Electronic Colloquium on Computational Complexity, Report No. 83 (2013)

Lower Bounds for RAMs and Quantifier Elimination

Miklós Ajtai
IBM Research, Almaden Research Center

May 31, 2013

Abstract. For each natural number d we consider a finite structure $\mathbf{M}_d$ whose universe is the set of all $0,1$-sequence of length $n = 2^d$, each representing a natural number in the set $\{0, 1, ..., 2^n - 1\}$ in binary form. The operations included in the structure are the four constants $0, 1, 2^n - 1, n$, multiplication and addition modulo 2^n, the unary function $\min\{2^x, 2^n - 1\}$, the binary functions $\lfloor x/y \rfloor$ (with $\lfloor x/0 \rfloor = 0$), $\max(x, y)$, $\min(x, y)$, and the boolean vector operations $\wedge, \vee, \neg$ defined on $0, 1$ sequences of length n, by performing the operations on all components simultaneously. These are essentially the arithmetic operations that can be performed on a RAM, with wordlength n, by a single instruction. We show that there exists an $\varepsilon > 0$ and a term (that is, an algebraic expression) $F(x, y)$ built up from the mentioned operations, with the only free variables x, y, such that if $G_d(y)$, $d = 0, 1, 2, ...$, is a sequence of terms, and for all $d = 0, 1, 2, ...$, $\mathbf{M}_d \models \forall x, [G_d(x) = 0 \leftrightarrow \exists y, F(x, y) = 0]$, then for infinitely many integers d, the depth of the term G_d, that is, the maximal number of nestings of the operations in it, is at least $\varepsilon(\log d)^{\frac{1}{2}} = \varepsilon(\log \log n)^{\frac{1}{2}}$.

The following is a consequence. We are considering RAMs N_n, with wordlength $n = 2^d$, whose arithmetic instructions are the arithmetic operations listed above, and also have the usual other RAM instructions. The size of the memory is restricted only by the address space, that is, it is 2^n words. The RAMs has a finite instruction set, each instruction is encoded by a fixed natural number independently of n. Therefore a program P can run on each machine N_n, if $n = 2^d$ is sufficiently large. We show that there exists an $\varepsilon > 0$ and a program P, such that it satisfies the following two conditions.

(i) For all sufficiently large $n = 2^d$, if P running on N_n gets an input consisting of two words a and b, then, in constant time, it gives a $0, 1$ output $P_n(a, b)$.

(ii) Suppose that Q is a program such that for each sufficiently large $n = 2^d$, if Q, running on N_n, gets a word a of length n as an input, then it decides whether there exists a word b of length n such that $P_n(a, b) = 0$. Then, for infinitely many positive integers d, there exists a word a of length $n = 2^d$, such that the running time of Q on N_n at input a is at least $\varepsilon(\log d)^{\frac{1}{2}}(\log \log d)^{-1} \geq (\log d)^{\frac{1}{2}-\varepsilon} = (\log \log n)^{\frac{1}{2}-\varepsilon}$.

ISSN 1433-8092

1 Introduction

1.1 Motivation, historical background

One of the central questions of complexity theory is the comparison of the computational resources needed for deterministic and nondeterministic computation. Namely, assume that we want to find a $0,1$-sequence satisfying a test T. Is it true, under some natural assumptions on the test and on the algorithm searching for x, that to find x requires essentially more computation, than checking that a given x really satisfies T? In the case when both the test and the searching algorithm must be performed in polynomial time (in the length of x) by a turing machine, this leads to the $P = NP$? question.

In an earlier paper [2] the author has shown that if both the test and the computation consist of an evaluation of an algebraic expression made from the operations described in the abstract, and the length of the algebraic expressions are constant then deterministic an nondeterministic computations can be separated. An equivalent formulation in term of RAMs is that there exists a constant time test P in the sense described in the abstract, such that there exists no constant time program Q, which decides for all n and for all words a of lengths n, while running on N_n, whether there exists a word b of length n with $P_n(a, b) = 0$. The main motivation of the present paper is to improve the time lower bound on Q. The methods in [2] show only that a Q with the given properties cannot work in constant time but do not give any specific unbounded function $f(n)$ as a lower bound.

First we compare our results to other theorems, where nonlinear lower bounds were given, or deterministic and nondeterministic computation were separated in general computational models. Some of these proofs were based on diagonalization arguments. In fact the high level structure of the present proof and the proof in [2] is very similar to the structures of the proofs given in [13], [17], or [15]. The technical details however are completely different.

For multi-tape turing machines linear time nondeterministic and deterministic computations were separated in [17] by Paul, Pippenger, Szemerédi, and Trotter in 1984. Their theorem and the present result are not comparable in the sense, that none of them follows from the other, since in the turing machine model longer bitwise computations can be done than in our RAM model with the given time limit, but the RAM model allows arithmetic operations e.g., multiplication, and division of n bit numbers, and it is not known whether these operations can be computed on a multitape turing machine in linear time. For uniform computational models where the working memory is smaller than the input, Fortnow gave nonlinear lower bounds in [15]. In a similar sense as in the case of [17] our results and the results of [15] are not comparable. The highlevel structures of the proofs in both [17] and [15] however are very close to the highlevel structure of the present proof. The argument which forms the highlevel structure of all of these proofs was used by Hopcroft, Paul, and Valiant (see [13]) in 1977. In this paper we will use the outline of the proofs in [17] as a model while giving the sketch of the present proof. There are also nonlinear lower bounds for nonuniform models of computations see [3], [10], [11], but the

results are also incomparable to the present ones and even the high level structures of the proofs are completely different.

We can say that the difference between these already existing lower bounds and the ones in the present paper and in [2] is that they are based on different properties of the computational models. Both in the case of the turing machine model, and in the models with small working memory, a lower bound proof is possible because of the organization of the memory, which in the second case includes the input. In both cases there is some restriction on the structure/use of the memory that is the crucial property used in the proof. In contrast, our present proofs, or the proofs in [2], are not based on properties of the memory structure or the memory access, but on properties of the set of arithmetic instructions. Therefore our results say something about the set of arithmetic operations multiplication, addition etc., which is used in the usual random access machines.

As an additional motivation we can say that solving several search problems, each within the framework of our theorem, frequently occurs as part of computational problems to be solved on a RAM. Of course our lower bound does not imply a lower bound for the solution for all of the search problems together, still it may show that we cannot hope for a fast solution by solving each of these search problems separately.

1.2 The formulation of the results

First we formulate our result about RAMs. For each positive integer n we define a von Neumann type machine N_n with word length n. (See also [5].) These machines have a common finite instruction set. Each instruction has a name, which is a natural number. We consider only the machines N_n for, say, $n > 10$, where such a name fits into a memory cell. The set of these names will be denoted by $\mathcal{I}$. A program P is a sequence from the elements of $\mathcal{I}$. When we say that the machine N_n executes the program P of length k, we mean that the machine starts to work from the state where the first k memory cells contains the elements of P in their natural order and the contents of the other memory cells are zeros. The total number of memory cells is restricted only by the address space, say, it is 2^n. The instruction set contains (i) arithmetic instructions: addition and multiplication modulo 2^n, the constants $0, 1, n, 2^{n-1}$, the unary function $\min\{2^x, 2^n - 1\}$, the binary functions $\lfloor x/y \rfloor$ with $\lfloor x/0 \rfloor = 0$, $\max(x, y)$, $\min(x, y)$, and the boolean vector operations $\wedge, \vee, \neg$ defined on $0, 1$ sequences of length n. (ii) read, write instructions, (iii) control transfer instructions, (iv) input/output instructions, (v) halt instruction.

Assume that c, k are positive integers. A program P will be called a c-size k-ary test, if $\texttt{length}(P) \leq c$, $k \leq c$ and for all positive integers $n > 10$, and for all integers $x_1, ..., x_k \in [0, 2^n - 1]$, the program P on machine N_n, at input $x_1, ..., x_k$ uses only the first c memory cells, and produces an output $P_n(x_1, ..., x_k) \in \{0, 1\}$. The time requirement of P on N_n is the smallest integer t such that for all integers $x_1, ..., x_k \in [0, 2^n - 1]$, the program P at input $x_1, ..., x_k$ provides an output in time at most t.

Theorem 1 *There exist an $\varepsilon > 0$, a positive integer c and a c-size binary test P, with time requirement at most c on each machine N_n, such that for all $c' > 0$, and for all c'-size*

unary tests Q the following holds. Suppose that for all sufficiently large positive integers n, and for all $a \in [0, 2^n - 1]$, the following two statements are equivalent:

(i) $\exists x \in [0, 2^n - 1]$, $P_n(x, a) = 0$,

(ii) $Q_n(a) = 0$.

Then for infinitely many positive integers n, the time requirement of Q on N_n, is at least

$$\varepsilon(\log\log n)^{\frac{1}{2}}(\log\log\log n)^{-1}$$

In other words, there exists a constant time test $P(x, a)$, depending on a parameter a, such that the question whether it has a solution in x or not, cannot be decided for all n by a constant size program Q which gets a as an input, even if the time used by Q on N_n can be as large as $\varepsilon(\log d)^{\frac{1}{2}}(\log\log d)^{-1}$, where $n = 2^d$. The theorem remains true even in the following stronger nonuniform version. Suppose that the sequence Q_n, $n = 1, 2, ...$ is a sequence of programs, and f, g are functions defined on the the set of natural numbers with real values. We say that the sequence Q_n is a family of unary tests with size bound f and time limit g, if for each sufficiently large n, Q_n is a program, that is, a sequence from the elements of $\mathcal{I}$, of length at most $f(n)$, and for each $a \in [0, 2^n - 1]$, Q_n, while running on the machine N_n at input a, gives a $0, 1$ output $Q_n(a)$ in time at most $g(n)$.

Theorem 2 *There exist an $\varepsilon > 0$, a positive integer c and a c-time binary test P, with time requirement at most c, such that for all families of unary tets Q_n, $n = 1, 2, ...$, with both size bound and time limit $\varepsilon(\log\log n)^{\frac{1}{2}}(\log\log\log n)^{-1}$ the following holds. For infinitely many positive integers n, there exists an $a \in [0, 2^n - 1]$, such that the following two statements are not equivalent:*

(i) $\exists x \in [0, 2^n - 1]$, $P_n(x, a) = 0$,

(ii) $Q_n(a) = 0$.

The proof of these theorems will be based on a theorem about the structures $\mathbf{M}_d$ described in the abstract. Our next goal is to formulate that result.

Definition. 1. The set of all natural numbers will be denoted by ω, that is, $\omega = \{0, 1, 2, \ldots\}$. Each natural number n is considered as the set of all natural numbers less than n, that is, $n = \{0, 1, \ldots, n-1\}$ and $0 = \emptyset$, $1 = \{\emptyset\}$, $2 = \{\emptyset, \{\emptyset\}\}$, etc.

2. Assume that $a, b \in \omega$, $b \geq 2$. The natural number a can be written in a unique way in the form of $\sum_{i=0}^{\infty} \alpha_i b^i$, where $\alpha_i \in \{0, 1, \ldots, b-1\}$ for $i \in \omega$. The integer α_i will be denoted by $\mathtt{coeff}_i(a, b)$. In other words $\mathtt{coeff}_i(a, b)$ is the ith "digit" of a in the numeral system with base b. We extend the definition of $\mathtt{coeff}_i(a, b)$ for negative integers i as well, by $\mathtt{coeff}_i(a, b) = 0$ for all $i = -1, -2, \ldots$.

3. $\mathcal{M}$ will denote a first-order language with equality, which does not contain any other relation symbols, and contains the following function and constant symbols. (We consider constant symbols as 0-ary function symbols as well.)

Constant symbols: $\mathbf{0}, \mathbf{1}, -\mathbf{1}, \mathbf{n}$.

Unary function symbol: $\mathcal{N}$, $\mathbf{p}$, ($\mathcal{N}$ stands for "*n*egation", $\mathbf{p}$ stands for "*p*ower").

Binary function symbols: $+$, $\times$, $\div$, max, min, $\cap$.

4. Since $\mathcal{M}$ is a language with equality, in the interpretations defined below, we do not define the interpretation of the relation "=", it is already given as "equality". Assume

that $d \in \omega = \{0, 1, 2, \ldots\}$ and $n = 2^d$. $\mathbf{M}_d$ will denote the following interpretation of the language $\mathcal{M}$: $\mathtt{universe}(\mathbf{M}_d) = \{0, 1, \ldots, 2^n - 1\} = 2^n$ and for all $x, y, z \in \mathtt{universe}(\mathbf{M}_d)$,
($\mathbf{M}_d \models +(x, y) = z$) iff $x + y \equiv z \pmod{2^n}$,
($\mathbf{M}_d \models \times(x, y) = z$) iff $xy \equiv z \pmod{2^n}$,
($\mathbf{M}_d \models \mathbf{p}(x) = z$) iff $z = \min\{2^x, 2^n - 1\}$,
($\mathbf{M}_d \models z = \div(x, y)$) iff $(y \neq 0 \wedge z = \lfloor x/y \rfloor) \vee (y = 0 \wedge z = 0)$
($\mathbf{M}_d \models z = \mathbf{0}$) iff $z = 0$,
($\mathbf{M}_d \models z = \mathbf{1}$) iff $z = 1$,
($\mathbf{M}_d \models z = \mathbf{n}$) iff $z = n$,
($\mathbf{M}_d \models z = -\mathbf{1}$) iff $z = 2^n - 1$,
($\mathbf{M}_d \models z = \max(x, y)$) iff $z = \max\{x, y\}$,
($\mathbf{M}_d \models z = \min(x, y)$) iff $z = \min\{x, y\}$,
($\mathbf{M}_d \models z = x \cap y$) iff
$\mathtt{coeff}_i(z, 2) = \min(\mathtt{coeff}_i(x, 2), \mathtt{coeff}_i(y, 2))$ for $i = 0, 1, \ldots, n - 1$,
($\mathbf{M}_d \models z = \mathcal{N}(x)$) iff $\mathtt{coeff}_i(z, 2) = 1 - \mathtt{coeff}_i(x, 2)$ for $i = 0, 1, \ldots, n - 1$.

We will call the interpretations $\mathbf{M}_d$, $d \in \omega$ of $\mathcal{M}$ the standard interpretations of $\mathcal{M}$.

5. Motivated by the definition of the standard interpretations we will use the following notation as well when we use the functions symbols of $\mathcal{M}$: $+(x, y) = x + y$, $\times(x, y) = x \times y = xy$, $\mathbf{p}(x) = 2^x$. Generally we will use this notation only if it is clear from the context the we mean the function symbol interpreted in a structure $\mathbf{M}_d$, otherwise $x + y, xy, 2^x$ retain their usual meaning as operations among real numbers. Although the relation $\leq$ is not included in the language $\mathcal{M}$ sometimes we will write $\mathbf{M}_d \models a \leq b$ as an abbreviation for $\mathbf{M}_d \models a = \min(a, b)$.

