m,d}$ is in $[\![\mathscr{D}]\!](A)$.

If $m = 0$, let K be the set of letters of A_d of the form (w) with $w \in A^d$. Then $P_{m,d} = \mu_d^{-1}(A_d^* K \cup \{\varepsilon\})$. Since $A_d^* K \cup \{\varepsilon\}$ belongs to $\mathsf{SU}(A_d)$ and therefore to $\mathscr{D}(A_d)$ by hypothesis on $\mathscr{D}$. It follows that $P_{m,d} \in [\![\mathscr{D}]\!]_d$ as desired.

If $m > 0$, we let similarly K be the set of letters of A_d of the form (w) with $w \in A^m$. Then $P_{m,d} = \mu_d^{-1}(A_d^* K)$ and, since $A_d^* K \in \mathsf{SU}(A_d)$, we have $P_{m,d} \in [\![\mathscr{D}]\!]_d(A)$. $\square$

To conclude the proof, we show that for every MOD-partition $\mathbf{P}$ and every language $K \in \mathscr{D}(\mathbf{P} \times A)$, we have $\tau_{\mathbf{P}}^{-1}(K) \in [\![\mathscr{D}]\!](A)$. We first establish the following lemma.

Lemma 6.9. *There exists a natural number $d \geq 1$ such that for any two words $w, w' \in A^*$, if $|w| = 0 \mod d$, then $\tau_{\mathbf{P}}(ww') = \tau_{\mathbf{P}}(w)\tau_{\mathbf{P}}(w')$.*

Proof. By Lemma 4.12, for each $P \in \mathbf{P}$, there exists $d_P \geq 1$ such that for any $u, v \in A^*$, if $|u| = |v| \mod d_P$, then $u \in P$ if and only if $u \in P$. Using the finiteness of $\mathbf{P}$, we let $d = \mathsf{lcm}\{d_P \mid P \in \mathbf{P}\}$. Then if two words u and v satisfy $|u| = |v| \mod d$, we have $[u]_{\mathbf{P}} = [v]_{\mathbf{P}}$.

Now suppose that $|w| = 0 \mod d$ and that $w' = a_1 \cdots a_n$ with each $a_i \in A$. Using Fact 4.5 recursively, we obtain,

$$\tau_{\mathbf{P}}(ww') = \tau_{\mathbf{P}}(w)([w]_{\mathbf{P}}, a_1)([wa_1]_{\mathbf{P}}, a_2) \cdots ([wa_1 \cdots a_{n-1}]_{\mathbf{P}}, a_n).$$

Moreover, since $|w| = 0 \mod d$, our choice of d implies that $[wa_1 \cdots a_i]_{\mathbf{P}} = [a_1 \cdots a_i]_{\mathbf{P}}$ for every $i \leq n - 1$. Therefore, we have

$$\tau_{\mathbf{P}}(ww') = \tau_{\mathbf{P}}(w)([\varepsilon]_{\mathbf{P}}, a_1)([a_1]_{\mathbf{P}}, a_2) \cdots ([a_1 \cdots a_{n-1}]_{\mathbf{P}}, a_n) = \tau_{\mathbf{P}}(w)\tau_{\mathbf{P}}(w'),$$

which concludes the proof. $\square$

We now show that if $K \in \mathscr{D}(\mathbf{P} \times A)$ and d is given by Lemma 6.9, then $\tau_{\mathbf{P}}^{-1}(K) \in \llbracket \mathscr{D} \rrbracket_d(A) \subseteq \llbracket \mathscr{D} \rrbracket(A)$. Let $\alpha \colon A_d^* \to (\mathbf{P} \times A)^*$ be the morphism given as follows: for each letter $b = (w) \in A_d$ (where $w \in A^+$ is a nonempty word of length at most d), let $\alpha(b) = \tau_{\mathbf{P}}(w)$.

This morphism satisfies $\tau_{\mathbf{P}} = \alpha \circ \mu_d$. Indeed, if $u \in A^*$, we consider the decomposition $u = w_1 \cdots w_n$ such that $|w_i| = d$ for every $i \leq n-1$ and $|w_n| < d$. Then $\mu_d(w) = (w_1) \cdots (w_n)$ and $\alpha \circ \mu_d(u) = \tau_{\mathbf{P}}(w_1) \cdots \tau_{\mathbf{P}}(w_{n-1}) \tau_{\mathbf{P}}(w_n)$. Lemma 6.9 shows then that $\alpha \circ \mu_d(u) = \tau_{\mathbf{P}}(u)$.

Note now that $|\tau_{\mathbf{P}}(w)| = |w|$ by definition, so α is length increasing. It follows that $\alpha^{-1}(K) \in \mathscr{D}(A_d)$ and hence $\tau_{\mathbf{P}}^{-1}(K) = \mu_d^{-1}(\alpha^{-1}(K)) \in \llbracket \mathscr{D} \rrbracket_d(A)$, as announced.

6.3. **From block abstraction to modulo enrichment.** The proof that $\llbracket \mathscr{C} \circ \mathsf{SU} \rrbracket \subseteq (\mathscr{C} \circ \mathsf{SU}) \circ \mathsf{MOD}$ is more involved. Consider a language $L \in \llbracket \mathscr{C} \circ \mathsf{SU} \rrbracket(A)$. By definition, $L \in \llbracket \mathscr{C} \circ \mathsf{SU} \rrbracket_d(A)$ for some integer $d \geq 1$, which we fix for the remainder of the proof. In particular, we let $\mathbf{M} = \{M_i \mid 0 \leq i < d\}$ be the MOD-partition of A^* which counts the length of words modulo d. That is, for any integer $0 \leq i < d$,

$$M_i = \{w \in A^* \mid |w| = i \mod d\}.$$

We reduce the problem to proving the following proposition.

Proposition 6.10. *There exists a language* $H \in (\mathscr{C} \circ \mathsf{SU})(\mathbf{M} \times A)$ *such that* $L = \tau_{\mathbf{M}}^{-1}(H)$.

Indeed, assuming temporarily Proposition 6.10, we see that

$$L = \bigcup_{M \in \mathbf{M}} \left(\tau_{\mathbf{M}}^{-1}(H) \cap M \right)$$

since $\mathbf{M}$ is a partition of A^*. It then follows from the definition that $L \in ((\mathscr{C} \circ \mathsf{SU}) \circ \mathsf{MOD})(A)$ as desired.

We now focus on proving Proposition 6.10. We start by introducing a convenient definition: given a word $w \in A^*$, the *d-cut* of w is the unique pair of words $(u,v) \in (A^*)^2$ such that $w = uv$, $|u| = 0 \mod d$ and $0 \leq |v| \leq d-1$ (in particular, u is the longest prefix of w with length a multiple of d). The following facts hold by definition of the maps $\mu_d \colon A^* \to A_d$ and $\tau_{\mathbf{M}} \colon A^* \to (\mathbf{M} \times A)^*$.

