

The Inverse of Ackermann Function is Computable in Linear Time

Claude Sureson*

Université Paris 7 Denis Diderot

5 Rue Thomas Mann, 75013 Paris, France

sureson@math.univ-paris-diderot.fr

Abstract. We propose a detailed proof of the fact that the inverse of Ackermann function is computable in linear time.

Keywords: Recursive functions, Complexity of computation.

1. Introduction

The Ackermann function was proposed in 1926 by W. Ackermann (see [1]) as a simple example of a total recursive function which is not primitive recursive. It is often presented, as done initially by R. Péter, under the form of a two argument function $A : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$.

The function $n \mapsto A(n, n)$ grows extremely fast (asymptotically faster than any primitive recursive function). Hence its inverse, denoted α , grows very slowly; it is known to be primitive recursive. The function α appears to express time complexities in data structure analysis as in the work of E. Tarjan [2] and in algorithmic geometry as in the work of B. Chazelles [3]. It is also used by G. Nivasch, R. Seidel and M. Sharir without reference to the original Ackermann function A in [4, 5, 6].

In a previous work [7], we needed a bound on the amount of time spent to compute the function α . But except for the fact that α is primitive recursive, we could not find a documented reference. This is why we proposed a detailed proof of the fact that α is computable in linear time (on a multitape Turing machine). Once our work was made public, L. Tran, A. Mohan and A. Hobor [8] informed us that they

*Address for correspondence: Université Paris 7 Denis Diderot, France.

had obtained a similar result by totally different methods (functional programming techniques). Our demonstration is elementary and builds partly on the exposition by G. Tourlakis [9] of the primitive recursiveness of the graph of A .

2. A few classical definitions

2.1. Some notation

\mathbb{N} , \mathbb{Z} and \mathbb{R} represent respectively the set of natural, integer and real numbers. $\{0, 1\}^*$ and $\{0, 1\}^{\mathbb{N}}$ denote the sets of finite and infinite binary sequences. \mathbb{N}^* and $\mathbb{N}^{\mathbb{N}}$ are the sets of finite and infinite sequences of natural numbers.

Definition 2.1.

1. Let \mathbf{x} be a finite or infinite sequence. For an integer $i \in \mathbb{N}$, $\mathbf{x} \upharpoonright_i$ is the restriction of \mathbf{x} onto the set $\{0, 1, \dots, i-1\}$.
2. If \mathbf{x} is a finite sequence, then $|\mathbf{x}|$ denotes its length.
3. $<_{lex}$ is the lexicographic order on \mathbb{N}^* .
4. Let $n \in \mathbb{N}$. Then $|n|$ is the length of the string σ_n corresponding to n under binary representation. For $n \geq 1$, $|n| = \lfloor \log_2 n \rfloor + 1$ ($|0| = 1$) and $n < 2^{|n|} \leq 2n$.
5. Let $\log : \mathbb{N} \setminus \{0\} \rightarrow \mathbb{N}$ be defined, for $n \geq 1$ by $\log(n) = \lfloor \log_2(n) \rfloor$. Then $|n| - 1 \leq \log(n) \leq |n|$.

All complexity notions refer to binary representation of integers. Given a function $f : \mathbb{N} \rightarrow \mathbb{N}$ which is time constructible (see [10]) and such that $f(n) \geq n$ for all $n \in \mathbb{N}$, we shall consider predicates checkable in time $\mathcal{O}(f(n))$ and functions computable in time $\mathcal{O}(f(n))$.

2.2. Definition of the Ackermann function

There exist different versions of Ackermann function depending on the initial definitions (*i.e.* the values of $A(0, n)$ and of $A(k, 0)$, for $k, n \in \mathbb{N}$). We refer to the definition in [11] and freely use the properties proved in this textbook.

Definition 2.2. ([11, 5.2.1])

- (a) Let $A : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$ be defined as follows: for $k, n \in \mathbb{N}$,
 - $A(0, n) = 2^n$,
 - $A(k, 0) = 1$,
 - $A(k+1, n+1) = A(k, A(k+1, n))$.
- (b) For $k \in \mathbb{N}$, let $A_k : \mathbb{N} \rightarrow \mathbb{N}$ be such that for all $n \in \mathbb{N}$, $A_k(n) = A(k, n)$.
- (c) Let $Ack : \mathbb{N} \rightarrow \mathbb{N}$ be such that $Ack(n) = A(n, n)$.

We chose this version rather than Turlakis' one because it allows some simplifications and because it is closely related to the version A^T proposed by Tarjan [2] and referred to in [3]. A^T is defined as follows:

- for $n \in \mathbb{N}$, $A^T(0, n) = 2n$,
 - for $k \in \mathbb{N}$, $A^T(k, 0) = 0$ and $A^T(k, 1) = 2$,
 - for $k \in \mathbb{N}, n \geq 1$, $A^T(k+1, n+1) = A^T(k, A^T(k+1, n))$.
- One can check that for any $k \in \mathbb{N}, n \geq 1$, $A^T(k+1, n) = A(k, n)$.

We recall the notion of inverse. The methods developed in this paper can be applied to inverse functions with two parameters (see [3, 2]), but we shall not consider them here. We should also mention the work of [6, 5] using “inverse Ackermann functions” without referring explicitly to the Ackermann function itself.

Definition 2.3.

- Let $f : \mathbb{N} \rightarrow \mathbb{N}$ be unbounded and nondecreasing. The inverse of f denoted Inv_f is defined as follows: for any $n \in \mathbb{N}$, $Inv_f(n)$ is the least $k \in \mathbb{N}$ such that $f(k) \geq n$.
- Let $\alpha : \mathbb{N} \rightarrow \mathbb{N}$ be Inv_{Ack} .

Because of the above relation between A and A^T , results about A , Ack and α can thus be applied to A^T and its related “inverses”.

We recall some basic properties of the functions A_k , for $k \in \mathbb{N}$:

Lemma 2.4. For any $k \in \mathbb{N}$,

- (a) A_k is strictly increasing (see [11, lemma 5.7]),
- (b) for any $n \geq 1$, $A_k(n) \leq A_{k+1}(n)$ (see [11, lemma 5.8]),

We shall consider iterates of a function:

Definition 2.5. Given a function $g : \mathbb{N} \rightarrow \mathbb{N}$ and $m \in \mathbb{N}$, the m th iterate of g , denoted $g^{(m)}$ is defined inductively by: $g^{(0)}(n) = n$ and $g^{(m+1)}(n) = g(g^{(m)}(n))$.

