Where automatic structures benefit from weighted automata

Dietrich Kuske

Institut für Theoretische Informatik, Technische Universität Ilmenau, Germany

Abstract. In this paper, we report on applications of weighted automata in the theory of automatic structures. All (except one) result were known before, but their proof using weighted automata is novel. More precisely, we prove that the extension of first-order logic by the infinity $\exists^\infty$, the modulo $\exists^{(p,q)}$, and the (new) boundedness quantifier $\exists\!\!\!\mathsf{B}$ is decidable. The first two quantifiers are handled using closure properties of the class of recognizable formal power series and the fact that the preimage of a value under a recognizable formal power series is regular if the semiring is finite. Our reasoning regarding the boundedness quantifier uses Weber's decidability result of finite-valued rational transductions. We also show that the isomorphism problem of automatic structures is undecidable using an undecidability result on recognizable formal power series due to Honkala.

1 Introduction

The idea of an automatic structure goes back to Büchi and Elgot who used finite automata to decide, e.g., Presburger arithmetic [12]. In essence, a structure is automatic if the elements of the universe can be represented as strings from a regular language and every relation of the structure can be recognized by a finite automaton with several heads that proceed synchronously. Automaton decidable theories [17] and automatic groups [13] are similar concepts. A systematic study was initiated by Khoussainov and Nerode [19] who also coined the name "*automatic structure*". They received increasing interest over the last years [4, 5, 9, 21, 22, 28, 1, 20, 25, 3, 32, 26, 24, 6]; the surveys [29, 2] give excellent overviews of the results in this area. One of the main motivations for investigating automatic structures is that their first-order theories are decidable. From the beginning, researchers were also interested in possible extensions of this result to stronger logics. The first part of this paper contributes to this search by (1) providing a new proof technique and (2) providing a further extension of first-order logic with this favorable property.

Another natural line of research dealt with the question which structures from a given class $\mathfrak{C}$ are automatic, i.e., can be represented by finite automata. There are only very few results in this direction (for instance, the characterisations are known for ordinals [10], Boolean algebras [20], and finitely generated groups [28].) and, as it turns out, the first two characterisations are accompanied by the decidability of the isomorphism problem of the automatic members in the given class $\mathfrak{C}$. On the other hand, it was shown that the isomorphism problem for all automatic structures is undecidable and even Σ^1_1-complete [20]. But these undecidability proofs depend crucially on binary non-transitive relations. The second part of this paper shows that weighted automata can be used to prove this undecidability for equivalence relations, a class of structures with a particularly simple transitive relation [24]. Honkala proved that it is undecidable whether a weighted automata over $(\mathbb{N}, +, \cdot, 0, 1)$ takes on all values from $\mathbb{N}$. We reduce this to our isomorphism problem. This proof technique differs from the original one in [24] only in that it makes the role of the weighted automata more transparent.

Acknowledgement I thank Martin Huschenbett for reading two earlier versions of this paper very carefully.

2 Preliminaries

Let Γ be an alphabet and $w \in \Gamma^*$ be a finite word over Γ. The length of w is denoted by $|w|$.

2.1 Structures

A *signature* is a finite set τ of relational symbols, where every symbol $R \in \tau$ has some fixed arity m_R. Then a τ*-structure* $\mathcal{A}$ consists of a non-empty universe A and, for every $R \in \tau$, an m_R-ary relation $R^{\mathcal{A}} \subseteq A^{m_R}$. Note that we only consider relational structures. Let us fix a τ-structure $\mathcal{A} = (A, (R^{\mathcal{A}})_{R\in\tau})$, where $R^{\mathcal{A}} \subseteq A^{m_R}$. To simplify notation, we will write $a \in \mathcal{A}$ for $a \in A$. In the rest of the paper, we will often identify a symbol $R \in \tau$ with its interpretation $R^{\mathcal{A}}$.

2.2 Automatic structures

Let us fix $m \in \mathbb{N}$ and a finite alphabet Γ. Let $\# \notin \Gamma$ be an additional padding symbol and set $\Gamma_\# = \Gamma \cup \{\#\}$. We will write $\Gamma_\#^m$ for $(\Gamma_\#)^m$. For words $w_i \in \Gamma^*$ $(1 \le i \le n)$ we define the *convolution* $w_1 \otimes w_2 \otimes \cdots \otimes w_m$, which is a word over the alphabet $\Gamma_\#^m$, as follows: Let $w_i = a_{i,1}a_{i,2}\cdots a_{i,k_i}$ with $a_{i,j} \in \Gamma$ and $k = \max\{k_1, \dots, k_m\}$. For $k_i < j \le k$ define $a_{i,j} = \#$. Then

$$w_1 \otimes \cdots \otimes w_m = (a_{1,1}, \dots, a_{m,1}) \cdots (a_{1,k}, \dots, a_{m,k}) .$$

Thus, for instance $aba \otimes bbabb = (a,b)(b,b)(a,a)(\#,b)(\#,b)$.

An *m-dimensional (synchronous) automaton* over Γ is just a finite automaton A over the alphabet $\Gamma_\#^m$ such that $L(A) \subseteq \{w_1 \otimes \cdots \otimes w_m \mid w_1, \dots, w_m \in \Gamma^*\}$. Such an automaton defines an m-ary relation

$$R(A) = \{(w_1, \dots, w_m) \mid w_1 \otimes \cdots \otimes w_m \in L(A)\} .$$

An m-ary relation $R \subseteq (\Gamma^*)^m$ is *automatic* if it is accepted by some m-dimensional automaton or, equivalently, if the language $R^\otimes = \{w_1 \otimes \cdots \otimes w_m \mid (w_1, \dots, w_m) \in R\} \subseteq (\Gamma_\#^m)^*$ is regular.

An *automatic presentation* is a tuple $P = (\Gamma, A_0, (A_R)_{R\in\tau})$, where:

- Γ is an alphabet.
- A_0 is a finite automaton over the alphabet Γ.
- τ is a signature, as before m_R is the arity of the symbol $R \in \tau$.
- For every $R \in \tau$, A_R is an m_R-dimensional automaton over the alphabet Γ such that $R(A_R) \subseteq L(A_0)^{m_R}$.

The structure presented by P is

$$\mathcal{A}(P) = (L(A_0), (R(A_R))_{R\in\tau}) .$$

A structure $\mathcal{A}$ is called *automatic* if there exists an automatic presentation P such that $\mathcal{A} \cong \mathcal{A}(P)$.

