Group separation strikes back

Thomas Place
LaBRI, Bordeaux University, France

Marc Zeitoun
LaBRI, Bordeaux University, France

Abstract

We consider *group languages*, which are those recognized by a *finite group*, or equivalently by a *permutation automaton* (*i.e.*, each letter induces a permutation on the set of states). We investigate the separation problem for this class: given two regular languages as input, decide whether there exists a group language containing the first, while being disjoint from the second. We prove that covering, which generalizes separation, is decidable. So far, this result could only be obtained as a corollary of an independent algebraic theorem by Ash, whose proof relies on involved algebraic notions. In contrast, our algorithm and its proof rely exclusively on standard notions from automata theory.

Additionally, we prove that covering is also decidable for two strict subclasses: languages recognized by *commutative groups*, and *modulo languages*. Both algorithms rely on the construction made for group languages, but the proof for commutative groups builds on independent ideas.

2012 ACM Subject Classification Theory of computation → Formal languages and automata theory; Theory of computation → Regular languages

Keywords and phrases Automata, Separation, Covering, Group languages

Digital Object Identifier 10.4230/LIPIcs.CVIT.2016.23

1 Introduction

Context. A prominent question in automata theory is to understand natural classes of languages defined by restricting standard definitions of the regular languages (such as regular expressions, automata, monadic second-order logic or finite monoids). Naturally, "understanding a class" is an informal goal. The standard approach is to show that the class under investigation is recursive by looking for *membership algorithms*: given a regular language as input, decide whether it belongs to the class. Rather than the procedure itself, the motivation is that formulating such an algorithm often requires a deep understanding of the class. This approach was initiated in the 60s by Schützenberger [24], who provided a membership algorithm for the class of *star-free languages* (those defined by a regular expression without Kleene star but with complement instead). This theorem started a fruitful line of research, which is now supported by a wealth of results. In fact, some of the most famous open problems in automata theory are membership questions (see [25, 13, 12] for surveys).

In the paper, we look at two problems, which both generalize membership. The first one is *separation*: given *two* regular languages L_1 and L_2 as input, decide whether there exists a third language that belongs to the investigated class, includes L_1 and is disjoint from L_2. The second one is *covering*. It generalizes separation to an arbitrary number of input languages. These problems have been getting a lot of attention recently, and one could even argue that they have replaced membership as the central question. The motivation is twofold. First, it has recently been shown [18] that separation and covering are key ingredients for solving some of the most difficult membership questions (see [17] for a survey). Yet, the main motivation is tied to our original goal: "understanding classes". In this respect, separation and covering are more rewarding than membership (albeit more difficult). Intuitively, a membership algorithm for a class $\mathcal{C}$ can only detect the languages in $\mathcal{C}$, while a covering algorithm provides information on how *arbitrary regular languages* interact with $\mathcal{C}$.

Group languages. In the paper, we look at three specific classes. The main one is the class of *group languages* GR. While natural, this class is rather unique since its only known definition is based on machines: group languages are those recognized by a finite group, or equivalently, by a *permutation automaton* (a deterministic finite automaton in which every letter induces a permutation on the set of states). On the other hand, no "descriptive" definition of GR is known (*e.g*, based on regular expressions or on logic). This makes it difficult to get an intuitive grasp about group languages, which may explain why this class remains poorly understood. We also consider two more intuitive subclasses: the first, AMT, consists of all languages recognized by *Abelian* (*i.e.*, commutative) groups. From a language theoretic point of view, these are the languages that can be defined by counting the occurrences of each letter modulo some fixed integer. The second is a subclass of AMT named MOD. A language is in MOD if membership of a word in the language only depends on its length modulo some fixed integer. Like all classes of group languages, these three classes are orthogonal and complementary to the classes for which separation and covering have been recently investigated (*i.e.*, subclasses of the star-free languages, see [17]). Indeed, only the empty and the universal languages are simultaneously star-free and group languages.

Let us point out that separation and covering are known to be decidable for group languages. This can be deduced from an algebraic theorem by Ash [1]. However, Ash's motivations were purely algebraic and independent from ours (see [6, 11, 10]). Ash does not mention separation nor even regular languages. More importantly, while there exist several proofs of Ash's theorem, they all rely on involved algebraic concepts and machinery outside of automata theory. Some proofs [1, 2] are based on the theory of *inverse semigroups* while others rely on topological arguments [14, 9, 22]. The situation is similar for the languages of Abelian groups: the decidability of separation can be deduced from results of Delgado [3] which are formulated and proved using topology. This means that these results (and their proofs) are not satisfying with respect to our primary goal: "understanding classes".

Motivations. GR and its sub-classes often serve as ingredients for building more complex classes. Let us illustrate using logic. One may associate several classes to a fixed fragment of first-order logic. Every such class corresponds to a choice of *signature* (*i.e.*, the allowed predicates). For each class of languages $\mathcal{C}$, we define a signature $\mathbb{P}_{\mathcal{C}}$ as follows: each language L in $\mathcal{C}$ gives rise to a predicate $P_L(x)$, which selects all positions x in a word w such that the prefix of w up to position x (excluded) belongs to L. For $\mathcal{C} = \mathrm{AMT}$ and $\mathcal{C} = \mathrm{MOD}$, we obtain in this way two natural signatures: the predicates of $\mathbb{P}_{\mathrm{AMT}}$ allow one to test, for each letter a of the alphabet, the number of a's before position x modulo some integer. Likewise, the predicates of $\mathbb{P}_{\mathrm{MOD}}$ make it possible to test the value of positions modulo some integer.

More generally, given an arbitrary class of group languages $\mathcal{G}$ with mild properties, it is natural to consider the signatures $\{<\} \cup \mathbb{P}_{\mathcal{G}}$ and $\{<, +1\} \cup \mathbb{P}_{\mathcal{G}}$ (where "+1" denotes the successor). It was recently shown that for many fragments of first-order logic $\mathcal{F}$, membership and sometimes even separation and covering are decidable for the classes $\mathcal{F}(<, \mathbb{P}_{\mathcal{G}})$ and $\mathcal{F}(<, +1, \mathbb{P}_{\mathcal{G}})$ as soon as *separation* is decidable for $\mathcal{G}$. Prominent examples include the whole first-order logic [19] (FO), the first levels of the well-known quantifier alternation hierarchy of FO [20, 21] (namely, the levels Σ_1, $\mathcal{B}\Sigma_1$, Σ_2 and Σ_3), and finally two variable first-order logic (FO^2) and its whole quantifier alternation hierarchy [15]. The proofs are based on language theoretic definitions of these classes: they can be built by applying operators to $\mathcal{G}$. Consequently, it is desirable to have accessible language theoretic proofs that separation is decidable for the most prominent classes of group languages: GR, AMT and MOD.

Contribution. We present new self-contained proofs that covering and separation are decidable for GR, AMT and MOD. The algorithms and their proofs rely exclusively on

basic notions of automata theory, making them accessible to computer scientists. We work with non-deterministic finite automata (NFA), and our arguments use non-determinism in a crucial way. Ironically, we use very few algebraic notions beyond the standard definition of groups. Essentially, the proof arguments are based on word combinatorics for GR and arithmetic for AMT, while MOD boils down to the other two for unary alphabets. Finally, while Ash did not formulate his theorem as a separation result, it is simple to deduce the NFA-based algorithm from his work, and vice-versa. The value of the present paper lies in the elementary proof rather than on the algorithm itself.

The algorithms themselves are simple. Let us consider GR-separation. We present a simple construction that takes an NFA $\mathcal{A}$ as input and outputs a new one $\lfloor \mathcal{A} \rfloor_\varepsilon$. Then, we show that the languages recognized by two NFAs $\mathcal{A}_1$ and $\mathcal{A}_2$ can be separated by a group language if and only if the languages recognized by $\lfloor \mathcal{A}_1 \rfloor_\varepsilon$ and $\lfloor \mathcal{A}_2 \rfloor_\varepsilon$ do **not** intersect. Since $\lfloor \mathcal{A}_1 \rfloor_\varepsilon$ and $\lfloor \mathcal{A}_2 \rfloor_\varepsilon$ can be computed in polynomial time, this shows that GR-separation is in P (this goes up to PSPACE for covering as the question boils down to deciding intersection between an arbitrary number of NFAs). The approach for AMT is similar with one key difference: we consider *Parikh images*. More precisely, we show that whether the languages recognized by two NFAs $\mathcal{A}_1$ and $\mathcal{A}_2$ can be separated by AMT boils down to some specific condition on the Parikh images of $\lfloor \mathcal{A}_1 \rfloor_\varepsilon$ and $\lfloor \mathcal{A}_2 \rfloor_\varepsilon$. Using standard results (namely that existential Presburger arithmetic is in NP [23]), this implies that AMT-separation is in co-NP. Actually, we show that both AMT-separation and AMT-covering are co-NP-complete. Finally, we show that in the much simpler case of MOD, separation is NL-complete.

	MOD	AMT	GR
Separation	NL-complete	co-NP-complete	P-complete
Covering	In co-NP	co-NP-complete	In PSPACE

Figure 1 Covering and separation for MOD, AMT and GR (inputs represented by NFAs).

Organization. In Section 2, we introduce preliminary definitions and an automata construction, which we use as a key ingredient in all algorithms. Section 3 is devoted to separation and covering for the class GR of all group languages. Section 4 is devoted to AMT. Finally, Section 5 is devoted to MOD. Due to space limitations, some results are proved in appendix.

2 Preliminaries

2.1 Words, languages, separation and covering

Languages and automata. In the paper, we fix a finite alphabet A. As usual, A^* denotes the set of all finite words over A, including the empty word ε. We let $A^+ = A^* \setminus \{\varepsilon\}$. For $u, v \in A^*$, we write uv the word obtained by concatenating u and v. A *language* (over A) is a subset of A^*. Finally, a *class of languages* $\mathcal{C}$ is a set of languages, *i.e.*, a subset of 2^{A^*}. Additionally, we say that $\mathcal{C}$ is a *Boolean algebra* when it is closed under union, intersection and complement: for every $K, L \in \mathcal{C}$, we have $K \cup L \in \mathcal{C}$, $K \cap L \in \mathcal{C}$ and $A^* \setminus K \in \mathcal{C}$.

We consider *regular languages*: those that can be equivalently defined by finite automata, finite monoids or monadic second-order logic. We work with automata. A non-deterministic finite automaton (NFA) over A is a tuple $\mathcal{A} = (Q, I, F, \delta)$ where Q is a finite set of states, $I \subseteq Q$ and $F \subseteq Q$ are sets of initial and final states, and $\delta \subseteq Q \times A \times Q$ is a set of

transitions. The language recognized by $\mathcal{A}$ is defined as follows. Given $q, r \in Q$ and $w \in A^*$, we say that there exists a *run labeled by w from q to r* (in $\mathcal{A}$) if there exist $q_0, \ldots, q_n \in Q$ and $a_1, \ldots, a_n \in A$ such that $w = a_1 \cdots a_n$, $q_0 = q$, $q_n = r$ and $(q_{i-1}, a_i, q_i) \in \delta$ for every $1 \leq i \leq n$. Moreover, we write $\delta^* \subseteq Q \times A^* \times Q$ for the set consisting of all triples $(q, w, r) \in Q \times A^* \times Q$ such that there exists a run labeled by w from q to r (note that $(q, \varepsilon, q) \in \delta^*$ for every $q \in Q$: this is the case $n = 0$). The *language recognized by $\mathcal{A}$*, denoted by $L(\mathcal{A}) \subseteq A^*$, consists of all $w \in A^*$ such that there exist $q \in I$ and $r \in F$ satisfying $(q, w, r) \in \delta^*$. A language is *regular* if and only if it is recognized by an NFA.

We also use NFAs with ε-transitions. In such an NFA $\mathcal{A} = (Q, I, F, \delta)$, a transition may also be labeled by the empty word "ε" (that is, $\delta \subseteq Q \times (A \cup \{\varepsilon\}) \times Q$). We use the standard semantics: an ε-transition can be taken without consuming an input letter. Note that unless otherwise specified, the NFAs that we consider are assumed to be *without* ε-transitions.

Separation and covering. These decision problems depend on an arbitrary fixed class $\mathcal{C}$. They are used as mathematical tools for investigating $\mathcal{C}$. They both take finitely many regular languages as input (which we represent with NFAs in the paper).

Given two languages L_1 and L_2, we say that L_1 is *$\mathcal{C}$-separable* from L_2 if there exists $K \in \mathcal{C}$ such that $L_1 \subseteq K$ and $L_2 \cap K = \emptyset$. The *$\mathcal{C}$-separation problem* takes two regular languages L_1 and L_2 as input and asks whether L_1 is $\mathcal{C}$-separable from L_2.

Covering was introduced in [16] as a generalization of separation. Given a language L, a *$\mathcal{C}$-cover of L* is a *finite* set of languages $\mathbf{K}$ such that every $K \in \mathbf{K}$ belongs to $\mathcal{C}$ and $L \subseteq \bigcup_{K \in \mathbf{K}} K$. Given a pair $(L_1, \mathbf{L}_2)$ where L_1 is a language and $\mathbf{L}_2$ a *finite set of languages*, we say that $(L_1, \mathbf{L}_2)$ is *$\mathcal{C}$-coverable* when there exists a $\mathcal{C}$-cover $\mathbf{K}$ of L_1 such that for every $K \in \mathbf{K}$, there exists $L \in \mathbf{L}_2$ satisfying $K \cap L = \emptyset$. The *$\mathcal{C}$-covering problem* takes as input a regular language L_1 and a finite set of regular languages $\mathbf{L}_2$ and asks whether $(L_1, \mathbf{L}_2)$ is $\mathcal{C}$-coverable.

Covering generalizes separation when $\mathcal{C}$ is closed under union: in this case, one may verify that L_1 is $\mathcal{C}$-separable from L_2, if and only if $(L_1, \{L_2\})$ is $\mathcal{C}$-coverable. Additionally, the definition of covering may be simplified when $\mathcal{C}$ is a *Boolean algebra*: it suffices to consider the case when the language L_1 that needs to be covered is A^*. Indeed, in that case, $(L_1, \mathbf{L}_2)$ is $\mathcal{C}$-coverable if and only if $(A^*, \{L_1\} \cup \mathbf{L}_2)$ is $\mathcal{C}$-coverable (the proof is simple, see [16]).

Since we only consider Boolean algebras, we only look at this special case. Given a finite set of languages $\mathbf{L}$, we say that $\mathbf{L}$ is $\mathcal{C}$-coverable if and only if $(A^*, \mathbf{L})$ is $\mathcal{C}$-coverable. For the classes $\mathcal{C}$ that we consider, $\mathcal{C}$-covering boils down to deciding whether an input finite set $\mathbf{L}$ of regular languages is $\mathcal{C}$-coverable. Additionally, $\mathcal{C}$-separation is the special case when $|\mathbf{L}| = 2$.

▶ Remark 1. When discussing complexity, we consider the alphabet A as part of the input.

Group languages. We first recall the algebraic definition of regular languages. A *monoid* is a set M endowed with an associative multiplication $(s, t) \mapsto s \cdot t$ (also denoted by st) having a neutral element 1_M, *i.e.*, such that $1_M s = s 1_M = s$ for every $s \in M$. Clearly, A^* is a monoid whose multiplication is concatenation (the neutral element is ε). Thus, we may consider monoid morphisms $\alpha : A^* \to M$ where M is an arbitrary monoid. Given such a morphism and some language $L \subseteq A^*$, we say that L is *recognized* by α when there exists a set $F \subseteq M$ such that $L = \alpha^{-1}(F)$. It is well-known and simple to verify that the regular languages are also those which can be recognized by a morphism into a *finite* monoid.

A *group* is a monoid G such that every element $g \in G$ has an inverse $g^{-1} \in G$, *i.e.*, $gg^{-1} = g^{-1}g = 1_G$. We write GR for the class of all *group languages*, *i.e.*, which are recognized by a morphism into a *finite group*. One can verify that GR is a Boolean algebra.

▶ Remark 2. No language theoretic definition of GR is known. There is however a definition based on automata: the group languages are those which can be recognized by a *permutation automaton* (*i.e.*, which is simultaneously deterministic, co-deterministic and complete).

We also look at two sub-classes of GR. The first one is the class MOD of *modulo languages*. For $w \in A^*$, we write $|w| \in \mathbb{N}$ for the *length* of w (its number of letters). For all $q, r \in \mathbb{N}$ such that $r < q$, we let $L_{q,r} = \{w \in A^* \mid |w| \equiv r \bmod q\}$. The class MOD consists of all *finite unions* of languages $L_{q,r}$. The following simple lemma is proved in Appendix C.

▶ **Lemma 3.** *Let $L \subseteq A^*$. Then, $L \in$ MOD if and only if L is recognized by a morphism $\alpha : A^* \to G$ into a finite group G such that $\alpha(a) = \alpha(b)$ for all $a, b \in A$.*

We turn to the class AMT of *alphabet modulo testable languages*. If $w \in A^*$ and $a \in A$, let $|w|_a \in \mathbb{N}$ be the number of copies of "a" in w. For all $q, r \in \mathbb{N}$ such that $r < q$ and all $a \in A$, let $L^a_{q,r} = \{w \in A^* \mid |w|_a \equiv r \bmod q\}$. We define AMT as the least class containing all languages $L^a_{q,r}$ and closed under union and intersection. The lemma is proved in Appendix B.

▶ **Lemma 4.** *Let $L \subseteq A^*$. Then, $L \in$ AMT if and only if L is recognized by a morphism $\alpha : A^* \to G$ into a finite commutative group G.*

One may verify that both MOD and AMT are Boolean algebras and MOD $\subseteq$ AMT $\subseteq$ GR. In the paper, we prove that covering and separation are decidable for GR, AMT and MOD. The proofs are based exclusively on elementary arguments from automata theory. We rely on a common automata-based construction, which we describe now.

