HAL
open science

Incompleteness Theorems, Large Cardinals, and Automata over Finite Words

Olivier Finkel

To cite this version:

Olivier Finkel. Incompleteness Theorems, Large Cardinals, and Automata over Finite Words. International Journal of Foundations of Computer Science, 2019. hal-02318263

HAL Id: hal-02318263

https://hal.science/hal-02318263

Submitted on 16 Oct 2019

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Incompleteness Theorems, Large Cardinals, and Automata over Finite Words

Olivier Finkel

Institut de Mathématiques de Jussieu - Paris Rive Gauche
CNRS et Université Paris 7, France.
Olivier.Finkel@math.univ-paris-diderot.fr

Abstract. We prove that one can construct various kinds of automata over finite words for which some elementary properties are actually independent from strong set theories like T_n =:**ZFC** + "There exist (at least) n inaccessible cardinals", for integers $n \geq 0$. In particular, we prove independence results for languages of finite words generated by context-free grammars, or accepted by 2-tape or 1-counter automata. Moreover we get some independence results for weighted automata and for some related finitely generated subsemigroups of the set $\mathbb{Z}^{3\times 3}$ of 3-3 matrices with integer entries. Some of these latter results are independence results from the Peano axiomatic system **PA**.

Keywords: Automata and formal languages; logic in computer science; finite words; context-free grammars; 2-tape automaton; Post Correspondence Problem; weighted automaton; finitely generated matrix subsemigroups of $\mathbb{Z}^{3\times 3}$; models of set theory; Incompleteness Theorems; large cardinals; inaccessible cardinals; independence from the axiomatic system "**ZFC** + there exist n inaccessible cardinals"; independence from Peano Arithmetic.

1 Introduction

We pursue in this paper a study of the links between automata theory and set theory we begun in previous papers [Fin09,Fin11,Fin15]

In [Fin09] we proved a surprising result: the topological complexity of an ω-language accepted by a 1-counter Büchi automaton, or of an infinitary rational relation accepted by a 2-tape Büchi automaton, is not determined by the axiomatic system **ZFC**; notice that here the topological complexity refers to the location of an ω-language in hierarchies, like Borel or Wadge hierarchies, in the Cantor space of infinite words over a finite alphabet Σ, and one assumes, as usually, that **ZFC** is consistent and thus has a model. In particular, there is a 1-counter Büchi automaton $\mathcal{A}$ (respectively, a 2-tape Büchi automaton $\mathcal{B}$) and two models $\mathbf{V}_1$ and $\mathbf{V}_2$ of **ZFC** such that the ω-language $L(\mathcal{A})$ (respectively, the infinitary rational relation $L(\mathcal{B})$) is Borel in $\mathbf{V}_1$ but not in $\mathbf{V}_2$. We have proved in [Fin11] other independence results, showing that some basic cardinality questions on automata reading infinite words actually depend on the models of **ZFC**.

The next step in this research project was to determine which properties of automata actually depend on the models of **ZFC**, and to achieve a more complete investigation of these properties.

Recall that a large cardinal in a model of set theory is a cardinal which is in some sense much larger than the smaller ones. This may be seen as a generalization of the fact that ω is much larger than all *finite* cardinals. The inaccessible cardinals are the simplest such large cardinals. Notice that it cannot be proved in **ZFC** that there exists an inaccessible cardinal, but one usually believes that the existence of such cardinals is consistent with the axiomatic theory **ZFC**. The assumed existence of large cardinals has many consequences in Set Theory as well as in many other branches of Mathematics like Algebra, Topology or Analysis, see [Jec02].

In [Fin15], we recently proved that there exist some 1-counter Büchi automata $\mathcal{A}_n$ for which some elementary properties are independent of theories like $T_n =:$ **ZFC** + "There exist (at least) n inaccessible cardinals", for integers $n \geq 1$. We first proved that "$L(\mathcal{A}_n)$ is Borel", "$L(\mathcal{A}_n)$ is arithmetical", "$L(\mathcal{A}_n)$ is ω-regular", "$L(\mathcal{A}_n)$ is deterministic", and "$L(\mathcal{A}_n)$ is unambiguous" are equivalent to the consistency of the theory T_n (denoted $\mathrm{Cons}(T_n)$). This implies that, if T_n is consistent, all these statements are provable from **ZFC** + "There exist (at least) $n+1$ inaccessible cardinals" but not from **ZFC** + "There exist (at least) n inaccessible cardinals".

We prove in this paper that independence results, even from strong set theories with large cardinals, occur in the theory of various automata over finite words, like 1-counter automata, pushdown automata (equivalent to context-free grammars), 2-tape automata accepting finitary rational relations, weighted automata. We first show that if T is a given recursive theory then there exists an instance of the Post Correspondence Problem (denoted PCP), constituted of two n-tuples $(x_1, x_2, \ldots, x_n)$ and $(y_1, y_2, \ldots, y_n)$ of non-empty words over a finite alphabet Γ, which has no solution if and only if T is consistent. In other words the theory T is consistent if and only if there does not exist any non-empty sequence of indices $i_1, i_2, \ldots, i_k$ such that $x_{i_1} x_{i_2} \cdots x_{i_k} = y_{i_1} y_{i_2} \cdots y_{i_k}$. This allows to find many elementary properties of some pushdown automata, context-free grammars, or 2-tape automata, which are independent from **ZFC** or from some strong theory in the form **ZFC** + "There exist some kind of large cardinals", since many properties of these automata are proved to be undecidable via some effective reductions of the PCP to these properties.

For instance we prove that, for every integer $n \geq 0$, there exist 2-tape automata $\mathcal{A}_n$, $\mathcal{B}_n$, $\mathcal{C}_n$, and $\mathcal{D}_n$, accepting subsets of $A^\star \times B^\star$, for two alphabets A and B, such that $\mathrm{Cons}(T_n)$ is equivalent to each of the following items: (1) $L(\mathcal{A}_n) \cap L(\mathcal{B}_n) = \emptyset$; (2) $L(\mathcal{C}_n) = A^\star \times B^\star$; (3) "$L(\mathcal{D}_n)$ is accepted by a *deterministic* 2-tape automaton"; (4) "$L(\mathcal{D}_n)$ is accepted by a *synchronous* 2-tape automaton". In particular, if **ZFC** + "There exist (at least) n inaccessible cardinals" is consistent, then each of the properties of these 2-tape automata given by items (1)-(4) is provable from **ZFC** + "There exist (at least) $n+1$ inaccessible cardinals" but not from **ZFC** + "There exist (at least) n inaccessible cardinals".

We also prove some independence results for weighted automata, via some independence results for finitely generated matrix subsemigroups of $\mathbb{Z}^{3\times 3}$. Notice that in this context we also obtain results of independence from Peano Arithmetic which make sense since in the context of finite words or of integer matrices everything can be formalized in first-order arithmetic. For instance we show that there exists a finite set of matrices $M_1, M_2, \ldots, M_n \in \mathbb{Z}^{3\times 3}$, for some integer $n \geq 1$, such that: (1) "the subsemigroup of $\mathbb{Z}^{3\times 3}$ generated by these matrices does not contain the zero matrix", and (2) "The property (1) is not provable from **PA**".
These results seem of more concrete mathematical nature than the fact that Cons(**PA**) is an arithmetical statement which is true but unprovable from **PA**. Indeed although our results follow from Gödel's Second Incompleteness Theorem, they express some properties about some natural and simple mathematical objects: the finitely generated subsemigroups of the semigroup $\mathbb{Z}^{3\times 3}$ of 3-3-matrices with integer entries.