To simplify notation (avoiding towers of exponentials), we shall apply the notion to the following function:

Definition 2.6. Let $exp : \mathbb{N} \rightarrow \mathbb{N}$ be such that $exp(n) = 2^n$, for $n \in \mathbb{N}$.

3. Properties of the functions A_k and of their inverses

We first note some elementary properties of A :

Fact 3.1. For any $i \in \mathbb{N}$,

- (1) $A(i, 1) = 2$,
- (2) $A(i, 2) = 4$,
- (3) $A(1, i) = exp^{(i)}(1)$.

Proof:

1. $A(0, 1) = 2$ by definition, and for any $i \in \mathbb{N}$,
 $A(i+1, 1) = A(i, A(i+1, 0)) = A(i, 1)$.
2. $A(0, 2) = 2^2 = 4$ by definition, and for any $i \in \mathbb{N}$,
 $A(i+1, 2) = A(i, A(i+1, 1)) = A(i, 2)$ by (1).
3. $A(1, 0) = 1 = \exp^{(0)}(1)$ by definition, and for any $i \in \mathbb{N}$,
 $A(1, i+1) = A(0, A(1, i)) = \exp(A(1, i))$.

□

The link between A_k and A_{k+1} is the following one:

Fact 3.2. For any $k, n \in \mathbb{N}$, $A_{k+1}(n) = A_k^{(n)}(1)$.

Proof:

Let k be fixed. This is true for $n = 0$: $A_{k+1}(0) = 1 = A_k^{(0)}(1)$.

Let us assume the equality holds for $n \in \mathbb{N}$. Then

$$A_{k+1}(n+1) = A_k(A_{k+1}(n)) = A_k(A_k^{(n)}(1)) = A_k^{(n+1)}(1).$$

□

We deduce from Fact 3.1, some lower bounds:

Fact 3.3. $A_3(3) > \exp^{(4)}(3)$.

Proof:

$$\begin{aligned}
 A_3(3) &= A_2(A_3(2)) \\
 &= A_2(4) && \text{(by 3.1(2))} \\
 &= A_1(A_2(3)) \\
 &= A_1(A_1(A_2(2))) \\
 &= A_1(A_1(4)) && \text{(by 3.1(2))} \\
 &= A_1(\exp^{(4)}(1)) && \text{(by 3.1(3))} \\
 &= A_1(2^{16}) \\
 &= \exp^{(2^{16}-2)}(4) && \text{(by 3.1(3))} \\
 &> \exp^{(4)}(3).
 \end{aligned}$$

□

Claim 3.4. For any $n \geq 3$, $A_3(n) > \exp^{(4)}(n)$.

Proof:

By the previous fact, this is true for $n = 3$.

We thus argue by induction, assuming the inequality holds for $n \geq 3$. Then

$$\begin{aligned}
 A_3(n+1) &= A_2(A_3(n)) > A_2(\exp^{(4)}(n)) \geq A_0(\exp^{(4)}(n)) \\
 &\geq \exp^{(5)}(n) = \exp^{(4)}(2^n) \geq \exp^{(4)}(n+1).
 \end{aligned}$$

□

Claim 3.5. For any $k \geq 3$, $A_k(3) > \exp^{(4)}(k)$.

Proof:

By 3.3, this holds for $k = 3$.

We assume $A_k(3) > \exp^{(4)}(k)$ for $k \geq 3$. Then

$$A_{k+1}(3) = A_k(A_{k+1}(2)) \stackrel{(3.1)}{=} A_k(4) = A_{k-1}(A_k(3)) \stackrel{\text{ind.}}{>} A_0(\exp^{(4)}(k)) = \exp^{(4)}(2^k) \geq \exp^{(4)}(k+1). \quad \square$$

We now evaluate the complexity of the functions Inv_{A_k} , for $k \in \mathbb{N}$.

Lemma 3.6. \log is computable in linear time.

Proof:

This is folklore. We propose a simple argument suggested by one referee: one counts in binary the number of digits of the input x .

The counter being written in reverse order, we change the first digit of the counter for all browsed positions on the input tape, change the second digit for every position out of 2,..., change the k th digit for every position r on the input tape such that $r-1$ has binary representation of the form $u1^{k-1} \dots$

Hence for some constant B , if $2^r \leq |x| < 2^{r+1}$, the number of steps required to obtain $|x|$ in binary is bounded by $B(|x| + \sum_{k=1}^{k=r} 2^{r-(k-1)}) = O(|x|)$. \square

One notes that $Inv_{A_0} = \lceil \log_2 \rceil = \log$. Hence we can state:

Claim 3.7. Inv_{A_0} is computable in linear time.

We now relate $Inv_{A_{k+1}}$ to Inv_{A_k} , for $k \in \mathbb{N}$.

Definition 3.8. Let $m, k \geq 0$ and let the sequence of integers $(n_r)_{r \leq s}$ be defined inductively as follows:

- $n_0 = m$,
- for $r \geq 0$ and n_r defined,
 - if $n_r \leq 1$, then we stop the construction and set $s = r$,
 - otherwise let $n_{r+1} = Inv_{A_k}(n_r)$.

Claim 3.9. Let m, k, s be as in the above definition.

- (a) The construction does stop.
- (b) $Inv_{A_{k+1}}(m) = s$.

Proof:

(a) If $m \leq 1$, then the construction stops at the first step and $s = 0$.

Hence let $m > 1$. We check that the sequence $(n_r)_r$ is strictly decreasing.

By definition, as long as n_{r+1} is defined,

$$A_k(n_{r+1} - 1) < n_r \leq A_k(n_{r+1}) \quad (1)$$

Hence $2^{n_{r+1}-1} = A_0(n_{r+1}-1) \leq A_k(n_{r+1}-1) < n_r$. This gives $2^{n_{r+1}} < 2n_r$. Since for any $t \in \mathbb{N}$, $2^t \geq 2t$, we deduce $n_{r+1} < n_r$.

(b) If $m \leq 1$, then $A_{k+1}(0) \geq m$. Hence $\text{Inv}_{A_{k+1}}(m) = 0 = s$.

Otherwise $s \geq 1$ and we verify both inequalities: $A_{k+1}(s) \geq m$ and $A_{k+1}(s-1) < m$.

$A_{k+1}(s) \geq m$:

We check by induction on $t \leq s$ that $n_{s-t} \leq A_k^{(t)}(1)$.

- This is true for $t = 0$ since $n_s \leq 1$.