2.2 Automata-based construction

First, we define an extension of A as a larger alphabet denoted by $\tilde{A}$. For each $a \in A$, we create a fresh letter a^{-1} (by "fresh", we mean that $a^{-1} \notin A$) and define $A^{-1} = \{a^{-1} \mid a \in A\}$. We let $\tilde{A}$ be the disjoint union $\tilde{A} = A \cup A^{-1}$. Observe that we have a bijection $a \mapsto a^{-1}$ from A to A^{-1}. We extend it as an involution of $\tilde{A}^*$: for every $a \in A$, we let $(a^{-1})^{-1} = a$. Then, for every $w = b_1 b_2 \cdots b_n \in \tilde{A}^*$ (with $b_1, \ldots, b_n \in \tilde{A}$), we define $w^{-1} = b_n^{-1} \cdots b_2^{-1} b_1^{-1}$ (we let $\varepsilon^{-1} = \varepsilon$). The map $w \mapsto w^{-1}$ is an involution of $\tilde{A}^*$: $(w^{-1})^{-1} = w$ for every $w \in \tilde{A}^*$.

Every morphism $\alpha : A^* \to G$ into a group G can be extended as morphism $\alpha : \tilde{A}^* \to G$. For all $a^{-1} \in A^{-1}$, we let $\alpha(a^{-1}) = (\alpha(a))^{-1}$ (the inverse of $\alpha(a)$). One may verify that the definition implies $\alpha(w^{-1}) = (\alpha(w))^{-1}$ for every $w \in \tilde{A}^*$. We shall use this fact implicitly.

▶ Remark 5. This construction is standard, and used to introduce the *free group* over A (which is a quotient of $\tilde{A}^*$). We do not need this notion. We use $\tilde{A}$ as a syntactic tool: we build auxiliary NFAs over $\tilde{A}$ from NFAs over A. We shall never consider arbitrary objects over $\tilde{A}$: all *arbitrary* NFAs that we encounter are implicitly assumed to be over A.

We now present the construction on automata. Consider an arbitrary NFA $\mathcal{A} = (Q, I, F, \delta)$ over the original alphabet A ($\delta \subseteq Q \times A \times Q$). We build a new NFA $\lfloor \mathcal{A} \rfloor$ over the extended alphabet $\tilde{A}$. We say that two states $q, r \in Q$ are *strongly connected* if there exist $u, v \in A^*$ such that $(q, u, r) \in \delta^*$ and $(r, v, q) \in \delta^*$ (*i.e.*, q and r are in the same strongly connected component of the graph representation of $\mathcal{A}$). Clearly, this is an equivalence relation. We define $\lfloor \delta \rfloor \subseteq Q \times \tilde{A} \times Q$ as the following extended set of transitions:

$$\lfloor \delta \rfloor = \delta \cup \{(r, a^{-1}, q) \mid (q, a, r) \in \delta \text{ and } q, r \text{ are strongly connected}\}.$$

We let $\lfloor \mathcal{A} \rfloor = (Q, I, F, \lfloor \delta \rfloor)$, so that $L(\lfloor \mathcal{A} \rfloor) \subseteq \tilde{A}^*$. Note that for all $q, r \in Q$ which are strongly connected and $u \in \tilde{A}^*$, we have $(q, u, r) \in \lfloor \delta \rfloor^*$ if and only if $(r, u^{-1}, q) \in \lfloor \delta \rfloor^*$. Observe that $\lfloor \mathcal{A} \rfloor$ may be computed from $\mathcal{A}$ in polynomial time: this boils down to computing the pairs of states which are strongly connected, which is a graph reachability problem. Finally, we use the following lemma to "simulate" the runs in $\lfloor \mathcal{A} \rfloor$ into the original NFA $\mathcal{A}$.

▶ **Lemma 6.** *Let $\mathcal{A} = (Q, I, F, \delta)$ be an NFA and $\alpha : A^* \to G$ be a morphism into a finite group. For every $q, r \in Q$ and $w \in \tilde{A}^*$ such that $(q, w, r) \in \lfloor\delta\rfloor^*$, there exists $w' \in A^*$ such that $(q, w', r) \in \delta^*$ and $\alpha(w) = \alpha(w')$.*

Proof. By definition of $\lfloor\delta\rfloor$, it suffices to show that every new transition $(s, a^{-1}, t) \in \lfloor\delta\rfloor$ with $a \in A$ can be "simulated" in $\mathcal{A}$ with a word $x \in A^*$ (*i.e.*, such that $(s, x, t) \in \delta^*$) such that $\alpha(x) = \alpha(a^{-1}) = (\alpha(a))^{-1}$. By definition of $\lfloor\delta\rfloor$, if $(s, a^{-1}, t) \in \lfloor\delta\rfloor$, we have $(t, a, s) \in \delta$ and s, t are strongly connected. Hence, we have $y \in A^*$ such that $(s, y, t) \in \delta^*$. Since G is a *finite* group, it is standard that there exists a number $p \geq 1$ such that $g^p = 1_G$ for all $g \in G$. Therefore, $\alpha((ay)^p) = 1_G$. Let $x = y(ay)^{p-1}$. Clearly, we have $(s, x, t) \in \delta^*$ by hypothesis on a and y. Moreover, $\alpha(ax) = \alpha((ay)^p) = 1_G$. Therefore, $\alpha(x) = (\alpha(a))^{-1}$, as desired. ◀

3 Covering and separation for group languages

We prove that separation and covering are decidable for GR. Historically, this result follows from a theorem of Ash [1]. Yet, Ash's results are purely algebraic and do not mention separation. This makes it difficult to compare them with what we do. In particular, Ash relies heavily on the theory of *inverse semigroups*. Here, we bypass this notion entirely: the algorithm and its proof rely on elementary notions from automata theory only.

3.1 Statement

The procedure is based on a theorem characterizing the finite sets of regular languages which are GR-coverable. To present it, we first extend the automata-based construction $\mathcal{A} \mapsto \lfloor\mathcal{A}\rfloor$ introduced in the previous section (this extended construction is specific to GR-covering).

Given an arbitrary NFA $\mathcal{A}$, we further modify the NFA $\lfloor\mathcal{A}\rfloor$ and construct a new NFA *with ε-transitions* $\lfloor\mathcal{A}\rfloor_\varepsilon$ (these are the only NFAs with ε-transitions that we consider). The definition is based on a language $L_\varepsilon \subseteq \tilde{A}^*$ that we define first. We introduce a standard rewriting rule that one may apply to words in $\tilde{A}^*$. If $w \in \tilde{A}^*$ contains an infix of the form aa^{-1} or $a^{-1}a$ for some $a \in A$, one may delete it. More precisely, given $w, w' \in \tilde{A}^*$, we write $w \to w'$ if there exist $x, y \in \tilde{A}^*$ and $a \in A$ such that either $w = xaa^{-1}y$ or $w = xa^{-1}ay$, and $w' = xy$. We write "$\xrightarrow{*}$" for the reflexive transitive closure of "$\to$". That is, given $w, w' \in \tilde{A}^*$, we have $w \xrightarrow{*} w'$ if $w = w'$ or there exist words $w_0, \ldots, w_n \in \tilde{A}^*$ with $n \geq 1$ such that $w = w_0 \to w_1 \to w_2 \to \cdots \to w_n = w'$. We let $L_\varepsilon = \{w \in \tilde{A}^* \mid w \xrightarrow{*} \varepsilon\}$. This is a variant of the well-known *Dyck language*. In particular, L_ε is *not* regular (it is only context-free).

Consider an NFA $\mathcal{A} = (Q, I, F, \delta)$ and the associated NFA $\lfloor\mathcal{A}\rfloor = (Q, I, F, \lfloor\delta\rfloor)$. We extend the set $\lfloor\delta\rfloor$ by adding ε-transitions. We define $\lfloor\delta\rfloor_\varepsilon \subseteq Q \times (\tilde{A} \cup \{\varepsilon\}) \cup Q$ as follows:

$$\lfloor\delta\rfloor_\varepsilon = \lfloor\delta\rfloor \cup \{(q, \varepsilon, r) \mid \text{there exists } w \in L_\varepsilon \text{ such that } (q, w, r) \in \lfloor\delta\rfloor^*\}.$$

Moreover, we let $\lfloor\mathcal{A}\rfloor_\varepsilon = (Q, I, F, \lfloor\delta\rfloor_\varepsilon)$. Note that one may compute $\lfloor\mathcal{A}\rfloor_\varepsilon$ from $\lfloor\mathcal{A}\rfloor$ (hence from $\mathcal{A}$) in polynomial time. Indeed, the construction creates a new ε-transition (q, ε, r) if and only if $\{w \in \tilde{A}^* \mid (q, w, r) \in \lfloor\delta\rfloor^*\}$ (which is regular) intersects L_ε (which is context-free). It is standard that this problem is decidable in polynomial time. We complete the definition with two simple but useful properties (see Appendix A for the proofs).

▶ **Fact 7.** *Let $\mathcal{A} = (Q, I, F, \delta)$ be an NFA. Let $q, r \in Q$ and $w \in \tilde{A}^*$ such that $(q, w, r) \in \lfloor\delta\rfloor_\varepsilon^*$. If $w \in L_\varepsilon$, then $(q, \varepsilon, r) \in \lfloor\delta\rfloor_\varepsilon$. Also, if q, r are strongly connected, then $(r, w^{-1}, q) \in \lfloor\delta\rfloor_\varepsilon^*$.*

Moreover, it is straightforward to extend Lemma 6 to this new automaton $\lfloor\mathcal{A}\rfloor_\varepsilon$.

▶ **Lemma 8.** *Let $\mathcal{A} = (Q, I, F, \delta)$ be an NFA and let $\alpha : A^* \to G$ be a morphism into a finite group. For every $q, r \in Q$ and $w \in \tilde{A}^*$ such that $(q, w, r) \in \lfloor \delta \rfloor_\varepsilon^*$, there exists $w' \in A^*$ such that $(q, w', r) \in \delta^*$ and $\alpha(w) = \alpha(w')$.*

We may now state the main theorem of this section. It characterizes the finite sets of regular languages that are GR-coverable using the construction $\mathcal{A} \mapsto \lfloor \mathcal{A} \rfloor_\varepsilon$.

▶ **Theorem 9.** *Let $k \geq 1$ and let k* NFAs *$\mathcal{A}_1, \ldots, \mathcal{A}_k$. The following conditions are equivalent:*

1. *The set $\{L(\mathcal{A}_1), \cdots, L(\mathcal{A}_k)\}$ is* GR*-coverable.*
2. *We have $\bigcap_{i \leq k} L(\lfloor \mathcal{A}_i \rfloor_\varepsilon) = \emptyset$.*

Clearly, the second condition in Theorem 9 can be decided. Indeed, for every $i \leq k$, we are able to compute $\lfloor \mathcal{A}_i \rfloor_\varepsilon$ from $\mathcal{A}_i$ in polynomial time. Moreover, it is well-known that one may decide whether an arbitrary number of NFAs intersect (in polynomial space). Hence, we obtain as desired that GR-covering is decidable and in PSPACE. Additionally, when the number k of inputs is fixed, intersection can be decided in polynomial *time*. In particular, we obtain that GR-separation (the case $k = 2$) is decidable and in P. We prove in Appendix A that the problem is actually P-complete by reducing the monotone circuit value problem.

3.2 Proof of Theorem 9

We fix a number $k \geq 1$ and for every $j \leq k$ an NFA $\mathcal{A}_j = (Q_j, I_j, F_j, \delta_j)$. The two implications in the theorem are handled independently. Let us start with 1) $\Rightarrow$ 2).

Implication 1) $\Rightarrow$ 2). Assume that $\{L(\mathcal{A}_1), \cdots, L(\mathcal{A}_k)\}$ is GR-coverable. We show that $\bigcap_{i \leq k} L(\lfloor \mathcal{A}_i \rfloor_\varepsilon) = \emptyset$. By contradiction, assume that there exists $w \in \bigcap_{i \leq k} L(\lfloor \mathcal{A}_i \rfloor_\varepsilon)$.

By hypothesis, we have a GR-cover $\mathbf{K}$ of A^* such that for every $K \in \mathbf{K}$, there exists $j \leq k$ such that $K \cap L(\mathcal{A}_j) = \emptyset$. Let $\mathbf{K} = \{K_1, \ldots, K_n\}$. By hypothesis, $K_i \in$ GR for every $i \leq n$: it is recognized by a morphism $\alpha_i : A^* \to G_i$ into a finite group. Clearly, $G = G_1 \times \cdots \times G_n$ is a finite group for the componentwise multiplication and the morphism $\alpha : A^* \to G$ defined by $\alpha(w) = (\alpha_1(w), \ldots, \alpha_n(w))$ recognizes all languages K_i. Since $w \in L(\lfloor \mathcal{A}_j \rfloor_\varepsilon)$ for every $j \leq k$, Lemma 8 yields $w_j \in A^*$ such that $w_j \in L(\mathcal{A}_j)$ and $\alpha(w_j) = \alpha(w)$. Since $\mathbf{K}$ is a cover of A^*, there exists $K \in \mathbf{K}$ such that $w_1 \in K$. Hence, since K is recognized by α and $\alpha(w_1) = \cdots = \alpha(w_k) = \alpha(w)$, it follows that $w_1, \ldots, w_k \in K$. We have shown that $K \cap L(\mathcal{A}_j) \neq \emptyset$ for every $j \leq k$ which contradicts the definition of $\mathbf{K}$.

Implication 2) $\Rightarrow$ 1). This is the technical core of the proof. We start with preliminary terminology. Let $\mathcal{A} = (Q, I, F, \delta)$ be an NFA. We say that $(q, a, r) \in \delta$ is a *frontier transition* if the states q and r are *not* strongly connected. Moreover, given $q, r \in Q$ and $w \in A^*$, we associate a number $d(q, w, r) \in \mathbb{N} \cup \{\infty\}$. If $(q, w, r) \notin \delta^*$, we let $d(q, w, r) = \infty$. Otherwise, $(q, w, r) \in \delta^*$ and $d(q, w, r)$ is the *least* number $n \in \mathbb{N}$ such there exists a run from q to r labeled by w in $\mathcal{A}$ which uses exactly n frontier transitions. Note that $d(q, w, r) = 0$ if and only if $(q, w, r) \in \delta^*$ and q, r are strongly connected. We have the following immediate fact.

▶ **Fact 10.** *Let $q, r \in Q$ and $w \in A^*$ be such that $(q, w, r) \in \delta^*$. Then, $d(q, w, r) \leq |Q|$. Moreover, if $w = uv$ with $u, v \in A^*$, we have $s \in Q$ such that $d(q, u, s) + d(s, v, r) = d(q, w, r)$.*

We turn to a key definition. Let $\mathcal{A} = (Q, I, F, \delta)$ be a NFA and $\ell \in \mathbb{N}$. An *ℓ-synchronizer* (for $\mathcal{A}$) is a morphism $\alpha : A^* \to G$ into a finite group G satisfying the two following properties:

1. for all $q, r \in Q$ and $w \in A^*$ such that $d(q, w, r) \leq \ell$ and $\alpha(w) = 1_G$, we have $(q, \varepsilon, r) \in \lfloor \delta \rfloor_\varepsilon^*$.
2. for all $q_1, \ldots, q_k, r_1, \ldots, r_k \in Q$ and $w_1, \ldots, w_k \in A^*$ such that $\sum_{i \leq k} d(q_i, w_i, r_i) \leq \ell - 1$ and $\alpha(w_1) = \cdots = \alpha(w_k)$, there exists $u \in \tilde{A}^*$ such that $(q_i, u, r_i) \in \lfloor \delta \rfloor_\varepsilon^*$ for every $i \leq k$.

▶ Remark 11. There is a subtle difference between these two properties. The first one requires that $d(q, w, r) \leq \ell$ while the second requires that $\sum_{i \leq k} d(q_i, w_i, r_i) \leq \ell - 1$. This will be important when proving Proposition 12 below. In particular, when $\ell = 0$, the second property is trivially satisfied since $\sum_{i \leq k} d(q_i, w_i, r_i)$ cannot be smaller than -1.

▶ **Proposition 12.** *Let $\mathcal{A}$ be an NFA. For every $\ell \in \mathbb{N}$, there exists an ℓ-synchronizer for $\mathcal{A}$.*

Let us first apply Proposition 12 to prove the implication 2) ⇒ 1) in Theorem 9. Assuming that $\bigcap_{j \leq k} L(\lfloor \mathcal{A}_j \rfloor_\varepsilon) = \emptyset$, we show that $\{L(\mathcal{A}_1), \cdots, L(\mathcal{A}_k)\}$ is GR-coverable. Recall that $\mathcal{A}_j = (Q_j, I_j, F_j, \delta_j)$. We may assume without loss of generality that the sets Q_j are pairwise disjoint. We define $Q = \bigcup_{j \leq k} Q_j$, $\delta = \bigcup_{j \leq k} \delta_j$ and $\mathcal{A} = (A, Q, \emptyset, \emptyset, \delta)$. Let $\ell = k|Q| + 1$. By Proposition 12, there exists an ℓ-synchronizer $\alpha : A^* \to G$ for $\mathcal{A}$. Consider the GR-cover $\{\alpha^{-1}(g) \mid g \in G\}$ of A^*. We show that for every $g \in G$, there exists $j \leq k$ such that $\alpha^{-1}(g) \cap L(\mathcal{A}_j) = \emptyset$, which means that $\{L(\mathcal{A}_1), \cdots, L(\mathcal{A}_k)\}$ is GR-coverable, as desired.

Let $g \in G$ and by contradiction, assume that $\alpha^{-1}(g) \cap L(\mathcal{A}_j) \neq \emptyset$ for every $j \leq k$. This yields $w_j \in L(\mathcal{A}_j)$ for each $j \leq k$ such that $\alpha(w_j) = g$. Since $w_j \in L(\mathcal{A}_j)$, there are two states $q_j \in I_j$ and $r_j \in F_j$ such that $(q_j, w_j, r_j) \in \delta^*$. By Fact 10, this implies $d(q_j, w_j, r_j) \leq |Q|$. We get $\sum_{j \leq k} d(q_j, w_j, r_j) \leq k|Q| = \ell - 1$. Thus, since $\alpha(w_1) = \cdots = \alpha(w_k) = g$ and α is an ℓ-synchronizer, the second property yields $u \in \tilde{A}^*$ such that $(q_j, u, r_j) \in \lfloor \delta \rfloor_\varepsilon^*$ for every $j \leq k$. Since $q_j \in I_j$ and $r_j \in F_j$, it follows that $u \in L(\lfloor \mathcal{A}_j \rfloor_\varepsilon)$ for every $j \leq k$. This contradicts the hypothesis that $\bigcap_{j \leq k} L(\lfloor \mathcal{A}_j \rfloor_\varepsilon) = \emptyset$, concluding the main argument.