Fact 6.11. *Let* $w \in A^*$ *and let* (u,v) *be its d-cut. Then either* $v = \varepsilon$ *and* $\mu_d(w) = \mu_d(u)$, *or* $v \neq \varepsilon$ *and* $\mu_d(w) = \mu_d(u) \, (v)$. *Moreover,* $\tau_{\mathbf{M}}(w) = \tau_{\mathbf{M}}(u) \, \tau_{\mathbf{M}}(v)$.

By definition of $\mathscr{C} \circ \mathsf{SU}$, the construction of the language $H \in (\mathscr{C} \circ \mathsf{SU})(\mathbf{M} \times A)$ announced in Proposition 6.10 requires first choosing an SU-partition of $(\mathbf{M} \times A)^*$.

Since $L \in \llbracket \mathscr{C} \circ \mathsf{SU} \rrbracket_d(A)$, there exists $K \in (\mathscr{C} \circ \mathsf{SU})(A_d)$ such that $L = \mu_d^{-1}(K)$ and, by definition of SU-enrichment, there exists an SU-partition $\mathbf{P}$ of A_d^* and languages $K_P \in \mathscr{C}(\mathbf{P} \times A_d)$ for every $P \in \mathbf{P}$ such that

$$K = \bigcup_{P \in \mathbf{P}} \left(\tau_{\mathbf{P}}^{-1}(K_P) \cap P \right) \subseteq A_d^*.$$

$\mathbf{P}$ contains finitely many languages in $\mathsf{SU}(A_d)$, so there exists $\ell \in \mathbb{N}$ such that every $P \in \mathbf{P}$ belongs to $\mathsf{SU}_\ell(A_d)$. We then let $k = d(\ell + 1)$ and $\mathbf{U}$ be the partition of $(\mathbf{M} \times A)^*$ into $\sim_k$-classes. By Lemma 4.19, $\mathbf{U}$ is an SU-partition.

To construct $H \in (\mathscr{C} \circ \mathsf{SU})(\mathbf{M} \times A)$ such that $L = \tau_{\mathbf{M}}^{-1}(H)$, we use the following two lemmas, whose proofs are deferred to Sections 6.4 and 6.5.

Lemma 6.12. *Let* $w_1, w_2 \in A^*$ *and* $(u_1, v_1), (u_2, v_2) \in (A^*)^2$ *be their d-cuts. Assume that* $\tau_{\mathbf{M}}(w_1) \sim_k \tau_{\mathbf{M}}(w_2)$. *Then* $[\mu_d(w_1)]_{\mathbf{P}} = [\mu_d(w_2)]_{\mathbf{P}}$, $[\mu_d(u_1)]_{\mathbf{P}} = [\mu_d(u_2)]_{\mathbf{P}}$ *and* $v_1 = v_2$

Lemma 6.13. *There exists a morphism $\alpha\colon (\mathbf{U} \times (\mathbf{M} \times A))^* \to (\mathbf{P} \times A_d)^*$ such that for any word $w \in A^*$ with d-cut $(u,v) \in (A^*)^2$, we have $\tau_{\mathbf{P}}(\mu_d(u)) = \alpha(\tau_{\mathbf{U}}(\tau_{\mathbf{M}}(w)))$.*

For each $U \in \mathbf{U}$, we construct a language $H_U \in \mathscr{C}(\mathbf{U} \times (\mathbf{M} \times A))$ as follows. If U does not intersect $\tau_{\mathbf{M}}(A^*)$, we let $H_U = \emptyset$. Otherwise, it follows from Lemma 6.12 that there exists $P, Q \in \mathbf{P}$ and $x \in A^*$ of length at most $d-1$ such that for any $w \in A^*$ whose d-cut is $(u,v) \in (A^*)^2$, if $\tau_{\mathbf{M}}(w) \in U$, then $[\mu_d(w)]_{\mathbf{P}} = P$, $[\mu_d(u)]_{\mathbf{P}} = Q$ and $v = x$. The definition of H_U in that case uses the morphism α in Lemma 6.13 and depends on whether $x = \varepsilon$ or $x \neq \varepsilon$. Note that if $x \neq \varepsilon$, then (x) is a letter of A_d and $(Q,(x))$ is a letter of $\mathbf{P} \times A_d$. We let

$$H_U = \begin{cases} \alpha^{-1}(K_P \cdot (Q,(x))^{-1}) & \text{when } x \neq \varepsilon \\ \alpha^{-1}(K_P) & \text{when } x = \varepsilon \end{cases}$$

Since $\mathscr{C}$ is closed under right quotients and inverse morphisms, and since $K_P \in \mathscr{C}(\mathbf{P} \times A_d)$, we have $H_U \in \mathscr{C}(\mathbf{U} \times (\mathbf{M} \times A))$. We then define a language H on alphabet $\mathbf{M} \times A$ as follows:

$$H = \bigcup_{U \in \mathbf{U}} \left(\tau_{\mathbf{U}}^{-1}(H_U) \cap U \right).$$

Since $\mathbf{U}$ is an SU-partition of $(\mathbf{M} \times A)^*$, the language H is in $(\mathscr{C} \circ \mathsf{SU})(\mathbf{M} \times A)$.

We now show that $L = \tau_{\mathbf{M}}^{-1}(H)$. Since $L = \mu_d^{-1}(K)$, this amounts to proving that for any $w \in A^*$, the following equivalence holds:

$$\mu_d(w) \in K \quad \text{if and only if} \quad \tau_{\mathbf{M}}(w) \in H \tag{6.1}$$

So let us fix $w \in A^*$ and let $(u,v) \in (A^*)^2$ be its d-cut. Since $\mathbf{U}$ is a partition, let U be the unique element of $\mathbf{U}$ such that $\tau_{\mathbf{M}}(w) \in U$, and let $P = [\mu_d(w)]_{\mathbf{P}}$ and $Q = [\mu_d(u)]_{\mathbf{P}}$. By Lemma 6.12, P, Q and v are entirely determined by U. By definition of K and H, proving (6.1) is equivalent to proving

$$\tau_{\mathbf{P}}(\mu_d(w)) \in K_P \quad \text{if and only if} \quad \tau_{\mathbf{U}}(\tau_{\mathbf{M}}(w)) \in H_U.$$

There are two cases depending on whether v is empty or not. We handle the case when $v \neq \varepsilon$, the other case is similar. By definition of H_U, we want to prove

$$\tau_{\mathbf{P}}(\mu_d(w)) \in K_P \quad \text{if and only if} \quad \alpha(\tau_{\mathbf{U}}(\tau_{\mathbf{M}}(w))) \in K_P \cdot (Q,v)^{-1}. \tag{6.2}$$

By Fact 6.11, we have $\tau_{\mathbf{P}}(\mu_d(w)) = \tau_{\mathbf{P}}(\mu_d(u) \cdot (v))$ and Fact 4.5 shows that

$$\tau_{\mathbf{P}}(\mu_d(w)) = \tau_{\mathbf{P}}(\mu_d(u)) \cdot ([\mu_d(u)]_{\mathbf{P}},(v)) = \tau_{\mathbf{P}}(\mu_d(u)) \cdot (Q,(v)).$$

Therefore $\tau_{\mathbf{P}}(\mu_d(w)) \in K_P$ if and only if $\tau_{\mathbf{P}}(\mu_d(u)) \in K_P \cdot (Q,(v))^{-1}$. Finally, Lemma 6.13 allows us to conclude since it shows that $\tau_{\mathbf{P}}(\mu_d(u)) = \alpha(\tau_{\mathbf{U}}(\tau_{\mathbf{M}}(w)))$. This completes the proof of Proposition 6.10.

