Computational complexity of logical theories of one successor and another unary function

Pascal MICHEL*
Équipe de logique de l'université Paris 7
and IUFM de l'académie de Versailles
michel@logique.jussieu.fr

January 23, 2007

Abstract

The first-order logical theory $\mathrm{Th}(\mathbb{N}, x+1, F(x))$ is proved to be complete for the class ATIME-ALT$(2^{O(n)}, O(n))$ when $F(x) = 2^x$, and the same result holds for $F(x) = c^x$, x^c ($c \in \mathbb{N}$, $c \geq 2$), and $F(x) =$ tower of x powers of two. The difficult part is the upper bound, which is obtained by using a bounded Ehrenfeucht-Fraïssé game.

Keywords: Computational complexity, logical theories, Ehrenfeucht-Fraïssé games.

1 Introduction

The structures we consider in this article have the set of natural numbers as universe, equality as unique basic relation, and some usual unary functions as basic operations. So they cannot be said to be contrived examples of structures. However, few results are known about decidability and complexity of the first-order theory of such structures.

On the one hand, Ferrante and Rackoff (1979) [6] proved that $\mathrm{Th}(\mathbb{N}, =, x+1)$ is PSPACE-complete, and the same result was proved for $\mathrm{Th}(\mathbb{N}, =, 2x)$, $\mathrm{Th}(\mathbb{N}, =, x^2)$, $\mathrm{Th}(\mathbb{N}, =, 2^x)$ by Michel (1992) [13].

*Corresponding address: 59 rue du Cardinal Lemoine, 75005 Paris, France.

On the other hand, it is easy to find unary functions f_1, f_2, f_3, f_4, definable in $\langle \mathbb{N}, =, +, \times \rangle$, such that $+$ and $\times$ are definable in $\langle \mathbb{N}, =, f_1, f_2, f_3, f_4 \rangle$, and so $\mathrm{Th}(\mathbb{N}, =, f_1, f_2, f_3, f_4)$ is undecidable. Indeed, if $g : \mathbb{N}^2 \to \mathbb{N}$ is a definable bijection, we take f_1, f_2 such that $g(f_1(x), f_2(x)) = x$, $f_1(g(x, y)) = x$, $f_2(g(x, y)) = y$, and $f_3 = f_1 + f_2$, $f_4 = f_1 f_2$. Then $+$ and $\times$ can be defined in $\langle \mathbb{N}, =, f_1, f_2, f_3, f_4 \rangle$ as follows.

$$x + y = z \iff \exists t[(f_1(t) = x) \wedge (f_2(t) = y) \wedge (f_3(t) = z)],$$

$$xy = z \iff \exists t[(f_1(t) = x) \wedge (f_2(t) = y) \wedge (f_4(t) = z)].$$

Moreover, Korec (2001) [10] claimed that function f_4 is redundant if $g(x, y) = (x+y)(x+y+1)/2+x$ (his example 6.7), and gave also structures with only two unary functions in which $+$ and $\times$ can be defined (ex. 4(b)16, 5.13).

Between these extreme cases, some results are known about theories of structures $\langle \mathbb{N}, =, x + 1, F(x) \rangle$. Semenov (1984) [14] proved that $\mathrm{Th}(\mathbb{N}, =, +, 2^x)$ is decidable (and Compton and Henson (1990) [3] proved that it is not elementary recursive), so $\mathrm{Th}(\mathbb{N}, =, x + 1, 2^x)$ is decidable. Semenov (1984) [14] proved also that $\mathrm{Th}(\mathbb{N}, \leq, x^2)$ is decidable, so $\mathrm{Th}(\mathbb{N}, =, x + 1, x^2)$ is decidable. In this paper, we prove that $\mathrm{Th}(\mathbb{N}, =, x + 1, F(x))$ is complete for ATIME-ALT$(2^{O(n)}, O(n))$ if $F(x) = 2^x$, and that this result can be easily extended to $F(x) = c^x$, x^c $(c \geq 2)$ and $F(x) = \exp_\infty(x)$ (i.e., $F(x)$ a tower of powers of two).

As a related result, note that Thomas (1975) [16], improving Elgot and Rabin (1966) [5], proved that the weak monadic second-order theory of $\langle \mathbb{N}, =, x + 1, F(x) \rangle$ is undecidable if $\{a : F^{-1}(a) \text{ infinite}\}$ is infinite, or if F is strictly monotone and $\{a : F(a) + 1 < F(a + 1)\}$ is infinite. So we know that the weak monadic second-order theory of $\langle \mathbb{N}, =, x + 1, 2^x \rangle$ is undecidable. Michel (1992) [13] considered structures without equality, but with the binary relation $\perp$ of coprimality, and proved that $\mathrm{Th}(\mathbb{N}, \perp, \times, 2x, x^2, 2^x)$ is in ATIME-ALT$(2^{O(n)}, O(n))$.

The paper is structured as follows. The main task is proving that $\mathrm{Th}(\mathbb{N}, =, x + 1, 2^x)$ is in the complexity class ATIME-ALT$(2^{O(n)}, n)$. The structure $\langle \mathbb{N}, =, x+1, 2^x \rangle$ is presented in Section 2 and the idea of the proof is given in Section 3. Sections 4 to 8 are devoted to the proof, which needs many technical lemmas. Then we show in Section 9 how the proof can be extended to theories $\mathrm{Th}(\mathbb{N}, =, x + 1, F(x))$ when $F(x) = c^x$, x^c or $\exp_\infty(x)$. These extensions of the proof are straightforward, and we have preferred focusing on one structure in the main body of the article, rather than adding more discussions

and computations to an already lengthy proof. The lower bound is proved in Section 10, and we conclude by giving prospects and open problems.

2 Preliminaries

2.1 Computational complexity

We use the complexity measure ATIME-ALT($\cdot$, $\cdot$), due to Berman (1980) [2]. This measure, based on alternating Turing machines, is particularly well suited to the study of logical theories. We give here only a brief description, and refer to books such as Balcázar et al. (1990) [1] for precise definitions.

As for nondeterministic Turing machines, the configurations of an alternating Turing machine are nodes of a computation tree, but the non-halting nodes are now labelled as existential or universal. A computation of an alternating Turing machine on an input x is accepting if there exists a finite subtree of the computation tree, with one child out of each existential node, all the children out of each universal node, and accepting halting leaves. An alternating Turing machine M works in $T(n)$ time and $A(n)$ alternations if, for all accepted input x of length n, there is an accepting computation subtree of M on x of height $T(n)$, such that there is at most $A(n)-1$ alternations of existential and universal configurations from the root to an accepting leaf. A language L is in ATIME-ALT($T(n), A(n)$) if there exists an alternating Turing machine accepting words in L in time $T(n)$ and number of alternations $A(n)$. We set ATIME-ALT($2^{O(n)}, n$) $= \bigcup_{c>0}$ ATIME-ALT($2^{cn}, n$).

2.2 Logic

We refer to Ferrante and Rackoff (1979) [6] for precise logical definitions.

A *vocabulary* is a set $V = \{f_1, \ldots, f_l, R_1, \ldots, R_m\}$ of symbols for functions f_i and relations R_j. We will use mainly the vocabularies $\{=, f_1, f_2\}$ and $\{=, R_1, R_2\}$, where f_1, f_2 are symbols for unary functions and R_1, R_2 are symbols for binary relations.

A *formula* over vocabulary V involves logical symbols $\neg$, $\vee$, $\wedge$, $\exists$, $\forall$, parentheses, formal variables $v_0, v_1, \ldots$ with subscripts written in binary, and symbols from vocabulary V. The length of a formula is its length as a word over the alphabet $\{\neg, \vee, \wedge, \exists, \forall, (,), v, 0, 1, f_1, \ldots, f_l, R_1, \ldots, R_m\}$, where v, 0, 1 are used for writing variables. The length of ϕ is denoted by $|\phi|$. A *sentence*

is a formula with no free variable. A sentence is in *prenex normal form* if it is written as $(Q_1x_1)\dots(Q_kx_k)\phi(x_1,\dots,x_k)$, where $Q_1,\dots,Q_k$ are quantifiers and $\phi(x_1,\dots,x_k)$ is quantifier-free. A k-tuple $(x_1,\dots,x_k)$ is also denoted by $\bar{x}_k$.

A *structure* $\mathcal{A} = \langle A, f_1,\dots,f_l,R_1,\dots,R_m\rangle$ is made of a nonempty *domain* A, functions f_i and relations R_j. We often use the same letter to denote symbols from vocabulary V and their interpretations as functions and relations on A. If $\phi(\bar{x}_k)$ is a formula over vocabulary V with free variables $\bar{x}_k$, and if $\bar{a}_k \in A^k$, then we write $\mathcal{A} \models \phi(\bar{a}_k)$ if $\phi(\bar{a}_k)$ is true in $\mathcal{A}$. The *theory* of a structure $\mathcal{A}$ is the set of sentences true in $\mathcal{A}$: $\mathrm{Th}(\mathcal{A}) = \{\phi : \mathcal{A} \models \phi\}$. We write $\mathrm{Th}(A, f_1,\dots,f_l,R_1,\dots,R_m)$ for $\mathrm{Th}(\langle A, f_1,\dots,f_l,R_1,\dots,R_m\rangle)$.

2.3 The structure

We consider the structure $\langle \mathbb{N}, =, S, P\rangle$, where $\mathbb{N} = \{0,1,2,\dots\}$ and S, P are the total functions defined by $S(x) = x+1$ and $P(x) = 2^x$ (S for successor and P for power). The partial functions S^{-1} and P^{-1} on $\mathbb{N}$ are defined by $S^{-1}(x) = x-1$ and $P^{-1}(x) = \log x$, base two logarithm of x. The binary relations R_S and R_P on $\mathbb{N}$ are defined by: $R_S(x,y)$ if $S(x) = y$, and $R_P(x,y)$ if $P(x) = y$.

The *segment* $[x,y]$ is the set $\{t \in \mathbb{N} : x \le t \le y\}$.

A k-tuple of functions $(f_1,\dots,f_k) \in \{S,P,S^{-1},P^{-1}\}^k$ is also denoted by $\bar{f}_k$. We often identify the k-tuple $\bar{f}_k = (f_1,\dots,f_k)$ with the partial function $f_k \circ f_{k-1} \circ \cdots \circ f_1$.

We use the terminology of graph theory applied to the undirected graph $(\mathbb{N}, E)$, where there is an edge between two numbers if one of them is the image of the other one by S or P (This is the Gaifman's graph [8] of the structure). A *walk* from x to y of length k is a $k+1$-tuple $(u_0,u_1,\dots,u_k)$ such that $u_0 = x$, $u_k = y$, and, for all $i \in [0,k-1]$, we have $R_S(u_i,u_{i+1})$ or $R_S(u_{i+1},u_i)$ or $R_P(u_i,u_{i+1})$ or $R_P(u_{i+1},u_i)$. A *subwalk* of this walk is a walk $(u_i,\dots,u_j)$ such that $0 \le i \le j \le k$. Note that there is no walk of length one from a number to itself. But such a walk can happen in other structures, such as $\langle \mathbb{N}, =, x+1, x^2\rangle$.

The k-tuple of functions $\bar{f}_k = (f_1,\dots,f_k)$ is *associated* to a walk $(u_0,\dots,u_k)$ if, for all $i \in [0,k-1]$, we have $f_{i+1}(u_i) = u_{i+1}$. Note that many k-tuples of functions can happen to be associated to a given walk. A walk is *unambiguous* if there is only one k-tuple of functions associated to this walk. Else this walk is *ambiguous*. The following facts can be proved easily.

Fact 2.1 *A walk* $(u_0, \ldots, u_k)$ *is unambiguous if and only if, for all* $i \in [0, k-1]$, $(u_i, u_{i+1}) \notin \{(0,1),(1,0),(1,2),(2,1)\}$.

Fact 2.2 *Every walk in* $\mathbb{N} - \{0,1\}$ *is unambiguous.*

A *path* is a walk with distinct vertices. A walk $(u_0, \ldots, u_k)$ is *closed* if $u_0 = u_k$. A *cycle* is a walk $(u_0, \ldots, u_k)$ with $k \geq 3$, $u_0, \ldots, u_{k-1}$ distinct, and $u_0 = u_k$. This cycle has length k. Note that, by definition, the length of a cycle is always at least 3. The following fact can be proved easily.

Fact 2.3 *(i) Up to a circular permutation, there is a unique cycle of length* 3*:* $(2,3,4,2)$.

(ii) There is no cycle of length 4 *or* 5.

(iii) Up to a circular permutation, there is a unique cycle of length 6*:* $(3,4,5,6,7,8,3)$.

A subset A of $\mathbb{N}$ is *connected* if, for all x, $y \in A$, there is a walk from x to y in A. A subset A of $\mathbb{N}$ is *regular* if A is nonempty, connected, and contains no ambiguous walk, no cycle, and no walk of length one from a number to itself (This last condition, here an empty one, is necessary for a structure such as $\langle \mathbb{N}, =, x+1, x^2 \rangle$). A subset of $\mathbb{N}$ which is not regular is called *singular*. The following fact can be proved easily.

