Minimization of semilinear automata

Mikoaj Bojaczyk and Sawomir Lasota

University of Warsaw

Abstract. We investigate finite deterministic automata in sets with non-homogeneous atoms: integers with successor. As there are uncountably many deterministic finite automata in this setting, we restrict our attention to automata with semilinear transition function. The main results is a minimization procedure for semilinear automata. The proof is subtle and refers to decidability of existential Presburger arithmetic with divisibility predicates. Interestingly, the minimization is not obtained by the standard partition refinement procedure, and we demonstrate that this procedure does not necessarily terminate for semilinear automata.

1 Introduction

This paper is a successor of a line of research aiming at studying models of computation in a new set theory, namy in *sets with atoms* (for motivation and a more detailed exposition see for instance [3, 5, 4]).

In set theory, elements of sets are other sets, organized in a well-founded way. In this paper we work in a new set theory, where one additionally postulates an infinite set of *atoms*. Then elements of sets are either other sets, or atoms, while atoms themselves have not elements. Examples of atoms that are often considered are *equality atoms* $(\mathbb{N}, =)$, i.e., natural numbers with equality, or *total order atoms* $(\mathbb{Q}, \leq)$, i.e., rational number with the natural order. In this paper we focus on *integer atoms*

$$(\mathbb{Z}, +1),$$

i.e., the integers with the successor function.

In general, atoms are an algebraic structure over some vocabulary. The structure is typically assumed to be *homogeneous* [12], i.e., to satisfy the following condition: every isomorphism between finite substructures extends to an automorphism of the whole structure. Sets with atoms have particularly good properties when atoms are a relational homogeneous structure over a finite vocabulary. Examples are the equality atoms or the total order atoms, but not the integer atoms.[1]

Sets with atoms were discovered in the 20ies by Fraenkel, and then investigated by Mostowski and others. In 90ies, sets with atoms have been rediscovered

[1] Integer atoms are homogeneous if one weakens the definition: only isomorphisms between *finitetely generated* substructures extend to the whole structure.

in semantics [10, 9]. The paper [3] rediscovers sets with atoms in automata theory and observes that one can naturally study different models of computation in the new set theory. The principal difference is that the notion of finiteness in sets with atoms is replaced by a more liberal notion of *orbit-finiteness*. This approach allows to capture in an elegant syntax-independent way some models of automata, for instance finite memory automata of Francez and Kaminski [8], or timed automata of Alur and Dill [2]. The paper [3] proves also the analog of Myhill-Nerode theorem for orbit-finite automata. The minimization is effective due to a powerful finite representation theorem provided in the paper. However, the representation theorem holds only when atoms are a homogeneous relational structure over a finite vocabulary.

Contribution of the paper. The present paper is a natural attempt to extend the above-mentioned results to non-homogeneous atoms. We investigate sets with atoms $(\mathbb{Z}, +1)$ and orbit-finite automata therein. However, the finite representation theorem of [3] is not applicable any more, and as one of the consequences the automaton model is far too powerful. In particular, there is uncountably many non-equivalent orbit-finite automata in sets with the integer atoms, thus the automata may not be finitely presented as an input to a procedure. This indicates a necessity of a reasonable restriction of the power of automata. Our restriction applies to transition relation of an automaton and requires this relation to be semilinear.

It turns out the under the restriction, the deterministic orbit-finite automata with the integer atoms admit a minimization procedure. This is the main result of this paper. The proof is a surprisingly subtle and complicated reduction to satisfiability of existential Presburger arithmetic with divisibility. The latter problem was shown decidable in [11].

Related research. The integer atoms exhibit significant similarity to the *timed atoms*, i.e., the structure

$$(\mathbb{Q}, <, +1).^{2}$$

In [5] orbit-finite automata with the timed atoms have been shown to subsume timed automata [2]. Moreover, effective minimization has been shown for a subclass of automata rich enough to subsume timed automata: automata with timed atoms, with transition relation definable in $\mathrm{FO}(\mathbb{Q}, <, +1)$ without quantifiers. This amounts to a more severe restriction than the semilinear restriction considered in this paper. In fact we suppose that techniques similar to those used in this paper would also apply to semilinear automata with timed atoms.

Other approaches to minimization of timed automata are discussed in [1, 14, 16, 15].

An extension of the representation theorem to non-homogeneous atoms has been recently formulated proved in [13]. It applies both to the integer atoms and to the timed atoms.

[2] Instead of $(\mathbb{Q}, <, +1)$, equally-well one could consider atoms $(\mathbb{R}, <, +)$.

2 Preliminaries

Sets with atoms. The set of atoms is assumed to come equipped with some algebraic structure, like the rationals $\mathbb{Q}$ with the natural order. The notion of *sets with atoms* makes sense for any algebraic structure of atoms. We fix in this section an arbitrary such structure, even if later on we will stick to the particular structure $(\mathbb{Z}, +1)$, the integers with successor.

The *cumulative hierarchy* of sets is a sequence of sets indexed by ordinal ranks. At any ordinal, sets of this rank are arbitrary sets whose elements are sets of smaller rank, or atoms. In particular, sets of rank 0 are all subsets of atoms. We restrict to only those sets in the cumulative hierarchy that are well-behaved in the sense described below.

The intuitive idea is that the given algebraic structure is the only relevant structure of atoms, thus we work 'up to automorphism of atoms'. Formally, given an automorphism π of atoms, i.e., a bijection that preserves the algebraic structure, π may be naturally lifted to any set in the cumulative hierarchy: apply π to all elements, then to all elements of elements, etc. Application of π to a set X we denote by $X \cdot \pi$. A set S of atoms is said to *support* a set x if every automorphism π being identity on S preserves x as well: $X \cdot \pi = X$. All atoms trivially support any set. As an example, consider the equality atoms and the set x of all atoms except 3 and 5, which is supported by $\{3, 5\}$. If we move to the total order atoms, the set $\{3, 5\}$ supports also the open interval $(3, 5)$. In the sequel we are interested in finitely-supported sets, i.e., those supported by some finite set of atoms.

Now we are prepared to define well-behaved sets: a set in cumulative hierarchy is *hereditarily finitely-supported* if it is finitely-supported itself, all its elements are finitely-supported, etc. A hereditarily finitely-supported set that is itself supported by the empty set of atoms we call *equivariant.* A particular but important special case is that of *equivariant function*, i.e., a function $f : X \to Y$ between two sets that commutes with any automorphism π of atoms:

$$f(x \cdot \pi) = f(x) \cdot \pi \qquad \text{for all } x \in X \text{ and all automorphisms } \pi.$$

The new set theory has a more liberal notion of finiteness than the usual one: orbit-finiteness. For a set S of atoms, the S*-orbit* of a set x is defined as follows:

$$\{x \cdot \pi : \pi \text{ is an automorphism of atoms being identity on } S\}.$$

If S is finite, the above set is called *single-orbit.* A set is orbit-finite if it is the union of finitely-many single-orbit sets. Note however that the precise number of orbits of a set may vary depending on the choice of S.