By SA, we denote the set of all automatic presentations. Similar notions of automaticity can be based on finite tree automata, on ω-string, and on ω-tree automata. The corresponding sets of presentations are denoted TA, $\omega\mathsf{SA}$, and $\omega\mathsf{TA}$, resp., but this paper will only be concerned with the set SA.

Examples

- All finite structures $\mathcal{A}$ are automatic with alphabet the universe of $\mathcal{A}$. While there are many infinite automatic structures (see below), there are no infinite automatic fields [20].
- The complete binary tree with universe $\{0,1\}^*$, together with the binary relations "first son" S_0, "second son" S_1, "prefix" $\leq$, and "equal length" is automatic.
- Presburger arithmetic $(\mathbb{N}, +)$ is automatic: the alphabet is $\{0,1\}$, the language of A_0 is $\{0,1\}^*1$ where the word $a_0a_1\dots a_n$ represents the number $\sum_{0\leq i\leq n} a_i 2^i$. Differently Skolem arithmetic $(\mathbb{N}, \cdot)$ is not automatic [4]. Blumensath also showed that Skolem arithmetic is tree-automatic [4].
- The linear order $(\mathbb{Q}, \leq)$ is automatic: the universe is $\{0,1\}^*$ with $u < v$ if and only if $(u \wedge v)0$ is a prefix of u or $(u \wedge v)1$ is a prefix of v (where $u \wedge v$ is the longest common prefix of u and v). This presentation is even "automatic-homogeneous": Let $u_1, \dots, u_n$ and $v_1, \dots, v_n$ be increasing sequences of equal length. Then there is an automatic automorphism f of $(\{0,1\}^*, \leq)$ mapping u_i to v_i [23]. The rational line is a particular Fraïssé-limit, other examples are the random graph and the universal and homogeneous poset [16]. It is known many such limits are not automatic [9, 20].
- The rewrite graph $(\Sigma^*, \to)$ of every semi-Thue system and therefore the configuration graph of every Turing machine are automatic.
- The extension of this configuration graph by the binary relation of reachability is in general not automatic. But for pushdown automata, the configuration graph with reachability $(Q\Gamma^*, \to, \to^*)$ is automatic: a configuration is represented by the control state followed by the stack content.
- The theory of automatic structures was preceded by that of automatic groups [13] and semigroups [7]. In terms of automatic structures, a semigroup is automatic (in the original sense) if its Cayley-graph has an automatic presentation such that $L(A_0)$ forms a rational cross-section of the (semi-)group. Many natural groups and semigroups were shown to be automatic and therefore to have automatic Cayley-graphs:

  - rational monoids [30],
  - virtually free finitely generated, virtually free Abelian finitely generated, and hyperbolic groups [13],
  - singular Artin monoids of finite type [8], and
  - graph products of such monoids [15].

  In contrast, it seems that not many infinite groups are automatic in the sense of this article. For instance, a finitely generated group is automatic if and only if it is virtually Abelian [28]. Braun and Strüngmann showed that every automatic torsion-free Abelian group is the extension of $(\mathbb{Z}^k, +)$ for some $k \in \mathbb{N}$ by a direct sum of finitely many Prüfer groups [6]. This implies Tsankov's celebrated result that $(\mathbb{Q}, +)$ is not automatic [32].
- An ordinal α is automatic if and only if $\alpha < \omega^\omega$ [10]. This proof was later generalized to show that the Hausdorff rank of every automatic linear order is finite [22]. This characterization (together with Theorem 1 below) can be used to show that the isomorphism of automatic ordinals is decidable. But note that this does not hold for automatic linear orders [24].
- Let $\mathcal{B}$ denote the Boolean algebra of all finite and co-finite subsets of $\mathbb{N}$. Then an infinite Boolean algebra is automatic if and only if it is a finite power of $\mathcal{B}$. Again, this characterisation leads to the decidability of the isomorphism of automatic Boolean algebras [20].

3 Definable relations

3.1 The classical result on first-order logic FO

Fix a signature τ. Then let V be a countably infinite set of variables. Formulas of FO are then built according to the following formation rules (where α and β are formulas, $x, y, y_1, \ldots, y_k \in V$ are variables, and R is a k-ary relation symbol):

(L1) $x = y$
(L2) $R(y_1, \ldots, y_k)$
(L3) $\alpha \vee \beta$
(L4) $\neg\alpha$
(L5) $\exists x \colon \alpha$

We next recall the semantics of formulas from FO. To this aim, let $\mathcal{A}$ be a τ-structure with universe A. An *interpretation in* $\mathcal{A}$ is a function $f \colon V \to \mathcal{A}$. Given such an interpretation, we set $\mathcal{A} \models_f \varphi$ (read as "φ holds in $\mathcal{A}$ under the interpretation f") if and only if one of the following hold

(S1) $\varphi = (x = y)$ and $f(x) = f(y)$.
(S2) $\varphi = (R(y_1, \ldots, y_k))$ and $(f(y_1), \ldots, f(y_k)) \in R^{\mathcal{A}}$.
(S3) $\varphi = (\alpha \vee \beta)$ and $\mathcal{A} \models_f \alpha$ or $\mathcal{A} \models_f \beta$.
(S4) $\varphi = \neg\alpha$ and not $\mathcal{A} \models_f \alpha$.
(S5) $\varphi = \exists x \colon \alpha$ and there exists $a \in \mathcal{A}$ with $\mathcal{A} \models_{f[\frac{a}{x}]} \alpha$ where $f[\frac{a}{x}]$ is the interpretation that differs from f only in that it maps x to a.

It is an easy exercise to show the following: let $\mathcal{A}$ be a τ-structure, φ a formula, and suppose $f(y) = g(y)$ for all $y \in \text{free}(\varphi)$, the set of variables occurring freely in φ. Then $\mathcal{A} \models_f \varphi$ if and only if $\mathcal{A} \models_g \varphi$. Assuming a fixed tuple of variables

$(y_1, \ldots, y_n)$ with $\mathrm{free}(\varphi) \subseteq \{y_1, \ldots, y_n\}$ for all $1 \leq i \leq n$, we can therefore simply write $\mathcal{A} \models \varphi(f(y_1), \ldots, f(y_n))$ for $\mathcal{A} \models_f \varphi$. In particular, for *sentences* (i.e., formulas without free variables), it makes sense to write $\mathcal{A} \models \varphi$.