Fact 2.4 *Let* x, y *be distinct numbers in a regular subset* A *of* $\mathbb{N}$. *Then there is a unique path from* x *to* y *in* A.

Two subsets A and B of $\mathbb{N}$ are *isomorphic*, denoted $A \cong B$, if the substructures $\langle A, =, R_{S|_A}, R_{P|_A} \rangle$ and $\langle B, =, R_{S|_B}, R_{P|_B} \rangle$ are isomorphic, that is if there is a bijective mapping $\sigma : A \to B$ such that, for all x, $y \in A$, $R_S(x,y)$ iff $R_S(\sigma(x), \sigma(y))$, and $R_P(x,y)$ iff $R_P(\sigma(x), \sigma(y))$. The following facts can be proved easily.

Fact 2.5 *If* A *is a finite connected subset of* $\mathbb{N}$, *and* σ *is an isomorphism from* A *to* A, *then* σ *is the identity.*

Fact 2.6 *If* $\sigma_1 : A \cong B$ *and* $\sigma_2 : A \cong B$ *are isomorphisms from a finite connected subset* A *of* $\mathbb{N}$ *into* B, *then* $\sigma_1 = \sigma_2$.

We define a *distance* d on $\mathbb{N}$ by $d(x,x) = 0$, and, if $x \neq y$, $d(x,y)$ is the length of a shortest walk from x to y (Note that this walk is not necessarily unique). If x, $k \in \mathbb{N}$, the *ball* centered at x of radius k is the closed ball $B(x,k) = \{y \in \mathbb{N} : d(x,y) \leq k\}$. The following facts can be proved easily.

Fact 2.7 *If $d(x,y) = n$, and $x = u_0, u_1, \ldots, u_n = y$ is a walk from x to y of length n, then, if $0 \leq i \leq j \leq n$, we have $d(u_i, u_j) = j - i$.*

Fact 2.8 *Let $x \in \mathbb{N}$. The ball of radius one $B(x,1)$ is regular if and only if $x \geq 5$ if and only if $d(0,x) \geq 4$.*

A tower of n powers of two is denoted by $\exp_\infty(n)$. Formally, $\exp_\infty$ is recursively defined by $\exp_\infty(0) = 1$, and $\exp_\infty(k+1) = 2^{\exp_\infty(k)}$. A near inverse of $\exp_\infty$ is $\log_\infty(n) = \min\{k \in \mathbb{N} : \exp_\infty(k) \geq n\}$. The following fact can be proved easily, by induction on $d(0,x)$.

Fact 2.9 *For all $x \in \mathbb{N} - \{0,1\}$, $d(0,x) \geq 1 + \log_\infty(x)$.*

The following fact follows easily from Fact 2.9.

Fact 2.10 *For all $n \in \mathbb{N}$, $d(0, \exp_\infty(n)) = n + 1$.*

3 Proof plan

The proof of $\mathrm{Th}(\mathbb{N}, =, S, P) \in \mathrm{ATIME\text{–}ALT}(2^{O(n)}, n)$ rests on a bounded Ehrenfeucht–Fraïssé game, as developped by Ferrante and Rackoff (1979) [6]. Informally, two k-tuples $\bar{a}_k$ and $\bar{b}_k$ in $\mathbb{N}^k$ belong to the same equivalence class of the equivalence relation E_k^n if they cannot be distinguished by formulas of quantifier depth at most n. Now, given $\bar{a}_k$ and $\bar{b}_k$ such that $\bar{a}_k E_k^{n+1} \bar{b}_k$, and a new $a_{k+1} \in \mathbb{N}$, the game consists in finding $b_{k+1} \in \mathbb{N}$ such that $\bar{a}_{k+1} E_{k+1}^n \bar{b}_{k+1}$.

Intuitively, if a_{k+1} is close to 0 or to some a_i, we have no choice: b_{k+1} must be close to 0 or to b_i. The most difficult case arises when a_{k+1} is far enough from 0 and a_is. In this case we have to find b_{k+1} far enough from 0 and b_is, and with a neighborhood similar to the neighborhood of a_{k+1}. The difference between the classical Ehrenfeucht–Fraïssé game of Ehrenfeucht (1961) [4] and Fraïssé (1954) [7] and the present bounded Ehrenfeucht–Fraïssé game is that we need to find b_{k+1} as small as possible, in order to get the smallest possible complexity. The length of the proof comes from the need to control the size of b_{k+1}.

Sections 4, 5 and 6 are devoted to the analysis of this most difficult case. To be far enough from 0 means to be the center of a big enough regular ball, and Section 4 gives a sufficient condition for a ball to be regular. To have similar neighborhoods means to be in two isomorphic regular balls, and Section 5 gives a sufficient condition for two regular balls to be isomorphic. Section 6 ends this analysis by providing, in each isomorphism class of regular balls, a ball with small enough center.

The aim of bounded Ehrenfeucht–Fraïssé games is to make easy the decision procedure of a prenex sentence by bounding its quantifiers. This is done in Section 7. Finally, in Section 8, we give the decision procedure. The input is a sentence over the vocabulary $\{=, S, P\}$. It is transformed into a sentence in prenex normal form over the relational vocabulary $\{=, R_S, R_P\}$. Then we can bound its quantifiers according to the results of Section 7. Alternations of existential and universal states are used for handling quantifiers, and atomic formulas are shown to be decidable in small time.

4 A sufficient condition for a ball to be regular

In this section, we prove that a ball $B(x, k)$ is regular if $d(0, x) \geq 2k+2$. We do this by proving that a singular ball contains a small enough cycle, and that a cycle contains a small enough element, giving a short path from 0 to the center of the ball.

Thus, we first prove the two following lemmas.

Lemma 4.1 *Let C be a cycle of length $n \geq 7$ in $\mathbb{N}$. Then there is a $u \in C$ such that $u \leq (n-1)/2$.*

Proof. Let C be a cycle in $\mathbb{N}$ of length $n \geq 7$, and let $z = \max C$. The numbers next to z in C are distinct, and can't be $z+1$ or 2^z by maximality of z. So they are $z-1$ and $\log z$. We can suppose C oriented in the direction $\ldots, z-1, z, \log z, \ldots$. Let p be the greatest integer such that $z-p, z-p+1, \ldots, z-1, z, \log z$ is a subwalk of C.

Case 1: $z - p = \log z$.

Then C is the cycle $(\log z, \log z + 1, \ldots, z-1, z, \log z)$, of length $n = z - \log z + 1$.

If $\log z \leq 3$, then $\log z \leq (n-1)/2$ because $n \geq 7$.

If $\log z \geq 4$, then $\log z \leq (z - \log z)/2 = (n-1)/2$.

Thus there is a $u = \log z$ in C such that $u \leq (n-1)/2$

Case 2: $z - p > \log z$.

Then the member of C just before $z - p$ can't be $z - p - 1$ by definition of p, can't be 2^{z-p} by maximality of z, and can't be $z - p + 1$ which is just after $z - p$. So this member is $\log(z-p)$, and C contains the subwalk $(\log(z-p), z-p, z-p+1, \ldots, z-1, z, \log z)$, of length $p+2$.

Since $\log(z-p) \leq \log z - 1$, we have $p \geq z/2$, so C has length $n \geq p+3 \geq z/2+3$, which yields $\log(z-p) \leq \log(z/2) \leq \log(n-3) \leq (n-1)/2$. Thus there is a $u = \log(z-p)$ in C such that $u \leq (n-1)/2$. $\square$

Lemma 4.2 *Let $B(x,k)$ be a singular ball, $B(x,k) \subseteq \mathbb{N} - \{0,1\}$. Then there is a cycle in $B(x,k)$ which has length at most $2k+1$.*

Proof. Let $B(x,k)$ be a singular ball that does not contain 0 and 1. By Fact 2.2, $B(x,k)$ does not contain an ambiguous walk, so $B(x,k)$ contains a cycle C. Let a be a member of C with maximal distance h from x: $d(x,a) = h \leq k$. Consider b and b' next to a in C. Their distances from x are either $h-1$ or h.

Case 1: Both b and b' are at distance $h-1$ from x.

Then let $x = u_0, u_1, \ldots, u_{h-1} = b$ and $x = v_0, v_1, \ldots, v_{h-1} = b'$ be paths from x to b and b' in $B(x,k)$, and $i = \max\{j \in [0, h-1] : u_i = v_j\}$. Cycle C has length at least 3, so $b \neq b'$ and $i < h-1$. We have $u_j \neq v_j$ for all $j \in [i+1, h-1]$. Note that, for all $j \in [0, h-1]$, $d(x,u_j) = d(x,v_j) = j$, so, if $j \neq j'$, then $u_j \neq v_{j'}$. Thus, the closed walk $(a, u_{h-1}, \ldots, u_{i+1}, u_i, v_{i+1}, \ldots, v_{h-1}, a)$ is a cycle, of length $2(h-i) \leq 2k+1$.

Case 2: One of b or b', for example b, is at distance h from x.

Then, as in Case 1, we consider the paths $x = u_0, u_1, \ldots, u_h = a$ from x to a, and $x = v_0, v_1, \ldots, v_h = b$ from x to b, and define $i = \max\{j \in [0,h] : u_j = v_j\} < h$. Then the closed walk $(a, u_{h-1}, \ldots, u_{i+1}, u_i, v_{i+1}, \ldots, v_{h-1}, b, a)$ is a cycle, of length $2(h-i)+1 \leq 2k+1$. $\square$

Note that the upper bound given by Lemma 4.2 is achieved in the singular balls $B(2^{2m-1}+m, 2^{2m-1}-m)$, $m \geq 1$, by the cycle $(2m, 2m+1, \ldots, 2^{2m}-1, 2^{2m}, 2m)$.

Proposition 4.3 *Let $x, k \in \mathbb{N}$. If $d(0,x) \geq 2k+2$, then the ball $B(x,k)$ is regular.*

Proof. If $k = 1$ and $d(0, x) \geq 4$, then $B(x, k)$ is regular by Fact 2.8.

If $k \geq 2$, we suppose that $B(x, k)$ is singular and we will prove that in this case $B(x, k) \cap [0, k] \neq \emptyset$. Then there is a $y \in B(x, k) \cap [0, k]$, and $d(0, x) \leq d(0, y) + d(y, x) \leq k + k = 2k$, which proves the proposition.

So, let $B(x, k)$ be a singular ball of radius $k \geq 2$.

If $B(x, k) \cap \{0, 1\} \neq \emptyset$, then $B(x, k) \cap [0, k] \neq \emptyset$.

If $B(x, k) \subseteq \mathbb{N} - \{0, 1\}$, then, by Lemma 4.2, there is a cycle C in $B(x, k)$ of length $n \leq 2k + 1$. By Fact 2.3, C can't have length 4 or 5. If C has length $n = 3$, then C is $(2, 3, 4, 2)$, and $2 \in B(x, k) \cap [0, k]$. If C has length $n = 6 \leq 2k+1$, then C is $(3, 4, 5, 6, 7, 8, 3)$, and $k \geq 3$, so $3 \in B(x, k) \cap [0, k]$.

At last, if C has length $n \geq 7$, then, by Lemma 4.1, there is a $u \in C$ such that $u \leq (n - 1)/2 \leq k$, and $u \in B(x, k) \cap [0, k]$. $\square$

5 A sufficient condition for two regular balls to be isomorphic

In this section, we prove that the isomorphism classes of regular balls are classified by the tuples of functions associated to the paths connecting the centers of the balls to their minimums. This needs a long analysis of the paths connecting two numbers (Lemma 5.1), and particularly two members of a regular ball (Lemmas 5.2, 5.3, 5.4 and 5.5). Moreover, Lemmas 5.1, 5.2 and 5.4 will be used again in the next section.

Lemma 5.1 *Let x, y, $t \in \mathbb{N}$, such that $x < y$ and $2^t \leq y < 2^{t+1}$. Then a shortest path from x to y belongs to at least one of the three following types:*

(i) s-path: $[x, y]$, of length $y - x$,

(ii) t-path: a shortest path from x to t, followed by $[2^t, y]$, of length $d(x, t) + y - 2^t + 1$,

(iii) $t+1$-path: a shortest path from x to $t+1$, followed by $[y, 2^{t+1}]$ (covered from 2^{t+1} to y), of length $d(x, t + 1) + 2^{t+1} - y + 1$.

Proof. If $t \in \{0, 1\}$, it is easy to see that the shortest paths from x to y are s-paths, so we suppose $y \geq 4$.

Let C be a shortest path from x to y: $x = u_0, u_1, \ldots, u_n = y$, of length $n = d(x, y)$, and let $z = \max C = \max\{u_i : i \in [0, n]\}$.

Case 1: $z = y$.

We consider u_{n-1}. By maximality of z, $u_{n-1} \in \{\log y, y-1\}$, and, if $u_{n-1} = \log y$, then C is a t-path.

We consider now the case $u_{n-1} = y - 1$. The set $\{k \in \mathbb{N} : (\forall i \in [0,k]) u_{n-i} = y - i\}$ is a nonempty bounded set, so has a maximum $m \geq 1$, and $u_{n-m} = y - m$.

If $m = n$, then C is an s-path.