Sets with atoms have particularly good properties if the atoms are a *homogeneous* relational structure over a finite vocabulary [12]. Examples are equality atoms, total order atoms, or the random graph considered as a relational structure. One of these good properties is preservation of orbit-finiteness by the Cartesian product. In consequence, an n-ary relation between orbit-finite sets is orbit-finite as well.

Sets with integer atoms. From now on we only consider integer atoms; the automorphism group contains all translations $x \mapsto x + z$, for some $z \in \mathbb{Z}$ and is thus isomorphic to $\mathbb{Z}$ with addition. This choice of atoms leads to a slightly pathological set theory. As an example, observe that every set is supported by any singleton $\{z\} \subseteq \mathbb{Z}$ as the translation with a fixed point is necessarily the identity. Thus all sets are in the cumulative hierarchy are hereditarily finitely-supported. This is why we will mostly work with equivariant sets in the sequel.

The structure $(\mathbb{Z}, +1)$ is not homogeneous as a relational structure; in fact there is no extension of the structure by a finite set of relations that would make the structure homogeneous. It is thus not surprising that integer atoms lead to a set theory that lacks certain important properties. One of the most important problems is that orbit-finiteness is not preserved by the Cartesian product. For instance, the atoms $\mathbb{Z}$ is a single-orbit set, but the product $\mathbb{Z} \times \mathbb{Z}$ has infinitely many orbits, namely for each $k \in \mathbb{Z}$, the diagonal $\{(i, i + k) : i \in \mathbb{Z}\}$ is an orbit. One of the consequences is that there are uncountably many equivariant binary relations in $\mathbb{Z}$.

By an equivariant isomorphism we mean a bijection between two sets that commutes with automorphisms of atoms. For $k \geq 0$, let $\mathbb{Z}_k$ denote integers modulo k, i.e., the set of equivalence classes of the congruence modulo k. In particular $\mathbb{Z}_0$ is the same as $\mathbb{Z}$ up to equivariant isomorphism. From the representation theorem of [13] it follows that single-orbit sets with integer atoms are particularly simple:

Lemma 1. *Up to equivariant isomorphism, every one-orbit set with integer atoms is $\mathbb{Z}_k$ for some $k \geq 0$.*

Automata with integer atoms. For any atoms, one can naturally define nondeterministic and deterministic finite automata. For instance, a NFA consists of:

- an orbit-finite alphabet A,
- an orbit-finite set Q of states,
- a transition relation $\delta \subseteq Q \times A \times Q$,
- subsets $I, F \subseteq Q$ of initial and accepting states.

All sets above are implicitly assumed to be hereditarily finitely-supported. A DFA is obtained by additionally restricting the set I to be a singleton and the relation δ to be a function $Q \times A \to Q$. Note that a NFA is equivariant iff all its components A, Q, I, F and δ are so.

For many choices of atoms, in particular for homogeneous atoms, the notion of automaton outlined above is very reasonable. For instance, if the alphabet is just the set of atoms, equivariant NFA with equality atoms are expressively equivalent to the finite memory automata of Francez and Kaminski [8] (called also register automata [6]). Similarly, in case of total order atoms, equivariant NFA correspond to a variant of finite memory automata with order testing (cf. e.g. [7]).

Unfortunately, automata with integer atoms are far too powerful, as illustrated in the example below.

Example 1. Suppose that $K \subseteq \mathbb{Z}$ is any set of integers, e.g. the positive integers that are prime numbers. Consider the following language

$$\mathrm{diff}(K) = \{x_1 \dots x_n \in \mathbb{Z}^* : \text{ for all } i \in \{2, \dots, n\},\ x_i - x_{i-1} \in K\}.$$

We claim that this language is recognized by an equivariant DFA with integer atoms. The automaton has: an initial state ϵ, a sink error state $\perp$, as well as one state z for every $z \in \mathbb{Z}$. It is easy to see that there are three orbits. The transition function is

$$\begin{aligned} \delta(\epsilon, y) &= y \\ \delta(z, y) &= \begin{cases} y & \text{if } y - z \in K \\ \perp & \text{otherwise} \end{cases} \\ \delta(\perp, y) &= \perp \end{aligned}$$

Of course, this is not a true finite automaton, because it refers to the set K in its transition relation, and the set K could be anything, e.g. undecidable. Note that there are uncountably many sets K, and each one gives a different language.

This is why starting from Section 3 on we restrict our attention to *semilinear* automata.

3 Semilinear sets with integer atoms

A problem with the integer atoms is that the Cartesian product does not preserve orbit-finiteness. To overcome this difficulty we widen our interest from orbit-finite sets to polynomial sets, defined below.

Polynomial sets. For any atoms, one may use the name *polynomial sets* for the smallest class of sets that contains all equivariant orbit-finite sets and is closed under finite products and disjoint unions. Thus a polynomial set is a finite disjoint union of *monomial sets*, i.e., of finite products of equivariant one-orbit sets.

Under the integer atoms, by Lemma 1 every monomial set is, up to equivariant isomorphism, of the form

$$\mathbb{Z}_{k_1} \times \mathbb{Z}_{k_2} \times \cdots \times \mathbb{Z}_{k_n} \qquad \text{where } k_1, \dots, k_n \in \mathbb{N}. \tag{1}$$

Without loss of generality we only consider monomials of the form $\mathbb{Z}^k$ or $\mathbb{Z}_k$:

Lemma 2. *Every polynomial set is isomorphic to a finite disjoint union of monomials of the form $\mathbb{Z}^k$ or $\mathbb{Z}_k$, for $k \in \mathbb{N}$.*

Proof. Using Lemma 1 and the following identities:

- for $k \geq 1$ there is an equivariant isomorphism between $\mathbb{Z}_k \times \mathbb{Z}$ and the disjoint union of k copies of $\mathbb{Z}$;

- for $k, l \geq 1$ there is an equivariant isomorphism between $\mathbb{Z}_k \times \mathbb{Z}_l$ and $\mathbb{Z}_m$, where m is the least common multiplicity of k and l.

□

Semilinear sets with integer atoms. As we have remarked above, the set $\mathbb{Z}^2$, when seen as a set with integer atoms, is isomorphic to a disjoint union of a countably infinite number of copies of $\mathbb{Z}$. As a consequence, there are uncountably many equivariant subsets of $\mathbb{Z}^2$: just choose any subset of the infinitely many orbits. This means that there is no hope of algorithms working with arbitrary equivariant subsets of the monomial $\mathbb{Z}^2$. This motivates us to restrict to subsets of polynomial sets that are not just equivariant, but also semilinear, as defined below.