6.4. **Proof of Lemma 6.12.** Let $w_1, w_2 \in A^*$ and $(u_1,v_1),(u_2,v_2) \in (A^*)^2$ be their d-cuts. Assume that $\tau_{\mathbf{M}}(w_1) \sim_k \tau_{\mathbf{M}}(w_2)$. We want to show that $[\mu_d(w_1)]_{\mathbf{P}} = [\mu_d(w_2)]_{\mathbf{P}}$, $[\mu_d(u_1)]_{\mathbf{P}} = [\mu_d(u_2)]_{\mathbf{P}}$ and $v_1 = v_2$. We first establish two facts.

Fact 6.14. *The lengths $|w_1|$ and $|w_2|$ are congruent modulo d.*

Proof. By definition of $\mathbf{M}$, the lengths modulo d of w_1 and w_2 are encoded in the rightmost letters of their $\tau_{\mathbf{M}}$-images, which are identical since $\tau_{\mathbf{M}}(w_1) \sim_k \tau_{\mathbf{M}}(w_2)$. $\qquad\square$

Recall that $\ell \in \mathbb{N}$ was defined so that every $P \in \mathbf{P}$ belongs to $\mathsf{SU}_\ell(A_s)$, and that $k = d(\ell + 1)$.

Fact 6.15. *We have $\mu_d(w_1) \sim_{\ell+1} \mu_d(w_2)$.*

Proof. Let $\mu_d(w_1) = (b_1) \cdots (b_m)$ and $\mu_d(w_2) = (c_1) \cdots (c_n)$. By definition, b_i and c_j are length d words in A^* for all $1 \le i < m$ and $1 \le j < n$, and b_m and c_n are non empty words of length at most d.

Let $x \in A_d^*$ be a suffix of $\mu_d(w_1)$ of length $h \le \ell + 1$. Then $x = (b_{m-h+1}) \cdots (b_m)$. Note that the word $b_{m-h+1} \cdots b_m$ in A^* has length $q \le hd \le k$, and that x is its μ_d-image. Note also that each suffix of w_1 is uniquely determined by the suffix of $\tau_\mathbf{M}(w_1)$ of the same length.

Since $\tau_\mathbf{M}(w_1) \sim_k \tau_\mathbf{M}(w_2)$, the length q suffix of $\tau_\mathbf{M}(w_1)$ is also a suffix of $\tau_\mathbf{M}(w_2)$, and hence the suffix of length q of w_1, namely $b_{m-h+1} \cdots b_m$, is also a suffix of w_2. In addition, the lengths of w_1 and w_2 are congruent modulo d by Fact 6.14, so we have $b_{m-i} = c_{n-i}$ for every $0 \le i < h$. It follows that x is also a suffix of $\mu_d(w_2)$.

This proves the announced fact by symmetry. $\qquad\qquad\qquad\qquad\qquad\qquad\square$

We now conclude the proof of Lemma 6.12. Since every $P \in \mathbf{P}$ belongs to $\mathsf{SU}_\ell(A_d)$ and since $\mu_d(w_1) \sim_{\ell+1} \mu_d(w_2)$ (Fact 6.15), we have $[\mu_d(w_1)]_\mathbf{P} = [\mu_d(w_2)]_\mathbf{P}$.

Since $|w_1|$ and $|w_2|$ are congruent modulo d (Fact 6.14), we know that $v_1 = \varepsilon$ if and only if $v_2 = \varepsilon$. If $v_1 = v_2 = \varepsilon$, then $w_1 = u_1$ and $w_2 = u_2$ and we already showed that $[\mu_d(w_1)]_\mathbf{P} = [\mu_d(w_2)]_\mathbf{P}$. If instead $v_1 \ne \varepsilon$ and $v_2 \ne \varepsilon$, then Fact 6.11 shows that $\mu_d(w_1) = \mu_d(u_1) \cdot (v_1)$ and $\mu_d(w_2) = \mu_d(u_2) \cdot (v_2)$. Using the fact that $\mu_d(w_1) \sim_{\ell+1} \mu_d(w_2)$, we find that $v_1 = v_2$ and $\mu_d(u_1) \sim_\ell \mu_d(u_2)$. It follows that $[\mu_d(u_1)]_\mathbf{P} = [\mu_d(u_2)]_\mathbf{P}$ since every $P \in \mathbf{P}$ belong to $\mathsf{SU}_\ell(A_d)$.

6.5. **Proof of Lemma 6.13.** We define a morphism $\alpha \colon (\mathbf{U} \times (\mathbf{M} \times A))^* \to (\mathbf{P} \times A_d)^*$ as follows. Let $(U, (M, a))$ be a letter in $\mathbf{U} \times (\mathbf{M} \times A)$. By definition of $\mathbf{M}$, $M = M_i$ for some $i < d$.

Suppose first that $i = d - 1$ and U contains an element of $\tau_\mathbf{M}(A^*)$. By Lemma 6.12, there exist $P \in \mathbf{P}$ and $v \in A_{d-1}$ such that, for every word $w \in A^*$ such that $\tau_\mathbf{M}(w) \in U$, the d-cut of w is of the form (u, v) with $[u]_\mathbf{P} = P$. Note also that (va) is a letter of A_d since $|v| \le d - 1$. We then let

$$\alpha((U, (M, a))) = (P, (va)).$$

Otherwise (that is: if $i \ne d - 1$ or $U \cap \tau_\mathbf{M}(A^*) = \emptyset$), we let $\alpha((U, (M, a))) = \varepsilon$. Note in particular that α is not length increasing.

Let us now verify that α satisfies the desired property: we show that if $w \in A^*$ has d-cut (u, v), then

$$\tau_\mathbf{P}(\mu_d(u)) = \alpha(\tau_\mathbf{U}(\tau_\mathbf{M}(w))).$$

We proceed by induction on the length of w. If $w = \varepsilon$, it is immediate that $\tau_\mathbf{P}(\mu_d(u)) = \alpha(\tau_\mathbf{U}(\tau_\mathbf{M}(w))) = \varepsilon$. Now assume that $|w| \ge 1$. There are two cases depending on whether $|w| = 0 \mod d$ (i.e. $w = u$ and $v = \varepsilon$) or not.