- We assume this holds for $t \geq 0$. By (1), we deduce

$$n_{s-(t+1)} \leq A_k(n_{s-t}) \underset{\text{ind.}}{\leq} A_k(A_k^{(t)}(1)) \leq A_k^{(t+1)}(1).$$

By applying the inequality to $t = s$, we obtain from Fact 3.2

$$m = n_0 \leq A_k^{(s)}(1) = A_{k+1}(s).$$

$A_{k+1}(s-1) < m$:

We check by induction on $1 \leq t \leq s$ that $A_k^{(t-1)}(1) < n_{s-t}$.

- Let $t = 1$. then $n_{s-1} > 1 = A_k^{(0)}(1)$. Hence the inequality holds.

- We assume $n_{s-t} > A_k^{(t-1)}(1)$ for $t \geq 1$. Hence $A_k^{(t-1)}(1) \leq n_{s-t} - 1$. We deduce

$$A_k^{(t)}(1) = A_k(A_k^{(t-1)}(1)) \leq A_k(n_{s-t} - 1) \underset{(1)}{<} n_{s-(t+1)}.$$

Applying the inequality to $t = s$, we obtain $m = n_0 > A_k^{(s-1)}(1) \underset{\text{Fact 3.2}}{=} A_{k+1}(s-1)$.

We conclude that $\text{Inv}_{A_{k+1}}(m) = s$. □

From this characterization of $\text{Inv}_{A_{k+1}}$, we shall derive:

Lemma 3.10. For any $k \in \mathbb{N}$, Inv_{A_k} is computable in linear time.

Proof:

We shall argue by induction on $k \in \mathbb{N}$.

- This holds for $k = 0$ by Claim 3.7.

- We assume now that Inv_{A_k} is computable in linear time and we check that it is also the case for $\text{Inv}_{A_{k+1}}$.

Starting with $m \geq 2^4$, we shall evaluate the time required to obtain the sequence $(n_r)_{r \leq s}$ of Definition 3.8. We recall that $n_{r+1} = \text{Inv}_{A_k}(n_r)$, if $n_r > 1$.

Since $n_{s-1} > 1$, $A_k(0) = 1$, $n_s \leq 1$ and $n_s = \text{Inv}_{A_k}(n_{s-1})$, necessarily $n_s = 1$.

Claim 3.11. For $m \geq 4$, $s \leq 2 \log^{(2)}(m)$.

Proof:

We note that since $A_k(1) = 2 < m = n_0$, necessarily $n_1 > 1$ and $s \geq 2$.

By definition, n_1 and n_2 satisfy the following:

$$2^{n_1-1} \leq A_k(n_1-1) < m \text{ and } 2^{n_2-1} \leq A_k(n_2-1) < n_1.$$

Now $2^{n_1} < 2m$ gives $n_1 \leq \log(m)$. Similarly we obtain $n_2 \leq \log(n_1)$ and hence

$$n_2 \leq \log^{(2)}(m) \quad (2)$$

Since $(n_r)_{r \leq s}$ is strictly decreasing and $n_s = 1$, one checks that $n_2 \geq 1 + (s-2)$.

Hence $s \leq n_2 + 1 \stackrel{(2)}{\leq} \log^{(2)}(m) + 1 \leq 2\log^{(2)}(m)$ (the last inequality holds because $\log^{(2)}(m) \geq 1$). \square

Let $m \geq 2^4$. By induction hypothesis, there is a constant C such that for any $u \in \mathbb{N}$, the computation of $\text{Inv}_{A_k}(u)$ takes at most $C|u|$ steps.

- Hence the obtention of n_1 and n_2 takes at most $2C|m|$ steps.

- We now bound the time required to compute $(n_r)_{2 < r \leq s}$. For each $2 \leq r < s$, the obtention of n_{r+1} (given n_r) takes at most $C|n_2|$ steps. Since $m \geq 2^4$, we have:

$$|n_2| \stackrel{(2)}{\leq} |\log^{(2)}(m)| \leq \log^{(3)}(m) + 1 \leq 2\log^{(3)}(m),$$

Hence to treat all $2 \leq r < s$, by Claim 3.11, one needs at most $4C\log^{(2)}(m)\log^{(3)}(m)$ steps.

There is a constant D such that for any $m \in \mathbb{N}$, one has

$$\log^{(2)}(m)\log^{(3)}(m) \leq D\log(m) \leq D|m|.$$

Hence we deduce that $\text{Inv}_{A_{k+1}}(m)$ is computable in time $\mathcal{O}(|m|)$. \square

There may be a way to use G. Nivasch (see [4]) development on inverse Ackermann function to evaluate the complexity of the functions Inv_{A_k} . One would have to clarify the link between Nivasch's function α_k and our Inv_{A_k} .

4. Encoding sequences

In this section, we introduce the coding of couples, triples or finite sequences of integers of arbitrary length.

Definition 4.1.

- For $u, v \in \mathbb{N}$, let $\langle u, v \rangle = \frac{(u+v)(u+v+1)}{2} + v$. Then $\langle \cdot, \cdot \rangle : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$ is a bijection.
- Let $(\cdot)_0$ and $(\cdot)_1$ be the “inverses” of $\langle \cdot, \cdot \rangle$: for any $w \in \mathbb{N}$, $\langle (w)_0, (w)_1 \rangle = w$.

Classically one has:

Claim 4.2. The function $\langle \cdot, \cdot \rangle$ and its inverses $(\cdot)_0, (\cdot)_1$ are polynomial time computable.

Proof:

To answer a referee's request, we justify the second assertion.

Let $s \in \mathbb{N}$. We must find the integer a such that $a(a+1) \leq 2s < (a+1)(a+2)$ because if $\Delta = s - \frac{a(a+1)}{2}$, then one has $(s)_0 = a - \Delta$ and $(s)_1 = \Delta$.

It takes quadratic time to get the “square root” of $2s$: the integer α such that $\alpha^2 \leq 2s < (\alpha + 1)^2$. Then either α or $\alpha - 1$ is the expected a . \square

We derive the coding of triples:

Definition 4.3. For $u, v, w \in \mathbb{N}$, let $\langle u, v, w \rangle = \langle \langle u, v \rangle, w \rangle$.

Claim 4.4. For $u, v, w \in \mathbb{N}$, $\langle u, v, w \rangle \leq 8(u + v + w)^4$.