The standard notion of semilinear sets applies to subsets of monomials of the form $\mathbb{Z}^k$. For monomials of the form $\mathbb{Z}_k$, every subset is considered to be semilinear. Then we extend definition to all monomials of the form:

$$\mathbb{Z}_{k_1} \times \mathbb{Z}_{k_2} \times \cdots \times \mathbb{Z}_{k_n} \qquad \text{where } k_1, \ldots, k_n \in \mathbb{N};$$

a subset of such set is semilinear if it is semilinear when translated along the isomorphism used in the proof of Lemma 2. The property does not depend on the choice of an isomorphism.

Definition 1 (Semilinear sets with integer atoms). *Consider a subset*

$$R \subseteq X_1 \times \ldots \times X_n$$

of an arbitrary equivariant monomial set. R is semilinear if for some n-tuple of equivariant isomorphisms

$$(f_i : X_i \to \mathbb{Z}_{k_i})_{i=1\ldots n}, \qquad \textit{where } k_1, \ldots, k_n \in \mathbb{N},$$

the image of R along the isomorphisms is a semilinear subset of the set

$$\mathbb{Z}_{k_1} \times \mathbb{Z}_{k_2} \times \cdots \times \mathbb{Z}_{k_n}$$

in the sense described above.

Finally, a semilinear subset of a polynomial set is defined by choosing a semilinear subset of each of its monomials.

Note certain delicacy of the above definition. Observe that $\mathbb{Z}^3$, when interpreted as a set with integer atoms, is, similarly like $\mathbb{Z}^2$, isomorphic to a countable disjoint union of copies of $\mathbb{Z}$. Therefore there is an equivariant isomorphism between $\mathbb{Z}^2$ and $\mathbb{Z}^3$; consider for instance any bijection between orbits. However, a semilinear subset of $\mathbb{Z}^2$, translated to $\mathbb{Z}^3$ via an equivariant isomorphism, is not a semilinear subset of $\mathbb{Z}^3$ in general.

Definition 1 immediately yields the notion of a semilinear n-ary relation on orbit-finite sets. Also as a special case, we get the notion of a semilinear function between polynomial sets.

We are interested in subsets of polynomial sets (which covers the case of relations and functions) which are both semilinear and equivariant. For instance, there is no semilinear and equivariant bijection between $\mathbb{Z}^2$ and $\mathbb{Z}^3$.

We conclude this section with the following observations useful later:

Lemma 3. *Every orbit-finite subset of a polynomial set is semilinear.*

Corollary 1. *Every equivariant function between single-orbit sets is semilinear.*

4 Semilinear automata and their decision problems

Consider the integer atoms. A NFA is called *semilinear* if its transition relation is semilinear.

Representation. In this section, we study semilinear automata and their decision problems. To speak of decision problems, we should first explain how a semilinear automaton is presented as the input to an algorithm. A finite representation of such automata is easily deducible from our knowledge collected by now. Basing on Lemma 1, we assume that every orbit is literrally $\mathbb{Z}_k$, and thus may be represented by the number k. An orbit-finite set is represented as a multiset of orbits. Transition relation of a semilinear automaton is represented separately for every monomial set.

We start with the observation that we must restrict ourselves to equivariant automata only, as non-equivariant automata have undecidable emptiness, even in deterministic case:

Theorem 1. *Emptiness is undecidable for semilinear DFA with the integer atoms.*

Proof. Recall that every set is finitely supported, namely supported by every singleton subset of atoms. In consequence, the transition function $\delta : Q \times A \to Q$ of a semilinear automaton may be an arbitrary semilinear function. We claim that DFAs with semilinear transition function may simulate deterministic two-counter machines.

Consider a deterministic two-counter machine with zero tests, which has n states. A configuration of this machine can be seen as an element of

$$\{0, \ldots, n-1\} \times \mathbb{N} \times \mathbb{N}.$$

Denote by *succ* the function which maps a configuration to its successor. It is well known that the following question is undecidable:

Given x and y, decide if there is some m such that $y = succ^m(x)$?

This question is undecidable even for a fixed machine, and of course also undecidable when the machine is part of the input. Consider a Gödel coding of configurations as numbers defined by

$$f(i, j, k) = n \cdot (2^j \cdot 3^k) + i.$$

Under this coding, the successor function is semilinar. More precisely, there is a semilinear function $g : \mathbb{Z} \to \mathbb{Z}$ such that for every configuration $x = (i, j, k)$,

$$f(succ(x)) = g(f(x)).$$

Therefore, it is undecidable if there is some m such that $g^m(f(x)) = f(y)$.

Define a semilinear DFA, with a singleton input alphabet, as follows. Its states are $\mathbb{Z}$, the initial and accepting states are $f(x)$ and $f(y)$, and the transition function updates state n to $g(n)$ ignoring input. The automaton is nonempty if and only if the two-counter machine halts. Thus emptiness of semilinear DFA is undecidable. □

Somehow surprisingly, equivariance of transition relation makes emptiness easily decidable:

Theorem 2. *Emptiness is decidable for semilinear equivariant NFA with the integer atoms.*

Proof. Consider an automaton, with input alphabet A, states Q, initial states $I \subseteq Q$, accepting states F, and transition relation $\delta \subseteq Q \times A \times Q$. Consider the sets

$$Q_0 \overset{\text{def}}{=} I \qquad \text{and} \qquad Q_n \overset{\text{def}}{=} Q_{n-1} \cup \delta(Q_{n-1}, A) \subseteq Q \text{ for } n \geq 1.$$

It is easy to see that Q_n is the set of states that can be reached after reading an input of length at most n, and that Q_n can be computed based on Q_{n-1} using Presburger arithmetic. Since the set Q_n is an equivariant subset of Q, there are finitely many possibilities for Q_n, and therefore the chain $Q_0 \subseteq Q_1 \subseteq \cdots$ must stabilize at some point. If it stabilizes without containing an accepting state, the automaton is empty, otherwise the automaton is nonempty. □

The above theorem makes semilinear equivariant NFA look deceptively simple. The following result illustrates that even in the deterministic case, semilinear equivariant automata are dangerously close to undecidability. We use below a term *constant word* for any word of the form x^n, for some $x \in \mathbb{Z}$ and $n \geq 0$.

Theorem 3. *The following problem is undecidable:*

- **Input.** *A semilinear equivariant DFA with the integer atoms, with input alphabet $\mathbb{Z}$.*
- **Question.** *Does the automaton accept some constant word?*

Proof. By reduction of the halting problem for two-counter machines. We will use the same notation as in the proof of Theorem 1. In particular we will make use of the Gödel encoding f of configurations of a two-counter machine with zero tests and of the semilinear function $g : \mathbb{Z} \to \mathbb{Z}$ that encodes the transition function of the machine.

