View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by UPCommons. Portal del coneixement obert de la UPC

Abstract

The complexity of the parameterized halting problem for nondeterministic Turing machines p-HALT is known to be related to the question of whether there are logics capturing various complexity classes [10]. Among others, if p-HALT is in para-AC^0, the parameterized version of the circuit complexity class AC^0, then AC^0, or equivalently, $(+, \times)$-invariant FO, has a logic. Although it is widely believed that p-HALT $\notin$ para-AC^0, we show that the problem is hard to settle by establishing a connection to the question in classical complexity of whether NE $\not\subseteq$ LINH. Here, LINH denotes the linear time hierarchy.

On the other hand, we suggest an approach toward proving NE $\not\subseteq$ LINH using bounded arithmetic. More specifically, we demonstrate that if the much celebrated MRDP (for Matiyasevich-Robinson-Davis-Putnam) theorem can be proved in a certain fragment of arithmetic, then NE $\not\subseteq$ LINH. Interestingly, central to this result is a para-AC^0 lower bound for the parameterized model-checking problem for FO on arithmetical structures.

A parameterized halting problem, the linear time hierarchy, and the MRDP theorem

Yijia Chen
School of Computer Science
Fudan University
China
yijia.chen@fudan.edu.cn

Moritz Müller
Computer Science Department
Universitat Politècnica de Catalunya
Spain
moritz.mueller@upc.edu

Keita Yokoyama
School of Information Science
Japan Advanced Institute of Science and Technology
Japan
y-keita@jaist.ac.jp

July 6, 2018

1. Introduction

The parameterized complexity of the following halting problem is still wide open.

p-HALT	
Instance:	$n \in \mathbb{N}$ in *unary* and a nondeterministic Turing machine (NTM) $\mathbb{M}$.
Parameter:	$\lvert\mathbb{M}\rvert$, the size of the machine $\mathbb{M}$.
Problem:	Decide whether $\mathbb{M}$ accepts the empty input tape in at most n steps.

The importance of p-HALT is derived from its close connections to some prominent open problems in proof complexity and descriptive complexity [10, 19]. Among others, if p-HALT can be decided by an algorithm $\mathbb{A}$ in time $n^{f(|\mathbb{M}|)}$ for a function $f : \mathbb{N} \to \mathbb{N}$, then there is a logic for PTIME. Although it is generally believed not to be the case, now we can only rule out such an algorithm $\mathbb{A}$ under some very strong *non-standard* complexity-theoretic assumption and with a further restriction that the corresponding function f is *computable* [9, 10]. On the other hand, for every fixed $k \in \mathbb{N}$ there is a linear time algorithm $\mathbb{A}_k$ such that for every NTM $\mathbb{M}$ with $|\mathbb{M}| = k$ the algorithm $\mathbb{A}_k$ decides whether $\mathbb{M}$ halts in at most n steps. More precisely, for every $k \in \mathbb{N}$ we can enumerate all NTM's

$$\mathbb{M}_{k,0}, \dots, \mathbb{M}_{k,\ell_k-1}$$

with $|\mathbb{M}_{k,i}| = k$ for every $i \in [\ell_k]$. Then let

$$s_{k,i} := \begin{cases} s & \mathbb{M}_{k,i} \text{ accepts the empty input tape,} \\ & \text{and a minimum accepting run has } s \text{ steps} \\ \infty & \mathbb{M}_{k,i} \text{ does not accept the empty input tape.} \end{cases}$$

The desired algorithm $\mathbb{A}_k$ accepts an input $(\mathbb{M}, n)$ if $\mathbb{M}$ is $\mathbb{M}_{k,i}$ for some $i \in [\ell_k]$ and $n \geq s_{k,i}$. Equivalently, it computes a simple family of Boolean functions:

$$F_{n,k}(x_0 \dots x_{n-1}, y_0 \dots y_{k-1}) = \bigvee_{\substack{i \in [\ell_k] \text{ such} \\ \text{that } n \geq s_{k,i}}} (x_0 \dots x_{n-1} = 1^n \wedge y_0 \dots y_{k-1} = \mathbb{M}_{k,i}).$$

Observe that $F_{n,k}$ can be understood as a circuit of depth 2 and size $O(k \cdot \ell_k \cdot n)$. Thus, each *slice* of p-HALT is in the circuit complexity class AC^0. Hence, p-HALT is in a *nonuniform* version of *parameterized* AC^0.

Recall that AC^0 is the class of classical problems that can be decided by families of circuits of constant depth and polynomial size. Parameterized AC^0, or para-AC^0, can be viewed as an analog of AC^0 in the parameterized world. There is some recent interest in para-AC^0 [13, 5, 11, 6]. Just like whether p-HALT $\in$ FPT, the question of whether p-HALT $\in$ para-AC^0 can be related to open problems in proof complexity and descriptive complexity as well. Following [10], it is not hard to see that p-HALT $\in$ para-AC^0 implies that there is a logic capturing $(+, \times)$-*invariant* FO. Recall that para-$AC^0 \subseteq$ FPT [13], and there is good evidence that p-HALT $\notin$ FPT [9], so the conjecture below seems highly plausible.

Conjecture 1.1. p-HALT $\notin$ para-AC^0.

Given that AC^0 is well understood, one would expect that Conjecture 1.1 should be within our reach. In fact, [11] establishes (unconditional) para-AC^0 lower bounds for many well-studied parameterized problems. It also shows that p-HALT is not in a natural subclass of para-AC^0. However, we show that settling Conjecture 1.1 either in the positive or the negative leads to the resolution of long standing open problems in complexity theory. On the positive side, we observe that if *nondeterministic exponential time with linear exponent* NE is contained in the *linear time hierarchy* LINH, then p-HALT $\in$ para-AC^0. This connection can be further tightened by considering the following variant of p-HALT.

p-HALT$_=$	
Instance:	$n \in \mathbb{N}$ in unary and an NTM $\mathbb{M}$.
Parameter:	$\lvert\mathbb{M}\rvert$.
Problem:	Decide whether $\mathbb{M}$ has an accepting run on the empty input tape of *exactly* n steps.

Theorem 1.2.

(i) p-HALT$_=$ $\in$ para-AC^0 *if and only if* NE $\subseteq$ LINH.

(ii) p-HALT$_=$ $\in$ para-AC^0 *implies* p-HALT $\in$ para-AC^0.

Thus, to settle Conjecture 1.1 one might try to first separate NE from LINH. Perhaps surprisingly, we tie this question to the provability of the MRDP (for Matiyasevich-Robinson-Davis-Putnam) theorem [12] in bounded arithmetic. The MRDP theorem states that every Σ_1-definable arithmetic relation of natural numbers is *Diophantine*. It has been long realized that proving MRDP in certain fragments of arithmetic has complexity-theoretic consequences. Based on [18], Wilkie [**?**] observed that, assuming NP $\neq$ coNP, MRDP is *not* provable in $I\Delta_0$, the fragment of Peano arithmetic where the induction scheme only applies to Δ_0-formulas.

We show that:

Theorem 1.3. *If* $I\Delta_0$ *proves* MRDP *for small numbers, then* NE $\not\subseteq$ LINH.

Basically, $I\Delta_0$ *proves* MRDP *for small numbers*[1] means that the equivalence of any Δ_0-formula $\varphi(\bar{x})$ to some Diophantine formula is proved in $I\Delta_0$ for all $\bar{x}$ of logarithmic order. Model-theoretically, the equivalence holds in any $I\Delta_0$-model for all $\bar{x}$ from the initial segment of numbers x such that 2^x exists, while proof-theoretically, we allow the $I\Delta_0$-proof to use exponentiation, but only once. Gaifman and Dimitracopoulos [15] showed that $I\Delta_0 + \forall x \exists y \ (2^x = y)$ does prove MRDP. Kaye [17] proved MRDP using only induction for bounded existential formulas plus an axiom stating the totality of a suitable function of exponential growth. It is a standing open question [15] whether $I\Delta_0$ or $I\Delta_0$ plus the totality of some subexponential function can prove MRDP. In fact, if the latter holds, then $I\Delta_0$ proves MRDP for small numbers.

Our proof of Theorem 1.3 relies on an analysis of the parameterized model-checking problem for FO$(+, \times)$, i.e., first-order logic on arithmetical structures:

[1] See Section 5 for the precise definition.

p-MC$\big($FO$(+,\times)\big)$	
Instance:	$n \geq 2$ in *unary* and $\varphi \in$ FO$(+,\times)$.
Parameter:	$\lvert\varphi\rvert$.
Problem:	Decide whether $\big([n],+,\times\big) \models \varphi$.

Theorem 1.4. p-MC$\big($FO$(+,\times)\big) \notin$ para-AC^0.

Could Conjecture 1.1 be false? We establish a connection between p-HALT $\in$ para-AC^0 and the existence of AC^0-bi-immune sets in NP. Let $\mathbf{C}$ be a complexity class. A problem $Q \subseteq \{0,1\}^*$ is **C**-*bi-immune*, if neither Q nor $\{0,1\}^* \setminus Q$ contains an infinite subset that belongs to $\mathbf{C}$. In [9] it is shown that p-HALT $\in$ FPT implies that NP does not have any P-bi-immune set. We prove a similar result with regard to AC^0:

Theorem 1.5. *If* p-HALT $\in$ para-AC^0*, then* NP *contains no* AC^0*-bi-immune set.*

An infinite set $Q \subseteq \{0,1\}^*$ is AC^0*-immune* if every infinite subset of Q is not in AC^0. In particular, every AC^0-bi-immune set is also AC^0-immune. The question of whether NP has an AC^0-immune set is another long standing open question and has been asked once it became known that the separations of standard time and space hierarchy theorems hold with bi-immunity, or, equivalently [4], almost everywhere [16, 1]. While Zimand [23] obtained some partial positive answers, Allender and Gore showed [2] that the answer to this question *relativizes*. That is, with the presence of different oracles, NP might or might not have AC^0-immune sets. Their oracle constructions can be adapted to the case of AC^0-bi-immunity. So Theorem 1.5 gives some evidence that also a negative solution of Conjecture 1.1 could be hard to obtain.