6. When we use the function symbols of $\mathcal{M}$ we will write $x - y$ for $x + (-\mathbf{1})y$ and $-y$ for $(-\mathbf{1})y$.

7. Assume that $F(x, y)$ is a term of $\mathcal{M}$ and $G = \langle G_d(y) \mid d \in \omega \rangle$, $d \in \omega$ is a sequence of terms of $\mathcal{M}$. We will say that the sequence G decides whether there exists a solution for F, if for all sufficiently large $d \in \omega$, we have

$$\mathbf{M}_d \models \forall y, [G_d(y) = \mathbf{0} \leftrightarrow \exists x, F(x, y)]$$

8. The length of a term τ of a first-order language $\mathcal{L}$ is the total number of symbols (counted with multiplicity) in it. This number will be denoted by $\mathtt{length}(\tau)$. The depth of the term τ, that will be denoted by $\mathtt{depth}(\tau)$, is the maximal number of nestings of the function symbols in it. □

Theorem 3 *There exists an $\varepsilon > 0$ and a term $F(x, y)$ of $\mathcal{M}$ such that the following holds. Assume that $G = \langle G_d(y) \mid d \in \omega \rangle$ is a sequence of terms of $\mathcal{M}$ such that G decides whether there exists a solution for F. Then for infinitely many $d \in \omega$, the depth of G_d is at least $\varepsilon(\log d)^{\frac{1}{2}} = \varepsilon(\log \log n)^{\frac{1}{2}}$, where $n = 2^d$.*

The depth of a propositional formula is the maximal number of nestings of function symbols and boolean operations together. It is easy to show that there exists a $c \in \omega$ such that for each propositional formula $P(x_1, ..., x_k)$ of $\mathcal{M}$, there exists

a term $F(x_1, ..., x_k)$ of $\mathcal{M}$, such that $\mathtt{depth}(F) \leq c\mathtt{depth}(P)$, and for all $d \in \omega$, $\mathbf{M}_d \models \forall x_1, ..., x_k, P(x_1, ..., x_k) \leftrightarrow F(x_1, ..., x_k) = 0$. This implies the following equivalent form of Theorem 3. The theorem says that over the structures $\mathbf{M}_d$ quantifier elimination is not possible in a strong quantitative sense.

Theorem 4 *There exists an $\varepsilon > 0$ and an existential formula $\psi(y)$ of $\mathcal{M}$ containing a single existential quantifier, such that, if $P_d(y)$, $d \in \omega$ is a sequence of propositional formulas and for all $d \in \omega$, $\mathbf{M}_d \models \forall y, \psi(y) \leftrightarrow P_d(y)$, then for infinitely many $d \in \omega$, $\mathtt{depth}(P_d) \geq \varepsilon(\log d)^{\frac{1}{2}}$.*

Weaker versions of Theorems 3 and Theorem 4 were proved in [2]. E.g., the weaker version of Theorem 3 is equivalent to the statement that if $G = \langle G_d \mid d \in \omega \rangle$ is a sequence of terms of $\mathcal{M}$ such that G decides whether there exists a solution for F then there exists a sequence $d_0, d_1, ...$ of natural numbers such that $\lim_{i\to\infty} \mathtt{depth}(G_{d_i}) = \infty$. The motivation for the formulation of Theorem 3, apart from the fact the it is used in the proofs about RAMs, is that it is a natural continuation of a long chain of results in mathematics which say that certain search problems, e.g., equations, cannot be solved by the same operations as were used in their formulation. For example Galois' theorem about the unsolvability of equations of degree five by algebraic operations belong to this category. (Sevaral other examples of this nature is described [2]). In the present case we give such a Theorem in a quantitative form by giving a lower bound on the depth on the algebraic expression which could compute a solution.

There are many important first-order structures where quantifier elimination is possible (e.g., the field of real numbers, field of complex numbers) and also where it is not possible (e.g., Peano Arithmetic). Theorem 4 gives us an example where quantifier elimination is not possible, moreover the statement is true in a quantitative form. The particular choice of the structures involved in the theorem is motivated by the connection with random access machines.

The first-order properties of structures similar to the structures $\mathbf{M}_d$ were studied for a long time in the theory of Fragments of Peano Arithmetic. In that case however the set of operations defined by function symbols is usually more restricted (although sometimes exponentiation in some restricted form is allowed). In that theory the basic structure is usually not a finite set as in the case of $\mathbf{M}_d$, but rather an infinite initial segment of a nonstandard model of Peano Arithmetic, which is closed under addition, multiplication and sometimes under the operation $x^{\lfloor \log y \rfloor}$. The advantage of this is that instead of speaking about an infinite sequence of structures the results can be formulated in a single structure. A similar solution may be possible in our case too, but then the connections with RAMs would be much more complicated than with the present formulation of the result. Namely, it would be difficult to maintain a fixed upper bound on the sizes of memory cells since each multiplication would double the number of bits in a word.

The following theorem shows that the lower bounds that we proved in the four theorems described above are probably very far from the truth.

Definition. Assume that $F(x, y)$ is a term of $\mathcal{M}$. We describe a problem in NP, which will be called "the solution of the equation $F(x, a) = 0$ in x".

If the size of he problem is n, where we assume that $n = 2^d$, then the input of the problem is an integer $a \in 2^n$. An integer $b \in \{0, 1, \ldots, 2^n - 1\}$ is a solution of the problem if $\mathbf{M}_d \models F(b, a) = \mathbf{0}$, where $n = 2^d$. $\square$

Theorem 5 *There exists a term $F(x, y)$ of $\mathcal{M}$, such that the solution of the equation $F(x, a) = 0$ in x is an NP-complete problem.*

The following two theorems are important steps in the proof of Theorem 3 and Theorem 4.

If $t \in \omega$ then the ith 2^{2^t}-ary digit of a natural number a will be denoted by $a[i, t]$, that is, $a = \sum_{i=0}^{\infty} a[i, t]2^{i2^t}$. Assume that $d, t \in \omega$, $d \geq t$. We may consider the elements of $\mathbf{M}_d$ as 2^{d-t} dimensional vectors whose components are in $\mathbf{M}_t$, namely the integer $a \in \mathbf{M}_d$ will represent the vector $\langle a[0, t], a[1, t], ..., a[2^{d-t} - 1, t]\rangle$, that is the 2^{2^t}-ary digits of a are the components of the vector represented by a.

Let $\mathbf{f}$ be a k-ary function symbol of $\mathcal{M}$ for some $k \in \{0, 1, 2\}$. For all $d, t \in \omega$ with $d \geq t$, we define a k-ary function $\mathbf{f}_{d,t}$ on the universe of $\mathbf{M}_d$ in the following way. Assume that $d, t \in \omega$ is fixed with $d \geq t$ and $a_0, ..., a_{k-1} \in \mathbf{M}_t$. Then $\mathbf{f}_{d,t}(a_0, ..., a_{k-1})$ is the unique element $b \in \mathbf{M}_d$ with the property that for all $i \in 2^{d-t}$, we have $\mathbf{M}_t \models \mathbf{f}(a_0[i, t], ..., a_{k-1}[i, t]) = b[i, t]$. In other words we consider each element of $a \in \mathbf{M}_d$ as a vector $\langle a[0, t], ..., a[2^{d-t} - 1, t]\rangle$ and perform the operation $\mathbf{f}$ component-wise in $\mathbf{M}_t$. The following theorem states that, if $\mathbf{f}$ is a function symbol and $\mathbf{f} \notin \{\times, \div, \mathbf{p}\}$, then the function $\mathbf{f}_{d,t}$ can be defined by an existential formula in $\mathbf{M}_d$, that is, vector operations apart from the exceptions of multiplication, division, and exponentiation are existentially definable.

Theorem 6 *Assume that $\mathbf{f}$ is a k-ary function symbol of $\mathcal{M}$ for some $k \in \{0, 1, 2\}$ and $\mathbf{f} \notin \{\times, \div, \mathbf{p}\}$. Then there exists an existential first-order formula $\psi(x_0, ..., x_{k-1}, y, z)$ of $\mathcal{M}$ such that for all $d, t \in \omega$ with $d \geq t$, and for all $a_0, ..., a_{k-1}, b \in \mathbf{M}_d$, the following two conditions are equivalent:*

(i) $\mathbf{f}_{d,t}(a_0, ..., a_{k-1}) = b$,

(ii) $\mathbf{M}_d \models \psi(a_0, ..., a_{k-1}, b, t)$.

For the exceptional function symbols $\times, \div, \mathbf{p}$ we do not know whether the statement in Theorem 6 holds. We may define the vector operations for these function symbols too in a somewhat larger structure $\mathbf{M}_v$ by an existential formula ψ, if $v \geq t + c(d - u)$, where c is a sufficiently large constant.

Theorem 7 *Assume that $\mathbf{f}$ is a k-ary function symbol of $\mathcal{M}$ for some $k \in \{0, 1, 2\}$. Then there exists a $c \in \omega$ and an existential first-order formula $\psi(x_0, ..., x_{k-1}, y, z, w)$ of $\mathcal{M}$, such that for all $d, t \in \omega$ with $d \geq t$, and for all $a_0, ..., a_{k-1}, b \in \mathbf{M}_d$, if $v \in \omega$, $v \geq t + c(d - t)$, then the following two conditions are equivalent:*

(i) $\mathbf{f}_{d,t}(a_0, ..., a_{k-1}) = b$,

(ii) $\mathbf{M}_v \models \psi(a_0, ..., a_{k-1}, b, d, t)$.

This theorem motivates the following definition. Assume that for all $d, t \in \omega$ with $d \geq t$, $F_{d,t}(x_0, ..., x_{i-1})$ is an i-ary function defined on $\mathbf{M}_d$ and with values in $\mathbf{M}_d$. We will say that the family of functions $F = \langle F_{d,t} \mid d, t \in \omega, d \geq t \rangle$ is polynomially existential in $\mathbf{M}$ if there exist a $c \in \omega$ and an existential first-order formula $\psi(x_0, ..., x_{i-1}, y, z, w)$ of $\mathcal{M}$ such that for all $d, t \in \omega$ with $d \geq t$ and for all $a_0, ..., a_{i-1}, b \in \mathbf{M}_d$ if $v \in \omega$, $v \geq t + c(d-t)$ then the following two conditions are equivalent:

(i) $F_{d,t}(a_0, ..., a_{k-1}) = b$,

(ii) $\mathbf{M}_v \models \psi(a_0, ..., a_{k-1}, b, d, t)$.

Therefore Theorem 7 says that for each function symbol $\mathbf{f}$ of $\mathcal{M}$ the family of functions $\mathbf{f}_{d,t}$, $d, t \in \omega$, $d \geq t$ is polynomially existential. We use the word polynomially because of the following reason. In Theorem 7 we consider the elements of $\mathbf{M}_d$ as vectors with 2^{d-u} components, where each component is an element of $\mathbf{M}_t$. In the formula ψ we existentially quantify elements of $\mathbf{M}_v$ which can be considered as vectors with $2^{c(d-t)}$ components which are in $\mathbf{M}_t$. Therefore the number of components of the existentially quantified vectors is a polynomial of the number of component in the arguments of the function. This is true not only for Theorem 7 but in general for polynomially existential families. In addition to this, as the following theorem will show the notion of polynomially existential families of functions is closely related to the notion of polynomial time computation.

For the following definition recall that N_m is a random access machine with word length m and with 2^m memory cells. In case $m = 2^d$, for some $d \in \omega$, the machine can compute each $\mathcal{M}$ operation in $\mathbf{M}_d$ by a single instruction.

Definition. Suppose that $F = \langle F_{d,t} \mid d, t \in \omega, d \geq t \rangle$ is a family of k-ary functions, where each function $F_{d,t}$, $d, t \in \omega$, $d \geq t$ is a k-ary function defined on $\mathbf{M}_d$ with values in $\{0, 1\}$. We will say that the family F is polynomial time computable with respect to $\mathbf{M}$ if there exist a $\gamma_1 \in \omega$ and a program P for the family of RAMs N_n such the the following holds,

(1) *for all sufficiently large $d \in \omega$, for all $t \in \omega$ with $d \geq t$, and for all $a_0, ..., a_{k-1} \in \mathbf{M}_d$, the machine N_m, where $m = 2^d$, with program P and input $k, d, t, a_0, ..., a_{k-1}$, using only the first $2^{\gamma_1(d-t)}$ memory cells in time $2^{\gamma_1(d-t)}$ computes $F_{d,t}(a_0, ..., a_{k-1})$.*

We assume that at time 0 the program and the input is in the first $\texttt{length}(P) + 3 + k$ memory cells, the program is in the first $\texttt{length}(P)$ cells and the input $k, d, t, a_0, ..., a_{k-1}$ is in the next $3 + k$ cells in the given order. □

Remark. 1. Since d is sufficiently large we may assume that 2^{2^d} the total number of memory cells of N_m is larger than $2^{\gamma_1(d-t)}$ the number of memory cells required for the computation, and 2^{2^d} is also larger than $\texttt{length}(P) + k + 3$ the number of memory cells required for the input.

2. We stated the definition for functions with $0, 1$-values. In fact, we may allow any value in $\mathbf{M}_d$ or even a sequence of length 2^{d-t} in $\mathbf{M}_d$, and everything that we prove about this notion remains true. We will use however this notion in a nondeterministic setting where the $0, 1$-valued functions are sufficient for our purposes. □

Theorem 8 *Suppose that $F = \langle F_{d,t} \mid d, t \in \omega, d \geq t \rangle$ is a family of k-ary functions, where each function $F_{d,t}$, $d, t \in \omega$, $d \geq t$ is a k-ary function defined on $\mathbf{M}_d$ with values in $\{0, 1\}$. Assume further that the family F is polynomial time computable with respect to $\mathbf{M}$. Then the family F is polynomially existential in $\mathbf{M}$.*

2 Sketch of the proof of Theorem 3.

2.1 Overview

As we have mentioned already, a weaker version of Theorem 3 was proved in [2], namely it has been shown that if $G = \langle G_d \mid d \in \omega \rangle$ is a sequence of terms of $\mathcal{M}$ such that G decides whether there exists a solution for F then there exists a sequence $d_0, d_1, ...$ of natural numbers such that $\lim_{i \to \infty} \mathtt{depth}(G_{d_i}) = \infty$. We will refer to this theorem as Theorem **A**. The proof of Theorem **A** did not provide any unbounded function $f(x)$ such that we could conclude that for infinitely many d, the depth of G_d is at least $f(d)$. It seems that the lack of such a function f is a consequence of the nature of the indirect proof given in [2]. The paper [2] also described a generalized version of Theorem **A**, which essentially abstracted those properties of the structures $\mathbf{M}_d$ which were needed in the proof. For the present proofs these properties are not sufficient. (It is possible that the improved lower bounds hold for the generalized version of Theorem **A** and can be proved by different methods.) We have to go back to the original definition of the structures $\mathbf{M}_d$ in terms of its arithmetic operations, and formulate new additional properties which will be used in the proof of Theorem 3.