We turn to the proof of Proposition 12, which we develop in the remainder of the section. We fix an NFA $\mathcal{A} = (Q, I, F, \delta)$. Using induction on $\ell \in \mathbb{N}$, we build an ℓ-synchronizer for $\mathcal{A}$.

Base case: $\ell = 0$. The definition of our 0-synchronizer is based on an equivalence. Let $q, r \in Q$. We write $q \simeq r$ when q and r are strongly connected and $(q, \varepsilon, r) \in \lfloor \delta \rfloor_\varepsilon^*$.

▶ **Lemma 13.** *The relation $\simeq$ is an equivalence. Moreover, let $q, r, q', r' \in Q$ with q, q' and r, r' strongly connected. If $(q, a, q') \in \delta$ and $(r, a, r') \in \delta$ for $a \in A$, then $q \simeq r \Leftrightarrow q' \simeq r'$.*

Proof. Clearly, $\simeq$ is reflexive: $(q, \varepsilon, q) \in \lfloor \delta \rfloor_\varepsilon^*$ for every $q \in Q$. Moreover, if $q \simeq r$, then q and r are strongly connected and $(q, \varepsilon, r) \in \lfloor \delta \rfloor_\varepsilon^*$. Since $\varepsilon = \varepsilon^{-1}$, Fact 7 yields $(r, \varepsilon, q) \in \lfloor \delta \rfloor_\varepsilon^*$ and we get $r \simeq q$, meaning that $\simeq$ is symmetric. Finally, let $q, r, s \in Q$ such that $q \simeq r$ and $r \simeq s$. By definition, q, r, s are strongly connected, $(q, \varepsilon, r) \in \lfloor \delta \rfloor_\varepsilon^*$ and $(r, \varepsilon, s) \in \lfloor \delta \rfloor_\varepsilon^*$. Clearly, $(q, \varepsilon, s) \in \lfloor \delta \rfloor_\varepsilon^*$ which yields $q \simeq s$ and we conclude that $\simeq$ is transitive.

Let now $q, r, q', r' \in Q$ and $a \in A$ be as in the statement. We prove that $q \simeq r \Leftrightarrow q' \simeq r'$. By definition, $(q', a^{-1}, q) \in \lfloor \delta \rfloor$ and $(r', a^{-1}, r) \in \lfloor \delta \rfloor$. If $q \simeq r$, then q', r' are strongly connected, and $(q, \varepsilon, r) \in \lfloor \delta \rfloor_\varepsilon^*$, so that $(q', a^{-1}a, r') \in \lfloor \delta \rfloor_\varepsilon^*$. Since $a^{-1}a \xrightarrow{*} \varepsilon$, Fact 7 yields $(q', \varepsilon, r') \in \lfloor \delta \rfloor_\varepsilon^*$: we get $q' \simeq r'$. Conversely, if $q' \simeq r'$, we have $(q', \varepsilon, r') \in \lfloor \delta \rfloor_\varepsilon^*$. Hence, $(q, aa^{-1}, r) \in \lfloor \delta \rfloor_\varepsilon^*$ and since $aa^{-1} \xrightarrow{*} \varepsilon$, Fact 7 yields $(q, \varepsilon, r) \in \lfloor \delta \rfloor_\varepsilon^*$: we obtain $q \simeq r$. ◀

For every $q \in Q$, we write $[q]_\simeq \in Q/\simeq$ for the $\simeq$-class of q. Moreover, we let G be the group of permutations of $Q/\simeq$. That is, G consists of all bijections $g : Q/\simeq \to Q/\simeq$ and the multiplication is composition (the neutral element is identity). We have the following fact.

▶ **Fact 14.** *For every $a \in A$, there exists an element $g_a \in G$ such that for every $q, q' \in Q$ which are strongly connected and such that $(q, a, q') \in \delta$, we have $g_a([q]_\simeq) = [q']_\simeq$.*

Proof. Consider $q \in Q$. By Lemma 13, if there exists $q' \in Q$ such that q, q' are strongly connected and $(q, a, q') \in \delta$, we know that for every $r, r' \in Q$ which are strongly connected and such that $(r, a, r') \in \delta$, we have $q \simeq r \Leftrightarrow q' \simeq r'$. Hence, we may define $g_a([q]_\simeq) = [q']_\simeq$. This yields a *partial* function $g_a : Q/\simeq \to Q/\simeq$ which satisfies the condition described in the fact and is injective. Hence, we may complete g_a into a bijection, concluding the proof. ◀

We define $\alpha : A^* \to G$ as the morphism defined by $\alpha(a) = g_a$ for every $a \in A$ and show that α is a 0-synchronizer. We prove the first property in the definition (the second one is trivially satisfied when $\ell = 0$). Let $q, r \in Q$ and $w \in A^*$, such that $d(q, w, r) = 0$ and $\alpha(w) = 1_G$. By definition, $\alpha(w)$ is a permutation of $Q/\simeq$. Moreover, since $d(q, w, r) = 0$, we have $(q, w, r) \in \delta^*$ and q, r are strongly connected. By definition of α from Fact 14 this implies that $\alpha(w)([q]_\simeq) = [r]_\simeq$. Finally, since $\alpha(w) = 1_G$, we also have $\alpha(w)([q]_\simeq) = [q]_\simeq$. Hence, $q \simeq r$ and the definition yields $(q, \varepsilon, r) \in \lfloor \delta \rfloor_\varepsilon^*$. We conclude that α is a 0-synchronizer.

Inductive step: $\ell \geq 1$. Induction on ℓ yields a $(\ell - 1)$-synchronizer $\beta : A^* \to H$. We define a new morphism $\alpha : A^* \to G$ from β and then prove that it is the desired ℓ-synchronizer.

For every pair $(h, a) \in H \times A$ and every $w \in A^*$, we define $\#_{h,a}(w) \in \mathbb{N}$ as the number of pairs $(x, y) \in A^* \times A^*$ such that $\beta(x) = h$ and $w = xay$. We choose α so that for every $w \in A^*$, the image $\alpha(w) \in G$ determines $\beta(w) \in H$ and, for every $(h, a) \in H \times A$, whether the number $\#_{h,a}(w) \in \mathbb{N}$ is even or odd. The definition is inspired from the work of Auinger [2]. Let $G = H \times \{0, 1\}^{H \times A}$. Every $g \in G$ is a pair $g = (h, f)$ where $h \in H$ and $f : H \times A \to \{0, 1\}$ is a function. We define a multiplication on G. If $g_1 = (h_1, f_1) \in G$ and $g_2 = (h_2, f_2) \in G$, we define $g_1 g_2 = (h_1 h_2, f)$ where $f : H \times A \to \{0, 1\}$ is the function $f : (h, a) \mapsto (f_1(h, a) + f_2(h_1^{-1} h, a)) \mod 2$. One may verify that G is indeed a group for this multiplication. For every $w \in A^*$, let $f_w : H \times A \to \{0, 1\}$ be the function defined by $f_w(h, a) = \#_{h,a}(w) \mod 2$. One may now verify that the map $\alpha : A^* \to G$ defined by $\alpha(w) = (\beta(w), f_w)$ is a monoid morphism. We show that it is an ℓ-synchronizer.

Let us first explain how to exploit the definition of α. A key point is that we are mainly interested in special pairs $(h, a) \in H \times A$. Given a subset $F \subseteq H$, we say that such a pair (h, a) is *F-alternating* when $h \in F \Leftrightarrow h\beta(a) \notin F$. Moreover, we say that a word $w \in A^*$ is *F-safe* if $\#_{h,a}(w)$ is *even* for every F-alternating pair $(h, a) \in H \times A$. By definition, the image $\alpha(w) \in G$ determines whether w is F-safe or not. In the latter case, we get an F-alternating pair (h, a) such that $\#_{h,a}(w)$ is *odd* (and thus, $\#_{h,a}(w) \geq 1$). In the former case, we shall use the following lemma.

▶ **Lemma 15.** *Let $F \subseteq H$ such that $1_H \in F$. For every $w \in A^*$ which is F-safe, $\beta(w) \in F$.*

Proof. For $w \in A^*$, let $\#_F(w) \in \mathbb{N}$ be the sum of all numbers $\#_{h,a}(w)$ where $(h, a) \in H \times A$ is F-alternating. We prove that for every $w \in A^*$, we have $\beta(w) \in F \Leftrightarrow \#_F(w)$ *is even*. This clearly implies the lemma: if w is F-safe, then $\#_F(w)$ is even which implies that $\beta(w) \in F$.

We use induction on the length of $w \in A^*$. When $w = \varepsilon$, $\beta(w) = 1_H \in F$ and $\#_F(w) = 0$. Hence, the property is trivially satisfied. Assume now that $w \in A^+$. This yields $v \in A^*$ and $a \in A$ such that $w = va$. Clearly, we have $|v| < |w|$ and we get $\beta(v) \in F \Leftrightarrow \#_F(v)$ *is even* by induction. Note that this implies $\beta(v) \notin F \Leftrightarrow \#_F(v)$ *is odd*. There are two cases. First, assume that $(\beta(v), a)$ is F-alternating. Since $w = va$, it follows that $\beta(w) \in F \Leftrightarrow \beta(v) \notin F$ and $\#_F(w) = \#_F(v) + 1$ (*i.e.*, $\#_F(w)$ *is even* $\Leftrightarrow \#_F(v)$ *is odd*). Combining the equivalences, we get $\beta(w) \in F \Leftrightarrow \#_F(w)$ *is even*, as desired. Assume now that $(\beta(v), a)$ is *not* F-alternating. Since $w = va$, it follows that $\beta(w) \in F \Leftrightarrow \beta(v) \in F$ and $\#_F(w) = \#_F(v)$ (*i.e.*, $\#_F(w)$ *is even* $\Leftrightarrow \#_F(v)$ *is even*). Again, we may combine the equivalences to get $\beta(w) \in F \Leftrightarrow \#_F(w)$ *is even*, as desired. This concludes the proof. ◀

It remains to prove that α is an ℓ-synchronizer. There are two conditions to verify. We first present preliminary results that will be useful in both arguments. In particular, we describe the sets $F \subseteq H$ for which we shall consider F-alternating pairs.

Preliminary results. For every $q \in Q$, we define a set $L(q) \subseteq \tilde{A}^*$. Given $v \in \tilde{A}^*$, we let $v \in L(q)$ if and only if there exists $q' \in Q$ such that q, q' are strongly connected and $(q, v, q') \in \lfloor \delta \rfloor_\varepsilon^*$. The next key lemma follows from the fact that β is an $(\ell - 1)$-synchronizer.

▶ **Lemma 16.** *Let $s, t \in Q$ and $w \in A^*$ such that $d(s, w, t) \leq \ell - 1$. The following holds:*

1. *for every $v \in L(s)$ such that $\beta(w) = \beta(v)$, we have $(s, v, t) \in \lfloor \delta \rfloor_\varepsilon^*$.*
2. *for every $v \in L(t)$ such that $\beta(w) = (\beta(v))^{-1}$, we have $(s, v^{-1}, t) \in \lfloor \delta \rfloor_\varepsilon^*$.*

Proof. Since both assertions can be proved similarly, we only prove the first (a proof of the second one is available in Appendix A). Consider $v \in L(s)$ such that $\beta(w) = \beta(v)$. By definition, we have $s' \in Q$ such that s, s' are strongly connected and $(s, v, s') \in \lfloor \delta \rfloor_\varepsilon^*$. By Fact 7, we have $(s', v^{-1}, s) \in \lfloor \delta \rfloor_\varepsilon^*$. Lemma 8 yields $x \in A^*$ such that $(s', x, s) \in \delta^*$ and $\beta(x) = \beta(v^{-1})$. Since $d(s, w, t) \leq \ell - 1$ and s', s are strongly connected, it follows that $d(s', xw, t) \leq \ell - 1$. Moreover, since $\beta(w) = \beta(v)$ and $\beta(x) = \beta(v^{-1})$, we have $\beta(xw) = 1_H$. Altogether, since β is an $(\ell - 1)$-synchronizer, we get $(s', \varepsilon, t) \in \lfloor \delta \rfloor_\varepsilon^*$. Since $(s, v, s') \in \lfloor \delta \rfloor_\varepsilon^*$, it follows that $(s, v, t) \in \lfloor \delta \rfloor_\varepsilon^*$ as desired. ◀

Let $q \in Q$ and $(h, a) \in H \times A$. We say that (h, a) *stabilizes* q if there exist $w \in A^*$ and $s \in Q$ such that $d(q, w, s) = 0$ and $\#_{h,a}(w) \geq 1$. The next lemma follows from Lemma 16.

▶ **Lemma 17.** *Let $q \in Q$ and $(h, a) \in H \times A$ which stabilizes q. The following holds:*

- *for every $v \in L(q)$ such that $\beta(v) = h$, we have $va \in L(q)$.*
- *for every $v \in L(q)$ such that $\beta(v) = h\beta(a)$, we have $va^{-1} \in L(q)$.*

Proof. By hypothesis, we have $w \in A^*$ and $s \in Q$ such that $d(q, w, s) = 0$ and $\#_{h,a}(w) \geq 1$. The latter yields $x, y \in A^*$ such that $w = xay$ and $\beta(x) = h$. Hence, since $d(q, w, s) = 0$, Fact 10 yields $q', q'' \in Q$ such that $d(q, x, q') = d(q', a, q'') = d(q'', y, s) = 0 \leq \ell - 1$.

Let $v \in L(q)$ such that $\beta(v) = h = \beta(x)$. Since $d(q, x, q') = 0$, Lemma 16 yields $(q, v, q') \in \lfloor \delta \rfloor_\varepsilon^*$. Since $(q', a, q'') \in \delta$, we get $(q, va, q'') \in \lfloor \delta \rfloor_\varepsilon^*$. This yields $va \in L(q)$ since q, q'' are strongly connected. We now consider $v \in L(q)$ such that $\beta(v) = h\beta(a) = \beta(xa)$. Since $d(q, xa, q'') = 0$, Lemma 16 yields $(q, v, q'') \in \lfloor \delta \rfloor_\varepsilon^*$. Moreover, since $(q', a, q'') \in \delta$ and q', q'' are strongly connected, we have $(q'', a^{-1}, q') \in \lfloor \delta \rfloor$ by definition. Therefore, we have $(q, va^{-1}, q') \in \lfloor \delta \rfloor_\varepsilon^*$. Since q, q' are strongly connected , this yields $va^{-1} \in L(q)$ as desired. ◀

We may now present the sets $F \subseteq H$ to which we shall apply Lemma 15. For every $S \subseteq Q$, we associate a set $F_S \subseteq H$. We define,

$$F_S = \Big\{ \beta(v) \mid v \in \bigcap_{q \in S} L(q) \Big\}.$$

A simple yet crucial observation is that for every $S \subseteq Q$, we have $1_H \in F_S$. Indeed, $\varepsilon \in L(q)$ for every $q \in Q$ since $(q, \varepsilon, q) \in \lfloor \delta \rfloor_\varepsilon^*$. This property means that we can apply Lemma 15 for the sets F_S. Finally, we have the following corollary of Lemma 17.

▶ **Corollary 18.** *Let $S \subseteq Q$ and $(h, a) \in H \times A$ which is F_S-alternating. There exists $q \in S$ such that (h, a) does **not** stabilize q.*

Proof. We proceed by contradiction. Assume that (h, a) stabilizes q for every $q \in S$. We show that $h \in F_S \Leftrightarrow h\beta(a) \in F_S$, contradicting the hypothesis that (h, a) is F_S-alternating. Assume first that $h \in F_S$. By definition, this yields $v \in \bigcap_{q \in S} L(q)$ such that $\beta(v) = h$. Since (h, a) stabilizes q for every $q \in S$, the first assertion in Lemma 17 yields $va \in \bigcap_{q \in S} L(q)$. Thus, $h\beta(a) \in F_S$. Conversely assume that $h\beta(a) \in F_S$. By definition, this yields $v' \in \tilde{A}^*$ such that $v' \in L(q)$ and $\beta(v') = h\beta(a)$. Since (h, a) stabilizes q for every $q \in S$, the second assertion in Lemma 17 yields $v'a^{-1} \in \bigcap_{q \in S} L(q)$. Thus, $h \in F_S$ which concludes the proof. ◀

First condition. Let $q, r \in Q$ and $w \in A^*$ with $d(q, w, r) \leq \ell$ and $\alpha(w) = 1_G$. We show that $(q, \varepsilon, r) \in \lfloor \delta \rfloor^*_\varepsilon$. By definition of α, have $\beta(w) = 1_H$. Hence, since β is a $(\ell - 1)$-synchronizer, the result is immediate when $d(q, w, r) \leq \ell - 1$. Thus, we assume that $d(q, w, r) = \ell$.

Since $\ell \geq 1$, w must be nonempty. Let $a_1, \ldots, a_n \in A$ such that $w = a_1 \cdots a_n$. By Fact 10, we have $q_0, \ldots, q_n \in Q$ such that $q_0 = q$, $q_n = r$ and $\sum_{1 \leq k \leq n} d(q_{k-1}, a_k, q_k) = d(q, w, r) = \ell$. Hence, there are exactly ℓ indices $k < n$ such that $(q_{k-1}, a_k, q_k) \in \delta$ is a frontier transition. For every $0 \leq k \leq n$, we let $x_k = a_1 \cdots a_k$ and $y_k = a_{k+1} \cdots a_n$ (we let $x_0 = y_n = \varepsilon$). Clearly, $w = x_k y_k$. We let $h_k = \beta(x_k)$ for every $k \leq n$. Since $\beta(w) = 1_H$, we also have $\beta(y_k) = h_k^{-1}$.