If $w \ne 0 \mod d$, then $v = v'a$ for some $v' \in A^*$ and $a \in A$. Note that $w = uv = uv'a$. Applying Fact 4.5 to $\tau_\mathbf{M}$ and again to $\tau_\mathbf{U}$, we get

$$\tau_\mathbf{M}(w) = \tau_\mathbf{M}(uv') \; ([uv']_\mathbf{M}, a)$$

$$\tau_\mathbf{U}(\tau_\mathbf{M}(w)) = \tau_\mathbf{U}(\tau_\mathbf{M}(uv')) \; ([\tau_\mathbf{M}(uv')]_\mathbf{U}, ([uv']_\mathbf{M}, a)).$$

By definition, $|u| = 0 \mod d$ and $|v| < d$, so $|v'| < d-1$ and $|uv'| \neq d-1 \mod d$ and hence $[uv']_\mathbf{M} \neq M_{d-1}$. In view of the definition of α, it follows that $\alpha(([\tau_\mathbf{M}(uv')]_\mathbf{U}, ([uv']_\mathbf{M}, a))) = \varepsilon$ and therefore

$$\alpha(\tau_\mathbf{U}(\tau_\mathbf{M}(w))) = \alpha(\tau_\mathbf{U}(\tau_\mathbf{M}(uv'))).$$

We now use the induction hypothesis on uv', whose length is $|w|-1$ and whose d-cut is (u, v'): this yields the equalities $\alpha(\tau_\mathbf{U}(\tau_\mathbf{M}(uv'))) = \tau_\mathbf{P}(\mu_d(u))$ and hence $\tau_\mathbf{P}(\mu_d(u)) = \alpha(\tau_\mathbf{U}(\tau_\mathbf{M}(w)))$ as desired.

Suppose finally that $|w| = 0 \mod d$, so $w = u$ and $v = \varepsilon$. Let $w' \in A^*$ and $a \in A$ such that $w = w'a$. In particular, $|w'| = d-1 \mod d$ and hence $[w']_\mathbf{M} = M_{d-1}$. Two successive applications of Fact 4.5 show that

$$\tau_\mathbf{M}(w) = \tau_\mathbf{M}(w') \ ([w']_\mathbf{M}, a) = \tau_\mathbf{M}(w') \ (M_{d-1}, a),$$

$$\tau_\mathbf{U}(\tau_\mathbf{M}(w)) = \tau_\mathbf{U}(\tau_\mathbf{M}(w')) \ ([\tau_\mathbf{M}(w')]_\mathbf{U}, (M_{d-1}, a)).$$

Let (u', v') be the d-cut of w'. By induction, we get $\tau_\mathbf{P}(\mu_d(u')) = \alpha(\tau_\mathbf{U}(\tau_\mathbf{M}(w')))$ and hence

$$\alpha(\tau_\mathbf{U}(\tau_\mathbf{M}(w))) = \tau_\mathbf{P}(\mu_d(u')) \cdot \alpha(([\tau_\mathbf{M}(w')]_\mathbf{U}, (M_{d-1}, a))).$$

By definition of α, we have $\alpha(([\tau_\mathbf{M}(w')]_\mathbf{U}, (M_{d-1}, a))) = ([\mu_d(u')]_\mathbf{P}, (v'a))$ and hence

$$\alpha(\tau_\mathbf{U}(\tau_\mathbf{M}(w))) = \tau_\mathbf{P}(\mu_d(u')) \cdot ([\mu_d(u')]_\mathbf{P}, (v'a))$$

$$= \tau_\mathbf{P}(\mu_d(u') \cdot (v'a)) \text{ by Fact 4.5.}$$

Finally since $w = w'a = u'v'a$ and $|u'| = 0 \mod d$, Fact 6.2 yields $\mu_d(w) = \mu_d(u') \ \mu_d(v'a)$. Moreover, since $|v'a| = d$, $\mu_d(v'a)$ is the single letter $(v'a) \in A_d$. Thus $\mu_d(w) = \mu_d(u') \ (v'a)$ and we conclude that $\alpha(\tau_\mathbf{U}(\tau_\mathbf{M}(w))) = \tau_\mathbf{P}(\mu_d(w))$. Since $u = w$, this is the desired result.

7. Transfer theorem

The main theorem of this section, Theorem 7.3 below, states that, for any class $\mathscr{C}$ closed under inverse length increasing morphisms, $[\![\mathscr{C}]\!]$-covering reduces to $\mathscr{C}$-covering. As explained at the beginning of Section 5, this is the last ingredient for the proof of Theorem 5.1.

Let us start with an outline of the steps involved in this reduction. Since an input pair $(L, \mathbf{L})$ for the $[\![\mathscr{C}]\!]$-covering problem in A^* involves only finitely many regular languages in A^*, we can compute a monoid morphism $\eta \colon A^* \to M$ which recognizes every one of them. Once this morphism is fixed, we construct (Section 7.1) a new alphabet $\mathbb{S}_\eta$ called the *alphabet of stably-formed words* and a map $L \mapsto \lfloor L \rfloor_\eta$ which associates a language $\lfloor L \rfloor_\eta$ over $\mathbb{S}_\eta$ with every language $L \subseteq A^*$ recognized by η.

Theorem 7.3 (in Section 7.2) then states that for any pair $(L, \mathbf{L})$ such that L and the languages in $\mathbf{L}$ are recognized by η, the announced reduction is given by the following equivalence:

$$(L, \mathbf{L}) \text{ is } [\![\mathscr{C}]\!]\text{-coverable} \quad \text{if and only if} \quad (\lfloor L \rfloor_\eta, \lfloor \mathbf{L} \rfloor_\eta) \text{ is } \mathscr{C}\text{-coverable}.$$

The proof of Theorem 7.3 is given in Sections 7.3 and 7.4.

7.1. **Stably-formed words.** Let $\eta\colon A^* \to M$ be a morphism into a finite monoid M. The *alphabet of stably-formed words* associated to η is the finite set $\mathbb{S}_\eta = \eta(A^+)$. To resolve ambiguity, an element $x \in \eta(A^+)$ will be written (x) if we view it as a letter in $\mathbb{S}_\eta$. We denote by EV the natural *evaluation* morphism EV$\colon (\mathbb{S}_\eta)^* \to M$, given by EV$((x)) = x$ for every letter $(x) \in \mathbb{S}_\eta$ (that is: for every $x \in \eta(A^+)$).

We will be interested in only certain words of $\mathbb{S}_\eta^*$, which we call *stably-formed*. To define this class of words, we remind the reader of the notion of *stability index* associated to the morphism η.

Fact 7.1. *If $\eta\colon A^* \to M$ is a morphism into a finite monoid M, there exists an integer $s \geq 1$ such that $\eta(A^s) = \eta(A^{2s})$.*

Proof. Every element x of a finite monoid S has a positive idempotent power, and we let n_x be the least such power. Now let $\omega(S) = \mathsf{lcm}\{n_x \mid x \in S\}$: then every $\omega(S)$-power is an idempotent of S. The powerset 2^M is a finite monoid for the following product operation: given $X_1, X_2 \in 2^M$, $X_1 \cdot X_2 = \{x_1 x_2 \mid w_1 \in X_1 \text{ and } x_2 \in X_2\}$. Letting $s = \omega(2^M)$ establishes Fact 7.1. $\square$

We call *stability index* of η the least natural number $s \geq 1$ such that $\eta(A^s) = \eta(A^{2s})$. By definition of s, $\eta(A^s)$ is a sub-semigroup of M which we call the *stable semigroup* of η. Note that the stable semigroup of η can also be viewed as a subset of the alphabet $\mathbb{S}_\eta$.