We start sketching the proof of Theorem 3 by comparing it to the proof of Paul, Pippenger, Szemerédi, and Trotter about the separation of deterministic and non-deterministic linear time computation on multitape turing machines (see [17]). We will refer to their theorem as the PPST Theorem. We will point out which are those steps in the proof of the PPST Theorem which has an analogue in the present paper.

The outline of the proof of the PPST Theorem is, roughly speaking, the following. The proof has three parts that we will call Collapsing, Simulation, and Diagonalization. The roles of these parts can be summarized this way.

Collapsing. This is an indirect argument. Assuming that the PPST theorem is not true it is shown that the alternating hierarchy of linear time computation on multitape turing machines is collapsing, that is, for each k there exists a c such that each computation with k alternation and time n can be also performed by a machine with no alternations and in time cn.

Simulation. It is shown, without the indirect assumption, that any computation performed by a multitape turing machine (without alternations) in time n, can be also performed on an alternating machine with four alternations in time $\varepsilon_n n$, where $\lim_{n \to \infty} \varepsilon_n \to 0$.

Diagonalization. Assume that the PPST theorem is not true. The Collapsing and Simulation results described above lead to a contradiction through a diagonalization argument.

First we describe what is the concept of "computation" in our case. We do not define a machine which performs the computation we only describe functions that we want to compute. We may think that the process of evaluating a term or a first-order formula is the computation. (The RAM model, described earlier, is not equivalent to this model of computation if the depth of the formulas can be larger than constant.) The analogue of non-alternating turing machine is the following. A term $\tau \in \mathcal{M}$ is given and an $n \in \omega$, $n = 2^d$ is fixed. We want to compute the function which assigns to each $a \in \mathbf{M}_d$ the truth value of $\mathbf{M}_d \models \tau(a) = \mathbf{0}$.

The analogue of a turing machine with k alternation is the following. A Σ_k or Π_k first-order formula φ of $\mathcal{M}$ is given and an $n \in \omega$, $n = 2^d$ is fixed. We want to compute the function which assigns to each $a \in \mathbf{M}_d$, the truth value of $\mathbf{M}_d \models \varphi(a)$.

The term τ and the formula φ in the "computations" described above will be taken from sets depending on n. Namely, let $\mathcal{T}_n$ be the set of all terms τ of $\mathcal{M}$ which can be computed by an algebraic circuit (whose gates perform $\mathcal{M}$-operations in $\mathbf{M}_d$, $n = 2^d$) of size at most $2^{d+\log d+3}$. $\mathcal{H}'_n$ will be a set containing only Σ_m formulas, where $m = c(d + \log d)^{\frac{1}{2}}$ for a constant c. (We will say more about it later.) $\mathcal{H}_n$ will be a similar but somewhat larger set of first-order formulas of $\mathcal{M}$ with the property that if we perform a constant number of boolean operations or variable changes on the elements of $\mathcal{H}'_n$ then we get an element of $\mathcal{H}_n$. With these definitions we can give a short description of the three parts of the present proof, which are analogues of the three parts in the proof of the PPST theorem.

Collapsing. Assuming that the theorem is not true we show that for each fixed $n = 2^d$ there exists a term $\tau(x, y) \in \mathcal{T}_n$ and there exists a function $\mathbf{g}$ (an analogue of the Gödel numbering) which assigns to each element of $\varphi \in \mathcal{H}_n$ an integer $\mathbf{g}(\varphi) \in \mathbf{M}_d$ such that if $q = \lfloor d + \log_2 d \rfloor$ then for all $a \in \mathbf{M}_d$, $\mathbf{M}_d \models \varphi(a) \leftrightarrow \mathbf{M}_q \models \tau(a, \mathbf{g}(\varphi)) = \mathbf{0}$.

Simulation. We show that for each $\tau \in \mathcal{T}_n$, there exists a $\lambda_\tau \in \mathcal{H}'_n$ such that for all $a, b \in \mathbf{M}_d$, $\mathbf{M}_d \models \lambda_\tau(a, b)$ is equivalent to $\mathbf{M}_q \models \tau(a, b) = \mathbf{0}$, where $q = \lfloor d + \log d \rfloor$.

Diagonalization. Using the Collapsing and Simulation statements we show that there exists a formula $\mu(x, y)$ of $\mathcal{H}_n$ such that for all $\varphi \in \mathcal{H}_n$, and for all $a \in \mathbf{M}_d$, $\mathbf{M}_d \models \varphi(a)$ iff $\mathbf{M}_d \models \mu(a, \mathbf{g}(\varphi))$, that is, the truth, at least for the formulas in $\mathcal{H}_n$, are definable in $\mathbf{M}_d$. This leads to a contradiction.

We give now a more detailed description of the various parts of the proof. We start with the diagonalization since it has the simplest proof.

2.2 Diagonalization.

This is similar to the argument in Gödel's incompleteness theorem or, more closely, to Tarski's proof about the non-definability of truth functions.

Starting with an arbitrary formula $\varphi(x) \in \mathcal{H}_n$ and the statement formulated in "Collapsing" we get a $\tau \in \mathcal{T}_n$ with $\mathbf{M}_d \models \varphi(a) \leftrightarrow \mathbf{M}_q \models \tau(a, \mathbf{g}(\varphi))$ for all $a \in \mathbf{M}_d$. It is important that τ does not depend on φ. Next by the "Simulation" statement we get, that there exists a first-order formula $\lambda_\tau(x, y) \in \mathcal{H}'_n$ for this particular τ. Clearly if $\mu(x, y) \equiv \lambda_\tau(x, y)$ then for all $\varphi \in \mathcal{H}_n$ and for all $a \in \mathbf{M}_d$, $\mathbf{M}_d \models \varphi(a)$ iff $\mathbf{M}_d \models \mu(a, \mathbf{g}(\varphi))$.

Now we apply this for $\varphi(x) \equiv \neg\mu(x,x)$. Since μ is in $\mathcal{H}'_n$, our assumptions about $\mathcal{H}_n$ imply that $\varphi \in \mathcal{H}_n$. With the choice $a{:=}\,\mathbf{g}(\varphi)$ we get $\mathbf{M}_d \models \varphi(\mathbf{g}(\varphi)) \leftrightarrow \mu(\mathbf{g}(\varphi),\mathbf{g}(\varphi))$, that is, we have $\mathbf{M}_d \models \neg\mu(\mathbf{g}(\varphi),\mathbf{g}(\varphi)) \leftrightarrow \mu(\mathbf{g}(\varphi),\mathbf{g}(\varphi))$ a contradiction.

2.3 Collapsing.

First we give the definitions of the sets $\mathcal{H}'_n$ and $\mathcal{H}_n$. Assume that φ is prenex first-order formula of $\mathcal{M}$. We form blocks from the quantifiers of φ, such that (a) each block is an interval of consecutive quantifiers of identical types, that is, existential or universal and (b) two consecutive quantifiers of identical type is always in the same block. Suppose that φ has k blocks and the number of quantifiers in the blocks are $\iota_1, ..., \iota_k$. We will say that the sequence $\langle \iota_1, ..., \iota_k \rangle$ is the quantifier pattern of φ. (We do not identify which are the universal and existential quantifiers.)

We describe now the sets $\mathcal{H}_n$, $\mathcal{H}'_n$. Assume that $M, j_1, ..., j_m$ are positive integers. The set of all prenex first-order formulas φ of $\mathcal{M}$ satisfying the following two conditions will be denoted by $\mathbf{L}(M, j_1, ..., j_m)$:

(i) if the quantifier pattern of φ is $\langle \iota_1, ..., \iota_k \rangle$ then $k \leq m$ and $\iota_i \leq j_i$ for all i=0,...,k-1.

(ii) if $\varphi \equiv Q_r x_r, ..., Q_1 x_1, P(x_r, ..., x_1)$, where $Q_r, ..., Q_1$ are quantifiers and P is a propositional formula of $\mathcal{M}$ then $\mathtt{length}(P(x_1, ..., x_r)) \leq M$, where $\mathtt{length}(P)$ is the number of symbols in P.

Let $\delta = \varepsilon(\log d)^{\frac{1}{2}}$, $m = \lfloor c\delta \rfloor$. The exact definitions of $\mathcal{H}'_n$, and $\mathcal{H}_n$ are too technical to describe them in this sketch, but we may think that they are essentially of the following form $\mathcal{H}_n = \mathbf{L}(c^\delta, c, c^2, ..., c^m)$, $\mathcal{H}'_n = \mathbf{L}(c_1^\delta, c_1, c_1^2, ..., c_1^m)$, where $c > 2$ and $c_1 > 2$ are constants, and c is sufficiently large with respect to c_1. The essential feature of these formulas are that there are upper bounds on the number of quantifier blocks, the lengths of the formulas, and the sizes of the quantifier blocks starting from c or c_1 can grow only exponentially.

Naturally the starting point of the collapsing argument is that, by the indirect assumption, if a first-order formula φ contains a subformula $\exists x, F(x,y) = \mathbf{0}$ then it can be replaced by the formula $G_d(y) = \mathbf{0}$, and by this replacement we have decreased the number of quantifiers in φ. Unfortunately it may happen that such a subformula does not exist. Indeed, if the prenex form of φ is $Q_1 y_1, ..., Q_k y_k, \exists x, F(x, y_1, ..., y_k) = \mathbf{0}$, where $Q_0, ..., Q_{k-1}$ are quantifiers, then for $k > 1$ the indirect assumption is not applicable since F depends on too many parameters. In this case however we may consider the formula not in $\mathbf{M}_d$ but in $\mathbf{M}_{d+r}$ for $r = \lceil \log_2 k \rceil$, where the sequence $y_1, ..., y_k$ from the elements of $\mathbf{M}_d$ can be encoded by a single element of $\mathbf{M}_{d+r}$. This is done in the proof of Theorem **A**, and can be done in the present case as well.

There is however another difficulty. The term $F(x,y)$ in the indirect assumption is of constant size and $n = 2^d$ can be arbitrarily large. Therefore the indirect assumption is not applicable if the size of $F(x,y)$ is not constant. Actually the definition of the set $\mathcal{H}'_n$ allows formulas whose sizes grow with n. This cannot be avoided since the terms G_d may have sizes growing with $n = 2^d$ so after a single application of the indirect assumption, when we replace $\exists x, F(x,y)$ by $G_d(y)$, we may get a formula containing a term of size

$\varepsilon(\log d)^{1/2}$. This problem did not arise in the proof of Theorem **A** since there the terms G_d were of constant sizes. (Another similar problem however arose since after we reduced $\mathbf{M}_d \models \varphi(a)$ to $\mathbf{M}_{d+c} \models \tau(a) = \mathbf{0}$, the size of term τ, although did not depend on d, but it still did depend on φ. The solution of that problem given in [2] is not applicable to the present case.)

The solution of the problem, caused by the non-constant size of a term F, is the main part of the proofs in this paper. For the solution we will use a lemma which says that the evaluation in $\mathbf{M}_t$ of an algebraic circuit C with $\mathcal{M}$-operations ($\mathcal{M}$-circuits) can be evaluated by an existential (or a universal) formula in $\mathbf{M}_v$, provided $v \geq t + c \log |C|$, where $c \in \omega$ is a sufficiently large constant. In other words the input-output relation of such a circuit can be defined by an existential formula. To give a rigorous formulation of this lemma we will encode each $\mathcal{M}$-circuit by two integers. (It is possible to encode the circuits by one integer, we use two integers only because it is more convenient.) We do this in the following way. We consider an $\mathcal{M}$-circuit as a directed graph whose nodes are the gates (and the input nodes) and are labeled with the name of the corresponding operations. For the sake of simplicity we assume now that the arity of each $\mathcal{M}$ operation is 2. At each node x which is not an input node there are exactly two incoming edges with tails, say y, z, one labeled with 0 the other labeled with 1. At x we perform an $\mathcal{M}$ operation assigned to x on the elements which are the outputs of the gates at nodes y and z.

Suppose that the $\mathcal{M}$-circuit C has m nodes, and the set of nodes is the set $\{0, 1, ..., m-1\}$. Then C can be described by three sequences. Sequence j for $j = 0, 1$ is defined in the following way. The ith element of sequence j is the tail of of the edge labeled by j whose head is the node i. (If there are no incoming edges at node i, that is, i is an input node then the ith element is 0). The definition of sequence 2: the ith elements of sequence 2 is a label which shows which $\mathcal{M}$ operation must be executed at node i, or whether node i is an input node. To encode the three sequences by two integers, first we choose the smallest integer d such that $m < 2^{2^d}$ and 2^{2^d} is also larger than the number of $\mathcal{M}$ operations. Then we encode the three sequences of length m by a single integer a with $3m$ digits in the 2^{2^d}-ary numeral system, such that the digits of a form the three sequences. This way the $\mathcal{M}$-circuit C is characterized by 2 integers the integer d that we denote by $\mathtt{Circ}_0(C)$ and the integer a that we denote by $\mathtt{Circ}_1(C)$. It is important that an $\mathcal{M}$-circuit C can be evaluated in any structure $\mathbf{M}_t$ with $t \in \omega$, but the encoding $\mathtt{Circ}_0(C)$, $\mathtt{Circ}_1(C)$ does not depend on the choice of the structure $\mathbf{M}_t$.

We also need a way the encode the input of the circuit. Assume that we want to evaluate an $\mathcal{M}$-circuit C in the structure $\mathbf{M}_t$ for some $t \in \omega$, and the number of input nodes of C is k and the input is the sequence $a_0, ..., a_{k-1} \in \mathbf{M}_t$. Then we encode this input with the single integer $\mathtt{enc}_{k,t}(a_0, ..., a_{k-1}) = \sum_{i=0}^{k-1} a_i 2^{i2^t}$. Here the arithmetic operations are performed as among the integers so the sum is not necessarily in $\mathbf{M}_t$.

Now we can formulate the lemma which says that the input output relation of a $\mathcal{M}$-circuit can be defined by an existential (or universal) formula of $\mathcal{M}$ in a not too large structure $\mathbf{M}_v$.

Circuit Simulation Lemma. (See Lemma 57) *There exists an existential formula*

$\varphi(x_0, ..., x_4)$ of $\mathcal{M}$ with the following property. For all sufficiently large $c \in \omega$, for all $\mathcal{M}$-circuits C with k inputs, and for all $t, v \in \omega$, if $v \geq t + c \log |C|$ then for all $a_0, \ldots, a_k, b \in \mathbf{M}_t$, we have that $\mathtt{Circ}_0(C) \in \mathbf{M}_v$, $\mathtt{Circ}_1(C) \in \mathbf{M}_v$, $\mathtt{enc}_{k,t}(a_0, \ldots, a_{k-1}) = \sum_{i=0}^{k-1} a_i 2^{i2^t} \in \mathbf{M}_v$, and

$$\mathbf{M}_t \models C(a_0, \ldots, a_{k-1}) = b \quad \leftrightarrow \quad \mathbf{M}_v \models \varphi(\mathtt{enc}_{k,t}(a_0, \ldots, a_{k-1}), b, t, \mathtt{Circ}_0(C), \mathtt{Circ}_1(C))$$

The lemma only states the existence of an *existential* formula with the required property, but if we can define a function with an existential formula then we can also define it by a *universal* formula by simply saying, that the function does not take any other values.