If $m < n$, we consider u_{n-m-1}. We know that $u_{n-m-1} \in \{u_{n-m}-1, u_{n-m}+1, 2^{u_{n-m}}, \log u_{n-m}\}$, and it is easy to check that only $u_{n-m-1} = \log u_{n-m}$ is possible. Since $u_{n-m} < y < 2^{t+1}$, we have $u_{n-m-1} < t+1$, so there is an $a \in [0,t]$ such that $u_{n-m-1} = t - a$. Then $y - m = u_{n-m} = 2^{t-a}$, so $m = y - 2^{t-a}$. We have $u_{n-m} = 2^{t-a} \leq 2^t$ so, by definition of m, $2^t = y - (y - 2^t) = u_{n-y+2^t}$.

Then, by Fact 2.7: $d(t-a, 2^t) = d(u_{n-m-1}, u_{n-y+2^t}) = n - y + 2^t - (n - m - 1) = 2^t - 2^{t-a} + 1$.

The path $[t-a, t] \cup \{2^t\}$ is a path from $t-a$ to 2^t of length $a+1$, thus $2^t - 2^{t-a} + 1 \leq a + 1$, which is possible only if $a = 1$, because $t \geq 2$.

Thus, $u_{n-m-1} = t$, $u_{n-m} = 2^t$, and C is a t-path.

Case 2: $y < z$.

Let $k \in [1, n-1]$, such that $z = u_k$, and consider u_{k-1} and u_{k+1}. By maximality of z, $u_{k-1}, u_{k+1} \in \{z-1, \log z\}$.

Subcase 2.1: $u_{k-1} = z - 1$ and $u_{k+1} = \log z$.

We prove that this subcase is impossible. The set $\{j \in \mathbb{N} : (\forall i \in [0,j]) u_{k-i} = z - i\}$ is a nonempty bounded set, so has a maximum $m \geq 1$. We have $u_{k-m} \neq x$ because $x < y < z$, so we can consider u_{k-m-1}.

We know that $u_{k-m-1} \in \{u_{k-m} - 1, u_{k-m} + 1, 2^{u_{k-m}}, \log u_{k-m}\}$. Now, $u_{k-m-1} = u_{k-m} - 1$ is impossible by definition of m, $u_{k-m-1} = u_{k-m} + 1$ is impossible because $u_{k-m} + 1 = u_{k-m+1}$, and $u_{k-m-1} = 2^{u_{k-m}}$ is impossible, for then $z - m = u_{k-m} < 2^{u_{k-m}} = u_{k-m-1} \leq z = \max C$, and there exists a $j \in [0,m]$ such that $u_{k-m-1} = z - j = u_{k-j}$.

The last case is $u_{k-m-1} = \log u_{k-m}$, and we now prove that it is impossible.

Let $a = \log z - u_{k-m-1}$. Then $z - m = u_{k-m} = 2^{u_{k-m-1}} = 2^{\log z - a} = z/2^a$, so $m = z(1 - 1/2^a)$. By Fact 2.7, $d(\log z - a, \log z) = d(u_{k-m-1}, u_{k+1}) = k + 1 - (k - m - 1) = m + 2 = z(1 - 1/2^a) + 2$. But the path $[\log z - a, \log z]$ is a path from $\log z - a$ to $\log z$ of length a, so $z(1 - 1/2^a) + 2 \leq a$, which cannot hold, since $z \geq 2^a$.

Subcase 2.2: $u_{k-1} = \log z$ and $u_{k+1} = z - 1$.

The set $\{j \in \mathbb{N} : (\forall i \in [0, j])u_{k+i} = z - i\}$ is a nonempty bounded set, so has a maximum $m \geq 1$. An analysis parallel to the one in Subcase 2.1 shows that $u_{k+m} \neq y$ is impossible, thus $u_{k+m} = y$.

Let $a = \log z - t$. We have $a \geq 1$, so $y < 2^{t+1} \leq z$. By Fact 2.7, $[y, z]$ is a shortest path from y to z, so $d(2^{t+1}, z) = z - 2^{t+1} = 2^{t+a} - 2^{t+1}$. But $\{2^{t+1}\} \cup [t+1, t+a] \cup \{2^{t+a}\}$ is a path from 2^{t+1} to $2^{t+a} = z$, of length $a+1$, so $a+1 \geq d(2^{t+1}, z) = 2^{t+a} - 2^{t+1} \geq 4(2^a - 2)$, because $t \geq 2$. This inequality is possible only if $a = 1$. Thus, $\log z = t + 1$ and C is a $t+1$-path. $\square$

Lemma 5.2 *Let $B(x, k)$ be a regular ball, $m = \min B(x, k)$, and let $\bar{f}_k$ be the k-tuple of functions associated to the path from m to x. Then $\bar{f}_k \in \{S, S^{-1}, P\}^k$.*

Proof. Note that, since the ball $B(x, k)$ is regular, there is a unique path from $m = \min B(x, k)$ to x in $B(x, k)$, this path has length k, and there is a unique k-tuple of functions $\bar{f}_k$ associated to this path.

We prove the lemma by induction on k. If $k = 1$, then either $m = x - 1$ or $m = \log x$.

Suppose that the result is true for all $l < k$, and let $B(x, k)$ be a regular ball, $m = \min B(x, k)$, and let $\bar{f}_k$ be the k-tuple associated to the path from m to x. Then $\bar{f}_{k-1}$ is the $(k-1)$-tuple associated to the path from m to $y = f_k^{-1}(x)$. Since $B(y, k-1) \subseteq B(x, k)$, the ball $B(y, k-1)$ is regular, and $m = \min B(y, k-1)$. By induction hypothesis, $\bar{f}_{k-1} \in \{S, S^{-1}, P\}^{k-1}$.

Now, we prove that $f_k \in \{S, S^{-1}, P\}$. Let $t \in \mathbb{N}$ such that $2^t \leq x < 2^{t-1}$. By Lemma 5.1, the path from m to x is an s-path, a t-path or a $t+1$-path. If it is an s-path, then $f_k = S$. If it is a t-path, then $f_k = S$ if $x > 2^t$ and $f_k = P$ if $x = 2^t$. If it is a $t+1$-path, then $f_k = S^{-1}$. So $f_k \in \{S, S^{-1}, P\}$ and $\bar{f}_k \in \{S, S^{-1}, P\}^k$. $\square$

Lemma 5.3 *Let $B(x, k)$ be a regular ball, let $[a, b] \subseteq B(x, k)$, and let $u, v \in \mathbb{N}$, such that $u < v$ and $2^u, 2^v \in [a, b]$. Then $v = u + 1$.*

Proof. Let $B(x, k)$ be a regular ball, $[a, b] \subseteq B(x, k)$, and $u < v$, such that $a \leq 2^u < 2^v \leq b$.

(1) The ball $B(x, k)$ is regular, thus we have $u \geq 2$, $v \geq 3$, and consequently $2^v - 2^u \geq 2^v - 2^{v-1} = 2^{v-1} \geq v + 1 > v - u + 2$. Thus the path from 2^u to 2^v of length $v - u + 2$, via u and v, is shorter than the path $[2^u, 2^v]$.

(2) Now, let $y \in [a,b]$ with a minimal distance h from x among the numbers in $[a,b]$. By unicity of paths in a regular ball, y is unique, and the paths from y to $t \in [a,y]$ and $t' \in [y,b]$ are respectively $[t,y]$ and $[y,t']$.

If $y \leq 2^u$, then by part (1) above, the path $[y,2^u] \cup [u,v] \cup \{2^v\}$ from y to 2^v is shorter than the path $[y,2^v]$. Now, if $w \in [u,v]$, then $d(x,w) \leq d(x,y) + d(y,w) \leq d(x,y) + d(y,2^v)$. By Fact 2.7, $d(x,y) + d(y,2^v) = d(x,2^v) \leq k$, so $w \in B(x,k)$. We have proved that $[u,v] \subseteq B(x,k)$, so $B(x,k)$ contains the cycle formed by $[u,v]$ and $[2^u,2^v]$, which is impossible.

A similar reasoning proves that $y \geq 2^v$ is impossible, so we have $2^u < y < 2^v$.

(3) Suppose there is a number w such that $u < w < v$. Then $2^u < 2^w < 2^v$, so either $y \leq 2^w < 2^v$, or $2^u < 2^w \leq y$. But the same reasoning as in part (2) above shows that this is impossible. Thus, we have $v = u + 1$. □

Lemma 5.4 *Let $B(x,k)$ be a regular ball, and let $\bar{f}_n$ be an n-tuple of functions associated to a path of length $n \geq 2$ in $B(x,k)$, such that there is an $i \in [1,n]$ such that $f_i = P$. Then, for any $j \in [i+1,n]$, we have $f_j \neq P^{-1}$.*

Proof. By contradiction. Suppose there is a path $u_0, u_1, \ldots, u_n$ of length $n \geq 2$ in a regular ball $B(x,k)$, such that the associated n-tuple of functions $\bar{f}_n$ contains both P and P^{-1} at i and $j > i$, that is, $f_i = P$, $f_j = P^{-1}$. Then we define $j_0 = \min\{j \in [1,n] : (\exists i < j) f_i = P \text{ and } f_j = P^{-1}\}$, and $i_0 = \max\{i \in [1,n] : i < j_0 \text{ and } f_i = P\}$. Then $u_{i_0} = 2^{u_{i_0}-1}$, $u_{j_0-1} = 2^{u_{j_0}}$, and, for any $h \in [i_0, j_0 - 2]$, $u_{h+1} = T(u_h)$, where $T = S$ or $T = S^{-1}$. We can suppose $T = S$, or change the orientation of the path. Then we can applied Lemma 5.3. Because $[u_{i_0}, u_{j_0-1}] \subseteq B(x,k)$, $u_{i_0-1} < u_{j_0}$, and $2^{u_{i_0}-1}$, $2^{u_{j_0}} \in [u_{i_0}, u_{j_0-1}]$, we have $u_{j_0} = u_{i_0-1} + 1$, and we get a cycle in a regular ball. □

Lemma 5.5 *Let $B(x,k)$ be a regular ball, $m = \min B(x,k)$, and $y \in B(x,k)$. Let $\bar{f}_k$ be associated to the path from x to m, and let $\bar{g}_l$ be associated to the path from x to y in $B(x,k)$. If $q \in [1,l]$ is such that $g_q = P^{-1}$, then $\bar{g}_q = \bar{f}_q$.*

Proof. Let $\bar{f}_k$ and $\bar{g}_l$ be associated to the paths from x to $m = \min B(x,k)$ and $y \in B(x,k)$ respectively. Then $l \leq k$. If $\bar{g}_i = \bar{f}_i$ for any $i \in [1,l]$, then $\bar{g}_q = \bar{f}_q$. Otherwise, let j be the smallest $i \in [0, l-1]$ such that $\bar{g}_{i+1} \neq \bar{f}_{i+1}$, and consider the walk from m to y obtained by concatenating the path from

m to u and the path from u to y in $B(x,k)$. Since $B(x,k)$ is regular, this walk is a path. Let $\bar{h}_p$ ($p = k+l-2j$) be the p-tuple of functions associated to this path. That is, $h_i = f_{k-i+1}^{-1}$ if $1 \leq i \leq k-j$, and $h_i = g_{2j-k+i}$ if $k-j+1 \leq i \leq k+l-2j$.

We will show that, if $g_q = P^{-1}$ for a $q \in [1,l]$, then it is impossible that $q \geq j+1$ (so $q \leq j$ and $\bar{g}_q = \bar{f}_q$).

Suppose that $q \geq j+1$. We have $h_{k-2j+q} = g_q = P^{-1}$, so, by Lemma 5.4, the h_is are distinct from P for $i \in [1, k-2j+q]$. For $i \in [1, k-j]$, these h_is are f_{k-i+1}^{-1}s, which, by Lemma 5.2, are in $\{S, S^{-1}, P\}$. Thus, for $i \in [1, k-j]$, the h_is are in $\{S, S^{-1}\}$. Since $m = \min B(x,k)$, $h_i = S$ for all $i \in [1, k-j]$. Now, we consider the g_is for $i \in [j+1, q]$, which are also h_is for $i \in [k-j+1, k+q-2j]$. Since $g_q = P^{-1}$, these functions are distinct from P by Lemma 5.4. Before the first P^{-1}, these functions are in $\{S, S^{-1}\}$. Since $g_{j+1} \neq f_{j+1} = S^{-1}$, these functions are Ss before the first P^{-1}, which is obtained for h_r. But then, the path from m to $\bar{h}_{r-1}(x)$ is $[m, \bar{h}_{r-1}(x)]$, and $\bar{h}_r(x) = P^{-1}(\bar{h}_{r-1}(x)) \geq m = \min B(x,r)$, and $\bar{h}_r(x) < \bar{h}_{r-1}(x)$. Thus $\bar{h}_r(x) \in [m, \bar{h}_{r-1}(x)]$, and $\bar{h}_r$ is associated to a walk from m to y which can't be a path. $\square$

Proposition 5.6 *Let $B(x,k)$ and $B(x',k')$ be two regular balls, such that the same k-tuple of functions is associated to the path from x to $m = \min B(x,k)$ and to the path from x' to $m' = \min B(x',k')$. Then $B(x,k)$ is isomorphic to $B(x',k')$.*

Proof. Let $\bar{f}_k$ be the k-tuple of functions associated to both paths from x to m and from x' to m'. We define σ from $B(x,k)$ to $B(x',k')$ the following way. If $y \in B(x,k)$ and $\bar{g}_l$ is the l-tuple of functions associated to the path from x to y, we define $\sigma(y) = \bar{g}_l(x')$. That is, $\sigma(\bar{g}_l(x)) = \bar{g}_l(x')$.