Proof:

If $u + v = k$, then $\langle u, v \rangle < \langle k + 1, 0 \rangle$. Hence

$$\langle u, v \rangle \leq \frac{(k+1)(k+2)}{2} - 1 \leq 2k^2 = 2(u+v)^2 \quad (3)$$

We deduce

$$\begin{aligned} \langle u, v, w \rangle &\leq \langle \langle u, v \rangle, w \rangle \leq \langle 2(u+v)^2, w \rangle && \text{(by (3))} \\ &\leq 2(2(u+v)^2 + w)^2 && \text{(by (3))} \\ &\leq 8(u+v+w)^4. && \square \end{aligned}$$

In order to deal with finite sequences of arbitrary length of integers, we follow one referee’s suggestion: writing successively the integers under binary representation while separating them with a new symbol. To keep binary sequences, we replace the symbol 0 by 00, 1 by 11 and the new symbol by 01. We thus consider the following:

Definition 4.5. Let Seq be the predicate on \mathbb{N} defined as follows: for $s \in \mathbb{N}$,

1. $Seq(s)$ iff $s = \sum_{i < 2t} \varepsilon_i 2^i$, for $t > 1$ such that
 - a) $\varepsilon_0 = \varepsilon_1$
 - b) $\varepsilon_{2t-2} = 0, \varepsilon_{2t-1} = 1$
 - c) for any $j < t - 2$, if $\varepsilon_{2j} = 0, \varepsilon_{2j+1} = 1$, then $\varepsilon_{2j+2} = \varepsilon_{2j+3}$.
2. Let $S(s) = \{i < t : \varepsilon_{2i} = 0, \varepsilon_{2i+1} = 1\}$ and $l(s) = |S(s)|$ (the cardinality of $S(s)$). If $(i_j)_{j < l(s)}$ is an increasing enumeration of $S(s)$, then we set
 - $s(0) = \sum_{n < i_0} \varepsilon_{2n} 2^{i_0 - 1 - n}$ and
 - for $1 \leq j < l(s)$, $s(j) = \sum_{i_{j-1} < n < i_j} \varepsilon_{2n} 2^{(i_j - 1) - n}$. $(s(j))_{j < l(s)}$ is the sequence of integers encoded in s .

We note the following:

Fact 4.6. Let $\mu, l \in \mathbb{N}$ and $\mathbf{a} = (a_i)_{i < l}$ be a sequence of integers such that for any $i < l$, $a_i \leq \mu$. Then by the previous definition, we can encode \mathbf{a} in $s \in \mathbb{N}$ such that $Seq(s)$ holds, $l(s) = l$, for any $i < l(s)$, $s(i) = a_i$ and $2l \leq |s| \leq 2l(|\mu| + 1)$.

One easily checks:

Claim 4.7. The predicate Seq can be checked in polynomial time and the functions $s \rightarrow l(s)$ and $(s, i) \rightarrow s(i)$, for $i < l(s)$, are computable in polynomial time.

5. The tree associated with the computation of A

This section is greatly inspired from Turlakis' exposition [9, Section 2.4.4] of the fact that $graph(A) = \{(u, v, w) : A(u, v) = w\}$ is primitive recursive (where A is defined with different initial conditions). In order to deal with the inverse α of the function $u \mapsto A(u, u)$, we shall consider in addition the predicate $A(u, v) < w$. To control the size of Turlakis' type tree witnessing $A_k(n) < m$, it will be helpful to add new leaves.

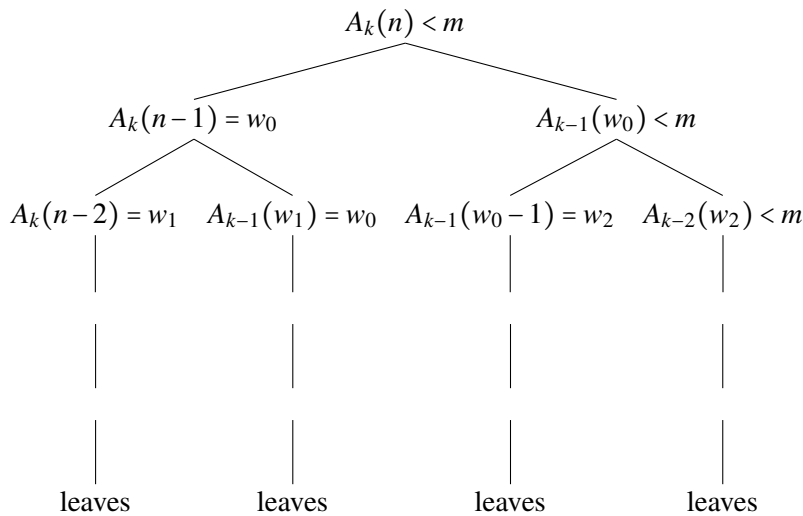
Let us first note that for $u, v \geq 1$, since $A_u(v) = A_{u-1}(A_u(v-1))$, one gets the following equivalences:

$$A_u(v) = w \Leftrightarrow \text{there exists } w' > 0 \text{ such that } \begin{cases} A_u(v-1) = w' \text{ and} \\ A_{u-1}(w') = w \end{cases} \tag{4}$$

$$A_u(v) < w \Leftrightarrow \text{there exists } w' > 0 \text{ such that } \begin{cases} A_u(v-1) = w' \text{ and} \\ A_{u-1}(w') < w \end{cases} \tag{5}$$

($w' > 0$ because for any $x, y \in \mathbb{N}$, $A_x(y) \geq A_0(0) = 1 > 0$)

As in [9], one can thus unroll a labeled binary tree witnessing the fact that $A_k(n) < m$. We shall restrict to the case $k \geq 4$ and $n \geq 3$. For some unique sequence $(w_i)_i$, the labels of the nodes in the following tree are true statements



Let us describe the structure of the tree and the labeling of nodes:

- the root is labeled $A_k(n) < m$.
- A node which is not a leaf is labeled
 - either by $A_u(v) = w$ for $u, v \geq 1$, and admits for a unique $w' > 0$, a left son labeled $A_u(v-1) = w'$ and a right son labeled $A_{u-1}(w') = w$,
 - or by $A_u(v) < w$ for $u \geq 4, v \geq 1$, and admits for a unique $w' > 0$, a left son labeled $A_u(v-1) = w'$ and a right son labeled $A_{u-1}(w') < w$.

- A node is a leaf if it is labeled
 - either by $A_0(v) = 2^v$,
 - or by $A_u(0) = 1$,
 - or by $A_u(v) < m$ with $u \leq 3$ or $v = 0$.