The smallest possible v guaranteed by the lemma namely $v = t + c \log |C|$ has the following significance. Let $m = |C|$. Then the input of the circuit is a sequence of length at most m from the elements of $\mathbf{M}_t$. The elements of $\mathbf{M}_v$ can be considered as sequences of length $2^{v-t} = m^c$ from the elements of $\mathbf{M}_t$. That is, the lemma says that if we are allowed to quantify existentially sequences from $\mathbf{M}_t$ whose length is a polynomial in m then we can define the input-output relation of the circuit C. We will prove this by showing the input-output relation of any computation done in time polynomial in m, can be defined in $\mathbf{M}_v$ by an existential formula, provided that the computation is done on a RAM with word length 2^t. (That is, each word is an element of $\mathbf{M}_t$.) If t is so small the with words of length t we cannot address m memory cells then the computation with time polynomial in m is done on a turing machine.

Now we may return to the sketch of the "Collapsing" part of the proof, which was interrupted because we needed a tool (the Circuit Simulation Lemma) to handle the problem with the size of the terms in the formula φ. Assume now that the first-order formula φ contains a propositional formula $H(x_1, ..., x_{k-1}) = 0$ whose size depends on d. The Circuit Simulation Lemma with $F := H$ makes it possible to replace the formula $H(x_1, ..., x_{k-1}) = 0$ in φ by an existential or universal formula ψ of constant size. Since the new quantifier can be included in the previous quantifier block, the number of blocks is not growing.

After these changes in φ we will get a formula φ' which is equivalent to φ (at least in a larger structure $\mathbf{M}_v$). The formula φ' contains a subformula of the form $\exists x, F(x, y)$. By the indirect assumption this can be replaced by a formula $G(y) = 0$ and this way we decreased the number of quantifier changes in φ. (The formula φ' is not in prenex form, because of the encoding problems, but after the replacement we take it to prenex form again.)

After repeated use of the Circuit Simulation Lemma we have a sequence of formulas $\varphi = \varphi_0, \varphi_1, ..., \varphi_k$ and a sequence of integers $d = v_0, v_1, ..., v_k$ such that the number of quantifier blocks in the formulas φ_i is strictly decreasing with i, and for all $i = 0, 1, ..., k$ we have the following: for all $a \in \mathbf{M}_d$, $\mathbf{M}_d \models \varphi(a)$ iff $\mathbf{M}_{v_i} \models \varphi_i(a_i, \mathbf{g}_i(\varphi))$. The integer $\mathbf{g}_i(\varphi)$ encodes the parameters of the formulas φ_j, $j \leq i$, which arose at the applications of the circuit simulation lemma till that stage of the proof. Meanwhile we are maintaining reasonable bounds on v_i and $\mathtt{length}(\varphi_i)$. Let k be the smallest integer such that φ_k has a single block of quantifiers, that is, φ_k is either universal or existential. We may assume

that φ_k is existential otherwise we may work with its negation. We may also assume, based on the techniques mentioned earlier, that φ_k has a single existential quantifier. The formula φ was chosen from the set $\mathcal{H}_n$, where $n = 2^d$. Using the upper bounds in the definition of $\mathcal{H}_n$, on the number of quantifier blocks, their sizes and the length of φ, and using the upper bounds in the circuit simulation lemma, we get that that $v_k \leq d + \log d$. It is easy to see that we may assume that $v_k = \lfloor d + \log d \rfloor$. Since φ_k is of the form $\varphi_k(y) \equiv \exists x, F_0(x, y) = 0$ we may apply again the indirect assumption and get a term τ of $\mathcal{M}$ such that $\mathtt{depth}(\tau) \leq \varepsilon(\log d)^{\frac{1}{2}}$, and for all $a \in \mathbf{M}_d$ the following three statements are equivalent:

(i) $\mathbf{M}_d \models \varphi(a)$

(ii) $\mathbf{M}_{v_k} \models \varphi_k(a))$

(iii) $\mathbf{M}_{v_k} \models \tau(a, \mathbf{g}(\varphi)) = \mathbf{0}$, where $\mathbf{g}(\varphi) = \mathbf{g}_k(\varphi)$

which completes the sketch of the collapsing argument.

2.3.1 Sketch of the Proof of the Circuit Simulation Lemma.

The Circuit Simulation Lemma is an easy consequence of Theorem 8. Theorem 8 essentially says that the result of a computation done on the machine N_{2^d} with word length 2^d and in space and time polynomial in 2^{d-t}, where $d \geq t$, can be expressed by an existential formula of $\mathcal{M}$ in the structure $\mathbf{M}_v$, if $v \geq t + c(d - t)$ and c is a sufficiently large constant. We will apply this for the proof of the circuit simulation lemma with the parameter t given in the lemma and with $d := t + c'\mathtt{Circ}_0(C)$, where $c' > 0$ is a sufficiently large constant. It is an easy consequence of the definition of $\mathtt{Circ}_0(C)$ that $2^{\mathtt{Circ}_0(C)} \geq \frac{1}{2}\log|C|$. (See Lemma 56.) Therefore the evaluation of the circuit C in the structure $\mathbf{M}_t$ trivially can be done on the RAM N_{2^d}, since an element of $\mathbf{M}_t$ can be stored in a single memory cell, and also an element of C can be stored in a single memory cell, the operations of $\mathcal{M}_t$ can be performed in constant time, and the time and memory that can be used is at least a sufficiently large polynomial of $|C|$. So circuit evaluation (or checking that a guessed output is correct) is polynomial time computable with respect to $\mathbf{M}$, and Theorem 8 implies the existence of the formula with the properties required by the Circuit Simulation Lemma.

2.3.2 Motivation for Theorem 6 and 7.

Our final goal is to prove Theorem 8. Theorem 6 and 7 can be considered as steps in this proof. Therefore as a motivation we look again at the statement of Theorem 8 which says that the result of a computation done on the machine N_{2^d} with word length 2^d and in space and time polynomial in 2^{d-t}, where $d \geq t$, can be expressed by an existential formula φ of $\mathcal{M}$ in the structure $\mathbf{M}_v$, if $v \geq t + c(d - t)$ and c is a sufficiently large constant. If we just think about what can we quantify in such a formula φ Theorem 8 is not surprising. Indeed with such a formula φ we can existentially quantify a sequence from the elements of $\mathbf{M}_d$ which is of length $2^{c(d-t)}$, so which can be the whole history of the mentioned a polynomial time computation. The problem arises when we want to verify that a given sequence of elements of $\mathbf{M}_d$ is really a history of a computation. Such a verification have

to check that we get certain elements of the sequence by arithmetic operations from other elements. This is the main motivation for Theorem 6 and Theorem 7, since they say that with a certain type of fromula we can simultaneously perform a large number of arithmetic operations. There will be another problem too, namely performing parallel arithmetic operations as in theorems 6 and 7 is not enough, we also have to be able to rearrange the sequence somehow such that the operands of the arithmetic operations are at the right places. This problem arises at several different parts of the proofs so we will discuss it in more detail there.

We were speaking about sequences formed from the elements of a structure $\mathbf{M}_d$. If we want to speak about such a sequence in a larger structure $\mathbf{M}_v$, then we have to represent it there as a single element of $\mathbf{M}_v$. We will represent a sequence $a_0, ..., a_{k-1} \in \mathbf{M}_d$ by the integer $a = \sum_{i=0}^{k-1} a_i 2^{i2^d}$. Therefore the elements of the sequence $a_0, ..., a_{k-1}$ are the "digits" of the integer a in the 2^{2^d}-ary numeral system. The ith digit of the integer a in the 2^{2^d}-ary system will be denoted by $a[i, d]$, so in our example $a_i = a[i, d]$ for $i \in k$ and $a[i, d] = 0$ for all $i \geq k$. In particular the ith binary bit of the natural number a will be denoted by $a[i, 0]$.

Our first results clarify what can we define by propositional or first-order existential formulas with such sequences. These results are all preparations for the proofs of Theorem 6 and Theorem 7

2.3.3 Basic results about propositional and existential definitions in $\mathbf{M}_d$.

Let $R = \langle R_d \mid d \in \omega \rangle$ be a family of k-ary relations where for each $d \in \omega$, R_d is a k-ary relation on $\mathbf{M}_d$. We will say that the family R is uniformly propositional/existential in $\mathbf{M}$, if the there exists a propositional/existential formula φ of $\mathcal{M}$ such that for all $d \in \omega$ and for all $a_0, ..., a_{k-1} \in \mathbf{M}_d$, $R_d(a_0, ..., a_{k-1})$ is equivalent to $\mathbf{M}_d \models \varphi(a_0, ..., a_{k-1})$. A family of k-ary functions $f = \langle f_d \mid d \in \omega \rangle$ is uniformly propositional/existential if the family of relations $R_d(x_0, ..., x_{k-1}, y) \leftrightarrow R_d(x_0, ..., x_{k-1}) = y$ is uniformly propositional/existential. Of course if $f(x) = y$ can be defined by an existential formula then it also can be defined by the universal formula $\forall z, z = y \vee \neg(f(x) = y)$, so a uniformly existential function is also uniformly universal, so we could call it a uniformly Δ_1-function.

Note that the notion of uniformly existential is a stronger one than the notion polynomially existential relations defined earlier, since here we have to define the relation R_d in the structure $\mathbf{M}_d$ and not in a larger extension $\mathbf{M}_v$. It is easy to see that every uniformly existential family is also polynomially existential.

Assume that $f = \langle f_d \mid d \in \omega \rangle$ is a family of k-ary function. We will say that the term τ uniformly defines the family f, if for all $d \in \omega$, and for all $a_0, ..., a_{k-1}, b \in \mathbf{M}_d$, we have $f_d(a_0, ..., a_{k-1}) = b$ iff $\mathbf{M}_d \models \tau(a_0, ..., a_{k-1}) = b$.

This part of the proof builds up tools which make it possible to prove about more and more specific families of functions and relations that they are uniformly propositional or existential or uniformly can be defined by a term. Frequently the proof is only the simple application of one or two arithmetic operations of $\mathcal{M}$. For example if we consider and element a of $\mathbf{M}_d$ as a $0, 1$ sequences of length 2^d, formed from its binary bits, that

is, a is represented by the sequence $\langle a[0,0], a[1,0], ..., a[2^d-1,0]\rangle$, then we can perform boolean operations component-wise on these sequences. Moreover we may also shift such a seqeunce by a given amount in either direction using a term. That is, there exists a term σ such that for all $a \in \mathbf{M}_d$, $i \in 2^d$ and we get $\sigma(a,i)$ from a by shifting a with i places toward the more significant digits (and putting zeros into the empty places). The term $\sigma(a,i) = a\mathbf{p}(i)$ (in this case $\mathbf{p}(i) = 2^i$) is good for this purpose. If we want to shift a in the other direction then we can use the term $\div(a, \mathbf{p}(i))$.

For each $d, t \in \omega$ we will denote by $e_{d,t}$ the unique element of $\mathbf{M}_d$ with $e_{d,t}[i,t] = 1$ for all $i \in 2^{d-t}$. There exists a term τ of $\mathbf{M}_d$ such that for all $d, t \in \omega$, with $d \geq t$, $\mathbf{M}_d \models \tau(t) = e_{d,t}$. For the proof of this fact we have to use only the closed form of the sum of a finite geometric series. (See Lemma 13.)

Using these simple facts, about the binary component-wise boolean operations, about the various types of shifts and about the element $e_{d,t}$ we already can prove about more interesting functions that they are uniformly propositional or existential. A trivial but very important observation is the following. Let $\mathcal{B}(x_0, ..., x_{k-1})$ be a boolean expression with k-variables and let $a_0, ..., a_{k-1} \in \mathbf{M}_d$.

(2) *Then the relation R_d defined by $\forall i \in 2^d, \mathcal{B}(a_0[i,0], ..., a_{k-1}[i,0])$ is propositional.*

Indeed, if the term τ is built up from the $\mathcal{M}$ operations, $\cap$ and $\mathcal{N}$ the same way as $\mathcal{B}$ from the boolean operations $\wedge$ and $\neg$, then $R_d(a_0, ..., a_{k-1})$ holds iff $\mathbf{M}_d \models \tau(a_0, ..., a_{k-1}) = -\mathbf{1}$, since all of the binary bits of $-\mathbf{1}$ is 1. This way we expressed a universal statement about the components of elements in $\mathbf{M}_d$ by a propositional formula. This elimination of universal quantifier will be very important in the proofs.

This argument about boolean expression can be mixed with the operation shift. As a result

(3) *we can express by a propositional formula a relation defined by*

$$\forall i \in 2^d, \mathcal{B}(a_0[i+j_0,0], ..., a_{k-1}[i+j_0,0], ..., a_0[i+j_{r-1},0], ..., a_{k-1}[i+j_{r-1},0])$$

where $\mathcal{B}$ is a boolean expression with rk variables, and $j_0, ..., j_{r-1}$ are integers.