We let $i \leq n$ be the least index such that (q_{i-1}, a_i, q_i) is a frontier transition. Symmetrically, we let $j \leq n$ be the greatest index such that (q_{j-1}, a_j, q_j) is a frontier transition. Clearly, $1 \leq i \leq j \leq n$ (we have $i = j$ when $\ell = 1$). By definition, we have the following fact.

▶ **Fact 19.** *Let $k \leq n$. If $i \leq k$, then $d(q_k, y_k, r) \leq \ell - 1$. If $k < j$, then $d(q, x_k, q_k) \leq \ell - 1$.*

We use the hypothesis that $\alpha(w) = 1_G$ and a case analysis to prove the following lemma.

▶ **Lemma 20.** *One of the three following properties holds:*

1. *there exists k such that $i \leq k < j$ and $h_k \in F_{\{q,r\}}$, or,*
2. *$h_{i-1} \in F_{\{q,r\}}$ and (h_{i-1}, a_i) stabilizes r, or,*
3. *$h_j \in F_{\{q,r\}}$ and (h_{j-1}, a_j) stabilizes q.*

Proof. We start with a preliminary definition. Since $w = x_j y_j$ and $\alpha(w) = 1_G$, we know that $\alpha(x_j) = \alpha(y_j^{-1})$. Moreover, $(q_j, y_j, r) \in \delta^*$ which yields $(r, y_j^{-1}, q_j) \in \lfloor \delta \rfloor^*$ since q_j, r are strongly connected by definition of j. Thus, Lemma 6 yields $z \in A^*$ such that $\alpha(z) = \alpha(y_j^{-1}) = \alpha(x_j)$ and $(r, z, q_j) \in \delta^*$. For every $(h, a) \in H \times A$, we have the following two properties:

- By definition of i, $d(q, x_{i-1}, q_{i-1}) = 0$. Thus, if $\#_{h,a}(x_{i-1}) \geq 1$, then (h, a) stabilizes q.
- By definition of j, $d(r, z, q_j) = 0$. Thus, if $\#_{h,a}(z) \geq 1$, then (h, a) stabilizes r.

We shall use these two properties and their contrapositives repeatedly in the proof. We consider two cases depending on whether x_i is $F_{\{q,r\}}$-safe.

First case: x_i is $F_{\{q,r\}}$-safe. Lemma 15, yields $h_i = \beta(x_i) \in F_{\{q,r\}}$. Thus, if $i < j$, Assertion 1 in the lemma holds for $k = i$. We now assume that $i = j$. Let $(h, a) = (h_{i-1}, a_i) = (h_{j-1}, a_j)$. The argument differs depending on whether $\#_{h,a}(x_{i-1}) \geq 1$ or not. If $\#_{h,a}(x_{i-1}) \geq 1$, then $(h, a) = (h_{j-1}, a_j)$ stabilizes q. Hence, Assertion 3 in the lemma holds since $h_j = h_i \in F_{\{q,r\}}$. Otherwise, $\#_{h,a}(x_{i-1}) = 0$. Since $x_i = x_{i-1}a_i$ and $(h, a) = (h_{i-1}, a_i)$, it follows that $\#_{h,a}(x_i) = 1$. In particular, $\#_{h,a}(x_i)$ is odd and since x_i is $F_{\{q,r\}}$-safe, it follows that (h, a) is **not** $F_{\{q,r\}}$-alternating. Hence, since $h\beta(a) = h_i \in F_{\{q,r\}}$, we also have $h_{i-1} = h \in F_{\{q,r\}}$. Finally, since $x_i = x_j$, we have $\alpha(x_i) = \alpha(x_j) = \alpha(z)$. Thus, since $\#_{h,a}(x_i) = 1$, we know that $\#_{h,a}(z)$ is odd by definition of α. In particular, $\#_{h,a}(z) \geq 1$ which implies that $(h_{i-1}, a_i) = (h, a)$ stabilizes r. Since $h_{i-1} \in F_{\{q,r\}}$, we conclude that Assertion 2 holds.

Second case: x_i is not $F_{\{q,r\}}$-safe. The argument differs depending on whether x_{i-1} is $F_{\{q,r\}}$-safe or not. Assume first that x_{i-1} is $F_{\{q,r\}}$-safe. By Lemma 15, we have $h_{i-1} = \beta(x_{i-1}) \in F_{\{q,r\}}$. Thus, if there exists k such that $i \leq k < j$ and $h_k = h_{i-1}$, Assertion 1 in the lemma holds. Otherwise, we have $\#_{h_{i-1},a_i}(x_i) = \#_{h_{i-1},a_i}(x_j)$. By hypothesis, $x_i = x_{i-1}a_i$ is not $F_{\{q,r\}}$-safe while x_{i-1} is $F_{\{q,r\}}$-safe. Thus, (h_{i-1}, a_i) is $F_{\{q,r\}}$-alternating and $\#_{h_{i-1},a_i}(x_i) = \#_{h_{i-1},a_i}(x_j)$ is odd. Since $\alpha(z) = \alpha(x_j)$, it follows that $\#_{h_{i-1},a_i}(z)$ is odd as well by definition of α. Thus, $\#_{h_{i-1},a_i}(z) \geq 1$ which implies that (h_{i-1}, a_i) stabilizes r. Since $h_{i-1} \in F_{\{q,r\}}$, Assertion 2 in the lemma holds.

Finally, assume that x_{i-1} is not $F_{\{q,r\}}$-safe: we have (h, a) which is $F_{\{q,r\}}$-alternating and such that $\#_{h,a}(x_{i-1})$ is odd. Observe that since $x_i = x_{i-1}a_i$ is not $F_{\{q,r\}}$-safe as well,

we may choose (h, a) so that $(h, a) \neq (h_{i-1}, a_i)$. Thus, $\#_{h,a}(x_i)$ is odd as well. Since $\#_{h,a}(x_{i-1}) \geq 1$, we know that (h, a) stabilizes q. By Corollary 18 it follows that (h, a) does *not* stabilize r. This implies $\#_{h,a}(z) = 0$ and since $\alpha(z) = \alpha(x_j)$, it follows that $\#_{h,a}(x_j)$ is even. Since $\#_{h,a}(x_i)$ is odd, this yields k such that $i \leq k < j$ and $(h_k, a_{k+1}) = (h, a)$. Since (h, a) is $F_{\{q,r\}}$-alternating either $h_k \in F_{\{q,r\}}$ or $h_{k+1} = h_k\beta(a_{k+1}) \in F_{\{q,r\}}$. If $h_k \in F_{\{q,r\}}$, Assertion 1 in the lemma holds. If $h_{k+1} \in F_{\{q,r\}}$, then either $i \leq k < j-1$ and Assertion 1 in the lemma holds, or $k = j-1$ which means that $h_j = h_{k+1} \in F_{\{q,r\}}$ and $(h_{j-1}, a_j) = (h, a)$ which stabilizes q: Assertion 2 in the lemma holds. ◀

By Lemma 20, there are three cases. First assume that we have k such that $i \leq k < j$ and $h_k \in F_{\{q,r\}}$. The definition of $F_{\{q,r\}}$ yields $v \in L(q) \cap L(r)$ such that $\beta(v) = h_k$. Fact 19 yields $d(q, x_k, q_k) \leq \ell - 1$. Thus, since $v \in L(q)$ and $\beta(x_k) = h_k = \beta(v)$, Lemma 16 yields $(q, v, q_k) \in \lfloor\delta\rfloor_\varepsilon^*$. Symmetrically, Fact 19 yields $d(q_k, y_k, r) \leq \ell - 1$. Thus, since $v \in L(r)$ and $\beta(y_k) = h_k^{-1} = (\beta(v))^{-1}$ Lemma 16 yields $(q_k, v^{-1}, r) \in \lfloor\delta\rfloor_\varepsilon^*$. Altogether, we obtain $(q, vv^{-1}, r) \in \lfloor\delta\rfloor_\varepsilon^*$. Since $vv^{-1} \xrightarrow{*} \varepsilon$, we get $(q, \varepsilon, r) \in \lfloor\delta\rfloor_\varepsilon$ by Fact 7, concluding this case.

In the second case, $h_{i-1} \in F_{\{q,r\}}$ and (h_{i-1}, a_i) stabilizes r. By definition of $F_{\{q,r\}}$, there exists $v \in L(q) \cap L(r)$ such that $\beta(v) = h_{i-1}$. We have $d(q, x_{i-1}, q_{i-1}) = 0$ by definition of i. Thus, since $v \in L(q)$ and $\beta(x_{i-1}) = \beta(v)$, Lemma 16 yields $(q, v, q_{i-1}) \in \lfloor\delta\rfloor_\varepsilon^*$. Moreover, since (h_{i-1}, a_i) stabilizes r, $v \in L(r)$ and $\beta(v) = h_{i-1}$, Lemma 17 implies that $va_i \in L(r)$. Fact 19 yields $d(q_i, y_i, r) \leq \ell - 1$. Thus, since $va_i \in F(r)$ and $\beta(y_i) = h_i^{-1} = (\beta(va_i))^{-1}$, Lemma 16 yields $(q_i, (va_i)^{-1}, r) \in \lfloor\delta\rfloor_\varepsilon^*$. Hence, since $(q_{i-1}, a_i, q_i) \in \delta$, we get $(q, va_i(va_i)^{-1}, r) \in \lfloor\delta\rfloor_\varepsilon^*$. Since $va_i(va_i)^{-1} \xrightarrow{*} \varepsilon$, it follows that $(q, \varepsilon, r) \in \lfloor\delta\rfloor_\varepsilon$ by Fact 7, concluding this case.

In the last case, $h_j \in F_{\{q,r\}}$ and (h_{j-1}, a_j) stabilizes q. By definition of $F_{\{q,r\}}$, there exists $v \in L(q) \cap L(r)$ such that $\beta(v) = h_j$. We have $d(q_j, y_j, r) = 0$ by definition of j. Consequently, since $v \in F(r)$ and $\beta(y_j) = h_j^{-1} = (\beta(v))^{-1}$, Lemma 16 yields $(q_j, v^{-1}, r) \in \lfloor\delta\rfloor_\varepsilon^*$. Moreover, we know that (h_{j-1}, a_j) stabilizes q, $v \in L(q)$ and $\beta(v) = h_j = h_{j-1}\beta(a_j)$. Thus, Lemma 17 yields $va_j^{-1} \in L(q)$. We have $d(q, x_{j-1}, q_{j-1}) \leq \ell - 1$ by Fact 19. Thus, since $va_j^{-1} \in L(q)$ and $\beta(x_{j-1}) = h_{j-1} = \beta(va_j^{-1})$, Lemma 16 yields $(q, va_j^{-1}, q_{j-1}) \in \lfloor\delta\rfloor_\varepsilon^*$. Since $(q_{j-1}, a_j, q_j) \in \delta$, we obtain $(q, va_j^{-1}a_jv^{-1}, r) \in \lfloor\delta\rfloor_\varepsilon^*$. Finally, since $va_j^{-1}a_jv^{-1} \xrightarrow{*} \varepsilon$, we obtain from Fact 7 that $(q, \varepsilon, r) \in \lfloor\delta\rfloor_\varepsilon$ as desired. This concludes the proof for the first condition.

Second condition. Consider $q_1, \ldots, q_k, r_1, \ldots, r_k \in Q$ and $w_1, \ldots, w_k \in A^*$ such that $\sum_{i \leq k} d(q_i, w_i, r_i) \leq \ell - 1$ and $\alpha(w_1) = \cdots = \alpha(w_k)$. We need to exhibit $u \in \tilde{A}^*$ such that $(q_i, u, r_i) \in \lfloor\delta\rfloor_\varepsilon^*$ for every $i \leq k$. By definition of α, we have $\beta(w_1) = \cdots = \beta(w_k)$. Let $S = \{q_1, \ldots, q_k\}$. There are two cases depending on whether w_1 is F_S-safe.

Assume first that w_1 is F_S-safe. By Lemma 15, it follows that $\beta(w_1) \in F_S$. We get $u \in \tilde{A}^*$ such that $u \in \bigcap_{i \leq k} L(q_i)$ and $\beta(u) = \beta(w_1) = \cdots = \beta(w_k)$. Thus, since $d(q_i, w_i, r_i) \leq \ell - 1$ by hypothesis, Lemma 16 yields $(q_i, u, r_i) \in \lfloor\delta\rfloor_\varepsilon^*$ for every $i \leq k$, concluding this case.

Assume now that w_1 is *not* F_S-safe: we have an F_S-alternating pair (h, a) such $\#_{h,a}(w_1)$ is odd. Since $\alpha(w_1) = \cdots = \alpha(w_k)$, we know that $\#_{h,a}(w_i)$ is odd for every $i \leq k$. Therefore, $\#_{h,a}(w_i) \geq 1$: we have $x_i, y_i \in A^*$ such that $w_i = x_iay_i$ and $\beta(x_i) = h$. Fact 10 yields $s_i, t_i \in Q$ such that $d(q_i, x_i, s_i) + d(s_i, a, t_i) + d(t_i, y_i, r_i) = d(q_i, w_i, r_i)$. In particular, we have $d(t_i, y_i, r_i) \leq d(q_i, w_i, r_i)$ for every $i \leq k$. Moreover, (h, a) is F_S-alternating and $S = \{q_1, \ldots, q_k\}$. Hence, Corollary 18 yields $j \leq k$ such that (h, a) does **not** stabilize q_j. Since $\#_{h,a}(x_ja) \geq 1$, this implies $d(q_j, x_ja_j, t_j) \geq 1$. Consequently, we have the *strict* inequality $d(t_j, y_j, r_j) < d(q_j, w_j, r_j)$. Altogether, we obtain $\sum_{i \leq k} d(t_i, y_i, r_i) < \sum_{i \leq k} d(q_i, w_i, r_i)$. By hypothesis, this implies that $\sum_{i \leq k} d(t_i, y_i, r_i) \leq (\ell - 1) - 1$. Moreover, $\beta(w_1) = \cdots = \beta(w_k)$, $\beta(x_1a) = \cdots = \beta(x_ka) = h\beta(a)$ and H is a group. Hence, we have $\beta(y_1) = \cdots = \beta(y_k)$ and since β is a $(\ell - 1)$-synchronizer, we obtain $z \in \tilde{A}^*$ such that $(t_i, z, r_i) \in \lfloor\delta\rfloor_\varepsilon^*$ for every $i \leq k$.

We now consider two subcases. Since (h, a) is F_S-alternating, either $h \in F_S$ or $h\beta(a) \in F_S$. Assume first that $h \in F_S$. We get $v \in \bigcap_{i \leq k} L(q_i)$ such that $\beta(v) = h = \beta(x_1) = \cdots = \beta(x_n)$. Since $d(q_i, x_i, s_i) \leq d(q_i, w_i, r_i) \leq \ell - 1$, Lemma 16 yields $(q_i, v, s_i) \in \lfloor \delta \rfloor_\varepsilon^*$ for every $i \leq k$. Moreover, we have $(s_i, a, t_i) \in \delta$. Altogether, it follows that $(q_i, vaz, r_i) \in \lfloor \delta \rfloor_\varepsilon^*$ for every $i \leq k$. This concludes the first subcase. Finally, assume that $h\beta(a) \in F_S$. This yields $v' \in \bigcap_{i \leq k} L(q_i)$ such that $\beta(v') = h\beta(a) = \beta(x_1 a) = \cdots = \beta(x_n a)$. Since $d(q_i, x_i a_i, t_i) \leq d(q_i, w_i, r_i) \leq \ell - 1$, Lemma 16 yields $(q_i, v', t_i) \in \lfloor \delta \rfloor_\varepsilon^*$ for every $i \leq k$. Altogether, it follows that $(q_i, v'z, r_i) \in \lfloor \delta \rfloor_\varepsilon^*$ for every $i \leq k$. This concludes the proof of Proposition 12.

4 Covering and separation for alphabet modulo testable languages

We prove that covering is decidable for AMT as well. Let us point out that this can be obtained from an algebraic theorem of Delgado [3]. Yet, this approach is indirect: Delgado's results are purely algebraic and do not mention separation. Formulating them would require a lot of groundwork. We use a direct approach based on standard arithmetical and automata theoretic arguments. As for GR, the procedure is based on a theorem characterizing the finite sets of regular languages which are AMT-coverable. We reuse the construction $\mathcal{A} \mapsto \lfloor \mathcal{A} \rfloor$ defined in Section 2. We start with terminology that we need to formulate the result.

Let $n = |A|$. We fix an arbitrary linear order A and let $A = \{a_1, \ldots, a_n\}$. We use this order to define a map $\zeta : \tilde{A}^* \to \mathbb{Z}^n$ (where $\mathbb{Z}$ is the set of integers). Given, $w \in \tilde{A}^*$, we define,

$$\zeta(w) = (|w|_{a_1} - |w|_{a_1^{-1}}, \ldots, |w|_{a_n} - |w|_{a_n^{-1}}) \in \mathbb{Z}^n.$$

For a language $L \subseteq \tilde{A}^*$ over $\tilde{A}$, we shall consider the direct image $\zeta(L) = \{\zeta(w) \mid w \in L\} \subseteq \mathbb{Z}^n$. We may now present the characterization theorem.

▶ **Theorem 21.** *Let $k \geq 1$ and k* NFAs *$\mathcal{A}_1, \ldots, \mathcal{A}_k$. The following conditions are equivalent:*

1. *The set $\{L(\mathcal{A}_1), \cdots, L(\mathcal{A}_k)\}$ is* AMT*-coverable.*
2. *We have $\bigcap_{i \leq k} \zeta(L(\lfloor \mathcal{A}_i \rfloor)) = \emptyset$.*

We first explain why Theorem 21 implies the decidability of AMT-covering. This follows from standard results and the decidability of Presburger arithmetic. Let us present a sketch.