(1) *σ is well defined.*

The l-tuple $\bar{g}_l$ is unique because $B(x,k)$ is regular. We have to prove that $\bar{g}_l(x')$ is defined. This is true if and only if, for any $i \in [1,l]$, if $g_i = P^{-1}$, then $\bar{g}_i(x')$ is defined. But then, by Lemma 5.5, $\bar{g}_i = \bar{f}_i$, and $\bar{g}_i(x') = \bar{f}_i(x')$ is defined.

(2) *σ is one-to-one.*

Let y_1, $y_2 \in B(x,k)$, $y_1 \neq y_2$, such that $y_1 = \bar{g}_{l_1}(x)$, $y_2 = \bar{h}_{l_2}(x)$ in the regular ball $B(x,k)$. Then $\bar{g}_{l_1} \neq \bar{h}_{l_2}$, so, in the regular ball $B(x',k')$, we have $\bar{g}_{l_1}(x') \neq \bar{h}_{l_2}(x')$, that is $\sigma(y_1) \neq \sigma(y_2)$.

(3) *σ is a bijection.*

The balls $B(x,k)$ and $B(x',k')$ have symmetric positions in the statement of Proposition 5.6, so a map τ from $B(x',k')$ to $B(x,k)$ can be defined, which is well defined and one-to-one by the same reasoning as in parts (1) and (2). So $B(x,k)$ and $B(x',k')$ have the same number of elements, and σ and τ are bijections because they are one-to-one maps between sets with same number of elements.

(4) *σ is an isomorphism.*

Let y and $z = g(y)$ be in $B(x,k)$, where $g \in \{S, S^{-1}, P, P^{-1}\}$. We can suppose that the path from x to y does not contain z (otherwise, we swap y and z and replace g by g^{-1}). Let $\bar{g}_{l-1}$ be the $(l-1)$-tuple of functions associated to the path from x to y, and let $\bar{g}_l$ be the l-tuple of functions associated to the path from x to z (so $g_l = g$). Then $\sigma(g(y)) = \sigma(z) = \sigma(\bar{g}_l(x)) = \bar{g}_l(x') = g(\bar{g}_{l-1}(x')) = g(\sigma(\bar{g}_{l-1}(x))) = g(\sigma(y))$. So σ is an isomorphism. □

6 End of analysis of the most difficult case

In this section, we prove that we can find, in the isomorphism class of a regular ball, a ball with a small enough center. The minimum of this ball is a power of two, which allow us to control the distance of its center from 0 (Lemma 6.2). The results of this section use all the machinery developped in Sections 4 and 5.

Lemma 6.1 *If t, $x \in \mathbb{N}$, and $x \leq 2^t$, then any shortest path from x to 2^t is an s-path (i.e., is $[x, 2^t]$), or a t-path (i.e., goes via t).*

Proof. If $t = 0$ and $x \leq 2^t$, then the shortest path from x to 2^t is $[x, 2^t]$.

If $t \geq 1$, then, by Lemma 5.1, any shortest path from x to 2^t is an s-path, a t-path, or a $t+1$-path. If it is a $t+1$-path, then $d(x, 2^t) = d(x, t+1) + 2^{t+1} - 2^t + 1 = d(x, t+1) + 2^t + 1$.

But $d(x, 2^t) \leq d(x, t+1) + d(t+1, t) + d(t, 2^t) = d(x, t+1) + 2$, so $2^t + 1 \leq 2$, which is impossible. □

Lemma 6.2 *Let $B(x,k)$ be a regular ball, and let $m = \min B(x,k)$ be a power of 2. Then $d(0,m) + k - 1 \leq d(0,x) \leq d(0,m) + k$.*

Proof. Let $B(x,k)$ be a regular ball with $k \geq 1$. If $m = \min B(x,k)$ is a power of 2, then $m \geq 4$. We have readily $d(0,x) \leq d(0,m) + d(m,x) \leq d(0,m) + k$, so we have to prove that $d(0,x) \geq d(0,m) + k - 1$.

Let C_1 be the unique path from x to m, and let C_2 be a path from x to 0 of length $d(0,x)$, so C_2 is the path $x = u_0, u_1, \ldots, u_{d(0,x)} = 0$. The set $\{i \in [0, d(0,x)] : u_i \in C_1\}$ is nonempty because it contains 0, so it has a maximum l. Let $y = u_l$. Then y is on both C_1 and C_2, so, by Fact 2.7, $d(0,x) = d(0,y) + d(y,x)$ and $d(m,x) = d(m,y) + d(y,x)$.

If $y = m$, then the walk $x = u_0, \ldots, u_l = m$ is a path from x to m in the regular ball $B(x,k)$, so it is C_1, which is then a subpath of C_2. Thus, $d(0,x) = d(0,m) + d(m,x) = d(0,m) + k$.

We suppose now on that $y \neq m$. Since $y \in B(x,k)$, we have $m < y$, by definition of m. We consider the subpath C_1' of C_1, from y to m, and the subpath C_2' of C_2, from y to 0. By definition of y, $C_1' \cap C_2' = \{y\}$. By Lemma 5.1, C_1' and C_2' (when covered, respectively, from m to y and from 0 to y) are s-paths, t-paths, or $t+1$-paths, but do not belong to the same type. Let $t \in \mathbb{N}$ such that $2^t \leq y < 2^{t+1}$. Since $m \geq 4$, we have $y \geq m + 1 \geq 5$, and $t \geq 2$. Note that C_2' can't be an s-path, because $[0,z]$ is a shortest path from 0 to z if and only if $z \leq 3$.

Case 1: $y = 2^t$.

We prove that this is impossible.

By Lemma 6.1, any shortest path from 0 to $y = 2^t$ is an s-path or a t-path. But C_2' can't be an s-path, so it is a t-path. Similarly, by Lemma 6.1, any shortest path from m to $y = 2^t$ is an s-path or a t-path. But C_1' can't belong to the same type as C_2', so C_1' is an s-path, that is, $C_1' = [m,y]$. But $k = d(x,m) = d(x,y) + d(y,m) \geq d(x,y) + 1$, so $d(x,y) \leq k - 1$. On the other hand, $d(y,t) = d(2^t,t) = 1$, so $d(x,t) \leq d(x,y) + d(y,t) \leq k - 1 + 1 = k$. Thus, $t \in B(x,k)$ and $m \leq t$. So $t \in [m,y] = C_1'$ and $t \in C_1' \cap C_2'$, which is impossible.

Case 2: $2^t < y < 2^{t+1}$.

By definition of y, one of the path C_1' and C_2' begins with $y, y+1, \ldots$, and the other one by $y, y-1, \ldots$, so there are three possible cases.

Subcase 2.1: C_1' is a t-path and C_2' is a $t+1$-path.

If we suppose $d(x,t+1) \leq k$, then the path from x to $t+1$ via $[y, 2^{t+1}]$ is in $B(x,k)$, and the regular ball $B(x,k)$ contains the cycle $t+1, t, 2^t, \ldots, 2^{t+1}, t+1$, which is impossible. Thus $d(x,t+1) \geq k+1$. We have $d(x,t+1) \leq d(x,t) + d(t,t+1) = d(x,t) + 1$, so $d(x,t) \geq k$. Thus, $k = d(x,m) =$

$d(x,t) + d(t,m) \geq k + d(t,m)$, so $d(t,m) = 0$, $t = m$, and $d(x,t) = k$, $d(x,t+1) = k+1$. Thus, $d(0,x) = d(0,t+1)+d(t+1,x) = d(0,t+1)+k+1$, and $d(0,m) = d(0,t) \leq d(0,t+1)+d(t+1,t) = d(0,x)-k-1+1 = d(0,x)-k$. We get what we wanted: $d(0,x) \geq d(0,m) + k$.

Subcase 2.2: C_1' is a $t+1$-path and C_2' is a t-path.

We argue as in Subcase 2.1, swapping t and $t+1$.

Subcase 2.3: C_1' is an s-path and C_2' is a $t+1$-path.

Then the shortest path from y to m is $[m,y]$, of length $d(y,m) = y - m$. If we suppose $m \leq 2^{t-1}$, then the path $[m, 2^{t-1}] \cup \{t-1, t\} \cup [2^t, y]$ is a path from m to y of length $y - m - 2^{t-1} + 3 \geq d(y,m) = y - m$, so $2^{t-1} \leq 3$, $t = 2$, $m \leq 2^{t-1} \leq 2$ and $B(x,k)$ is not regular. Thus, $m > 2^{t-1}$. Since m is a power of 2, $m \geq 2^t$. But $2^t < y < 2^{t+1}$, so $m = 2^t$. Then $t+1 < 2^t = m$, so $t+1$ is not in $B(x,k)$ and $d(x,t+1) \geq k+1$. Since $t+1$ is on C_2, $d(0,x) = d(0,t+1) + d(t+1,x)$. Thus, $d(0,m) \leq d(0,t+1) + d(t+1,t) + d(t,m) = d(0,x) - d(t+1,x) + 2 \leq d(0,x) - (k+1) + 2$, and $d(0,x) \geq d(0,m) + k - 1$. □

Proposition 6.3 *Let $B(x,k)$ be a regular ball, $m = \min B(x,k)$, $x = \bar{f}_k(m)$. Let $l \geq 3k+1$ and $y = \bar{f}_k(\exp_\infty(l))$. Then*

(i) $B(y,k)$ is regular,

(ii) $\exp_\infty(l) = \min B(y,k)$,

(iii) $B(y,k)$ is isomorphic to $B(x,k)$,

(iv) $k + l \leq d(0,y) \leq k + l + 1$.

Proof. We can suppose $k \geq 1$. Note that, in the hypotheses of this proposition, $\bar{f}_k(\exp_\infty(l))$ is defined, because, by Lemma 5.2, $f_i \in \{S, S^{-1}, P\}$ for all $i \in [1,k]$, and $\exp_\infty(l) \geq \exp_\infty(3k+1) \geq k$.

(i) We first prove that $B(y,k)$ is regular. Since $\bar{f}_k$ defines a path from $\exp_\infty(l)$ to y of length k, we have $d(y, \exp_\infty(l)) \leq k$. By Fact 2.10, we have $d(0, \exp_\infty(l)) = l + 1 \geq 3k + 2$. Thus, $3k + 2 \leq d(0, \exp_\infty(l)) \leq d(0,y) + d(y, \exp_\infty(l)) \leq d(0,y) + k$, so $d(0,y) \geq 2k + 2$. By Proposition 4.3, $B(y,k)$ is regular.

(ii) Let $\exp_\infty(l) = v$. We have $y = \bar{f}_k(v)$ and we want to prove that $v = \min B(y,k)$. Let $N = \min B(y,k)$, and let $\bar{g}_k$ be the k-tuple of functions

associated to the path from y to N. We saw that there is no P^{-1} in $\bar{f}_k$ and, by Lemma 5.2, there is no P in $\bar{g}_k$.

Suppose $v \neq N$, and let u be the point after which the paths from y to N and from y to v are distinct.

Suppose that there is a P in the path from v to u. Then, by Lemma 5.4, there is no P^{-1} from u to N. Thus there are only S and S^{-1} from u to N. Since $N = \min B(x,k)$, there are only S^{-1}, and the path from u to N is $[N,u]$. Let w be on the path from u to v, such that there is no P^{-1} from u to w and a P^{-1} just after w. Since there is no P from u to w, there are only S or S^{-1}. Thus the path from N to w via u is $[N,w]$. But $P^{-1}(w)$ is on the path from u to v, so is in $B(x,k)$, and $P^{-1}(w) \geq N$. Since $P^{-1}(w) < w$, we have $P^{-1}(w) \in [N,w]$, which is impossible.

Thus, there is no P from v to u. Since there is no P^{-1}, there are only S or S^{-1}. Thus the path from v to u is $[v,u]$. Since the paths from u to N and from u to v are distinct, there is a P^{-1}just after u on the path from u to N. So let t be such that $u = 2^t$. We have $k = d(y,v) = d(y,u) + d(u,v) = d(y,u) + u - v$.

If $u - v \geq 2$, then $d(y, t-1) \leq d(y,u) + d(u,t) + d(t,t-1) = d(y,u) + 2 = k - (u-v) + 2 \leq k$, so $t - 1 \in B(y,k)$, and the regular ball $B(y,k)$ contains the cycle $t-1, t, u, u-1, \ldots, 2^{t-1}, t-1$, which is impossible.

Thus $u - v \leq 1$. But u and v are both powers of 2 in the regular ball $B(x,k)$, which is impossible.

Thus $v = N = \min B(y,k)$.

(iii) Comes from (i) and (ii) by Proposition 5.6.