Given a machine, define a semilinear equivariant automaton, with input alphabet $\mathbb{Z}$, as follows. Its states are

$$\mathbb{Z} \cup \{\epsilon, \top, \bot\},$$

where ϵ, $\top$ and $\bot$ have singleton orbits. The initial state is ϵ, and the only accepting state is $\top$. For the initial state, the transition function is defined by

$$\delta(\epsilon, i) = f(x) + i \in \mathbb{Z}.$$

For a state $i \in \mathbb{Z}$, the transition function is defined by

$$\delta(i, j) = \begin{cases} \top & \text{if } g(i-j) = f(y) \\ j + g(i-j) & \text{otherwise} \end{cases}$$

The state $\top$ leads to $\bot$ on every input, and $\bot$ is a sink state:

$$\delta(\top, i) = \bot \qquad \delta(\bot, i) = \bot.$$

It is not difficult to see that δ is equivariant, and that an input of the form 0^m is accepted if and only if the two-counter machine goes from configuration x to configuration y in exactly m steps. An equivariant automaton accepts a constant word if and only if it accepts a word 0^m for some m. This completes the proof. □

Corollary 2. *It is undecidable if two semilinear equivariant DFA have nonempty intersection.*

Proof. The language of all constant words is easily seen to be recognized by a semilinear equivariant DFA. □

Observe how the delicacy of the decidability border between Theorem 2 and Theorem 3. Consider a semilinear equivariant DFA with states Q. For $n \in \mathbb{N}$, define $P_n \subseteq Q$ to be the set of states that can be reached after reading a constant word of length n. It is not difficult to see that P_n is an equivariant subset of Q, and therefore there are finitely many possibilities for P_n. However, by Theorem 3, it is undecidable if there is some n such that P_n contains an accepting state.

5 Minimizing semilinear equivariant automata

In this section we turn to the problem of minimizing DFAs. For any choice of atoms, in particular for the integer atoms, every DFA has an equivalent minimal DFA. We start by proving that when one starts with a semilinear equivariant DFA, the minimization operation stays in the realm of semilinear DFAs.

Theorem 4. *If a language $L \subseteq A^*$ is recognized by a semilinear equivariant DFA with the integer atoms then its minimal automaton is also a semilinear equivariant DFA.*

Proof. Let $\mathcal{A}$ be a semilinear equivariant DFA recognizing L. Let Q be the state space of $\mathcal{A}$ and let P be the state space of the syntactic automaton, which is always equivariant. Let $f : Q \to P$ be the mimimizing function, again always equivariant. By Corollary 1 we know that f is semilinear. Let $\delta : Q \times A \to Q$ be the transition function of the automaton $\mathcal{A}$, which is semilinear by assumption. Our goal is to show that the transition function $\gamma : P \times A \to P$ of the syntactic automaton is semilinear. The function γ is the same as the relation

$$\{(f(q), a, f(\delta(q, a))) : q \in Q, a \in A\},$$

which can be easily seen to be semilinear, assuming that δ and f are. □

The theorem, however, says nothing about computing the minimal automaton. It even says nothing about deciding if an automaton is already minimal.

Proposition 1. *As far as decidability is concerned, deciding minimality is equivalent to computing the minimal automaton.*

Proof. Suppose that one can decide if an automaton is minimal. We show how to compute the minimal automaton. The algorithm runs two nested loops.

- In the outer loop, we input a semilinear automaton $\mathcal{A}$ with states. First, we test if $\mathcal{A}$ is already minimal. If yes, the algorithm terminates and outputs $\mathcal{A}$. Otherwise, the algorithm enters the inner loop.
- In the inner loop, the algorithm searches through all equivariant functions $f : Q \to P$, and tests each one to see if it is an automaton homomorphism, which can be expressed in Presburger arithmetic. Under the assumption that $\mathcal{A}$ is not minimal, the inner loop finds some homomorphism f which is not a bijection. Upon finding such a homomorphism, the inner loop terminates, and the outer loop is executed again.

We claim that the outer loop can only be executed finitely many times. This is because the order

$$X > Y \qquad \text{if there is a surjective, non bijective, equivariant function } f : X \to Y$$

is well founded. The reason is that a non-bijective equivariant function must either decrease the number of orbits, or decrease the characteristic of some orbit. By a characteristic of $\mathbb{Z}_k$ we mean here the number k. Observe that the order does admit arbitrarily long decreasing chains with the same starting point, e.g.

$$\mathbb{Z} > \mathbb{Z}_{2^k} > \mathbb{Z}_{2^{k-1}} > \cdots > \mathbb{Z}_2 > \mathbb{Z}_1 \qquad \text{for any } k \in \mathbb{N}.$$

□

5.1 Partition refinement fails

One natural approach to minimization problem would be to use a partition refinement algorithm, described below.

Consider semilinear equivariant DFA $\mathcal{A}$, with states Q. For $n \in \mathbb{N}$, define an equivalence relation $\sim_n$ on Q, which identifies two states if they accept the same inputs of length at most n. It is not difficult to see that $\sim_n$ is a semilinear relation, because its definition can be expressed in Presburger arithmetic. Also, $\sim_n$ is an equivariant equivalence relation on Q, which means that there is an orbit-finite quotient $Q/_{\sim_n}$. Suppose that these equivalences stabilize at some $n \in \mathbb{N}$, which means that the equivalence relations $\sim_n$ and $\sim_{n+1}$ are the same. Then it is not difficult to prove that $\sim_n$ is the Myhill-Nerode equivalence on states of the automaton, and the minimal automaton has states $Q/_{\sim_n}$.

Unfortunately, the equivalence might never stabilize:

Proposition 2. *There is a semilinear equivariant DFA, such that equivalences $\sim_n$ never stabilize.*

Proposition 2 is shown using an automaton such that for every $n \in \mathbb{N}$, the set $Q/_{\sim_n}$ has three orbits, with characteristics $1, 1$ and 2^n respectively.

Proof. Consider an input alphabet

$$A = \{\mathit{start}, \underline{0}, \underline{1}\} \times \mathbb{Z}.$$

Consider an automaton defined as follows. Its state space is:

$$Q = \mathbb{Z} \uplus \{\epsilon, \bot\}.$$

The initial state is ϵ. The orbit $\mathbb{Z}$ is accepting, while the orbits $\{\epsilon\}$ and $\{\bot\}$ are rejecting. The transition function is defined below, for $i, j \in \mathbb{Z}$. When reading the definition below it is a good idea to look at the case $j = 0$.

$$\delta(\epsilon, (\sigma, i)) = \begin{cases} i & \text{when } \sigma = \mathit{start} \\ \bot & \text{otherwise} \end{cases}$$

$$\delta(i, (\sigma, j)) = \begin{cases} \frac{i-j-\sigma}{2} + j & \text{when } \underline{\sigma} \in \{0, 1\} \text{ and } i - j - \sigma \text{ is even} \\ \bot & \text{otherwise} \end{cases}$$

$$\delta(\bot, (\sigma, j)) = \bot$$

Consider inputs to the automaton which are of the form

$$\mathit{start}(i) \cdot \sigma_1(0) \cdots \sigma_n(0) \qquad \text{for } i \in \mathbb{N} \text{ and } \sigma_1, \ldots, \sigma_n \in \{\underline{0}, \underline{1}\}.$$

It is not difficult to see that such an input is accepted if and only if $\sigma_1 \cdots \sigma_n$ is a prefix of the binary representation of i (the binary representation written with the least significant bit coming first).