Organization of the paper. We recall some basic notions of complexity and logic in Section 2. The connection between p-HALT and the complexity classes NE and LINH is then discussed in Section 3. After that, Section 4 proves the para-AC^0 lower bound for the problem p-MC$\big($FO$(+,\times)\big)$. Building on this lower bound, in Section 5 we show that proving MRDP in an appropriate fragment of arithmetic separates NE from LINH. Section 6 is devoted to a proof of Theorem 1.5. Finally, we conclude in Section 7.

2. Preliminaries

$\mathbb{N}$ denotes the set of natural numbers, i.e., non-negative integers. For every $n \in \mathbb{N}$ let $[n] := \{0,\dots,n-1\}$. The *length* of $n \in \mathbb{N}$, i.e., the length of the binary expansion n, is $|n| := \lceil \log(n+1) \rceil$.

We assume that the reader is familiar with basic notions in logic and complexity theory, so the following only covers those central to our purposes.

2.1. Complexity. We view *(classical) problems* as subsets of $\{0,1\}^*$, the set of binary strings; the length of a binary string s is denoted $|s|$. For $n \in \mathbb{N}$ we let 1^n denote the binary string consisting of n many 1's. We use multitape Turing machines as our basic model of computation. When considering *dlogtime* Turing machines, i.e. deterministic machines running in time $O(\log n)$, it is understood that they access their input via an address tape (cf. e.g. [7]). As usual, P and NP denote deterministic and nondeterministic polynomial time $n^{O(1)}$, and E and NE denote deterministic and nondeterministic exponential time with linear exponent, i.e., $2^{O(n)}$. The *linear time hierarchy* LINH is the set of problems acceptable by alternating Turing machines in linear time $O(n)$ with $O(1)$ alternations. Clearly,

$$\text{LINH} \subseteq \text{E} \subseteq \text{NE}.$$

Following [7] we define (dlogtime uniform) AC^0 as the set of problems decided by AC^0*-circuit families* $\big(\mathsf{C}_n\big)_{n\in\mathbb{N}}$:

- C_n is a circuit (with $\wedge, \vee, \neg$ gates and unbounded fan-in) with n variables, size $\leq n^c$ and depth $\leq d$, where $c, d \in \mathbb{N}$ are two constants independent of n;
- there is a dlogtime Turing machine which given $\langle 1^n, i, b\rangle$ where $n, i \in \mathbb{N}$ and $b \in \{0,1\}$ decides whether the i-th bit of the binary encoding of C_n is b.

Here, for two binary strings $s = s_0 \cdots s_{|s|-1}$ and $r = r_0 \cdots r_{|r|-1}$ we use a standard pairing function

$$\langle s, r\rangle := s_0 s_0 \cdots s_{|s|-1} s_{|s|-1} 01 r_0 r_0 \cdots r_{|r|-1} r_{|r|-1}, \tag{1}$$

and similarly for more arguments.

For $s \in \{0,1\}^*$ let $num(s)$ be the natural number with binary expansion $1s$. For a problem Q let

$$un(Q) := \left\{ 1^{num(s)} \mid s \in Q \right\}.$$

The last statement of the following is [2, Proposition 5], and the first two are trivial:

Proposition 2.1 ([2])**.** *Let Q be a problem. Then:*

(i) $Q \in$ NE *if and only if* $un(Q) \in$ NP.

(ii) $Q \in$ E *if and only if* $un(Q) \in$ P.

(iii) $Q \in$ LINH *if and only if* $un(Q) \in$ AC^0.

A *parameterized problem* is a pair (Q, κ) of an *underlying* classical problem $Q \subseteq \{0,1\}^*$ and a polynomial time computable *parameterization* $\kappa : \{0,1\}^* \to \mathbb{N}$ mapping an instance $s \in \{0,1\}^*$ to its *parameter* $\kappa(s) \in \mathbb{N}$. As mentioned in the Introduction, the central parameterized complexity class in this paper is para-AC^0. Instead of its original definition using the para-operator of [14], we use the following characterization of para-AC^0.

Proposition 2.2 ([11])**.** *Let (Q, κ) be a parameterized problem such that Q is decidable and κ is computable by an* AC^0*-circuit family. Then the following are equivalent.*

(i) $(Q, \kappa) \in$ para-AC^0.

(ii) There is a family $(\mathsf{C}_{n,k})_{n,k\in\mathbb{N}}$ of circuits such that

- *there is a computable function $f : \mathbb{N} \to \mathbb{N}$ and constants $c, d \in \mathbb{N}$ such that for all $n, k \in \mathbb{N}$ the circuit $\mathsf{C}_{n,k}$ has n variables, size $\leq f(k) \cdot n^c$, and depth $\leq d$;*
- *for all $s \in \{0,1\}^*$ we have*
$$s \in Q \iff \mathsf{C}_{|s|,\kappa(s)}(s) = 1;$$
- *there is a deterministic Turing machine which given as input $\langle 1^n, 1^k, i, b\rangle$ where $n, k, i \in \mathbb{N}$ and $b \in \{0,1\}$ decides in time $g(k) + O(\log n)$ whether the i-th bit of the binary encoding of $\mathsf{C}_{n,k}$ is b, where $g : \mathbb{N} \to \mathbb{N}$ is a computable function.*

(iii) There is a computable $h : \mathbb{N} \to \mathbb{N}$ and an AC^0*-circuit family $(\mathsf{C}_n)_{n\in\mathbb{N}}$ such that for all $s \in \{0,1\}^*$ with $|s| > h(\kappa(s))$: $s \in Q \iff \mathsf{C}_{|s|}(s) = 1$.*

2.2. Logic. A *vocabulary* τ is a finite set of relation symbols and constants. Each relation symbol has an arity. A τ-structure $\mathcal{A}$ consists of a nonempty *universe* A, an r-ary relation $R^{\mathcal{A}} \in A^r$ for each relation symbol $R \in \tau$ of arity r, and an element $c^{\mathcal{A}} \in A$ for each constant $c \in \tau$.

The set of *τ-formulas φ of first-order logic* FO is built up from *atomic τ-formulas* using Boolean connectives $\neg, \vee, \wedge$ and the existential $\exists$ and universal $\forall$ quantifiers. An atomic τ-formula is of the form either $t_0 = t_1$ or $Rt_0 \ldots t_{r-1}$, where $t_0, \ldots, t_{r-1}$ are either variables or constants in τ, and where R is an r-ary relation symbol in τ. When the vocabulary τ is clear from context, we simply call φ a formula. In case it has no free variables, then φ is a *sentence*. On the other hand, writing φ as $\varphi(x_0, \ldots, x_{k-1})$ means that the free variables in φ are among $x_0, \ldots, x_{k-1}$. And $\mathcal{A} \models \varphi(a_0, \ldots, a_{k-1})$ for a τ-structure $\mathcal{A}$ and $a_0, \ldots, a_{k-1} \in A$ means that the assignment of $a_0, \ldots, a_{k-1}$ to $x_0, \ldots, x_{k-1}$ satisfies φ in $\mathcal{A}$. Formally, $\varphi(a_0, \ldots, a_{k-1})$ is a sentence in the language τ plus the a_i's as new constants understood to be interpreted by themselves in $\mathcal{A}$.

An *arithmetical structure* is of the form either $\big(\mathbb{N}, +, \times\big)$ or $\big([n], +, \times\big)$ for some $n \geq 2$.[2] More precisely, they are τ_{arith}-structures $\mathcal{A}$ with $\tau_{\text{arith}} = \{+, \times, 1\}$ where both $+$ and $\times$ are ternary relations, and where 1 is a constant. The universe of $\mathcal{A}$ is either $\mathbb{N}$ or $[n]$ with $n \geq 2$,

$$+^{\mathcal{A}} := \big\{(a, b, c) \in A^3 \;\big|\; a + b = c\big\},$$
$$\times^{\mathcal{A}} := \big\{(a, b, c) \in A^3 \;\big|\; a \times b = c\big\},$$

and $1^{\mathcal{A}} = 1$. A binary string $s = s_0 \dots s_{n-1}$ with $n \geq 2$ can be naturally viewed as the arithmetical structure $\big([n], +, \times\big)$ expanded with a unary relation ONE^s containing those positions $i \in [n]$ with $s_i = 1$. More precisely, we define the *string structure* $\mathcal{S}(s)$ *of* s:

$$\mathcal{S}(s) := \big([n], +, \times, ONE^s\big),$$
$$\text{where } ONE^s = \big\{i \in [n] \;\big|\; s_i = 1\big\}.$$

A τ_{arith}-formula is also called an FO$(+, \times)$*-formula*. To improve readability, atomic FO$(+, \times)$-formulas $+t_1t_2t_3$ and $\times t_1t_2t_3$ are written as $t_3 = t_1 + t_2$ and $t_3 = t_1 \times t_2$. Similarly, FO$(+, \times, ONE)$-*formulas* refer to the FO-formulas of vocabulary $\tau_{\text{arith}} \cup \{ONE\}$. It is well known that definability in FO$(+, \times, ONE)$ coincides with computability by $\big($dlogtime uniform$\big)$ AC^0-circuit families:

Theorem 2.3 ([7])**.** *A problem Q is in* AC^0 *if and only if there is an* FO$(+, \times, ONE)$*-sentence φ such that for every string $s \in \{0, 1\}^*$ with $|s| \geq 2$*

$$s \in Q \quad \Longleftrightarrow \quad \mathcal{S}(s) \models \varphi.$$

2.3. Bounded formulas and the MRDP Theorem. Let $p(\bar{x})$ be a polynomial with natural coefficients. It is straightforward to define a *quantifier-free* formula $\mathit{poly}_p(\bar{x}, y, \bar{z})$ such that for every $\bar{a} \in \mathbb{N}^{|\bar{x}|}$ and $b \in \mathbb{N}$

$$p(\bar{a}) = b \quad \Longleftrightarrow \quad \big(\mathbb{N}, +, \times\big) \models \exists \bar{z}\, \mathit{poly}_p(\bar{a}, b, \bar{z}).$$

For example, for $p(x) = x_1^2 + x_2 + 1$ we let

$$\mathit{poly}_p := (z_1 = x_1 \times x_1) \wedge (z_2 = z_1 + x_2) \wedge (y = z_2 + 1).$$

Then for every formula $\varphi(\bar{x}, y)$ and every polynomial $p(\bar{x})$ with natural coefficients we use $\exists y{<}p\ \varphi$ to denote the self-evident formula

$$\exists y\big(\exists x' \exists \bar{z}\, \mathit{poly}_{p(\bar{x})+x'+1}(\bar{x}, x', y, \bar{z}) \wedge \varphi\big).$$

Here, x' is a new variable distinct from $\bar{x}$, y and $\bar{z}$. Similarly we can define $\forall y{<}p\ \varphi$ as

$$\forall y\big(\exists x' \exists \bar{z}\, \mathit{poly}_{p(\bar{x})+x'+1}(\bar{x}, x', y, \bar{z}) \to \varphi\big).$$

We call $\exists y{<}p$ and $\forall x{<}p$ *bounded quantifiers*.

Definition 2.4. An FO$(+, \times)$-formula φ is in Δ_0 if it can be constructed from atomic FO$(+, \times)$-formulas using the Boolean connectives and the bounded quantifiers.

Theorem 2.5 (Gödel)**.** *Let $f : \mathbb{N} \to \mathbb{N}$ be a computable function. Then there is a Δ_0-formula $\varphi_f(x, y, \bar{z})$ such that for every $a, b \in \mathbb{N}$*

$$f(a) = b \quad \Longleftrightarrow \quad \big(\mathbb{N}, +, \times\big) \models \exists \bar{z}\, \varphi_f(a, b, \bar{z}).$$

We use the following version of the MRDP theorem.

[2] Thus, 1 is always an element in $[n]$.

Theorem 2.6. *For every Δ_0-formula $\varphi(\bar{x})$ there are two polynomials $p(\bar{x},\bar{y})$ and $q(\bar{x},\bar{y})$ with natural coefficients such that*

$$\big(\mathbb{N},+,\times\big) \models \forall\bar{x}\big(\varphi(\bar{x}) \leftrightarrow \exists\bar{y}\; p(\bar{x},\bar{y}) = q(\bar{x},\bar{y})\big),$$

where $p(\bar{x},\bar{y}) = q(\bar{x},\bar{y})$ denotes the formula

$$\exists w\exists\bar{z}\exists\bar{z}'\big(\mathit{poly}_p(\bar{x},\bar{y},w,\bar{z}) \wedge \mathit{poly}_q(\bar{x},\bar{y},w,\bar{z}')\big).$$

Since both poly_p and poly_q are quantifier-free, Theorem 2.6 implies that the formula φ_f in Theorem 2.5 can be further simplified:

Corollary 2.7. *Let $f : \mathbb{N} \to \mathbb{N}$ be a computable function. Then there is a quantifier-free formula $\varphi_f(x,y,\bar{z})$ such that for every $a,b \in \mathbb{N}$*

$$f(a) = b \quad\iff\quad \big(\mathbb{N},+,\times\big) \models \exists\bar{z}\; \varphi_f(a,b,\bar{z}).$$

3. p-HALT, NE, and LINH

Recall that E and NE denote deterministic and nondeterministic exponential time with with linear exponent, i.e., the classes of problems decidable by deterministic/nondeterministic Turing machines in time $2^{O(n)}$. Whether p-HALT and p-HALT$_=$ are fixed-parameter tractable is closely related to the relationship between E and NE.

Theorem 3.1 ([3, 8])**.**

(i) p-HALT$_=$ $\in$ FPT *if and only if* E $=$ NE*.*

(ii) p-HALT$_=$ $\in$ FPT *implies* p-HALT $\in$ FPT*.*

As a matter of fact, the proof of Theorem 3.1 can be adapted to show Theorem 1.2.

Proof of Theorem 1.2: (i) Consider the classical problem:

Q	
Instance:	$n \in \mathbb{N}$ in *binary* and an NTM $\mathbb{M}$.
Problem:	Decide whether $\mathbb{M}$ accepts the empty input tape in exactly n steps.

Clearly, $Q \in$ NE. Thus, assuming NE $\subseteq$ LINH, we conclude that $un(Q) \in$ AC^0 by Proposition 2.1 (iii). Observe that

$$un(Q) = \Big\{1^{num(\langle n,\mathbb{M}\rangle)} \;\Big|\; n \in \mathbb{N} \text{ in binary and the NTM } \mathbb{M} \text{ accepts the empty input tape in exactly } n \text{ steps}\Big\},$$

where

$$\Big|1^{num(\langle n,\mathbb{M}\rangle)}\Big| = \ell, \text{ where } \ell \text{ is the natural number with binary expansion } 1\,\langle n,\mathbb{M}\rangle$$
$$= O\left(2^{|\langle n,\mathbb{M}\rangle|}\right) = O\left(2^{2\cdot|\mathbb{M}|}\cdot n^2\right) \big(\text{by } n \text{ in binary and (1)}\big).$$

Then from the circuits witnessing $un(Q) \in$ AC^0, it is routine to construct a family $\big(\mathsf{C}_{n,k}\big)_{n,k\in\mathbb{N}}$ of circuits such that

– for every $n,k \in \mathbb{N}$, the circuit $\mathsf{C}_{n,k}$ has constant depth and size $2^{O(|\mathbb{M}|)}\cdot n^{O(1)}$;

– for every $n \in \mathbb{N}$ and every NTM $\mathbb{M}$, the machine $\mathbb{M}$ accepts the empty input tape in exactly n steps if and only if $\mathsf{C}_{n,|\mathbb{M}|}(\langle n, \mathbb{M}\rangle) = 1$;

– the circuit $\mathsf{C}_{n,k}$ is easy to construct from n and k.

Thus, Proposition 2.2 implies that p-HALT$_=$ $\in$ para-AC^0, which establishes the direction from right to left in (i).

Conversely, assume that p-HALT$_=$ $\in$ para-AC^0. Let $Q \subseteq \{0,1\}^*$ be a problem in NE. To show that $Q \in$ LINH, it suffices to prove $un(Q) \in$ AC^0 again by Proposition 2.1 (iii). Recall that

$$un(Q) = \left\{ 1^{num(s)} \mid s \in Q \right\}.$$

Also observe that

$$num(s) \neq num(s') \text{ for every } s, s' \in Q \text{ with } s \neq s'. \tag{2}$$

As $Q \in$ NE there is an NTM $\mathbb{M}$ and a constant $c \in \mathbb{N}$ such that $\mathbb{M}$ decides whether $s \in Q$ in time $2^{c \cdot |s|}$ and every run of $\mathbb{M}$ on input s has length at most $2^{c \cdot |s|}$. It is clear that

$$2^{c \cdot |s|} \leq num(s)^c. \tag{3}$$

We define a nondeterministic Turing machine $\mathbb{M}^*$ that started with empty input tape runs as follows:

1. guess a string $t \in \{0,1\}^*$
2. simulate $\mathbb{M}$ on input t for $num(t)^c$ many steps
3. **if** $\mathbb{M}$ rejects, **then** reject
4. make some additional dummy steps such that so far the total running time of $\mathbb{M}^*$ is $2 \cdot num(t)^c - 1$
5. accept.

By (2) and (3) we have for every $s \in \{0,1\}^*$:

$$\begin{aligned} s \in Q \quad \Longleftrightarrow \quad & \mathbb{M}^* \text{ accepts the empty input tape} \\ & \text{in exactly } 2 \cdot num(s)^c \text{ many steps.} \end{aligned} \tag{4}$$

Now, we apply the assumption that p-HALT $\in$ para-AC^0 to obtain a family of circuits

$$\left(\mathsf{C}_{n,|\mathbb{M}^*|}\right)_{n \in \mathbb{N}}$$

with the following properties.

(C1) The circuits $\mathsf{C}_{n,|\mathbb{M}^*|}$ have constant depth and size bounded by $f(|\mathbb{M}^*|) \cdot n^{O(1)}$ for a computable function $f : \mathbb{N} \to \mathbb{N}$. But since $\mathbb{M}^*$ is a fixed machine, we have $\left|\mathsf{C}_{n,|\mathbb{M}^*|}\right| = n^{O(1)}$.

