Automatic Equivalence Structures of Polynomial Growth

Moses Ganardi
University of Siegen, Siegen, Germany
ganardi@eti.uni-siegen.de

Bakhadyr Khoussainov
University of Auckland, Auckland, New Zealand
bmk@cs.auckland.ac.nz

Abstract

In this paper we study the class EqP of automatic equivalence structures of the form $\mathfrak{E} = (D, E)$ where the domain D is a regular language of polynomial growth and E is an equivalence relation on D. Our goal is to investigate the following two foundational problems (in the theory of automatic structures) aimed for the class EqP. The first is to find algebraic characterizations of structures from EqP, and the second is to investigate the isomorphism problem for the class EqP. We provide full solutions to these two problems. First, we produce a characterization of structures from EqP through multivariate polynomials. Second, we present two contrasting results. On the one hand, we prove that the isomorphism problem for structures from the class EqP is undecidable. On the other hand, we prove that the isomorphism problem is decidable for structures from EqP with domains of quadratic growth.

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

Keywords and phrases automatic structures, polynomial growth, isomorphism problem

Digital Object Identifier 10.4230/LIPIcs.CSL.2020.21

Funding *Moses Ganardi*: This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No 731143.

1 Introduction

Automatic structures are relational structures $\mathfrak{A} = (D, R_1, \dots, R_k)$ where the domain D is a regular language and every relation $R_i \subseteq D^{r_i}$ is recognized by a finite automaton with r_i many synchronous heads [3, 8]. They constitute a robust class of finitely presented structures with good algorithmic and often algebraic properties; in particular, the model checking problem for first-order logic (and some of its extensions such as $(\mathrm{FO} + \exists^\infty)$–logic) is decidable over automatic structures [3, 7, 11]. However, going beyond first-order logic, problems quickly become undecidable over automatic structures, e.g. the reachability problem is undecidable for automatic structures.

An important problem in the theory of automatic structures is the isomorphism problem. The problem asks to design an algorithm that given two automatic structures decides if the structures are isomorphic. Blumensath and Grädel proved that the isomorphism problem is undecidable [3]. Furthermore, it turns out that the isomorphism problem for automatic structures is complete for the first level of the analytical hierarchy Σ_1^1 [9]. In addition, Nies [15] proved that the problem remains Σ_1^1-complete for the class of undirected graphs and partial orders, and Kuske, Liu and Lohrey [4] showed that the problem is Σ_1^1-complete for even automatic linear orders. In contrast, the isomorphism problem is decidable for automatic ordinals [10] and Boolean algebras [9]. These decidability results follow from full characterization results for automatic ordinals and Boolean algebras [10, 9]. Interestingly, full characterizations of isomorphism types do not immediately imply decidability of the isomorphism problem for automatic structures. For instance, Thomas and Oliver [16] proved that automata presented finitely generated groups are virtually abelian. However, it is still unknown if the isomorphism problem for this class of automatic groups is decidable.

The class of equivalence structures, these are structures of the form (D, E) where E is an equivalence relation on D, are among the simplest algebraic structures (in terms of descriptions of the their isomorphism types). The isomorphism type of each such structure (D, E) is fully characterized by the function $f : \mathbb{N}_+ \cup \{\infty\} \to \mathbb{N} \cup \{\infty\}$ defined as follows:

$$f(n) = \text{the number of equivalence classes of size } n \tag{1}$$

This description immediately implies that the isomorphism problem for automatic equivalence structures is a Π^0_1-predicate. It had been a long-standing open question if the isomorphism problem for automatic equivalence structures is decidable. Kuske, Liu and Lohrey [4] proved that the isomorphism problem over automatic equivalence structures is Π^0_1-complete, and hence undecidable. It is worth to mention the following simple observation from [4]. There is an algorithm that, given two automatic isomorphic equivalence structures, builds a computable isomorphism between them. This is in spite the fact that the isomorphism problem for automatic equivalence relations is undecidable.

In light of the (undecidability) results above, the following question arises. Find classes of automatic structures for which the isomorphism problem is decidable. One approach to address the question is to put algebraic restrictions on the class of automatic structures. For instance, one can consider the classes of automatic torsion free abelian groups and ask if the isomorphism problem for this class of structures is decidable. The second approach is to consider classes of automatic structures whose domains belong to some robust class of regular languages. For instance, in [2, 18, 13] automatic structures with unary domains are studied; it is proved the isomorphism problem is decidable for unary automatic linear orders, equivalence structures, and trees. Although, we still do not know if the isomorphism problem for unary automatic structures is decidable. Bárány [1] initiated the study of automatic structures with domains of polynomial growth. He provided examples of universal structures in this class and proved that the isomorphism problem in this class of structures is undecidable. The third way to address the problem is to combine the above two approaches by restricting both the class of structures and the class of regular domains. This is exactly what we do in this paper. We focus on automatic equivalence structures of the form (D, E) where D is a regular language of polynomial growth and E is an equivalence relation on D. We denote this class of automatic structures by EqP. The choice of this class is partly motivated by the facts mentioned above: (1) The isomorphism types of equivalence structures have full descriptions, and (2) the isomorphism problem for automatic equivalence structures is undecidable.

In this paper we thus address two foundational problems for the class EqP. The first is to find algebraic characterizations of structures from EqP, and the second is to investigate the isomorphism problem for the class EqP. We fully solve these two problems. First, we produce a characterization of automatic equivalence structures from EqP in the language of multivariate polynomials. Second, we present two contrasting results. On the one hand, we prove that the isomorphism problem for automatic structures from the class EqP is undecidable. On the other hand, we prove that the isomorphism problem is decidable for structures from EqP with domains bounded by a quadratic growth.

2 Summary of results

Let $\mathbb{N} = \{0, 1, 2, \dots\}$ and $\mathbb{N}_+ = \{1, 2, \dots\}$ be the sets of nonnegative and positive integers. Polynomials $f \in \mathbb{N}[x_1, \dots, x_k]$ are viewed as functions $f : \mathbb{N}^k \to \mathbb{N}$. The number k is also denoted by $\mathrm{var}(f)$; the degree of g is denoted by $\deg(f)$.

An *equivalence structure* $\mathfrak{E} = (D, E)$ consists of a domain D and an equivalence relation E on D. We denote by $[x] = \{y \in D \mid (x, y) \in E\}$ the equivalence class of $x \in D$. As described in (1), the isomorphism type of $\mathfrak{E}$ can be described by specifying the number of equivalence classes of every finite or infinite size. Since we will only deal with countable domains, there is only one infinite cardinality. We defer the formal definition of automatic structures to Section 3.

Let D be a regular language. Its growth is the function gr_D that for each n computes the number of strings of length n that belong to D. We say that the language D has a polynomial growth if its growth function gr_D is bounded by a polynomial in n. We denote by EqP the class of all automatic equivalence structures (D, E) such that D is a regular language of polynomial growth. Here is a simple yet an important example of a structure from EqP:

▶ **Example 1.** Consider the equivalence structure $\mathfrak{E} = (D, E)$ defined as follows: The domain is $D = 0^*1^*2^*3^*$ and the equivalence relation E consists of pairs (u, v) from the domain such that $(u, v) \in E$ if and only if $|u|_0 + |u|_1 = |v|_0 + |v|_1$ and $|u|_2 + |u|_3 = |v|_2 + |v|_3$. Here, $|w|_\sigma$ denotes the number of times σ appears in w. It is easy to see that the equivalence structure $\mathfrak{E}$ is automatic. A *set of representatives* is a subset $R \subseteq D$ containing exactly one element from each equivalence class. An example of a regular set of representatives of E is the language 0^*2^*. Note that the class $[0^{t_0}2^{t_2}]$ has size $(t_0 + 1)(t_2 + 1)$. One could say that the polynomial $g(t_0, t_2) = (t_0 + 1)(t_2 + 1)$ defines $\mathfrak{E}$ up to isomorphism: for each tuple $(t_0, t_2) \in \mathbb{N}^2$ it contains a class of size $g(t_0, t_2)$.