(iv) Since $B(x,k)$ is regular and $\exp_\infty(l)$ is a power of 2, Lemma 6.2 yields: $d(0, \exp_\infty(l)) + k - 1 \leq d(0,y) \leq d(0, \exp_\infty(l)) + k$. By Fact 2.10, $d(0, \exp_\infty(l)) = l + 1$, so $k + l \leq d(0,y) \leq k + l + 1$ $\square$

7 How to bound quantifiers

The following Proposition 7.1 encompasses the bounded Ehrenfeucht–Fraïssé game argument. It is implicit in Ferrante and Rackoff (1979) [6], more explicit in Lo (1988) [12], and fully stated in Michel (1992) [13]. It gives conditions that allow to reduce the satisfaction by a relational structure of a prenex sentence to the satisfaction by this relational structure of a sentence with bounded quantifiers.

Using Proposition 4.3 and 6.3, we prove in Proposition 7.2 and Lemma 7.3 that these conditions are fulfilled. Then Theorem 7.4 follows, on which

the decision procedure of Section 8 rests.

Proposition 7.1 *Let $\mathcal{A} = \langle A, R_1, \ldots, R_l \rangle$ be a structure, where $R_1, \ldots, R_l$ are relations on A.*

Let E_k^n, $n \in \mathbb{N}$, $k \in \mathbb{N} - \{0\}$, be a family of equivalence relations on A^k.

Let $\|\cdot\| : A \to \mathbb{N}$. If $x \in A$ and $m \in \mathbb{N}$, then $x \preceq m$ means that $\|x\| \leq m$.

Let $H : \mathbb{N}^3 \to \mathbb{N}$, and $\mu \in \mathbb{N}$.

Suppose that the following conditions holds:

(i) For all $k \in \mathbb{N} - \{0\}$, $m \geq \mu$, $\bar{a}_k, \bar{b}_k \in A^k$, if $\bar{a}_k E_k^{n+1} \bar{b}_k$ and, for all $i \in [1,k]$, $\|b_i\| \leq m$, then, for any $a_{k+1} \in A$, there is a $b_{k+1} \in A$ such that $\bar{a}_{k+1} E_{k+1}^n \bar{b}_{k+1}$ and $\|b_{k+1}\| \leq H(n,k,m)$.

(ii) For all $k \in \mathbb{N} - \{0\}$, $\bar{a}_k, \bar{b}_k \in A^k$, if $\bar{a}_k E_k^0 \bar{b}_k$, then $\bar{a}_k$ and $\bar{b}_k$ satisfy the same atomic formulas.

Let $k \in \mathbb{N} - \{0\}$, and let $(Q_1 x_1) \ldots (Q_k x_k) F(\bar{x}_k)$ be a sentence in prenex normal form, with $F(\bar{x}_k)$ quantifier-free.

Let $(m_0, m_1, \ldots, m_k) \in \mathbb{N}^{k+1}$ such that $\mu \leq m_0 \leq m_1 \leq \cdots \leq m_k$ and, for all $i \in [1,k]$, $m_i \geq H(k-i, i-1, m_{i-1})$. Then $\mathcal{A} \models (Q_1 x_1) \ldots (Q_k x_k) F(\bar{x}_k)$ if and only if $\mathcal{A} \models (Q_1 x_1 \preceq m_1) \ldots (Q_k x_k \preceq m_k) F(\bar{x}_k)$. □

We specify now the definitions of the relations E_k^n that we need here.

If $a, b, k \in \mathbb{N}$, such that $d(a,b) \leq k$, we denote by $N(a,b,k)$ the common neighborhood of a and b, that is, $N(a,b,k) = B(a,k) \cup B(b,k) = \{x \in \mathbb{N} : d(a,x) \leq k \text{ or } d(b,x) \leq k\}$.

When we write $\sigma : N(a,b,k) \cong N(a',b',k)$, we suppose that isomorphism σ, which is unique by Fact 2.6, satisfies $\sigma(a) = a'$ and $\sigma(b) = b'$.

Let $a_1, a_2, b_1, b_2 \in \mathbb{N}$ and $n \in \mathbb{N}$. We write $(a_1, a_2) \equiv_n (b_1, b_2)$ if

- either $d(a_1, a_2) > 2^n$ and $d(b_1, b_2) > 2^n$,
- or $d(a_1, a_2) = d(b_1, b_2) \leq 2^n$, and $N(a_1, a_2, 2^n) \cong N(b_1, b_2, 2^n)$.

Note that, if $(a_1, a_2) \equiv_n (b_1, b_2)$ and $m \leq n$, then $(a_1, a_2) \equiv_m (b_1, b_2)$.

Let $n, k \in \mathbb{N}$, $k \geq 1$ and $\bar{a}_k, \bar{b}_k \in \mathbb{N}^k$. Then $\bar{a}_k E_k^n \bar{b}_k$ if

(i) For all $i \in [1,k]$, $(0, a_i) \equiv_{n+2} (0, b_i)$.

(ii) For all $i \in [1,k]$, $B(a_i, 2^n) \cong B(b_i, 2^n)$.

(iii) For all $i, j \in [1, k]$, $i \neq j$ implies $(a_i, a_j) \equiv_n (b_i, b_j)$.

Note that, if $\bar{a}_k E_k^n \bar{b}_k$, then $(0, a_i) \equiv_2 (0, b_i)$, so $a_i = b_i$ if $d(0, a_i) \leq 4$.

If $x \in \mathbb{N}$, we define $\|x\| = d(0, x)$, and we denote $x \preceq k$ if $\|x\| \leq k$.

Proposition 7.2 *Let $k, n \in \mathbb{N}$, $k \geq 1$, $m \geq 1$, $\bar{a}_k, \bar{b}_k \in \mathbb{N}^k$, such that $\bar{a}_k E_k^{n+1} \bar{b}_k$ and, for all $i \in [1, k]$, $\|b_i\| = d(0, b_i) \leq m$, and let $a_{k+1} \in \mathbb{N}$.*

Then there exists $b_{k+1} \in \mathbb{N}$ such that $\bar{a}_{k+1} E_{k+1}^n \bar{b}_{k+1}$ and $\|b_{k+1}\| = d(0, b_{k+1}) \leq 2^{n+2} + m + 1$.

Proof. The hypothesis $\bar{a}_k E_k^{n+1} \bar{b}_k$ means that

(H1) For all $i \in [1, k]$, either $d(0, a_i) > 2^{n+3}$ and $d(0, b_i) > 2^{n+3}$, or $a_i = b_i$.

(H2) For all $i \in [1, k]$, $B(a_i, 2^{n+1}) \cong B(b_i, 2^{n+1})$.

(H3) For all $i, j \in [1, k]$, $i \neq j$, either $d(a_i, a_j) > 2^{n+1}$ and $d(b_i, b_j) > 2^{n+1}$, or $d(a_i, a_j) = d(b_i, b_j) \leq 2^{n+1}$ and $N(a_i, a_j, 2^{n+1}) \cong N(b_i, b_j, 2^{n+1})$.

Then a_{k+1} is given, and we are looking for b_{k+1} such that $\bar{a}_{k+1} E_{k+1}^n \bar{b}_{k+1}$, that is, such that (H1), (H2) and (H3) above are satisfied, and such that, moreover, we have

(C1) Either $d(0, a_{k+1}) > 2^{n+2}$ and $d(0, b_{k+1}) > 2^{n+2}$, or $a_{k+1} = b_{k+1}$.

(C2) $B(a_{k+1}, 2^n) \cong B(b_{k+1}, 2^n)$.

(C3) For all $i \in [1, k]$, either $d(a_i, a_{k+1}) > 2^n$ and $d(b_i, b_{k+1}) > 2^n$, or $d(a_i, a_{k+1}) = d(b_i, b_{k+1}) \leq 2^n$ and $N(a_i, a_{k+1}, 2^n) \cong N(b_i, b_{k+1}, 2^n)$.

Case 1: $d(0, a_{k+1}) \leq 2^{n+2}$.

Then we set $b_{k+1} = a_{k+1}$. Conditions (C1) and (C2) are satisfied. For Condition (C3), let $i \in [1, k]$.

Subcase 1.1: $d(0, a_i) \leq 2^{n+3}$.

Then, by (H1), $b_i = a_i$, so Condition (C3) is satisfied.

Subcase 1.2: $d(0, a_i) > 2^{n+3}$.

Then, by (H1), $d(0, b_i) > 2^{n+3}$. We show that $d(a_i, a_{k+1}) > 2^n$ and $d(b_i, b_{k+1}) > 2^n$.

We have $d(a_i, a_{k+1}) \geq d(0, a_i) - d(0, a_{k+1}) > 2^{n+3} - 2^{n+2} > 2^n$, and $d(b_i, b_{k+1}) \geq d(0, b_i) - d(0, b_{k+1}) = d(0, b_i) - d(0, a_{k+1}) > 2^{n+3} - 2^{n+2} = 2^{n+1} > 2^n$.

Case 2: $d(0, a_{k+1}) > 2^{n+2}$ and there is an $h \in [1, k]$ such that $a_{k+1} \in B(a_h, 2^n)$.

Then, by (H2), there is an isomorphism $\sigma : B(a_h, 2^{n+1}) \to B(b_h, 2^{n+1})$, and we set $b_{k+1} = \sigma(a_{k+1})$.

Condition (C1) is satisfied, that is $d(0, b_{k+1}) > 2^{n+2}$, because, otherwise, if $d(0, b_{k+1}) \leq 2^{n+2}$, we get $d(0, b_h) \leq d(0, b_{k+1}) + d(b_{k+1}, b_h) \leq 2^{n+2} + 2^n \leq 2^{n+3}$, so by (H1), $a_h = b_h$, and by Fact 2.5, σ is the identity on $B(a_h, 2^{n+1})$. Thus $b_{k+1} = a_{k+1}$, and $d(0, a_{k+1}) \leq 2^{n+2}$, contradicting the hypothesis.

To show Condition (C2), we want an isomorphism $\tau : B(a_{k+1}, 2^n) \to B(b_{k+1}, 2^n)$. We set $\tau = \sigma|_{B(a_{k+1}, 2^n)}$, which is defined because $B(a_{k+1}, 2^n) \subseteq B(a_h, 2^{n+1})$.

For Condition (C3), let $i \in [1, k]$. If $i = h$, then $\sigma|_{N(a_h, a_{k+1}, 2^n)}$ is an isomorphism from $N(a_h, a_{k+1}, 2^n)$ to $N(b_h, b_{k+1}, 2^n)$.

Suppose $i \neq h$.

Subcase 2.1: $d(a_i, a_h) > 2^{n+1}$.

Then, by (H3), $d(b_i, b_h) > 2^{n+1}$, so $d(a_i, a_{k+1}) \geq d(a_i, a_h) - d(a_h, a_{k+1}) > 2^{n+1} - 2^n = 2^n$, and $d(b_i, b_{k+1}) \geq d(b_i, b_h) - d(b_h, b_{k+1}) > 2^{n+1} - 2^n = 2^n$. Condition (C3) is satisfied.

Subcase 2.2: $d(a_i, a_h) \leq 2^{n+1}$.

Then, by (H3), $d(b_i, b_h) \leq 2^{n+1}$ and there is an isomorphism τ from $N(a_i, a_h, 2^{n+1})$ to $N(b_i, b_h, 2^{n+1})$. Now, $\tau|_{B(a_h, 2^{n+1})}$ is an isomorphism from $B(a_h, 2^{n+1})$ to $B(b_h, 2^{n+1})$, so by Fact 2.6, $\tau|_{B(a_h, 2^{n+1})} = \sigma$. Isomorphism τ is an extension of σ. In particular, $\tau(a_{k+1}) = b_{k+1}$. Isomorphism τ preserves distances, so $d(a_i, a_{k+1}) = d(b_i, b_{k+1})$. Then either $d(a_i, a_{k+1}) = d(b_i, b_{k+1}) > 2^{k+1}$, or $d(a_i, a_{k+1}) = d(b_i, b_{k+1}) \leq 2^{k+1}$, and $\tau|_{N(a_i, a_{k+1}, 2^n)}$ is an isomorphism from $N(a_i, a_{k+1}, 2^n)$ into $N(b_i, b_{k+1}, 2^n)$, so Condition (C3) is satisfied.

Case 3: $d(0, a_{k+1}) > 2^{n+2}$ and for all $i \in [1, k]$, $d(a_i, a_{k+1}) > 2^n$.

This is the most difficult case, for which the machinery of the previous sections was developed. We have $d(0, a_{k+1}) \geq 2^{n+2} + 1 \geq 2.2^n + 2$, so, by Proposition 4.3, $B(a_{k+1}, 2^n)$ is a regular ball. Let $M = \min B(a_{k+1}, 2^n)$, and let $\bar{f}_{2^n}$ be defined by $\bar{f}_{2^n}(M) = a_{k+1}$. We set $b_{k+1} = \bar{f}_{2^n}(\exp_\infty(m + 3.2^n))$. We have $m + 3.2^n \geq 3.2^n + 1$ because $m \geq 1$, so the hypotheses of Proposition 6.3 are satisfied. Thus, we get $B(a_{k+1}, 2^n) \cong B(b_{k+1}, 2^n)$, and $2^n + m + 3.2^n \leq d(0, b_{k+1}) \leq 2^n + m + 3.2^n + 1$, that is $2^{n+2} + m \leq d(0, b_{k+1}) \leq 2^{n+2} + m + 1$.