Claim 5.1. Let us consider a binary tree witnessing $A_k(n) < m$, for $k \geq 4$, $n \geq 3$.

- (a) 1. If a node in the tree is labeled $A_u(v) = w$, then $u, v, w < \log^{(4)}(m)$.
2. If it is labeled $A_u(v) < m$, then $3 \leq u, v < \log^{(4)}(m)$.
- (b) If a node labeled $A_u(v) = w$ or $A_u(v) < m$ admits a son labeled $A_{u'}(v') = w'$ or $A_{u'}(v') < m$, then $(u', v') <_{lex} (u, v)$.

Proof:

(a) We argue by induction on the level of the node:

Level 0: The root is labeled $A_k(n) < m$. By hypothesis, $k, n \geq 3$. Hence

$$\exp^{(4)}(n) \leq A_3(n) \leq A_k(n) < m \quad (\text{by Claim 3.4})$$

$$\exp^{(4)}(k) \leq A_k(3) \leq A_k(n) < m \quad (\text{by Claim 3.5})$$

Therefore both $k, n < \log^{(4)}(m)$ and (a) 2. holds.

Level 1: there are two nodes of level 1: the left node is labeled $A_k(n-1) = w_0$ and the right node $A_{k-1}(w_0) < m$.

$k \geq 4$ implies $k-1 \geq 3$. Also $A_k(n-1) \geq A_0(2) = 2^2$ implies $w_0 \geq 4 \geq 3$.

It remains to check $w_0 < \log^{(4)}(m)$. By Claim 3.4, $k-1 \geq 3$ and $w_0 \geq 3$ imply

$$\exp^{(4)}(w_0) \leq A_3(w_0) \leq A_{k-1}(w_0) < m.$$

Hence (a) 1. and (a) 2. hold at level 1.

level $r+1$ with $r \geq 1$: We assume the properties hold for the nodes at level r and we check that it is also true for their sons.

- Let thus the node of level r be labeled $A_u(v) = w$ with $u, v, w < \log^{(4)}(m)$.
 - Its left son is labeled $A_u(v-1) = w'$,
 - its right son is labeled $A_{u-1}(w') = w$.

Since $w' = A_u(v-1) < A_u(v) = w$, (a) 1. holds for both sons.

- Let now the node of level r be labeled $A_u(v) < m$ with $3 \leq u, v < \log^{(4)}(m)$. Since it is not a leaf, $u \geq 4$.

- Its left son is labeled $A_u(v-1) = w'$,
- its right son is labeled $A_{u-1}(w') < m$.

As for level 1, $v-1 \geq 2$ implies $w' = A_u(v-1) \geq A_0(2) \geq 3$. Also $u-1 \geq 3$ and $A_{u-1}(w') < m$ give $w' < \log^{(4)}(m)$. We thus deduce that (a) 1. holds for the left son and (a) 2. for the right one.

(b) Keeping the notation of the claim, we simply note $(u', v') = \begin{cases} (u-1, w') & \text{or} \\ (u, v-1). \end{cases}$

Hence $(u', v') <_{lex} (u, v)$. □

Remark 5.2.

- (a) 2. implies that the last type of leaf labeled $A_u(v) < m$ with $u \leq 3$ or $v = 0$, is necessarily of the form $A_3(v) < m$ for $v \geq 3$.
- We also deduce from this claim that the binary tree witnessing $A_k(n) < m$, for $k \geq 4$, $n \geq 3$, has height at most $(\log^{(4)}(m))^2$.

We do not know whether different nodes in the tree may have the same label. This made the exposition a bit more tedious. We now focus on labels (which are true statements) occurring in the binary tree witnessing $A_k(n) < m$ and encode this set.

let us first note that if $A_u(v) = w$, then $w \geq A_0(0) = 1$. Hence we shall represent the label $A_u(v) = w$ by the integer $\langle u, v, w \rangle$ and the label $A_u(v) < m$ by the integer $\langle u, v, 0 \rangle$ (this will reduce the size of the encoding). We identify the label with its code. Let us introduce the following notation:

Definition 5.3. If $x' = \langle u', v', w' \rangle$ and $x = \langle u, v, w \rangle$, then

$$x' <_{lex}^3 x \quad \text{iff} \quad (u', v', w') <_{lex} (u, v, w).$$

By Claim 5.1 (b), if $\langle u', v', w' \rangle$ labels the son of a node labeled $\langle u, v, w \rangle$, then $\langle u', v', w' \rangle <_{lex}^3 \langle u, v, w \rangle$. This motivates the following:

Claim 5.4. Let $\mathbf{a} = (a_i)_{i < l}$ enumerate, according to increasing $<_{lex}^3$ order, all labels occurring in the tree witnessing $A_k(n) < m$, for $k \geq 4$, $n \geq 3$. Then

(a) $a_{l-1} = \langle k, n, 0 \rangle$ and for any $i < l$,

- either $(a_i$ labels a leaf) $a_i = \begin{cases} \langle 0, v, 2^v \rangle & \text{or} \\ \langle v, 0, 1 \rangle & \text{or} \\ \langle 3, v, 0 \rangle, \end{cases}$
- or $a_i = \langle u, v, w \rangle$ and there exist $j, j' < i$, $w' > 0$ such that $a_j = \langle u, v-1, w' \rangle$ and $a_{j'} = \langle u-1, w', w \rangle$.

(b) $2 \leq l \leq (\log^{(4)}(m))^3$ and for each $i < l$, $a_i < 6^4 (\log^{(4)}(m))^4$.

Proof:

(a) holds by definition of the labeled tree, Claim 5.1 (b) and Remark 5.2.