This example suggests us to give the following definition (construction):

▶ **Definition 2.** *For a function $g : \mathbb{N}^k \to \mathbb{N}$, the equivalence structure $\mathfrak{E}(g)$ is defined (up to isomorphism) as follows. The number of classes of size $s \in \mathbb{N}_+$ in $\mathfrak{E}(g)$ is given by the cardinality $|\{\bar{t} \in \mathbb{N}^k \mid g(\bar{t}) = s\}|$. Furthermore $\mathfrak{E}(g)$ has no infinite classes.*

Note that $\mathfrak{E}(g)$ can have infinitely many classes of a certain size s. For instance, if $g(t_0, t_1) = t_0$ is the polynomial in two variables t_0, t_1, then for all $s \in \mathbb{N}_+$ there are infinitely many classes of size s in $\mathfrak{E}(g)$. However, all classes in $\mathfrak{E}(g)$ are finite. We remark that tuples which are mapped to 0 are irrelevant for the definition of $\mathfrak{E}(g)$. Our characterization theorem for equivalence structures from the class EqP is the following:

▶ **Theorem 3.** *Let $\mathfrak{E}$ be an equivalence structure and $k \in \mathbb{N}$. Then the following statements are equivalent:*

1. *$\mathfrak{E}$ is isomorphic to an automatic equivalence structure (D, E) where D has growth $O(n^k)$.*
2. *$\mathfrak{E}$ is a finite disjoint union of equivalence structures $\mathfrak{E}(g_1), \dots, \mathfrak{E}(g_m)$ where each g_i is a polynomial with natural coefficients and $\mathrm{var}(g_i) + \deg(g_i) \le k + 1$ and a number of infinite classes (which must be finitely many if $k = 0$).*

Furthermore, this correspondence is effective.

The decomposition into equivalence structures $\mathfrak{E}(g_i)$ defined by polynomials g_i is obtained by applying a result from Woods [22] who characterized *counting functions* of Presburger definable relations. The bound on the degree and the number of variables is obtained by a growth argument.

The characterization theorem provides us with two contrasting results. The first result is undecidability of the isomorphism problem for the class EqP.

▶ **Theorem 4.** *There exists a number $k \geq 0$ such that it is Π_1^0-complete to decide whether two automatic equivalence structures of growth $O(n^k)$ are isomorphic.*

The proof of Theorem 4 follows the ideas of the undecidability proof of [4], which uses the MRDP-theorem [14]. The second result is decidability of the isomorphism problem for structures from EqP of quadratic growth:

▶ **Theorem 5.** *It is decidable whether two given automatic equivalence structures of growth $O(n^2)$ are isomorphic.*

The proof idea of Theorem 5 is to reduce it to equality of multisets defined by quadratic polynomials, which can be decided with the help of the theory of quadratic Diophantine equations. The outline of the paper is as follows. After giving the necessary definitions in Section 3 we prove the characterization theorem (Theorem 3) in Section 4. In Section 5 we prove the undecidability result (Theorem 4) and in Section 6 we prove Theorem 5.

3 Preliminaries

We presuppose basic definitions in regular languages and first-order logic. Let us recall the definition of automatic structures. The *convolution* of k words $v_1, \dots, v_k$ where $v_i = a_{i,1} \cdots a_{i,n_i}$ is the word $(a_{1,1}, \dots, a_{k,1}) \cdots (a_{1,m}, \dots, a_{k,m})$ of length $m = \max\{n_1, \dots, n_k\}$ over the alphabet $\Sigma_\diamond^k = (\Sigma \cup \{\diamond\})^k$ where $a_{i,j} = \diamond$ for all $n_j < i \leq m$ and $1 \leq j \leq k$. It is denoted by $v_1 \otimes v_2 \otimes \cdots \otimes v_k$. A relation $R \subseteq D^k$ over a language D is *automatic* if $\otimes R_i = \{v_1 \otimes \cdots \otimes v_k \mid (v_1, \dots, v_k) \in R\}$ is regular. A relational structure $\mathfrak{A} = (D, R_1, \dots, R_m)$ is *automatic* if the domain D is a regular language and each relation R_i automatic. Given an automatic structure $\mathfrak{A} = (D, R_1, \dots, R_m)$ and a first-order formula $\varphi(\bar{x})$ with infinity quantifiers $\exists^\infty$, one can compute an automaton recognizing $\otimes\{\bar{v} \mid \mathfrak{A} \models \varphi(\bar{v})\}$, see [8, 3]. Here a formula of the form $\exists^\infty x \varphi(x, \bar{y})$ states that there are infinitely many elements x satisfying $\varphi(x, \bar{y})$. In particular, if $\varphi(x)$ is such a formula then the restriction of $\mathfrak{A}$ to $\{v \in D \mid \mathfrak{A} \models \varphi(v)\}$ is also automatic.

The *growth function* of a language L is the function $n \mapsto |\{w \in L \mid |w| = n\}|$. It is known that a regular language has growth $O(n^k)$ if and only if it can be written as a finite union of languages defined by regular expressions of the form $x_0 y_0^* \cdots x_\ell y_\ell^* x_{\ell+1}$ where $0 \leq \ell \leq k$, see [21]. Furthermore, we can compute such regular expressions such that the union is disjoint and that each expression is *unambiguous*, i.e. the function $(i_0, \dots, i_\ell) \mapsto x_0 y_0^{i_0} \cdots x_\ell y_\ell^{i_\ell} x_{\ell+1}$ is injective, cf. [21, Proof of Lemma 3].

Semilinear sets and Presburger arithmetic. A set $S \subseteq \mathbb{N}^k$ is *semilinear* if it is a finite union of *linear sets*

$$L = \bar{v}_0 + \langle \bar{v}_1, \dots, \bar{v}_n \rangle = \{\bar{v}_0 + \sum_{i=1}^{n} \lambda_i \bar{v}_i \mid \lambda_1, \dots, \lambda_n \in \mathbb{N}\}.$$

A linear set is *fundamental* if the period vectors $\bar{v}_1, \dots, \bar{v}_n$ are linearly independent in $\mathbb{R}^k$. It is known that every semilinear set is a finite disjoint union of fundamental linear sets [6] and that such a representation can be computed effectively. In the one-dimensional case this means that every semilinear set $S \subseteq \mathbb{N}$ is a finite disjoint union of singleton sets and arithmetic progressions $\{a + bn \mid n \in \mathbb{N}\}$ with $a, b \in \mathbb{N}$, $b \neq 0$.

An important theorem which connects context-free languages and semilinear sets is Parikh's theorem. For an ordered alphabet $\Sigma = \{a_1, \dots, a_k\}$ the *Parikh mapping* $\Phi \colon \Sigma^* \to \mathbb{N}^k$ is defined by $\Phi(w) = (|w|_{a_1}, \dots, |w|_{a_k})$. Parikh's theorem states that for every context-free language $L \subseteq \Sigma^*$ the Parikh image $\Phi(L) = \{\Phi(w) \mid w \in L\}$ is effectively semilinear [17]. Recall that *Presburger arithmetic* is the first-order logic over the structure $(\mathbb{N}, +, 0, \leq)$. It is known that a relation $R \subseteq \mathbb{N}^k$ is definable by a Presburger formula $\varphi(x_1, \dots, x_k)$ if and only if R is semilinear, and this correspondence is effective [5].

Counting functions. Given a formula $\varphi(\bar{s}, \bar{t})$ of Presburger arithmetic, we will in our arguments employ the counting function $c(\bar{t}) = |\{\bar{s} \mid \varphi(\bar{s}, \bar{t})\}|$ where we assume that this quantity is finite. For example, given the formula $\varphi(s, t_1, t_2) = \exists x(s = x + x \wedge t_1 \leq s \wedge s \leq t_2)$ the function $c(t_1, t_2) = |\{s \mid \varphi(s, t_1, t_2)\}|$ counts the number of even numbers s between t_1 and t_2.

We will also use quasi-polynomials. A *quasi-polynomial* is a function $g \colon \mathbb{N}^k \to \mathbb{Q}$ such that there is a k-dimensional lattice $\Lambda \subseteq \mathbb{Z}^k$ (that is, Λ is a finite index subgroup of $\mathbb{Z}^k$) and polynomials $q_{\lambda+\Lambda}(\bar{t})$ such that $g(\bar{t}) = q_{\lambda+\Lambda}(\bar{t})$ for all $\bar{t} \in \lambda + \Lambda$, where $\lambda + \Lambda$ belongs to the quotient set $\mathbb{Z}^k/\Lambda$. Notice that each coset $\lambda + \Lambda \in \mathbb{Z}^k/\Lambda$ is semilinear. A *piecewise quasi-polynomial* is a function $g \colon \mathbb{N}^k \to \mathbb{Q}$ such that there exist a finite partition $\bigcup_i (P_i \cap \mathbb{N}^k) = \mathbb{N}^k$ with rational polyhedra P_i and quasi-polynomials g_i such that $g(\bar{t}) = g_i(\bar{t})$ for all $\bar{t} \in P_i \cap \mathbb{N}^k$. Recall that a rational polyhedron is the finite intersection of half-spaces $\{(x_1, \dots, x_k) \in \mathbb{R}^k \mid \sum_{i=1}^k a_i x_i \leq b\}$ where the coefficients $a_1, \dots, a_k$ and the right hand side b are integers. If $P \subseteq \mathbb{R}^k$ is a rational polyhedron then $P \cap \mathbb{N}^k$ is clearly effectively Presburger-definable and hence effectively semilinear.