The definition of the map $\zeta : \tilde{A}^* \to \mathbb{Z}^n$ is a variation on a standard notion. Given a word $w \in \tilde{A}^*$, its *Parikh image* (also called commutative image) is defined as the following vector,

$$\pi(w) = (|w|_{a_1}, \ldots, |w|_{a_n}, |w|_{a_1^{-1}}, \ldots, |w|_{a_n^{-1}}) \in \mathbb{N}^{2n}.$$

Clearly, $\pi(w)$ determines $\zeta(w)$ and for every $L \subseteq \tilde{A}^*$, $\pi(L) \subseteq \mathbb{N}^{2n}$ determines $\zeta(L) \subseteq \mathbb{Z}^n$. Consider k NFAs $\mathcal{A}_1, \ldots, \mathcal{A}_k$. We know that $\lfloor \mathcal{A}_i \rfloor$ can be computed from $\mathcal{A}_i$ in polynomial time for every $i \leq k$. Moreover, it is known [5] that an *existential* Presburger formula φ_i describing the set $\pi(L(\lfloor \mathcal{A}_i \rfloor)) \subseteq \mathbb{N}^{2n}$ can be computed from $\tilde{\mathcal{A}}_i$ in polynomial time. It is then straightforward to combine the formulas φ_i into a single *existential* Presburger sentence which is equivalent to $\bigcap_{i \leq k} \zeta(L(\lfloor \mathcal{A}_i \rfloor)) \neq \emptyset$. Finally, it is known [23] that the existential fragment of Presburger arithmetic can be decided in NP. Hence, deciding whether $\bigcap_{i \leq k} \zeta(L(\lfloor \mathcal{A}_i \rfloor)) \neq \emptyset$ can be achieved in NP. It then follows from Theorem 21 that AMT-covering (and therefore AMT-separation as well) can be decided in co-NP. It turns out that this complexity upper bound is optimal: AMT-covering and AMT-separation are both co-NP-complete (we present a simple proof for the lower bound in Appendix B using a reduction from 3-SAT).

We prove the implication 2) $\Rightarrow$ 1) in Theorem 21. The converse is shown in Appendix B (the proof is similar to what we did for GR in Section 3). We use standard arithmetical

tools. We consider the componentwise addition on $\mathbb{Z}^n$. Moreover, we abuse terminology and write "0" for the neutral element (*i.e.*, the vector whose entries are all equal to zero). Given a single vector $\bar{v} \in \mathbb{Z}^n$ and a *finite* set of vectors $V = \{\overline{v_1}, \dots, \overline{v_\ell}\} \subseteq \mathbb{Z}^n$, we write,

$$\mathcal{L}(\bar{v}, V) = \{\bar{v} + k_1\overline{v_1} + \cdots + k_\ell\overline{v_\ell} \mid k_1, \dots, k_\ell \in \mathbb{Z}\} \subseteq \mathbb{Z}^n.$$

The sets $\mathcal{L}(\bar{v}, V)$ are called the *linear subsets* of $\mathbb{Z}^n$. Finally, the *semi-linear* subsets of $\mathbb{Z}^n$ are the finite unions of linear sets (note that this includes $\emptyset$, which is the empty union). We need two results about these sets. The first one is a variation on Parikh's theorem (which states that the Parikh images of regular languages are semi-linear subsets of $\mathbb{N}^n$). Yet, it is specific to the automata built with $\mathcal{A} \mapsto \lfloor \mathcal{A} \rfloor$. The proof is presented in Appendix B.

▶ **Lemma 22.** *Let $\mathcal{A}$ be a NFA. Then, $\zeta(L(\lfloor \mathcal{A} \rfloor))$ is a semi-linear subset of $\mathbb{Z}^n$.*

The second result is more general. We prove it in Appendix B as a corollary of a standard theorem concerning the bases of subgroups of free commutative groups (*i.e.*, the groups $\mathbb{Z}^n$). See [7, Theorem 1.6] for example. The statement is as follows.

▶ **Proposition 23.** *Let $n \geq 1$ and S a semi-linear subset of $\mathbb{Z}^n$. Assume that for every $d \geq 1$, there exists $\bar{u} \in \mathbb{Z}^n$ such that $d\bar{u} \in S$. Then, $0 \in S$.*

Proof of 2) ⇒ 1) **in Theorem 21.** We actually prove the contrapositive. More precisely, we Assume that $\{L(\mathcal{A}_1), \cdots, L(\mathcal{A}_k)\}$ is *not* AMT-coverable and prove that $\bigcap_{i \leq k} \zeta(L(\lfloor \mathcal{A}_i \rfloor)) \neq \emptyset$. First, we use our hypothesis to prove the following lemma.

▶ **Lemma 24.** *For every $d \geq 1$, there exist $\bar{x}, \overline{y_1}, \dots, \overline{y_k} \in \mathbb{Z}^n$ such that $\bar{x} + d\overline{y_i} \in \zeta(L(\lfloor \mathcal{A}_i \rfloor))$ for every $i \leq k$.*

Proof. Given two words $w, w' \in A^*$, we write $w \sim_d w'$ if and only if $|w|_a \equiv |w'|_a \bmod d$ for every $a \in A$. Clearly, $\sim_d$ is an equivalence of finite index on A^* and one may verify that every $\sim_d$-class belongs to AMT. Hence, the partition $\mathbf{K}$ of A^* into $\sim_d$-classes is an AMT-cover of A^*. Therefore, since $\{L(\mathcal{A}_1), \cdots, L(\mathcal{A}_k)\}$ is not AMT-coverable, there exists a $\sim_d$-class which intersects all languages $L(\mathcal{A}_i)$ for $i \leq k$. We get $w_1 \in L(\mathcal{A}_1), \dots, w_k \in L(\mathcal{A}_k)$ such that $w_1 \sim_d \cdots \sim_d w_n$. Let $\bar{x} = \zeta(w_1) \in \mathbb{N}^n$. Consider $i \leq k$. Since $w_i \sim_d w_1$, one may verify that there exists $\overline{y_i} \in \mathbb{Z}^n$ such that $\zeta(w_i) = \bar{x} + d\overline{y_i}$. Finally, since $w_i \in L(\mathcal{A}_i) \subseteq L(\lfloor \mathcal{A}_i \rfloor)$, we have $\zeta(w_i) \in \zeta(L(\lfloor \mathcal{A}_i \rfloor))$ which concludes the proof. ◀

By Lemma 22, the sets $\zeta(L(\lfloor \mathcal{A}_i \rfloor)) \subseteq \mathbb{Z}^n$ are semi-linear for all $i \leq k$. We use them to build a semi-linear subset of $\mathbb{Z}^{kn}$. We use vector concatenation: given $i, j \geq 1$, $\bar{x} \in \mathbb{Z}^i$ and $\bar{y} \in \mathbb{Z}^j$, we write $\bar{x} \cdot \bar{y} \in \mathbb{Z}^{i+j}$ for the vector obtained by concatenating $\bar{x}$ with $\bar{y}$. We define,

$$S = \{\overline{u_1} \cdots \overline{u_k} + \bar{x}^k \mid \overline{u_i} \in \zeta(L(\lfloor \mathcal{A}_i \rfloor)) \text{ for every } i \leq k \text{ and } \bar{x} \in \mathbb{Z}^n\} \subseteq \mathbb{Z}^{kn}.$$

Since the sets $\zeta(L(\lfloor \mathcal{A}_i \rfloor)) \subseteq \mathbb{Z}^n$ are semi-linear, one may verify that $S \subseteq \mathbb{Z}^{kn}$ is semi-linear as well. Lemma 24 implies that for every $d \geq 1$, there exist $\bar{x}, \overline{y_1}, \dots, \overline{y_k} \in \mathbb{Z}^n$ such that $\bar{x} + d\overline{y_i} \in \zeta(L(\lfloor \mathcal{A}_i \rfloor))$ for all $i \leq k$. By definition of S, this implies $d(\overline{y_1} \cdots \overline{y_k}) \in S$. Altogether, it follows that for all $d \geq 1$, there exists $\bar{y} \in \mathbb{Z}^{kn}$ such that $d\bar{y} \in S$. Since S is semi-linear, this yields $0 \in S$ by Proposition 23. By definition of S, we get $\bar{x} \in \mathbb{Z}^n$ such that $\bar{x} \in \zeta(L(\lfloor \mathcal{A}_i \rfloor))$ for every $i \leq k$. Thus, $\bigcap_{i \leq k} \zeta(L(\lfloor \mathcal{A}_i \rfloor)) \neq \emptyset$ which completes the proof. ◀

5 Covering and separation for modulo languages

Getting a "naive" direct algorithm for MOD-covering is fairly straightforward. Here, we prove that MOD-covering reduces to both GR-covering and AMT-covering (in logarithmic space). This approach provides much better complexity upper bounds than the naive one.

The reduction is based on a simple construction which takes a language $L \subseteq A^*$ as input and builds a new one over a *unary alphabet* (*i.e.*, which contains a unique letter). We let $U = \{\$\}$ and write $\upsilon : A^* \to U^*$ for the morphism defined by $\upsilon(a) = \$$ for every $a \in A$. Given a regular language $L \subseteq A^*$, is standard that $\upsilon(L) \subseteq U^*$ is also regular. Moreover, given an NFA $\mathcal{A}$ recognizing L as input, one may compute an NFA recognizing $\upsilon(L)$ in logarithmic space (this amounts to relabeling every transition with "$").

▶ **Theorem 25.** *Let $k \geq 1$ and $L_1, \ldots, L_k \subseteq A^*$. The following conditions are equivalent:*

1. *The set $\{L_1, \cdots, L_k\}$ is* MOD*-coverable.*
2. *The set $\{\upsilon(L_1), \cdots, \upsilon(L_k)\}$ is* AMT*-coverable.*
3. *The set $\{\upsilon(L_1), \cdots, \upsilon(L_k)\}$ is* GR*-coverable.*

In view of Theorem 25, we have a logarithmic space reduction from MOD-covering to AMT-covering. By the results of Section 4, this implies that MOD-covering is decidable and in co-NP. Moreover, Theorem 25 also provides a logarithmic space reduction from MOD-separation to GR-separation. By the results of Section 3, it follows that MOD-separation is decidable and in P. We prove in Appendix C that MOD-separation is in NL (this is based on a simple analysis of the GR-separation procedure for *unary alphabets*). This implies that MOD-separation is NL-complete as NL is a generic lower bound for separation. There exists a reduction from NFA emptiness (which is NL-complete) to $\mathcal{C}$-separation for an arbitrary Boolean algebra $\mathcal{C}$: given an NFA $\mathcal{A}$, $L(\mathcal{A}) = \emptyset$ if and only if $L(\mathcal{A})$ is $\mathcal{C}$-separable from A^*.

Proof of Theorem 25. We prove that 1) ⇒ 2) ⇒ 3) ⇒ 1). Let us start with 1) ⇒ 2). Assume that $\{L_1, \cdots, L_k\}$ is MOD-coverable: there exists a MOD-cover $\mathbf{K}$ of A^* such that for every $K \in \mathbf{K}$, there exists $i \leq k$ satisfying $K \cap L_i = \emptyset$. Consider the set $\mathbf{H} = \{\upsilon(K) \mid K \in \mathbf{K}\}$. Since $\mathbf{K}$ is a cover of A^* and υ is surjective, $\mathbf{H}$ must be a cover of U^*. It is also simple to verify that every $H \in \mathbf{H}$ belongs to MOD since this is the case for every $K \in \mathbf{K}$. Hence, since MOD $\subseteq$ AMT, we obtain that $\mathbf{H}$ is an AMT-cover of U^*. It remains to verify for every $H \in \mathbf{H}$, there exists $i \leq k$ such that $H \cap \upsilon(L_i) = \emptyset$. We fix $H \in \mathbf{H}$ for the proof. By definition, $H = \upsilon(K)$ for some $K \in \mathbf{K}$. By hypothesis on $\mathbf{K}$, we get $i \leq k$ such that $K \cap L_i = \emptyset$. We show that $H \cap \upsilon(L_i) = \emptyset$. By contradiction, assume that there exists $u \in H \cap \upsilon(L_i) = \emptyset$. Since $H = \upsilon(K)$, we get $w \in K$ and $w' \in L_i$ such that $\upsilon(w) = \upsilon(w') = u$. By definition of υ, this implies $|w| = |w'| = |u|$. Since $w \in K$ and $K \in$ MOD, one may verify that this implies $w' \in K$. Thus, $w' \in K \cap L_i$, contradicting the hypothesis that $K \cap L_i = \emptyset$.

The implication 2) ⇒ 3) is trivial since AMT $\subseteq$ GR. Hence, it remains to show that 3) ⇒ 1). Assume that $\{\upsilon(L_1), \cdots, \upsilon(L_k)\}$ is GR-coverable. This yields a GR-cover $\mathbf{H}$ of U^* such that for every $H \in \mathbf{H}$, there exists $i \leq k$ satisfying $H \cap \upsilon(L_i) = \emptyset$. We let $\mathbf{K} = \{\upsilon^{-1}(H) \mid H \in \mathbf{H}\}$. By definition of $\mathbf{H}$, one may verify that $\mathbf{K}$ is a cover of A^* and that for every $K \in \mathbf{K}$, there exist $i \leq k$ such that $K \cap L_i = \emptyset$. We show that $\mathbf{K}$ is actually a MOD-cover, which implies, as desired, that $\{L_1, \cdots, L_k\}$ is MOD-coverable. Given $H \in \mathbf{H}$, we have to verify that $\upsilon^{-1}(H) \in$ MOD. By hypothesis, we have $H \in$ GR. Therefore, there exists a morphism $\alpha : U^* \to G$ into a finite group G recognizing H. Hence, $\upsilon^{-1}(H)$ is recognized by the morphism $\alpha \circ \upsilon : A^* \to G$. By definition of υ, it is immediate that $\alpha(\upsilon(a)) = \alpha(\upsilon(b))$ for every $a, b \in A$. This yields $\upsilon^{-1}(H) \in$ MOD by Lemma 3, concluding the proof. ◀

6 Conclusion

We proved simple separation and covering algorithms for the classes GR, AMT and MOD using only standard notions from automata theory. For GR and AMT, the algorithms are based on the automata-theoretic construction "$\mathcal{A} \mapsto \lfloor \mathcal{A} \rfloor$". In particular, the statements behind the two algorithms (*i.e.*, Theorem 9 and Theorem 21) are quite similar. Hence, a natural question is whether their proofs can be unified (as of now, they are independent).

References

1. Christopher J. Ash. Inevitable graphs: a proof of the type II conjecture and some related decision procedures. *International Journal of Algebra and Computation*, 1(1):127–146, 1991.
2. Karl Auinger. A new proof of the Rhodes type II conjecture. *International Journal of Algebra and Computation*, 14(5-6):551–568, 2004.
3. Manuel Delgado. Abelian poinlikes of a monoid. *Semigroup Forum*, 56(3):339–361, 1998.
4. Leslie M. Goldschlager. The monotone and planar circuit value problems are log space complete for P. *SIGACT News*, 9:25–29, 1977.
5. Peter Habermehl, Anca Muscholl, Thomas Schwentick, and Helmut Seidl. Counting in trees for free. In *Proceedings of the 31st International Colloquium on Automata, Languages and Programming*, ICALP'04, pages 1136–1149, Berlin, Heidelber, 2004. Springer-Verlag.
6. Karsten Henckell, Stuart Margolis, Jean-Eric Pin, and John Rhodes. Ash's type II theorem, profinite topology and Malcev products. *International Journal of Algebra and Computation*, 1:411–436, 1991.
7. Thomas W. Hungerford. *Algebra / Thomas W. Hungerford*. Springer-Verlag, 1980.
8. Eryk Kopczynski and Anthony Widjaja To. Parikh images of grammars: Complexity and applications. In *Proceedings of the 25th Annual IEEE Symposium on Logic in Computer Science, LICS 2010*, pages 80–89, 2010.
9. Stuart W. Margolis and Jean-Eric Pin. New results on the conjecture of rhodes and on the topological conjecture. *Journal of Pure and Applied Algebra*, 80(3):305 – 313, 1992.
10. Jean-Eric Pin. Polynomial closure of group languages and open sets of the hall topology. In *Proceedings of the 21st International Colloquium on Automata, Languages, and Programming*, ICALP'94, pages 424–435, Berlin, Heidelberg, 1994. Springer-Verlag.
11. Jean-Eric Pin. BG = PG: A success story. 1995.
12. Jean-Eric Pin. *The dot-depth hierarchy, 45 years later*, chapter 8, pages 177–202. World Scientific, 2017.
13. Jean-Eric Pin. *Open Problems About Regular Languages, 35 Years Later*, chapter 7, pages 153–175. World Scientific, 2017.
14. Jean-Eric Pin and Christophe Reutenauer. A Conjecture on the Hall Topology for the Free Group. *Bulletin of the London Mathematical Society*, 23(4):356–362, 1991.
15. Thomas Place. The amazing mixed polynomial closure and its applications to two-variable first-order logic, 2022. `arXiv:2202.03989`.
16. Thomas Place and Marc Zeitoun. The covering problem. *Logical Methods in Computer Science*, 14(3), 2018.
17. Thomas Place and Marc Zeitoun. Generic results for concatenation hierarchies. *Theory of Computing Systems (ToCS)*, 63(4):849–901, 2019. Selected papers from CSR'17.
18. Thomas Place and Marc Zeitoun. Going higher in first-order quantifier alternation hierarchies on words. *Journal of the ACM*, 66(2):12:1–12:65, 2019.
19. Thomas Place and Marc Zeitoun. On all things star-free. In *Proceedings of the 46th International Colloquium on Automata, Languages, and Programming*, ICALP'19, pages 126:1–126:14, 2019.
20. Thomas Place and Marc Zeitoun. Separation and covering for group based concatenation hierarchies. In *Proceedings of the 34th Annual ACM/IEEE Symposium on Logic in Computer Science*, LICS'19, pages 1–13, 2019.

705 **21** Thomas Place and Marc Zeitoun. Characterizing level one in group-based concatenation
706 hierarchies, 2022. `arXiv:2201.06826`.
707 **22** Luis Ribes and Pavel A. Zalesskii. On the profinite topology on a free group. *Bulletin of the*
708 *London Mathematical Society*, 25(1):37–43, 1993.
709 **23** Bruno Scarpellini. Complexity of subcases of presburger arithmetic. *Transactions of the*
710 *American Mathematical Society*, 284:203–218, 1984.
711 **24** Marcel Paul Schützenberger. On finite monoids having only trivial subgroups. *Information*
712 *and Control*, 8(2):190–194, 1965.
713 **25** Pascal Tesson and Denis Therien. Logic Meets Algebra: the Case of Regular Languages.
714 *Logical Methods in Computer Science*, Volume 3, Issue 1, 2007.