This could be compared to the fact that if **PA** (respectively, **ZFC**) is consistent then there is a polynomial $P(x_1, \ldots, x_n)$ which has no integer roots, but for which this cannot be proved from **PA** (respectively, **ZFC**); this result can be inferred from Matiyasevich's Theorem, see [EFT94, end of chapter 10.7]. Notice that Matiyasevich's Theorem is also called the DPRM Theorem since M. Davis, H. Putnam, and J. Robinson spent much time developing the machinery necessary to assert the theorem, before Yuri Matiyasevich finally proved it in 1971. The above results could also be compared with other independence results obtained by Kanamori and McAloon [KM87].

Notice that we recently discovered that in older papers it had been noted that undecidability and incompleteness in automata theory were intimately related and that one could for instance obtain some results about automata which are true but unprovable in some recursive theory extending Peano Arithmetic like **ZFC**, [Har85,JY81]. However the results presented here, although they are not very difficult to prove, exhibit in our opinion the following novelties:

1. We obtain results of a different kind: we show that a large number of elementary properties of automata over finite words, are actually independent from strong set theories.
2. We show how we can effectively construct some automata, like 1-counter or 2-tape automata, for which many elementary properties *reflect the scale of a hierarchy of large cardinals axioms like* "There exist (at least) n inaccessible cardinals" for integers $n \geq 1$.
3. We show how we can use Post Correspondence Problem to get simple combinatorial statements about finite words which are independent from strong set theories.

Altogether we think that the collection of results presented in this paper will be of interest for computer scientists and also for set theorists.

This paper is an extended version of a conference paper which appeared in the Proceedings of the 14th Annual Conference on Theory and Applications

of Models of Computation TAMC 2017, Bern, Switzerland, April 20-22, 2017, [Fin17]. It contains the full proofs which could not be included in the conference paper, due to lack of space.

The paper is organized as follows. We recall some notions and results of set theory in Section 2. We prove some independence results for various kinds of automata over finite words in Section 3. Concluding remarks are given in Section 4.

2 Some Results of Set Theory

We now recall some basic notions of set theory which will be useful in the sequel, and which are exposed in any textbook on set theory, like [Kun80,Jec02]. The logical language of set theory is the language of first-order predicate calculus with equality, with only one binary predicate symbol $\in$. The usual axiomatic system **ZFC** is Zermelo-Fraenkel system **ZF** plus the axiom of choice **AC**.

The axioms of **ZFC** express some natural facts that we consider to hold in the universe of sets. For instance a natural fact is that two sets x and y are equal iff they have the same elements. This is expressed by the *Axiom of Extensionality*:

$$\forall x \forall y \ [\ x = y \leftrightarrow \forall z (z \in x \leftrightarrow z \in y)\ ].$$

Another natural axiom is the *Pairing Axiom* which states that for all sets x and y there exists a set $z = \{x, y\}$ whose elements are x and y:

$$\forall x \forall y \ [\ \exists z (\forall w (w \in z \leftrightarrow (w = x \vee w = y)))].$$

Similarly the *Powerset Axiom* states the existence of the set $\mathcal{P}(x)$ of subsets of a set x. Notice that these axioms are first-order sentences in the usual logical language of set theory whose only non logical symbol is the membership binary relation symbol $\in$. We refer the reader to any textbook on set theory for an exposition of the other axioms of **ZFC**.

A model $(\mathbf{V}, \in)$ of an arbitrary set of axioms $\mathbb{A}$ is a collection $\mathbf{V}$ of sets, equipped with the membership relation $\in$, where "$x \in y$" means that the set x is an element of the set y, which satisfies the axioms of $\mathbb{A}$. We often say "the model $\mathbf{V}$" instead of "the model $(\mathbf{V}, \in)$".

We say that two sets A and B have same cardinality iff there is a bijection from A onto B and we denote this by $A \approx B$. The relation $\approx$ is an equivalence relation. Using the axiom of choice **AC**, one can prove that any set A can be well-ordered so there is an ordinal γ such that $A \approx \gamma$. In set theory the cardinal of the set A is then formally defined as the smallest such ordinal γ.

The infinite cardinals are usually denoted by $\aleph_0, \aleph_1, \aleph_2, \ldots, \aleph_\alpha, \ldots$ The cardinal $\aleph_\alpha$ is also denoted by ω_α, when it is considered as an ordinal. The first infinite ordinal is ω and it is the smallest ordinal which is countably infinite so $\aleph_0 = \omega$ (which could be written ω_0). The first uncountable ordinal is ω_1, and formally $\aleph_1 = \omega_1$.

Let **ON** be the class of all ordinals. Recall that an ordinal α is said to be a successor ordinal iff there exists an ordinal β such that $\alpha = \beta + 1$; otherwise the ordinal α is said to be a limit ordinal and in this case $\alpha = \sup\{\beta \in \mathbf{ON} \mid \beta < \alpha\}$.

We recall now the notions of cofinality of an ordinal and of regular cardinal which may be found for instance in [Jec02]. Let α be a limit ordinal, the cofinality of α, denoted $cof(\alpha)$, is the least ordinal β such that there exists a strictly increasing sequence of ordinals $(\alpha_i)_{i<\beta}$, of length β, such that $\forall i < \beta \quad \alpha_i < \alpha$ and $\sup_{i<\beta} \alpha_i = \alpha$. This definition is usually extended to 0 and to the successor ordinals: $cof(0) = 0$ and $cof(\alpha + 1) = 1$ for every ordinal α. The cofinality of a limit ordinal is always a limit ordinal satisfying: $\omega \leq cof(\alpha) \leq \alpha$. Moreover $cof(\alpha)$ is in fact a cardinal. A cardinal κ is said to be *regular* iff $cof(\kappa) = \kappa$. Otherwise $cof(\kappa) < \kappa$ and the cardinal κ is said to be *singular*.

A cardinal κ is said to be a *(strongly) inaccessible* cardinal iff $\kappa > \omega$, κ is regular, and for all cardinals $\lambda < \kappa$ it holds that $2^\lambda < \kappa$, where 2^λ is the cardinal of $\mathcal{P}(\lambda)$.

We now give the definition of a few more large cardinals.

A cardinal κ is said to be an hyperinaccessible cardinal iff it is an inaccessible cardinal and there are κ inaccessible cardinals below κ. So in that case κ is the κ-th inaccessible cardinal.

Recall that if X is a set of ordinals and $\alpha > 0$ is a limit ordinal, then α is a limit point of X if $\sup(X \cap \alpha) = \alpha$. If κ is an uncountable regular cardinal then a subset $C \subseteq \kappa$ is a closed unbounded set of κ if C is unbounded in κ and if it contains all of its limit points less than κ. A set $S \subseteq \kappa$ is a stationary set if $S \cap C \neq \emptyset$ for every closed unbounded set of κ.

An inaccessible cardinal κ is said to be a Mahlo cardinal iff the set of all regular cardinals below κ is stationary. Notice that every Mahlo cardinal is an hyperinaccessible cardinal, but the converse is not true: if κ is a Mahlo cardinal then κ is actually the κ-th hyperinaccessible cardinal.

There are many other notions of large cardinals which have been studied in set theory. A remarkable fact is that the strenghs of these notions appear to be linearly ordered (and in fact well ordered). For instance if κ is a measurable cardinal then κ is the κ-th Mahlo cardinal, i.e. κ is an hyperMahlo cardinal and thus also an hyperinaccessible cardinal. We refer the interested reader to [Dra74,Kan97,Jec02,Dra85,Pet09] for more results about large cardinals.