We will need the following two theorems:

▶ **Theorem 6** ([22]). *For every Presburger formula $\varphi(\bar{s}, \bar{t})$ the function $c(\bar{t}) = |\{\bar{s} \mid \varphi(\bar{s}, \bar{t})\}|$ is piecewise quasi-polynomial. Furthermore, the representation of c can be effectively computed.*

For example the counting function $c(t_1, t_2)$ from above which counts the number of even numbers between t_1 and t_2 can be seen to be piecewise quasi-polynomial: Choose the polyhedron $P = \{(x_1, x_2) \in \mathbb{R}^2 \mid x_1 \leq x_2\}$ and the lattice $\Lambda = 2\mathbb{Z} \times 2\mathbb{Z}$. Then $c(t_1, t_2) = 0$ for all $(t_1, t_2) \in \mathbb{N}^2 \setminus P$ and

$$c(t_1, t_2) = \begin{cases} \frac{t_2 - t_1}{2} + 1, & \text{for } (t_1, t_2) \in P \cap \Lambda, \\ \frac{t_2 - t_1 + 1}{2}, & \text{for } (t_1, t_2) \in P \cap (((1,0) + \Lambda) \cup ((0,1) + \Lambda)), \\ \frac{t_2 - t_1}{2}, & \text{for } (t_1, t_2) \in P \cap ((1,1) + \Lambda). \end{cases}$$

Since every semilinear set is a disjoint union of fundamental linear sets for every counting function c of a Presburger formula there exists a finite partition $\mathbb{N}^k = \bigcup_i L_i$ and polynomials g_i such that each L_i is a fundamental linear set and the counting function c coincides with g_i on L_i. Furthermore, this representation is effectively computable. Theorem 6 can be strengthened for the special case where the tuple $\bar{s}$ is a single variable:

▶ **Theorem 7** ([20]). *For every Presburger formula $\varphi(y, \bar{z})$ there exists a formula $\psi(x, \bar{z})$ which states that x is the number of elements y such that $\varphi(y, \bar{z})$ holds.*

Multisets. A *multiset* over a set A is a function $M \colon A \to \mathbb{N}_\infty$ where $\mathbb{N}_\infty = \mathbb{N} \cup \{\infty\}$. The number $M(a)$ is the *multiplicity* of a in M. The support of M is the set $\mathrm{supp}(M) = \{a \in A \mid M(a) > 0\}$. We call M *finite* if its support is finite and every multiplicity is finite. If $f \colon A \to B$ is a function and $X \subseteq A$, then we define $f(X)$ to be the multiset over B with $f(X)(b) = |f^{-1}(\{b\}) \cap X|$. Instead of $f(A)$ we also write $\mathrm{Rg}(f)$, which is the *range* of f. The union and difference of two multisets $M_1, M_2 \colon A \to \mathbb{N}_\infty$ is defined by $(M_1 \uplus M_2)(a) = M_1(a) + M_2(a)$ and $(M_1 \setminus M_2)(a) = \max(M_1(a) - M_2(a), 0)$ where $n - \infty = 0$ for all $n \in \mathbb{N}_\infty$. We define $M_1 \subseteq M_2$ iff $M_1(a) \leq M_2(a)$ for all $a \in A$. Given a multiset M over A and a subset $S \subseteq A$, we define $M \restriction S$ as $(M \restriction S)(a) = M(a)$ if $a \in S$ and $(M \restriction S)(a) = 0$ otherwise.

4 Characterization: Proof of Theorem 3

Our proof consists of several lemmas. To prove the implication (2) → (1), we first observe that the class of automatic equivalence structures with polynomially bounded growth is closed under disjoint union.

▶ **Lemma 8.** *Let $\mathfrak{E}_1 = (D_1, E_1)$ and $\mathfrak{E}_2 = (D_2, E_2)$ be two automatic equivalence structures. Then there exists an automatic equivalence structure $\mathfrak{E} = (D, E)$ isomorphic to the disjoint union of $\mathfrak{E}_1$ and $\mathfrak{E}_2$. If D_1 and D_2 have growth $O(n^k)$ then also D has growth $O(n^k)$.*

Proof. Say $D_1, D_2 \subseteq \Sigma^*$ and let $\#_1, \#_2 \notin \Sigma$ be fresh symbols. The disjoint union $\mathfrak{E}_1 \cup \mathfrak{E}_2$ is isomorphic to (D, E) where $D = \#_1 D_1 \cup \#_2 D_2$ and $E = \bigcup_{i \in \{1,2\}} \{(\#_i u, \#_i v) \mid (u, v) \in E_i\}$. For $n \geq 1$ we have $|D \cap \Sigma^n| = |D_1 \cap \Sigma^{n-1}| + |D_2 \cap \Sigma^{n-1}| \leq O(n^k)$. ◀

To complete the proof of the implication (2) → (1), it suffices to consider equivalence structures of the form $\mathfrak{E}(g)$ and equivalence structures where all classes are infinite. If $\mathfrak{E}$ consists of $n \in \mathbb{N}$ infinite classes, then $\mathfrak{E}$ is isomorphic to $(0^*, E)$ where two words 0^i and 0^j are equivalent iff i and j are congruent mod n. If $\mathfrak{E}$ consists of infinitely many infinite classes then $\mathfrak{E}$ is isomorphic to $(0^*1^*, E)$ where two words are equivalent iff the number of 0's is equal.

▶ **Lemma 9.** *Given a non-zero polynomial $g \in \mathbb{N}[t_1, \dots, t_k]$ with degree d one can compute an automatic equivalence structure (D, E) isomorphic to $\mathfrak{E}(g)$ where the growth of D is $O(n^{k+d-1})$.*

Proof. Kuske, Lohrey, Liu [4] construct a finite automaton $\mathcal{A} = (Q, \Sigma, I, \Delta, F)$ over the alphabet $\Sigma = \{1, \dots, k\}$ such that the number of accepting runs of $\mathcal{A}$ on $1^{t_1} \cdots k^{t_k}$ is $g(t_1, \dots, t_k)$ for all $t_1, \dots, t_k \in \mathbb{N}$. A run in $\mathcal{A}$ can be described as a sequence of transitions

$$(q_0, a_1, q_1)(q_1, a_2, q_2) \cdots (q_{n-1}, a_n, q_n) \in \Delta^*.$$

Let $D \subseteq \Delta^*$ be the set of all accepting runs of $\mathcal{A}$, which is a regular language, and let two runs be E-equivalent iff they are runs on the same word. Notice that E is automatic and (D, E) is isomorphic to $\mathfrak{E}(g)$. The number of accepting runs of $\mathcal{A}$ on words of length $n \in \mathbb{N}$ is bounded by

$$\sum_{t_1 + \dots + t_k = n} g(t_1, \dots, t_k) \leq O(n^{k-1}) \cdot g(n, \dots, n) \leq O(n^{k+d-1}),$$

which concludes the proof. ◀

With respect to Lemma 8, note that the class EqP is closed under the product operation (although this fact is not used in our arguments). Namely, let $\mathfrak{E}_1 = (D_1, E_1)$ and $\mathfrak{E}_2 = (D_2, E_2)$ be two structures from EqP. Then the equivalence structure $\mathfrak{E}_1 \cdot \mathfrak{E}_2 = (D_1 \times D_2; E_1 \cdot E_2)$, where $((x, y), (x', y')) \in E_1 \cdot E_2$ iff $(x, x') \in E_1$ and $(y, y') \in E_2$, belong to EqP.

In the rest of the section, we prove the implication (1) $\to$ (2). We consider an automatic equivalence structure $\mathfrak{E} = (D, E)$ and show that it can be decomposed as stated in Theorem 3. We will start with some preprocessing. First one can define the set of elements in finite E-classes by the formula $\varphi_{fin}(x) = \neg\exists^\infty y\, Exy$. Hence we can assume that all classes are finite.

▶ **Lemma 10.** *If $D \subseteq 0^*$ then $\mathfrak{E}$ contains only finitely many infinite classes.*

Proof. We call a set $C \subseteq 0^*$ *eventually d-periodic* ($d \in \mathbb{N}$) if there exists a number $t \in \mathbb{N}$ such that for all $i \geq t$ we have $0^i \in C$ iff $0^{i+d} \in C$. Let $\mathcal{A}$ be a deterministic finite automaton (DFA) for $\otimes E$ with transition function δ. We claim that there are numbers $t \geq 0$ and $d \geq 1$ such that $\delta(q, (0, \diamond)^t) = \delta(q, (0, \diamond)^{t+d})$ for all states q in $\mathcal{A}$. Clearly, for every state q there are numbers $t_q \geq 0$ and $d_q \geq 1$ such that $\delta(q, (0, \diamond)^{t_q}) = \delta(q, (0, \diamond)^{t_q+d_q})$. Then it suffices to take the maximum over all t_q and the product of all d_q over all states q.