Let $\varphi \in \mathrm{FO}$ be some formula with $\mathrm{free}(\varphi) \subseteq \{x_1, \ldots, x_n\}$ and let $\mathcal{A}$ be some τ-structure. Then

$$\varphi^{\mathcal{A}} = \{(u_1, \ldots, u_n) \in \mathcal{A}^n \mid \mathcal{A} \models \varphi(u_1, \ldots, u_n)\}$$

is a relation on the universe of the structure $\mathcal{A}$ that represents the semantics of the formula φ. The study of this relation is central in model theory [16] as well as in computable model theory (for computable instead of arbitrary structures) [14]. Consequently, they have also been studied in the context of automatic structures in which case $\varphi^{\mathcal{A}}$ is a relation on the set of words Γ^* for some alphabet Γ. The most important result is that they are effectively automatic (see below). Before we prove this result, we make the following definition: for a relation $R \subseteq X^{n+1}$ with $n \geq 0$, define the relation $(\exists R) \subseteq X^n$ by

$$(\exists R) = \{(x_1, \ldots, x_n) \in X^n \mid \text{ there exists } x \in X \text{ with } (x_1, \ldots, x_n, x) \in R\}.$$

Let $X = \Gamma^*$ and $n = 0$. Then we get $(\exists R) \subseteq (\Gamma^*)^0 = \{()\}$ and consequently $(\exists R)^{\otimes} \subseteq \{\varepsilon\}$. We then have the following:

Proposition 1. *If $R \subseteq (\Gamma^*)^{n+1}$ is automatic with $n \geq 0$, then $(\exists R)$ is automatic and an automaton accepting $(\exists R)^{\otimes}$ can be computed from an automaton accepting $R^{\otimes}$.*

Proof. Let $\mathrm{proj}\colon \Gamma_\#^{n+1} \to \Gamma_\#^n$ be the projection that deletes the last component. We naturally extend it to a monoid homomorphism $\mathrm{proj}\colon (\Gamma_\#^{n+1})^* \to (\Gamma_\#^n)^*$. Now let $u_1, \ldots, u_n \in \Gamma^*$. Then we have

$$\begin{aligned}
u_1 \otimes \cdots \otimes u_n \in (\exists R)^{\otimes} &\iff (u_1, u_2, \ldots, u_n) \in (\exists R) \\
&\iff \text{there is some } u \in \Gamma^* \text{ with } (u_1, u_2, \ldots, u_n, u) \in R \\
&\iff \text{there is some } u \in \Gamma^* \text{ with } u_1 \otimes \cdots \otimes u_n \otimes u \in R^{\otimes} \\
&\iff (u_1 \otimes \cdots \otimes u_n)(\#, \ldots, \#)^* \cap \mathrm{proj}(R^{\otimes}) \neq \emptyset \\
&\iff (u_1 \otimes \cdots \otimes u_n) \in \mathrm{proj}(R^{\otimes})((\#, \ldots, \#)^*)^{-1}
\end{aligned}$$

where $KL^{-1} = \{x \mid \text{there is some } y \in L \text{ with } xy \in K\}$ for two languages K and L. Hence $(\exists R)^{\otimes} = \mathrm{proj}(R^{\otimes})((\#, \ldots, \#)^*)^{-1}$. Since $R^{\otimes}$ is regular and proj is a monoid morphism, it follows that $(\exists R)^{\otimes}$ is regular, i.e., that $(\exists R)$ is automatic. □

Using this proposition, we easily get the following central result.

Theorem 1 (cf. [17, 19]). *Let $P = (\Gamma, A_0, (A_R)_{R \in \tau})$ be an automatic presentation and $\varphi \in \mathrm{FO}$ a formula with $\mathrm{free}(\varphi) \subseteq \{y_1, \ldots, y_n\} \subseteq V$. Then the relation $\varphi^{\mathcal{A}(P)}$ is automatic. Even more, an n-dimensional automaton for this relation can be computed from P and φ.*

Proof (sketch). The automaton is constructed by induction on the structure of the formula φ (where we assume that α and β are formulas such that $\alpha^{\mathcal{A}(P)}$ and $\beta^{\mathcal{A}(P)}$ are effectively regular):

- if $\varphi = (x_i = x_j)$, then an automaton for $\varphi^{\mathcal{A}(P)}$ is obtained from A_0.
- if $\varphi = R(x_1, \dots, x_n)$, then $\varphi^{\mathcal{A}(P)} = R(A_R)$ is effectively automatic.
- if $\varphi = (\alpha \vee \beta)$, then $\varphi^{\mathcal{A}(P)} = \alpha^{\mathcal{A}(P)} \cup \beta^{\mathcal{A}(P)}$ is effectively automatic.
- if $\varphi = \neg\alpha$, then $\varphi^{\mathcal{A}(P)} = L(A_0)^n \setminus \alpha^{\mathcal{A}(P)}$ is effectively automatic.
- if $\varphi = \exists x\colon \alpha$, then $\varphi^{\mathcal{A}(P)} = (\exists \alpha^{\mathcal{A}(P)})$ which is effectively automatic by Prop. 1. □

Our principal aim is to extend first-order logic by additional quantifiers and prove the corresponding extension of Theorem 1. To simplify terminology, we introduce the following notation.

Definition 1. *Let* $\exists$ *be a function that maps* $2^{(\Gamma^*)^{n+k}}$ *to* $2^{(\Gamma^*)^n}$ *for all* $n \in \mathbb{N}$ *and some fixed* $k \in \mathbb{N}$*. Then* $\exists$ preserves automaticity effectively *if one can compute an* n*-dimensional automaton accepting* $\exists(R(A)))$ *from the* $(n+k)$*-dimensional automaton* A*.*

For $n = 0$, we have $\exists(R(A)) \subseteq \{()\}$, i.e., $(\exists(R(A)))^\otimes \subseteq \{\varepsilon\}$ and therefore $\varepsilon \in (\exists(R(A)))^\otimes$ if and only if $\exists(R(A)) \neq \emptyset$. Thus, to show that $\exists(R(A))$ is effectively regular (at least for $n = 0$), we have to device an algorithm that decides whether $\exists(R(A))$ is empty or not. In other words, the property that $\exists$ preserves automaticity effectively is a generalization of the decidability of the emptiness problem for $\exists(R(A))$.