Recall that the class of sets in a model $\mathbf{V}$ of **ZF** may be stratified in a transfinite hierarchy, called the *Cumulative Hierarchy*, which is defined by $\mathbf{V} = \bigcup_{\alpha \in \mathbf{ON}} \mathbf{V}_\alpha$, where the sets $\mathbf{V}_\alpha$ are constructed by induction as follows:

(1). $\mathbf{V}_0 = \emptyset$

(2). $\mathbf{V}_{\alpha+1} = \mathcal{P}(\mathbf{V}_\alpha)$ is the set of subsets of $\mathbf{V}_\alpha$, and

(3). $\mathbf{V}_\alpha = \bigcup_{\beta<\alpha} \mathbf{V}_\beta$, for α a limit ordinal.

It is well known that if $\mathbf{V}$ is a model of **ZFC** and κ is an inaccessible cardinal in $\mathbf{V}$ then $\mathbf{V}_\kappa$ is also a model of **ZFC**. If there exist in $\mathbf{V}$ at least n inaccessible cardinals, where $n \geq 1$ is an integer, and if κ is the n-th inaccessible cardinal, then $\mathbf{V}_\kappa$ is also a model of **ZFC** + "There exist exactly $n - 1$ inaccessible cardinals"

(and the same result is true if we replace "inaccessible" by "hyperinaccessible"). This implies that one cannot prove in **ZFC** that there exists an inaccessible cardinal, because if κ is the first inaccessible cardinal in $\mathbf{V}$ then $\mathbf{V}_\kappa$ is a model of **ZFC** + "There exist no inaccessible cardinals".

The theory **ZFC** + "There exist at least n inaccessible cardinals" will be often denoted **ZFC** + $\mathbf{IC}(n)$ in the sequel.

We now recall that a (first-order) theory T in the language of set theory is a set of (first-order) sentences, called the axioms of the theory. If T is a theory and φ is a sentence then we write $T \vdash \varphi$ iff there is a formal proof of φ from T; this means that there is a finite sequence of sentences φ_j, $1 \leq j \leq n$, such that $\varphi_1 \vdash \varphi_2 \vdash \ldots \varphi_n$, where φ_n is the sentence φ and for each $j \in [1, n]$, either φ_j is in T or φ_j is a logical axiom or φ_j follows from $\varphi_1, \varphi_2, \ldots \varphi_{j-1}$ by usual rules of inference which can be defined purely syntactically. A theory T is said to be consistent iff for no (first-order) sentence φ does $T \vdash \varphi$ and $T \vdash \neg\varphi$. If T is inconsistent, then for every sentence φ it holds that $T \vdash \varphi$. Notice that a theory T is inconsistent iff $T \vdash \exists x\ x \neq x$. We shall denote Cons(T) the sentence "the theory T is consistent".

Recall that one can code in a recursive manner the sentences in the language of set theory by finite sequences over a finite alphabet, and then simply over the alphabet $\{0, 1\}$, by using a classical Gödel numbering of the sentences. We say that the theory T is recursive iff the set of codes of axioms in T is a recursive set of words over $\{0, 1\}$. In that case one can also code formal proofs from axioms of a recursive theory T and then Cons(T) is an arithmetical statement. The theory **ZFC** is recursive and so are the theories $T_n =:$ **ZFC** + $\mathbf{IC}(n)$, for any integer $n \geq 1$.

We now recall Gödel's Second Incompleteness Theorem, [Göd63]. Notice the theorem was not originally stated for **ZF**, but we give it for **ZF** since we shall mainly use this form in the sequel.

Theorem 1 (Gödel 1931 [Göd63]). *Let T be a consistent recursive extension of* **ZF**. *Then $T \nvdash \mathrm{Cons}(T)$.*

We now state the following lemma.

Lemma 2. *Let T be a recursive theory in the language of set theory. Then there exists a Turing machine $\mathcal{M}_T$, starting on an empty tape, such that $\mathcal{M}_T$ halts iff T is inconsistent.*

Proof. We describe informally the behaviour of the machine $\mathcal{M}_T$. Essentially the machine works as a program which enumerates all the formal proofs from T and enters in an accepting state and then halts iff the last sentence of the proof is the sentence "$\exists x(x \neq x)$". If the theory T is consistent the machine will never enter in an accepting state q_f and never halts. But if the theory is inconsistent then at some point of the computation the machine sees a proof whose last sentence is actually "$\exists x(x \neq x)$" and halts. □

Remark 3. *Notice that this lemma is proved in* **ZFC**. *This means that if n_T is the index of a Turing machine accepting the (codes of) axioms of the recursive*

theory T, then we can construct from n_T, within **ZFC**, *without verifying that T is consistent or not, a Turing machine $\mathcal{M}_T$ such that $\mathcal{M}_T$ halts iff T is inconsistent. Similar remarks could be stated for other results in the sequel.*

In [Fin15] we have focused our results on set theories, even if we noticed that some of our results could be extended to weaker arithmetical theories and to other recursive theories. We have shown that some elementary properties of automata may be independent from strong set theories like **ZFC** + **IC**(n). We are going to show in this paper that some similar phenomena still hold for some kinds of automata on finite words. However in the context of automata over finite words, we can notice that automata and their behaviour can be coded by integers and this can be done in Peano arithmetic; this will be often assumed in the sequel. Then we shall also obtain some new independence results from the axiomatic system of Peano Arithmetic **PA**. Indeed while we have first stated Gödel's Second Incompleteness Theorem for consistent recursive extensions of **ZF** in the above Theorem 1, the proof of this Theorem leads also to the following version, see [Poi00] for a proof.

Theorem 4 (Gödel 1931). *Let* **PA** *be Peano Arithmetic. Then* $\mathbf{PA} \nvdash \mathrm{Cons}(\mathbf{PA})$.

Notice that **PA** is known to be consistent, since the axioms of Peano Arithmetic are satisfied in the standard model of the natural numbers. Thus the above Theorem 4 gives a true arithmetical statement which is not provable from Peano Arithmetic. Notice that Gentzen gave in 1936 a proof of the consistency of Peano Arithmetic which uses only transfinite induction up to the Cantor ordinal ε_0, see [Gen36,Hor14]; this proof can be considered as being finitistic since the ordinal ε_0 can be coded with finite objects, like finite trees.

3 Incompleteness results for automata over finite words

We assume the reader to be familiar with the theory of formal languages [HMU01]. We recall the usual notations of formal language theory.

If Σ is a finite alphabet, a *non-empty finite word* over Σ is any sequence $x = a_1 \ldots a_k$, where $a_i \in \Sigma$ for $i = 1, \ldots, k$, and k is an integer ≥ 1. The *length* of x is k, denoted by $|x|$. The *empty word* has no letters and is denoted by ε; its length is 0. $\Sigma^\star$ is the *set of finite words* (including the empty word) over Σ.

The usual concatenation product of two finite words u and v is denoted $u \cdot v$ (and sometimes just uv). This product is extended to the product of a finite word u and an ω-word v: the infinite word $u \cdot v$ is then the ω-word such that:

$(u \cdot v)(k) = u(k)$ if $k \leq |u|$, and $(u \cdot v)(k) = v(k - |u|)$ if $k > |u|$.

We now recall the well known Post Correspondence Problem (PCP), see [HMU01, pages 392-402]. It is one of the famous undecidable problems in Theoretical Computer Science and in Formal Language Theory. The PCP is an abstract problem involving strings, and it has been very useful to prove the undecidability of many other problems by reduction of PCP to those problems.