Consider the equivalence relation $\sim_n$ on Q defined by

$$q \sim_n p \qquad \text{if } \ q, p \in \mathbb{Z} \ \text{ and } \ q = p \mod 2^n.$$

It is not difficult to see that for every $a \in A$, we have

$$q \sim_n p \qquad \text{implies} \qquad \delta(q,a) \sim_{n-1} \delta(p,a).$$

It follows that states equivalent under $\sim_n$ have the same futures of length at most n. Also, the converse holds: if states are not equivalent under $\sim_n$, then they have different futures of length at most n. It follows that the equivalences $\sim_n$ have more and more equivalence classes, as n grows, and never stabilize. □

5.2 Computing the minimal automaton

So, how does one effectively minimize an automaton? Our approach is to reduce the minimization problem to satisfiability for an extension of Presburger arithmetic, which allows a limited use of the divisibility predicate.

A formula of *existential Presburger arithmetic with divisibility* (EPAD) is a formula of the form

$$\exists x_1 \cdots \exists x_n \ \phi \tag{2}$$

where the variables $x_1, \ldots, x_n$ quantify over integers; and ϕ is a quantifier-free formula in the language $(\mathbb{Z}, 0, 1, +, |)$, where $|$ stands for divisibility. A typical instance of EPAD is deciding if there is a solution to the system

$$\begin{aligned} 3x &= 3 \mod y \\ 5y &= 7 \mod x \\ 2x &= y - 18 \end{aligned}$$

Theorem 5. *[11] Satisfiability is decidable for EPAD.*

By a lengthy reduction to Theorem 5, we prove that one can effectively minimize a semilinear equivariant DFA. This is the main result of this paper.

Theorem 6. *Given a semilinear equivariant DFA with the integer atoms, one can compute the minimal automaton.*

The remaining part of the paper is devoted to the proof of the theorem.

6 Proof of Theorem 6

After some preparatory lemmas (Lemma 4 and Lemma 5 below) we formulate Theorem 7 below that essentially says that minimality is decidable for semilinear equivariant DFAs. By the virtue of Proposition 1 we know that this is sufficient for proving Theorem 6.

6.1 Decidability of minimality

The following lemma shows that semilinear and equivariant subsets of monomial sets can be interpreted as semilinear, but not necessarily equivariant, subsets of monomial sets of lower dimensions.

Lemma 4. *The function*

$$X \subseteq \mathbb{Z}^k \qquad \mapsto \qquad \{(i_2, \ldots, i_k) : (0, i_2, \ldots, i_k) \in X\} \subseteq \mathbb{Z}^{k-1}$$

is a bijection between semilinear and equivariant subsets of $\mathbb{Z}^k$, and semilinear but not necessarily equivariant subsets of $\mathbb{Z}^{k-1}$.

Proof. It is easy to see that the function produces semilinear sets, because the result of the function can be defined in Presburger arithmetic. The inverse of the function is defined by

$$Y \subseteq \mathbb{Z}^{k-1} \qquad \mapsto \qquad \{(l, i_1 + l, \ldots, i_{k-1} + l) : (i_1, \ldots, i_{k-1}) \in Y\}$$

□

Consider a semilinear equivariant DFA $\mathcal{A}$ with states Q, input alphabet A, and transition function δ. In the input alphabet, choose letters

$$a_1, \ldots, a_n \in A$$

so that every orbit is represented. For each of these letters, consider the function

$$\delta_i : Q \to Q \qquad \delta_i(q) = \delta(q, a_i).$$

Lemma 5. *An equivariant equivalence relation $\equiv$ on Q is a congruence in the automaton $\mathcal{A}$ if and only if it respects the final states and is a congruence for the functions $\delta_1, \ldots, \delta_n$.*

Proof. Choose any states $p, q \in Q$ such that $p \equiv q$. We need to show that

$$\delta(p, a) \equiv \delta(q, a) \qquad \text{for every } a \in A.$$

Choose then some letter $a \in A$. By choice of $a_1, \ldots, a_n$, there must be some a_i and some permutation π such that $a \cdot \pi = a_i$. By equivariance of δ, we have

$$\delta(q, a) \cdot \pi = \delta(q \cdot \pi, a \cdot \pi) = \delta_i(q \cdot \pi)$$

Because $\equiv$ is equivariant, it follows that $p \cdot \pi \equiv q \cdot \pi$, and therefore by the assumption on $\equiv$, we have

$$\delta_i(q \cdot \pi) \equiv \delta_i(p \cdot \pi).$$

By the same reasoning as above, we have

$$\delta_i(p \cdot \pi) \equiv \delta(p, a) \cdot \pi.$$

We have just proved that

$$\delta(q, a) \cdot \pi \equiv \delta(p, a) \cdot \pi.$$

By equivariance of $\equiv$, it follows that $\delta(q, a) \equiv \delta(p, a)$. □

Observe that the functions $\delta_1, \dots, \delta_n$ are not necessarily equivariant. Actually, they can be completely aribtrary, because every choice of functions $\delta_1, \dots, \delta_n$ can be lifted to an equivariant transition function

$$\delta : Q \times A \to Q \qquad \text{defined by} \qquad \delta(q, a) = \delta_i(q) \cdot \pi$$

where a_i and $\pi \in \mathbb{Z}$ are the unique elements satisfying $a = a_i \cdot \pi$. Because we are dealing with a semilinear automaton, all that we know is that $\delta_1, \dots, \delta_n$ are semilinear. That is why, in order to prove Theorem 6, we need to decide if there is an equivalence relation on Q which respects the final states, and which is a nontrivial congruence with respect to the arbitrary semilinear unary operations $\delta_1, \dots, \delta_n$. This is shown in Theorem 7, which is the main result of Section 6.

Theorem 7. *The following problem is decidable:*

- **Input.** *An orbit finite set Q, an equivariant subset $F \subseteq Q$, semilinear but not necessarily equivariant functions $\delta_1, \dots, \delta_n : Q \to Q$.*
- **Question.** *Is there an equivalence relation $\equiv$ on Q which:*
  1. *is nontrivial, i.e. identifies at least two different elements;*
  2. *respects F;*
  3. *is a congruence with respect to $\delta_1, \dots, \delta_n$;*
  4. *is equivariant.*

The proof strategy for the theorem is as follows.

1. We show that every equivariant equivalence relation $\equiv$ on Q can be described by a *signature*, which consists of:
   (a) The *equivalence type*: an equivalence relation $\sim$ on the orbits of Q.
   (b) The *equivalence parameters*: a finite vector of integer parameters.
   This step is done in Section 6.2.
2. We show that for every choice of the equivalence type (there are finitely many choices), whether or not the equivalence relation $\equiv$ is a congruence with respect to $\delta_1, \dots, \delta_n$ can be described, in terms of the equivalence parameters, by an existential formula of Presburger arithmetic with divisibility predicates. This step is done in Section 6.3.
3. We recall Theorem 5, which says that satisfiability is decidable for existential formulas of Presburger arithmetic with divisibility predicates.