Then Conditions (C1) and (C2) are satisfied, and Condition (C3) is satisfied because $d(b_i, b_{k+1}) > 2^n$, since otherwise $2^{n+2} + m \leq d(0, b_{k+1}) \leq d(0, b_i) + d(b_i, b_{k+1}) \leq m + 2^n$, which cannot holds.

Upper bound on $\|b_{k+1}\|$:

Case 1: $d(0, b_{k+1}) \leq 2^{n+2}$.

Case 2: we have $d(b_k, b_{k+1}) \leq 2^n$, so $d(0, b_{k+1}) \leq d(0, b_k) + d(b_k, b_{k+1}) \leq m + 2^n$.

Case 3: $d(0, b_{k+1}) \leq 2^{n+2} + m + 1$.

In all cases, we get $\|b_{k+1}\| = d(0, b_{k+1}) \leq 2^{n+2} + m + 1$. □

Lemma 7.3 *Let $\bar{a}_k, \bar{b}_k \in \mathbb{N}$ ($k \geq 1$). If $\bar{a}_k E_k^0 \bar{b}_k$, then $\bar{a}_k$ and $\bar{b}_k$ satisfy the same atomic formulas.*

Proof. By definition of E_k^0, if $\bar{a}_k E_k^0 \bar{b}_k$, we have:

(i) For all $i \in [1, k]$, $(0, a_i) \equiv_2 (0, b_i)$, that is, either $d(0, a_i) > 4$ and $d(0, b_i) > 4$, or $a_i = b_i$.

(ii) For all $i \in [1, k]$, $B(a_i, 1) \cong B(b_i, 1)$.

(iii) For all $i, j \in [1, k]$, $i \neq j$, we have $(a_i, a_j) \equiv_0 (b_i, b_j)$, that is, either $d(a_i, a_j) > 1$ and $d(b_i, b_j) > 1$, or $d(a_i, a_j) = d(b_i, b_j) = 1$ and $N(a_i, a_j, 1) \cong N(b_i, b_j, 1)$.

Thus, if $a_i = a_j$, then $b_i = b_j$, and if $R(a_i, a_j)$, with $R \in \{R_S, R_P\}$, then $d(a_i, a_j) = 1$, so $d(b_i, b_j) = 1$ and $N(a_i, a_j, 1) \cong N(b_i, b_j, 1)$, so we have $R(b_i, b_j)$. □

Theorem 7.4 *Let $(Q_1 x_1) \dots (Q_k x_k) F(\bar{x}_k)$ be a sentence in prenex normal form over the vocabulary $\{=, R_S, R_P\}$, with $F(\bar{x}_k)$ quantifier-free. For all $i \in [1, k]$, let $m_i = 2^{k+2} - 2^{k-i+2} + i + 1$.*

Then

$$\langle \mathbb{N}, =, R_S, R_P \rangle \models (Q_1 x_1) \dots (Q_k x_k) F(\bar{x}_k)$$

if and only if

$$\langle \mathbb{N}, =, R_S, R_P \rangle \models (Q_1 x_1 \preceq m_1) \dots (Q_k x_k \preceq m_k) F(\bar{x}_k).$$

Proof. By Proposition 7.2 and Lemma 7.3, the hypotheses of Proposition 7.1 are satisfied, with $\|b\| = d(0, b)$, $\mu = 1$, $H(n, k, m) = 2^{n+2} + m + 1$. We set $m_0 = \mu = 1$, and for $i \in [1, k]$, $m_i = H(k - i, i - 1, m_{i-1})$. By induction on i, we get easily $m_i = 2^{k+2} - 2^{k-i+2} + i + 1$. □

8 The decision procedure

We saw in the previous section that Proposition 7.1 applies to relational structures, and Theorem 7.4 applies to sentences in prenex normal form. Thus, first we have to transform an arbitrary sentence over a functional vocabulary into a sentence in prenex normal form over a relational vocabulary. This transformation will increase the length polynomially, so using a reduction, such as polynomial time many-one reduction for example, would waste precision. It is better to insert this transformation at the beginning of the decision procedure. So we present this transformation in the following form, which may have an independent interest.

Proposition 8.1 *There exists a function Ψ, computable in deterministic polynomial time, which, on a sentence ϕ on the vocabulary $\{=, f_1, \ldots, f_k\}$, where $f_1, \ldots, f_k$ are symbols for unary functions, returns a sentence $\Psi(\phi)$ on the vocabulary $\{=, R_1, \ldots, R_k\}$, where $R_1, \ldots, R_k$ are symbols for binary relations, and which verifies the following conditions.*

(i) *$\Psi(\phi)$ is in prenex normal form.*

(ii) *$\Psi(\phi)$ has at most $2|\phi|$ quantifiers.*

(iii) *$\Psi(\phi)$ has at most $|\phi|$ quantifiers alternations.*

(iv) *If f_i is interpretated by $\tilde{f}_i : \mathbb{N} \to \mathbb{N}$, and R_i by $\tilde{R}_i \subseteq \mathbb{N} \times \mathbb{N}$, such that, for all $i \in [1, k]$ and all $a, b \in \mathbb{N}$, $\tilde{f}_i(a) = b$ if and only if $\tilde{R}_i(a, b)$, then $\langle \mathbb{N}, =, \tilde{f}_1, \ldots, \tilde{f}_k \rangle \models \phi$ if and only if $\langle \mathbb{N}, =, \tilde{R}_1, \ldots, \tilde{R}_k \rangle \models \Psi(\phi)$.*

Proof. The standard way to convert a sentence ϕ into prenex normal form consists in moving quantifiers to the beginning of the sentence after renaming variables. Ferrante and Rackoff (1979) [6], page 23, show that this routine takes polynomial time, leaves unchanged the number of quantifiers, and yields a sentence ϕ_1 of length $O(|\phi| \log |\phi|)$. We need to make precise what happens.

Let q be the number of quantifiers in ϕ, and let r be the number of occurrences of a functional symbol $f_1, \ldots,$ or f_k in ϕ . Then we have $q + r \leq |\phi|$. The sentence ϕ_1 obtained by the standard transformation has same number q of quantifiers, and same number r of functional symbols as ϕ. Let $\phi_1 = (Q_1 x_1) \ldots (Q_q x_q) F_1(\bar{x}_q)$, in prenex normal form, $F_1(\bar{x}_q)$ being quantifier-free. The number of quantifiers alternations in ϕ_1 is at most $\max(0, q - 1)$.

Then, we eliminate one by one the occurrences of a functional symbol f_i in $F_1(\bar{x}_q)$, by replacing them by R_i, according to the following recursive procedure.

If x, x' are already existing variables, t_1, t_2 are terms that are not variables, and y, y' are new variables, then

(a) $x' = f_i(x)$ and $f_i(x) = x'$ are replaced by $R_i(x, x')$,

(b) $x = f_i(t_1)$ and $f_i(t_1) = x$ are replaced by $(\exists y)(y = t_1 \wedge R_i(y, x))$,

(c) $t_1 = f_i(x)$ and $f_i(x) = t_1$ are replaced by $(\exists y)(y = t_1 \wedge R_i(x, y))$,

(d) $t_2 = f_i(t_1)$ and $f_i(t_1) = t_2$ are replaced by $(\exists y)(\exists y')(y = t_1 \wedge y' = t_2 \wedge R_i(y, y'))$.

Each replacement increases the length of the sentence by a constant, plus the length of new variables. There are r replacements, so the number of added quantifiers is at most $2r$, and the new variables are at most $x_{q+1}, \ldots, x_{q+2r}$. Each replacement is made in linear time, so r replacements are made in polynomial time.

Let $\phi_2 = (Q_1 x_1) \ldots (Q_q x_q) F_2(\bar{x}_q)$ be the sentence obtained after the r replacements. Let us transform $F_2(\bar{x}_q)$ in prenex normal form. We do not need to rename variables $x_{q+1}, \ldots, x_{q+2r}$, because each of them appears only once. Moreover, in formula $F_2(\bar{x}_q)$, quantifiers coming from distinct atomic formulas (that is formulas $t_1 = t_2$, where t_1 and t_2 are terms) are independent from each others, and those coming from the same atomic formula are existential ones, so all these quantifiers can be put together in the end of the prefix:

- as $(\exists u_1) \ldots (\exists u_l)(\forall v_1) \ldots (\forall v_m)$ if $Q_q = \exists$,
- as $(\forall v_1) \ldots (\forall v_m)(\exists u_1) \ldots (\exists u_l)$ if $Q_q = \forall$.

Then only one quantifiers alternation is added.

The achieved sentence $\Psi(\phi)$ satisfies the conditions of the proposition. It has at most $q+2r \leq 2(q+r) \leq 2|\phi|$ quantifiers, and at most $\max(0, q-1)+1 = \max(1, q) \leq |\phi|$ quantifiers alternations. Note that $|\Psi(\phi)| = O(|\phi|(\log |\phi|)^2)$, but we do not need this result. $\square$

Lemma 8.2 *Let $x \in \mathbb{N}$, and let $\bar{f}_n$ be an n-tuple of functions associated to a shortest path from 0 to x. Then $\bar{f}_n \in \{S, S^{-1}, P\}^n$, that is no f_i is a P^{-1}.*

Proof. The lemma is proved by induction on $n = d(0, x)$. If $n = 1$, then $x = S(0)$ or $x = P(0)$. Suppose the lemma proved for all $u \in \mathbb{N}$ such that $d(0, u) \leq n - 1$, and let $x \in \mathbb{N}$ such that $d(0, x) = n$. Let C be a shortest path of length n from 0 to x and let $\bar{f}_n$ be an n-tuple of functions associated to C. By Lemma 5.1, three cases can occur.

Case 1: C is an s-path, that is $C = [0, x]$. Then $\bar{f}_n = S^n \in \{S, S^{-1}, P\}^n$.

Case 2: C is a t-path, that is, if $2^t \leq x < 2^{t+1}$, C is made of a shortest path C' from 0 to t, followed by $[2^t, x]$. If $k = d(0, t)$, then $\bar{f}_k$ is a k-tuple of functions associated to C', and $k < n$, so, by induction hypothesis, $\bar{f}_k \in \{S, S^{-1}, P\}^k$. Then $\bar{f}_n = S^{x-2t} \circ P \circ \bar{f}_k$, so $\bar{f}_n \in \{S, S^{-1}, P\}^n$.

Case 3: C is a $t + 1$-path, that is, if $2^t \leq x < 2^{t+1}$, C is made of a shortest path C' from 0 to $t + 1$, followed by $[x, 2^{t+1}]$, covered from 2^{t+1} to x. If $k = d(0, t + 1)$, then $\bar{f}_k$ is a k-tuple of functions associated to C', and $k < n$, so, by induction hypothesis, $\bar{f}_k \in \{S, S^{-1}, P\}^k$. Then $\bar{f}_n = (S^{-1})^{2^{t+1}-x} \circ P \circ \bar{f}_k$, so $\bar{f}_n \in \{S, S^{-1}, P\}^n$. □

Note that, in the previous lemma, there can be more than one shortest paths from 0 to x, and more than one n-tuples of functions associated to the same shortest path from 0 to x.

Proposition 8.3 *Deciding, on input* $\bar{f}_p = S^{n_h} \circ P \circ S^{n_{h-1}} \circ P \circ \cdots \circ S^{n_1} \circ P \circ S^{n_0}$, *with* $n_0, \ldots, n_h \in \mathbb{Z}$, *whether* $\bar{f}_p(0)$ *is defined, can be done in deterministic time polynomial in* $\log p$.

Proof. Let

$$\bar{f}_p = S^{n_h} \circ P \circ S^{n_{h-1}} \circ P \circ \cdots \circ S^{n_1} \circ P \circ S^{n_0},$$

with $n_0, \ldots n_h \in \mathbb{Z}$, and the conventions: $S^n = (S^{-1})^{-n}$ if $n < 0$, and $S^0 =$ Id. Because $\bar{f}_p$ contains no P^{-1}, $\bar{f}_p(0)$ is defined if and only if, for all $i \in [1, p]$, $\bar{f}_i(0) \geq 0$. Let $u_0 = S^{n_0}(0)$ and, for all $j \in [1, h]$, $u_j = S^{n_j} \circ P(u_{j-1}) = n_j + 2^{u_{j-1}}$. Then u_j is defined if and only if u_{j-1} is defined and $u_j \geq 0$. We have $p = h + \sum_{j=0}^{h} |n_j|$, so, for all $j \in [0, h]$, $n_j \geq -p$. Note that, for all integers $x \geq 1$, we have $2^{(\log x)^2+1} \geq x + (\log x)^2 + 1$, so, if $u_{j-1} \geq (\log p)^2 + 1$, then $u_j = n_j + 2^{u_{j-1}} \geq n_j + 2^{(\log p)^2+1} \geq n_j + p + (\log p)^2 + 1 \geq (\log p)^2 + 1$, and, in particular, u_j is defined because it is positive.