A Appendix: Group languages

This appendix presents the missing proofs in Section 3. We also present a proof that GR-separation is P-hard.

A.1 Missing proofs

We first present the proof of Fact 7. Let us recall the statement.

▶ **Fact 7.** *Let $\mathcal{A} = (Q, I, F, \delta)$ be an NFA. Let $q, r \in Q$ and $w \in \tilde{A}^*$ such that $(q, w, r) \in \lfloor\delta\rfloor_\varepsilon^*$. If $w \in L_\varepsilon$, then $(q, \varepsilon, r) \in \lfloor\delta\rfloor_\varepsilon$. Also, if q, r are strongly connected, then $(r, w^{-1}, q) \in \lfloor\delta\rfloor_\varepsilon^*$.*

Proof. Since $(q, w, r) \in \lfloor\delta\rfloor_\varepsilon^*$, one may verify from the definition of $\lfloor\delta\rfloor_\varepsilon$ that there exist $u_0, \ldots, u_n \in \tilde{A}^*$ and $v_1, \ldots, v_n \in L_\varepsilon$ such that $w = u_0 \cdots u_n$ and $(q, x, r) \in \lfloor\delta\rfloor^*$ where $x = u_0 v_1 u_1 \cdots v_n u_n$. We may now prove the fact. Assume first that $w \in L_\varepsilon$. Since $v_1, \ldots, v_n \in L_\varepsilon$, we have $v_i \xrightarrow{*} \varepsilon$ for every $i \leq n$. Hence, $x \xrightarrow{*} w$ and since $w \in L_\varepsilon$, we get $x \xrightarrow{*} \varepsilon$. Thus, since $(q, x, r) \in \lfloor\delta\rfloor^*$, we get $(q, \varepsilon, r) \in \lfloor\delta\rfloor_\varepsilon$ by definition. Assume now that q, r are strongly connected. Since $(q, x, r) \in \lfloor\delta\rfloor^*$, this implies $(r, x^{-1}, q) \in \lfloor\delta\rfloor^*$ by definition of $\lfloor\delta\rfloor$. Moreover, $x^{-1} = u_n^{-1} v_n^{-1} \cdots u_1^{-1} v_1^{-1} u_0^{-1}$ and since $v_i \xrightarrow{*} \varepsilon$ for every $i \leq n$, we also have $v_i^{-1} \xrightarrow{*} \varepsilon$ for every $i \leq n$. Thus, since $(r, x^{-1}, q) \in \lfloor\delta\rfloor^*$, it is immediate that $(r, u_n^{-1} \cdots u_0^{-1}, q) \in \lfloor\delta\rfloor_\varepsilon^*$ by definition of $\lfloor\delta\rfloor_\varepsilon$. Since $u_n^{-1} \cdots u_0^{-1} = w^{-1}$ (recall that $w = u_0 \cdots u_n$), this concludes the proof ◀

We turn to Lemma 8. The statement is as follows.

▶ **Lemma 8.** *Let $\mathcal{A} = (Q, I, F, \delta)$ be an NFA and let $\alpha : A^* \to G$ be a morphism into a finite group. For every $q, r \in Q$ and $w \in \tilde{A}^*$ such that $(q, w, r) \in \lfloor\delta\rfloor_\varepsilon^*$, there exists $w' \in A^*$ such that $(q, w', r) \in \delta^*$ and $\alpha(w) = \alpha(w')$.*

Proof. Since $(q, w, r) \in \lfloor\delta\rfloor_\varepsilon^*$, one may verify from the definition of $\lfloor\delta\rfloor_\varepsilon$ that there exist $u_0, \ldots, u_n \in \tilde{A}^*$ and $v_1, \ldots, v_n \in L_\varepsilon$ such that $w = u_0 \cdots u_n$ and $(q, x, r) \in \lfloor\delta\rfloor^*$ where $x = u_0 v_1 u_1 \cdots v_n u_n$. By Lemma 6, there exists $w' \in A^*$ such that $(q, w', r) \in \delta^*$ and $\alpha(x) = \alpha(w')$. Moreover, since $v_1, \ldots, v_n \in L_\varepsilon$, we have $v_i \xrightarrow{*} \varepsilon$ for every $i \leq n$. Clearly, this implies $\alpha(v_i) = 1_G$ for every $i \leq n$. Therefore, $\alpha(w) = \alpha(x) = \alpha(w')$ which concludes the proof. ◀

Finally, we complete the proof of Lemma 16.

▶ **Lemma 16.** *Let $s, t \in Q$ and $w \in A^*$ such that $d(s, w, t) \leq \ell - 1$. The following holds:*

1. *for every $v \in L(s)$ such that $\beta(w) = \beta(v)$, we have $(s, v, t) \in \lfloor\delta\rfloor_\varepsilon^*$.*
2. *for every $v \in L(t)$ such that $\beta(w) = (\beta(v))^{-1}$, we have $(s, v^{-1}, t) \in \lfloor\delta\rfloor_\varepsilon^*$.*

Proof. First, consider $v \in L(s)$ such that $\beta(w) = \beta(v)$. By definition, we have $s' \in Q$ such that s, s' are strongly connected and $(s, v, s') \in \lfloor\delta\rfloor_\varepsilon^*$. By Fact 7, we have $(s', v^{-1}, s) \in \lfloor\delta\rfloor_\varepsilon^*$. Lemma 8 yields $x \in A^*$ such that $(s', x, s) \in \delta^*$ and $\beta(x) = \beta(v^{-1})$. Since $d(s, w, t) \leq \ell - 1$ and s', s are strongly connected, it follows that $d(s', xw, t) \leq \ell - 1$. Moreover, since $\beta(w) = \beta(v)$ and $\beta(x) = \beta(v^{-1})$, we have $\beta(xw) = 1_H$. Altogether, since β is an $(\ell - 1)$-synchronizer, we get $(s', \varepsilon, t) \in \lfloor\delta\rfloor_\varepsilon^*$. Since $(s, v, s') \in \lfloor\delta\rfloor_\varepsilon^*$, it follows that $(s, v, t) \in \lfloor\delta\rfloor_\varepsilon^*$ as desired.

We now consider $v \in L(t)$ such that $\beta(w) = (\beta(v))^{-1}$. By definition, we have $t' \in Q$ such that t, t' are strongly connected and $(t, v, t') \in \lfloor\delta\rfloor_\varepsilon^*$. Lemma 8 yields $y \in A^*$ such that $(t, y, t') \in \delta^*$ and $\beta(y) = \beta(v)$. Since $d(s, w, t) \leq \ell - 1$ and t, t' are strongly connected, it follows that $d(s, wy, t) \leq \ell - 1$. Moreover, since $\beta(w) = (\beta(v))^{-1}$ and $\beta(y) = \beta(v)$, we

have $\beta(wy) = 1_H$. Altogether, since β is an $(\ell-1)$-synchronizer, we get $(s, \varepsilon, t') \in \lfloor \delta \rfloor_\varepsilon^*$. Finally, since $(t, v, t') \in \lfloor \delta \rfloor_\varepsilon^*$ and t, t' are strongly connected, Fact 7 yields $(t', v^{-1}, t) \in \lfloor \delta \rfloor_\varepsilon^*$. Altogether, we get $(s, v^{-1}, t) \in \lfloor \delta \rfloor_\varepsilon^*$ as desired. ◀

A.2 Complexity of GR-separation

We prove that GR-separation is P-complete. We already presented the upper bound in the main text: GR-separation is in P. Here, we concentrate on the lower bound: we show that the problem is P-hard. In fact, we show this lower bound for the special case of GR-separation when one of the two inputs is the singleton $\{\varepsilon\}$.

We present a logarithmic space reduction from the Circuit Value problem. We use the variant in which all gates are either a disjunction ($\vee$) or a conjunction ($\wedge$), which is P-complete [4]. A Boolean circuit is a finite directed acyclic graph such that:

- There are arbitrarily many *input vertices* with no incoming edge. There must all be labeled by truth value (0 for *false*, 1 for *true*).
- The other vertices have exactly two incoming edges. They are called *gates* and are labeled by a logical connective: "$\vee$" or "$\wedge$". They may have arbitrarily many outgoing edges.
- There is a single gate with no outgoing edge. It is called the *output vertex*.

We present an Example of Boolean circuit in Figure 2 below:

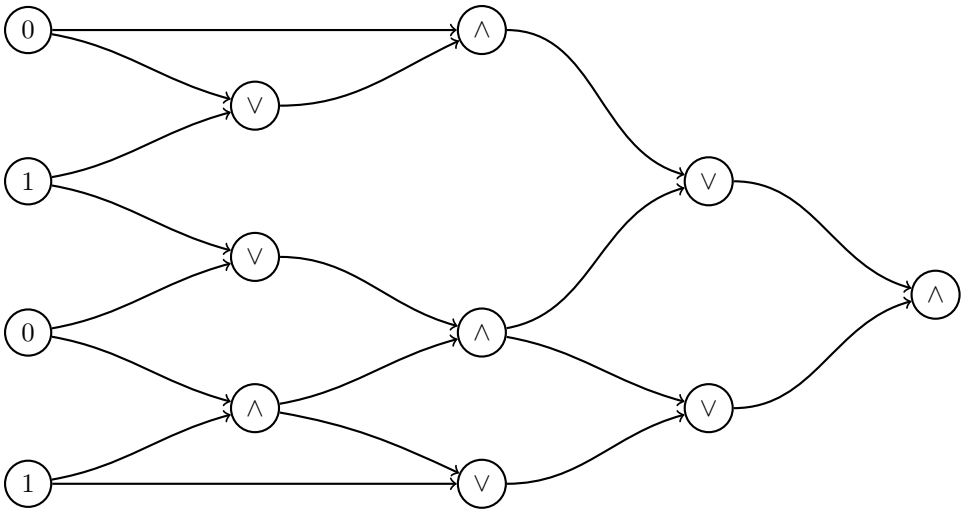


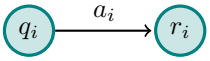
Figure 2 An example of Boolean circuit which evaluates to 0.

Clearly, a Boolean circuit computes a truth value for each gate. The decision problem takes as input a Boolean circuit C and asks whether the logical value computed by the output vertex is true. We present a logarithmic space reduction from this problem to *non*-separability by GR. More precisely, given as input a Boolean circuit C, we construct an NFA $\mathcal{A}_C$ such that C evaluates to true if and only if $\{\varepsilon\}$ is not GR-separable from $L(\mathcal{A}_C)$. This implies that GR-separation is P-hard, as desired. Note that we only present the construction of $\mathcal{A}_C$. That it can be implemented in logarithmic space is straightforward and left to the reader.

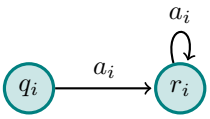
We fix the Boolean circuit C for the construction and describe the NFA $\mathcal{A}_C = (Q, I, F, \delta)$. We let n be the number of vertices in C and $\{v_1, \ldots, v_n\}$ be the set of all these vertices, with v_n as the output vertex. The NFA $\mathcal{A}$ uses an alphabet $A = \{a_1, \ldots, a_n\}$ of size n. For each $i \leq n$, the set of states Q contains three states q_i, r_i and s_i associated to the vertex v_i

(note that while q_i and r_i are always used, s_i is only used when v_i is a gate labeled by "$\wedge$"). Moreover, we also associate several transitions in δ connecting these three states to those associated to other vertices. There are several cases depending on v_i.

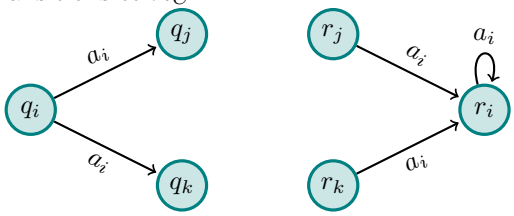
- First, we consider the case when v_i is an input vertex. If v_i is labeled by "0" (false), we add the following states and transition to $\mathcal{A}_C$:



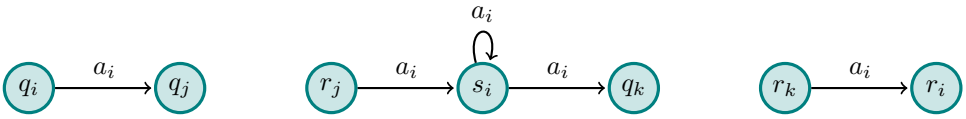
Ifv_i is labeled by "1". In that case, we add the following states and transitions to $\mathcal{A}_C$:



- We now consider the case when v_i is a gate. Let $j, k \leq n$ be the two indices such that there are edges from v_j to v_i and from v_k to v_i in C. If v_i is labeled by "$\vee$", we add the following states and transitions to $\mathcal{A}_C$:



Finally, when v_i is labeled by "$\wedge$", we add the following states and transitions to $\mathcal{A}_C$:



Recall that v_n is the output vertex of C. We let $\mathcal{A}_C = (Q, \{q_n\}, \{r_n\}, \delta)$. One may now verify from the definition that the output vertex of C evaluates to 1 if and only if $\{\varepsilon\}$ is not GR-separable from $L(\mathcal{A}_C)$. Let us point out that the proof argument should not consider GR-separation directly: we use Theorem 9 instead. Indeed, Theorem 9 implies that $\{\varepsilon\}$ is not GR-separable from $L(\mathcal{A}_C)$ if and only if $\varepsilon \in L(\lfloor \mathcal{A}_C \rfloor_\varepsilon)$. It is straightforward to verify that the latter property is equivalent to the the output vertex of C evaluating to 1. This completes the presentation of our reduction.

B Appendix: Alphabet modulo testable languages

This appendix is devoted to the alphabet modulo testable languages. We first provide a proof for Lemma 4. Then we turn to the missing parts in the proof of followed by the proof of Theorem 21 (which we partially presented in the main text. Finally, we prove that both AMT-separation and AMT-covering are co-NP-complete.

B.1 Proof of Lemma 4

For the proof, we shall need an equivalence on A^* that we already encountered in the proof of Lemma 24. We first recall it and prove the correspondence with AMT properly. For every number $d \geq 1$, we associate an equivalence $\sim_d$ over A^* and use it to characterize the languages in AMT. Let $d \geq 1$ and $w, w' \in A^*$, we write $w \sim_d w'$ if and only if $|w|_a \equiv |w'|_a \bmod d$ for every $a \in A$. It is immediate from the definition that $\sim_d$ is an equivalent of finite index. We have the following lemma.

▶ **Lemma 26.** *For every language $L \subseteq A^*$, we have $L \in$ AMT if and only if there exists $d \geq 1$ such that L is a union of $\sim_d$-classes.*

Proof. Assume first that $L \in$ AMT. By definition, L is built from finitely many languages $L^a_{q,r}$ (with $a \in A$ and $q, r \in \mathbb{N}$ such that $r < q$) using only unions and intersections. Let d be the least common multiplier of all numbers $q \geq 1$ used in these languages. We show that L is a union of $\sim_d$-classes. Given $w, w' \in A^*$ such that $w \sim_d w'$, we have to show that $w \in L \Leftrightarrow w' \in L$. By hypothesis, it suffices to show that each language $L^a_{q,r}$ in the definition of L satisfies $w \in L^a_{q,r} \Leftrightarrow w' \in L^a_{q,r}$. Since d is a multiple of q (by choice of d), the hypothesis that $w \sim_d w'$ yields $|w|_a \equiv |w'|_a \bmod q$. Hence, since $L^a_{q,r} = \{w \in A^* \mid |w|_a \equiv r \bmod q\}$ by definition, we have $w \in L^a_{q,r} \Leftrightarrow w' \in L^a_{q,r}$ as desired.

Conversely, assume that L is a union of $\sim_d$-classes for some $d \geq 1$ and show that $L \in$ AMT. Since $\sim_d$ has finite index and AMT is closed under union, it suffices to show that every $\sim_d$-class belongs to AMT. Let $w \in A^*$ and consider its $\sim_d$-class. For every $a \in A$, let $r_a < d$ by the remainder of the Euclidean division of $|w|_a$ by d. By definition, for every $w' \in A^*$, we have $w' \sim_d w$ if and only if $|w'|_a \equiv r_a \bmod d$ for every $a \in A$. It follows that the $\sim_d$-class of w is the language $\bigcap_{a \in A} L^a_{d,r_a}$ which belongs to AMT by definition. ◀

We turn to Lemma 4 itself. Let us first recall the statement.

▶ **Lemma 4.** *Let $L \subseteq A^*$. Then, $L \in$ AMT if and only if L is recognized by a morphism $\alpha : A^* \to G$ into a finite commutative group G.*

Proof. Assume first that $L \in$ MOD. We show that L is recognized by a morphism $\alpha : A^* \to G$ into a finite commutative group G. By definition of MOD, it suffices to prove that this property is true for all basic languages $L^a_{q,r}$ and that it is preserved by union and intersection. We first look at the language $L^a_{q,r} = \{w \in A^* \mid |w|_a \equiv r \bmod q\}$ for $a \in A$ and $q, r \in \mathbb{N}$ such that $r < q$. Clearly, $L^a_{q,r}$ is recognized by the morphism $\alpha : A^* \to \mathbb{Z}/q\mathbb{Z}$ defined by $\alpha(a) = 1$ and $\alpha(b) = 0$ for $b \in A \setminus \{a\}$ (where $\mathbb{Z}/q\mathbb{Z} = \{0, \ldots, q-1\}$ is the standard cyclic group): we have $L^a_{q,r} = \alpha^{-1}(r)$. Now, let $L_1, L_2 \subseteq A^*$ such that for $i = 1, 2$, L_i is recognized by a morphism $\alpha_i : A^* \to G_i$ into a finite commutative group G_i such that $\alpha_i(a) = \alpha_i(b)$ for all $a, b \in A$. Clearly, $L_1 \cup L_2$ and $L_1 \cap L_2$ are both recognized by the morphism $\alpha : A^* \to G_1 \to G_2$ (where $G_1 \times G_2$ is the commutative group equipped with the componentwise multiplication). This completes the proof for this direction.