Now a word $w \in \mathbb{S}_\eta^*$ is said to be *stably-formed* if either $w = \varepsilon$, or $w = (x_1)(x_2) \cdots (x_n)$ with $n \geq 1$ and the letters $(x_1), \ldots, (x_{n-1})$ belong to the stable semigroup of η (the rightmost letter (x_n) can be any letter in $\mathbb{S}_\eta$). The following fact is immediate from the definition.

Fact 7.2. *For any morphism $\eta\colon A^* \to M$, the language of stably-formed words in $(\mathbb{S}_\eta)^*$ is regular.*

We now associate with every language $L \subseteq A^*$ recognized by η a language $\lfloor L \rfloor_\eta \subseteq (\mathbb{S}_\eta)^*$ called the *language of stably-formed words associated to L*:

$$\lfloor L \rfloor_\eta = \{w \in (\mathbb{S}_\eta)^* \mid w \text{ is stably-formed and } \text{EV}(w) \in \eta(L)\}.$$

Note that $\lfloor L \rfloor_\eta$ is the intersection of EV$^{-1}(\eta(L))$ and the set of stably-formed words, both regular languages: it follows that $\lfloor L \rfloor_\eta$ is regular as well.

Let us emphasize the fact that $\lfloor L \rfloor_\eta$ is only defined when the language L is recognized by η. We extend our definition to multisets of languages recognized by η: given such a multiset $\mathbf{L}$, we let $\lfloor \mathbf{L} \rfloor_\eta = \{\lfloor L \rfloor_\eta \mid L \in \mathbf{L}\}$, a multiset as well.

7.2. **The transfer theorem.** We now state the main theorem of this section, namely the reduction between the $[\![\mathscr{C}]\!]$-covering and the $\mathscr{C}$-covering problems.

Theorem 7.3. *Let $\mathscr{C}$ be a class closed under inverse length increasing morphisms, let $\eta\colon A^* \to M$ be a morphism into a finite monoid M and let s be the stability index of η. For every language L_1 and finite multiset of languages $\mathbf{L}_2$, all recognized by η, the following properties are equivalent:*

(1) *$(L_1, \mathbf{L}_2)$ is $[\![\mathscr{C}]\!]$-coverable;*
(2) *$(L_1, \mathbf{L}_2)$ is $[\![\mathscr{C}]\!]_s$-coverable;*
(3) *$(\lfloor L_1 \rfloor_\eta, \lfloor \mathbf{L}_2 \rfloor_\eta)$ is $\mathscr{C}$-coverable.*

Note that one may adapt this statement to handle the weaker separation problem (i.e. the special case of inputs $(L_1, \mathbf{L}_2)$ where $\mathbf{L}_2$ is a singleton by Fact 2.3).

Corollary 7.4. *Let $\mathscr{C}$ be a class closed under inverse length increasing morphisms, let $\eta\colon A^* \to M$ be a morphism into a finite monoid M and let s be the stability index of η. $s \geq 1$. For all languages L_1, L_2, both recognized by η, the following properties are equivalent:*

    (1) *L_1 is $[\![\mathscr{C}]\!]$-separable from L_2;*
    (2) *L_1 is $[\![\mathscr{C}]\!]_s$-separable from L_2;*
    (3) *$\lfloor L_1 \rfloor_\eta$ is $\mathscr{C}$-separable from $\lfloor L_2 \rfloor_\eta$.*

The remainder of this section is devoted to the proof of Theorem 7.3. $\mathscr{C}$, η and s are fixed throughout the proof, satisfying the hypotheses of the theorem. With reference to the statement of Theorem 7.3, we prove the implications $(1) \Rightarrow (3) \Rightarrow (2) \Rightarrow (1)$.

The implication $(2) \Rightarrow (1)$ is actually trivial since $[\![\mathscr{C}]\!]_s \subseteq [\![\mathscr{C}]\!]$ by definition. The implication $(1) \Rightarrow (3)$ is proved in Section 7.3, and the implication $(3) \Rightarrow (2)$ is proved in Section 7.4.

7.3. From $[\![\mathscr{C}]\!]$-covering to $\mathscr{C}$-covering.

Our argument is based on the following technical proposition.

Proposition 7.5. *Let $d \geq 1$. There exists a morphism $\alpha\colon (\mathbb{S}_\eta)^* \to A^*$ such that:*

    (i) *if $L \subseteq A^*$ is recognized by η and $w \in (\mathbb{S}_\eta)^*$ is stably-formed, then $w \in \lfloor L \rfloor_\eta$ if and only if $\alpha(w) \in L$;*
    (ii) *for every $K \in [\![\mathscr{C}]\!]_d(A)$, there exists $H_K \in \mathscr{C}(\mathbb{S}_\eta)$ such that, for any stably-formed word $w \in (\mathbb{S}_\eta)^*$, $w \in H_K$ if and only if $\alpha(w) \in K$.*

Before we establish Proposition 7.5, let us prove the implication $(1) \Rightarrow (3)$ in Theorem 7.3. Let L_1 be a language and $\mathbf{L}_2$ be a finite multiset of languages, all recognized by η, such that $(L_1, \mathbf{L}_2)$ is $[\![\mathscr{C}]\!]$-coverable. We prove that $(\lfloor L_1 \rfloor_\eta, \lfloor \mathbf{L}_2 \rfloor_\eta)$ is $\mathscr{C}$-coverable.

Let $\mathbf{K}$ be a $[\![\mathscr{C}]\!]$-cover of L_1 which is separating for $\mathbf{L}_2$. Since every $K \in \mathbf{K}$ belongs to $[\![\mathscr{C}]\!]$, Corollary 6.4 yields a natural number $d \geq 1$ such that $K \in [\![\mathscr{C}]\!]_d$ for all $K \in \mathbf{K}$. Let $\alpha\colon (\mathbb{S}_\eta)^* \to A^*$ be the morphism given by Proposition 7.5 for this value of d and let $\mathbf{H} = \{H_K \mid K \in \mathbf{K}\}$. It suffices to show that $\mathbf{H}$ is a $\mathscr{C}$-cover of $\lfloor L_1 \rfloor_\eta$ which is separating for $\lfloor \mathbf{L}_2 \rfloor_\eta$.

Let $w \in \lfloor L_1 \rfloor_\eta$. By definition, w is stably-formed and by Proposition 7.5 (i), we have $\alpha(w) \in L_1$. Since $\mathbf{K}$ is a cover of L_1, $\alpha(w) \in K$ for some $K \in \mathbf{K}$, and Proposition 7.5 (ii) now shows that $w \in H_K$. Thus $\mathbf{H}$ is a cover of L_1, and a $\mathscr{C}$-cover since every H_K is in $\mathscr{C}$ (Proposition 7.5 (ii) again).