If $u \leq d$ then with this type of propositional formula we can say that the sequences $a_i[0,0], ..., a_i[2^d-1,0]$, $i = 0, ..., l-1$ describe the history of a turing machine with a tape with 2^u cells, each containing a $0,1$ bit which works from time 0 till time $2^{d-u}-1$ and whose finite automaton $\mathcal{A}$, directing the movement of the head etc., has 2^{l-2}. states. The contents of the cells of the tape at time t, will be given by the sequence $a_0[t2^u,0], ..., a_0[t2^u+2^u-1,0]$. If at time t the head is a cell j for some $j \in 2^u$, then $a_1[t2^u+j,0] = 1$, and $a_1[t2^u+i,0] = 0$ for all $i \in 2^u$, $i \neq j$. Finally the state of the finite automaton $\mathcal{A}$ at time t will be determined by the $l-2$ bits $a_2[t2^u+j,0], ..., a_{l-1}[t2^u+j,0]$, where the head is at cell j at time t. (For all $i \in 2^u$, $i \neq j$ we have $a_2[t2^u+j,0] = ... = a_{l-1}[t2^u+j,0] = 0$.) It is easy to see that there exists a Boolean expression $\mathcal{B}$ as in statement (3), with $r = 6$,

$j_0 = -1$, $j_1 = 0$, $j_2 = 1$, $j_3 = 2^u - 1$, $j_4 = 2^u$, $j_5 = 2^{u+1}$, $k = l + 1$, $a_0{:=}\, a_0, ..., a_{l-1}{:=}\, a_{l-1}$, $a_{k-1}{:=}\, e_{d,u}$ such that

$$\forall i \in 2^d, \mathcal{B}(a_0[i + j_0, 0], ..., a_{k-1}[i + j_0, 0], ..., a_0[i + j_{r-1}, 0], ..., a_{k-1}[i + j_{r-1}, 0])$$

holds iff the sequence $a_0[2^u t + j, 0]$, $j \in 2^u$, $t \in 2^{d-u}$ is the history of a turing machine with the finite automaton $\mathcal{A}$, in the sense that at time t the content of `cell` number j is $a_0[2^u t + j, 0]$. The reason is that if at time t the head is at cell j, then the changes from time t to $t + 1$ may involve only the contents of cell $j - 1, j$ or $j + 1$ and the state of the head. Therefore the rule defined by the finite automaton $\mathcal{A}$ involves only the bits of $a_i[t2^u + j + \delta]$ and $a_i[(t + 1)2^u + j + \delta]$ for $i \in k$ and $\delta \in \{-1, 0, 1\}$ (not all of them are needed) and this can be expressed by a boolean expression $\mathcal{B}$. The role of the integer $e_{d,u}$ is that it signals if the head is at the end of the tape, where the rules of the head movement may be different than at other locations.

This argument is sufficient the prove the NP-completeness result but we also use it for other purposes. In the case of NP-completeness it must be aplied with $u = \lfloor d/c \rfloor$ where $c > 1$ is a constant. The fact that "to be a history of turing machine with a fixed finite automaton $\mathcal{A}$" is uniformly propositional in $\mathbf{M}$ implies that the input-output relation for the same turing machine is uniformly existential, if stated in the same structure $\mathbf{M}_v$, and naturally this remains true for the history of a nondeterministic turing machine. (If we are speaking about turing machines with tape length ℓ that are working till time T then the existential formula that defines the input/output relation is formulated in $\mathbf{M}_v$ where $v \geq \log_2 \ell + \log_2 T$.)

For the proof Theorem 6 we do not use turing machines, but the techniques are similar to the one that were used for the proof related to them. One important difference will, be that in the case of turing machines we needed only the binary bits, that is, $a[i, 0]$ of various elements $a \in \mathbf{M}_d$, while in the proof of Theorem 6 we will need that 2^{2^u}-ary digits, that is, $a[i, u]$ for some $u \leq d$. We do not give here an outline of the proof of Theorem 6 because it consists of several independent lemmas related to the various operations of $\mathcal{M}$. The only common idea in these result is the one that we have illustrated in the case of turing machines.

2.3.4 Sketch of the proof of Theorem 7

The statement of Theorem 7 follows from Theorem 6 if $\mathbf{f} \notin \{\times, \div, \mathbf{p}\}$. The most important case is $\mathbf{f} = \times$, once we have the theorem for $\mathbf{f} = \times$ the $\mathbf{f} = \div$ case is relatively easy. For $\mathbf{f} = \mathbf{p}$ we have a somewhat longer proof but it is conceptually simpler.

We sketch here the basic idea of the proof of Theorem 7 for $\mathbf{f} = \times$.

We have to show that there exists an existential formula $\psi(x_0, x_1, y, z, w)$ of $\mathcal{M}$ and a $c \in \omega$ such that for all $d, u \in \omega$ with $d \geq u$, and for all $a_0, a_1, b \in \mathbf{M}_d$, if $v \in \omega$, $v \geq u + c(d - u)$, then the following two conditions are equivalent:

(i) $\times_{d,u}(a_0, a_1) = b$,

(ii) $\mathbf{M}_v \models \psi(a_0, ..., a_{k-1}, b, d, u)$.

To get $\times_{d,u}(a,b)$ in $\mathbf{M}_d$ we want to use $\times(a,b)$ that is ab in $\mathbf{M}_d$. We want to get an element h of $\mathbf{M}_d$, such that $h[i,u] = a[i,u]b[i,u]$ for all $i \in 2^{d-u}$. The choice $h = ab$ is obviously not good since $(ab)[i,u]$ is a linear combination of various products $a[k,u]b[l,u]$. To separate the products $a[k,u]b[k,u]$ that we need from the products $a[i,u]b[j,u]$, $i \neq j$ that we do not need we replace a and b by two other integers $F_0(a)$ and $F_1(b)$ so that they have the same 2^{2^u}-ary digits as a and b only these digits are stretched out on longer intervals. We hope that this way all of the products $a[i,u]b[j,u]$ will contribute to different digits of $F_0(a)F_1(b)$. Let $s = 2^{d-u}$. We may try first $F_0(a) = \sum_{i=1}^{s-1} a[i,u]2^{is2^u}$, and $F_1(b) = b$, so the distance of the 2^{2^u}-ary $a[i,u]$ digits in $F_0(a)$ is s. The integer b is smaller than 2^{s2^u} therefore each product $a[k,u]b[l,u]$ will contribute to at most one digit of $F_0(a)F_1(b)$, if we disregard the carryover. The carryover however is a problem since a product $a[k,u]b[l,u]$ is a two digit 2^{2^u}-ary number so it contributes both to the $sk+l$th digit and the $sk+l+1$th digit of $F_0(a)F_1(b)$.

To avoid the complications caused by the carryover problem, we stretch out the sequence of digits of a by a factor of $2s$ and the sequence of digits of b by factor of 2. That is, we have $F_0(a) = \sum_{i=1}^{s-1} a[i,u]2^{2si2^u} \in \mathbf{M}_{q+(q-u)+1}$, $F_1(b) = \sum_{i=1}^{s-1} b[i,u]2^{2i2^u} \in \mathbf{M}_{q+1}$. Now the carryover is not a problem since we care about only the values of the digits of $F_1(a)F_1(b)$ at even numbered places, while the carryovers influence only digits at odd numbered places. Note here that the functions F_0, F_1 were defined by moving the 2^{2^u}-ary digits into new places. We will have to show that the functions F_0 and F_1 can be defined by an existential formula in $\mathbf{M}_v$, where $v \geq u + c(d-u)$. For the moment we accept that this can be done somehow and continue the computation of $\times_{d,u}$, but later we will return to this question.

We have that if $w = F_0(a)F_1(b)$ then $w < 2^{(2s^2+2s)2^u} \in \mathbf{M}_{v'}$, where $v' = u + 4(d-u)$ and for all $k \in s$, $(a[k,u]b[k,u])_{\mathbf{M}_u} = w[2ks+2k,u]$, where $(xy)_{\mathbf{M}_u}$ means that we have to take the product in $\mathbf{M}_u$, that is, modulo 2^{2^u}.

We define a function F_2 by $F_2(p) = \sum_{k=0}^{s-1} p[2sk+2k,u]2^{k2^u}$ for all $p \in \mathbf{M}_{v'}$. Clearly we have $(F_2(w))[k,u] = a[k,u]b[k,u]$. So we have shown that $F_2(F_0(a)F_1(b)) = \times_{d,u}(a,b)$. The function $F_2(p)$ is also defined by moving the 2^{2^u}-ary digits of the integer p to other places, and turning some of the digits into zeros. As in the case of the functions F_0, F_1 we have to show that F_2 can be defined by an existential formula in $\mathbf{M}_v$. Finally it is easy to prove that if all of the three functions F_0, F_1, F_2 are defined by an existential formula in $\mathbf{M}_v$, then their composition $F_2(F_0(a)F_1(b))$ can be also defined by an existential formula in $\mathbf{M}_v$.

Now we show that the functions F_i, $i = 0,1,2$ described above can be defined by an existential formula in $\mathbf{M}_v$ provided that $v \geq u + c(d-u)$ and $c \in \omega$ is a sufficiently large constant. Recall that for each $0,1,2$ the value $F_i(p)$ was defined in the following way. We took the 2^{2^u}-ary digits of p and replaced some of them by 0 and took the others to new places, to get the 2^{2^u}-ary form of $F_i(p)$. All of this, which digits must be replaced by zero, and where we put the remaining digits, was explicitly described in the sense that we could compute it in time polynomial in $s = 2^{d-u}$ by a turing machine which needed only the input s. Motivated by this we prove here a general statement which says that functions with this property are polynomially existential which will imply in our case that

F_i, $i = 0, 1, 2$ are existentially definable in $\mathbf{M}_v$ is c is a sufficiently large constant. Later we will need this result for the proof of Theorem 8 as well, where its very general nature will be fully used.

The result in a simple form which is sufficient for proving the required properties of F_i, $i = 0, 1, 2$ is the following.

Digit Relocation Lemma (See also Lemma 40) *Assume that $\lambda(x, y)$ is a function defined for all $x \in \omega$, $y \in x$ such that the value of λ is in the set $\{0, 1, ..., x\}$, and given the input x, y, $\lambda(x, y)$ can be computed by a turing machine in time and space polynomial in x. Then the family $R = \langle R_{d,u} \mid d, u \in \omega, d \geq u\rangle$ of binary relations is polynomially existential, where for all $d, u \in \omega$ with $d \geq u$ and for all $a, b \in \mathbf{M}_d$, $R_d(a, b)$ holds if for all $i \in 2^{d-u}$, $b[i, u] = a[\lambda(2^{d-u}, i), u]$.*

According to this lemma the integer b is defined in a way that its 2^{2^u}-ary digits are selected from the 2^{2^u}-ary digits of the integer a. The selection is made by a turing machine but without the knowledge of the integer a. According to the assumptions of the lemma the value of $\lambda(x, y)$ can be x. In this case if $\lambda(2^{d-u}, i) = 2^{d-u}$ then we get that $b[i, u] = a[2^{d-u}, u] = 0$, since $a < 2^{2^d}$. Therefore 0 is always among the digits of a which can be used as digits of b (this is important in the case of the functions F_j, $j = 0, 1, 2$). (In Lemma 40 we formulate a somewhat more general form of this result namely we allow λ depend on a parameter which is an element of $\mathbf{M}_d$ representing a $0, 1$ sequence of length 2^{d-u}.)

In the proof of the Digit Relocation Lemma we will construct the integer b from the integer a by constructing a sequence $\alpha_0 = a, \alpha_1, ..., \alpha_\nu = b$, where $\alpha_i \in \mathbf{M}_d$ and we get each α_{i+1} from α_i by one of the following operations $\eta_{i,\iota}$ defined below. In describing these operations we will consider an element w of $\mathbf{M}_d$ as the sequence $\langle w[0, u], w[1, u], ..., w[s - 1, u]\rangle$ of length $s = 2^{d-u}$ from the elements of $\mathbf{M}_u$. Therefore we define operations acting on such sequences and they induce a corresponding operations on $\mathbf{M}_d$ as well. For each $i \in s$, $\iota \in 4$ we define an operation $\eta_{i,\iota}$, which applied to the sequence $x = \langle x_0, ..., x_{s-1}\rangle \in (\mathbf{M}_u)^s$ gives the following:

$\eta_{i,0}(x) = \langle y_0, ..., y_{s-1}\rangle$, where for all $j \in \{0, 1, ..., s - 2\}\backslash\{i\}$, $y_j = x_j$, and $y_i = 0$. That is, we get $\eta_{i,0}(x)$ from x by replacing x_i with 0.

$\eta_{i,1}(x) = \langle y_0, ..., y_{s-1}\rangle$, where for all $j \in \{0, 1, ..., s-2\}\backslash\{i, i+1\}$, $y_j = x_j$, and $y_i = x_{i+1}$, $y_{i+1} = x_i$. That is, we get $\eta_{i,1}(x)$ from x by swapping x_i and x_{i+1}.

$\eta_{i,2}(x) = \langle y_0, ..., y_{s-1}\rangle$, where for all $j \in \{0, 1, ..., s - 2\}\backslash\{i\}$, $y_j = x_j$, and $y_i = x_{i+1}$. That is, we get $\eta_{i,0}(x)$ from x by replacing x_i with x_{i+1}.

$\eta_{i,3}(x) = x$ that is the sequence remain unchanged. (In the detailed proof this operation will be missing because we will reach the same effect in a different way.)

Therefore our assumption is that a turing machine computes in polynomial time a sequence of pairs $\langle i_m, \iota_m\rangle$, for $m = 0, 1, ..., \nu-2$ and $\alpha_{m+1} = \eta_{i_m,\iota_m}\alpha_m$ for $m = 0, 1, ..., \nu-2$. In other words

$$b = \eta_{i_{\nu-2},\iota_{\nu-2}}(\ldots \eta_{i_0,\iota_0}(a)\ldots)$$

To show that this whole construction is uniformly existential we need a turing machine, in some generalized sense, which can perform the operations $\eta_{i,\iota}$ if the sequence $x = \langle x_0, ..., x_{s-1}\rangle$ is the sequence of contents of the cells. More precisely we will consider a

turing machine $\mathcal{T}$ with a fixed tape length $s = 2^{d-u}$ such that each cell contains a pair $\langle \delta, w \rangle$, where δ is $0,1$-sequence $\delta = \langle \delta_0, ..., \delta_{k-1} \rangle$ of length k, where k is a constant and $w \in \mathbf{M}_u$. The finite automaton $\mathcal{A}$ directing the head movement and the changes in the contents of the cell from time t to time $t+1$ works in the following way. If the head is at time t at cell j whose content is the pair $\langle \delta, w \rangle$ $\delta \in \{0,1\}_k$, $w \in \mathbf{M}_u$ then the input of the finite automaton $\mathcal{A}$ is δ, that is, the finite automaton simply does *not* see the element w of $\mathbf{M}_u$. Suppose that at time t the content of cell j is $\langle \delta^{(t)}, w_{t,j} \rangle$. We will denote the sequence $\langle w_{t,0}, ..., w_{t,s-1} \rangle$ by W_t. (In the detailed proof we do not allow the cells to contain elements in $w \in \mathbf{M}_u$. We let only the turing machine compute the sequence of operations and then execute the operations on sequences of elements from $\mathbf{M}_u$, and show that both steps are existentially definable. The two versions has the same basic idea, and the one that we sketch here is perhaps more intuitive, but we need the version of turing machines that we describe in the detailed proof for other purposes as well.)

Suppose that the head is at cell j at time t. Then depending on the input of $\mathcal{A}$ described above, it gives an output which consists of three different things:

(i) $\mathcal{A}$ directs the head either to change the content of cell j or leave it unchanged,

(ii) $\mathcal{A}$ directs the head to stay at cell j or to move either to cell $j+1$ or to cell $j-1$ (if the destination cell does not exist then the head does not move)

(iii) $\mathcal{A}$ also give as an output an integer $\iota \in \{0,1,2,3\}$. If the head is at time t at cell $s-1$ then $W_{t+1} = W_t$. If the head is is at time t at cell i, where $i \neq s-1$ then $W_{t+1} = \eta_{i,\iota}(W_t)$.