Using this definition, Prop. 1 can now be phrased more concisely: The function $\exists$ that maps $R \subseteq (\Gamma^*)^{n+1}$ to $(\exists R) \subseteq (\Gamma^*)^n$ preserves automaticity effectively.

3.2 The infinity quantifier

For a relation $R \subseteq X^{n+1}$ with $n \geq 0$ let

$$(\exists^\infty R) = \{(x_1, \dots, x_n) \in X^n \mid \text{there are infinitely many } x \in X \text{ with } (x_1, \dots, x_n, x) \in R\}\,.$$

We will show that $\exists^\infty$ preserves automaticity effectively. A short proof of this fact was given by Blumensath [4] using Theorem 1. Our admittedly longer proof uses classical results from the theory of weighted automata and therefore fits into the setting of this paper.

Consider the complete semiring $\mathbb{N}_\infty = (\mathbb{N} \cup \{\infty\}, +, \cdot, 0, 1)$ with $0 \cdot \infty = \infty \cdot 0 = 0$.

Lemma 1. *From an* $n+1$*-dimensional automaton* $\mathcal{A}$*, one can construct an* $\mathbb{N}_\infty$*-weighted automaton* $\mathcal{B}$ *over the alphabet* $\Gamma_\#^n$ *such that*

$$(||\mathcal{B}||, V) = \begin{cases} |\{u \mid (u_1, u_2, \dots, u_n, u) \in R\}| & \text{if } V = u_1 \otimes u_2 \otimes \cdots \otimes u_n \\ 0 \text{ otherwise} \end{cases}$$

Proof. Since $R^\otimes$ is regular, the mapping

$$\mathbf{1}_{R^\otimes} : (\Gamma_\#^{n+1})^* \to \mathbb{N}_\infty : U \mapsto \begin{cases} 1 & \text{if } U \in R^\otimes \\ 0 & \text{otherwise} \end{cases}$$

is a recognizable and therefore rational formal power series. Recall that the projection morphism proj from the proof of Prop. 1 is length-preserving. Hence the formal power series $\mathbf{1}_{R^\otimes} \circ \mathrm{proj}^{-1}$ defined by

$$S_1 = \mathbf{1}_{R^\otimes} \circ \mathrm{proj}^{-1} \colon (\Gamma_\#^n)^* \to \mathbb{N}_\infty \colon V \mapsto \sum \big((\mathbf{1}_{R^\otimes}, U) \mid \mathrm{proj}(U) = V \big)$$

is rational by [11, Prop. 3.6(ii)]. Note that $(S_1, V) = |\mathrm{proj}^{-1}(V) \cap R^\otimes|$. Hence, for $V = (u_1 \otimes u_2 \otimes \cdots \otimes u_n)(\#, \ldots, \#)^k$, we have

$$(S_1, V) = |\{u \in \Gamma^* \mid (u_1, \ldots, u_n, u) \in R \text{ and } |u| = \max(|u_1|, |u_2|, \ldots, |u_n|) + k\}| \,.$$

If V is not of this form, then $(S_1, V) = 0$.

Next let $\mathrm{del} \colon (\Gamma_\#^n)^* \to (\Gamma_\#^n)^*$ be the monoid morphism with $\mathrm{del}(\#, \ldots \#) = \varepsilon$ and $\mathrm{del}(A) = A$ for all other letters $A \in \Gamma_\#^n$. In other words, del deletes all occurrences of $(\#, \ldots, \#)$ from a word. Since the semiring $\mathbb{N}_\infty$ is complete, the formal power series

$$S_2 = S_1 \circ \mathrm{del}^{-1} \colon (\Gamma_\#^n)^* \to \mathbb{N}_\infty \colon V \mapsto \sum \big((S_1, W) \mid \mathrm{del}(W) = V \big)$$

is rational and therefore recognizable by [11, Prop. 3.6(ii)]. Note that $(S_2, u_1 \otimes u_2 \otimes \cdots \otimes u_n)$ is the number of words u with $(u_1, \ldots, u_n, u) \in R$.

All the results cited have effective proofs, so from the above arguments we can extract an algorithm for the construction of a weighted automaton $\mathcal{B}$ for the series S_2. □

We now come to the central result on $\exists^\infty$:

Proposition 2 ([4]). *The function $\exists^\infty$ that maps $R \subseteq (\Gamma^*)^{n+1}$ to $(\exists^\infty R)$ preserves automaticity effectively.*

Proof. Let $\mathcal{B}$ be the weighted automaton from Lemma 1.

Now consider the semiring $(\{0, 1, \infty\}, \max, \cdot, 0, 1)$ with $0 \cdot \infty = \infty \cdot 0 = 0$. Then $h \colon \mathbb{N}_\infty \to \{0, 1, \infty\}$ with $h(0) = 0$, $h(\infty) = \infty$, and $h(m) = 1$ for all $0 < m < \infty$ is a semiring homomorphism. Hence, by [31, Prop. 4.5],

$$S = h \circ ||\mathcal{B}|| \colon (\Gamma_\#^n)^* \to \{0, 1, \infty\} \colon V \mapsto h((||\mathcal{B}||, V))$$

is a recognizable formal power series into a finite semiring. Therefore the set

$$\{V \in (\Gamma_\#^n)^* \mid (S, V) = \infty\}$$

is effectively regular [31, Prop. 6.3]. Since the set $((\Gamma^*)^n)^\otimes$ of convolutions of n words over Γ is regular, also the set

$$\{V \in (\Gamma_\#^n)^* \mid (S, V) = \infty\} \cap ((\Gamma^*)^n)^\otimes$$

is effectively regular.