(C2) For every $n \in \mathbb{N}$ the NTM $\mathbb{M}^*$ accepts the empty input tape in exactly n steps if and only if $\mathsf{C}_{n,|\mathbb{M}^*|}(\langle 1^n, \mathbb{M}^*\rangle) = 1$.

(C3) We can construct the circuits $\mathsf{C}_{n,|\mathbb{M}^*|}$ easily from n.

Then we define for every $n \in \mathbb{N}$ a circuit $\mathsf{D}_n(t)$ with $t \in \{0,1\}^n$ as follows. For $s \in \{0,1\}^*$ with $num(s) = n$ we have

$$\mathsf{D}_n\left(1^{num(s)}\right) := \mathsf{C}_{2 \cdot num(s)^c, |\mathbb{M}^*|}\left(\left\langle 1^{2 \cdot num(s)^c}, \mathbb{M}^* \right\rangle\right).$$

Note that $2 \cdot num(s)^c = 2 \cdot n^c$. For $t \neq 1^{num(s)}$ let

$$\mathsf{D}_n(t) := 0.$$

It is routine to see that the circuits

$$\big(\mathsf{D}_n\big)_{n\in\mathbb{N}}$$

can be chosen in AC^0. Moreover, for every $t \in \{0,1\}^n$

$$\begin{aligned}
&\mathsf{D}_n(t) = 1\\
&\quad\iff \text{for some } s \in \{0,1\}^*\colon\ t = 1^{num(s)} \text{ and}\\
&\qquad\quad \mathsf{C}_{2\cdot num(s)^c,|\mathbb{M}^*|}\Big(\Big\langle 1^{2\cdot num(s)^c}, \mathbb{M}^*\Big\rangle\Big) = 1\\
&\quad\overset{\text{by (C2)}}{\iff} \text{for some } s \in \{0,1\}^*\colon\ t = 1^{num(s)} \text{ and } \mathbb{M}^* \text{ accepts the}\\
&\qquad\quad \text{empty input tape in exactly } 2\cdot num(s)^c \text{ steps}\\
&\quad\overset{\text{by (4)}}{\iff} \text{for some } s \in \{0,1\}^*\colon\ t = 1^{num(s)} \text{ and } s \in Q\\
&\quad\iff \text{for some } s \in \{0,1\}^*\colon\ t = 1^{num(s)} \text{ and } 1^{num(s)} \in un(Q)\\
&\quad\iff t \in un(Q).
\end{aligned}$$

In other words, $\big(\mathsf{D}_n\big)_{n\in\mathbb{N}}$ decides $un(Q)$. Hence $un(Q) \in \mathrm{AC}^0$.

(ii) follows easily from the equivalence that for every $n \in \mathbb{N}$ and every NTM $\mathbb{M}$

$$\begin{aligned}
&\mathbb{M} \text{ accepts the empty input tape in at most } n \text{ steps}\\
&\qquad\iff \mathbb{M} \text{ accepts the empty input tape}\\
&\qquad\quad \text{in exactly } n' \text{ steps for some } n' \le n.
\end{aligned}$$

□

Remark 3.2. The reader might notice that in the proof of the direction from left to right in (i) all we need is that for every fixed NTM $\mathbb{M}$ the problem

Instance:	$n \in \mathbb{N}$ in unary.
Problem:	Decide whether $\mathbb{M}$ has an accept run on the empty input tape of exactly n steps.

is in AC^0. Or equivalently, we might say that p-$\textsc{Halt}_=$ is in *nonuniform slicewise* AC^0. Hence, NE $=$ LINH if an only if nonuniform slicewise AC^0 contains p-$\textsc{Halt}_=$. In contrast, as noted in the Introduction, this class trivially contains p-$\textsc{Halt}$.

4. The complexity of p-MC$\big(\mathbf{FO}(+,\times)\big)$

In this section we prove Theorem 1.4. Some further preparations are in order.

Elementary extension. Recall that a structure $\mathcal{M}$ is an *elementary extension* of $\big(\mathbb{N},+,\times\big)$ if $\mathbb{N} \subseteq M$, and if for every FO$(+,\times)$-formulas $\varphi(\bar{x})$ and $\bar{n} \in \mathbb{N}^{|\bar{x}|}$ we have

$$\big(\mathbb{N},+,\times\big) \models \varphi(\bar{n}) \quad\iff\quad \mathcal{M} \models \varphi(\bar{n}). \tag{5}$$

Furthermore, if $\mathbb{N} \subsetneq M$, then $\mathcal{M}$ is a *proper* elementary extension of $\big(\mathbb{N},+,\times\big)$. It is well known that such an $\mathcal{M}$ exists.

Let $\varphi(\bar{x})$ be a formula and u a variable not occurring in $\varphi(\bar{x})$. Then the formula $\varphi^{<u}(\bar{x})$ is obtained from $\varphi(\bar{x})$ by replacing every quantifier $\exists y$ and $\forall y$ by the bounded one $\exists y{<}u$ and $\forall y{<}u$.

Lemma 4.1. *Let $f : \mathbb{N} \to \mathbb{N}$ be a computable function. Then there is a formula $\chi_f(x,y)$ satisfying the following two properties.*

(i) For every $n, b \in \mathbb{N}$

$$f(n) = b \quad \iff \quad \big(\mathbb{N}, +, \times\big) \models \chi_f(n, b).$$

(ii) Let $\mathcal{M}$ be a proper elementary extension $\mathcal{M}$ of $\big(\mathbb{N}, +, \times\big)$ and $a \in M \setminus \mathbb{N}$. Then for every $n \in \mathbb{N}$ and every $b \in M$ with [3] $b < a$

$$f(n) = b \quad \iff \quad \mathcal{M} \models \chi_f^{<a}(n, b).$$

Proof: By Corollary 2.7, there is a quantifier-free formula $\varphi_f(x, y, \bar{z})$ such for every $n, b \in \mathbb{N}$

$$f(n) = b \quad \iff \quad \big(\mathbb{N}, +, \times\big) \models \exists \bar{z}\ \varphi_f(n, b, \bar{z}). \tag{6}$$

We define

$$\chi_f(x, y) := \exists \bar{z}\ \varphi_f(x, y, \bar{z}).$$

And hence (6) proves (i). Note with (5) this also implies that $\mathcal{M} \models \chi_f(n, f(n))$ for every $n \in \mathbb{N}$.

Since φ_f is quantifier-free, the formula $\varphi_f^{<u}(x, y, \bar{z})$ is equivalent to $\varphi_f(x, y, \bar{z}) \wedge u = u$. Therefore[4]

$$\chi_f^{<u}(x, y) \equiv \exists \bar{z}{<}u\ \varphi_f(x, y, \bar{z}).$$

Let $n \in \mathbb{N}$ and $b := f(n) \in \mathbb{N}$. Then (6) implies that $\big(\mathbb{N}, +, \times\big) \models \varphi_f(n, b, \bar{m})$ for some $\bar{m} \in \mathbb{N}^{|\bar{z}|}$. It follows that

$$\mathcal{M} \models \varphi_f(n, b, \bar{m}) \wedge a = a, \text{ i.e., } \mathcal{M} \models \varphi_f^{<a}(n, b, \bar{m}).$$

Thus $\mathcal{M} \models \exists \bar{z}{<}a\ \varphi_f^{<a}(n, b, \bar{z})$.

Conversely, let $n \in \mathbb{N}$ and $b \in M$ with $b < a$ and $\mathcal{M} \models \exists \bar{z}{<}a\ \varphi_f^{<a}(n, b, \bar{z})$. Thus

$$\mathcal{M} \models \exists \bar{z}\ \varphi_f(n, b, \bar{z}), \quad \text{i.e., } \mathcal{M} \models \chi_f(n, b).$$

As we have already seen that $\mathcal{M} \models \chi_f(n, f(n))$, so if $b \neq f(n)$, then $\mathcal{M}$ satisfies

$$\exists y_1 \exists y_2 \big(y_1 \neq y_2 \wedge \chi_f(x, y_1) \wedge \chi_f(x, y_2)\big).$$

By (5), also $\big(\mathbb{N}, +, \times\big)$ satisfies this sentence. But this contradicts (6), as $f(n)$ is unique. □

Let $n \in \mathbb{N}$. It is easy to write a formula $\psi_n(x)$ such that for every elementary extension $\mathcal{M}$ of $\big(\mathbb{N}, +, \times\big)$ and $b \in M$

$$\mathcal{M} \models \psi_n(b) \quad \iff \quad b = n.$$

Then for every formula $\varphi(x, \bar{y})$ we use $\varphi(\underline{n}, \bar{y})$ to denote the formula

$$\exists x \big(\psi_n(x) \wedge \varphi(x, \bar{y})\big).$$

Hence, for every $\bar{b} \in M^{|\bar{y}|}$ we have the equivalence

$$\mathcal{M} \models \varphi(n, \bar{b}) \quad \iff \quad \mathcal{M} \models \varphi(\underline{n}, \bar{b}).$$

Moreover, if $\mathcal{M}$ is a proper elementary extension, $a \in M \setminus \mathbb{N}$, and $\bar{b} < a$,[5] then

$$\mathcal{M} \models \varphi^{<a}(n, \bar{b}) \quad \iff \quad \mathcal{M} \models \varphi^{<a}(\underline{n}, \bar{b}). \tag{7}$$

[3] The natural order $<$ on $\mathbb{N}$ can be FO-defined in $\big(\mathbb{N}, +, \times\big)$ by the formula $\varphi_<(x, y) = \exists z\ x + z + 1 = y$. Thus $\varphi_<$ also defines an order on M, which is an extension of $<$. For simplicity we denote this order again by $<$.