Conversely, assume that L is recognized by a morphism $\alpha : A^* \to G$ into a finite commutative group G. We show that $L \in$ AMT. Since G is a finite group, it is standard that there exists a number $q \geq 1$ such that $g^q = 1_G$ for every $g \in G$. We use q to define an equivalence $\sim_q$ over A^*. We prove that L is a union of $\sim_q$-classes which yields $L \in$ AMT by Lemma 26. Let $u, v \in A^*$. We show that $u \in L \Leftrightarrow v \in L$. Since L is recognized by α it suffices to show that $\alpha(u) = \alpha(v)$. We write $A = \{a_1, \ldots, a_n\}$. As G is commutative, reorganizing the letters in u and v does not change their image under α. Thus, we have,

$$\alpha(u) = \alpha(a_1^{|u|_{a_1}} \cdots a_n^{|u|_{a_n}}) \qquad \text{and} \qquad \alpha(v) = \alpha(a_1^{|v|_{a_1}} \cdots a_n^{|v|_{a_n}}).$$

Moreover, since $u \sim_q v$, we have $|u|_{a_i} \equiv |v|_{a_i} \bmod q$ for every $i \leq n$. We get $r_i < q$ and $h_i, k_i \in \mathbb{N}$ such that $|u|_{a_i} = r_i + h_i \times q$ and $|v|_{a_i} = r_i + k_i \times d$. Therefore, since $g^d = 1_G$ for every $g \in G$, we obtain that for every $i \leq n$,

$$\alpha(a_i^{|u|_{a_i}}) = \alpha(a_i^{|v|_{a_i}}) = \alpha(a_i^{r_i}).$$

Altogether, it follows that $\alpha(u) = \alpha(v) = \alpha(a_1^{r_1} \cdots a_n^{r_n})$, which concludes the proof. ◀

B.2 Proof of Theorem 21

Recall that we write $n = |A|$. Moreover, an arbitrary linear order on A is fixed and we write $A = \{a_1, \ldots, a_n\}$. We used this linear order to define the map $\zeta : \tilde{A}^* \to \mathbb{Z}^n$. Let us now recall the statement of Theorem 21.

▶ **Theorem 21.** *Let $k \geq 1$ and k NFAs $\mathcal{A}_1, \ldots, \mathcal{A}_k$. The following conditions are equivalent:*
1. *The set $\{L(\mathcal{A}_1), \cdots, L(\mathcal{A}_k)\}$ is* AMT*-coverable.*
2. *We have $\bigcap_{i \leq k} \zeta(L(\lfloor \mathcal{A}_i \rfloor)) = \emptyset$.*

We already proved the implication 2) ⇒ 1) in the main text. Yet, we still need to provide proofs for Lemma 22 and Proposition 23. We start with the former.

▶ **Lemma 22.** *Let $\mathcal{A}$ be a NFA. Then, $\zeta(L(\lfloor \mathcal{A} \rfloor))$ is a semi-linear subset of $\mathbb{Z}^n$.*

Proof. The argument is based on standard ideas which are typically used to prove the automata variant of Parikh's theorem. However, let us point out that we do require a specific property of the automaton $\lfloor \mathcal{A} \rfloor$ at some point (the lemma is not true for an arbitrary NFA over the extended alphabet $\tilde{A}$). For all $q \in Q$, we associate a finite set $V_q \subseteq \mathbb{Z}^n$. We define,

$$V_q = \{\zeta(w) \mid w \in \tilde{A}^*, |w| \leq |Q| \text{ and } (q, w, q) \in \lfloor \delta \rfloor^*\}.$$

Observe that if $(q, w, q) \in \lfloor \delta \rfloor^*$ for some $w \in \tilde{A}^*$, the states encountered on this run are strongly connected. Hence, in that case, we also have $(q, w^{-1}, q) \in \lfloor \delta \rfloor^*$ by definition of $\lfloor \mathcal{A} \rfloor$. Moreover, we have $\zeta(w^{-1}) = -\zeta(w)$ by definition of ζ. Consequently, for every $\bar{v} \in V_q$, the opposite vector also belongs to V_q: we have $-\bar{v} \in V_q$. This property is where we need the hypothesis that are considering an automata built with the construction $\mathcal{A} \mapsto \lfloor \mathcal{A} \rfloor$ (it fails for an arbitrary NFA over $\tilde{A}$). For every $P \subseteq Q$, we write $V_P = \bigcup_{q \in P} V_q$.

Finally, we associate a second finite set $X_P \subseteq \mathbb{Z}^n$ to every $P \subseteq Q$. Let $w \in \tilde{A}^*$. We say that w is a P-witness if there exist $q \in I$ and $r \in F$ such that there is a run from q to r labeled by w such that P is exactly the set of all states encountered in that run (in particular, this means that $w \in L(\mathcal{A})$). We define,

$$X_P = \{\zeta(w) \mid w \text{ is a } P\text{-witness and } |w| \leq |Q|^2\}.$$

We now prove the following,

$$\zeta(L(\lfloor \mathcal{A} \rfloor)) = \bigcup_{P \subseteq Q} \bigcup_{\bar{v} \in X_P} \mathcal{L}(\bar{v}, V_P).$$

This equality concludes the proof: $\zeta(L(\lfloor \mathcal{A} \rfloor))$ is a semi-linear subset of $\mathbb{Z}^n$, as desired. We start with the right to left inclusion. Let $P \subseteq Q$ and $\bar{v} \in X_P$. We show that $\mathcal{L}(\bar{v}, V_P) \subseteq \zeta(L(\lfloor \mathcal{A} \rfloor))$.

Let $\bar{u} \in \mathcal{L}(\bar{v}, V_P)$. By definition, we have $\overline{v_1}, \ldots, \overline{v_\ell} \in V_P$ and $k_1, \ldots, k_\ell \in \mathbb{Z}$ such that $\bar{u} = \bar{v} + k_1\overline{v_1} + \cdots + k_\ell\overline{v_\ell}$. Moreover, recall that by construction, for every $\overline{v_i}$, the opposite vector $-\overline{v_i}$ belongs to V_P as well. Therefore, we may assume without loss of generality that $k_1, \ldots, k_\ell \in \mathbb{N}$: they are *positive integers*. By definition of V_P, we know that for every $i \leq \ell$, we have $\overline{v_i} \in V_{q_i}$ for some $q_i \in P$. Hence, there exists $x_i \in \tilde{A}^*$ such that $\zeta(w_i) = \overline{v_i}$ and $(q_i, y_i, q_i) \in \lfloor \delta \rfloor^*$. Let $y_i = (w_i)^{k_i}$ (this is well-defined since $k_i \in \mathbb{N}$). Clearly, $\zeta(y_i) = k_i\overline{v_i}$ and $(q_i, y_i, q_i) \in \lfloor \delta \rfloor^*$. Moreover, $\bar{v} \in X_P$ which yields a P-witness $w \in \tilde{A}^*$ such that $\zeta(w) = \bar{v}$. Since $q_1, \ldots, q_\ell \in P$ and w is a P-witness, we have $q \in I$ and $r \in F$ such that there exists a run from q to r labeled by w which encounters all states $q_1, \ldots, q_\ell$. Therefore, we have a permutation σ of $\{1, \ldots, \ell\}$ and $w_0, \ldots, w_\ell \in \tilde{A}^*$ such that $w = w_0 \cdots w_\ell$, $(q, w_0, q_{\sigma(1)}) \in \lfloor \delta \rfloor^*$, $(q_{\sigma(i)}, w_i, q_{\sigma(i+1)}) \in \lfloor \delta \rfloor^*$ for $1 \leq i \leq n-1$

and $(q_{\sigma(\ell)}, w_\ell, r) \in \lfloor\delta\rfloor^*$. Consider the word $w' = w_0 y_{\sigma(1)} w_1 \cdots y_{\sigma(\ell)} w_\ell$. It is clear from the definitions that $(q, w', r) \in \lfloor\delta\rfloor^*$ which yields $w' \in L(\lfloor\mathcal{A}\rfloor)$ and $\zeta(w') \in \zeta(L(\lfloor\mathcal{A}\rfloor))$. Moreover, $\zeta(w') = \zeta(w) + \zeta(y_1) + \cdots + \zeta(y_\ell) = \bar{v} + k_1\overline{v_1} + \cdots + k_\ell\overline{v_\ell} = \bar{u}$. Thus, we obtain $\bar{u} \in \zeta(L(\lfloor\mathcal{A}\rfloor))$ as desired.

We turn to the converse inclusion which is based on pumping arguments. Given a word $w \in L(\lfloor\mathcal{A}\rfloor)$, we need to prove that $\zeta(w) \in \bigcup_{P\subseteq Q} \bigcup_{\bar{v}\in X_P} \mathcal{L}(\bar{v}, V_P)$. Since $w \in L(\lfloor\mathcal{A}\rfloor)$, there exists $q \in I$ and $r \in F$ such that $(q, w, r) \in \delta^*$. We let $P \subseteq Q$ be the set of all states which are encountered in the corresponding run: w is a P-witness. We use induction on the length of w to show that there exists $\bar{v} \in X_P$ such that $\zeta(w) \in \mathcal{L}(\bar{v}, V_P)$ (which concludes the argument). There are two cases. First assume that $|w| \leq |Q|^2$. This implies $\zeta(w) \in X_P$ by definition and we have $\zeta(w) \in \mathcal{L}(\zeta(w), V_P)$, concluding this case. Assume now that $|w| > |Q|^2$. One may verify with a pumping argument that there exist $x_1, x_2 \in A^*$ and $y \in A^+$ such that $w = x_1yx_2$, the word $w' = x_1x_2$ remains a P-witness, $|y| \leq |Q|$ and $(q, y, q) \in \lfloor\delta\rfloor^*$ for some $q \in P$. Since $y \in A^+$ and $w = x_1yx_2$, we have $|w'| < |w|$. Thus, since w' is a P-witness, induction yields $\bar{v} \in X_P$ such that $\zeta(w') \in \mathcal{L}(\bar{v}, V_P)$. Moreover, since $|y| \leq |Q|$ and $(q, y, q) \in \lfloor\delta\rfloor^*$ for some $q \in P$, we have $\zeta(y) \in V_P$ by definition. Thus, $\zeta(w') + \zeta(y) \in \mathcal{L}(\bar{v}, V_P)$. Finally, since $w = x_1yx_2$ and $w' = x_1x_2$, it is clear that $\zeta(w) = \zeta(w') + \zeta(y)$. Altogether, we obtain $\zeta(w) \in \mathcal{L}(\bar{v}, V_P)$ which concludes the proof. ◀

We turn to Proposition 23. As we explained in the main text this is a corollary of a standard theorem about free abelian groups. We first introduce terminology that we need to state this theorem. Clearly, $\mathbb{Z}^n$ is a commutative group for addition (called "free abelian group of rank n"). We consider the subgroups of $\mathbb{Z}^n$ (the subsets which are closed under addition and inverses). Additionally, we need the notion of *basis*. Given a subgroup G of $\mathbb{Z}^n$, a basis of G is a finite set of vectors $\{\overline{v_1}, \ldots, \overline{v_m}\} \subseteq G$ which satisfies the two following conditions:

1. G is generated by $\{\overline{v_1}, \ldots, \overline{v_m}\}$. That is, $G = \{k_1\overline{v_1} + \cdots + k_m\overline{v_m} \mid k_1, \ldots, k_m \in \mathbb{Z}\}$.
2. For every $k_1, \ldots, k_m \in \mathbb{Z}$ such that $k_1\overline{v_1} + \cdots + k_m\overline{v_m} = 0$, we have $k_1 = \cdots = k_m = 0$.

We need the following standard theorem (see for example Theorem 1.6 in [7]).

▶ **Theorem 27.** *Let G be a nontrivial subgroup of $\mathbb{Z}^n$. There exist a basis $\{\overline{x_1}, \ldots, \overline{x_n}\}$ of $\mathbb{Z}^n$, a number $m \leq n$ and $d_1, \ldots, d_m \geq 1$ such that d_i divides d_{i+1} for every $i \leq m-1$ and $\{d_1\overline{x_1}, \ldots, d_m\overline{x_m}\}$ is a basis of G.*

We are now ready to prove Proposition 23. Let us first recall the statement.

▶ **Proposition 23.** *Let $n \geq 1$ and S a semi-linear subset of $\mathbb{Z}^n$. Assume that for every $d \geq 1$, there exists $\bar{u} \in \mathbb{Z}^n$ such that $d\bar{u} \in S$. Then, $0 \in S$.*

Proof. Observe first that we may assume without loss of generality that S is a linear subset of $\mathbb{Z}^n$. Indeed, by definition S is a *finite* union of linear subsets. Hence, by hypothesis, for every $d \geq 1$, there exists $\bar{u} \in \mathbb{Z}^n$ and a linear set S' in this union such that $d\bar{u} \in S'$. In particular, this is true when $d = h!$ for some $h \geq 1$. Hence, since the union is finite, it contains a fixed linear set S' such that there exists infinitely many d such that $d = h!$ for some $h \geq 1$ and $d\bar{u} \in S'$. It then follows that for every $d \geq 1$, there exists $\bar{u} \in \mathbb{Z}^n$ such that $d\bar{u} \in S'$. Therefore, we may replace S with S'.

We assume from now on that S is linear: we have $\bar{v} \in \mathbb{Z}^n$ and a finite set $V \subseteq \mathbb{Z}^n$ such that $S = \mathcal{L}(\bar{v}, V)$. If $V = \emptyset$ or $V = \{0\}$, we have $\mathcal{L}(\bar{v}, V) = \{\bar{v}\}$. Thus, for every $d \geq 1$, there exists $\bar{u} \in \mathbb{Z}^n$ such that $\bar{v} = d\bar{u}$. In particular, this holds for a number d which is strictly larger than the absolute values of all entries in $\bar{v}$. Clearly, this implies $\bar{v} = 0$ and we get $0 \in \mathcal{L}(\bar{v}, V)$. We now assume that V contains a non-zero vector.

Let $G \subseteq \mathbb{Z}^n$ be the subgroup of $\mathbb{Z}^n$ generated by the set $V \subseteq \mathbb{Z}^n$. By hypothesis on V, G is nontrivial. Therefore, Theorem 27 yields a basis $\{\overline{x_1}, \dots, \overline{x_n}\}$ of $\mathbb{Z}^n$, a number $m \leq n$ and $d_1, \dots, d_m \geq 1$ such that $\{d_1\overline{x_1}, \dots, d_m\overline{x_m}\}$ is a basis of G.

Since $\{\overline{x_1}, \dots, \overline{x_n}\}$ is a basis of $\mathbb{Z}^n$, we have $h_1, \dots, h_n \in \mathbb{Z}$ such that $\bar{v} = h_1\overline{x_1} + \cdots + h_n\overline{x_n}$. Let d be the least common multiplier of $|h_1|+1, \dots, |h_n|+1, d_1, \dots, d_m \geq 1$. By hypothesis, there exists $\bar{u} \in \mathbb{Z}^n$ such that $d\bar{u} \in \mathcal{L}(\bar{v}, V)$. Thus, since G is the subgroup generated by V, there exists $\bar{y} \in G$ such that $d\bar{u} = \bar{v} + \bar{y}$. Since $\{\overline{x_1}, \dots, \overline{x_n}\}$ is a basis of $\mathbb{Z}^n$, we have $k_1, \dots, k_n \in \mathbb{Z}$ such that $\bar{u} = k_1\overline{x_1} + \cdots + k_n\overline{x_n}$. Moreover, since $\{d_1\overline{x_1}, \dots, d_m\overline{x_m}\}$ is a basis of G, we have $\ell_1, \dots, \ell_m \in \mathbb{Z}$ such that $\bar{y} = \ell_1 d_1\overline{x_1} + \cdots + \ell_m d_m\overline{x_m}$. Altogether, we obtain,

$$h_1\overline{x_1} + \cdots + h_n\overline{x_n} + \ell_1 d_1\overline{x_1} + \cdots + \ell_m d_m\overline{x_m} = dk_1\overline{x_1} + \cdots + dk_n\overline{x_n}.$$

Since $\{\overline{x_1}, \dots, \overline{x_n}\}$ is a basis, this implies that for every $i > m$, we have $h_i = dk_i$. By definition $d > |h_i|$ (it is a nonzero multiple of $|h_i|+1$). Thus, $dk_i = h_i$ implies that $k_i = h_i = 0$. Since this holds for every $i > m$, we obtain

$$h_1\overline{x_1} + \cdots + h_n\overline{x_n} + \ell_1 d_1\overline{x_1} + \cdots + \ell_m d_m\overline{x_m} = dk_1\overline{x_1} + \cdots + dk_m\overline{x_m}.$$

This yields the following,

$$\bar{v} + (\ell_1 d_1 - dk_1)\overline{x_1} + \cdots + (\ell_m d_m - dk_m)\overline{x_m} = 0.$$

By definition d is a multiple of d_i for every $i \leq m$. Therefore, there exists $\ell_i' \in \mathbb{Z}$ such that $\ell_i d_i - dk_i = \ell_i' d_i$. Thus, we obtain,

$$\bar{v} + \ell_1' d_1\overline{x_1} + \cdots + \ell_m' d_m\overline{x_m} = 0.$$

Since $\{d_1\overline{x_1}, \dots, d_m\overline{x_m}\}$ is a basis of G which is the subgroup generated by V, we obtain $0 \in F(\bar{v}, V)$ which concludes the proof. ◀

Finally, it remains to prove the implication 1) ⇒ 2) in Theorem 21. This is straightforward.