(b) By Claim 5.1 (a), if $\langle u, v, w \rangle$ labels a node, then $u, v, w < \log^{(4)}(m)$. Hence $l \leq (\log^{(4)}(m))^3$. By Claim 4.4, $\langle u, v, w \rangle \leq 8(u+v+w)^4$. Hence

$$\langle u, v, w \rangle < 2^3 3^4 (\log^{(4)}(m))^4 \leq 6^4 (\log^{(4)}(m))^4. \quad \square$$

To reduce the time of computation, instead of checking for several v 's whether $A_3(v) < m$ (to recognize a leaf), we shall compute once $r_m = \text{Inv}_{A_3}(m)$ and then check $v < r_m$, for the different v 's. We thus set:

Definition 5.5. Let us consider the predicate $Comput_{<}$ defined as follows: for $s, k, n, r \in \mathbb{N}$,

$$\begin{aligned} Comput_{<}(s, k, n, r) \quad \text{iff} \quad & Seq(s) \wedge s(l(s) - 1) = \langle k, n, 0 \rangle \wedge \forall i < l(s) \\ & \left[\exists v (s(i) = \langle 0, v, 2^v \rangle \vee (s(i) = \langle v, 0, 1 \rangle \vee \right. \\ & \qquad \qquad \qquad \left. (s(i) = \langle 3, v, 0 \rangle \wedge v < r)) \right] \vee \\ & \left[\exists u, v, w \exists w' > 0 \exists j, j' < i (s(i) = \langle u, v, w \rangle \wedge \right. \\ & \qquad \qquad \qquad \left. s(j) = \langle u, v - 1, w' \rangle \wedge s(j') = \langle u - 1, w', w \rangle) \right]. \end{aligned}$$

We obtain:

Claim 5.6. There exists $C \in \mathbb{N}$ such that for all $k \geq 4, n \geq 3, m \geq 0$ if $A_k(n) < m$ and $r_m = Inv_{A_3}(m)$, then there is $s \leq C \log^{(2)}(m)$ such that $Comput_{<}(s, k, n, r_m)$ holds.

Proof:

Let $\mathbf{a} = (a_i)_{i < l}$ be the sequence of Claim 5.4 enumerating the different labels occurring in the tree witnessing $A_k(n) < m$. By (b) of this claim, if $\mu = (6 \log^{(4)}(m))^4$, then for any $i < l$, $a_i < \mu$. By Fact 4.6, let $s \in \mathbb{N}$ encode \mathbf{a} and satisfy $|s| \leq 2l(|\mu| + 1)$.

- We first note that $Comput(s, k, n, r_m)$ holds: if for some $i < l$, $s(i) = a_i = \langle 3, v, 0 \rangle$, then this implies $A_3(v) < m$ and hence $v < r_m$.

- It remains to bound s . By Claim 5.4 (b), one has $l \leq (\log^{(4)}(m))^3$. Since $|s| \leq 2l(|\mu| + 1)$ for $\mu = (6 \log^{(4)}(m))^4$, applying $s < 2^{|s|}$ and $2^{|\mu|} \leq 2\mu$, we obtain $s \leq 2^{2l(|\mu|+1)} \leq (2\mu)^{2l} 2^{2l}$.

Hence $s \leq (6 \log^{(4)}(m))^{8(\log^{(4)}(m))^3} \cdot 2^{2(\log^{(4)}(m))^3}$. There exists K, K' (independent of m) such that

$$\begin{aligned} (6 \log^{(4)}(m))^{8(\log^{(4)}(m))^3} \cdot 2^{2(\log^{(4)}(m))^3} &\leq K 2^{(\log^{(4)}(m))^4} \\ &\leq KK' 2^{\log^{(3)}(m)} \\ &\leq 2KK' \log^{(2)}(m). \end{aligned}$$

(We use the fact that if $f(m) \leq g(m)$ almost everywhere, then there is θ such that $f(m) \leq g(m) + \theta$ for all m , and hence $2^{f(m)} \leq 2^\theta 2^{g(m)}$ for all m).

Therefore $s \leq 2KK' \log^{(2)}(m)$. □

Conversely, one obtains:

Claim 5.7. Let $m \in \mathbb{N}$ and $r_m = Inv_{A_3}(m)$. If $Comput_{<}(s, k, n, r_m)$ holds for some $s, k, n \in \mathbb{N}$, then $A_k(n) < m$.

Proof:

We assume $Comput_{<}(s, k, n, r_m)$ is satisfied and we check by induction on $i < l(s)$ that

(a) if $s(i) = \langle u, v, w \rangle$ with $w > 0$, then $A_u(v) = w$.

(b) if $s(i) = \langle u, v, 0 \rangle$, then $A_u(v) < m$.

Let us note that by definition, $l(s) \geq 2$.

- Let $i = 0$. By definition of $Comput_{<}$, $s(i)$ is necessarily of a “leaf type”. That is

- either $s(i) = \langle 0, v, 2^v \rangle$ or $\langle u, 0, 1 \rangle$, and by definition of the function A , (a) is satisfied,
- or $s(i) = \langle 3, v, 0 \rangle$ and $Comput(s, k, n, r_m)$ implies $v < r_m$. Therefore one has $A_3(v) < m$ and (b) holds.

- Let now $i > 0$. We assume that for any $j < i$, according to the nature of $s(j)$, (a) or (b) holds for $s(j)$.

If $s(i)$ is of the “leaf type”, then one argues as for $i = 0$. Otherwise $s(i) = \langle u, v, w \rangle$ and there exist $j, j' < i$ and $w' > 0$ such that we have $s(j) = \langle u, v-1, w' \rangle$ and $s(j') = \langle u-1, w', w \rangle$.

By induction hypothesis,

- $A_u(v-1) = w'$ (the fact that $w' > 0$ is important)
- and $\begin{cases} \text{if } w = 0, A_{u-1}(w') < m, \\ \text{if } w > 0, A_{u-1}(w') = w. \end{cases}$

We thus deduce $A_u(v) = A_{u-1}(A_u(v-1)) = A_{u-1}(w')$. Hence according to whether $w = 0$ or not, we conclude that (a) or (b) holds for $s(i) = \langle u, v, w \rangle$.

Hence by (b) applied to $i = l(s-1)$ and $s(l(s)-1) = \langle k, n, 0 \rangle$, we derive $A_k(n) < m$. \square

Combining Claims 5.6 and 5.7, we obtain:

Lemma 5.8. There is $C \geq 1$ such that for any $k \geq 4, n \geq 3, m \in \mathbb{N}$, if $r_m = \text{Inv}_{A_3}(m)$, then the following equivalence holds:

$$A_k(n) < m \quad \text{iff} \quad \exists s \leq C \log^{(2)}(m) \text{ Comput}_{<}(s, k, n, r_m).$$

6. Computation time

We first estimate the complexity of $Comput_{<}$:

Claim 6.1. There exist $B, t \in \mathbb{N}$ such that the predicate “ $k \geq 4 \wedge n \geq 3 \wedge \text{Comput}_{<}(s, k, n, r)$ ” can be checked in at most $B(\max(|s|, |k|, |n|, |r|))^t$ steps.