[4] $\exists \bar{z}{<}u$ means $\exists z_0{<}u \ldots \exists z_{k-1}{<}u$, where $\bar{z} = z_0 \ldots z_{k-1}$.

[5] $\bar{b} < a$ is understood as $b_i < a$ for every $i \in [k]$, where $\bar{b} = b_0, \ldots, b_{k-1}$.

Interpretation. Let τ and τ' be two vocabularies with $\tau = \{R_0, \ldots, R_{m-1}, c_1, \ldots, c_{\ell-1}\}$, where each R_i is an r_i-ary relation symbol, and each c_i is a constant. An FO-*interpretation $\mathcal{I}$ of τ in τ' of width w* consists of FO$[\tau']$-formulas

$$\varphi_{\text{uni}}(\bar{x}), \varphi_{R_0}(\bar{x}_0, \ldots, \bar{x}_{r_1-1}),$$
$$\ldots, \varphi_{R_{m-1}}(\bar{x}_0, \ldots, \bar{x}_{r_m-1}), \varphi_{c_0}(\bar{x}), \ldots, \varphi_{c_{\ell-1}}(\bar{x}),$$

where all tuples $\bar{x}, \bar{x}_0, \ldots, \bar{x}_{r_m-1}$ have length w. In a τ'-structure $\mathcal{A}$ the interpretation $\mathcal{I}$ induces the τ-structure $\mathcal{A}^{\mathcal{I}}$ with universe

$$A^{\mathcal{I}} := \{\bar{a} \in A^{\ell} \mid \mathcal{A} \models \varphi_{\text{uni}}(\bar{a})\} \neq \emptyset,$$

with

$$R_i^{\mathcal{A}^{\mathcal{I}}} := \{(\bar{a}_0, \ldots, \bar{a}_{r_i-1}) \in (A^{\mathcal{I}})^{r_i} \mid \mathcal{A} \models \varphi_{R_i}(\bar{a}_0, \ldots, \bar{a}_{r_i-1})\},$$

and with

$$c_i^{\mathcal{A}^{\mathcal{I}}} := \bar{a} \quad \text{where } \bar{a} \text{ is the } \textit{unique} \text{ element in } A^{\mathcal{I}} \text{ with } \mathcal{A} \models \varphi_{c_i}[\bar{a}].$$

In case the set defining $A^{\mathcal{I}}$ is empty, or there are more than one tuple $\bar{a}$ satisfying φ_{c_i}, then the structure $\mathcal{A}^{\mathcal{I}}$ is undefined.

The following is standard.

Lemma 4.2. *Let $\mathcal{I}$ be an interpretation of τ in τ'. Then for every* FO$[\tau]$*-sentence φ there is an* FO$[\tau']$*-sentence $\varphi^{\mathcal{I}}$ such that for all τ'-structures $\mathcal{A}$ such that $\mathcal{A}^{\mathcal{I}}$ is defined we have*

$$\mathcal{A}^{\mathcal{I}} \models \varphi \iff \mathcal{A} \models \varphi^{\mathcal{I}}.$$

Among others, the next lemma implies that for every fixed $d \geq 1$ the string structures $\mathcal{S}(1^{n^d})$ can be interpreted in the string structures $\mathcal{S}(1^n)$. Its proof can be founded in [22, Appendix] and in [7, Lemma 10.5].

Lemma 4.3. *For every $d \in \mathbb{N}$ there is an interpretation $\mathcal{I}_d$ of width d such that for every $n \geq 2$ the structure $([n], +, \times)^{\mathcal{I}_d}$ is defined and isomorphic to $([n^d], +, \times)$.*

Let $n \geq 2$. It is often very useful to consider the *BIT predicate*, a binary relation, on the arithmetical structures $([n], +, \times)$. That is

$$BIT^{[n]} = \{(i, j) \in [n]^2 \mid \text{the } j\text{-th bit of the binary expansion of } i \text{ is } 1\}.$$

We omit the superscript $[n]$ in case it is clear from the context. It turns out that the BIT predicate is definable in FO$(+, \times)$.

Proposition 4.4. [cf. [22, Theorem 3.2]] *There is a formula $\varphi(x, y)$ such that for every $n \geq 2$ and $i, j \in [n]$*

$$([n], +, \times) \models \varphi(i, j) \iff (i, j) \in BIT.$$

Now we are ready to prove Theorem 1.4, which for the reader's convenience is repeated below.

Theorem 4.5. p-MC$(\text{FO}(+, \times)) \notin$ para-AC^0.

Proof: Towards a contradiction, let us assume that p-MC$(\text{FO}(+, \times)) \in$ para-AC^0. By Proposition 2.2 (iii) and Theorem 2.3, there is an increasing computable function $h : \mathbb{N} \to \mathbb{N}$ and an FO-sentence *sat* such that for every $n \in \mathbb{N}$ and $\varphi \in \text{FO}(+, \times)$ with $n \geq h(num(\varphi))$ we have

$$([n], +, \times) \models \varphi \iff \mathcal{S}(\langle 1^n, \varphi \rangle) \models \textit{sat}.$$

Then, using Lemma 4.3 and Proposition 4.4 it is routine to define an FO$(+,\times)$-formula *form-sat*(x) such that

$$\mathcal{S}\big(\langle 1^n,\varphi\rangle\big)\models \textit{sat} \quad\iff\quad \big([n],+,\times\big)\models \textit{form-sat}\big(num(\varphi)\big)$$

for $n\geq h(num(\varphi))\geq num(\varphi)$.

By definition, *form-sat*$^{<u}(x)$ is obtained from *form-sat*(x) by replacing every quantifier occurrence of the form $\forall z$ and $\exists z$ by $\forall z{<}u$ and $\exists z{<}\,u$. Thus

$$\begin{aligned}\big([n],+,\times\big)&\models \textit{form-sat}\big(num(\varphi)\big)\\ &\iff \big(\mathbb{N},+,\times\big)\models \textit{form-sat}^{<n}\big(num(\varphi)\big)\end{aligned}$$

for every FO$(+,\times)$-sentence φ and every $n\geq 1$.

Since $h:\mathbb{N}\to\mathbb{N}$ is computable, Corollary 2.7 implies that there is a formula *h-bound*(x,y) such that

$$n\geq h(num(\varphi)) \quad\iff\quad \big(\mathbb{N},+,\times\big)\models \textit{h-bound}\big(num(\varphi),n\big)$$

for every $n\in\mathbb{N}$ and every FO$(+,\times)$-sentence φ.

Combining all the above together, for every FO$(+,\times)$-sentence φ we obtain a sentence

$$\begin{aligned}\textit{h-sat}_\varphi := \forall u\big(&\textit{h-bound}(\underline{num(\varphi)},u)\\ &\to\big(\varphi^{<u}\leftrightarrow \textit{form-sat}^{<u}(\underline{num(\varphi)})\big)\big).\end{aligned}$$

Thereby, $\big(\mathbb{N},+,\times\big)\models \textit{h-sat}_\varphi$.

Now let $\mathcal{M}$ be a proper elementary extension of $\big(\mathbb{N},+,\times\big)$ and $a\in M\setminus\mathbb{N}$. In particular, $\mathcal{M}\models n<a$ for every $n\in\mathbb{N}$. As a consequence, for every φ

$$\mathcal{M}\models \textit{h-bound}\big(num(\varphi),a\big).$$

By our definition of *h-sat*$_\varphi$, $\big(\mathbb{N},+,\times\big)\models$ *h-sat*$_\varphi$, and by (5)

$$\mathcal{M}\models\Big(\varphi^{<a}\leftrightarrow \textit{form-sat}^{<a}(\underline{num(\varphi)})\Big). \tag{8}$$

As stated in [21, proof of Proposition 3] this contradicts Tarski's undefinability of truth. We include the details as they are omitted in [21].

It is clear that the function which for every FO$(+,\times)$-formula $\varphi(x)$ maps $num(\varphi)$ to

$$num(\varphi(\underline{num(\varphi)}))$$

is computable. So by Lemma 4.1, there is a formula *sub*(x,y) with the following properties.

(S1) Let $\varphi(x)$ be an FO$(+,\times)$-formula and $n\in\mathbb{N}$. Then

$$\begin{aligned}\big(\mathbb{N},+,\times\big)&\models \textit{sub}\big(num(\varphi),n\big)\\ &\iff n=num(\varphi(\underline{num(\varphi)})).\end{aligned}$$

(S2) For every formula $\varphi(x)$ and every $b\in M$ with $b<a$ we have

$$\begin{aligned}\mathcal{M}&\models \textit{sub}^{<a}(num(\varphi),b)\\ &\iff b=num(\varphi(\underline{num(\varphi)})).\end{aligned}$$

Let $\theta:=\chi(\underline{num(\chi)})$, where

$$\chi(x)=\forall y\big(\textit{sub}(x,y)\to\neg\textit{form-sat}(y)\big)$$

and note

$$num(\theta) = num(\chi(\underline{num(\chi)})). \tag{9}$$

Then we can deduce

$$\begin{aligned}
&\mathcal{M} \models \theta^{<a} \\
&\iff \mathcal{M} \models \forall y{<}a\big(\mathit{sub}^{<a}(num(\chi), y) \to \neg \mathit{form\text{-}sat}^{<a}(y)\big) \\
&\qquad\qquad \big(\text{by (7)}\big) \\
&\iff \mathcal{M} \models \big(\mathit{sub}^{<a}(num(\chi), b) \to \neg \mathit{form\text{-}sat}^{<a}(b)\big) \\
&\qquad\qquad \text{for all } b \in M \text{ with } b < a \\
&\iff \mathcal{M} \models \neg \mathit{form\text{-}sat}^{<a}(num(\theta)) \qquad \big(\text{by (S2) and (9)}\big) \\
&\iff \mathcal{M} \models \neg\theta^{<a} \qquad \big(\text{by (8)}\big).
\end{aligned}$$

This is the desired contradiction. □

5. The provability of MRDP and LINH vs. NE

Definition 5.1. A set of FO$(+,\times)$-sentences T is often called a *theory*. A theory T is *true* if

$$\big(\mathbb{N}, +, \times\big) \models \varphi$$

for every $\varphi \in T$. T is Π_1 if every sentence in T is of the form $\forall\bar{x}\psi(\bar{x})$ where ψ is a Δ_0-formula.