In particular, many problems about context-free languages, those accepted by pushdown automata or generated by context-free grammars, have been shown to be undecidable by this method. For instance it follows from the undecidability of the Post Correspondence Problem that the universality problem, the inclusion and the equivalence problems for context-free languages are also undecidable.

An instance of the Post Correspondence Problem consists of two lists of finite words over some finite alphabet Γ: $(x_1, x_2, \ldots, x_n)$ and $(y_1, y_2, \ldots, y_n)$. Notice that the two lists must have the same length $n \geq 1$. One says that this instance has a solution if there exists a non-empty sequence of indices $i_1, i_2, \ldots, i_k$ such that $x_{i_1} x_{i_2} \cdots x_{i_k} = y_{i_1} y_{i_2} \cdots y_{i_k}$. The Post Correspondence Problem is:

"Given an instance of the PCP, tell whether this instance has a solution".

We now recall Post's result, well-known as the undecidability of the Post Correspondence Problem.

Theorem 5. *[Post, see [HMU01]] Let Γ be an alphabet having at least two elements. Then it is undecidable to determine, for arbitrary n-tuples $(x_1, x_2, \ldots, x_n)$ and $(y_1, y_2, \ldots, y_n)$ of non-empty words in $\Gamma^\star$, whether there exists a non-empty sequence of indices $i_1, i_2, \ldots, i_k$ such that $x_{i_1} x_{i_2} \cdots x_{i_k} = y_{i_1} y_{i_2} \cdots y_{i_k}$.*

Recall that we know, from the standard proof of the undecidability of the PCP, that the halting problem for Turing machines can be reduced to the PCP, see [HMU01]: to every Turing machine $\mathcal{M}_z$ of index z, we can associate an instance of the PCP such that this instance has a solution iff the Turing machine $\mathcal{M}_z$, starting with an empty tape, halts.

We can now state the following result. Notice that the following theorem is stated in a very general form. In particular, it holds for *any recursive theory T in the language of set theory with no restrictions on T*, or for Peano arithmetic.

Theorem 6. *Let T be a recursive theory in the language of set theory or $T = \mathbf{PA}$. Then there exist two n-tuples $X_T = (x_1, x_2, \ldots, x_n)$ and $Y_T = (y_1, y_2, \ldots, y_n)$ of finite words over a finite alphabet Σ, such that there exists a non-empty sequence of indices $i_1, i_2, \ldots, i_k$ such that $x_{i_1} x_{i_2} \cdots x_{i_k} = y_{i_1} y_{i_2} \cdots y_{i_k}$ iff T is inconsistent.*

Proof. Let T be a recursive theory in the language of set theory or $T = \mathbf{PA}$. Then there exists a Turing machine $\mathcal{M}$, starting with an empty tape, which halts if and only if the theory T is inconsistent. We can now deduce the announced result from the fact, recalled after Theorem 5, that the halting problem for Turing machines can be reduced to the PCP. $\square$

Remark 7. *We can easily see that the above theorem is true for the two-letter alphabet $\Sigma = \{a, b\}$. Indeed if $\Sigma = \{a_1, a_2, \ldots, a_p\}$ is an alphabet having more than two letters, we can use the coding given by: $a_j \to b^j a$, where a and b are two letters, which provides the announced claim.*

Corollary 8. *For every integer $n \geq 0$, there exist $p \geq 1$ and two p-tuples $X_{T,n} = (x_{1,n}, x_{2,n}, \ldots, x_{p,n})$ and $Y_{T,n} = (y_{1,n}, y_{2,n}, \ldots, y_{p,n})$ of finite words over $\Sigma =$*

$\{a, b\}$, *such that: "P_n: there exist no non-empty sequence of indices $i_1, i_2, \ldots, i_k$ such that: $x_{i_1,n}x_{i_2,n}\cdots x_{i_k,n} = y_{i_1,n}y_{i_2,n}\cdots y_{i_k,n}$ " iff T_n=: **ZFC** + **IC**(n) is consistent.*

In particular, if **ZFC** + **IC**(n) *is consistent, then P_n is provable from* **ZFC** + **IC**$(n+1)$ *but not from* **ZFC** + **IC**(n).

Proof. By Theorem 6, for each integer $n \geq 0$, there exist $p \geq 1$ and two p-tuples $X_{T,n} = (x_{1,n}, x_{2,n}, \ldots, x_{p,n})$ and $Y_{T,n} = (y_{1,n}, y_{2,n}, \ldots, y_{p,n})$ of finite words over $\Sigma = \{a, b\}$, such that: "P_n: there exist no non-empty sequence of indices $i_1, i_2, \ldots, i_k$ such that $x_{i_1,n}x_{i_2,n}\cdots x_{i_k,n} = y_{i_1,n}y_{i_2,n}\cdots y_{i_k,n}$ " iff T_n=: **ZFC** + **IC**(n) is consistent.

Recall that one can prove from **ZFC** + **IC**$(n+1)$ that if κ is the $n+1$-th inaccessible cardinal, then the set $\mathbf{V}_\kappa$ of the cumulative hierarchy is also a model of **ZFC** + **IC**(n). This implies, by the Completeness Theorem, that the theory **ZFC** + **IC**(n) is consistent since it has a set model. This shows that:

$$\mathbf{ZFC} + \mathbf{IC}(n+1) \vdash \mathrm{Cons}(\mathbf{ZFC} + \mathbf{IC}(n))$$

Thus **ZFC** + **IC**$(n+1)$ also implies that there exist no non-empty sequence of indices $i_1, i_2, \ldots, i_k$ such that:

$$x_{i_1,n}x_{i_2,n}\cdots x_{i_k,n} = y_{i_1,n}y_{i_2,n}\cdots y_{i_k,n}$$

On the other hand assume that T_n=: **ZFC** + **IC**(n) is consistent. Then, since T_n is a consistent recursive extension of **ZFC**, we can infer from Gödel's Second Incompleteness Theorem that $T_n \nvdash \mathrm{Cons}(T_n)$. Thus P_n, which is (provably in **ZFC**) equivalent to $\mathrm{Cons}(T_n)$, is also not provable from T_n. □

Moreover, since **PA** is consistent, we also get the following result.

Corollary 9. *There exist two p-tuples $X = (x_1, x_2, \ldots, x_p)$ and $Y = (y_1, y_2, \ldots, y_p)$ of finite words over $\Sigma = \{a, b\}$, such that:*
(1) *there exist no non-empty sequence of indices $i_1, i_2, \ldots, i_k$ such that:*

$$x_{i_1}x_{i_2}\cdots x_{i_k} = y_{i_1}y_{i_2}\cdots y_{i_k}$$

(2) *The property* (1) *is not provable from* **PA**.

We can now infer from Theorem 6 some incompleteness results for context-free languages generated by context-free grammars or equivalently accepted by pushdown automata. We use the reductions of PCP to some problems about context-free grammars and context-free languages given in [HMU01, pages 404-408]. We refer the reader to this textbook for background about context-free grammars and context-free languages.

We first state the following result about ambiguity of context-free grammars.

Theorem 10. *Let T be a recursive theory in the language of set theory or $T =$* **PA**. *Then there exists a context-free grammar G_T which is unambiguous iff T is consistent.*

Proof. We refer here to the proof of the undecidability of the unambiguity of a given context-free grammar in [HMU01, pages 404-406]. From a given instance of the PCP constituted by two n-tuples $(x_1, x_2, \ldots, x_n)$ and $(y_1, y_2, \ldots, y_n)$ of finite words over a finite alphabet Σ, is constructed a context-free grammar G such that G is ambiguous if and only if this instance of PCP has a solution. The result now follows from this construction and from the above Theorem 6. $\square$

Corollary 11. *For every integer $n \geq 0$, there exists a context-free grammar G_n such that G_n is unambiguous iff T_n is consistent.*

In particular, if **ZFC** + **IC**(n) *is consistent, then " G_n is unambiguous" is provable from* **ZFC** + **IC**$(n+1)$ *but not from* **ZFC** + **IC**(n).