Let C be an equivalence class and let $0^i \in C$ be the shortest word. By the property above we have $(0^i, 0^j) \in E$ iff $(0^i, 0^{j+d}) \in E$ for all $j \geq i + t$, i.e. C is eventually d-periodic. Any $d + 1$ infinite eventually d-periodic sets cannot be pairwise disjoint, which proves the claim. ◀

If D has growth $O(n^k)$, then we can assume that $D \subseteq 0^* \cdots k^*$ as stated in the next lemma.

▶ **Lemma 11** ([1])**.** *If $\mathfrak{A} = (D, R_1, \ldots, R_m)$ is an automatic structure where D has growth $O(n^k)$ then there exists an automatic structure $\mathfrak{A}' = (D', R'_1, \ldots, R'_m)$ which is isomorphic to $\mathfrak{A}$ and $D' \subseteq 0^*1^* \cdots k^*$.*

In the following assume that $D \subseteq 0^* \cdots k^*$ and that every E-class is finite. Let $R \subseteq D$ be the set of minimal elements from the equivalence classes with respect to the length-lexicographical order. A standard pumping argument shows that there exists a constant $b \in \mathbb{N}$ such that the length difference between any two equivalent elements is bounded by b.

▶ **Lemma 12.** *There exists $b \in \mathbb{N}$ such that $(u, v) \in E$ implies $||u| - |v|| \leq b$.*

Proof. Let b the number of states in an automaton $\mathcal{A}$ for $\otimes E$. Assume that $|v| > |u| + b$ (the other case is symmetric). The word $u \otimes v$ is accepted by $\mathcal{A}$ and has a suffix of the form $\diamond^{b+1} \otimes w$ for some suffix w of v. In this suffix $\mathcal{A}$ visits some state twice, and hence a nonempty infix of $\diamond^{b+1} \otimes w$ can be pumped, yielding infinitely many equivalent elements to u. This contradicts the assumption that all classes are finite. ◀

▶ **Lemma 13.** *There is a Presburger formula $\varphi(t_0, \ldots, t_k, s_0, \ldots, s_k)$ stating that $r = 0^{t_0} \cdots k^{t_k} \in R$, $v = 0^{s_0} \cdots k^{s_k} \in D$ and $(r, v) \in E$.*

Proof. Since $E \cap R \times D$ is an automatic relation the set $L = \otimes(E \cap R \times D)$ is by definition a regular language over the alphabet $\Gamma = \{0, \ldots, k, \diamond\}^2$. Notice that the restriction of the Parikh mapping Φ to L is injective since the letters in words of L are naturally ordered. By Parikh's theorem $\Phi(L)$ is effectively semilinear and hence effectively definable by Presburger formula. This allows to construct a formula φ stating that there exists a vector $x \in \Phi(L)$ indexed by pairs in Γ such that

- $\sum_{j \in \{0,\ldots,k,\diamond\}} x_{(i,j)} = t_i$ for all $0 \leq i \leq k$
- $\sum_{i \in \{0,\ldots,k,\diamond\}} x_{(i,j)} = s_j$ for all $0 \leq j \leq k$.

This concludes the proof. ◀

Now we are ready to finish the proof of Theorem 3. Let φ be the formula from Lemma 13. By Theorem 6 the counting function $c(\bar{t}) = |\{\bar{s} \mid \varphi(\bar{t}, \bar{s})\}|$ is a piecewise quasi-polynomial function, and one can compute a representation of c. If $r = 0^{t_0} \cdots k^{t_k} \in R$ then $c(t_0, \dots, t_k)$ is the size of the equivalence class of r; otherwise $c(t_0, \dots, t_k) = 0$. By definition of $\mathfrak{E}(c)$ we have $\mathfrak{E}(c) \cong \mathfrak{E}$. It remains to decompose $\mathfrak{E}(c)$ into equivalence structures $\mathfrak{E}(h_i)$ defined by polynomials h_i and prove that $\deg(h_i) + \mathrm{var}(h_i) \le k + 1$.

We can assume that c is presented by a finite partition $\mathbb{N}^{k+1} = \bigcup_i L_i$ and polynomials g_i such that each L_i is a fundamental linear set and c coincides with g_i on L_i [6]. Let h_i be the function obtained from g_i by substituting the linear representation of vectors in L_i into g_i. More formally, let $L_i = \bar{v}_0 + \langle \bar{v}_1, \dots, \bar{v}_\ell \rangle$ where the period vectors are linearly independent and let $\alpha_i \colon \mathbb{N}^\ell \to \mathbb{N}^{k+1}$ be defined by $\alpha_i(\lambda_1, \dots, \lambda_\ell) = \bar{v}_0 + \sum_{j=1}^{\ell} \lambda_j \bar{v}_j$. Then $g_i \circ \alpha_i$ is a polynomial and $\mathfrak{E}$ is isomorphic to the disjoint union $\bigcup_i \mathfrak{E}(g_i \circ \alpha_i)$.

Now fix i and let $h_i = g_i \circ \alpha_i$, which is a polynomial in the variables $\lambda_1, \dots, \lambda_\ell$. It remains to show that $\deg(h_i) + \ell \le k + 1$. Let $R_i = R \cap \{0^{t_0} \cdots k^{t_k} \mid \bar{t} \in L_i\}$ and $D_i = \{v \in D \mid \exists r \in R_i : (v, r) \in E\}$. Then $\mathfrak{E}(h_i)$ is isomorphic to the restriction of $\mathfrak{E}$ to D_i. The representatives in R_i of length n are

$$R_{i,n} = \{0^{t_0} \cdots k^{t_k} \mid \exists \bar{\lambda} \in \mathbb{N}^\ell \colon \alpha_i(\bar{\lambda}) = \bar{t}, \ \sum_j t_j = n\}.$$

Each $r \in R_{i,n}$ is only equivalent to words of length at least n, since r is length-lexicographically minimal in its class, and at most $n + b$, by Lemma 12. Since b is a constant we know that $|\{v \in D_i \mid n \le |v| \le n + b\}| = O(n^k)$ and hence

$$\sum_{r \in R_{i,n}} |[r]| = |\bigcup_{r \in R_{i,n}} [r]| = O(n^k). \tag{2}$$

For a tuple $\bar{\lambda} = (\lambda_1, \dots, \lambda_\ell)$ let $\mathrm{len}(\bar{\lambda})$ be the sum of all entries in $\alpha_i(\bar{\lambda})$, which is an affine function in $\bar{\lambda}$, namely $\mathrm{len}(\lambda_1, \dots, \lambda_\ell) = a_0 + \sum_{j=1}^{\ell} a_j \lambda_j$ where $a_j \in \mathbb{N}$ is the sum of all entries in $\bar{v}_i$. Since α_i is injective, none of the vectors $\bar{v}_i$ can be the zero vector and therefore we must have $a_1, \dots, a_\ell \ge 1$. We obtain

$$\sum_{\mathrm{len}(\lambda_1, \dots, \lambda_\ell) = n} h_i(\lambda_1, \dots, \lambda_\ell) = \sum_{\mathrm{len}(\lambda_1, \dots, \lambda_\ell) = n} g_i(\alpha_i(\lambda_1, \dots, \lambda_\ell))$$
$$= \sum_{0^{t_0} \cdots k^{t_k} \in R_{i,n}} g_i(t_0, \dots, t_k) = \sum_{r \in R_{i,n}} c(r) \overset{(2)}{=} O(n^k).$$

Let a be the least common multiple of $a_1, \dots, a_\ell$ and assume that $n = a_0 + a \cdot m$ for some $m \in \mathbb{N}$. We restrict the left handside to those tuples $(\lambda_1, \dots, \lambda_\ell)$ where each $a_j \lambda_j$ is divisible by a, i.e. $a_j \cdot \lambda_j = a \cdot \mu_j$ for some μ_j. We get

$$\sum_{\mu_1 + \cdots + \mu_\ell = m} h_i(a\mu_1, \dots, a\mu_\ell) = O(n^k).$$

The number of tuples $(\mu_1, \dots, \mu_\ell) \in \mathbb{N}^\ell$ with $m/(\ell - 1) \le \mu_j$ for all j and $\mu_1 + \cdots + \mu_\ell = m$ is $\Omega(m^{\ell-1}) = \Omega(n^{\ell-1})$ because in the coordinates 1 to $\ell - 1$ we can pick any integer in the interval $[m/(\ell - 1), m/\ell]$ and pick $\mu_\ell \ge m/\ell$ such that the sum equals n. This implies $\Omega(n^{\ell-1}) \cdot h_i(am', \dots, am') \le O(n^k)$ where $m' = m/(\ell - 1)$. Since $m' = \Theta(n)$ the degree of h_i must satisfy $\ell - 1 + \deg(h_i) \le k$.