Proof:

This is a consequence of Claim 4.7 about the complexity of Seq , the definition of $Comput_{<}$ (Definition 5.5) and the fact that $l(s) \leq |s|$ (see Fact 4.6). \square

Our goal is now to obtain:

Lemma 6.2. There is $D \in \mathbb{N}$ such that the predicate “ $k \geq 4 \wedge n \geq 3 \wedge A_k(n) < m$ ” can be checked in at most $D \max(|k|, |n|, |m|)$ steps.

Proof:

Let $C \geq 1$ be the constant mentioned in Lemma 5.8.

The algorithm which decides the predicate “ $k \geq 4 \wedge n \geq 3 \wedge A_k(n) < m$ ”:

- (1) We check $k \geq 4, n \geq 3$ and then $k, n \leq \log^{(2)}(m)$,
- (2) we compute $r_m = \text{Inv}_{A_3}(m)$ and check $r_m > 3$.
- (3) If these previous steps have been successfully completed, we try all $s \leq C \log^{(2)}(m)$ to obtain $\text{Comput}_{<}(s, k, n, r_m)$. If we fail to obtain such an s or to satisfy steps (1) and (2), then we output “No”. Otherwise it is “yes”.

We note that $r_m \leq 3$ implies $A_3(3) \geq m$ and hence $A_k(n) \geq A_3(3) \geq m$. Hence as the requirement “ $k, n \leq \log^{(2)}(m)$ ”, the condition $r_m > 3$ can be harmlessly added in the definition of the algorithm. Their role is only to reduce the running time of the algorithm.

By Lemma 5.8, the algorithm is correct.

Running time:

- (1) By Lemma 3.6, step (1) requires at most $\mathcal{O}(\max(|k|, |n|, |m|))$ steps
- (2) By Lemma 3.10, step (2) needs at most $\mathcal{O}(|m|)$ steps.
- (3) If $r_m > 3$, then $r_m - 1 \geq 3$ and $A_3(r_m - 1) < m$ implies because of Claim 3.4 $r_m \leq \log^{(4)}(m)$. We thus have $s, k, n, r_m \leq C \cdot \log^{(2)}(m)$ and hence

$$|s|, |k|, |n|, |r_m| \leq 2C \cdot \log^{(3)}(m)$$

(because if $d, \log(v) \geq 1$, then $u \leq dv$ implies $|u| \leq 2d \log(v)$).

By Claim 6.1, there are $B, t \in \mathbb{N}$ such that, for each $s \in \mathbb{N}$, checking $\text{Comput}_{<}(s, k, n, r_m)$ takes at most $B(\max(|s|, |k|, |n|, |r_m|))^t$ steps.

Hence checking for all $s \leq C \log^{(2)}(m)$, whether $\text{Comput}_{<}(s, k, n, r_m)$ holds, requires at most $T = B2^t C^{t+1} \log^{(2)}(m) (\log^{(3)}(m))^t$ steps.

There is $K \in \mathbb{N}$ (independent of m) such that $T \leq K(\log^{(2)}(m))^2$

Using $(\log(r))^2 \leq 4r$, for $r \geq 4$, we deduce $T \leq 4K \log(m) \leq 4K|m|$.

Lemma 6.2 follows from the time estimates of (1),(2) and (3). □

It suffices now to remove the hypothesis “ $k \geq 4 \wedge n \geq 3$ ”.

Lemma 6.3. There is a constant $D \in \mathbb{N}$ such that for any $k, n, m \in \mathbb{N}$, the predicate “ $A_k(n) < m$ ” can be checked in at most $D \max(|k|, |n|, |m|)$ steps.

Proof:

Let $U(k, n, m)$ iff $k \geq 4 \wedge n \geq 3 \wedge A_k(n) < m$,

$V(n, k, m)$ iff $k \leq 3 \wedge A_k(n) < m$,

$W(k, n, m)$ iff $n \leq 2 \wedge A_k(n) < m$.

Then $A_k(n) < m$ iff $U(k, n, m) \vee V(k, n, m) \vee W(k, n, m)$.

- By Lemma 6.2, $U(k, n, m)$ can be checked in $\mathcal{O}(\max(|k|, |n|, |m|))$ steps.

- For any k, n, m , one has the equivalence: $V(k, n, m) \Leftrightarrow k \leq 3 \wedge \text{Inv}_{A_k}(m) > n$
Hence by Lemma 3.10, $V(k, n, m)$ can be checked in $\mathcal{O}(\max(|k|, |n|, |m|))$ steps.
- By Fact 3.1, for any k, n, m , one has the equivalences:

$$\begin{aligned} W(k, n, m) &\Leftrightarrow (n = 0 \wedge A_k(0) < m) \vee (n = 1 \wedge A_k(1) < m) \vee (n = 2 \wedge A_k(2) < m) \\ &\Leftrightarrow (n = 0 \wedge m > 1) \vee (n = 1 \wedge m > 2) \vee (n = 2 \wedge m > 4). \end{aligned}$$

Hence $W(k, n, m)$ can also be verified in $\mathcal{O}(\max(|k|, |n|, |m|))$ steps. □

Let $\text{Graph}(A) = \{(k, n, m) \in \mathbb{N}^3 : A_k(n) = m\}$. We deduce:

Proposition 6.4. The predicate “ $(k, n, m) \in \text{Graph}(A)$ ” is checkable in linear time.

Proof:

For any $k, n, m \in \mathbb{N}$, $A_k(n) = m$ iff $A_k(n) < m + 1 \wedge \neg(A_k(n) < m)$. □

Let us recall that the function Ack is such that, for any $k \in \mathbb{N}$, $Ack(k) = A(k, k)$ and α is its inverse Inv_{Ack} (definitions 2.2(c) and 2.3).

To obtain the fact that $\text{Graph}(A)$ is checkable in linear time, we could have as in Tourlakis’ book, considered the predicate “ $A_k(n) = m$ ” in place of “ $A_k(n) < m$ ”. But to prove that α itself, can be computed in linear time, it seemed to us that the use of the predicate “ $A_k(n) < m$ ” was necessary. It is not the case for some approximations; for instance $\alpha' : n \mapsto \alpha(\log^{(2)}(n))$ satisfies for any $n \in \mathbb{N}$, $0 \leq \alpha(n) - \alpha'(n) \leq 2$ and the fact that it is computable in linear time can be deduced from the fact that $\text{Graph}(A)$ is checkable in linear time.

Proposition 6.5. The function α is computable in linear time.

Proof:

Let $C \geq 1$ be the constant of Lemma 5.8. We now propose an algorithm which on input $m \in \mathbb{N}$, outputs $\alpha(m)$.