Let us now verify that $\mathbf{H}$ is separating for $\lfloor \mathbf{L}_2 \rfloor_\eta$. Let $H \in \mathbf{H}$: by definition, there exists $K \in \mathbf{K}$ such that $H = H_K$. Since $\mathbf{K}$ is separating for $\mathbf{L}_2$, there exists $L_2 \in \mathbf{L}_2$ such that $K \cap L_2 = \emptyset$. We prove that $H \cap \lfloor L_2 \rfloor_\eta = \emptyset$ by contradiction: if $w \in H \cap \lfloor L_2 \rfloor_\eta$, then Proposition 7.5 (i) yields $\alpha(w) \in L_2$ and Proposition 7.5 (ii) yields $\alpha(w) \in K$. Thus $\alpha(w) \in K \cap L_2$, which is a contradiction. This concludes the proof of the implication $(1) \Rightarrow (3)$ in Theorem 7.3.

Proof of Proposition 7.5. Let $d \geq 1$ and let $s \geq 1$ be the stability index of η. We define a morphism $\alpha\colon (\mathbb{S}_\eta)^* \to A^*$ as follows. Let $x \in \mathbb{S}_\eta = \eta(A^+)$. If $x \notin \eta(A^s)$, we pick any non-empty word $w \in A^+$ such that $\eta(w) = x$ and we let $\alpha(x) = w$. If instead $x \in \eta(A^s)$, then we also have $x \in \eta(A^{ds})$ by definition of the stability index: we pick a word $w \in A^{ds}$ of length ds such that $\eta(w) = x$ and we let $\alpha(x) = w$.

Let L be a language recognized by η and let $w = (x_1) \cdots (x_n) \in (\mathbb{S}_\eta)^*$ be a stably-formed word. We first want to show Proposition 7.5 (1), namely that $w \in \lfloor L \rfloor_\eta$ if and

only if $\alpha(w) \in L$. We have $\alpha(w) = \alpha(x_1) \cdots \alpha(x_n)$ and, by definition of α, we have $\eta(\alpha(w)) = x_1 \cdots x_n = \text{EV}(w)$. Since L is recognized by η and hence $\alpha(w) \in L$ if and only if $\eta(\alpha(w)) \in \eta(L)$, it follows that $\alpha(w) \in L$ if and only if $\text{EV}(w) \in \eta(L)$. By definition of $\lfloor L \rfloor_\eta$, this is equivalent to $w \in \lfloor L \rfloor_\eta$, as announced.

To establish Proposition 7.5 (2), we consider the morphism $\gamma \colon (\mathbb{S}_\eta)^* \to A_d^*$ defined by letting $\gamma(x) = \mu_d(\alpha(x))$ for each letter $x \in \mathbb{S}_\eta$. Since each $\alpha(x)$ is non-empty, the morphism γ is length increasing.

Fact 7.6. *For every stably-formed word $w \in \mathbb{S}_\eta^*$, we have $\gamma(w) = \mu_d(\alpha(w))$.*

Proof. The proof is by induction on the length of w. If $w = \varepsilon$, then $\gamma(w) = \mu_d(\alpha(w)) = \varepsilon$. We now assume that $|w| \geq 1$ and we let $(x) \in \mathbb{S}_\eta$ be the leftmost letter in w: $w = (x)\, w'$ for some $w' \in (\mathbb{S}_\eta)^*$. Then we have

$$\gamma(w) = \gamma(x)\, \gamma(w')$$
$$= \mu_d(\alpha(x))\, \gamma(w') \text{ by definition of } \gamma$$
$$= \mu_d(\alpha(x))\, \mu_d(\alpha(w')) \text{ by induction.}$$

If $w' = \varepsilon$, then $w = x$ and we get $\gamma(x) = \mu_d(\alpha(x))$ as desired. If $w' \neq \varepsilon$, then (x) is not the rightmost letter of w and by definition of stably-formed words, we have $x \in \eta(A^s)$ (i.e. the stable semigroup). By definition of α, it follows that $\alpha(x) \in A^+$ has length sd and we can use Fact 6.2 to show that

$$\gamma(w) = \mu_d(\alpha(x))\, \mu_d(\alpha(w')) = \mu_d(\alpha((x)\, w')) = \mu_d(\alpha(w)),$$

as desired. $\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad$ $\square$

We want to show that, for any language $K \in [\![\mathscr{C}]\!]_d(A)$, there exists $H_K \in \mathscr{C}(\mathbb{S}_\eta)$ such that for any stably-formed word $w \in (\mathbb{S}_\eta)^*$, $w \in H_K$ if and only if $\alpha(w) \in K$.

By definition of $[\![\mathscr{C}]\!]_d(A)$, there exists $P \in \mathscr{C}(A_d)$ such that $K = \mu_d^{-1}(P)$ and we let $H_K = \gamma^{-1}(P)$. Since $\mathscr{C}$ is closed under inverse length increasing morphisms, we have $H_K \in \mathscr{C}(\mathbb{S}_\eta)$.

Now let $w \in \mathbb{S}_\eta^*$ be stably-formed. By definition of H_K, $w \in H_K$ if and only if $\gamma(w) \in P$. By Fact 7.6, this is equivalent to $\mu_d(\alpha(w)) \in P$ and hence to $\alpha(w) \in \mu_d^{-1}(P) = K$, as desired. $\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad$ $\square$

7.4. From $\mathscr{C}$-covering to $[\![\mathscr{C}]\!]$-covering.

We turn to the implication $(3) \Rightarrow (2)$ in Theorem 7.3. We first introduce auxiliary maps σ and ρ.

The morphism $\sigma \colon A_s^* \to \mathbb{S}_\eta^*$ is defined as follows: if x is a letter in A_s (i.e., $x \in A^+$ is a non-empty word of length at most s), we let $\sigma(x) = \eta(x) \in \mathbb{S}_\eta$ (recall that $\mathbb{S}_\eta = \eta(A^+)$). In particular, σ is length increasing. We now define the map $\rho \colon A^* \to (\mathbb{S}_\eta)^*$ to be the composition $\rho = \sigma \circ \mu_s$. Note that ρ is not a morphism. Useful properties of ρ are summarized in the following lemma.

Lemma 7.7. *The following properties hold.*
   (i) *If $w \in A^*$, then $\rho(w) \in \mathbb{S}_\eta^*$ is stably-formed.*
   (ii) *If $L \subseteq A^*$ is recognized by η, then $L = \rho^{-1}(\lfloor L \rfloor_\eta)$.*
   (iii) *If $K \in \mathscr{C}(\mathbb{S}_\eta)$, then $\rho^{-1}(K) \in [\![\mathscr{C}]\!]_s(A)$.*

Proof. Let $w \in A^*$. If $w = \varepsilon$, then $\rho(w) = \varepsilon$, which is stably-formed. If $w \neq \varepsilon$, then $\mu_s(w) = (x_1) \cdots (x_n)$ with $n \geq 1$ and $x_1, \ldots, x_{n-1} \in A^s$. Then $\rho(w) = \sigma(\mu_s(w)) = (\eta(x_1)) \cdots (\eta(x_n))$ and $\eta(x_1), \ldots, \eta(x_{n-1}) \in \eta(A^s)$: this is exactly the definition of a stably-formed word. Thus (i) holds.