5 Undecidability: Proof of Theorem 4

Using Theorem 3 we can state an equivalent formulation of the isomorphism problem for automatic equivalence structures with growth $O(n^k)$. For this we define two sets. The first set is the set of polynomials f such that the number of variables in f plus the degree of f is not greater than $k+1$:

$$\mathcal{P}_k = \{f \in \mathbb{N}[x_1,\dots,x_\ell] \mid 0 \le \ell \le k+1,\ \mathrm{var}(f) + \deg(f) \le k+1\}.$$

The second set defines a collection of multi-sets determined by tuples of polynomials from $\mathcal{P}_k$. Formally:

$$\mathcal{M}_k = \left\{ \biguplus_{i=1}^{m} \mathrm{Rg}(f_i) \mid f_1,\dots,f_m \in \mathcal{P}_k,\ m \in \mathbb{N} \right\}.$$

▶ **Definition 14.** *Let $\mathcal{P}$ be a set of polynomials. A* $\mathcal{P}$-representation *for a multiset M over $\mathbb{N}$ is a list of polynomials $(f_1,\dots,f_m) \in \mathcal{P}^m$ such that $M = \biguplus_{i=1}^m \mathrm{Rg}(f_i)$.*

For example, the list (x, x^2) is a representation of the multiset $\{0,0,1,1,2,3,4,4,5,6,\dots\}$. The decision problem $\mathcal{P}$-Multiset-Eq asks whether two given $\mathcal{P}$-representations define the same multiset.

▶ **Lemma 15.** *For each constant $k \ge 0$, the isomorphism problem for automatic equivalence structures of growth $O(n^k)$ is equivalent to $\mathcal{P}_k$-*Multiset-Eq*.*

Proof. The equivalence follows basically from Theorem 3. However, we need to pay attention to infinite equivalence classes and multisets containing 0.

First we observe that the isomorphism problem for automatic equivalence structures of growth $O(n^k)$ is equivalent to the question whether $F \restriction \mathbb{N}_+ = G \restriction \mathbb{N}_+$ for two given multisets $F, G \in \mathcal{M}_k$, i.e. we exclude 0 from the multisets. Let us call this decision problem $\mathcal{P}_k$-Pos-Multiset-Eq. To solve the isomorphism problem we first compute for the given equivalence structures representative sets for the set of infinite equivalence classes and compare their cardinality. If they are unequal, we reject. Otherwise we restrict the equivalence structures to those elements which are contained in finite classes. By Theorem 3 we can compute representations $\bigcup_i \mathfrak{E}(f_i)$ and $\bigcup_i \mathfrak{E}(g_i)$ for the restricted equivalence structures where $f_i, g_i \in \mathcal{P}_k$. Then the equivalence structures are isomorphic if and only if $(\biguplus_i \mathrm{Rg}(f_i)) \restriction \mathbb{N}_+ = (\biguplus_i \mathrm{Rg}(g_i)) \restriction \mathbb{N}_+$. Conversely, given two $\mathcal{M}_k$-multisets $F = \biguplus_i \mathrm{Rg}(f_i)$ and $G = \biguplus_i \mathrm{Rg}(g_i)$, we have $F \restriction \mathbb{N}_+ = G \restriction \mathbb{N}_+$ if and only if $\bigcup_i \mathfrak{E}(f_i)$ and $\bigcup_i \mathfrak{E}(g_i)$ are isomorphic. By Theorem 3 we can compute two automatic structures equivalent to $\bigcup_i \mathfrak{E}(f_i)$ and $\bigcup_i \mathfrak{E}(g_i)$, respectively.

It remains to prove the equivalence of $\mathcal{P}_k$-Pos-Multiset-Eq and $\mathcal{P}_k$-Multiset-Eq. Since $\mathrm{Rg}(x_1)$ is the multiset containing 0 infinitely often, we have $(\biguplus_i \mathrm{Rg}(f_i)) \restriction \mathbb{N}_+ = (\biguplus_i \mathrm{Rg}(g_i)) \restriction \mathbb{N}_+$ if and only if $\biguplus_i \mathrm{Rg}(f_i) \cup \mathrm{Rg}(x_1) = \biguplus_i \mathrm{Rg}(g_i) \cup \mathrm{Rg}(x_1)$. This yields a reduction from $\mathcal{P}_k$-Pos-Multiset-Eq to $\mathcal{P}_k$-Multiset-Eq. For the other direction, suppose we are given two multisets $F = \biguplus_i \mathrm{Rg}(f_i)$ and $G = \biguplus_i \mathrm{Rg}(g_i)$ from $\mathcal{M}_k$. Then $F = G$ if and only if $F(0) = G(0)$ and $F \restriction \mathbb{N}_+ = G \restriction \mathbb{N}_+$. The latter is equivalent to the $\mathcal{P}_k$-Multiset-Eq-instance $\bigcup_i \mathfrak{E}(f_i) = \bigcup_i \mathfrak{E}(g_i)$. To test $F(0) = G(0)$ it suffices to show how to compute $\mathrm{Rg}(g)(0)$ for a given polynomial $g \in \mathbb{N}[x_1,\dots,x_\ell]$. First notice that $\mathrm{Rg}(g)(0)$ is the number of solutions $\bar{u} \in \mathbb{N}^\ell$ for $g(\bar{u}) = 0$. If $\bar{u}, \bar{v} \in \mathbb{N}^\ell$ are tuples with the same non-zero coordinates then $g(\bar{u}) = 0$ if and only if $g(\bar{v}) = 0$. Hence $g(\bar{u}) = 0$ either has zero, one, or infinitely many solutions, and it suffices to search for solutions in $\bar{u} \in \{0,1\}^\ell$. ◀

We also consider the related problem over sets. Let us write $\mathrm{Img}(f)$ for the image of a polynomial $f \in \mathbb{N}[x_1, \dots, x_k]$, i.e. the *set* $\{f(\bar{x}) \mid \bar{x} \in \mathbb{N}^k\}$. If $\mathcal{P}$ is a set of polynomials, a $\mathcal{P}$-representation for a set $M \subseteq \mathbb{N}$ is a list of polynomials $(f_1, \dots, f_m) \in \mathcal{P}^m$ such that $M = \bigcup_{i=1}^m \mathrm{Img}(f_i)$. The decision problem $\mathcal{P}$-Set-Eq asks whether two given $\mathcal{P}$-representations define the same set.

▶ **Lemma 16.** *If $k \in \mathbb{N}$, then $\mathcal{P}_k$-Set-Eq is reducible to $\mathcal{P}_{k+1}$-Multiset-Eq.*

Proof. Let $(f_1, \dots, f_m, g_1, \dots, g_m)$ be an instance for $\mathcal{P}_k$-Set-Eq. If $f_i \colon \mathbb{N}^k \to \mathbb{N}$ then let $f_i' \colon \mathbb{N}^{k+1} \to \mathbb{N}$ be the polynomial defined by $f_i'(\bar{x}, y) = f_i(\bar{x})$ for all $\bar{x} \in \mathbb{N}^k, y \in \mathbb{N}$, and similarly g_i'. Since every element has either multiplicity 0 or ∞ in $\mathrm{Rg}(f_i')$ and $\mathrm{Rg}(g_i')$ we have

$$\bigcup_{i=1}^{m} \mathrm{Img}(f_i) = \bigcup_{i=1}^{n} \mathrm{Img}(g_i) \iff \biguplus_{i=1}^{m} \mathrm{Rg}(f_i') = \biguplus_{i=1}^{n} \mathrm{Rg}(g_i').$$

The polynomials f_i', g_i' have one more variable and hence belong to $\mathcal{P}_{k+1}$. ◀

Proof of Theorem 4. We use the MRDP-theorem [14] stating that a set of natural numbers $X \subseteq \mathbb{N}$ is recursively enumerable if and only if it is *Diophantine*, i.e. there exists a polynomial $p(x, y_1, \dots, y_k) \in \mathbb{Z}[x, y_1, \dots, y_k]$ such that

$$X = \{a \in \mathbb{N} \mid \exists y_1, \dots, y_k \in \mathbb{N} : p(a, y_1, \dots, y_k) = 0\}.$$

Let $X \subseteq \mathbb{N}$ be a Σ_1^0-complete set and $p \in \mathbb{Z}[x, x_1, \dots, x_k]$ be a polynomial as above defining X.[1] By splitting p into its monomials with positive and negative coefficients we obtain polynomials $p_1, p_2 \in \mathbb{N}[x, x_1, \dots, x_k]$ such that

$$a \in X \iff \exists y_1, \dots, y_k \in \mathbb{N} : p_1(a, y_1, \dots, y_k) = p_2(a, y_1, \dots, y_k). \tag{3}$$

If we define $N = \{(x, y) \mid x \neq y \in \mathbb{N}\}$, then $a \in X$ is also equivalent to

$$\{(p_1(a, \bar{y}), p_2(a, \bar{y})) \mid \bar{y} \in \mathbb{N}^k\} \not\subseteq N. \tag{4}$$