The algorithm: let $m \in \mathbb{N}$.

- (1) For each $k \leq 3$, we compute $\rho_k = \text{Inv}_{A_k}(m)$. If there is $k \leq 3$ such that $\rho_k \leq k$, then we output the least such k . Otherwise we go to step 2.
- (2) We compute $\log^{(4)}(m)$ (we shall see that necessarily it is greater or equal to 4). For each j such that $4 \leq j \leq \log^{(4)}(m)$, we test all $s \leq C \log^{(2)}(m)$ to obtain $\text{Comput}_{<}(s, j, j, \rho_3)$.

We output the least $j_0 \geq 4$ for which we fail to find such an $s \leq C \log^{(2)}(m)$.

Validity of the algorithm:

- (1) If we stopped after step (1) and $k_0 \leq 3$ is least such that $\rho_{k_0} \leq k_0$, then $k_0 \geq \text{Inv}_{A_{k_0}}(m)$ implies

$$A_{k_0}(k_0) \geq m. \tag{6}$$

- If $k_0 = 0$, then by (6) $\alpha(m) = 0$,

- otherwise, by definition, $\rho_{k_0-1} > k_0 - 1$. Hence $\rho_{k_0-1} - 1 \geq k_0 - 1$ and we deduce

$$A_{k_0-1}(k_0 - 1) \leq A_{k_0-1}(\rho_{k_0-1} - 1) < m. \quad (7)$$

(6)+(7) give $\alpha(m) = k_0$.

- (2) We thus assume now that for any $k \leq 3$, $\rho_k > k$. Hence $\rho_3 > 3$ and $A_3(3) < m$. By Fact 3.3

$$\log^{(4)}(m) > 3. \quad (8)$$

Hence the following inequalities hold:

$$\begin{aligned} A(\log^{(4)}(m), \log^{(4)}(m)) &\geq A_3(\log^{(4)}(m)) && \text{(by (8))} \\ &\geq \exp^{(4)}(\log^{(4)}(m)) && \text{(by (8) and Claim 3.4)} \\ &\geq m. \end{aligned}$$

Hence $4 \leq \alpha(m) \leq \log^{(4)}(m)$. Let $j_0 = \alpha(m)$. Then for any $i < j_0$, one has $A(i, i) < m$. By Lemma 5.8, we must succeed in finding $s \leq C \log^{(2)}(m)$ such that $\text{Comput}_{<}(s, i, i, \rho_3)$ and we must fail in finding one such s satisfying $\text{Comput}_{<}(s, j_0, j_0, \rho_3)$ since $A(j_0, j_0) \geq m$.

Hence the algorithm outputs $\alpha(m)$.

Running time of the algorithm:

- (1) By Lemma 3.10, step (1) takes $\mathcal{O}(|m|)$ steps.
 (2) We know $\rho_3 > 3$. By Claim 3.4, $\rho_3 - 1 \geq 3$ and $A_3(\rho_3 - 1) < m$ imply $\rho_3 - 1 < \log^{(4)}(m)$ and $\rho_3 \leq \log^{(4)}(m)$.

For each $4 \leq j \leq \log^{(4)}(m)$ and for all $s \leq C \log^{(2)}(m)$, we check $\text{Comput}_{<}(s, j, j, \rho_3)$.

Since $s, j, \rho_3 \leq C \log^{(2)}(m)$, as in the proof of Lemma 6.2, we obtain

$$|s|, |j|, |\rho_3| \leq 2C \log^{(3)}(m).$$

By Lemma 6.1, there are $B, t \in \mathbb{N}$ such that $\text{Comput}_{<}(s, j, j, \rho_3)$ can be checked in at most $B(\max(|s|, |j|, |\rho_3|))^t$ steps.

We deduce that step (3) can be completed in at most

$$T = B2^t C^{t+1} \log^{(2)}(m) \log^{(4)}(m) (\log^{(3)}(m))^t \text{ steps.}$$

There is $K \in \mathbb{N}$ (independent of m) such that $T \leq K \log(m) \leq K|m|$.

Hence steps (1) and (2) take time $\mathcal{O}(|m|)$. □

These methods can be applied to the different two argument inverse Ackermann functions proposed in [2, 3, 6, 5].

References

- [1] Ackermann W. Zum Hilbertschen Aufbau der reellen Zahlen. *Math. Ann.*, 1928. **99**:118–133. doi: 10.1007/BF01459088.

- [2] Tarjan RE. Efficiency of a good but not linear set union algorithm. *J. Assoc. Comput. Mach.*, 1975. **22**:215–225. doi:10.1145/321879.321884.
- [3] Chazelle B. A minimum spanning tree algorithm with inverse-ackermann type complexity. *J. ACM*, 2000. **47**:1028–1047. doi:10.1145/355541.355562.
- [4] Nivasch G. Inverse Ackermann without pain. Accessed: 2019-10-7. URL <http://www.gabrielnivasch.org/fun/inverse-ackermann>.
- [5] Seidel R. Understanding the inverse Ackermann function. 22nd European Workshop on Computational Geometry, 2006. URL <http://cgi.di.uoa.gr/~ewcg06/invited/Seidel.pdf>.
- [6] Seidel R, Sharir M. Top-down analysis of path compression. *SIAM J. Comput.*, 2005. **34**(3):515–525. doi:10.1137/S0097539703439088.
- [7] Sureson C. Subcomputable Hausdorff Function Dimension. To appear in the *J. Theor. Comput. Science*, 2021. doi:10.1016/j.tcs.2021.08.27.
- [8] Tran L, Mohan A, Hobor A. A functional Proof Pearl: Inverting the Ackermann Hierarchy. *CCP 2020: Proceedings of the 9th ACM SIGPLAN International Conference on Certified Programs and Proofs: 2020* pp. 129–142. <https://doi.org/10.1145/3372885.3373837>.
- [9] Turlakakis G. *Theory of computation*. Hoboken, NJ: John Wiley & Sons, 2012. ISBN:978-1-118-01478-3, 978-1-118-31536-1.
- [10] Arora S, Barak B. *Computational complexity. A modern approach*. Cambridge: Cambridge University Press, 2009. ISBN:978-0-521-42426-4.
- [11] Cori R, Lascar D. *Mathematical logic. A course with exercises. Part II. Recursion theory, Gödel’s theorems, set theory, model theory*. Translated from the 1993 French original by Donald H. Pelletier. Oxford: Oxford University Press, 2001. ISBN-10:0198500505, 13:978-0198500506.