We now state some other results about elementary properties of context-free languages.

Theorem 12. *Let T be a recursive theory in the language of set theory or $T =$* **PA**. *Then there exist context-free grammars $G_{1,T}$ $G_{2,T}$, $G_{3,T}$, and $G_{4,T}$, such that* $\mathrm{Cons}(T)$ *is equivalent to each of the following items:*
(1) $L(G_{1,T}) \cap L(G_{2,T}) = \emptyset$;
(2) $L(G_{3,T}) = L(G_{4,T})$;
(3) $L(G_{3,T}) = \Gamma^\star$, for some alphabet Γ.

Proof. We refer here to the proof of Theorem 9.22 in [HMU01, page 408]. In this proof, from a given instance of the PCP constituted by two n-tuples $(x_1, x_2, \ldots, x_n)$ and $(y_1, y_2, \ldots, y_n)$ of finite words over a finite alphabet Σ, are constructed some context-free grammars G_1 G_2, G_3, and G_4, such that:
(1) $L(G_1) \cap L(G_2) = \emptyset$ iff this instance of PCP has no solution.
(2) $L(G_3) = L(G_4)$ iff this instance of PCP has no solution.
(3) $L(G_3) = \Gamma^\star$, for some alphabet Γ, iff this instance of PCP has no solution.

The announced result now follows from these constructions and from the above Theorem 6. $\square$

Corollary 13. *For every integer $n \geq 0$, there exist context-free grammars $G_{1,n}$ $G_{2,n}$, $G_{3,n}$, and $G_{4,n}$, such that* $\mathrm{Cons}(T_n)$ *is equivalent to each of the following items:*
(1) $L(G_{1,n}) \cap L(G_{2,n}) = \emptyset$;
(2) $L(G_{3,n}) = L(G_{4,n})$;
(3) $L(G_{3,n}) = \Gamma^\star$, for some alphabet Γ.

In particular, if **ZFC** + **IC**(n) *is consistent, then each of the properties of these context-free languages given by Items (1)-(3) is provable from* **ZFC** + **IC**$(n+1)$ *but not from* **ZFC** + **IC**(n).

We are now going to state some similar independence results for other very simple finite machines reading finite words: the class of 2-tape automata (or transducers) accepting finitary rational relations. We shall refer to the book [Ber79] in which some elementary problems about finitary rational relations are

proved to be undecidable by reducing the PCP to these problems, see pages 79-82 in this book.

We now state the following results.

Theorem 14. *Let T be a recursive theory in the language of set theory or $T =$ **PA**. Then there exist 2-tape automata $\mathcal{A}$, $\mathcal{B}$, and $\mathcal{C}$, accepting finitary rational relations $X, Y, Z \subseteq A^\star \times B^\star$, for two alphabets A and B having at least two letters, and such that* $\mathrm{Cons}(T)$ *is equivalent to each of the following items:*
(1) $X \cap Y = \emptyset$;
(2) $Z = A^\star \times B^\star$;
(3) $A^\star \times B^\star \subseteq Z$.

Proof. We refer to the proof of [Ber79, Theorem 8.4, page 81]. We assume, as in this proof, that A contains exactly two letters and that $A = \{a, b\}$. For two sequences $u_1, u_2, \ldots, u_p$, and $v_1, v_2, \ldots, v_p$, of finite words over the alphabet B, we define $U = \{(ab, u_1), \ldots, (ab^p, u_p)\}$, and $V = \{(ab, v_1), \ldots, (ab^p, v_p)\}$. Then U^+ and V^+ are rational relations and, by [Ber79, Lemma 8.3, page 80], the relations $\bar{U} = A^\star \times B^\star \setminus U^+$ and $\bar{V} = A^\star \times B^\star \setminus V^+$ are also rational. It is noticed in the proof of Theorem 8.4 in [Ber79] that if we set $X = U^+$ and $Y = V^+$, then it holds that $X \cap Y \neq \emptyset$ iff the instance of the PCP given by $(u_1, u_2, \ldots, u_p)$, and $(v_1, v_2, \ldots, v_p)$ has a solution. Item (1) of the Theorem follows then from the above Theorem 6. Moreover if we set $Z = \bar{U} \cup \bar{V}$, then $Z = A^\star \times B^\star$ iff $X \cap Y = \emptyset$, and this implies Items (2) and (3). $\square$

Using a 2-tape automaton $\mathcal{C}$ accepting the finitary relation Z given by the above theorem, it is easy to construct, with similar methods as in the paper [Fin03] about infinitary rational relations, another 2-tape automaton $\mathcal{D}$ accepting a finitary rational relation $L \subseteq A^\star \times B^\star$ such that L is accepted by a *deterministic* 2-tape automaton iff L is accepted by a *synchronous* 2-tape automaton iff $Z = A^\star \times B^\star$. Thus we can state the following result. The detailed proof is here left to the reader.

Theorem 15. *Let T be a recursive theory in the language of set theory or $T =$ **PA**. Then there exists a 2-tape automaton $\mathcal{D}$, accepting a finitary rational relation $L \subseteq A^\star \times B^\star$, for two alphabets A and B having at least two letters, and such that* $\mathrm{Cons}(T)$ *is equivalent to each of the following items:*
(1) L is accepted by a deterministic 2-tape automaton;
(2) L is accepted by a synchronous 2-tape automaton.

Corollary 16. *For every integer $n \geq 0$, there exist 2-tape automata $\mathcal{A}_n$, $\mathcal{B}_n$, $\mathcal{C}_n$, and $\mathcal{D}_n$, accepting subsets of $A^\star \times B^\star$, for two alphabets A and B having at least two letters, such that* $\mathrm{Cons}(T_n)$ *is equivalent to each of the following items:*
(1) $L(\mathcal{A}_n) \cap L(\mathcal{B}_n) = \emptyset$;
(2) $L(\mathcal{C}_n) = A^\star \times B^\star$;
(3) $L(\mathcal{D}_n)$ is accepted by a deterministic 2-tape automaton;
(4) $L(\mathcal{D}_n)$ is accepted by a synchronous 2-tape automaton.

In particular, if **ZFC** + **IC**(n) *is consistent, then each of the properties of these 2-tape automata given by Items (1)-(4) is provable from* **ZFC** + **IC**$(n+1)$ *but not from* **ZFC** + **IC**(n).

Since **PA** is consistent, we get the following result from Theorems 14 and 15 (where we assume, as we have already said at the beginning of this section, that automata are coded by integers):

Corollary 17. *There exist 2-tape automata $\mathcal{A}$, $\mathcal{B}$, $\mathcal{C}$, and $\mathcal{D}$, accepting subsets of $A^\star \times B^\star$, for two alphabets A and B having at least two letters, such that*
(1) $L(\mathcal{A}) \cap L(\mathcal{B}) = \emptyset$.
(2) $L(\mathcal{C}) = A^\star \times B^\star$.
(3) $L(\mathcal{D})$ is accepted by a deterministic 2-tape automaton.
(4) $L(\mathcal{D})$ is accepted by a synchronous 2-tape automaton.
But none of the items $(1) - (4)$ is provable from **PA**.