Using the injective pairing function $C(x, y) = (x + y)^2 + 3x + y$ we can alternatively state this by

$$\mathrm{Img}(C(p_1(a, \bar{y}), p_2(a, \bar{y}))) \not\subseteq \mathrm{Img}(C(y, x + y + 1)) \cup \mathrm{Img}(C(x + y + 1, y)).$$

Since $A \not\subseteq B$ iff $A \neq A \cup B$ we obtain a reduction from X to the complement of $\mathcal{P}_m$-Set-Eq where m is bounded in a function of $\mathrm{var}(p)$ and $\deg(p)$. Hence $\mathcal{P}_m$-Set-Eq is Π_1^0-hard. Therefore also $\mathcal{P}_{m+1}$-Multiset-Eq and the isomorphism problem over automatic equivalence structures of growth $O(n^{m+1})$ is Π_1^0-hard. ◀

6 Decidability: Proof of Theorem 5

Now we prove Theorem 5 by proving:

▶ **Theorem 17.** *The problem $\mathcal{P}_2$-Multiset-Eq is decidable.*

To prove Theorem 17 we proceed in three steps. First we reduce it to the case that the multisets have only finite multiplicities. In the second step we test equality of the multisets on their "unbounded linear part" and reduce the problem to testing equality of unions of degree-two polynomial ranges. In the third step we provide a decision procedure for the latter problem.

[1] It is known that p can be chosen to have degree at most four [14, Section 1.2].

6.1 Closure properties

▶ **Lemma 18.** *If $f \in \mathbb{N}[x_1, \dots, x_k]$ has degree d and $T \subseteq \mathbb{N}^k$ is semilinear, then $f(T)$ is a finite union of ranges $\mathrm{Rg}(g_i)$ where $\mathrm{var}(g_i) \le k$ and $\deg(g_i) = d$. The polynomials g_i can be computed effectively. In particular, $f(T)$ belongs effectively to $\mathcal{M}_{d+k-1}$.*

Proof. Let $T = \bigcup_i T_i$ be a representation of T as a disjoint union of fundamental linear sets T_i. Since $f(T) = \biguplus_i f(T_i)$ we can assume that T is a fundamental linear set, say $T = \bar{v}_0 + \langle \bar{v}_1, \dots, \bar{v}_m \rangle$ where the period vectors are linearly independent; in particular, we have $m \le k$. Consider the polynomial $g \in \mathbb{N}[\lambda_1, \dots, \lambda_m]$ defined by

$$g(\lambda_1, \dots, \lambda_m) = f(\bar{v}_0 + \sum_{j=1}^{m} \lambda_j \bar{v}_j),$$

which satisfies $f(T) = \mathrm{Rg}(g)$ and $\deg(g) = \deg(f) = d$. ◀

▶ **Lemma 19.** *If $F \in \mathcal{M}_2$ and $S \subseteq \mathbb{N}$ is semilinear, then $F \restriction S$ belongs effectively to $\mathcal{M}_2$.*

Proof. Let $F = \biguplus_{i=1}^m \mathrm{Rg}(f_i)$ with $f_1, \dots, f_m \in \mathcal{P}_2$. Since $F \restriction S = \biguplus_{i=1}^m (\mathrm{Rg}(f_i) \restriction S)$ we can assume that $F = \mathrm{Rg}(f)$ for some $f \in \mathcal{P}_2$. First assume that $\deg(f) \le 1$. Since S is semilinear and f is an affine function, the set $L = \{\bar{t} \mid f(\bar{t}) \in S\}$ is effectively semilinear. By Lemma 18 we know that $\mathrm{Rg}(f) \restriction S = f(L)$ belongs to $\mathcal{M}_2$. Now assume that $\deg(f) = 2$, i.e. $f(t) = at^2 + bt + c$ for some $a \ne 0$, $b, c \in \mathbb{N}$. Since f is injective, the multiset $F = \mathrm{Rg}(f)$ is a set, and therefore $F \restriction S = F \cap S$. Consider a representation of S as a finite disjoint union $S = \bigcup_i S_i$ of singleton sets and arithmetic progressions. Since $F \cap S = \biguplus_i (F \cap S_i)$ we can assume that S itself is either a singleton or an arithmetic progression. If $S = \{s\}$ then $\mathrm{Rg}(f) \cap S$ is either empty or $\{s\}$, which can be decided. Assume $S = \{e + dn \mid n \in \mathbb{N}\}$ for some $e \in \mathbb{N}$ and $d \ge 1$. It is enough to prove that $T = \{t \in \mathbb{N} \mid \exists n \in \mathbb{N}\colon at^2 + bt + c = e + dn\}$ is effectively semilinear, since then, $\mathrm{Rg}(f) \cap S = f(T)$ belongs to $\mathcal{M}_2$ by Lemma 18.

Notice that $t \in T$ if and only if $at^2 + bt + c$ is congruent to e mod d and $at^2 + bt + c \ge e$. Define the function $h\colon \mathbb{Z}_d \to \mathbb{Z}_d$ with $h(t) = at^2 + bt + c$. We obtain a semilinear representation for $\{t \in \mathbb{N} \mid f(t) \equiv e \pmod{d}\}$ from $h^{-1}(e + \mathbb{Z}_d)$. Finally, we intersect this set with the interval $[t_0, \infty)$ where t_0 is the smallest number with $at_0^2 + bt_0 + c \ge e$ to obtain T. ◀

6.2 Reduction to multisets with finite multiplicities

Let $\mathcal{P}_{2,\mathrm{fin}} \subseteq \mathcal{P}_2$ be the set of all polynomials of the form:

- $f = a$
- $f(t) = at^2 + bt + c$ where $a \ne 0$ or $b \ne 0$,
- $f(s,t) = as + bt + c$ where $a, b \ne 0$

Notice that $\mathrm{Rg}(g)$ of a polynomial $g \in \mathcal{P}_2$ has finite multiplicities, i.e. $\mathrm{Rg}(g)(a) < \infty$ for all $a \in \mathbb{N}$, if and only if $g \in \mathcal{P}_{2,\mathrm{fin}}$. Let $\mathcal{M}_{2,\mathrm{fin}}$ be the set of all multisets $\biguplus_{i=1}^m \mathrm{Rg}(f_i)$ where $f_1, \dots, f_m \in \mathcal{P}_{2,\mathrm{fin}}$. We will show that $\mathcal{P}_2$-Multiset-Eq is reducible to $\mathcal{P}_{2,\mathrm{fin}}$-Multiset-Eq and start with a useful lemma.

▶ **Lemma 20.** *If $F = \mathrm{Rg}(f)$ with $f \in \mathcal{P}_2$, then one can construct a Presburger formula $\varphi(x,y)$ stating that $F(x) = y < \infty$.*

Proof. Suppose f has two variables, say $f(s,t) = as + bt + c$. If $a = 0$, then F contains every number of the form $bt + c$ infinitely often, and does not contain any other number. The case $b = 0$ is similar. If both $a \ne 0$ and $b \ne 0$, then F has only finite multiplicities. Using Theorem 7 we can count for a given number x the number $|\{s \in \mathbb{N} \mid \exists t \in \mathbb{N} : as + bt + c = x\}|$.

Suppose f has one variable, say $f(t) = at^2 + bt + c$. If $a = b = 0$, then F contains only c infinitely often. Otherwise F contains each number of the form $at^2 + bt + c$ exactly once. ◀

▶ **Lemma 21.** $\mathcal{P}_2$-Multiset-Eq *is reducible to* $\mathcal{P}_{2,\mathrm{fin}}$-Multiset-Eq.

Proof. Given two multisets $F, G \in \mathcal{M}_2$ and let $F_\infty = \{n \in \mathbb{N} \mid F(n) = \infty\}$ and $G_\infty = \{n \in \mathbb{N} \mid G(n) = \infty\}$. We have

$$F = G \iff F_\infty = G_\infty \text{ and } (F \upharpoonright \overline{F_\infty} = G \upharpoonright \overline{G_\infty})$$

where the complements are taken with respect to $\mathbb{N}$. Using Lemma 20 we can compute the semilinear sets F_∞ and G_∞ and test whether $F_\infty = G_\infty$. Using Lemma 19 we can compute $\mathcal{P}_2$-representations for $F \upharpoonright \overline{F_\infty}$ and $G \upharpoonright \overline{G_\infty}$. ◀

6.3 Elimination of linear polynomials

Let $\mathcal{P}_{2,0} \subseteq \mathcal{P}_2$ be the set of all polynomials $f(t) = at^2 + bt + c$ where $a \neq 0$ and $b, c \in \mathbb{N}$ and polynomials $f = a$, and let $\mathcal{M}_{2,0}$ be the corresponding set of multisets.