The remaining part of Section 6 is devoted to the proof of Theorem 7.

6.2 The signature of an equivariant equivalence relation

In this section, we present the first step of the proof of Theorem 7. We show how every equivariant equivalence relation on an orbit finite set can be described by a finite piece of information and a vector of numbers.

Consider an orbit-finite equivariant set Q, together with an equivariant equivalence relation $\equiv$. Define a relation $[\equiv]$ on orbits of Q by:

$$\tau_1 \; [\equiv] \; \tau_2 \qquad \text{if } q_1 \equiv q_2 \text{ for some } q_1 \in \tau_1 \text{ and some } q_2 \in \tau_2.$$

This relation $[\equiv]$ is called the *equivalence type* of $\equiv$.

Lemma 6. *The relation $[\equiv]$ is an equivalence relation.*

Proof. The only nontrivial part, transitivity, follows from equivariance, as shown below. Suppose that

$$\tau_1 \; [\equiv] \; \tau_2 \qquad \text{and} \qquad \tau_2 \; [\equiv] \; \tau_3$$

hold for three orbits τ_1, τ_2, τ_3. This means that

$$q_1 \equiv q_2 \qquad \text{and} \qquad p_1 \equiv p_2 \qquad \text{for some } q_1 \in \tau_1, q_2, p_2 \in \tau_2, p_2 \in \tau_3.$$

Sincd q_2 and p_1 are in the same orbit, there must be some π such that $p_1 \cdot \pi = q_2$. By equivariance of $\equiv$, we have $p_1 \cdot \pi \equiv p_2 \cdot \pi$. Therefore, by transitivity of $\equiv$, we have $q_1 \equiv p_2 \cdot \pi$, and therefore $\tau_1 \; [\equiv] \; \tau_3$. □

We denote by $Q/{\equiv}$ the set of equivalence classes of Q under $\equiv$. Consider the quotient mapping

$$f : Q \to Q/{\equiv}$$

which maps an element of q to its equivalence class under $\equiv$, denoted by $[q]_\equiv$. It is not difficult to see that f is an equivariant function. As an image of an orbit-finite set under an equivariant function, the quotient $Q/{\equiv}$ is orbit-finite. Also, it is not difficult to see that the orbits of $Q/{\equiv}$ are in one-to-one correspondence to equivalence classes of the equivalence type $[\equiv]$.

So far we have defined the equivalence type of $\equiv$. This does not yet determine the equivalence relation $\equiv$. The missing information is: what are the characteristics of the orbits in the quotient $Q/\equiv$, and how does the quotient function identify elements of Q.

- Let Σ be an equivalence class of $[\equiv]$, corresponding to an orbit of $Q/\equiv$. Define $\mathrm{char}(\Sigma) \in \mathbb{N}$ to be the unique number such that the orbit of $Q/{\equiv}$ that corresponds to Σ is isomorphic to $\mathbb{Z}_{\mathrm{char}_\Phi(\Sigma)}$.
- Let Σ be an equivalence class of $[\equiv]$, and let $\tau, \sigma \in \Sigma$ be orbits of Q. The images $f(\tau)$ and $f(\sigma)$ are equal, and isomorphic to $\mathbb{Z}_{\mathrm{char}_\Phi(\Sigma)}$. Let $0_\tau, 0_\sigma$ be the copies of 0 in the orbits τ, σ. Define

  $$\mathrm{diff}(\tau, \sigma) \overset{\mathrm{def}}{=} f(0_\sigma) - f(0_\tau) \in \mathbb{Z}_{\mathrm{char}(\Sigma)}.$$

  In principle, $\mathrm{diff}(\tau, \sigma)$ is an element[3] of $\mathbb{Z}_{\mathrm{char}(\Sigma)}$. However, it will be convenient to treat it as an integer. That is why, we think of $\mathrm{diff}(\tau, \sigma)$ as any integer in the set

  $$\mathrm{diff}(\tau, \sigma) + \mathrm{char}(\Sigma) \cdot \mathbb{Z}.$$

  If there will be a need to make $\mathrm{diff}(\tau, \sigma)$ unique, we can choose it to be the smallest positive integer in the set above.

[3] In the definition of $\mathrm{diff}(\tau, \sigma)$, we implicitly use some isomorphism between $\mathbb{Z}_{\mathrm{char}(\Sigma)}$ and the orbit $f(\tau) = f(\sigma)$. There are, however, many possible isomorphisms. It can easily be checked that the difference $f(0_\sigma) - f(0_\tau)$ does not depend on the isomorphism.

Define *signature* of the equivariant equivalence relation $\equiv$ to be the triple

$$\Phi_{\equiv} \quad \overset{\text{def}}{=} \quad ([\equiv], \text{diff}, \text{char}),$$

which contains all the information defined above. This defines a mapping

$$\equiv \quad \mapsto \quad \Phi_{\equiv}. \tag{3}$$

We claim that the signature determines $\equiv$ uniquely. To prove this, we claim that there is an inverse transformation

$$\Phi \quad \mapsto \quad \equiv_{\Phi} \tag{4}$$

which maps a signature to an equivariant congruence.

Of course, the input to the inverse transformation needs to be consistent. This consistency condition is captured by the notion of an *equivalence signature.* An equivalence signature is a triple

$$\Phi = (\sim, \text{diff}, \text{char})$$

where $\sim$ is an equivalence relation on orbits of Q and diff, char are vectors

$$\begin{aligned} \text{diff} &: \{(\tau, \sigma) \in \mathit{orbits}(Q) \times \mathit{orbits}(Q) : \tau \sim \sigma\} \to \mathbb{Z} \\ \text{char} &: \mathit{classes}(\sim) \to \mathbb{N}. \end{aligned}$$

such that the following consistency conditions hold for every equivalence class Σ of $\sim$:

- for all $\tau_1, \tau_2, \tau_3 \in \Sigma$:

  $$\text{diff}(\tau_1, \tau_2) + \text{diff}(\tau_2, \tau_3) = \text{diff}(\tau_1, \tau_3) \mod \text{char}(\Sigma).$$

- for all $\tau \in \Sigma$,

  $$k = 0 \mod \text{char}(\Sigma),$$

  where τ is isomorphic to $\mathbb{Z}_k$.

The first condition above implies, in particular, that

$$\text{diff}(\tau, \tau) = 0 \mod \text{char}(\Sigma) \qquad \text{and} \qquad \text{diff}(\tau, \sigma) = -\text{diff}(\sigma, \tau) \mod \text{char}(\Sigma).$$

In the sequel we will write $\text{char}(\tau)$ instead of $\text{char}(\Sigma)$, when $\tau \in \Sigma$. Clearly, the mapping (3) is surjective onto equivalence signatures.