We are now going to state some incompleteness results about weighted automata. We shall also state some incompleteness results about finitely generated semigroups of matrices with integer entries (with the semigroup operation of multiplication of matrices) which can be presented by automata with multiplicities, see [Har02].

We first recall the notion of an n-state $\mathbb{Z}$-automaton, i.e. a non-deterministic automaton with integer multiplicities, as presented in [Har02].

A non-deterministic $\mathbb{Z}$-automaton is a 5-tuple $\mathcal{A} = (\Sigma, Q, \delta, J, F)$, where: $\Sigma = \{a_1, a_2, \ldots, a_k\}$ is a finite input alphabet and the letter a_i is associated to a matrix $M_i \in \mathbb{Z}^{n\times n}$; $Q = \{1, 2, \ldots, n\}$ is the state set (and i corresponds to the ith row and column of the matrices); J is the set of initial states and $F \subseteq Q$ is the set of final states; δ is the set of transitions that provides the rules

$$r \xrightarrow{\binom{a_i}{m}} s,$$

where $a_i \in \Sigma$, and $m = (M_i)_{rs}$ is the multiplicity of the rule.

A path

$$\pi = s_1 \xrightarrow{\binom{b_1}{m_1}} s_2 \xrightarrow{\binom{b_2}{m_2}} s_3 \longrightarrow \cdots \longrightarrow s_t \xrightarrow{\binom{b_t}{m_t}} s_{t+1}$$

is a computation of the automaton $\mathcal{A}$ reading a word $w = b_1 b_2 \ldots b_t \in \Sigma^\star$ and the multiplicity of this path is equal to $\|\pi\| = m_1 m_2 \ldots m_t \in \mathbb{Z}$. For a word $w \in \Sigma^\star$ we denote by Π_{rs} the set of the paths of $\mathcal{A}$ reading the word w which go from state r to state s. Then the multiplicity of the word $w = a_{i_1} a_{i_2} \cdots a_{i_t} \in \Sigma^\star$ from r to s is the sum

$$\mathcal{A}_{rs}(w) = \sum_{\pi \in \Pi_{rs}} \|\pi\| = (M_{i_1} M_{i_2} \ldots M_{i_t})_{rs}$$

and we get the multiplicity of w in $\mathcal{A}$ from the accepting paths:

$$\mathcal{A}(w) = \sum_{r \in J, s \in F} \mathcal{A}_{rs}(w) = \sum_{r \in J, s \in F} (M_{i_1} M_{i_2} \ldots M_{i_t})_{rs}.$$

We first state the following result.

Theorem 18. *Let T be a recursive theory in the language of set theory or $T = \mathbf{PA}$. Then there exists a finite set of matrices $M_1, M_2, \ldots, M_n \in \mathbb{Z}^{3\times 3}$, for some integer $n \geq 1$, such that the subsemigroup of $\mathbb{Z}^{3\times 3}$ generated by these matrices does not contain any matrix M with $M_{13} = 0$ if and only if T is consistent.*

Proof. Let T be a recursive theory in the language of set theory or $T = \mathbf{PA}$, and let two n-tuples $X_T = (x_1, x_2, \ldots, x_n)$ and $Y_T = (y_1, y_2, \ldots, y_n)$ of finite words over a finite alphabet Σ, which are given by the above Theorem 6. Then there exists a non-empty sequence of indices $i_1, i_2, \ldots, i_k$ such that $x_{i_1} x_{i_2} \cdots x_{i_k} = y_{i_1} y_{i_2} \cdots y_{i_k}$ iff T is inconsistent.

It follows from the proof of [Har02, Theorem 8 page 62] that there exists a finite set of matrices $M_1, M_2, \ldots, M_n \in \mathbb{Z}^{3\times 3}$, such that the subsemigroup of $\mathbb{Z}^{3\times 3}$ generated by these matrices contains a matrix M with $M_{13} = 0$ if and only if the instance $X_T = (x_1, x_2, \ldots, x_n)$ and $Y_T = (y_1, y_2, \ldots, y_n)$ of the PCP has a solution.

Therefore the subsemigroup of $\mathbb{Z}^{3\times 3}$ generated by these matrices does not contain any matrix M with $M_{13} = 0$ if and only if the instance $X_T = (x_1, x_2, \ldots, x_n)$ and $Y_T = (y_1, y_2, \ldots, y_n)$ of the PCP has no solution if and only if T is consistent. □

One can easily state corollaries of the above Theorem for strong set theories, as for previous results in this paper. Details are here left to the reader. Moreover, since **PA** is consistent, we also get the following result.

Corollary 19. *There exists a finite set of matrices $M_1, M_2, \ldots, M_n \in \mathbb{Z}^{3\times 3}$, for some integer $n \geq 1$, such that:*
(1) the subsemigroup of $\mathbb{Z}^{3\times 3}$ generated by these matrices does not contain any matrix M with $M_{13} = 0$, and
(2) The property (1) is not provable from **PA**.

We also get the following result as a corollary of the above Theorem 18.

Corollary 20. *Let T be a recursive theory in the language of set theory or $T = \mathbf{PA}$. Then there exists a 3-state $\mathbb{Z}$-automaton $\mathcal{A}$ such that $\mathcal{A}$ accepts a word with multiplicity zero iff T is inconsistent.*

Proof. It follows from the above Theorem 18 in the same way as Corollary 1 follows from Theorem 8 in [Har02]. □

Corollary 21. *Let T be a recursive theory in the language of set theory or $T = \mathbf{PA}$. Then there exists two 2-state $\mathbb{N}$-automata $\mathcal{A}$ and $\mathcal{B}$ such that $\mathcal{A}$ and $\mathcal{B}$ accept a word w with the same multiplicity iff T is inconsistent.*

Proof. It is proved in the same way as for the above Corollary 20 following the proof of Corollary 2 in [Har02]. □

One can easily state corollaries of the above one for strong set theories or for Peano Arithmetic, as for previous results in this paper. Details are here left to the reader.

Following an idea of Paterson, Halava and Harju proved in [HH01] that it is undecidable for finitely generated subsemigroups S of $\mathbb{Z}^{3\times 3}$ whether S contains a matrix with $M_{11} = 0$. We now prove the following result.

Theorem 22. *Let T be a recursive theory in the language of set theory or $T =$ **PA**. Then there exists a finite set of matrices $M_1, M_2, \ldots, M_n \in \mathbb{Z}^{3\times 3}$, for some integer $n \geq 1$, such that the subsemigroup of $\mathbb{Z}^{3\times 3}$ generated by these matrices does not contain any matrix M with $M_{11} = 0$ if and only if T is consistent.*

Proof. Let T be a recursive theory in the language of set theory or $T = \mathbf{PA}$, and let two n-tuples $X_T = (x_1, x_2, \ldots, x_n)$ and $Y_T = (y_1, y_2, \ldots, y_n)$ of finite words over a finite alphabet Σ, which are given by the above Theorem 6. Then there exists a non-empty sequence of indices $i_1, i_2, \ldots, i_k$ such that $x_{i_1} x_{i_2} \cdots x_{i_k} = y_{i_1} y_{i_2} \cdots y_{i_k}$ iff T is inconsistent.

It follows from the proof of [HH01, Theorem 3 page 651] that there exists a finite set of matrices $N_1, N_2, \ldots, N_n$ and $N'_1, N'_2, \ldots, N'_n \in \mathbb{Z}^{3\times 3}$, such that the subsemigroup of $\mathbb{Z}^{3\times 3}$ generated by all these matrices contains a matrix M with $M_{11} = 0$ if and only if the instance $X_T = (x_1, x_2, \ldots, x_n)$ and $Y_T = (y_1, y_2, \ldots, y_n)$ of the PCP has a solution.