Thus, we get the following procedure to verify that $\bar{f}_p(0)$ is defined: compute $u_0, u_1, \ldots$, until we reach one of the three following cases:

(i) $u_j < 0$: return $\bar{f}_p(0)$ undefined.

(ii) $u_j \geq (\log p)^2 + 1$: return $\bar{f}_p(0)$ defined.

(iii) $j = h$ and $u_h \geq 0$: return $\bar{f}_p(0)$ defined.

In these computations, numbers are less than $p + 2^{(\log p)^2} = 2^{O((\log p)^2)}$, so they have a length polynomial in $\log p$. Thus, these computations are done in time polynomial in $\log p$. $\square$

The following proposition clears up a surprising fact: even if terms with stacks of Ps appear in the sentence to be decided, leading to threateningly high numbers, only small numbers have to be handled during the decision procedure.

Proposition 8.4 *Let $n \in \mathbb{N} - \{0\}$, and let $\bar{f}_n$ be an n-tuple of functions, such that:*

(i) For all $i \in [1, n-1]$, $f_{i+1} \neq f_i^{-1}$.

(ii) $\bar{f}_n(0) = 0$.

Then, for all $i \in [1, n]$, $\bar{f}_i(0) \leq 2n$.

Proof. No n-tuple $\bar{f}_n$ satisfies Hypotheses (i) and (ii) for $n = 1$ and $n = 3$, and the 2-tuples (S, P^{-1}) and (P, S^{-1}) that satisfy these hypotheses also satisfy the conclusion. So, from now on, we suppose $n \geq 4$.

Let $m \in [1, n]$ such that $\bar{f}_m(0) = \max\{\bar{f}_i(0) : i \in [1, n]\}$. We have to prove that $\bar{f}_m(0) \leq 2n$. If $\bar{f}_m(0) \leq 8$, then $\bar{f}_m(0) \leq 8 \leq 2n$, because $n \geq 4$. So we can suppose $\bar{f}_m(0) > 8$. Moreover, if $k \leq 3$, then $\bar{f}_k(0)$ and $\bar{f}_{n-k}(0)$ are in $\{0, 1, 2, 3, 4\}$, so we have $4 \leq m \leq n - 4$ and $n \geq 8$.

By definition of m, we have $f_m \in \{S, P\}$ and $f_{m+1} \in \{S^{-1}, P^{-1}\}$. So, by Hypothesis (i), $(f_m, f_{m+1}) = (S, P^{-1})$ or $(f_m, f_{m+1}) = (P, S^{-1})$. In the second case, we can consider the n-tuple $\bar{f}_n^{-1}$, which satisfies the same hypotheses as $\bar{f}_n$. So, from now on, we suppose $f_m = S$ and $f_{m+1} = P^{-1}$.

Let $x = \bar{f}_m(0)$. Since $\bar{f}_{m-1}(0) = x - 1$ and $\bar{f}_{m+1}(0) = \log x$, we know that x is a power of 2. But $x = \bar{f}_m(0) > 8$, so $x \geq 16$, and $\log x \geq 4$. We have to prove that $x \leq 2n$.

The set $\{j \in [1, m] : (\forall i \in [j, m]) f_i = S\}$ contains m, so is not empty. Let l be its minimum. If $l = 1$, then $\bar{f}_m(0) = S^m(0) = m \leq n - 4 \leq 2n$. If $l = 2$, then $\bar{f}_m(0) = S^{m-1} \circ P(0) = m \leq 2n$. Thus, from now on, we suppose $l \geq 3$.

We have $x = \bar{f}_{l-1}(0) + m - l + 1$. If $\bar{f}_{l-1}(0) \leq 1$, then $x \leq m - l + 2 \leq m - 1 \leq n - 5 \leq 2n$, so, from now on, we suppose $\bar{f}_{l-1}(0) \geq 2$.

Case 1: $\bar{f}_{l-1}(0) \leq \bar{f}_{m+1}(0) = \log x$.

Then there exists $k \in [l-1, m-1]$ such that $\bar{f}_k(0) = \log x$, and so $\bar{f}_k(0) = \log x, \log x + 1, \ldots, x - 1, x, \log x = \bar{f}_{m+1}(0)$ is a cycle of length $x - \log x + 1$. So $x - \log x + 1 \leq n$, and $x \leq 2(x - \log x + 1) \leq 2n$.

Case 2: $\bar{f}_{l-1}(0) > \bar{f}_{m+1}(0) = \log x$.

Since $f_l = S$, we have $f_{l-1} \neq S^{-1}$ by Hypothesis (i), $f_{l-1} \neq S$ by definition of l, and $f_{l-1} \neq P^{-1}$, because otherwise $\bar{f}_{l-2}(0) = 2^{\bar{f}_{l-1}(0)} > 2^{\bar{f}_{m+1}(0)} = \bar{f}_m(0)$, contradicting the definition of m.

Thus, $f_{l-1} = P$, and $\bar{f}_{l-2}(0) = \log \bar{f}_{l-1}(0), \bar{f}_{l-1}(0), \bar{f}_{l-1}(0) + 1, \ldots, \bar{f}_m(0), \bar{f}_{m+1}(0) = \log x$ is a path of length $x - \bar{f}_{l-1}(0) + 2$. So $x - \bar{f}_{l-1}(0) + 2 \leq n$. But $\bar{f}_{l-2}(0) = \log \bar{f}_{l-1}(0) \leq \log x - 1$, so $\bar{f}_{l-1}(0) \leq 2^{\log x - 1} = x/2$, and $x/2 = x - x/2 \leq x - \bar{f}_{l-1}(0) \leq x - \bar{f}_{l-1}(0) + 2 \leq n$, so we have $x \leq 2n$. □

Theorem 8.5 $\mathrm{Th}(\mathbb{N}, =, S, P) \in \mathrm{ATIME\text{-}ALT}(2^{O(n)}, n)$.

Proof. Let ϕ be a sentence of length n over the vocabulary $\{=, S, P\}$. By Proposition 8.1, ϕ can be transformed, in deterministic polynomial time, into a sentence $(Q_1 x_1) \ldots (Q_k x_k) F(\bar{x}_k)$ over the vocabulary $\{=, R_S, R_P\}$, such that $F(\bar{x}_k)$ is quantifier-free, $k \leq 2n$, $|F(\bar{x}_k)| \leq s(n)$ for a polynomial s, and there is at most n alternations of quantifiers.

By Theorem 7.4,

$$\langle \mathbb{N}, =, R_S, R_P \rangle \models (Q_1 x_1) \ldots (Q_k x_k) F(\bar{x}_k)$$

if and only if

$$\langle \mathbb{N}, =, R_S, R_P \rangle \models (Q_1 x_1 \preceq m_1) \ldots (Q_k x_k \preceq m_k) F(\bar{x}_k),$$

where $m_i = 2^{k+2} - 2^{k-i+2} + i + 1 \leq m_k = 2^{O(n)}$.

We need a procedure which produces numbers $a_i \preceq m_i$, for all $i \in [1, k]$, existentially if $Q_i = \exists$, universally if $Q_i = \forall$, and then decides $F(\bar{a}_k)$.

Numbers $a_i \preceq m_i$ are produced by writing them as $a_i = \bar{f}_p(0)$, for a p-tuple $\bar{f}_p$ of functions, with $p \leq m_i$. By Lemma 8.2, $\bar{f}_p$ can be chosen to be in the form

$$\bar{f}_p = S^{n_h} \circ P \circ S^{n_{h-1}} \circ P \circ \cdots \circ S^{n_1} \circ P \circ S^{n_0},$$

with $n_0, \dots n_h \in \mathbb{Z}$, and the conventions: $S^n = (S^{-1})^{-n}$ if $n < 0$, and $S^0 =$ Id.

By Proposition 8.3, we can verify that $\bar{f}_p(0)$ is defined in deterministic time polynomial in $\log p$. Since $p \leq m_k = 2^{O(n)}$, this verification is polynomial in n.

When we get $\bar{a}_k \in \mathbb{N}$ such that, for all $i \in [1,k]$, $a_i \preceq m_i$, we need a procedure to decide $F(\bar{a}_k)$, which is a Boolean formula over the atomic formulas $R_S(a_i, a_j)$, $R_P(a_i, a_j)$ and $a_i = a_j$. Let $\bar{f}_p$, $\bar{g}_q$ be tuples of functions such that $a_i = \bar{f}_p(0)$, $a_j = \bar{g}_q(0)$, and $p \leq m_i$, $q \leq m_j$. The atomic formulas above can be written respectively: $\bar{g}_q(0) = S \circ \bar{f}_p(0)$, $\bar{g}_q(0) = P \circ \bar{f}_p(0)$ and $\bar{g}_q(0) = \bar{f}_p(0)$, which can also be written $\bar{f}_p^{-1} \circ S^{-1} \circ \bar{g}_q(0) = 0$, $\bar{f}_p^{-1} \circ P^{-1} \circ \bar{g}_q(0) = 0$, $\bar{f}_p^{-1} \circ \bar{g}_q(0) = 0$. The occurrences of two consecutive functions inverse of each other can be cancelled, so we have to decide $\bar{h}_r(0) = 0$, with, for all $i \in \mathbb{N}$, $h_{i+1} \neq h_i^{-1}$, and $r \leq p + q + 1 \leq m_i + m_j + 1 \leq 2m_k + 1$. If this formula is true, then the hypotheses of Proposition 8.4 are satisfied, so, for all $i \in [1,r]$, $\bar{h}_i(0) \leq 2r \leq 4m_k + 2$. Thus, when $\bar{h}_1(0), \dots, \bar{h}_r(0)$ are computed, if one of these numbers exceeds $4m_k + 2$, we can stop the computation and be sure that $\bar{h}_r(0) = 0$ is false. Hence the following decision procedure.

Decision procedure:

1. Write a tuple $\bar{f}_{p_i} \in \{S, S^{-1}, P\}^{p_i}$ of length $p_i \leq m_i$, for all $i \in [1,k]$,

   - in an existential state if $Q_i = \exists$,
   - in a universal state if $Q_i = \forall$.

   Verify that $\bar{f}_{p_i}(0)$ is defined. If $\bar{f}_{p_i}(0)$ is undefined, stops in a rejecting state if $Q_i = \exists$ and in an accepting state if $Q_i = \forall$, in order to discard this computation branch.

   We get $a_i \in \mathbb{N}$, written as $\bar{f}_{p_i}(0)$, such that $\|a_i\| \leq m_i$ for all $i \in [1,k]$.

2. Consider $F(\bar{a}_k)$. This is a Boolean formula over atomic formulas $R_S(a_i, a_j)$, $R_P(a_i, a_j)$, $a_i = a_j$. Write each atomic formula as $\bar{h}_r(0) = 0$, with, for all $i \in [1, r-1]$, $h_{i+1} \neq h_i^{-1}$, and $r \leq 2m_k + 1$.

3. For each formula $\bar{h}_r(0) = 0$, compute $\bar{h}_1(0), \bar{h}_2(0), \dots$, and:

   - If one of these numbers is undefined, because it is negative or logarithm of a number which is not a power of 2, stop computing them and return: $\bar{h}_r(0) = 0$ false.

- If one of these numbers exceeds $4m_k + 2$, stop computing them and return: $\bar{h}_r(0) = 0$ false.
- Else, compute $\bar{h}_r(0)$ and return the truth value of $\bar{h}_r(0) = 0$.

4. Compute the truth value of the Boolean formula $F(\bar{a}_k)$.

Computing time:

(a) Time to write $a_i = \bar{f}_{p_i}(0)$ for all $i \in [1, k]$.

We have $p_i \leq m_i \leq m_k = 2^{O(n)}$, and we can verified that $\bar{f}_p(0)$ is defined in deterministic polynomial time so the total time is $2^{O(n)}$.

(b) Time to compute the truth value of an atomic formula $\bar{h}_r(0) = 0$.

Computations are done on numbers at most $4m_k + 2 = 2^{O(n)}$, thus in time polynomial in $O(n)$, and there are at most $r \leq 2m_k + 1 = 2^{O(n)}$ such computations, so the total time is $n^{O(1)}2^{O(n)} = 2^{O(n)}$.

(c) Time to compute the truth value of $F(\bar{a}_k)$.

Writing an atomic formula as $\bar{h}_r(0) = 0$ is done in time $O(2^{O(n)}) = 2^{O(n)}$. There are at most $s(n)$ atomic formulas. When the truth values of all atomic formulas are known, the truth value of $F(\bar{a}_k)$ can be computed in time $q(n)$, for a polynomial q.

Thus the total time is $2^{O(n)}$.

Alternations of existential and universal states are used only according to alternations of quantifiers Q_i, and there are at most n such alternations. So $\mathrm{Th}(\mathbb{N}, =, S, P) \in \text{ATIME-ALT}(2^{O(n)}, n)$. $\square$

9 Extension to other functions

Theorem 8.5, that is, $\mathrm{Th}(\mathbb{N}, =, S, P) \in \text{ATIME-ALT}(2^{O(n)}, n)$, and its proof can be extended to other functions than $P(x) = 2^x$.