Theorem 5.2 (Parikh [20])**.** *Let T be a Π_1-theory and $\varphi(\bar{x},\bar{y})$ a Δ_0-formula with $T \vdash \forall\bar{x}\exists\bar{y}\ \varphi(\bar{x},\bar{y})$. Then there is a polynomial $p(\bar{x})$ with natural coefficients such that*

$$T \vdash \forall\bar{x}\exists\bar{y}{<}p(\bar{x})\ \varphi(\bar{x},\bar{y}).$$

It is well known $\big($see, e.g., [15]$\big)$ that there is a Δ_0-formula $\mathit{exp}(x,y)$ such that for every $n, m \in \mathbb{N}$

$$\big(\mathbb{N}, +, \times\big) \models \mathit{exp}(n,m) \quad \iff \quad 2^n = m.$$

Again for simplicity we identify the formula $\mathit{exp}(x,y)$ with $2^x = y$.

Definition 5.3. Let T be a theory. We say that T *proves* MRDP if for every Δ_0-formula $\varphi(\bar{x})$ there are two polynomials $p(\bar{x},\bar{y})$ and $q(\bar{x},\bar{y})$ with natural coefficients such that

$$T \vdash \forall\bar{x}\big(\varphi(\bar{x}) \leftrightarrow \exists\bar{y}\ p(\bar{x},\bar{y}) = q(\bar{x},\bar{y})\big).$$

As mentioned in the Introduction, Gaifman and Dimitracopoulos showed that $I\Delta_0 + \forall x\exists y\ \mathit{exp}(x,y)$ proves MRDP. Additionally they observed [15, p.204] that the existential quantifier $\exists\bar{y}$ can be bounded by $2^{2^{p(\bar{x})}}$ for some polynomial $p(\bar{x})$ (depending on φ). As noted by Wilkie [**?**] this bound could be improved to $p(\bar{x})$ if MRDP would be provable in $I\Delta_0$ alone $\big($by Parikh's theorem 5.2$\big)$. In this case LINH equals nondeterministic linear time NLIN and thus NE $\not\subseteq$ LINH by the nondeterministic time hierarchy theorem. Theorem 1.3 derives this conclusion from a weaker provability assumption, defined next.

Definition 5.4. Let T be a theory. We say that T *proves* MRDP *for small numbers* if for every $k \in \mathbb{N}$ and every Δ_0-formula $\varphi(\bar{x}) = \varphi(x_0,\dots,x_{k-1})$ there are two polynomials $p(\bar{x},\bar{y})$ and $q(\bar{x},\bar{y})$ with natural coefficients such that

$$\begin{aligned}
T \vdash \forall\bar{x}\Big(\Big(\textstyle\bigwedge_{i\in[k]} \exists y\ 2^{x_i} = y\Big) \\
\to \big(\varphi(\bar{x}) \leftrightarrow \exists\bar{y}\ p(\bar{x},\bar{y}) = q(\bar{x},\bar{y})\big)\Big).
\end{aligned}$$

Intuitively, provability of MRDP for small numbers, say in $I\Delta_0$, seems to be much weaker than provability in $I\Delta_0$. Indeed, $I\Delta_0$ proves MRDP for small numbers if $I\Delta_0+\forall x\exists y\,\big(f(x)=y\big)$ proves MRDP for some subexponential f.[6] It is asked in [15, p.188] whether this holds for $f(x)=x^{\log x}$ or $f(x)=x^{\log\log x}$ etc.

We prove the following slightly more general version of Theorem 1.3.

Theorem 5.5. *Let T be a true Π_1-theory. Moreover, assume that T is recursively enumerable. If T proves* MRDP *for small numbers, then* NE $\not\subseteq$ LINH.

The proof uses the following two lemmas, both easy to show.

Lemma 5.6. *The problem*

Instance:	A polynomial $p(x)$ and $n\in\mathbb{N}$.
Problem:	Output $p(n)$.

can be computed in time

$$\big(|p|+\log n\big)^{O(1)},$$

where we encode p by a list of its natural coefficients, and $|p|$ is the length of this encoding. (As consequences, the degree of p is bounded by $O(|p|)$, and any coefficient in p is bounded by $O(2^{|p|})$).

Lemma 5.7. *The following functions are all computable by* AC^0*-circuit families.*

(i) $(x,y)\mapsto\langle x,y\rangle$, $\langle x,y\rangle\mapsto x$, $\langle x,y\rangle\mapsto y$, *where* $x,y\in\{0,1\}^*$.

(ii) $x\mapsto num(x)$ *for* $x\in\{0,1\}^*$.

(iii) $1^n\mapsto n$ *for* $n\in\mathbb{N}$, *that is, mapping every unary n to its binary expansion.*

(iv) The mapping $(n,x)\mapsto 1^n$, *where* $n\in\mathbb{N}$ *and* $x\in\{0,1\}^*$ *with* $n\le|x|^{O(1)}$.

Proof of Theorem 5.5: Assume that both T proves MRDP for small numbers and NE $\subseteq$ LINH. Our goal is to derive a contradiction to Theorem 1.4. To that end, let $n\ge 2$ and φ be an FO$(+,\times)$-sentence, i.e., $\big(1^n,\varphi\big)$ is an instance of the problem p-MC$\big(\mathrm{FO}(+,\times)\big)$. Then for the Δ_0-formula $\varphi^{<x}$, we have

$$\big([n],+,\times\big)\models\varphi\quad\iff\quad\big(\mathbb{N},+,\times\big)\models\varphi^{<n}. \tag{10}$$

Claim 1. There are polynomials $p_\varphi(x,\bar y)$, $q_\varphi(x,\bar y)$, and $u_\varphi(x,z)$ such that

$$T\vdash\forall x\forall z\Big(2^x=z\to \big(\varphi^{<x}\leftrightarrow\exists\bar y{<}u_\varphi(x,z)\;p_\varphi(x,\bar y)=q_\varphi(x,\bar y)\big)\Big).$$

Moreover, $p_\varphi(x,\bar y)$, $q_\varphi(x,\bar y)$, and $u_\varphi(x,z)$ can be computed from φ.

Proof of the claim: Since T proves MRDP for small numbers and $\varphi^{<x}\in\Delta_0$, there are polynomials $p_\varphi(x,\bar y)$ and $q_\varphi(x,\bar y)$ such that

$$T\vdash\forall x\forall z\Big(2^x=z\to \big(\varphi^{<x}\leftrightarrow\exists\bar y\;p_\varphi(x,\bar y)=q_\varphi(x,\bar y)\big)\Big). \tag{11}$$

[6] i.e., for any $n\in\mathbb{N}$, there exists an $m\in\mathbb{N}$ such that $I\Delta_0$ proves that $\forall x{\ge}m\;\; f^n(x)\le 2^x$. Here, $f^n(x)$ denotes the value $\underbrace{f(f(\cdots f}_{n\text{ times}}(x)\cdots))$.

This shows that for *any* polynomial $u(x,z)$ with natural coefficients we have

$$T \vdash \forall x \forall z \Big(2^x = z \\ \to \big(\exists \bar{y} {<} u(x,z)\ p_\varphi(x,\bar{y}) = q_\varphi(x,\bar{y}) \to \varphi^{<x} \big) \Big). \tag{12}$$

Next, observe that the sentence

$$\forall x \forall z \Big(2^x = z \to \big(\varphi^{<x} \to \exists \bar{y}\ p_\varphi(x,\bar{y}) = q_\varphi(x,\bar{y}) \big) \Big)$$

is equivalent to

$$\forall x \forall z \exists \bar{y} \underbrace{\Big(\neg 2^x = z \vee \neg \varphi^{<x} \vee p_\varphi(x,\bar{y}) = q_\varphi(x,\bar{y}) \Big)}_{\text{a } \Delta_0\text{-formula}}.$$

Thus by Theorem 5.2 and (11) there is a polynomial $u_\varphi(u,z)$ with natural coefficients such that

$$T \vdash \forall x \forall z \exists \bar{y} {<} u_\varphi(x,z) \\ \Big(\neg 2^x = z \vee \neg \varphi^{<x} \vee p_\varphi(x,\bar{y}) = q_\varphi(x,\bar{y}) \Big),$$

i.e.,

$$T \vdash \forall x \forall z \Big(2^x = z \to \\ \big(\varphi^{<x} \to \exists \bar{y} {<} u_\varphi(x,z)\ p_\varphi(x,\bar{y}) = q_\varphi(x,\bar{y}) \big) \Big).$$