▶ **Lemma 22.** $\mathcal{P}_{2,\mathrm{fin}}$-Multiset-Eq *is reducible to* $\mathcal{P}_{2,0}$-Multiset-Eq.

Proof. Given two multisets $F, G \in \mathcal{M}_{2,\mathrm{fin}}$ where $F = \biguplus_i \mathrm{Rg}(f_i)$ and $G = \biguplus_i \mathrm{Rg}(g_i)$. Let F_1 be the restriction of the union $\biguplus_i \mathrm{Rg}(f_i)$ to those polynomials f_i with $\deg(f_i) \leq 1$ and F_2 be the restriction to those polynomials of degree 2, and similarly G_1, G_2 for $\biguplus_i \mathrm{Rg}(g_i)$.

Since polynomials of degree 2 are injective, the maximum multiplicity in F_2 and G_2 is bounded by the total number, say k, of polynomials f_i and g_i, respectively. Hence, if $F = G$ then $|F_1(a) - G_1(a)| \leq k$ for all $a \in \mathbb{N}$. We can verify the latter property using the Presburger formulas $\varphi_{F_1}(x, y)$ and $\varphi_{G_1}(x, y)$ from Lemma 20, and return a negative instance if either one of the properties is violated (since $F \neq G$).

Now assume that the maximum multiplicity in $F_1 \setminus G_1$ and in $G_1 \setminus F_1$ is bounded by k. One can verify that $F = G$ if and only if

$$(F_1 \setminus G_1) \uplus F_2 = (G_1 \setminus F_1) \uplus G_2, \tag{5}$$

using the definition of difference between two multisets. If both $\mathrm{supp}(F_1 \setminus G_1)$ and $\mathrm{supp}(G_1 \setminus F_1)$ are finite, then also $F_1 \setminus G_1$ and $G_1 \setminus F_1$ are finite and we can return the instance (5). Otherwise we claim that $F \neq G$, and hence we return a negative instance. Towards a contradiction assume $F = G$ and that $\mathrm{supp}(F_1 \setminus G_1)$ is infinite. The set $\mathrm{supp}(F_1 \setminus G_1)$ is in fact effectively semilinear by Lemma 20 since

$$\mathrm{supp}(F_1 \setminus G_1) = \{x \in \mathbb{N} \mid F_1(x) > G_1(x)\}.$$

Therefore the growth of $\mathrm{supp}(F_1 \setminus G_1)$ is $\Omega(n)$ whereas the growth of $\mathrm{supp}(G_2)$ is $O(\sqrt{n})$ because it is a finite union of ranges of quadratic polynomials and singletons. This contradicts the fact that $\mathrm{supp}(F_1 \setminus G_1) \subseteq \mathrm{supp}(G_2)$. ◀

6.4 Decicision procedure for degree-two polynomials

In preparation for the decidability proof of $\mathcal{P}_{2,0}$-Multiset-Eq we show the following lemma concerning the solutions of quadratic Diophantine equations. The *growth function* of a subset $M \subseteq \mathbb{N}$ is the function $n \mapsto |M \cap [1, n]|$.

▶ **Lemma 23.** *Let $f, g \in \mathbb{N}[x]$ with $\deg(f) = \deg(g) = 2$. Let $S = \{(x, y) \in \mathbb{N}^2 \mid f(x) = g(y)\}$ and S_x be the projection to the first component. Then exactly one of the following cases holds:*

1. *the growth of S_x is $\Omega(n)$ and S is infinite and semilinear.*
2. *the growth of S_x is $o(n)$.*

It is decidable whether (1) or (2) holds. Moreover, if (1) holds then S can be effectively computed.

Proof. We follow the analysis of quadratic bivariate Diophantine equations from [19]. Consider the equation

$$ax^2 + cy^2 + dx + ey + f = 0 \tag{6}$$

where $a, c \neq 0$, $d \geq 0$, $e \leq 0$ and $f \in \mathbb{N}$. Define $D = -4ac \neq 0, E = -2ae, F = d^2 - 4af$ and $Y = 2ax + d$. Then (6) implies $DY^2 = (Dy + E)^2 + DF - E^2$. If $N = E^2 - DF$ and $X = Dy + E$ then we obtain the generalized Pell equation

$$X^2 - DY^2 = N. \tag{7}$$

Let L be the set of solutions $(X, Y) \in \mathbb{N}^2$ of (7) and let L_Y be the projection to the second component. Notice that the transformation $(x, y) \mapsto (X, Y) = (Dy + E, 2ax + d)$ is an injective function from S to L, and that if the growth of S_x is $\Omega(n)$ then also the growth of L_Y is $\Omega(n)$. Also notice that if $X^2 = DY^2 + N$ and $Y \geq 1$ then $X^2 \leq \max(D, |N|) \cdot Y^2$, hence X is linearly bounded in Y for all solutions $(X, Y) \in L$.

We will do a case distinction:

1. If $D < 0$ then any solution (X, Y) of (7) satisfies $X^2 + Y^2 \leq N$. Then L is finite, and hence also S is finite.
2. If $D > 0$ is a square number then L is finite, hence also S is finite.
3. If $D > 0$ and $N = 0$, then (7) is solvable if and only if D is a square number. In this case the solutions of (7) are $L = \{(\sqrt{D}Y, Y) \mid Y \in \mathbb{N}\}$. Hence the solutions of (6) are of the form
$$S = \{(x, y) \in \mathbb{N}^2 \mid Dy + E = \sqrt{D}(2ax + d)\}.$$
From the equation we can compute a semilinear representation of S.
4. Now suppose that $D > 0$ is not a square number and $N \neq 0$. In this case we will show that L_Y, and therefore also S_x, has growth $o(n)$. Let $t, u \in \mathbb{N}$ be the smallest solution of the Pell equation $t^2 - Du^2 = 1$, the so called *fundamental solution*. We define an equivalence relation on $\mathbb{Z}^2$ where two pairs (X, Y) and (X', Y') are equivalent if $X + Y\sqrt{D} = (X' + Y'\sqrt{D})(t + u\sqrt{D})^m$ for some $m \in \mathbb{Z}$. It is known that the set of solutions of (7) over $\mathbb{Z}$ is a finite union of equivalence classes, see [12, Theorem 8-8, 8-9]. Hence the number of solutions $(X, Y) \in L$ with $X + \sqrt{D}Y \leq n$ is bounded by $O(\log n)$. Since X is linearly bounded in Y for all solutions $(X, Y) \in L$, this implies that L_Y has growth $O(\log n)$, which is contained in $o(n)$.

This concludes the proof. ◀

▶ **Theorem 24.** $\mathcal{P}_{2,0}$-Multiset-Eq *is decidable.*

Proof. We will prove how to solve the following inclusion problem: Given polynomials $f, g_1, \ldots, g_m \in \mathcal{P}_{2,0}$, test whether

$$\mathrm{Rg}(f) \subseteq \biguplus_{i=1}^{m} \mathrm{Rg}(g_i) \tag{8}$$

holds and, if so, compute a $\mathcal{P}_{2,0}$-representation for $[\biguplus_{i=1}^m \mathrm{Rg}(g_i)] \setminus \mathrm{Rg}(f)$. Then, given an instance $(f_1, \dots, f_m, g_1, \dots, g_n)$ of $\mathcal{P}_{2,0}$-MULTISET-EQ, we can test $\biguplus_i \mathrm{Rg}(f_i) \subseteq \biguplus_i \mathrm{Rg}(g_i)$ as follows (the other inclusion is symmetric):

1. Initialize $G_0 = \biguplus_{i=1}^m \mathrm{Rg}(g_i)$.
2. For all $1 \le k \le m$:
   a. Test whether $\mathrm{Rg}(f_k) \subseteq G_{k-1}$,
   b. If so, compute $G_k = G_{k-1} \setminus \mathrm{Rg}(f_k)$ otherwise return "no".
3. Return "yes".

It remains to show how to solve the defined inclusion problem. We assume that the polynomials g_i are sorted by $\mathrm{var}(g_i)$, i.e. there exists some $0 \le \ell \le m$ such that $\mathrm{var}(g_i) = 1$ for all $1 \le i \le \ell$ and $\mathrm{var}(g_i) = 0$ for all $\ell + 1 \le i \le m$, i.e. $\biguplus_{i=\ell+1}^m \mathrm{Rg}(g_i)$ is a finite multiset.

Case 1. If $f = a$, then we can test whether there exists some i such that $a \in \mathrm{Rg}(g_i)$. If there is no such index, we reject. Otherwise pick such an index i. If $1 \le i \le \ell$ then we decompose $\mathrm{Rg}(g_i) \setminus \{a\}$ into the finite set $\{g_i(0), \dots, g_i(x_0 - 1)\}$ and $\mathrm{Rg}(g_i(x + x_0 + 1))$. If $\ell + 1 \le i \le m$ we can remove g_i from the list.