Now let $L \subseteq A^*$ be recognized by η and let $w \in A^*$. By definition of $\lfloor L \rfloor_\eta$, L contains the empty word if and only if $\lfloor L \rfloor_\eta$ does. Now let $w \in A^+$. Then $\mu_s(w) = (x_1) \cdots (x_n)$ with $n \geq 1$ and each x_i is a non-empty word of length at most s. In particular $w = x_1 \cdots x_n$ and $\rho(w) = (\eta(x_1)) \cdots (\eta(x_n))$. Then we have $\mathrm{EV}(\rho(w)) = \eta(x_1) \cdots \eta(x_n) = \eta(w)$. By definition of $\lfloor L \rfloor_\eta$ and since $\rho(w)$ is stably-formed, we have $\rho(w) \in \lfloor L \rfloor_\eta$ if and only if $\mathrm{EV}(\rho(w)) \in \eta(L)$, if and only if $\eta(w) \in \eta(L)$. This is equivalent to $w \in L$ since η recognizes L and hence, (ii) holds.

Finally, let $K \in \mathscr{C}(\mathbb{S}_\eta)$ and let $P = \sigma^{-1}(K) \subseteq A_s^*$. In particular $P \in \mathscr{C}(A_s)$ since $\mathscr{C}$ is closed under inverse length increasing morphisms. Moreover $\rho^{-1}(K) = \mu_s^{-1}(\sigma^{-1}(K)) = \mu_s^{-1}(P)$, which belongs to $[\![\mathscr{C}]\!]_s(A)$ by definition. This concludes the proof of (iii). $\square$

We now prove the implication $(3) \Rightarrow (2)$ in Theorem 7.3. Let L_1 be a language and $\mathbf{L}_2$ be a finite multiset of languages, all recognized by η, such that $(\lfloor L_1 \rfloor_\eta, \lfloor \mathbf{L}_2 \rfloor_\eta)$ is $\mathscr{C}$-coverable. Let $\mathbf{K}$ be a $\mathscr{C}$-cover of $\lfloor L_1 \rfloor_\eta$ which is separating for $\lfloor \mathbf{L}_2 \rfloor_\eta$ and let

$$\mathbf{U} = \{\rho^{-1}(K) \mid K \in \mathbf{K}\}.$$

In order to complete the proof, we verify that $\mathbf{U}$ is a $[\![\mathscr{C}]\!]_s$-cover of L_1 which is separating for $\mathbf{L}_2$.

Lemma 7.7 (iii) shows that each element of $\mathbf{U}$ is in $[\![\mathscr{C}]\!]_s(A)$. Now let $w \in L_1$. By Lemma 7.7 (ii), $\rho(w) \in \lfloor L_1 \rfloor_\eta$ and since $\mathbf{K}$ is a cover of $\lfloor L_1 \rfloor_\eta$, $\rho(w) \in K$ for some $K \in \mathbf{K}$. Then $w \in \rho^{-1}(K)$, which is an element of $\mathbf{U}$ by definition. Thus $\mathbf{U}$ is a $[\![\mathscr{C}]\!]_s$-cover of L_1.

Now let $U \in \mathbf{U}$, say, $U = \rho^{-1}(K)$ for some $K \in \mathbf{K}$. Since $\mathbf{K}$ is separating for $\lfloor \mathbf{L}_2 \rfloor_\eta$, there exists $L_2 \in \mathbf{L}_2$ such that $K \cap \lfloor L_2 \rfloor_\eta = \emptyset$. Then $\rho^{-1}(K) \cap \rho^{-1}(\lfloor L_2 \rfloor_\eta) = \emptyset$. Now $U = \rho^{-1}(K)$ and $\rho^{-1}(\lfloor L_2 \rfloor_\eta) = L_2$ by Lemma 7.7 (ii). Therefore $U \cap L_2 = \emptyset$, which shows that $\mathbf{U}$ is separating for $\mathbf{L}_2$.

8. Conclusion

We showed that for every positive variety $\mathscr{C}$, the covering problem for $(\mathscr{C} \circ \mathsf{SU}) \circ \mathsf{MOD}$ is effectively reducible to the same problem for $\mathscr{C}$. Exploiting the connection between language theoretic enrichment and logical enrichment by local and modular predicates, we used this result to obtain that covering is decidable for the fragments $\mathsf{FO}(<, \mathbf{MOD})$, $\mathsf{FO}^2(<, +1, \mathbf{MOD})$, $\Sigma_n(<, +1, \mathbf{MOD})$ for $n = 1, 2, 3$ and $\mathscr{B}\Sigma_n(<, +1, \mathbf{MOD})$ for $n = 1, 2$.

Naturally, a downside of this result is that we are only able to hand MOD-enrichment for classes which have been built with SU-enrichment. Therefore a natural question is whether there exists a complementary theorem which states that for any positive variety $\mathscr{C}$, covering for $\mathscr{C} \circ \mathsf{MOD}$ reduces to the same problem for $\mathscr{C}$. Such a theorem would make it possible to handle logical classes equipped with the modular predicates but not the local ones, such as $\mathsf{FO}^2(<, \mathbf{MOD})$, $\Sigma_n(<, \mathbf{MOD})$ or $\mathscr{B}\Sigma_n(<, \mathbf{MOD})$. Let us point out that this would be a complementary result and not a generalization of our main theorem: the classes of the form $\mathscr{C} \circ \mathsf{SU}$, which we can handle, are positive **li**-varieties but usually not positive varieties.

Finally let us point out that a natural generalization of our results concerns languages of infinite words, for which regularity and modular predicates are well-defined. Such a

generalization, for **SU**-enrichment and the addition of local predicates, is treated in detail by Place and Zeitoun in [PZ18]. An analogous reasoning for **MOD**-enrichment and the addition of modular predicates would yield analogous results.

References

[Alm99]   Jorge Almeida. Some algorithmic problems for pseudovarieties. *Publ. Math. Debrecen*, 54(suppl.):531–552, 1999. Automata and formal languages, VIII (Salgótarján, 1996).

[BCST92] David A. Mix Barrington, Kevin Compton, Howard Straubing, and Denis Thérien. Regular languages in NC^1. *J. Comput. System Sci.*, 44(3):478–499, 1992.

[BK78]   Janusz A. Brzozowski and Robert Knast. The dot-depth hierarchy of star-free languages is infinite. *Jcss*, 16(1):37–55, 1978.

[CMM13]   Wojciech Czerwiński, Wim Martens, and Tomáš Masopust. Efficient separability of regular languages by subsequences and suffixes. In *Automata, languages, and programming. Part II*, volume 7966 of *Lecture Notes in Comput. Sci.*, pages 150–161. Springer, Heidelberg, 2013.