The following proposition shows that an equivariant equivalence relation on Q is completely described by its signature. (Note however that there are in general many different signatures defining the same equivalence, because $\text{diff}(\tau, \sigma)$ is only determined modulo $\text{char}(\tau) = \text{char}(\sigma)$.)

Proposition 3. *The exists a mapping* (4) *that maps equivalence signatures to equivariant equivalences, that is an inverse of the mapping* (3)*, namely:*

$$\equiv_{\Phi_{\equiv}} \quad = \quad \equiv \qquad\qquad \textit{for any equivariant equivalence } \equiv .$$

6.3 Which signatures describe congruences

Proposition 4. *Let $\sim$ be an equivalence relation on orbits of Q, and let*

$$f : Q \to Q$$

be a semilinear function. There set

$$\begin{aligned} X_{f,\sim} = \{(\mathrm{diff}, \mathrm{char}) :\ & (\sim, \mathrm{diff}, \mathrm{char}) \textit{ is an equivalence signature and} \\ & \equiv_{(\sim,\mathrm{diff},\mathrm{char})} \textit{ is a nontrivial congruence for } f\} \end{aligned}$$

is definable in EPAD.

Before proving Proposition 4, we show how it implies Theorem 7.

Proof (of Theorem 7). Recall that Theorem 7 says that one can decide if there exists some nontrivial equivariant equivalence relation on Q, which respects $F \subseteq Q$, and which is a congruence with respect to semilinear operations $\delta_1, \ldots, \delta_n$. By Proposition 3, every equivariant equivalence relation on Q is of the form $\equiv_\Phi$, for some equivalence signature

$$\Phi = (\sim, \mathrm{diff}, \mathrm{char}).$$

Since the set F is equivariant, it is a union of orbits $F = \tau_1 \cup \cdots \cup \tau_k$. This means that $\equiv_\Phi$ respects F if and only if the equivalence relation $\sim$ respects the set $\{\tau_1, \ldots, \tau_k\}$. Recall the sets $X_{f,\sim}$ from Proposition 4. There is a nontrivial congruence on Q which respects F if and only if the following set is nonempty

$$\bigcup_{\sim \text{ respects } \tau_1, \ldots, \tau_k} \quad \bigcap_{i \in \{1,\ldots,n\}} \quad X_{\delta_i,\sim}.$$

As EPAD admits positive boolean combinations, it follows from Proposition 4 that the above set is definable in EPAD. We can therefore invoke Theorem 5 to test if the set is nonempty. □

The rest of Section 6.3 is devoted to proving Proposition 4. Fix the relation $\sim$ on orbits of Q for the rest of this section.

We will identify an element of Q with a pair (τ, i), where τ is an orbit and i is an integer. When the orbit τ has characteristic $k > 0$, then this representation is many-to-one, because the pairs (τ, i) and $(\tau, i+k)$ represent the same element.

Lemma 7. *Let $\Phi = (\sim, \mathrm{diff}, \mathrm{char})$ be an equivalence signature. The equivalence $\equiv_\Phi$ is a congruence with respect to a function f if and only if*

$$\forall i \in \mathbb{Z} \qquad f(\tau, i) \equiv_\Phi f(\tau, i + \mathrm{char}(\tau)) \qquad \textit{for every orbit } \tau \tag{5}$$

$$\forall i \in \mathbb{Z} \qquad f(\tau, i) \equiv_\Phi f(\sigma, i + \mathrm{diff}(\tau, \sigma)) \qquad \textit{for every orbits } \tau \sim \sigma \tag{6}$$

Proof. The left-to-right implication is immediate. We only do the right-to-left implication. A short argument is that the relation $\equiv_\Phi$ is the smallest equivalence relation generated by the pairs

$$(\tau, i) \equiv_\Phi (\tau, i + \mathrm{char}(\tau)) \qquad (\tau, i) \equiv_\Phi (\sigma, i + \mathrm{diff}(\tau, \sigma))$$

ranging over integers $i \in \mathbb{Z}$ and orbits $\tau \sim \sigma$. Therefore, if f respects the generators, it will also respect the whole equivalence relation. □

The key technical lemma is Lemma 8, stated below.

Lemma 8. *Fix f, $\sim$ and orbits τ, σ. The set*

$$X_{f,\sim,\tau,\sigma} \;=\; \{(\mathrm{diff}, \mathrm{char}, \Delta) \;:\; \forall i \in \mathbb{Z} \quad f(\tau, i) \equiv_{(\sim,\mathrm{diff},\mathrm{char})} f(\sigma, i + \Delta)\} \qquad (7)$$

is definable in EPAD.

Before proving the lemma, we show how, together with Lemma 7, it implies Proposition 4.

Proof (of Proposition 4). In order to prove Proposition 4, it is sufficient to establish two conditions. First, we claim that for every choice of $\sim$, the set

$$\{(\mathrm{diff}, \mathrm{char}) : (\sim, \mathrm{diff}, \mathrm{char}) \text{ is an equivalence signature}\}$$

is definable in EPAD. Then, by Lemma 7, it suffices to show that for every choice of $\sim$, each of the properties (5), (6) can be defined in EPAD. This is exactly what Lemma 8 says. □

The key obstacle for expressing (7) in EPAD is that it has the universal quantifier $\forall i$, which is not allowed in EPAD. The is idea to use a technique of quantifier elimination, which is presented in the following lemma about arithmetic progressions. A finite arithmetic progression is a set $a + p \cdot \{0, \ldots, k\}$. An infinite arithmetic progression is a set $a + p \cdot \mathbb{N}$. Both the base a and the period p can be negative.

Lemma 9. *Fix an equivalence signature $\Phi = (\sim, \mathrm{diff}, \mathrm{char})$. Let $f_1, f_2 : \mathbb{Z} \to Q$ be affine functions defined by*

$$f_1(x) = (\tau_1, a_1 \cdot x + b_1) \qquad f_2(x) = (\tau_2, a_2 \cdot x + b_2),$$

for orbits $\tau_1 \sim \tau_2$ and coefficients $a_1, b_1, a_2, b_2 \in \mathbb{Z}$. Let $X \subseteq \mathbb{Z}$ be a finite or infinite arithmetic progression. For any two consecutive elements $x_0, x_1 \in X$,

$$\forall x \in X \quad f_1(x) \equiv_\Phi f_2(x) \qquad \textit{iff} \qquad \bigwedge_{x \in \{x_0, x_1\}} f_1(x) \equiv_\Phi f_2(x)$$

Proof. We only prove the nontrivial right-to-left implication. By unraveling the definition of functions f_1 and f_2, $f_1(x) \equiv_\Phi f_2(x)$ is equivalent to

$$\alpha(x) = 0 \mod \mathrm{char}(\tau_1)$$

for the function $\alpha : \mathbb{Z} \to \mathbb{Z}$ defined by

$$\alpha(x) = a_1 \cdot x + b_1 - \mathrm{diff}(\tau_1, \tau_2) - a_2 \cdot x - b_2.$$