Case 2. If $f(x) = ax^2 + bx + c$ with $a \ne 0$ we test for each $1 \le i \le \ell$ whether the solution set

$$S_i = \{(x, y) \in \mathbb{N}^2 \mid f(x) = g_i(y)\}$$

is infinite and semilinear, and, if so, compute a semilinear representation for it using Lemma 23. Let $D_i = \{x \in \mathbb{N} \mid f(x) \in \mathrm{Rg}(g_i)\}$ for all $1 \le i \le m$. Notice that (8) is equivalent to $\bigcup_{i=1}^m D_i = \mathbb{N}$. We rearrange the indices such that exactly the sets $S_1, \dots, S_k$ are infinite and semilinear and hence by Lemma 23 the sets $D_{k+1}, \dots, D_\ell$ have growth $o(n)$. The sets $D_{\ell+1}, \dots, D_m$ have at most size 1. Define $X = \bigcup_{i=1}^k D_i$, which is effectively semilinear since each set D_i is the projection of S_i to the first component. We also define subsets $X_i \subseteq D_i$ for all $1 \le i \le k$ by

$$X_i = D_i \setminus \bigcup_{j=1}^{i-1} X_j,$$

which form a disjoint union $X_1 \cup \dots \cup X_k$ of X. Compute the semilinear sets $Y_i = \{y \in \mathbb{N} | \exists x \in X_i : (x, y) \in S_i\}$ for $1 \le i \le k$. Then we have $f(X_i) = g(Y_i)$ for all $1 \le i \le k$. We can rewrite (8) as

$$f(X) \uplus f(\mathbb{N} \setminus X) \subseteq \biguplus_{i=1}^k (g_i(Y_i) \uplus g_i(\mathbb{N} \setminus Y_i)) \uplus \biguplus_{i=k+1}^m \mathrm{Rg}(g_i).$$

Since $f(X_i) = g(Y_i)$ and $f(\mathbb{N} \setminus X)$ is disjoint from all sets $g_i(\mathbb{N} \setminus Y_i)$, this is equivalent to

$$f(\mathbb{N} \setminus X) \subseteq \biguplus_{i=k+1}^m \mathrm{Rg}(g_i) =: G.$$

We will do a case distinction.

Case 2a. If $\mathbb{N} \setminus X$ is finite, then we can test for each $x \in \mathbb{N} \setminus X$ whether $f(x)$ belongs to G and compute a representation for $G \setminus \{f(x)\}$, as above in case 1.

Case 2b. If $\mathbb{N} \setminus X$ is infinite we claim that $X \cup D_{k+1} \cup \dots \cup D_m \ne \mathbb{N}$ and hence (8) does not hold. Assume that $X \cup D_{k+1} \cup \dots \cup D_m = \mathbb{N}$ and therefore $\mathbb{N} \setminus X \subseteq D_{k+1} \cup \dots \cup D_m$. Since $\mathbb{N} \setminus X$ is infinite and semilinear, its growth must be $\Omega(n)$. However, all sets $D_{k+1}, \dots, D_m$ have growth $o(n)$, contradiction.

Notice that we can distinguish cases 2a and 2b since X is effectively semilinear. ◀

7 Conclusion

We have characterized automatic equivalence structures over polynomially growing domains, and have investigated the decidability of the isomorphism problem. Since equivalence structures can be viewed as trees of height 2, as a next step one could study automatic trees over polynomially growing domains. Also it is still open whether the isomorphism problem over *unary* automatic structures is decidable (automatic structures whose domains are unary regular languages).

References

1 Vince Bárány. *Automatic presentations of infinite structures.* PhD thesis, RWTH Aachen University, Germany, 2007. URL: `http://darwin.bth.rwth-aachen.de/opus3/volltexte/2007/2019/`.

2 Achim Blumensath. Automatic Structures. Master's thesis, RWTH Aachen University, 1999.

3 Achim Blumensath and Erich Grädel. Finite Presentations of Infinite Structures: Automata and Interpretations. *Theory Comput. Syst.*, 37(6):641–674, 2004. `doi:10.1007/s00224-004-1133-y`.

4 Jiamou Liu Dietrich Kuske and Markus Lohrey. The isomorphism problem on classes of automatic structures with transitive relations. *Trans. Amer. Math. Soc.*, 365:5103–5151, 2013.

5 Ginsburg, Seymour and Spanier, Edwin. Semigroups, Presburger formulas, and languages. *Pacific journal of Mathematics*, 16(2):285–296, 1966.

6 Ryuichi Ito. Every Semilinear Set is a Finite Union of Disjoint Linear Sets. *J. Comput. Syst. Sci.*, 3(2):221–231, 1969. `doi:10.1016/S0022-0000(69)80014-0`.

7 Lukasz Kaiser, Sasha Rubin, and Vince Bárány. Cardinality and counting quantifiers on omega-automatic structures. In *STACS 2008, 25th Annual Symposium on Theoretical Aspects of Computer Science, Bordeaux, France, February 21-23, 2008, Proceedings*, pages 385–396, 2008. `doi:10.4230/LIPIcs.STACS.2008.1360`.

8 Bakhadyr Khoussainov and Anil Nerode. Automatic Presentations of Structures. In *Logical and Computational Complexity. Selected Papers. Logic and Computational Complexity, International Workshop LCC '94, Indianapolis, Indiana, USA, 13-16 October 1994*, pages 367–392, 1994. `doi:10.1007/3-540-60178-3_93`.

9 Bakhadyr Khoussainov, André Nies, Sasha Rubin, and Frank Stephan. Automatic Structures: Richness and Limitations. *Logical Methods in Computer Science*, 3(2), 2007. `doi:10.2168/LMCS-3(2:2)2007`.

10 Bakhadyr Khoussainov, Sasha Rubin, and Frank Stephan. Automatic linear orders and trees. *ACM Trans. Comput. Log.*, 6(4):675–700, 2005. `doi:10.1145/1094622.1094625`.

11 Dietrich Kuske and Markus Lohrey. First-order and counting theories of omega-automatic structures. *J. Symb. Log.*, 73(1):129–150, 2008. `doi:10.2178/jsl/1208358745`.

12 W.J. LeVeque. *Topics in Number Theory.* Number Bd. 1 in Dover Books on Mathematics. Dover Publications, 2002. URL: `https://books.google.de/books?id=ocAySqjVLeEC`.

13 Jiamou Liu and Mia Minnes. Deciding the isomorphism problem in classes of unary automatic structures. *Theor. Comput. Sci.*, 412(18):1705–1717, 2011. `doi:10.1016/j.tcs.2010.12.045`.

14 Yuri V Matiyasevich. *Hilbert's tenth problem*, volume 105. MIT press Cambridge, 1993.

15 André Nies. Describing Groups. *Bulletin of Symbolic Logic*, 13(3):305–339, 2007. URL: `http://www.math.ucla.edu/%7Easl/bsl/1303/1303-001.ps`, `doi:10.2178/bsl/1186666149`.

16 G. Oliver and R. Thomas. Automatic presentations of finitely generated groups. In *STACS '05: Proceedings of the 22nd Annual Symposium on Theoretical Aspects of Computer Science*. Springer-Verlag, 2005.

17 Rohit Parikh. On Context-Free Languages. *Journal of the ACM*, 13(4):570–581, 1966.

18 Sasha Rubin. *Automatic Structures.* PhD thesis, University of Auckland, 2004.

19 Reginald E. Sawilla, Alan K. Silvester, and Hugh C. Williams. A New Look at an Old Equation. In Alfred J. van der Poorten and Andreas Stein, editors, *Algorithmic Number Theory, 8th International Symposium, ANTS-VIII, Banff, Canada, May 17-22, 2008, Proceedings*, volume 5011 of *Lecture Notes in Computer Science*, pages 37–59. Springer, 2008. doi:10.1007/978-3-540-79456-1_2.

20 Nicole Schweikardt. Arithmetic, first-order logic, and counting quantifiers. *ACM Trans. Comput. Log.*, 6(3):634–671, 2005. doi:10.1145/1071596.1071602.

21 Andrew Szilard, Sheng Yu, Kaizhong Zhang, and Jeffrey Shallit. Characterizing Regular Languages with Polynomial Densities. In Ivan M. Havel and Václav Koubek, editors, *Mathematical Foundations of Computer Science 1992, 17th International Symposium, MFCS'92, Prague, Czechoslovakia, August 24-28, 1992, Proceedings*, volume 629 of *Lecture Notes in Computer Science*, pages 494–503. Springer, 1992. doi:10.1007/3-540-55808-X_48.

22 Kevin Woods. Presburger Arithmetic, Rational Generating Functions, and quasi-polynomials. *J. Symb. Log.*, 80(2):433–449, 2015. doi:10.1017/jsl.2015.4.