Proof of 1) ⇒ 2) **in Theorem 21.** We fix $k \geq 1$ and k NFAs $\mathcal{A}_1, \dots, \mathcal{A}_k$ for the proof. We actually prove the contrapositive of 1) ⇒ 2). Assuming that there exists a vector $\bar{v} \in \bigcap_{i \leq k} \zeta(L(\lfloor \mathcal{A}_i \rfloor))$, we show that $\{L(\mathcal{A}_1), \cdots, L(\mathcal{A}_k)\}$ is *not* AMT-coverable. We write $(v_1, \dots, v_n) = \bar{v} \in \mathbb{Z}^n$ for the proof. By definition, it suffices to prove that if $\mathbf{K}$ is an arbitrary AMT-cover of A^*, then there exists $K \in \mathbf{K}$ such that $K \cap L(\mathcal{A}_j) \neq \emptyset$ for every $j \leq k$. Let $\mathbf{K} = \{K_1, \dots, K_\ell\}$. By hypothesis $K_i \in$ AMT for every $i \leq \ell$ and Lemma 4 yields a morphism $\alpha_i : A^* \to G_i$ into a finite commutative group recognizing G_i. Clearly, $G = G_1 \times \cdots \times G_\ell$ is a finite commutative group for the componentwise multiplication and the morphism $\alpha : A^* \to G$ defined by $\alpha(w) = (\alpha_1(w), \dots, \alpha_n(w))$ recognizes all languages K_i.

Let $w = (a_1)^{v_1} \cdots (a_n)^{v_n} \in \tilde{A}^*$ (note that when v_i is negative, $(a_i)^{v_i}$ is defined as $(a_i^{-1})^{|v_i|}$). Clearly, we have $\zeta(w) = \bar{v}$. Moreover, since $\bar{v} \in \bigcap_{i \leq k} \zeta(L(\lfloor \mathcal{A}_i \rfloor))$, we have $w_i \in L(\lfloor \mathcal{A}_i \rfloor)$ such that $\zeta(w_i) = \bar{v}$ for every $i \leq k$. Since G is a *commutative* group, it is straightforward to verify that this implies $\alpha(w) = \alpha(w_1) = \cdots = \alpha(w_k)$. Finally, since $\mathbf{K}$ is a cover of A^*, there exists $K \in \mathbf{K}$ such that $w_1 \in K$. Hence, since K is recognized by α and $\alpha(w_1) = \cdots = \alpha(w_k) = \alpha(w)$, it follows that $w_1, \dots, w_k \in K$. Thus, $K \cap L(\mathcal{A}_j) \neq \emptyset$ for every $j \leq k$ which completes the proof. ◀

B.3 Complexity lower bound

We prove that AMT-covering and AMT-separation are co-NP-complete. As we explained in the main text, the upper bound follows from Theorem 21. Here, we prove the lower bound: both problems are co-NP-hard. Actually since separation is a special case of covering, it suffices to show that AMT-separation is co-NP-hard. Let us start with an important remark.

▶ Remark 28. When considering complexity, it is important to distinguish the case when the alphabet is fixed from the one when it is a parameter of the problem. Here, we consider the latter case: we show that given an alphabet A and two NFAs over A, deciding whether the recognized languages are AMT-separable is co-NP-hard. Actually, when the alphabet is fixed, one may show that the problem is in P (roughly, this boils down to disjointedness of Parikh images for NFAs which is known to be in P when the alphabet is fixed [8]).

We actually show that *non* AMT-separability is NP-hard. More precisely, we present a logarithmic space reduction from 3-satisfiability (3-SAT) to this problem. Given a 3-SAT formula φ, we explain how to construct two regular languages L_1, L_2 and show that they are not AMT-separable if and only if φ is satisfiable. We only describe the construction: that NFAs for the regular languages L_1 and L_2 can be computed from φ in logarithmic space is straightforward and left to the reader.

Let $C_1, \ldots, C_k$ be the 3-clauses such that $\varphi = \bigwedge_{i \leq k} C_i$ and let $x_1, \ldots, x_n$ be the propositional variables in φ. We construct two *finite* languages L_1 and L_2 over the alphabet $A = \{x_1, \ldots, x_n, \overline{x_1}, \ldots, \overline{x_n}\}$. Intuitively, we code assignments of truth values for the variables $\{x_1, \ldots, x_n\}$ by words in A^*. Given $w \in A^*$, we say that w *is an encoding* if for all $i \leq n$, w contains either the letter x_i or the letter $\overline{x_i}$, but not both. It is immediate that an assignment of truth values for the variables $\{x_1, \ldots, x_n\}$ can be uniquely defined from any such encoding.

For every $i \leq n$, we let H_i be the language $H_i = \{x_i^p \mid 1 \leq p \leq k\} \cup \{\overline{x_i}^p \mid 1 \leq p \leq k\}$. We may now define $L_1 \subseteq A^*$. We let,

$$L_1 = H_1 H_2 \cdots H_n.$$

Clearly L_1 is finite and all the words in L_1 are encodings. We turn to the definition of L_2. For every $j \leq k$, we associate a language T_j to the 3-clause C_j. Assume that $C_j = \ell_1 \vee \ell_2 \vee \ell_3$ where $\ell_1, \ell_2, \ell_3 \in \{x_1, \overline{x_1}, \ldots, x_n, \overline{x_n}\}$ are literals. We define,

$$T_j = \{\ell_1, \ell_2, \ell_3\}.$$

Finally, we define,

$$L_2 = T_1 \cdots T_k (\{\varepsilon\} \cup H_1) \cdots (\{\varepsilon\} \cup H_n).$$

Clearly, L_2 is finite as well. Observe that the words in L_2 need not be encodings. On the other hand, all encodings within L_2 (if any) correspond to an assignment of truth values which satisfies $\{C_1, \ldots, C_k\}$.

It remains to show that L_1, L_2 are not AMT-separable if and only if the φ is satisfiable. We start with the right to left implication. Assume that there exists a truth assignment satisfying φ. By definition of L_1 and L_2, one may verify that there exists $w_1 \in L_1$ and $w_2 \in L_2$ which are both encodings of this assignment. Moreover, one may verify that we can choose w_1 and w_2 so that for every letter $a \in A$, we have $|w_1|_a = |w_2|_a$. This clearly implies that for every morphism $\alpha : A^* \to G$ into an commutative group G, we have $\alpha(w_1) = \alpha(w_2)$. Hence, in view of Lemma 4, every language $K \in \mathrm{AMT}$ which contains w_1 must contain w_2 as well. Since $w_1 \in L_1$ and $w_2 \in L_2$, it follows that L_1 and L_2 are not AMT-separable.

Conversely, assume that L_1 and L_2 are not AMT-separable. By definition, L_1 and L_2 are finite. Thus, there exists $d \in \mathbb{N}$ such that $|w| < d$ for every $w \in L_1 \cup L_2$. We consider the equivalence $\sim_d$ over A^*. By Lemma 26, every union of $\sim_d$-classes belongs to AMT. Hence, since L_1 and L_2 are not AMT-separable, there exists a $\sim_d$-class which intersects both L_1 and L_2. We obtain $w_1 \in L_1$ and $w_2 \in L_2$ such that $w_1 \sim_d w_2$: we have $|w_1|_a \equiv |w_2'|_a \bmod d$ for every $a \in A$. Moreover, since $|w_1| < d$ and $|w_2| < d$ by definition of d, this yields $|w_1|_a = |w_2|_a$ for every $a \in A$. By definition of L_1, the word $w_1 \in L_1$ encodes an assignment of truth values. Moreover, since $|w_1|_a = |w_2|_a$ for every $a \in A$, the word w_2 encodes the same assignment of truth values. Finally, since $w_2 \in L_2$, this assignment satisfies φ which completes the proof.

C Appendix: Modulo testable languages

This appendix is devoted to the class MOD of modulo languages. We present the missing proofs for the statements in the main paper and look more closely at the complexity of MOD-separation.

C.1 Proof of Lemma 3

Let us first recall the statement of Lemma 3.

▶ **Lemma 3.** *Let $L \subseteq A^*$. Then, $L \in$ MOD if and only if L is recognized by a morphism $\alpha : A^* \to G$ into a finite group G such that $\alpha(a) = \alpha(b)$ for all $a, b \in A$.*

Proof. Assume first that $L \in$ MOD. We show that L is recognized by a morphism $\alpha : A^* \to G$ into a finite group G such that $\alpha(a) = \alpha(b)$ for every $a, b \in A$. By definition of MOD, it suffices to prove that this property is true for all basic languages $L_{q,r}$ and that it is preserved by union. We first look at the language $L_{q,r} = \{w \in A^* \mid |w| \equiv r \bmod q\}$ for $q, r \in \mathbb{N}$ such that $r < q$. Clearly, $L_{q,r}$ is recognized by the morphism $\alpha : A^* \to \mathbb{Z}/q\mathbb{Z}$ defined by $\alpha(a) = 1$ for every $a \in A$ (where $\mathbb{Z}/q\mathbb{Z} = \{0, \dots, q-1\}$ is the standard cyclic group): we have $L_{q,r} = \alpha^{-1}(r)$. Now, let $L_1, L_2 \subseteq A^*$ such that for $i = 1, 2$, L_i is recognized by a morphism $\alpha_i : A^* \to G_i$ into a finite group G_i such that $\alpha_i(a) = \alpha_i(b)$ for all $a, b \in A$. Clearly, $L_1 \cup L_2$ is recognized by the morphism $\alpha : A^* \to G_1 \to G_2$ (where $G_1 \times G_2$ is the group equipped with the componentwise multiplication). This completes the proof for this direction.

We now assume that L is recognized by a morphism $\alpha : A^* \to G$ into a finite group G such that $\alpha(a) = \alpha(b)$ for every $a, b \in A$. We show that $L \in$ MOD. By hypothesis, there exists $s \in M$ such that $\alpha(a) = s$ for all $a \in A$. Since G is a *finite* group, it is standard that there exists $q \geq 1$ such that $s^q = 1_G$. We prove that L is a finite union of languages $L_{r,q}$ for r such that $0 \leq r < q$. This implies that $L \in$ MOD, as desired. Since α is recognized by α, it suffices to prove that for all r such that $0 \leq r < q$, if $w, w' \in L_{r,q}$, then $\alpha(w) = \alpha(w')$. We fix r for the proof and show that for every $w \in L_{r,q}$, we have $\alpha(w) = s^r$. By hypothesis, there exists $k \in \mathbb{N}$ such that $|w| = kq + r$. Hence, since all letters have image s under α by hypothesis, we get $\alpha(w) = s^{kq}s^r$. Moreover, we have $s^{kq} = 1_G$ by definition of q. Altogether, this yields $\alpha(w) = s^r$, which concludes the proof. ◀

C.2 Complexity of MOD-separation

We prove that MOD-separation is in NL. Theorem 25 presents a logarithmic space reduction from MOD-separation to GR-separation for languages over *unary alphabets*. Hence, it suffices to prove that the latter problem is in NL. We fix an alphabet $A = \{a\}$ containing a single

letter "a" and prove that given as input two NFAs $\mathcal{A}_1$ and $\mathcal{A}_2$ over A, one may decide in NL whether $L(\mathcal{A}_1)$ is *not* GR-separable from $L(\mathcal{A}_2)$. Since NL = co-NL by the Immerman-Szelepcsényi theorem, this implies as desired that GR-separation is in NL for languages over unary alphabets. By Theorem 9, the two following conditions are equivalent:

1. $L(\mathcal{A}_1)$ is not GR-separable from $L(\mathcal{A}_2)$.
2. $L(\lfloor \mathcal{A}_1 \rfloor_\varepsilon) \cap L(\lfloor \mathcal{A}_2 \rfloor_\varepsilon) \neq \emptyset$.

Therefore, we have to prove that the second condition can be decided in NL. For $j = 1, 2$, we write $\mathcal{A}_j = (Q_j, I_j, F_j, \delta_j)$. By definition, $\lfloor \mathcal{A}_j \rfloor_\varepsilon$ is built from $\mathcal{A}_j$ by adding new transitions labeled by a^{-1} (this is the construction of $\lfloor \mathcal{A}_j \rfloor = (Q_j, I_j, F_j, \lfloor \delta_j \rfloor)$ from $\mathcal{A}_j$) and ε-transitions (this is the construction of $\lfloor \mathcal{A}_j \rfloor_\varepsilon = (Q_j, I_j, F_j, \lfloor \delta_j \rfloor_\varepsilon)$ from $\lfloor \mathcal{A}_j \rfloor$). It is standard that if we have $\lfloor \mathcal{A}_1 \rfloor_\varepsilon$ and $\lfloor \mathcal{A}_2 \rfloor_\varepsilon$ in hand, deciding whether $L(\lfloor \mathcal{A}_1 \rfloor_\varepsilon) \cap L(\lfloor \mathcal{A}_2 \rfloor_\varepsilon) \neq \emptyset$ can be achieved in NL since this boils down to graph reachability (in the product of $\mathcal{A}_1$ and $\mathcal{A}_2$ whose set of states is $Q_1 \times Q_2$). Therefore, we have to prove that one may decide whether a given transition belongs to $\lfloor \delta_1 \rfloor_\varepsilon$ or $\lfloor \delta_2 \rfloor_\varepsilon$ in NL.

This is immediate for the transitions labeled by $a \in A$ as they already belong to δ_1 and δ_2. Let us now consider the transitions labeled by $a^{-1} \in A^{-1}$ which belong to $\lfloor \delta_1 \rfloor$ and $\lfloor \delta_2 \rfloor$. By definition, for $j = 1, 2$, and $q, r \in Q_j$, we have $(r, a^{-1}, q) \in \lfloor \delta_j \rfloor$ if and only if $(q, a, r) \in \delta_j$ and q, r are strongly connected. Clearly, this can be checked in NL since testing whether q, r are strongly connected boils down to a graph reachability problem (which is in NL). It remains to consider the ε-transitions in $\lfloor \delta_1 \rfloor_\varepsilon$ and $\lfloor \delta_2 \rfloor_\varepsilon$. We treat this case in the following lemma (this is where we use the hypothesis that the alphabet is unary).

▶ **Lemma 29.** *Let $j \in \{1, 2\}$ and $q, r \in Q_j$, one may decide in* NL *whether $(q, \varepsilon, r) \in \lfloor \delta_j \rfloor_\varepsilon$.*

Proof. By definition, we have $(q, \varepsilon, r) \in \lfloor \delta_j \rfloor_\varepsilon$ if and only if there exists $w \in \tilde{A}^*$ such that $w \in L_\varepsilon \subseteq \tilde{A}^*$ such that $(q, w, r) \in \lfloor \delta_j \rfloor^*$. Observe that since $A = \{a\}$, we have $L_\varepsilon = \{w \in \tilde{A}^* \mid |w|_a = |w|_{a^{-1}}\}$. We use this property to prove that deciding whether $(q, \varepsilon, r) \in \lfloor \delta_j \rfloor_\varepsilon$ boils down to a graph reachability problem that can be decided in NL.

We let $U = Q_j \times \mathbb{Z}$ be a set of vertices and write $V = \{(q, k) \in U \mid |k| \leq |Q_j|^2\}$. We consider the following set of edges:

$$E = \{((q, k), (q', k + 1)) \mid (q, a, q') \in \lfloor \delta_j \rfloor\} \cup \{((q, k), (q', k - 1)) \mid (q, a^{-1}, q') \in \lfloor \delta_j \rfloor\}.$$

Consider the graph $G = (U, E)$. One may verify from the definitions that $(q, \varepsilon, r) \in \lfloor \delta_j \rfloor_\varepsilon$, if and only if there exists a path from $(q, 0)$ to $(r, 0)$ in G. Hence, it suffices to prove that the latter condition can be checked in NL. We show that there exists a path $(q, 0)$ to $(r, 0)$ in G if and only if there exists a path from $(q, 0)$ to $(r, 0)$ in G using only states in V. It is then straightforward to verify that this can can be tested in NL (this is a graph reachability problem over a graph with $|V| = |Q_j| \times (2|Q_j| + 1)$ vertices whose edges can be computed from $\mathcal{A}_j$ in NL).

The right to left implication is immediate. For the converse one, we consider a path from $(q, 0)$ to $(r, 0)$ in G. We prove that if this path contains a vertex in $U \setminus V$, then there exists a strictly shorter path from $(q, 0)$ to $(r, 0)$. One may then iterate the result to build a path which only contains states in V, completing the proof. Let $(s_0, k_0), \ldots, (s_n, k_n) \in U$ be the vertices along our path: we have $(s_0, k_0) = (q, 0)$, $(s_n, k_n) = (r, 0)$, and for every $i \leq n$, we have $((s_i, k_i), (s_{i+1}, k_{i+1})) \in E$. Moreover, we know that there exits some index $h \leq n$ such that $(s_h, k_h) \notin V$, *i.e.* such that $|k_h| > |Q_j|^2$. By symmetry, we assume that $k_h > |Q_j|^2$ and leave the case $k_h < |Q_j|^2$ to the reader. We write $m = k_h$ for the proof. By definition of E and since $k_0 = k_m = 0$, there exists $0 < i_1 < \cdots < i_{m-1} < h < i'_{m-1} < \cdots < i'_1 < n$ such that $k_{i_1} = k_{i'_1} = 1, \ldots, k_{i_{m-1}} = k_{i'_{m-1}} = m - 1$. We also write $i_0 = 0$ and $i'_0 = n$. By

hypothesis, we have $k_{i_0} = k_{i'_0} = 0$. Since $m > |Q_j|^2$, it now follows from the pigeon-hole principle that there exists $0 \leq \ell_1 < \ell_2 \leq m-1$ such that $s_{i_{\ell_1}} = s_{i_{\ell_2}}$ and $s_{i'_{\ell_1}} = s_{i'_{\ell_2}}$. Let $\ell = \ell_1 = \ell_2$. One may verify from the definition of E that the following paths exist in G:

$$(s_0, k_0) \to \cdots \to (s_{i_{\ell_1}}, k_{i_{\ell_1}}) \to (s_{i_{\ell_2+1}}, k_{i_{\ell_2+1}} - \ell) \to \cdots \to (s_h, k_h - \ell).$$
$$(s_h, k_h - \ell) \to \cdots \to (s_{i'_{\ell_2-1}}, k_{i'_{\ell_2-1}} - \ell) \to (s_{i'_{\ell_1}}, k_{i'_{\ell_1}}) \to \cdots \to (s_n, k_n).$$

Altogether, we get a strictly shorter path from $(q, 0)$ to $(r, 0)$ which completes the proof. ◀