This is an affine function. Suppose then that

$$\bigwedge_{x \in \{x_0, x_1\}} \alpha(x) = 0 \mod \mathrm{char}(\tau_1)$$

holds. Then it follows that

$$\forall k \in \mathbb{Z} \qquad \alpha(x_0 + k \cdot (x_1 - x_0)) = 0 \mod \mathrm{char}(\tau_1).$$

In particular, because x_1 and x_0 are consecutive elements in the progression X, it follows that

$$\forall x \in X \qquad \alpha(x) = 0 \mod \mathrm{char}(\tau_1),$$

which means that

$$\forall x \in X \quad f_1(x) \equiv_{\varPhi} f_2(x)$$

as required. □

Proof (of Lemma 8). Consider the functions $g, h : \mathbb{Z} \to Q$ defined by

$$g(x) = f(\tau, x) \qquad \text{and} \qquad h(x) = f(\sigma, x).$$

As f is semilinear, we know that there is a partition of $\mathbb{Z}$ into a finite family of arithmetic progressions $\{X_i\}_{i \in I}$ (respectively, $\{Y_j\}_{j \in J}$), and a family of affine functions $\{g_i : \mathbb{Z} \to Q\}_{i \in I}$ (respectively, $\{h_j : \mathbb{Z} \to Q\}_{j \in J}$), such that on arguments from X_i, the functions g_i and g coincide (respectively, on arguments from Y_j, the functions h_j and h coincide).

Expressed in terms of these partitions and affine functions, condition (7) from Lemma 8 becomes

$$\forall x \qquad \bigwedge_{i \in I, j \in J} \big(x \in X_i \wedge (x + \varDelta \in Y_j)\big) \quad \Rightarrow \quad g_i(x) \equiv_{\varPhi} h_j(x + \varDelta)$$

(we write shortly $\varPhi$ instead of $(\sim, \mathrm{diff}, \mathrm{char})$ here and in the sequel) which is the same as the conjunction, ranging over all choices of $i \in I$ and $j \in J$, of the properties

$$\forall x \in (X_i \cap (Y_j - \varDelta)) \quad g_i(x) \equiv_{\varPhi} h_j(x + \varDelta) \tag{8}$$

Therefore, it is sufficient to provide a formula of EPAD for each formula of the form (8). Let us fix then i and j in the sequel.

As an intersection of two arithmetic progressions, the set $X_i \cap (Y_j - \varDelta)$ is an arithmetic progression. The sets X_i and Y_j are known, only $\varDelta$ is unknown. Depending on the value of $\varDelta$, the progression $X_i \cap (Y_j - \varDelta)$ might have zero, one or at least two elements. Thanks to Lemma 9, we know that (8) is equivalent to the following property:

(A1) If $X_i \cap (Y_j - \mathit{\Delta})$ has at least one element x, then

$$g_i(x) \equiv_{\mathit{\Phi}} h_j(x + \mathit{\Delta}).$$

(A2) If $X_i \cap (Y_j - \mathit{\Delta})$ has at least two elements x_1, x_2, and they are consecutive, then

$$\bigwedge_{k \in \{1,2\}} g_i(x_k) \equiv_{\mathit{\Phi}} h_j(x_k + \mathit{\Delta}).$$

We claim that both these properties can be formalized in EPAD. Let us focus on the more difficult property (A2). It is not difficult to see that the set

$$\mathit{cons} = \{(\mathit{\Delta}, x_1, x_2) : \; x_1, x_2 \text{ are consecutive elements of } X_i \cap (Y_j - \mathit{\Delta})\}$$

are Presburger definable. Property (A2) is an implication. The head of the implication, "if $X_i \cap (Y_j - \mathit{\Delta})$ has at least two elements x_1, x_2" is defined by a Presburger formula $\exists\ x_1 x_2\ \mathit{cons}(\mathit{\Delta}, x_1, x_2)$. The tail of the implication can be seen as the formula:

$$\exists\ x_1 x_2 \qquad \mathit{cons}(\mathit{\Delta}, x_1, x_2) \wedge \bigwedge_{k \in \{1,2\}} g_i(x_k) \equiv_{\mathit{\Phi}} h_j(x_k + \mathit{\Delta}),$$

which is definable in EPAD. This completes the proof of Lemma 8, being the last part of the proof of Theorem 7. □

References

1. R. Alur, C. Courcoubetis, N. Halbwachs, D. L. Dill, and H. Wong-Toi. Minimization of timed transition systems. In *CONCUR*, pages 340–354, 1992.
2. R. Alur and D. L. Dill. A theory of timed automata. *Theor. Comput. Sci.*, 126(2):183–235, 1994.
3. M. Bojańczyk, B. Klin, and S. Lasota. Automata with group actions. In *Proc. LICS'11*, pages 355–364, 2011.
4. M. Bojanczyk and S. Lasota. Fraenkel-mostowski sets with non-homogeneous atoms. In *RP*, pages 1–5, 2012.
5. M. Bojańczyk and S. Lasota. A machine-independent characterization of timed languages. In *Proc. ICALP'12*, pages 92–103, 2012.
6. Stéphane Demri and Ranko Lazic. Ltl with the freeze quantifier and register automata. *ACM Trans. Comput. Log.*, 10(3), 2009.
7. D. Figueira, P. Hofman, and S. Lasota. Relating timed and register automata. In *Proc. EXPRESS'10*, volume 41 of *EPTCS*, pages 61–75, 2010.
8. N. Francez and M. Kaminski. Finite-memory automata. *TCS*, 134(2):329–363, 1994.
9. M. Gabbay. Foundations of nominal techniques: logic and semantics of variables in abstract syntax. *Bulletin of Symbolic Logic*, 17(2):161–229, 2011.
10. M. Gabbay and A. M. Pitts. A new approach to abstract syntax with variable binding. *Formal Asp. Comput.*, 13(3-5):341–363, 2002.

11. L. Lipshitz. The Diophantine problem for addition and divisibility. *Trans. Amer. Math. Soc.*, 235:217–283, 1978.
12. D. Macpherson. A survey of homogeneous structures. *Discrete Mathematics*, 311(15):1599–1634, 2011.
13. J. Ochremniak. Nominal sets for symmetrie with function symbols. Unpublished note, 2012.
14. J. Springintveld and F. W. Vaandrager. Minimizable timed automata. In *FTRTFT*, pages 130–147, 1996.
15. S. Tripakis. Folk theorems on the determinization and minimization of timed automata. *Inf. Process. Lett.*, 99(6):222–226, 2006.
16. M. Yannakakis and D. Lee. An efficient algorithm for minimizing real-time transition systems. *Formal Methods in System Design*, 11(2):113–136, 1997.