Together with (12)

$$T \vdash \forall x \forall z \Big(2^x = z \to \\ \big(\varphi^{<x} \leftrightarrow \exists \bar{y} {<} u_\varphi(x,z)\ p_\varphi(x,\bar{y}) = q_\varphi(x,\bar{y}) \big) \Big).$$

Since T is recursively enumerable, we conclude that p_φ, q_φ, and u_φ all can be computed from φ by the Completeness Theorem. ⊣

Claim 2. There is a computable function $f : \mathbb{N} \to \mathbb{N}$ and an NTM $\mathbb{M}$ such that for every $n \geq 2$ and FO$(+,\times)$-formula φ the machine $\mathbb{M}$ decides whether $\big([n],+,\times\big) \models \varphi$ in time

$$f(|\varphi|) \cdot n^{O(1)}.$$

Proof of the claim: By Claim 1 we can compute from φ three polynomials p_φ, q_φ, and u_φ such that $\big(\mathbb{N},+,\times\big)$ satisfies

$$\forall x \forall z \Big(2^x = z \to \big(\varphi^{<x} \leftrightarrow \exists \bar{y} {<} u_\varphi(x,z) \\ p_\varphi(x,\bar{y}) = q_\varphi(x,\bar{y}) \big) \Big). \tag{13}$$

Let

$$s := u_\varphi\big(n, 2^n\big).$$

Then by (10) and (13) we conclude that $\big([n],+,\times\big) \models \varphi$ if and only if there is some $\bar{m} \in [s]^{|\bar{y}|}$ such that

$$p_\varphi(n,\bar{m}) = q_\varphi(n,\bar{m}).$$

By first guessing $\bar{m}$, Lemma 5.6 implies that all these can be tested in nondeterministic time

$$\big(|u_\varphi| + |p_\varphi| + |q_\varphi| + n \big)^{O(1)}.$$

This proves the claim. ⊣

Without loss of generality, we choose the function $f : \mathbb{N} \to \mathbb{N}$ in Claim 2 to be time constructible and $f(n) \geq 2^n$ for every $n \in \mathbb{N}$. It follows that the following classical problem Q is in NE.

Q	
Instance:	$n \geq 2$ in *binary* and $\varphi \in \mathrm{FO}(+,\times)$ with $n \geq f(\lvert\varphi\rvert)$.
Problem:	Decide whether $\big([n],+,\times\big) \models \varphi$.

Since NE $=$ LINH by assumption, $Q \in$ LINH, and thus

$$un(Q) = \Big\{ 1^{num(\langle n,\varphi\rangle)} \;\Big|\; n \geq f(|\varphi|) \text{ and } \big([n],+,\times\big) \models \varphi \Big\}$$

is in AC^0 by Proposition 2.1 (iii).

Observe that Lemma 5.7 implies that the mapping

$$\langle 1^n, x\rangle \mapsto 1^{num(\langle n,x\rangle)},$$

where $n \in \mathbb{N}$ and $x \in \{0,1\}^*$ with $n \geq 2^{|x|}$, is computable in AC^0. Thus,

$$\Big\{ \langle 1^n, \varphi\rangle \;\Big|\; n \geq f(|\varphi|) \text{ and } \big([n],+,\times\big) \models \varphi \Big\}$$

is in AC^0, too. Then Proposition 2.2 (iii) implies that

$$p\text{-MC}\big(\mathrm{FO}(+,\times)\big) \in \text{para-AC}^0,$$

which contradicts Theorem 1.4. □

6. p-HALT and a universal AC^0-easy set in NP

Recall that we can identify every natural number $n \in \mathbb{N}$ with the string of its binary expansion. And in case $n \geq 2$, it can be further identified with the string structure $\mathcal{S}(n)$. The next lemma is an easy consequence of the definability of the BIT predicate in FO$(+,\times)$, i.e., Proposition 4.4.

Lemma 6.1. *Let $U \subseteq \mathbb{N}$. If $\big\{\mathcal{S}(n) \;\big|\; n \in U \text{ and } n \geq 2\big\}$ is definable in* FO$(+,\times, ONE)$*, then the class*

$$\big\{\mathcal{S}(1^n) \;\big|\; n \in U \text{ and } n \geq 2\big\}$$

is also definable in FO$(+,\times, ONE)$.

Lemma 6.2. *Let $f : \mathbb{N} \to \mathbb{N}$ be a computable function. Then there is an increasing function $h : \mathbb{N} \to \mathbb{N}$ that satisfies the following properties.*

(i) $h(n) \geq f(n^2)$ *for every* $n \in \mathbb{N}$.

(ii) The mapping $1^n \mapsto 1^{h(n)}$ *can be computed in time* $h(n)^{O(1)}$.

(iii) The class of string structures

$$\Big\{\mathcal{S}\big(1^{h(n)}\big) \;\Big|\; n \geq 2\Big\}$$

is definable in FO$(+,\times, ONE)$.

(iv) There is an FO$(+,\times, ONE)$*-formula $\varphi(x)$ such that for every $n \geq 2$ and $a \in [h(n)]$*

$$\mathcal{S}\big(1^{h(n)}\big) \models \varphi(a) \quad\Longleftrightarrow\quad a = n.$$

Proof: Given a deterministic Turing machine $\mathbb{M}$ and an input $s \in \{0,1\}^*$ we let $w_{\mathbb{M},s}$ be a binary string encoding the computation of $\mathbb{M}$ on s. It is well known that the encoding can be chosen in such a way that:

(E1) The function $s \mapsto w_{\mathbb{M},s}$ is computable in time $|w_{\mathbb{M},x}|^{O(1)}$.

(E2) The problem $\{ \langle s, w_{\mathbb{M},s} \rangle \mid s \in \{0,1\}^* \}$ is in AC^0.

From (E2) it is straightforward to define an FO$(+, \times, ONE)$-sentence $comp_{\mathbb{M}}$ by Theorem 2.3 such that for every $s, w \in \{0,1\}^*$

$$\mathcal{S}(num(\langle s, w \rangle)) \models comp_{\mathbb{M}} \iff w = w_{\mathbb{M},s} \tag{14}$$

Now let $\mathbb{M}_f$ be a Turing machine that computes the mapping $1^n \mapsto 1^{f(n)}$. We consider the following simple machine.

$\mathbb{M}(1^n)$ // $n \in \mathbb{N}$

1. **for all** $0 \le i \le n$ **do**
2. run the machine $\mathbb{M}_f$ on input 1^{i^2}.

Then we define the *increasing* function $h : \mathbb{N} \to \mathbb{N}$ by

$$h(n) = num\big(\langle 1^n, w_{\mathbb{M},1^n} \rangle \big) \tag{15}$$

It should be clear that the string $w_{\mathbb{M}_f,1^{n^2}}$ encoding the computation of $\mathbb{M}_f$ on input 1^{n^2} has length at least $f(n^2)$. Similarly, $|w_{\mathbb{M},1^n}| \ge f(n^2)$. Thus $h(n) \ge f(n^2)$ for every $n \in \mathbb{N}$, i.e., (i) holds.

(ii) is also immediate by (E1). By (14) and our definition (15) of h the class

$$\big\{ \mathcal{S}(h(n)) \mid n \ge 2 \big\}$$

is definable in FO$(+, \times, ONE)$. Thus (iii) follows from Lemma 6.1.

Finally, on the structure $\mathcal{S}\big(1^{h(n)}\big)$ we can first define the string of the binary expansion of $h(n)$ using the BIT predicate by Proposition 4.4. Then by (15) we can obtain the string 1^n, from which n can be defined using the BIT predicate again. □

Theorem 6.3. *Assume* p-HALT $\in$ para-AC^0. *Then there is an infinite set* $I \subseteq \{0,1\}^*$ *such that for every* NP*-problem* $Q \subseteq \{0,1\}^*$ *we have* $Q \cap I \in \mathrm{AC}^0$.

Proof: Let us assume that p-HALT $\in$ para-AC^0. By Proposition 2.2 and Theorem 2.3 there is a computable and increasing function $f : \mathbb{N} \to \mathbb{N}$ and an FO$(+, \times, ONE)$-sentence φ such that for every $\langle 1^n, \mathbb{M} \rangle$ with $n \ge f(|\mathbb{M}|)$

$$\begin{aligned} &\mathcal{S}\big(\langle 1^n, \mathbb{M} \rangle \big) \models \varphi \\ &\quad \iff \mathbb{M} \text{ accepts the empty input tape in at most } n \text{ steps.} \end{aligned} \tag{16}$$

Now let $h : \mathbb{N} \to \mathbb{N}$ be the increasing function as stated in Lemma 6.2. In particular, there is a deterministic Turing machine $\mathbb{M}_h$ and a constant $c \ge 1$ such that on input 1^m the machine $\mathbb{M}_h$ outputs the string $1^{h(m)}$ in time $h(m)^c$. The desired set I is defined by

$$I := \Big\{ 1^{h(m)} \mid m \ge 2 \Big\}.$$

By Lemma 6.2 (iii), there is an FO$(+, \times, ONE)$-sentence φ_I such that for every string $s \in \{0,1\}^*$ with $|s| \ge 2$

$$\mathcal{S}(s) \in I \iff \mathcal{S}(s) \models \varphi_I. \tag{17}$$

Now let $Q \subseteq \{0,1\}^*$ be a problem in NP. In particular, there is an NTM $\mathbb{M}_Q$ and a constant $d \ge 1$ such that on input $s \in \{0,1\}^*$ the machine $\mathbb{M}_Q$ decides whether $s \in Q$ in time $|s|^d$. Then for every $m \ge 2$ we define the following nondeterministic Turing machine:

$\mathbb{M}_{Q,h,m}$

1. run the machine $\mathbb{M}_h$ on 1^m to output $1^{h(m)}$
2. run the machine $\mathbb{M}_Q$ on $1^{h(m)}$ to decide whether $1^{h(m)} \in Q$, then accept and reject accordingly.