This completes the definition of the turing machine $\mathcal{T}$ that we will call a generalized turing machine so the word turing machine in itself will mean a turing machine in its original sense. If the finite automaton $\mathcal{A}$ and its initial state at time 0 and the contents of the cells at time 0 are given, the rules described above uniquely determine the history of the generalized turing machine $\mathcal{T}$. We will consider a generalized turing machine $\mathcal{T}$ of this type where $W_0 = \langle a[0,u], ..., a[s-1,u] \rangle$ and the generalized turing machine determines the type (iii) output of the automaton $\mathcal{A}$ in a way that $W_{s^\gamma - 1} = \langle b[0,u], ..., b[s-1,u] \rangle$. Since the function λ is computable in time polynomial in s, such a generalized turing machine exists if $\gamma \in \omega$ is a sufficiently large constant.

We claim that the same way as we have seen earlier with a turing machine, where each cell contained only a single $0,1$ bit, the history of the generalized turing machine also can be defined by an existential formula in $\mathbf{M}_v$, where $v = u + (\gamma+2)(d-u)$. This is true in the following sense.

When we proved the existential definability of the history of a turing machine, then we encoded the the $0,1$ bits occurring in the cells of the machine at various times as the binary bits of an integers $a_i \in \mathbf{M}_d$, $i \in l$ for a suitably chosen $d \in \omega$. Even when the integers a_i encoded the position of the head and the state of the head at each time, the integer l remained a constant. Now however the situation is changed since the contents of the cells are elements of $\mathbf{M}_u$ so we cannot encode them with a constant number of $0,1$, bit. To keep the advantages of the $0,1$-bits that can be the arguments of boolean expressions, and at the same time allow the encoding of sequences from the elements of $\mathbf{M}_u$, we will do the following. The history of the generalized turing machine with tape

length $\ell = 2^{d-u}$, which works till time $T = 2^{\gamma(d-u)}$ will be encoded by the integers in $\mathbf{M}_v$, where $v = u + (\gamma+1)(d-u)$. For example the δ_i in cell j at t time will be encoded by the $a_{0,i}[t\ell + j]$, where $a_{0,i} \in \mathbf{M}_v$. This way even for encoding $0,1$ bits we use the 2^{2^u}-ary form of integers. Therefor to define the history in an existential way we have to define the set of integers a in $\mathbf{M}_v$ whose 2^{2^u}-ary bits are all zeros and ones by an existential formula. This is not a problem since a has this property iff $a \leq_{v,u} e_{v,u}$, and Theorem 6 implies that the family of relations $\leq_{v,u}$ is uniformly existential.

We also need to encode the position of the head and the state of the finite automaton this will be done, as before, by the integers $a_1, a_2, ..., a_{l-1}$, but now using their 2^{2^u}-ary digits which are only ones and zeros. Consequently if at time t the head is at cell j, then $a_1[t\ell + j, u] = 1$, $a_1[t\ell + j', u] = 0$ for all $j' \in \ell \backslash \{j\}$. If $a_1[t\ell + j, u] = 1$ $a_2[t2^{d-u} + j, u], ..., a_{l-1}[t2^{d-u} + j, u]$ determines the state of the finite automaton at time t while $a_2[t2^{d-u} + i, 0] = ... = a_{l-1}[t2^{d-u} + i, 0] = 0$ for all $i \neq j$.

In the generalized turing machine the content of a cell is a pair $\langle \delta, w \rangle$ where the content of each cell is a $0,1$-sequence $\delta = \langle \delta_0, ..., \delta_{k-1} \rangle \in \{0,1\}^k$ and $w \in \mathbf{M}_u$. The history of the contents w of the cells will be represented by an integer $\beta \in \mathbf{M}_v$ such that if at time t the content of cell j is $w_{t,j}$ then $\beta[t2^{d-u} + j, u] = w_{t,j}$.

We define the family of $k + l + 1$-ary relations relation $R_{\mathcal{A}} = \langle R_{v,\mathcal{A}} \mid v \in \omega \rangle$ by: for all $v \in \omega$, and for all $a_{0,0}, ..., a_{0,k-1}, a_2, ..., a_{l-1}, \beta, d, u \in \mathbf{M}_v$, $R_{v,\mathcal{A}}(a_{0,0}, ..., a_{0,k-1}, a_2, ..., a_{l-1}, \beta, d, u)$ iff $v \geq d \geq u$, $v = u + (\gamma+1)(u-d)$ and the sequence $a_{0,0}, ..., a_{0,k-1}, a_2, ..., a_{l-1}, \beta$ describes a history of the turing machine with the finite automaton $\mathcal{A}$.

The proof of the fact that the family of relations $R_{\mathcal{A}}$ is uniformly existential is almost the same as in the case of (non-generalized) turing machines, since $a_{0,i}[r, u] \in \{0,1\}$ for $i \in k$, $r \in \ell T$ and $a_\nu[r, u] \in \{0,1\}$ for $\nu =, 1..., l-1$, $r \in \ell T$, we are able to express the the rules defining the turing machine by boolean expressions, provided that twe disregard the elements $w_{t,j} \in \mathbf{M}_u$. Instead of using the elements $w_{t,j}$ directly we will use the elements $D_{t,j,t,',j'}$ defined by $D_{t,j,t',j'} = 1$ if $w_{t,j} = w_{t',j'}$ and $D_{t,j,t',j'} = 0$ if $w_{t,j} = w_{t',j'}$. Since these elements take only $0,1$ values we will be able to express evrything about the working of the turing machine by boolean expressions. For the description of the rules defining the turing machine we need $D_{t,j,t',j'}$ only in the special cases $t' \in \{t, t+1\}$, $j' \in H_j = \{j-2, j-1, j, j+1, j+2\}$. In terms of the integer β this means that we need to know the boolean values of the statements $\beta[t2^{d-u} + j, u] = \beta[t'2^{d-u} + j']$ for $t' \in \{t, t+1\}$, $j' \in H_j$. We define an element $\beta_{\xi,\eta} = 2^{\eta + \xi(d-u)2^u} \in \mathbf{M}_v$, for $\xi \in \{0,1\}$, $\eta \in H_0$. We get that the sequence of 2^{2^u}-ary digits of $\beta_{\xi,\eta}$ by shifting the digit sequence of β toward the more significant digits (for negative values of η it means shifting to the opposite direction.) As we have seen for all relevant values of ξ, η there exists a term $\tau_{\xi,\eta}$ such that $\mathbf{M}_v \models \beta_{\xi,\eta} = \tau_{\xi,\eta}(\beta)$. Therefore in the existential formula that will define the relation $R_{d,\mathcal{A}}$ in $\mathbf{M}_v$ we can use the integers $\beta_{\xi,\eta}$, $\xi \in \{0,1\}$, $\eta \in H$. Therefore we get the required $0,1$-bits $D_{t,j,t',j'}$, $t' \in \{t, t+1\}$, $j' \in H_j$ as the 2^{2^u}-ary digits of the integers $\rho_{\xi,\eta,\xi'\eta'}$, where $\rho_{\xi,\eta,\xi',\eta'}$, $\xi, \xi' \in \{0,1\}$, $\eta, \eta' \in H_0$ is defined by

$$\mathbf{M}_v \models \rho_{\xi,\eta,\xi'\eta'} = \min_{v,u}(2^{2^v} - 1, \beta_{\xi,\eta} - \beta_{\xi',\eta'})$$

Since the operation $\min_{v,u}$ can be defined by an existential formula in $\mathbf{M}_v$ this is also true for the integers $\rho_{\xi,\eta,\xi'\eta'}$. Finally using the integers $\rho_{\xi,\eta,\xi'\eta'}$ and also the integers $a_{0,0}, ..., a_{0,k-1}, a_2, ..., a_{l-1}$ we are able to express the rules defining the turing machine in the form of

$$\forall i \in 2^{v-u}\mathcal{B}(a_{0,0}, ..., a_{0,k-1}, a_2, ..., a_{l-1}, \vec{\rho}_{\xi,\eta,\xi',\eta'})$$

where $\vec{\rho}_{\xi,\eta,\xi',\eta'}$ is the sequence of all expressions $\rho_{\xi,\eta,\xi',\eta'}$, $\xi, \xi' \in \{0,1\}$, $\eta, \eta' \in H_0$.

This implies, as we have seen in statement (2), that the relation $R_{v,\mathcal{A}}$ can be expressed by an existential formula in $\mathbf{M}_v$. Form this it is easy to get the statement of the Theorem 7, since we have to say only that there exists a history of the generalized turing machine with a given initial and final states.

2.3.5 Sketch of the proof of Theorem 8

The assumption of the theorem is that the functions $F_{d,t}$ are computable on the RAM N_{2_d} in time $2^{\gamma_1(d-t)}$ using only the first $2^{\gamma_1(d-t)}$ memory cells.

Such a computation can be performed also by a circuit C of size $2^{\gamma_2}(d-t)$ whose gates perform operations in $\mathbf{M}_d$, where γ_2 depends only on γ and C is given independently of the program and input of the machine $N_{2^{d-u}}$. Moreover the circuit C can be chosen in a way that it is computable by a turing machine $\mathcal{T}$ with the intput 2^{d-t} in time $2^{\gamma_3(d-t)}$ where γ_3 depend only on γ_1.

If we want to define existentially the $F_{d,t}(a_0, ..., a_{k-1})$ then we may guess what will be the outputs of the gates of C and then verify by an existential formula that these values are consistent with each other and the input. The verification has two steps. Suppose that at each gate G both the guessed output of gate G and given the (guessed) inputs of the gate G are given. We associate each gate with one of the natural numbers $0, 1, ..., |C| - 1$, and for example, the sequence of outputs is represented by the integer $\sum_{i=0}^{|C-1|} b_i 2^{i2^t}$, where $b_i \in \mathbf{M}_t$ is the guessed output at gate number i. The two (or less) inputs at each gate are encoded in a similar way. Then we have to verify that the values which are given more than once as inputs and outputs are the same. Since the structure of the circuit can be calculated by a turing machine this verification can be done using the Digit Relocation Lemma. The other step in the verification is that each gate performs correctly the operation assigned to it. Here we assume that at each gate together with the inputs and output also the name of the operation is also given (where such a name a natural number in the set $\{0, 1, ..., \mathbf{k}\}$, where $\mathbf{k}$ is the number of $\mathcal{M}$ operations). The assignment of the operations to the gates is encoded by an integer $\sum_{i=0}^{|C-1|} q_i 2^{i2^t}$ where $q_i \in \mathbf{k}$ is the name of the operation at gate i. (Here we assume that $2^{2^t} > \mathbf{k}$ but this is only a technical problem that can be avoided easily.)

Using Theorem 7 we can perform parallel all of the operations at the all of the gates, in the sense the we can define the result by an existential formula. Now we have the results of all of the operations performed on the twp inputs at each gate. With another existential formula we can check that the output at G is identical to the result which corresponds to the name of the operation assigned to gate G. For this checking we use the same technique as was used to conclude the proof of Theorem 7, that is, first we

express the equalities between that various integers at gate G in terms of $0,1$-bits and then use statement (2).

2.4 Simulation

Our goal is to show that *for each $\tau \in \mathcal{T}_n$, there exists a $\lambda_\tau \in \mathcal{H}'_n$ such that for all $a, b \in \mathbf{M}_d$, $\mathbf{M}_d \models \lambda_\tau(a,b)$ is equivalent to $\mathbf{M}_q \models \tau(a,b) = \mathbf{0}$, where $q = \lfloor d + \log d \rfloor$*.

Recall that $\mathcal{T}_n$ is a set of terms of $\mathcal{M}$ with some bounds on their sizes and $\mathcal{H}'_n$ is a set of first-order formulas with some restriction on the number of quantifier changes and on the sizes of the formulas. For the moment we disregard the quantitative bounds on the term τ and the formula λ, we consider only the following general question.

Assume that $\tau(x,y)$ is a term of $\mathcal{M}$, $a, b \in \mathbf{M}_d$ and we want to know whether $\mathbf{M}_q \models \tau(a,b) = \mathbf{0}$, but we are allowed only to evaluate first-order formulas in $\mathbf{M}_d$, where $q = \lfloor d + \log d \rfloor$. How can we do this? Since the structure $\mathbf{M}_d$ is much smaller than $\mathbf{M}_q$ we cannot simply perform the computation of $(\tau(a,b))_{\mathbf{M}_q}$ in $\mathbf{M}_d$. It is true that the starting points for the computation of $(\tau(a,b))_{\mathbf{M}_q}$, namely the elements a, b are in $\mathbf{M}_d$, but during the computation we may get partial results which are in $\mathbf{M}_q$ but not in $\mathbf{M}_d$.

In spite of this difficulty our plan is to follow the computation of $(\tau(a,b))_{\mathbf{M}_q}$ step by step in $\mathbf{M}_d$, that is, we want to simulate the computation of $\tau(a,b)$ in $\mathbf{M}_q$ by doing something in $\mathbf{M}_d$. During this simulation we have to represent the partial results, which are elements of $\mathbf{M}_q$, in some way in $\mathbf{M}_d$. The structure $\mathbf{M}_d$ does not have enough elements for this. So we will represent each element h of $\mathbf{M}_q$ by a binary relation $\eta^{(h)}$ on $\mathbf{M}_d$, and we will do it in a way that all of the elements w of $\mathbf{M}_q$ which occur as partial result during the computation of $(\tau(a,b))_{\mathbf{M}_q}$ will be represented by a binary relation $\eta^{(w)}$ which can be defined by a first-order formula φ_w on $\mathbf{M}_d$ in the sense that for all $x, y \in \mathbf{M}_d$, we have $\eta^{(w)}(x,y)$ iff $\mathbf{M}_d \models \varphi_w(x,y)$. At the beginning of the computation that is if $w = a$ or $w = b$ or w can be defined by a constant symbol in $\mathbf{M}_q$, then the formula φ_w will be of constant size. As we will proceed with the computation of $(\tau(a,b))_{\mathbf{M}_q}$, the formulas φ_w corresponding to the partial results w will be larger and larger, at each step the number of quantifier alternations in φ_w will grow by an additive constant and the size of the formula φ_w by a multiplicative constant.

We will define the formulas φ_w in the following way. First we define φ_w for each element $w \in \mathbf{M}_d$, and when $\mathbf{M}_q \models w = \mathbf{c}$, where $\mathbf{c}$ is a constant symbol of $\mathcal{M}$. Then we give a general rule such that in the knowledge of φ_w and $\varphi_{w'}$ it will be possible to construct $\varphi_{\mathbf{f}(w,w')}$ or $\varphi_{\mathbf{g}(w)}$ for all function binary function symbols $\mathbf{f}$ and unary function symbols $\mathbf{g}$ of $\mathcal{M}$.