Therefore the subsemigroup of $\mathbb{Z}^{3\times 3}$ generated by these matrices does not contain any matrix M with $M_{11} = 0$ if and only if the instance $X_T = (x_1, x_2, \ldots, x_n)$ and $Y_T = (y_1, y_2, \ldots, y_n)$ of the PCP has no solution if and only if T is consistent. $\square$

Recall that Paterson proved in 1970 that the mortality problem for finitely generated subsemigroups S of $\mathbb{Z}^{3\times 3}$ is undecidable, i.e. that one cannot decide, for a given set of matrices $M_1, M_2, \ldots, M_n \in \mathbb{Z}^{3\times 3}$, whether the zero matrix (whose all coefficients are equal to zero) belongs to the subsemigroup generated by the matrices $M_1, M_2, \ldots, M_n$, i.e. whether there exists a sequence of integers $i_1, i_2, \ldots i_k$, such that $M_{i_1} M_{i_2} \ldots M_{i_k} = 0$. Halava and Harju gave a proof of this result in [HH01].

We can now state the following result.

Theorem 23. *Let T be a recursive theory in the language of set theory or $T =$ **PA**. Then there exists a finite set of matrices $M_1, M_2, \ldots, M_n \in \mathbb{Z}^{3\times 3}$, for some integer $n \geq 1$, such that the subsemigroup of $\mathbb{Z}^{3\times 3}$ generated by these matrices does not contain the zero matrix if and only if T is consistent.*

Proof. If follows from the proof of the undecidability of the mortality problem for finitely generated subsemigroups S of $\mathbb{Z}^{3\times 3}$ given in [HH01], and from the above Theorem 22.

Indeed the above Theorem 22 states that there exists a finite set of matrices $M_1, M_2, \ldots, M_n \in \mathbb{Z}^{3\times 3}$, for some integer $n \geq 1$, such that the subsemigroup S of $\mathbb{Z}^{3\times 3}$ generated by these matrices does not contain any matrix M with $M_{11} = 0$ if and only if T is consistent. Then it follows from the proof of Theorem 4 of [HH01] that if B is the idempotent matrix $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$ and if R is the subsemigroup of $\mathbb{Z}^{3\times 3}$ generated by the matrices $M_1, M_2, \ldots, M_n$ and B, then the subsemigroup R does not contain the zero matrix if and only if the subsemigroup S does not contain any matrix M with $M_{11} = 0$ and thus if and only if the theory T is consistent. □

Corollary 24. *For every integer $p \geq 0$, there exists a finite set of matrices $M_1, M_2, \ldots, M_{n_p} \in \mathbb{Z}^{3\times 3}$, for some integer $n_p \geq 1$, such that the subsemigroup of $\mathbb{Z}^{3\times 3}$ generated by these matrices does not contain the zero matrix if and only if T'_p is consistent.*

In particular, **ZFC** + **IC**(p) *is consistent, then the property "The subsemigroup of $\mathbb{Z}^{3\times 3}$ generated by the matrices $M_1, M_2, \ldots, M_{n_p}$, does not contain the zero matrix" is provable from* **ZFC** + **IC**$(p+1)$ *but not from* **ZFC** + **IC**(p).

Moreover, since **PA** is consistent, we also get the following result.

Corollary 25. *There exists a finite set of matrices $M_1, M_2, \ldots, M_n \in \mathbb{Z}^{3\times 3}$, for some integer $n \geq 1$, such that:*
(1) the subsemigroup of $\mathbb{Z}^{3\times 3}$ generated by these matrices does not contain the zero matrix, and
(2) The property (1) is not provable from **PA**.

We have used in the proof of the above results some effective reductions of the PCP to some undecidable problems and an independence result about the solutions of some instances of the PCP. We can also sometimes use directly some effective reductions of the halting problem for Turing machines to some undecidable problems along with the above Lemma 2.

We now give some examples of independence results we can get by using this lemma.

Theorem 26. *Let T be a recursive theory in the language of set theory or $T =$* **PA**. *Then there exists a 1-counter automaton $\mathcal{A}$, reading finite words over a finite alphabet Σ, such that $L(\mathcal{A}) = \Sigma^\star$ if and only if T is consistent.*

Proof. Recall that Ibarra proved in [Iba79] that the universality problem for languages of 1-counter automata (and actually for some very restricted classes of 1-counter automata) is undecidable. He constructed, for each single-tape Turing machine $\mathcal{M}$, a 1-counter automaton $\mathcal{A}$, reading finite words over a finite alphabet Σ, such that $L(\mathcal{A}) = \Sigma^\star$ iff the machine $\mathcal{M}$ does not halt on the blank tape. The result now follows from the above Lemma 2. □

We can now prove the following result.

Theorem 27. *Let T be a recursive theory in the language of set theory or $T = \mathbf{PA}$. Then there exists a 1-counter automaton $\mathcal{A}$, reading finite words over a finite alphabet Σ, such that* $\mathrm{Cons}(T)$ *is equivalent to each of the following items:*
(1) $L(\mathcal{A}) = \Sigma^\star$;
(2) $L(\mathcal{A})$ is accepted by a deterministic 1-counter automaton;
(3) $L(\mathcal{A})$ is accepted by an unambiguous 1-counter automaton.

Proof. Let T be a recursive theory in the language of set theory or $T = \mathbf{PA}$. We first assume that the 1-counter automaton $\mathcal{A}$ given by Theorem 26 reads words over a two-letter alphabet $\Sigma = \{a, b\}$; it is easy to get this result by a simple coding if Σ has more than two letters.

Let now $\Gamma = \{a, b, c\}$ where c is a new letter not in Σ and let $L \subseteq \Gamma^\star$ be the finitary language defined by:

$$L = \{a^n b^n a^p \mid n \geq 1 \text{ and } p \geq 1\} \cup \{a^n b^p a^p \mid n \geq 1 \text{ and } p \geq 1\}$$

and let $\mathcal{L} \subseteq \Gamma^\star$ be the finitary language defined by:

$$\mathcal{L} = L(\mathcal{A})c\Sigma^\star \cup \Sigma^\star cL \cup L_c$$

where $L_c \subseteq \Gamma^\star$ is the set of finite words over Γ containing not any letter c or at least two letters c.

It is then easy to see that the language $\mathcal{L}$ is accepted by a 1-counter automaton $\mathcal{B}$ which can be effectively constructed from the 1-counter automaton $\mathcal{A}$ since the language L is obviously accepted by a 1-counter automaton, the language L_c is regular and thus accepted by an automaton (without any counter), and the class of finitary languages accepted by non-deterministic 1-counter automata is closed under finite union.

There are now two cases.
(1) First case. The theory T is consistent and then the automaton $\mathcal{A}$ given by Theorem 26 satisfies $L(\mathcal{A}) = \Sigma^\star$. Therefore $\mathcal{L} = L(\mathcal{B}) = \Gamma^\star$ is regular and thus it is accepted by a deterministic hence unambiguous automaton (without any counter).