[CPS06]   Laura Chaubard, Jean-Eric Pin, and Howard Straubing. First order formulas with modular predicates. In *21st IEEE Symposium on Logic in Computer Science (LICS 2006), 12-15 August 2006, Seattle, WA, USA, Proceedings*, pages 211–220, 2006.

[DP13]   Luc Dartois and Charles Paperman. Two-variable first order logic with modular predicates over words. In *30th International Symposium on Theoretical Aspects of Computer Science*, volume 20 of *LIPIcs. Leibniz Int. Proc. Inform.*, pages 329–340. Schloss Dagstuhl. Leibniz-Zent. Inform., Wadern, 2013.

[DP15a]   Luc Dartois and Charles Paperman. Adding modular predicates to first-order fragments. `arXiv:1401.6576`, 2015.

[DP15b]   Luc Dartois and Charles Paperman. Alternation hierarchies of first order logic with regular predicates. In *Fundamentals of computation theory*, volume 9210 of *Lecture Notes in Comput. Sci.*, pages 160–172. Springer, Cham, 2015.

[Eil76]   Samuel Eilenberg. *Automata, Languages, and Machines*, volume B. Academic Press, Inc., Orlando, FL, USA, 1976.

[Hen88]   Karsten Henckell. Pointlike sets: the finest aperiodic cover of a finite semigroup. *J. Pure Appl. Algebra*, 55(1-2):85–126, 1988.

[HRS10]   Karsten Henckell, John Rhodes, and Benjamin Steinberg. Aperiodic pointlikes and beyond. *Internat. J. Algebra Comput.*, 20(2):287–305, 2010.

[Koz97]   Dexter C. Kozen. *Automata and computability*. Undergraduate Texts in Computer Science. Springer-Verlag, New York, 1997.

[KW15]   Manfred Kufleitner and Tobias Walter. One quantifier alternation in first-order logic with modular predicates. *RAIRO Theor. Inform. Appl.*, 49(1):1–22, 2015.

[MP71]   Robert McNaughton and Seymour A. Papert. *Counter-Free Automata*. MIT Press, 1971.

[Pin86]   Jean-Éric Pin. *Varieties of Formal Languages*. North Oxford Academic, London, 1986.

[Pin17]   Jean-Éric Pin. The dot-depth hierarchy, 45 years later. In *The Role of Theory in Computer Science. Essays Dedicated to Janusz Brzozowski*. World Scientific, 2017.

[Pla15]   Thomas Place. Separating regular languages with two quantifiers alternations. In *Proceedings of the 30th Annual ACM/IEEE Symposium on Logic in Computer Science*, LICS'15, pages 202–213. IEEE Computer Society, 2015.

[Pla18]   Thomas Place. Separating regular languages with two quantifier alternations. *Logical Methods in Computer Science*, 14(4), 2018.

[PvRZ13]   Thomas Place, Lorijn van Rooijen, and Marc Zeitoun. Separating regular languages by piecewise testable and unambiguous languages. In *Proceedings of the 38th International Symposium on Mathematical Foundations of Computer Science*, MFCS'13, pages 729–740, 2013.

[PW97]   Jean-Éric Pin and Pascal Weil. Polynomial closure and unambiguous product. *Theory of Computing Systems*, 30(4):383–422, 1997.

[PZ14a]   Thomas Place and Marc Zeitoun. Going higher in the first-order quantifier alternation hierarchy on words. In *Proceedings of the 41st International Colloquium on Automata, Languages, and Programming*, ICALP'14, pages 342–353, 2014.

[PZ14b]   Thomas Place and Marc Zeitoun. Going higher in the first-order quantifier alternation hierarchy on words. In *Automata, languages, and programming. Part II*, volume 8573 of *Lecture Notes in Comput. Sci.*, pages 342–353. Springer, Heidelberg, 2014.

[PZ15a]   Thomas Place and Marc Zeitoun. Separation and the successor relation. In *32nd International Symposium on Theoretical Aspects of Computer Science*, volume 30 of *LIPIcs. Leibniz Int. Proc. Inform.*, pages 662–675. Schloss Dagstuhl. Leibniz-Zent. Inform., Wadern, 2015.

[PZ15b]   Thomas Place and Marc Zeitoun. The tale of the quantifier alternation hierarchy of first-order logic over words. *SIGLOG news*, 2(3):4–17, 2015.

[PZ16a]   Thomas Place and Marc Zeitoun. The covering problem: a unified approach for investigating the expressive power of logics. In *41st International Symposium on Mathematical Foundations of Computer Science*, volume 58 of *LIPIcs. Leibniz Int. Proc. Inform.*, pages Art. No. 77, 15. Schloss Dagstuhl. Leibniz-Zent. Inform., Wadern, 2016.

[PZ16b]   Thomas Place and Marc Zeitoun. Separating regular languages with first-order logic. *Logical Methods in Computer Science*, 12(1), 2016.

[PZ17a]   Thomas Place and Marc Zeitoun. Adding successor: a transfer theorem for separation and covering. arXiv:1709.10052, 2017.

[PZ17b]   Thomas Place and Marc Zeitoun. Concatenation hierarchies: New bottle, old wine. In *Computer Science - Theory and Applications - 12th International Computer Science Symposium in Russia, CSR 2017, Kazan, Russia, June 8-12, 2017, Proceedings*, pages 25–37, 2017.

[PZ17c]   Thomas Place and Marc Zeitoun. Separation for dot-depth two. In *32th Annual ACM/IEEE Symposium on Logic in Computer Science*, LICS'17, 2017.

[PZ18]   Thomas Place and Marc Zeitoun. The covering problem. *Log. Methods Comput. Sci.*, 14(3):Paper No. 1, 54, 2018.

[RW95]   John Rhodes and Pascal Weil. Algebraic and topological theory of languages. *RAIRO Inform. Théor. Appl.*, 29(1):1–44, 1995.

[Sch65]   Marcel Paul Schützenberger. On finite monoids having only trivial subgroups. *Information and Control*, 8(2):190–194, 1965.

[Sim75]   Imre Simon. Piecewise testable events. In *Proceedings of the 2nd GI Conference on Automata Theory and Formal Languages*, pages 214–222, 1975.

[Ste01]   Benjamin Steinberg. A delay theorem for pointlikes. *Semigroup Forum*, 63(3):281–304, 2001.

[Str85]   Howard Straubing. Finite semigroup varieties of the form $V * D$. *Journal of Pure and Applied Algebra*, 36(1):53–94, 1985.

[Str94]   Howard Straubing. *Finite Automata, Formal Logic, and Circuit Complexity*. Birkhäuser, Boston, Basel and Berlin, 1994.

[TW98]   Denis Thérien and Thomas Wilke. Over words, two variables are as powerful as one quantifier alternation. In *STOC*, pages 234–240, 1998.

[vGS18a] Samuel van Gool and Benjamin Steinberg. Merge decompositions, two-sided Krohn-Rhodes, and aperiodic pointlikes. *Canadian Mathematical Bulletin*, pages 1–10, 2018.

[vGS18b] Samuel van Gool and Benjamin Steinberg. Pointlike sets for varieties determined by groups. arXiv:1801.04638, 2018.