First we indicate how can we do this with unary relations. The simplest solution is to represent each element of $\mathbf{M}_q$ by a unary relation using the binary form of w. For each $w \in \mathbf{M}_q$ let $\xi^{(w)}$ be the unary relation on $\mathbf{M}_d$ defined by "for all $i \in \mathbf{M}_d$, $\xi^{(i)}(a)$ iff $w[i,0] = 1$", that is, $\xi^{(i)}(a)$ holds iff the ith binary bit of w is 1. If d is sufficiently large and $q = \lfloor d + \log d \rfloor$ we have that $w \to \xi^{(w)}$ is a one-to-one map of $\mathbf{M}_q$ into the set of unary relations on $\mathbf{M}_d$. The next question is that if we have the relations $\xi^{(w)}$ and $\xi^{(w')}$ how can we get from them the relations $\xi^{(w+w')}$, $\xi^{(ww')}$, $\xi^{\div(w,w')}$ etc. We will see that these

relations can be defined by a first-order formulas from the relations $\xi^{(w)}$ and $\xi^{(w')}$.

We will use binary not unary relations to represent the elements of $\mathbf{M}_q$ but we do this only because it is technically more convenient but the binary representation that we will use is, in some sense, equivalent to the unary representation described above.

We may think that the structures $\mathbf{M}_t$, $t = 0, 1, ...$ are constructed in this order. The property of the operations of $\mathcal{M}$ on these structure that we sketched above and will define below means that at the time when we have constructed the structure $\mathbf{M}_d$ we are able to "predict" what will be the result of various operations in $\mathbf{M}_q$ for some $q > d$. This motivates the term "predictive" that we will use in the following definition. (Recall that $\mathtt{coeff}_i(a, b)$ is the ith digit of a in the b-ary numeral system.)

Definition. 1. The set of functions symbols of $\mathcal{M}$ (including the constant symbols) will be denoted by $\mathtt{fsymb}(\mathcal{M})$

2. Let $\mathcal{J}$ be a function. We will say that $\mathbf{M}$ is $\mathcal{J}$-predictive if the following conditions are satisfied.

(4) *The function $\mathcal{J}$ is a monotone increasing function defined on ω and with values in ω.*

(5) *For all sufficiently large $d \in \omega$, $\mathcal{J}(d) \in \mathbf{M}_d$ and $\mathcal{J}(d) > d$.*

(6) *There exists a function defined on $\mathtt{fsymb}(\mathcal{M})$ assigning to each function symbol $f(x_0, \dots, x_{k-1})$ of $\mathcal{M}$, a first-order formula $\Phi_f(x, y, z, Y_0, \dots, Y_{k-1})$ of $\mathcal{M}$, where x, y, z are free first-order variables and $Y_0, \dots, Y_{k-1}$ are free variables for binary relations, such that the following holds. For all $d, r \in \omega$ with $d + r \le \mathcal{J}(d)$ there exists a map $a \to \eta^{(a)}_{d,r}$ of $\mathtt{universe}(\mathbf{M}_{d+r})$ into the set of binary relations on $\mathtt{universe}(\mathbf{M}_d)$ with the following properties:*

(i) For each $a, u, v \in \mathbf{M}_d$, we have $\eta^{(a)}_{d,r}(u, v)$ iff "$u = 0$ and $\mathtt{coeff}_v(a, 2) = 1$".

(ii) Suppose that $f(x_0, \dots, x_{k-1})$ is a k-ary function symbol of $\mathcal{M}$, for some $k = 0, 1, 2$ (including the constant symbols for $k = 0$), $\bar{f} = (f)_{\mathbf{M}_{d+r}}$, and $a_0, \dots, a_{k-1} \in \mathbf{M}_{d+r}$. Then for all $u, v \in \mathbf{M}_d$, $\eta^{(\bar{f}(a_0,\dots,a_{k-1}))}_{d,r}(u, v)$ iff

$$\mathbf{M}_d \models \Phi_f(u, v, r, \eta^{(a_0)}_{d,r}, \dots, \eta^{(a_{k-1})}_{d,r}).$$

□

The proof of the simulation statement is based on the following lemma.

Lemma 1 *Assume that $c > 0$ is a real, and $\mathcal{J}(x) = \lfloor x + c \log x \rfloor$. Then $\mathbf{M}$ is $\mathcal{J}$ predictive.*

In [2] a weaker result of similar nature is proved which implies that there exists a function $g(x)$ with $\lim_{x\to\infty} g(x) = \infty$, such that if $\mathcal{J}_0 = x + g(x)$ then $\mathbf{M}$ is $\mathcal{J}_0$-predictive. Some of the partial results of the proof given there were stronger than what was needed for the theorem formulated in [2]. We get Lemma 1 by using the full strength of these partial results in particular about the first-order definability of the bits of the results of multiplication and division between large numbers. The proof is given in section 9.2. This completes the sketches of the various parts of the theorem.

3 Existential and propositional families of relations on M

A large part of our proofs consists of constructions of first-order formulas of $\mathcal{M}$ which define relations or functions in the structures $\mathbf{M}_d$, $d \in \omega$ with properties which are useful in proving our theorems. For example the "Collapsing statement" and "Simulation statement" claim the existence of certain first-order formulas of $\mathcal{M}$ that we will construct during our proofs. In spite of the fact that Theorem 3 and Theorem 4 are "non-existence" statements, which claim that formulas of $\mathcal{M}$ with given properties do not exist for their proof we use statements which claim the existence of formulas of $\mathcal{M}$ with other properties. (This is a typical situation in lower bound proofs.)

In the Collapsing and Simulation statements we are speaking about first-order formulas which are interpreted in a structure $\mathbf{M}_d$ where $d \in \omega$. The sizes of these formulas may depend on d. In this section we consider a simpler question where there is only one formula. More precisely let R_d, $d \in \omega$ be a family of relations, where for all $d \in \omega$, R_d is a k-ary relations on $\mathbf{M}_d$. If there exists a first-order formula $\varphi(x_0, ..., x_{k-1})$ of $\mathcal{M}$ such that for all $d \in \omega$ and for all $a_0, ..., a_{k-1}$, $R_d(a_0, ..., a_{k-1})$ iff $\mathbf{M}_d \models \varphi(a_0, ..., a_{k-1})$ then we will say that the formula φ defines the family R_d. This means that the whole family can be defined by a single first-order formula. We will say that such a family of relations is uniformly first-order definable. The special cases when φ is propositional or existential will be very important and then the corresponding families of relations will be called uniformly propositional and uniformly existential. We will use similar definitions for families of functions as well.

The importance of these notions is that there is a large number of explicitly defined relations and functions, which are either uniformly propositional or uniformly existential, and we use them in the proofs of the Collapsing statement. This section contains the formulations and proofs of results of these types.

It is easy to see that for each propositional formula $P(x_0, ..., x_{k-1})$ there exists a term $t(x_0, ..., x_{k-1})$ of $\mathcal{M}$ such that for all $d \in \omega$, $\mathbf{M}_d \models \forall x_0, ..., x_{k-1}, P(x_0, ..., x_{k-1}) \leftrightarrow t(x_0, ..., x_{k-1}) = \mathbf{0}$. (See Lemma 3 below.) This implies that for all uniformly propositional family of relations $R_d(x_0, ..., x_{k-1})$, $d \in \omega$, there exists a term t of $\mathcal{M}$ such that for all $a_0, ..., a_{k-1} \in \mathbf{M}_d$, $\mathbf{M}_d \models t(a_0, ..., a_{k-1}) = \mathbf{0}$ is equivalent to $R_d(a_0, ..., a_{k-1})$. In particular if f_d, $d \in \omega$ is a family of $k-1$-ary functions such that $R_d(a_0, ..., a_{k-1})$ holds iff $f_d(x_0, ..., x_{k-2}) = x_{k-1}$ then for all $a_0, ..., a_{k-1} \in \mathbf{M}_d$, $\mathbf{M}_d \models t(a_0, ..., a_{k-1}) = \mathbf{0}$ is equivalent to $f_d(a_0, ..., a_{k-2}) = a_{k-1}$. In this case we say that the family of functions f_d is propositional. We will be also interested in families where each functions f_d is computable by the same term. This requirement can be formulated as follows.

There exists a term $s(x_0, ..., x_{k-2})$ of $\mathcal{M}$ such that for all $d \in \omega$ and for all $a_0, ..., a_{k-2}, a_{k-1} \in \mathbf{M}_d$, $\mathbf{M}_d \models s(a_0, ..., a_{k-1}) = f_d(a_0, ..., a_{k-2}) = a_{k-1}$.

If this last condition is satisfied then we will say that the family function f_d, $d \in \omega$ can be uniformly expressed by a term. This clearly implies that the family of function f_d is propositional. In some cases we will need this stronger property. (When we say stronger we mean only that the definition is formally stronger but we do not know whether there

exists a uniformly propositional family of function which cannot be expressed uniformly by a term.)

If $f(x_0, ..., x_{k-1})$ is a function which is defined by an existential formula $\varphi(x_0, ..., x_{k-1}, y)$ in $\mathbf{M}_d$, that is, for all $a_0, ..., a_{k-1}, b$ we have $\mathbf{M}_d \models f(a_0, \ldots, a_{k-1}) = b \leftrightarrow \varphi(a_0, \ldots, a_{k-1}, b)$ then the function f can be also defined by a universal formula namely $\mathbf{M}_d \models f(a_0, \ldots, a_{k-1}) = b \leftrightarrow \forall x, x = b \vee \neg\varphi(a_0, \ldots, a_{k-1}, b)$. Therefore each existential family of functions is also universal.

Most of the families of relations and functions where we will prove that they are uniformly existential or propositional are related to the notion of "*digits*" of integers in various numeral systems. For example it is easy to show that the family of relations $R_d(u, i, a, t)$ defined by "$t \leq d$ and u is that ith digit of a in the numeral system with base 2^{2^t}" is propositional. The numeral systems with base 2^{2^t} has a particular importance for us since if $d \leq t$ the a sequence $u_0, ..., u_{k-1} \in \mathbf{M}$, $k = 2^{d-t}$, can be encoded as the sequence of 2^{2^t}-ary digits of a single element $a \in \mathbf{M}_d$, namely $a = \sum_{i=0}^{k-1} u_i 2^{2^{it}}$. As we have mentioned already in section 2 we will frequently need to encode sequences from the elements of a structure $\mathbf{M}_t$ by a single element of a larger structure $\mathbf{M}_d$. A very important and characteristic example is the Circuit Simulation Lemma whose intuitive statement was described in section 2. Here the a circuit, by definition, will be the sequence of its nodes with various labelings which describe the operations and the "wires" between the nodes. A circuit given this way will be encoded by a single element a of a sufficiently large structure $\mathbf{M}_d$ and the 2^{2^t}-ary digits of the integer a will define the sequences of nodes and labelings, for a suitably chosen positive integer $t < d$.

We will need also to perform operations on sequences of integers which are encoded as the 2^{2^t}-ary digits of an integer $a \in \mathbf{M}_d$. This is very important for the Vector Property Lemma (see the formulation of this lemma in section 2 and the explanation before the statement of the lemma). In this section we prove the Vector Property Lemma for each of the operations $\mathbf{f} \notin \{\times, \div, \mathbf{p}\}$. We actually get in these cases a stronger version of the lemma with $c = 0$. Th most problematic cases proved in this section will be the operations min and max.

3.1 Existential and propositional formulas in $\mathbf{M}_d$, basic properties

Definition. $\mathtt{func}(A, B)$ will denote the set of all functions defined on the set A with values in the set B. □

Definition. 1. Assume that $k \in \omega$ and $R = \langle R^{(d)} \mid d \in \omega \rangle$ is a family of k-ary relations, such that for each $d \in \omega$, $R^{(d)}$ is a k-ary relation on $\mathbf{M}_d$. Then we will say that R is a family of k-ary relations on $\mathbf{M}$.

2. Suppose that $k \in \omega$ and $R = \langle R^{(d)} \mid d \in \omega \rangle$ is a family of k-ary relations on $\mathbf{M}$. We will say that the family R is uniformly propositional on $\mathbf{M}$ if there exists a propositional formula $P(x_0, \ldots, x_{k-1})$ of $\mathcal{M}$ such that, for all $d \in \omega$, and for all $a_0, \ldots, a_{k-1} \in \mathbf{M}_d$, $R^{(d)}(a_0, \ldots, a_{k-1})$ is equivalent to $\mathbf{M}_d \models P(a_0, \ldots, a_{k-1})$. In a similar

way the family R is called uniformly existential on $\mathbf{M}$ if there exists an existential first-order formula $\varphi(x_0, \ldots, x_{k-1})$ of $\mathcal{M}$ such that, for all $d \in \omega$, and for all $a_0, \ldots, a_{k-1} \in \mathbf{M}_d$, $R^{(d)}(a_0, \ldots, a_{k-1})$ is equivalent to $\mathbf{M}_d \models \varphi(a_0, \ldots, a_{k-1})$. $\square$

Definition. 1. Assume that $f = \langle f^{(d)} \mid d \in \omega \rangle$ is a family of k-ary functions, such that for each $d \in \omega$, $f^{(d)}$ is a k-ary function defined on $\mathbf{M}_d$ and with values in $\mathbf{M}_d$. Then we will say that f is a family of k-ary functions on $\mathbf{M}$.

2. Suppose that $k \in \omega$ and $f = \langle f^{(d)} \mid d \in \omega \rangle$ is a family of k-ary functions on $\mathbf{M}$. We will say that the family f is uniformly propositional on $\mathbf{M}$ if there exists a propositional formula $P(x_0, \ldots, x_{k-1}, y)$ of $\mathcal{M}$ such that, for all $d \in \omega$, and for all $a_0, \ldots, a_{k-1}, b \in \mathbf{M}_d$, $f^{(d)}(a_0, \ldots, a_{k-1}) = b$ is equivalent to $\mathbf{M}_d \models P(a_0, \ldots, a_{k-1}, b)$. In a similar way the family f is called uniformly existential on $\mathbf{M}$ if there exists an existential first-order formula $\varphi(x_0, \ldots, x_{r-1}, y)$ of $\mathcal{M}$ such that, for all $d \in \omega$, and for all $a_0, \ldots, a_{k-1}, b \in \mathbf{M}_d$, $f^{(d)}(a_0, \ldots, a_{k-1}) = d$ is equivalent to $\mathbf{M}_d \models \varphi(a_0, \ldots, a_{k-1}, b)$. $\square$

Definition. 1. If $a, t \in \omega$ and i is an integer then we will use the notation $a[i, t] = \mathtt{coeff}_i(a, 2^{2^t})$. (By the definition of the function `coeff` if i is negative then $a[i, t] = 0$.) E.g., the ith binary bit of the natural number a is $a[i, 0]$.