(2) Second case. The theory T is inconsistent and then the automaton $\mathcal{A}$ given by Theorem 26 satisfies $L(\mathcal{A}) \neq \Sigma^\star$. Therefore there exists a finite word $u \in \Sigma^\star \setminus L(\mathcal{A})$. Let us now consider the language

$$L_1 = uc\Sigma^\star \cap L(\mathcal{B}) = ucL$$

It is straightforward to see that this language is accepted by a 1-counter automaton, since $uc\Sigma^\star$ is rational and the class of 1-counter languages is closed under intersection with rational languages. On the other hand it is well known that the language L is not accepted by any unambiguous 1-counter automaton (and even by any unambiguous pushdown automaton). This implies easily that the language L_1 itself is not accepted by any unambiguous 1-counter automaton (and even by any unambiguous pushdown automaton). Moreover this implies that the

language $L(\mathcal{B})$ is not accepted by any unambiguous 1-counter automaton, and thus also by any deterministic 1-counter automaton, because the class of languages accepted by unambiguous 1-counter automata (respectively, deterministic 1-counter automata) is closed under intersection with rational languages. $\square$

Corollary 28. *For every integer $n \geq 0$, there exists a 1-counter automaton $\mathcal{A}_n$, reading finite words over a finite alphabet Σ, such that* $\mathrm{Cons}(T_n)$ *is equivalent to each of the following items:*
(1) $L(\mathcal{A}_n) = \Sigma^\star$;
(2) $L(\mathcal{A}_n)$ is accepted by a deterministic 1-counter automaton;
(3) $L(\mathcal{A}_n)$ is accepted by an unambiguous 1-counter automaton.

In particular, if $\mathbf{ZFC} + \mathbf{IC}(n)$ *is consistent, then each of the properties of the 1-counter automaton $\mathcal{A}_n$ given by Items (1)-(3) is provable from* $\mathbf{ZFC} + \mathbf{IC}(n+1)$ *but not from* $\mathbf{ZFC} + \mathbf{IC}(n)$.

Remark 29. *Part of Theorem 27 and of Corollary 28 subsumes Items (2) and (3) of Theorem 12 and of Corollary 13. Indeed we can construct, from a given pushdown automaton (and thus also from a given 1-counter automaton) accepting a finitary language, a context-free grammar generating the same language.*

4 Concluding remarks

We have shown that some very elementary properties of some automata over finite words are actually independent from strong set theories like $\mathbf{ZFC} + \mathbf{IC}(n)$. The results of this paper are true for other large cardinals than inaccessible ones. For instance we can replace inaccessible cardinals by hyperinaccessible, Mahlo, hyperMahlo, ... and still other ones and obtain similar results.

Some of our results are even more general because they could have been stated for more general recursive theories,

Acknowledgements. We thank the anonymous referees for their very useful comments on a preliminary version of this paper.

References

[Ber79] J. Berstel. *Transductions and context free languages.* Teubner Studienbücher Informatik, 1979. Available from: http://www-igm.univ-mlv.fr/ berstel/LivreTransductions/LivreTransductions.html.

[Dra74] F.R. Drake. *Set Theory, An Introduction to Large cardinals*, volume 76 of *Studies in Logic and the Foundations of Mathematics.* North-Holland, 1974.

[Dra85] F. R. Drake. How recent work in mathematical logic relates to the foundations of mathematics. *The Mathematical Intelligencer*, 7(4):27–35, 1985.

[EFT94] H.-D. Ebbinghaus, J. Flum, and W. Thomas. *Mathematical logic.* Undergraduate Texts in Mathematics. Springer-Verlag, New York, second edition, 1994. Translated from the German by Margit Meßmer.

[Fin03] O. Finkel. Undecidability of topological and arithmetical properties of infinitary rational relations. *RAIRO-Theoretical Informatics and Applications*, 37(2):115–126, 2003.

[Fin09] O. Finkel. The complexity of infinite computations in models of set theory. *Logical Methods in Computer Science*, 5(4:4):1–19, 2009.

[Fin11] O. Finkel. Some problems in automata theory which depend on the models of set theory. *RAIRO - Theoretical Informatics and Applications*, 45(4):383–397, 2011.

[Fin15] O. Finkel. Incompleteness theorems, large cardinals, and automata over infinite words. In Magnús M. Halldórsson, Kazuo Iwama, Naoki Kobayashi, and Bettina Speckmann, editors, *Automata, Languages, and Programming - 42nd International Colloquium, ICALP 2015, Kyoto, Japan, July 6-10, 2015, Proceedings, Part II*, volume 9135 of *Lecture Notes in Computer Science*, pages 222–233. Springer, 2015.

[Fin17] O. Finkel. Incompleteness theorems, large cardinals, and automata over finite words. In T. V. Gopal, Gerhard Jäger, and Silvia Steila, editors, *Proceedings of the 14th Annual Conference on Theory and Applications of Models of Computation TAMC 2017, Bern, Switzerland, April 20-22, 2017*, volume 10185 of *Lecture Notes in Computer Science*, pages 231–246, 2017.

[Fri11] Harvey M. Friedman. My forty years on his shoulders. In *Kurt Gödel and the foundations of mathematics*, pages 399–432. Cambridge Univ. Press, Cambridge, 2011.

[Gen36] G. Gentzen. Die Widerspruchsfreiheit der reinen Zahlentheorie. *Mathematische Annalen*, 112(1):493–565, 1936.

[Göd63] K. Gödel. *On formally undecidable propositions of Principia Mathematica and related systems.* Translated by B. Meltzer, with an introduction by R. B. Braithwaite. Basic Books, Inc., Publishers, New York, 1963.

[Har85] J. Hartmanis. Independence results about context-free languages and lower bounds. *Information Processing Letters*, 20(5):241–248, 1985.

[Har02] T. Harju. Decision questions on integer matrices. In *Proceedings of the International Conference Developments in language theory (Vienna, 2001)*, volume 2295 of *Lecture Notes in Computer Science*, pages 57–68. Springer, Berlin, 2002.

[HH01] V. Halava and T. Harju. Mortality in matrix semigroups. *American Mathematical Monthly*, 108(7):649–653, 2001.

[HMU01] J. E. Hopcroft, R. Motwani, and J. D. Ullman. *Introduction to automata theory, languages, and computation.* Addison-Wesley Publishing Co., Reading, Mass., 2001. Addison-Wesley Series in Computer Science.

[Hor14] A. Horská. *Where is the Gödel-point hiding: Gentzen's consistency proof of 1936 and his representation of constructive ordinals.* Springer Briefs in Philosophy. Springer, Cham, 2014.

[Iba79] Oscar H. Ibarra. Restricted one-counter machines with undecidable universe problems. *Mathematical Systems Theory*, 13:181–186, 1979.

[Jec02] T. Jech. *Set theory, third edition.* Springer, 2002.

[JY81] D. Joseph and P. Young. Independence results in computer science? *Journal of Computer and System Sciences*, 23(2):205–222, 1981.

[Kan97] A. Kanamori. *The Higher Infinite.* Springer-Verlag, 1997.

[KM87] A. Kanamori and K. McAloon. On Gödel incompleteness and finite combinatorics. *Annals of Pure and Applied Logic*, 33(1):23–41, 1987.

[Kun80] K. Kunen. *Set theory*, volume 102 of *Studies in Logic and the Foundations of Mathematics*. North-Holland Publishing Co., Amsterdam-New York, 1980. An introduction to independence proofs.

[Pet09] J. Petitot. A transcendental view on the continuum: Woodin's conditional platonism. In M. De Glas, editor, *Le continu mathématique. Nouvelles conceptions, nouveaux enjeux, Intellectica*, volume 51, pages 93–133. 2009.

[Poi00] B. Poizat. *A course in model theory*. Universitext. Springer-Verlag, New York, 2000. An introduction to contemporary mathematical logic, Translated from the French by Moses Klein and revised by the author.