It remains to verify that this set equals $(\exists^\infty R)^\otimes$: So let $V = (u_1 \otimes \cdots \otimes u_n)$. Then $(||\mathcal{B}||, V)$ is the number of words u with $(u_1, \ldots, u_n, u) \in R$. Hence $(S, V) = \infty$ if and only if $(||\mathcal{B}||, V) = \infty$ if and only if $V \in (\exists^\infty R)^\otimes$ which proves the claim. □

3.3 The modulo quantifier

For a relation $R \subseteq X^{n+1}$ with $n \geq 0$ and $0 \leq p < q$ let

$$(\exists^{(p,q)} R) = \{(x_1, \ldots, x_n) \in X^n \mid |\{x \in X \mid (x_1, \ldots, x_n, x) \in R\}| \text{ is finite and congruent } p \text{ modulo } q\}\,.$$

Proposition 3 ([21]). *The function $\exists^{(p,q)}$ that maps $R \subseteq (\Gamma^*)^{n+1}$ to the relation $(\exists^{(p,q)} R)$ preserves automaticity effectively uniformly in (p, q). In other words, there exists* one *algorithm that takes as input p, q, and an automaton for R and returns an automaton for $(\exists^{(p,q)} R)$.*

The result was first stated in [21] where one finds a proof for the case $q = 2$, a proof of the general case can be found in [29, Thm. 3.19]. Both these proofs construct the automaton for $(\exists^{(p,q)} R)$ directly. Differently, the new proof below is based on the theory of weighted automata.

Proof. First note that $R \setminus ((\exists^\infty R) \times \Gamma^*)$ is the set of tuples $(u_1, \ldots, u_{n+1}) \in R$ such that there are only finitely many $u \in \Gamma_\#^*$ that can replace u_{n+1}, i.e., that satisfy $(u_1, \ldots, u_n, u) \in R$. Hence

$$(\exists^{(p,q)} R) = (\exists^{(p,q)} (R \setminus ((\exists^\infty R) \times \Gamma^*)))\,.$$

Since $R \setminus ((\exists^\infty R) \times \Gamma^*)$ is effectively automatic by Prop. 2 (in conjunction with the effective closure of automatic relations under Boolean operations and direct products), it suffices to consider the case $R = R \setminus ((\exists^\infty R) \times \Gamma^*)$.

Let $\mathcal{B}$ be the weighted automaton from Lemma 1.

If V is the convolution of n words, then $(||\mathcal{B}||, V) \in \mathbb{N}$ by our assumption on R. If V is not a convolution of n words, then $(||\mathcal{B}||, V) = 0 \in \mathbb{N}$. It follows that $||\mathcal{B}||$ is even a rational formal power series over the natural semiring $(\mathbb{N}, +, \cdot, 0, 1)$ (simply replace all weights ∞ in $\mathcal{B}$ by 0 or any other natural number).

We now consider the (semi)ring $\mathbb{Z}/q\mathbb{Z} = (\{0, 1, \ldots, q-1\}, +, \cdot, 0, 1)$. Applying [11, Prop. 3.5], we find that

$$S \colon (\Gamma_\#^n)^* \to \mathbb{Z}/q\mathbb{Z} \colon V \mapsto (||\mathcal{B}||, V) \bmod q$$

is a rational formal power series into a finite semiring. As in the proof of Prop. 2, it follows that the set

$$\{V \in (\Gamma_\#^n)^* \mid (S, V) = p\} \cap ((\Gamma^*)^n)^\otimes$$

is effectively regular.

It remains to verify that this set equals $(\exists^{(p,q)} R)^\otimes$: So let $V = (u_1 \otimes \cdots \otimes u_n)$. Then $(||\mathcal{B}||, V)$ is the number of words u with $(u_1, \ldots, u_n, u) \in R$. Hence $(S, V) = p$ if and only if $(||\mathcal{B}||, V) \equiv p \pmod{q}$ if and only if $V \in (\exists^{(p,q)} R)^\otimes$ which proves the claim. □

3.4 The boundedness quantifier

For a relation $R \subseteq X^{n+2}$ with $n \geq 0$ let

$$(\exists R) = \{(x_1, \ldots, x_n) \in X^n \mid \text{there is some } m \in \mathbb{N} \text{ such that } |\{z \mid (x_1, \ldots, x_n, y, z) \in R\}| \leq m \text{ for all } y \in X\}.$$

We will show that $(\exists R)$ is effectively automatic if R is automatic. A central notion in this proof is that of a *finite valued* function $f\colon X \to 2^Y$ by which we mean that there is some $m \in \mathbb{N}$ such that $|f(y)| \leq m$ for all $y \in X$. We first handle the case $n = 0$.

Lemma 2. *If $R \subseteq (\Gamma^*)^2$ is automatic, then $(\exists R)$ is automatic and an automaton accepting $(\exists R)^\otimes$ can be computed from an automaton accepting $R^\otimes$.*

Proof. As explained after Definition 1, we have to decide whether the function

$$\Gamma^* \to 2^{\Gamma^*} : y \mapsto \{z \in \Gamma^* \mid (y, z) \in R\}$$

is finite valued. Since R is an automatic relation, it is a rational transduction. Hence the result follows from [33]. $\square$

From now on, let $n \geq 1$. It will be convenient to consider $(\exists R)$ as the intersection of the following two relations:

$$(\exists_{\leq} R) = \{(x_1, \ldots, x_n) \in (\Gamma^*)^n \mid \text{there is some } m \in \mathbb{N} \text{ such that } |\{z \mid (x_1, \ldots, x_n, y, z) \in R\}| \leq m \text{ for all } y \in \Gamma^* \text{ with } |y| \leq |x_i| \text{ for all } 1 \leq i \leq n\}$$

$$(\exists_{>} R) = \{(x_1, \ldots, x_n) \in (\Gamma^*)^n \mid \text{there is some } m \in \mathbb{N} \text{ such that } |\{z \mid (x_1, \ldots, x_n, y, z) \in R\}| \leq m \text{ for all } y \in \Gamma^* \text{ with } |y| > |x_i| \text{ for all } 1 \leq i \leq n\}$$

Lemma 3. *The function $\exists_{\leq}$ that maps $R \subseteq (\Gamma^*)^{n+2}$ to $(\exists_{\leq} R)$ preserves automaticity effectively.*

Proof. For notational convenience, we only prove this lemma for $n = 1$, the general case can easily be shown along the same lines.

Let A be a deterministic finite automaton accepting $R^\otimes$. Let Q denote its set of states, ι the initial state, and F the set of accepting states. For three words $x, y, z \in \Gamma^*$ and a state $q \in Q$, we write $q.(x, y, z)$ for the state reached from q when executing $x \otimes y \otimes z$. Finally, let $\ell_q = |\{z'' \in \Gamma^+ \mid q.(\varepsilon, \varepsilon, z'') \in F\}| \in \mathbb{N}_\infty$ for $q \in Q$.