9.1 Extension to $\mathbf{Th}(\mathbb{N}, =, x + 1, c^x)$

We did not directly study the structures $\langle \mathbb{N}, =, x + 1, c^x \rangle$, with $c \in \mathbb{N}$, $c \geq 2$, because it would have added, to an already burdensome proof, another parameter, and discussions according to this parameter.

But it is easy to extend the results from Sections 2–8 to these structures. Facts 2.1, 2.3 and 2.8 must be adapted. For Fact 2.10, we define $\exp_\infty(k+1) = c^{\exp_\infty(k)}$. Statements remain true, 2^x being replaced by c^x, and proofs are easily modified, for example by replacing base two logarithms by base c logarithms.

9.2 Extension to Th$(\mathbb{N}, =, x+1, x^c)$

The statements of facts, lemmas, propositions and theorems in Sections 2–8 remain true for the structure $\langle \mathbb{N}, =, x+1, x^c \rangle$, with $c \in \mathbb{N}$, $c \geq 2$, 2^x being replaced by x^c, with the following exceptions.

- Facts 2.1 and 2.3 must be adapted, which can be done easily.
- In Fact 2.9, $d(0,x) \geq 1 + \log_\infty(x)$ for all $x \geq 2$ must be replaced by $d(0,x) \geq c + \log_c \log_c x$ for all $x \geq c$.
- In Fact 2.10, $d(0, \exp_\infty(n)) = n+1$ for all $n \in \mathbb{N}$ must be replaced by $d(0, (c+1)^{c^{n-c}}) = n+1$ for all $n \geq c$.
- In Lemma 4.1, the better hypothesis $n \geq 5$ can be taken.
- In Lemma 6.2, the hypothesis "m is a power of 2" must be replaced by "m is a cth power".
- In Proposition 6.3, $\exp_\infty(l)$ must be replaced by $(c+1)^{c^{l-c}}$.
- In Proposition 8.4, the upper bound $\bar{f}_i(0) \leq 2n$ is false and must be replaced by the weaker one $\bar{f}_i(0) \leq ((n-1)/2)^c$.

The proofs of the results from Sections 4–8 can be adapted easily, the main differences being handling small numbers and the following special cases.

- The proof of Proposition 8.3 is modified as follows. Because $(x+1)^c \geq 2x+1$, we have, if $u_{j-1} \geq p+1$, then $u_j = n_j + u_{j-1}^c \geq n_j + (p+1)^c \geq n_j + 2p + 1 \geq p+1$, so $u_0, u_1, \ldots$ are computed until $u_j \geq p+1$. In these computations, numbers are less than $p + p^c$, so their lengths are $O(\log p)$, and the time is polynomial in $\log p$.
- In the proof of Theorem 8.5, when Proposition 8.4 is used, the bound $\bar{h}_i(0) \leq 2r \leq 4m_k + 2$ is replaced by the weaker bound $\bar{h}_i(0) \leq ((r-1)/2)^c \leq m_k^c$. But $m_k = 2^{O(n)}$, so we still get $m_k^c = 2^{O(n)}$.

9.3 Extension to $\mathbf{Th}(\mathbb{N}, =, x+1, \exp_\infty(x))$

The statements of the results from Sections 4–8 remain true for the structure $\langle \mathbb{N}, =, x+1, \exp_\infty(x)\rangle$, 2^x being replaced by $\exp_\infty(x)$, with the following exceptions.

- Fact 2.3 can be adapted easily.
- We define $\exp^*_\infty$ by $\exp^*_\infty(0) = 1$ and $\exp^*_\infty(n+1) = \exp_\infty(\exp^*_\infty(n))$, and we define $\log^*_\infty(n) = \min\{k \in \mathbb{N} : \exp^*_\infty(k) \geq n\}$. Then we replace $\log_\infty(x)$ by $\log^*_\infty(x)$ in Fact 2.9, and $\exp_\infty(n)$ by $\exp^*_\infty(n)$ in Fact 2.10.
- In Lemma 4.1, the better hypothesis $n \geq 5$ can be taken.
- In Lemma 6.2, the hypothesis "m is a power of 2" must be replaced by "m is a tower of powers of 2".
- In Lemma 6.3, $\exp_\infty(l)$ must be replaced by $\exp^*_\infty(l)$.

The proofs of the results from Sections 4–8 can be adapted easily. The proof of Proposition 8.3 is modified as follows. Because, for all $x \geq 0$, $\exp_\infty(\log_\infty(x)+1) \geq x + \log_\infty(x) + 1$, we have, if $u_{j-1} \geq \log_\infty(p)+1$, then $u_j = n_j + \exp_\infty(u_{j-1}) \geq n_j + \exp_\infty(\log_\infty(p)+1) \geq n_j + p + \log_\infty(p) + 1 \geq \log_\infty(p) + 1$, so $u_0, u_1, \ldots$ are computed until $u_j \geq \log_\infty(p)+1$. In these computations, numbers are less than $p + \exp_\infty(\log_\infty(p))$, but $\exp_\infty(\log_\infty(p))$ can be as large as 2^{p-1}, so a predefined bound on computation time must be set in order to keep it polynomial in $\log p$.

10 Lower bound of complexity

We give a lower bound that matches the upper bound ATIME-ALT$(2^{O(n)}, O(n))$, by proving that $\mathrm{Th}(\mathbb{N}, =, x+1, F(x))$ is complete for this complexity class, when $F(x) = c^x$, x^c or $\exp_\infty(x)$. This is proved in a standard way by defining within $\langle \mathbb{N}, =, x+1, F(x)\rangle$ a structure the theory of which is complete for this class.

Consider the *binary tree with two successors* $\langle \{0,1\}^*, =, s_0, s_1\rangle$, where $\{0,1\}^*$ is the set of words on alphabet $\{0,1\}$ and, for all $u \in \{0,1\}^*$, $s_0(u) = u0$, $s_1(u) = u1$. It is known that $\mathrm{Th}(\{0,1\}^*, =, s_0, s_1)$ is complete for ATIME-ALT$(2^{O(n)}, O(n))$. This was proved by Volger (1983) [17] for the

polynomial time reduction and by Compton and Henson (1990) [3] for the reset log-lin reduction. We define functions r_0 and r_1 on $\mathbb{N} \times \{0,1\}^*$ by $r_i(n,u) = (n, s_i(u))$, for $i \in \{0,1\}$, $n \in \mathbb{N}$ and $u \in \{0,1\}^*$. In the following proposition, we prove that a structure isomorphic to $\langle \mathbb{N} \times \{0,1\}^*, =, r_0, r_1 \rangle$ can be defined within $\langle \mathbb{N}, =, x+1, F(x) \rangle$, which yields the required lower bound.

Proposition 10.1 *Let $F(x) = c^x$, x^c or $\exp_\infty(x)$ ($c \geq 2$). Functions S_0, S_1 can be defined in $\langle \mathbb{N}, =, x+1, F(x) \rangle$ such that $\langle \mathbb{N}, =, S_0, S_1 \rangle$ is isomorphic to $\langle \mathbb{N} \times \{0,1\}^*, =, r_0, r_1 \rangle$.*

Proof. We choose functions S_0, S_1 as the simplest ones such that, for all $(x,y) \in \mathbb{N}^2$, $S_0(x) \neq x$, $S_1(x) \neq x$ and $S_0(x) \neq S_1(y)$.

- If $F(x) = 2^x$, then $S_0(x) = 2^x$, $S_1(x) = 2^x + 5$.
- If $F(x) = c^x$, $c \geq 3$, then $S_0(x) = c^x$, $S_1(x) = c^x + 1$.
- If $F(x) = x^c$, $c \geq 2$, then $S_0(x) = x^c + 1$, $S_1(x) = x^c + 3$.
- If $F(x) = \exp_\infty(x)$, then $S_0(x) = \exp_\infty(x)$, $S_1(x) = \exp_\infty(x) + 4$.

Then there exists an isomorphism

$$\alpha : \langle \mathbb{N} \times \{0,1\}^*, =, r_0, r_1 \rangle \cong \langle \mathbb{N}, =, S_0, S_1 \rangle,$$

such that, if $n \in \mathbb{N}$ and λ is the empty word, then $\alpha(n, \lambda)$ is the $n+1$-st natural number not in the ranges of S_0 and S_1, and, if $i \in \{0,1\}$, $n \in \mathbb{N}$ and $u \in \{0,1\}^*$, then $\alpha(r_i(n,u)) = \alpha(n, s_i(u)) = S_i(\alpha(n,u))$. □

Corollary 10.2 *Let $F(x) = c^x$, x^c or $\exp_\infty(x)$ ($c \geq 2$). Then* $\mathrm{Th}(\mathbb{N}, =, x+1, F(x))$ *is complete for* $\mathrm{ATIME\text{-}ALT}(2^{O(n)}, O(n))$. □

11 Conclusion

The results of this paper lead naturally to some questions. First, what happens if we add the linear order on natural numbers? Then equality and successor function are definable in the structure $\langle \mathbb{N}, \leq \rangle$. As we saw in the introduction, $\mathrm{Th}(\mathbb{N}, \leq, 2^x)$ and $\mathrm{Th}(\mathbb{N}, \leq, x^2)$ are decidable, but their complexities are open problems.

We can also consider $\mathrm{Th}(\mathbb{N}, =, x+1, 2x)$. We proved that this theory is also complete for ATIME-ALT$(2^{O(n)}, O(n))$ (unpublished).

We can consider theories of structures with successor function and two other unary functions. Then, these structures become rather complex. Note that, in $\langle \mathbb{N}, =, x+1, 2x, x^2 \rangle$, we can express the famous Diophantine equation $x^2 + 1 = 2y^4$. Ljunggren (1942) [11] proved that this equation has exactly two solutions: $x = y = 1$ and $x = 239$, $y = 13$. The proof was hard enough to justify the publication of a simplified proof by Steiner and Tzanakis (1991) [15], which was simplified again by Hua (1994) [9], without turning out trivial. In fact, the decidability of $\mathrm{Th}(\mathbb{N}, =, x+1, 2x, x^2)$ is an open problem.

We know that in $\langle \mathbb{N}, =, x^2, 2^x \rangle$ we can define $2x$ by

$$y = 2x \iff 2^y = (2^x)^2,$$

and then we can define $x + 1$ by

$$y = x + 1 \iff 2^y = 2.2^x,$$

but the decidability of $\mathrm{Th}(\mathbb{N}, =, x^2, 2^x)$ is an open problem.

Acknowledgements

We thank Serge Grigorieff for helpful discussions.

References

1. Balcázar, J.L., Díaz, J., Gabarró, J.: Structural Complexity II. Springer, Berlin (1990).

2. Berman, L.: The complexity of logical theories. Theoret. Comput. Sci. **11**, 71–77 (1980).

3. Compton, K.J., Henson, C.W.: A uniform method for proving lower bounds on the computational complexity of logical theories. Ann. Pure Appl. Logic **48**, 1–79 (1990) (Updated version in: Abramsky, S. et al. (eds.) Handbook of Logic and Computer Science, Vol. 5: Logic and Algebraic Methods, pp. 129–216. Oxford University Press, Oxford (2000)).

4. Ehrenfeucht, A.: An application of games to the completeness problem for formalized theories. Fundamenta Mathematica **49**, 129–141 (1961).

5. Elgot, C.C., Rabin, M.O.: Decidability and undecidability of extensions of second (first) order theory of (generalized) successor. J. Symb. Logic **31**, 169–181 (1966).

6. Ferrante, J., Rackoff, C.W.: The computational complexity of logical theories, Lecture Notes in Mathematics 718. Springer, Berlin (1979).

7. Fraïssé, R.: Sur quelques classifications des systèmes de relations. Université d'Alger, Publications Scientifiques, Séries A, **1**, 35–182 (1954).

8. Gaifman, H.: On local and nonlocal properties. In: Stern, J. (ed.) Logic Colloquium'81, pp. 105–135. North Holland, Amsterdam (1982).

9. Hua, C.J.: A new solution of the Diophantine equation $X^2 + 1 = 2Y^4$. J. Number Theory **48**, 62–74 (1994).

10. Korec, I.: A list of arithmetical structures complete with respect to the first-order definability. Theoret. Comput. Sci. **257**, 115–151 (2001).

11. Ljunggren : Zur Theorie der Gleichung $X^2 + 1 = DY^4$. Avh. Nordske Vid. Akad. Oslo **1**, No. 5 (1942).

12. Lo, L.: On the computational complexity of the theory of abelian groups. Ann. Pure Appl. Logic **37**, 205–248 (1988).

13. Michel, P.: Complexity of logical theories involving coprimality. Theoret. Comput. Sci. **106**, 221–241 (1992).

14. Semenov, A.L.: Logical theories of one-place functions on the set of natural numbers. Math. USSR Izv. **22**, 587–618 (1984) (Russian original: 1983).

15. Steiner, R., Tzanakis, N.: Simplifying the solution of Ljunggren's equation. J. Number Theory **37**, 123–132 (1991).

16. Thomas, W.: A note on undecidable extensions of monadic second order successor arithmetic. Arch. math. Logik **17**, 43–44 (1975).

17. Volger, H.: Turing machines with linear alternation, theories of bounded concatenation and the decision problem of first order theories. Theoret. Comput. Sci. **23**, 333–337 (1983).