Let

$$n := h(m)^c + h(m)^d.$$

The following equivalences are immediate.

$$\begin{aligned} 1^{h(m)} \in Q &\iff \mathbb{M}_{Q,h,m} \text{ accepts the empty input tape} \\ &\iff \mathbb{M}_{Q,h,m} \text{ accepts the empty input tape} \\ &\qquad\qquad \text{in at most } n \text{ steps.} \end{aligned} \tag{18}$$

Also observe that the size of $\mathbb{M}_{Q,h,m}$ is

$$\big|\mathbb{M}_{Q,h,m}\big| = |\mathbb{M}_h| + |\mathbb{M}_Q| + m + e.$$

for some constant $e \in \mathbb{N}$. Hence, if $m \geq |\mathbb{M}_h| + |\mathbb{M}_Q| + e \geq 2$, we have

$$\begin{aligned} n = h(m)^c + h(m)^d &\geq h(m) \geq f(m^2) \\ &\geq f(|\mathbb{M}_h| + |\mathbb{M}_Q| + m + e) = f(|\mathbb{M}_{Q,h,m}|). \end{aligned}$$

Then (16) and (18) imply that

$$1^{h(m)} \in Q \iff \mathcal{S}\big(\langle 1^n, \mathbb{M}_{Q,h,m}\rangle\big) \models \varphi. \tag{19}$$

On the other hand, using Lemma 6.2 (iv) it is easy to construct an interpretation $\mathcal{I}$ such that for every $m \in \mathbb{N}$

$$\mathcal{I}\Big(\mathcal{S}\big(1^{h(m)}\big)\Big) = \mathcal{S}\big(\langle 1^n, \mathbb{M}_{Q,h,m}\rangle\big).$$

Thus by Lemma 4.2

$$\mathcal{S}\big(\langle 1^n, \mathbb{M}_{Q,h,m}\rangle\big) \models \varphi \iff \mathcal{S}\big(1^{h(m)}\big) \models \varphi^{\mathcal{I}}.$$

Combined with (17) and (19), for every string $s \in \{0,1\}^*$ with $|s| \geq h(|\mathbb{M}_h| + |\mathbb{M}_Q| + e)$

$$\begin{aligned} &\mathcal{S}(s) \models \varphi_I \wedge \varphi^{\mathcal{I}} \\ &\quad\iff s = 1^{h(m)} \text{ for some } m \geq |\mathbb{M}_h| + |\mathbb{M}_Q| + e \text{ and } s \in Q, \\ &\qquad\qquad\qquad\qquad \text{i.e., } s \in Q \cap I. \end{aligned}$$

Since there are only finitely many strings in $Q \cap I$ with length smaller than $h(|\mathbb{M}_h| + |\mathbb{M}_Q| + e)$, the class

$$\big\{\mathcal{S}(s) \;\big|\; s \in Q \cap I\big\}$$

is definable in FO$(+, \times, \mathit{ONE})$. So Theorem 2.3 implies that $Q \cap I$ is in AC^0. □

Proof of Theorem 1.5: Assume that p-HALT $\in$ para-AC^0 and an NP-problem $Q \subseteq \{0,1\}^*$ is an AC^0-bi-immune set. Let I be the infinite set as stated in Theorem 6.3. Then either $Q \cap I$ or $(\{0,1\}^* \setminus Q) \cap I$ is infinite. And by Theorem 6.3 they are both in AC^0, which contradicts the AC^0-bi-immunity of Q. □

.

7. Conclusions

Our initial goal was to prove unconditionally that p-HALT $\notin$ para-AC^0, but without success after several years' attempt. The results of the current paper show why. On the positive side, p-HALT $\notin$ para-AC^0 would lead to the separation of NE from LINH, a long standing open problem in complexity theory. On the negative side, p-HALT $\in$ para-AC^0 implies that NP has no AC^0-bi-immune set, which is also an open question.

Since it is generally believed that p-HALT $\notin$ para-AC^0, one could try to settle the conjecture NE $\not\subseteq$ LINH first. Here, we provide an approach using bounded arithmetic. In particular, we showed that if a true Π_1 theory of arithmetic can prove the MRDP theorem for small numbers, then LINH $\neq$ NE. At the core of our proof, it is a para-AC^0 lower bound for the parameterized problem p-MC$\big(\text{FO}(+,\times)\big)$, which might be of some independent interest.

Acknowledgements. Moritz Müller has been supported by the Austrian Science Fund (FWF) under Project P28699, and is supported by the European Research Council (ERC) under the European Unions Horizon 2020 research programme (grant agreement ERC-2014-CoG 648276 AUTAR). Keita Yokoyama is partially supported by JSPS KAKENHI (grant numbers 16K17640 and 15H03634). The collaboration of Yijia Chen and Keita Yokoyama has been supported by NSFC-JSPS Bilateral Joint Research Project (Grant No. 61511140100).

References

[1] E. Allender, R. Beigel, U. Hertrampf, and S. Homer. Almost-everywhere complexity hierarchies for nondeterministic time. *Theoretical Compututer Science*, 115(2):225–241, 1993.

[2] E. Allender and V. Gore. On strong separations from AC^0. In Jin-Yi Cai, editor, *Advances In Computational Complexity Theory*, volume 13 of *DIMACS Series in Discrete Mathematics and Theoretical Computer Science*, pages 21–38, 1990.

[3] Y. Aumann and Y. Dombb. Fixed structure complexity. In *Parameterized and Exact Computation, Third International Workshop, IWPEC 2008, Victoria, Canada, May 14-16, 2008. Proceedings*, pages 30–42, 2008.

[4] J. L. Balcázar and U. Schöning. Bi-immune sets for complexity classes. *Mathematical Systems Theory*, 18(1):1–10, 1985.

[5] M. Bannach, C. Stockhusen, and T. Tantau. Fast parallel fixed-parameter algorithms via color coding. In *10th International Symposium on Parameterized and Exact Computation (IPEC 2015)*, pages 224–235, 2015.

[6] M. Bannach and T. Tantau. Parallel multivariate meta-theorems. In *11th International Symposium on Parameterized and Exact Computation (IPEC 2016)*, pages 4:1–4:17, 2016.

[7] D. A. M. Barrington, N. Immerman, and H. Straubing. On uniformity within NC1. *Journal of Computer and System Sciences*, 41(3):274–306, 1990.

[8] Y. Chen and J. Flum. A logic for PTIME and a parameterized halting problem. In *Proceedings of the 24th Annual IEEE Symposium on Logic in Computer Science, LICS 2009, 11-14 August 2009, Los Angeles, CA, USA*, pages 397–406, 2009.

[9] Y. Chen and J. Flum. On the complexity of Gödel's proof predicate. *The Journal of Symbolic Logic*, 75(1):239–254, 2010.

[10] Y. Chen and J. Flum. From almost optimal algorithms to logics for complexity classes via listings and a halting problem. *Journal of the ACM*, 59(4):17:1–17:34, 2012.

[11] Y. Chen and J. Flum. Some lower bounds in parameterized AC^0. In *Proceedings of the 41st International Symposium on Mathematical Foundations of Computer Science (MFCS'16)*, pages 27:1–27:14, 2016.

[12] M. Davis. Hilbert's tenth problem is unsolvable. *The American Mathematical Monthly*, 80(3):233–269, 1973.

[13] M. Elberfeld, C. Stockhusen, and T. Tantau. On the space and circuit complexity of parameterized problems: Classes and completeness. *Algorithmica*, 71(3):661–701, 2015.

[14] J. Flum and M. Grohe. Describing parameterized complexity classes. *Information and Computation*, 187(2):291–319, 2003.

[15] H. Gaifman and C. Dimitracopoulos. Fragments of arithmetic and the MRDP theorem. In *Logic and algorithmic*, volume 30 of *Monographie de L'Enseignement Mathematique*, pages 187–206, 1982.

[16] J. G. Geske, D. T. Huynh, and J. I. Seiferas. A note on almost-everywhere-complex sets and separating deterministic-time-complexity classes. *Information and Computation*, 92(1):97–104, 1991.

[17] R. Kaye. Diophantine induction. *Annals of Pure and Applied Logic*, 46:1–40, 1990.

[18] K. L. Manders and L. Adleman. NP-complete decision problems for binary quadratics. *Journal of Computer and System Sciences*, 16:168–184, 1978.

[19] A. Nash, J. B. Remmel, and V. Vianu. PTIME queries revisited. In *Proceedings of the 10th International Conference of Database Theory (ICDT'05)*, pages 274–288, 2005.

[20] R. Parikh. Existence and feasibility in arithmetic. *The Journal of Symbolic Logic*, 36:494–508, 1971.

[21] J. B. Paris and C. Dimitracopoulos. Truth definitions for Δ_0 formulae. In *Logic and algorithmic*, volume 30 of *Monographie de L'Enseignement Mathematique*, pages 317–329, 1982.

[22] N. Schweikardt. Arithmetic, first-order logic, and counting quantifiers. *ACM Transactions on Computational Logic*, 6(3):634–671, 2005.

[23] M. Zimand. Large sets in AC^0 have many strings with low Kolmogorov complexity. *Information Processing Letters*, 62(3):165–170, 1997.