Now let $x, y \in \Gamma^*$ with $|y| \leq |x|$. Then we have

$$\begin{aligned}|\{z \mid (x, y, z) \in R\}| &= |\{z \in \Gamma^{\leq |x|} \mid (x, y, z) \in R\}| + |\{z \in \Gamma^{>|x|} \mid (x, y, z) \in R\}| \\ &\leq |\Gamma^{\leq |x|}| + \sum_{q \in Q} \begin{pmatrix} |\{z' \in \Gamma^{=|x|} \mid \iota.(x, y, z') = q\}| \\ \cdot |\{z'' \in \Gamma^+ \mid q.(\varepsilon, \varepsilon, z'') \in F\}| \end{pmatrix} \\ &\leq |\Gamma^{\leq |x|}| + |\Gamma^{=|x|}| \cdot \sum_{q \in H} \ell_q\end{aligned}$$

where H is the set of all states $\iota.(x,y,z')$ for some $z' \in \Gamma^{=|x|}$.

Hence $x \notin (\exists_{\leq} R)$ if and only if there exist some $y, z' \in \Gamma^*$ with $|y| \leq |x| = |z'|$ and $\ell_{\iota.(x,y,z')} = \infty$. But this is a regular property, so also $(\exists_{\leq} R)$ is regular.

Note that ℓ_q can be computed from the automaton A and the state q. Hence an automaton for $(\exists_{\leq} R)$ can be computed. □

Lemma 4. *The function $\exists_{>}$ that maps $R \subseteq (\Gamma^*)^{n+2}$ to $(\exists_{>} R) \subseteq (\Gamma^*)^n$ preserves automaticity effectively.*

Proof. We use the notation from the first paragraph of the proof of Lemma 3 (except for ℓ_q). Now let $x, y \in \Gamma^*$ with $|y| > |x|$ and write $y = y'y''$ with $|y'| = |x|$. Then we have

$$\begin{aligned}
|\{z \mid (x,y,z) \in R\}| &= |\{z \in \Gamma^{\leq |x|} \mid (x,y,z) \in R\}| + |\{z \in \Gamma^{>|x|} \mid (x,y,z) \in R\}| \\
&\leq |\Gamma^{\leq |x|}| + \sum_{q \in Q} \begin{pmatrix} |\{z' \in \Gamma^{=|x|} \mid \iota.(x,y',z') = q\}| \\ \cdot |\{z'' \in \Gamma^{+} \mid q.(\varepsilon, y'', z'') \in F\}| \end{pmatrix} \\
&\leq |\Gamma^{\leq |x|}| + |\Gamma^{|x|}| \cdot \sum_{q \in H} |\{z'' \in \Gamma^{+} \mid q.(\varepsilon, y'', z'') \in F\}| \,.
\end{aligned}$$

where H is the set of all states $\iota.(x,y',z')$ for some $z' \in \Gamma^{=|x|}$.

We now define a set $F' \subseteq Q$ of states (that plays the role of the set of states q with $\ell_q \in \mathbb{N}$ from the proof of Lemma 3). Let $q \in F'$ if the mapping

$$\Gamma^* \to 2^{\Gamma^*} : y'' \mapsto \{z'' \in \Gamma^{+} \mid q.(\varepsilon, y'', z'') \in F\} \tag{1}$$

is finite valued. Then it is easily seen that $x \notin (\exists_{>} R)$ if and only if there are words $y', z' \in \Gamma^{=|x|}$ with $\iota.(x,y',z') \notin F'$. But this is a regular property, so also $(\exists_{>} R)$ is regular.

By [33], one can decide from the automaton A and the state q whether the mapping (1) is finite valued. Hence an automaton for $(\exists_{>} R)$ can be computed. □

Proposition 4. *The function $\exists$ that maps $R \subseteq (\Gamma^*)^{n+2}$ to $(\exists R)$ preserves automaticity effectively.*

Proof. The proof is immediate by Lemmas 2, 3, and 4 since, for $n \geq 1$, we have $(\exists R) = (\exists_{\leq} R) \cap (\exists_{>} R)$ and since automatic relations are effectively closed under intersection. □

This proposition and consequently its proof are genuinely new, the case $n = 2$ was used in [24] to show that the set of presentations of trees of finite height is decidable.

3.5 Summary and model checking

Recall that first-order formulas were defined by the formation rules (L1-5). The central theorem on first-order logic was proved using that the existential quantifier preserves automaticity effectively. This statement was also shown for other "quantifiers". We will now extend first-order logic by these quantifiers, state the extended version of Theorem 1, and infer that the model checking problem for this large logic and automatic structures is decidable.

Formulas of $\mathrm{FO}_{\mathrm{ext}}$ are built according to the formation rules (L1-9) (where α is a formula):

(L6) $\exists^\infty x\colon \alpha$
(L7) $\exists^{(p,q)} x\colon \alpha$ for $0 \le p < q$
(L8) $\text{ᗺ}(y,z)\colon \alpha$
(L9) $\text{Ꝺ}^k(y_1,\dots,y_k)\colon \alpha$ for $k \ge 1$

We set $\mathcal{A} \models_f \varphi$ if and only if one of (S1-9) hold:

(S6) $\varphi = \exists^\infty x\colon \alpha$ and there exist infinitely many $a \in \mathcal{A}$ with $\mathcal{A} \models_{f[\frac{a}{x}]} \alpha$. For instance, $\forall y \neg\exists^\infty z\colon E(y,z)$ says of a directed graph that it has finite out-degree.

(S7) $\varphi = \exists^{(p,q)} x\colon \alpha$ and the number of elements $a \in \mathcal{A}$ with $\mathcal{A} \models_{f[\frac{a}{x}]} \alpha$ is finite and congruent p modulo q. For instance, $\exists^{(0,2)} x\colon x = x$ expresses that a structure is finite and has an even number of elements.

(S8) $\varphi = \text{ᗺ}(y,z)\colon \alpha$ and there exists $m \in \mathbb{N}$ such that, for all $a \in \mathcal{A}$, the set

$$\{b \in \mathcal{A} \mid \mathcal{A} \models_{f[\frac{ab}{yz}]} \alpha\}$$

contains at most m elements. In other words, $\text{ᗺ}(y,z)\colon \alpha$ expresses the existence of some natural number m such that any element y has at most m partners z that make α true. For instance, $\text{ᗺ}(y,z)\colon E(y,z)$ says of a directed graph that it has bounded out-degree.

(S9) $\text{Ꝺ}^k(y_1,\dots,y_k)\colon \alpha$ for some $k \ge 1$ and there exists some infinite set $X \subseteq \mathcal{A}$ such that $\mathcal{A} \models_g \alpha$ for all $a_1,\dots,a_k \in X$ with $g = f\,[\frac{a_1 \dots a_k}{y_1 \dots y_k}]$. For instance, $\text{Ꝺ}^2(y,z)\colon (y = z \vee (E(y,z) \wedge E(z,y))$ expresses that a directed graph has an infinite clique. For this reason, Ꝺ^k is called *Ramsey quantifier*. In [29], it is shown that the Ramsey quantifier preserves automaticity effectively (uniformly in k).

Theorem 2. *Let $P = (\Gamma, A_0, (A_R)_{R\in\tau})$ be an automatic presentation and $\varphi \in \mathrm{FO}_{\mathrm{ext}}$ a formula with $\mathrm{free}(\varphi) \subseteq \{y_1,\dots,y_n\} \subseteq V$. Then the relation $\varphi^{\mathcal{A}(P)}$ is automatic. Even more, an n-dimensional automaton for this relation can be computed from P and φ.*

Proof. The proof is an immediate extension of the proof of Theorem 1 using in addition Prop. 2, 3, 4 and [29, Thm. 3.20]. □

Corollary 1. *The set of pairs (P,φ) where P is an automatic presentation and φ a sentence from $\mathrm{FO}_{\mathrm{ext}}$ with $\mathcal{A}(P) \models \varphi$ is decidable.*

Proof. From Theorem 2, we get an automaton A accepting $(\varphi^{\mathcal{A}(P)})^{\otimes} \subseteq \{\varepsilon\}$. Then ε is accepted by A if and only if $\mathcal{A}(P) \models \varphi$. □

Open question In [26], we present a generalisation of the Ramsey quantifier and show Corollary 1 for the extension of first-order logic by all the infinity, the modulo, and this generalized quantifier (and therefore the Ramsey quantifier). In other words, we have two extensions of the logic with infinity, modulo, and Ramsey quantifier (namely by the boundedness quantifier and by the generalized Ramsey quantifier) such that Corollary 1 holds. But it is not clear whether these two extensions together give decidability.

4 Isomorphism

The *isomorphism problem* for automatic structures is the set of pairs of automatic presentations P and Q such that $\mathcal{A}(P) \cong \mathcal{A}(Q)$. Using a result by Honkala on weighted automata over $(\mathbb{N}, +, \cdot, 0, 1)$, we show in this section that the isomorphism problem for automatic structures is not decidable. More precisely, we present a single structure $\mathcal{E}_{\text{good}} = (V, \sim)$ where $\sim$ is an equivalence relation on V such that the set of automatic presentations of $\mathcal{E}_{\text{good}}$ is not decidable.

An *equivalence structure* is a structure $\mathcal{E} = (V, \sim)$ such that V is at most countably infinite and $\sim$ is an equivalence relation on V. Let $\mathcal{E}_{\text{good}}$ be the equivalence structure with universe $a^*b^*c^*$ and $a^k b^\ell c^m \sim a^{k'} b^{\ell'} c^{m'}$ if and only if $k + \ell = k' + \ell'$ and $m = m'$. It has, for every $n \in \mathbb{N}$, infinitely many equivalence classes of size $n + 1$, and no infinite equivalence class.

Now let $\mathcal{B}$ be a weighted automaton over the natural semiring $(\mathbb{N}, +, \cdot, 0, 1)$ and the alphabet Σ. Without changing the behavior of $\mathcal{B}$, i.e., the formal power series $||\mathcal{B}||\colon \Sigma^* \to \mathbb{N}$, we can assume $\mathcal{B}$ to be normalized, i.e., all the initial and final weights 0 or 1.

From $\mathcal{B}$, we now construct an equivalence structure as follows: Let $m \in \mathbb{N}$ be the maximal weight appearing in $\mathcal{B}$. Let Γ be the set of states of $\mathcal{B}$ together with all pairs (a, k) where $a \in \Sigma$ and $0 \leq k < m$. Then the universe of the equivalence structure $\mathcal{E}_{\mathcal{B}}$ is the set of sequences

$$\rho = q_0\,(a_1, k_1)\,q_1\,(a_1, k_1)\,q_1 \ldots (a_n, k_n)\,q_n\,\$^\ell$$

such that k_i is properly smaller than the weight of the transition (q_{i-1}, a_i, q_i) in $\mathcal{B}$ (for $1 \leq i \leq n$), the entry weight of q_0 and the final weight of q_n are 1. The sequence ρ and the sequence

$$\rho' = q_0'\,(b_1', k_1')\,q_1'\,(b_1', k_1')\,q_1' \ldots (b_{n'}, k_{n'})\,q_{n'}\,\$^{\ell'}$$

are equivalent ($\rho \sim \rho'$) if

$$a_1 a_2 \ldots a_n = b_1 b_2 \ldots b_{n'} \text{ and } \ell = \ell'\,.$$

Then the equivalence class of ρ with respect to $\sim$ has precisely $(||\mathcal{B}||, a_1 a_2 \ldots a_n)$ elements. If $\sim$ has one equivalence class of size k, then it has infinitely many such equivalence classes because of the suffix from $\$^*$. Hence we get

$$\mathcal{E}_{\text{good}} \cong \mathcal{E}_{\mathcal{B}} \iff \forall n \in \mathbb{N}\, \exists u \in \Sigma^*\colon (||\mathcal{B}||, u) = n + 1\,.$$

By [18], this latter question is undecidable. Hence we showed

Theorem 3 ([24]). *The isomorphism for automatic equivalence structures is undecidable (more precisely: Π^0_1-complete since it is in Π^0_1 by [29]).*

One can easily transform an equivalence structure $\mathcal{E} = (V, \sim)$ into a tree $T_\mathcal{E}$ of height 2: V is the root, $V/\sim$ is the set of children of the root, and V is the set of leaves. A leaf $v \in V$ is a child of $a \in V/\sim$ if and only if $v \in a$. It is even possible to construct an automatic presentation of this tree. Then

$$\mathcal{E} \cong \mathcal{E}' \iff T_\mathcal{E} \cong T_{\mathcal{E}'}$$

implies

Corollary 2 ([24]). *The isomorphism problem for automatic trees of height* 2 *is undecidable (more precisely: Π^0_1-hard).*

In [24], we showed that the isomorphism problem for automatic trees of height n is complete for Π^0_{2n-3} and the isomorphism problem for all order trees is Σ^1_1-complete; the above result is the (idea of the) base case. Prior to these results, it was known that the isomorphism problem for automatic successor trees is Σ^1_1-complete [20, 27].

Open question In [24], we also show that the isomorphism problem for automatic linear orders is Σ^1_1-complete. Recall that a linear order is *scattered* if it does not contain a copy of $(\mathbb{Q}, \leq)$. We also showed that the isomorphism problem for scattered automatic linear orders is significantly simpler (namely, in Δ^0_ω, i.e., reducible to true first order arithmetic). But it is still not known whether this problem is decidable (we only have an undecidability proof for tree-automatic scattered linear orders).

References

1. Bárány, V.: Invariants of automatic presentations and semi-synchronous transductions. In: STACS'06. pp. 289–300. Lecture Notes in Comp. Science vol. 3884, Springer (2006)
2. Bárány, V., Grädel, E., Rubin, S.: Automata-based presentations of infinite structures. In: Finite and Algorithmic Model Theory, pp. 1–76. Cambridge University Press (2011)
3. Bárány, V., Kaiser, Ł., Rubin, S.: Cardinality and counting quantifiers on omega-automatic structures. In: STACS'08. pp. 385–396. IFIB Schloss Dagstuhl (2008)
4. Blumensath, A.: Automatic structures. Tech. rep., RWTH Aachen (1999)
5. Blumensath, A., Grädel, E.: Automatic Structures. In: LICS'00. pp. 51–62. IEEE Computer Society Press (2000)
6. Braun, G., Strüngmann, L.: Breaking up finite automata presentable torsion-free abelian groups. International Journal of Algebra and Computation (2011), accepted
7. Campbell, C., Robertson, E., Ruškuc, N., Thomas, R.: Automatic semigroups. Theoretical Computer Science 250, 365–391 (2001)

8. Corran, R., Hoffmann, M., Kuske, D., Thomas, R.: Singular Artin monoids of finite type are automatic. In: LATA'11. pp. 249–260. Lecture Notes in Comp. Science vol. 6638, Springer (2011)
9. Delhommé, C.: Automaticité des ordinaux et des graphes homogènes. C. R. Acad. Sci. Paris, Ser. I 339, 5–10 (2004)
10. Delhommé, C., Goranko, V., Knapik, T.: Automatic linear orderings (2003), manuscript
11. Droste, M., Kuich, W.: Semirings and formal power series. In: Droste, M., Kuich, W., Vogler, H. (eds.) Handbook of Weighted Automata, pp. 3–28. Springer (2009)
12. Elgot, C.: Decision problems of finite automata design and related arithmetics. Trans. Am. Math. Soc. 98, 21–51 (1961)
13. Epstein, D., Cannon, J., Holt, D., Levy, S., Paterson, M., Thurston, W.: Word Processing In Groups. Jones and Bartlett Publishers, Boston (1992)
14. Ershov, Y., Goncharov, S., Nerode, A., Remmel, J. (eds.): Handbook of recursive mathematics vol. 1 and 2. Elsevier (1998)
15. Fohry, E., Kuske, D.: On graph products of automatic and biautomatic monoids. Semigroup forum 72, 337–352 (2006)
16. Hodges, W.: Model Theory. Cambridge University Press (1993)
17. Hodgson, B.: On direct products of automaton decidable theories. Theoretical Computer Science 19, 331–335 (1982)
18. Honkala, J.: On the problem whether the image of an $\mathbb{N}$-rational series equals $\mathbb{N}$. Fundamenta Informaticae 73(1-2), 127–132 (2006)
19. Khoussainov, B., Nerode, A.: Automatic presentations of structures. In: Logic and Computational Complexity. pp. 367–392. Lecture Notes in Comp. Science vol. 960, Springer (1995)
20. Khoussainov, B., Nies, A., Rubin, S., Stephan, F.: Automatic structures: richness and limitations. Log. Methods in Comput. Sci. 3(2) (2007)
21. Khoussainov, B., Rubin, S., Stephan, F.: Definability and regularity in automatic structures. In: STACS'04. pp. 440–451. Lecture Notes in Comp. Science vol. 2996, Springer (2004)
22. Khoussainov, B., Rubin, S., Stephan, F.: Automatic linear orders and trees. ACM Transactions on Computational Logic 6(4), 675–700 (2005)
23. Kuske, D.: Is Cantor's theorem automatic? In: LPAR'03. pp. 332–345. Lecture Notes in Comp. Science vol. 2850, Springer (2003)
24. Kuske, D., Liu, J., Lohrey, M.: The isomorphism problem on classes of automatic structures. In: LICS 2010. pp. 160–169. IEEE Computer Society (2010)
25. Kuske, D., Lohrey, M.: First-order and counting theories of ω-automatic structures. Journal of Symbolic Logic 73, 129–150 (2008)
26. Kuske, D., Lohrey, M.: Some natural problems in automatic graphs. Journal of Symbolic Logic 75(2), 678–710 (2010)
27. Nies, A.: Describing groups. Bulletin of Symbolic Logic 13(3), 305–339 (2007)
28. Oliver, G., Thomas, R.: Automatic presentations for finitely generated groups. In: STACS'05. pp. 693–704. Lecture Notes in Computer Science vol. 3404, Springer (2005)
29. Rubin, S.: Automata presenting structures: A survey of the finite string case. Bulletin of Symbolic Logic 14, 169–209 (2008)
30. Sakarovitch, J.: Easy multiplications. I. The realm of Kleene's Theorem. Information and Computation 74, 173–197 (1987)
31. Sakarovitch, J.: Rational and recognizable series. In: Droste, M., Kuich, W., Vogler, H. (eds.) Handbook of Weighted Automata, pp. 405–453. Springer (2009)

32. Tsankov, T.: The additive group of the rationals does not have an automatic presentation (2009), http://arxiv.org/abs/0905.1505
33. Weber, A.: On the valuedness of finite transducers. Acta Informatica 27, 749–780 (1990)