2. The elements of $\mathbf{M}_d$ are natural numbers, in the set $\{0, 1, \ldots, 2^{2^d} - 1\}$, but sometimes it is useful to represent them as sequences of various types. For each fixed $d \in \omega$ and $p \in \{0, 1, \ldots, d\}$ each element $a \in \mathbf{M}_d$ will be represented by a sequence $\langle a[0, p], a[1, p], \ldots, a[2^{d-p} - 1, p] \rangle$, that we will denote by $[\![a, d, p]\!]$. This is a sequence of length 2^{d-p} whose elements are the 2^{2^p}-ary digits of the natural number a. $\square$

Lemma 2 *There exist binary terms h, g of $\mathcal{M}$ such that for all $d \in \omega$ and for all a, b in $\mathbf{M}_d$,*

(7) *$a = b$ implies $\mathbf{M}_d \models g(a, b) = \mathbf{1}$ and $a \neq b$ implies $\mathbf{M}_d \models g(a, b) = \mathbf{0}$.*

(8) *$a < b$ implies $\mathbf{M}_d \models h(a, b) = \mathbf{1}$ and $a \geq b$ implies $\mathbf{M}_d \models h(a, b) = \mathbf{0}$.*

Proof. The definitions of the terms are $g(x, y) = \mathbf{1} - \min(\mathbf{1}, x - y)$, and $h(x, y) = (\mathbf{1} - g(x, y))(\mathbf{1} - g(\min(x, y), y))$. *Q.E.D.*(Lemma 2)

For the following definition recall that the interpretation of the function symbol $\mathbf{p}(x)$ in the structure $\mathbf{M}_d$ was the function $\min(2^n - 1, 2^x)$, where $n = 2^d$.

Definition. We define a term $\mathbf{q}(x)$ of $\mathcal{M}$ by $\mathbf{q}(x) = h(x, \mathbf{n})\mathbf{p}(x)$ where $h(x, y)$ is the term defined in Lemma 2. This definition implies that for all $x, z \in \mathbf{M}_d$, if $n = 2^d$ then

($\mathbf{M}_d \models \mathbf{q}(x) = z$) iff "either $x < 2^d$ and $z = \min\{2^x, 2^n - 1\} = 2^x$, or $x \geq 2^d \wedge z = 0$. Therefore the terms $\mathbf{q}(x)$ and $\mathbf{p}(x)$ take different values only if $x \geq 2^d$. In this case $\mathbf{p}(x) = 2^{2^d} - 1$ and $\mathbf{q}(x) = 0$. $\square$

Lemma 3 *For each propositional formula $P(x_0, ..., x_{k-1})$ there exists a term $t(x_0, ..., x_{k-1})$ of $\mathcal{M}$ such that for all $d \in \omega$, $\mathbf{M}_d \models \forall x_0, ..., x_{k-1}, (P(x_0, ..., x_{k-1}) \rightarrow t(x_0, ..., x_{k-1}) = \mathbf{0}) \wedge (\neg P(x_0, ..., x_{k-1}) \rightarrow t(x_0, ..., x_{k-1}) = \mathbf{1})$.*

We need this lemma so frequently that we will use it without a reference.

Proof of Lemma 3. We prove the lemma by induction on the number of logical connectives in the formula P. If P is an atomic formula then it is of the form $t_0 = t_1$, where t_0, t_1 are terms of $\mathcal{M}$. If g is a term with the properties described in Lemma 2 then the term $t = \mathbf{1} - g(t_0, t_1)$ meets the requirements of the lemma.

Suppose that $P = \neg P'$ and the term t' is chosen so that the conditions of the Lemma are satisfied with $P{:=}\ P'$, $t{:=}\ t'$. Then $t = \mathbf{1} - t'$ is the required term. Assume that $P = P_0 \vee P_1$, and the terms t_i, $i = 0, 1$ are chosen so that the conditions of the Lemma are satisfied with $P{:=}\ P_i$, $t{:=}\ t_i$ for $i = 0, 1$. Then $t = t_0 t_1$ meets the requirements of the lemma. The remaining logical connectives can be expressed as combinations of $\neg$ and $\vee$. *Q.E.D.*(Lemma 3)

Lemma 4 *There exists a term $\kappa(x)$ of $\mathcal{M}$ such that for all $d, t \in \omega$ if $t \leq d$ and $b = 2^{2^t} - 1$ then $\mathbf{M}_d \models \kappa(t) = b$.*

Proof of Lemma 4. The term $\mathbf{q}(\mathbf{q}(x)) - \mathbf{1}$ satisfies the requirements of the lemma. (The choice $\kappa(x) = \mathbf{p}(\mathbf{p}(x)) - 1$ is not satisfactory since in the $t = d$ case the definition of $(\mathbf{p})_{\mathbf{M}_d}$ would imply $\mathbf{M}_d \models \kappa(d) = r$, where $r = \min(2^{2^d} - 1, 2^{2^d} - 1 - 1) = 2^{2^d} - 2$.) *Q.E.D.*(Lemma 4)

Lemma 5 *There exists a term σ of $\mathcal{M}$ such that for all $d, b, a, j, k, \alpha_0, ..., \alpha_{k-1} \in \omega$, if $\alpha_0, ..., \alpha_{k-1} < 2^b$, $2^{kb} - 1 \in \mathbf{M}_d$, $a = \sum_{i=0}^{k-1} \alpha_i 2^{ib}$, and $j \in k$, then $\mathbf{M}_d \models \alpha_j = \sigma(a, b, j)$.*

Proof of Lemma 5. We have that for all $l \in k$ if $S_l = \sum_{i=0}^{l-1} \alpha_i 2^{ib}$, then $\mathbf{M}_d \models S_l = a - \div(a, 2^{lb})$. Since $\alpha_j = \frac{S_j - S_{j-1}}{2^{(j-1)b}}$ this implies our statement. *Q.E.D.*(Lemma 5)

In the following definition if $0 \leq t \leq d$, then for each an element $a \in \mathbf{M}_d$ we consider the sequence $[\![a, d, t]\!]$, that is, the sequence of 2^{2^t}-ary digits of the integer a. We define a unary operation $\mathtt{shift}_{d,t,i}(a)$ which shifts this sequence by i places toward the more significant places if $i \geq 0$. Those which would represent a number larger that 2^{2^d} will disappear and on the other end of the sequence the new elements will be zeros. If $i < 0$ then the shift is in the other direction with similar rules. First we consider the special case when $t = 0$, the corresponding function will be denoted by $\mathtt{shift}_{d,i}$.

Definition. Assume that $d \in \omega$ and i is an integer. We define a function $\mathtt{shift}_{d,i}$ on $\mathbf{M}_d$. For all $a, b \in \mathbf{M}_d$, $\mathtt{shift}_{d,i}(a) = b$ iff for all $k \in 2^d$, $b[k, 0] = a[k - i, 0]$. (Recall that $a[j, 0]$ is defined for all integers j, and if j is negative then $a[j, 0] = 0$.) For each $d, t \in \omega$, $d \geq t$ and integer i, we define a function $\mathtt{shift}_{d,t,i}$ on $\mathbf{M}_d$: for all $a, b \in \mathbf{M}_d$, $\mathtt{shift}_{d,t,i}(a) = b$ iff for all $k \in 2^{d-t}$, $b[k, t] = a[k - i, t]$. These definitions imply that for each $d, t \in \omega$ with $t \leq d$, if i is an integer then $\mathtt{shift}_{d,i} \in \mathtt{func}(\mathbf{M}_d, \mathbf{M}_d)$ and $\mathtt{shift}_{d,t,i} \in \mathtt{func}(\mathbf{M}_d, \mathbf{M}_d)$. □

The next two lemma shows that the function shift can be defined uniformly with a term. In the formulation of Lemma 6 it is important that we have defined the interpretation of the operation $\div$ such that for all $d \in \omega$, and $a \in \mathbf{M}_d$, we have $\mathbf{M}_d \models \div(a, \mathbf{0}) = \mathbf{0}$.

Lemma 6 *Assume that $d, t \in \omega$, $d \geq t$, $a, i \in \mathbf{M}_d$. Then $\mathtt{shift}_{d,t,i}(a)$ is the unique element b of $\mathbf{M}_d$ such that $\mathbf{M}_d \models b = a\mathbf{q}(i)$, and the integer $\mathtt{shift}_{d,t,-i}(a)$ is the unique element b of $\mathbf{M}_d$ such that $\mathbf{M}_d \models b = \div(a, \mathbf{q}(i))$.*

Proof of Lemma 6. The statement of the lemma is an immediate consequence of the definitions of the function $\mathtt{shift}_{d,t,i}$ and the structure $\mathbf{M}_d$. *Q.E.D.*(Lemma 6)

Lemma 7 *There exists a term τ of $\mathcal{M}$ such that for all $d, t \in \omega$, with $d \geq t$, and for all $a, i \in \mathbf{M}_d$, $\delta \in \{-\mathbf{1}, \mathbf{1}\}$, the following holds. Assume that and an integer b is defined by $b = \mathtt{shift}_{d,t,i}(a)$ if $\delta = \mathbf{1}$, and $b = \mathtt{shift}_{d,t,-i}(a)$ if $\delta = -\mathbf{1}$. Then $\mathbf{M}_d \models b = \tau(a, i, t, \delta)$.*

Remark. In this lemma the possible values of δ are terms of $\mathcal{M}$. Since the integer -1 is not in $\mathbf{M}_d$, we cannot use it as an argument for the term σ. The term $-\mathbf{1}$ takes the value $2^{2^d} - 1$ in $\mathbf{M}_d$, which plays the role of -1. □

Proof of Lemma 7. Lemma 6 implies that there exists a term σ_+ which meets the requirements with the lemma with $\sigma := \sigma_+$ provided that $\delta = \mathbf{1}$. In a similar way there exists another term σ_- that meets the requirements of the lemma if $\delta = -\mathbf{1}$. Consequently the term $\sigma = g(\delta, \mathbf{1})\sigma_+ + g(\delta, -\mathbf{1})\sigma_-$ meets the requirements of the lemma in all cases, where g is the term defined in Lemma 2. *Q.E.D.*(Lemma 7)

Lemma 8 *There exists a term $\sigma(x, y, z, w)$ of $\mathcal{M}$ such that if $d, i, j \in \omega$, $t \in d$, $0 \leq i \leq j < 2^{d-t}$, $a \in \mathbf{M}_d$, $a = \sum_{k=0}^{2^{d-t}-1} a_k (2^{2^t})^k$ and $b = \sum_{k=i}^{j} a_k (2^{2^t})^k$ then $\mathbf{M}_d \models b = \sigma(a, i, j, t)$.*

Proof of Lemma 8 The statement of the lemma is a consequence of Lemma 7. We shift the digits of a first toward the more significant digits, in a way that some of the digits which are not needed in b disappear. Then we repeat this in the other direction. More precisely. Let $q = 2^{d-t} - j - 1$, and let $b_0 = \mathtt{shift}_{d,-q,t}(\mathtt{shift}_{d,q,t}(a))$. Then $b = \mathtt{shift}_{d,-i,t}(\mathtt{shift}_{d,i,t}(b_0))$. By Lemma 7 the function $\mathtt{shift}$ can be expressed uniformly by a term of $\mathcal{M}$. *Q.E.D.*(Lemma8)

Lemma 9 *There exists a term σ of $\mathcal{M}$ such that the following holds. Assume that $d, t \in \omega$ with $d \geq t$, $r = 2^{d-t}$, $a_0, ..., a_{r-1} \in \mathbf{M}_t$ and $S = \sum_{i=0}^{r-1} a_i 2^{i2^t}$. Then for all $i \in r$ we have $\mathbf{M}_d \models \sigma(S, i, t) = a_i$*

Proof of Lemma 9. This is an immediate consequence of Lemma 8 in the $i = j$ special case. *Q.E.D.*(Lemma 9)

Lemma 10 *$Q(x, y)$ will denote either the relation $x = y$ or the relation $x \leq y$ among the integers. The following statement holds in both cases. Assume that $p(x_1, \ldots, x_k, y, z), q(x_1, \ldots, x_k, y, z)$ are terms of $\mathcal{M}$ and for each $d \in \omega$, f_d is a $k+2$-ary function on $\mathbf{M}_d$ defined by: for all $a_1, \ldots, a_k, u, v \in \mathbf{M}_d$,*

if $Q(u, v)$ then $\mathbf{M}_d \models f_d(a_1, \ldots, a_k, u, v) = p(a_1, \ldots, a_k, u, v)$, and

if $\neg Q(u, v)$ then $\mathbf{M}_d \models f_d(a_1, \ldots, a_k, u, v) = q(a_1, \ldots, a_k, u, v)$.

Then there exists a term $t(x_1, \ldots, x_k, y, z)$ of $\mathcal{M}$ such that for all $d \in \omega$ and for all $a_1, \ldots, a_k, u, v \in \mathbf{M}_d$, $\mathbf{M}_d \models f_d(a_1, \ldots, a_k, u, v) = t(a_1, \ldots, a_k, u, v)$.

Proof of Lemma 10. Assume the Q is the relation $x = y$ and h, g are the terms whose existence are sated in Lemma 2. Then

$$t(x_1, \dots, x_k, y, z) = g(y, z)p(x_1, \dots, x_k, y, z) + (\mathbf{1} - g(y, z))q(x_1, \dots, x_k, y, z)$$

If Q is the relation $x \leq y$ then the term h is used in a similar way. *Q.E.D.*(Lemma KB1)

Lemma 11 *There exist terms $\sigma(x, y), \tau(x, y)$ of the language $\mathcal{M}$ such that for all $d \in \omega$ if $r, j, k \in \mathbf{M}_d$, $k > 1$ and $r = 2^j$ then the following two conditions are satisfied.*

(9) *$r^{k+1} \leq 2^{2^d}$, and $S = \sum_{i=0}^{k} r^i$ implies $S \in \mathbf{M}_d$ and $\mathbf{M}_d \models S = \sigma(j, k)$,*

(10) *$(k + 1)r^k(r - 1) < 2^{2^d}$, and $T = \sum_{i=1}^{k} ir^{i-1}$ implies $T \in \mathbf{M}_d$ and $\mathbf{M}_d \models T = \tau(j, k)$.*

Proof of Lemma 11. Condition (9)). $S = \sum_{i=0}^{k} r^i = \frac{r^{k+1}-1}{r-1}$, therefore the assumption $r^{k+1} \leq 2^{2^d}$ implies $S \in \mathbf{M}_d$ and $\mathbf{M}_d \models S = \div(\mathbf{q}((k + 1)j) - \mathbf{1}, 2^j - \mathbf{1})$. Condition (10)). The proof is similar to the previous case, but here we use that

$$\sum_{i=1}^{k} ir^{i-1} = \frac{1 - r^{k+1}}{(1 - r)^2} - \frac{(k + 1)r^k}{1 - r} = \frac{(k + 1)r^k(r - 1) - r^{k+1} - 1}{(r - 1)^2}$$

Q.E.D.(Lemma 11)

Lemma 12 *There exists a term η of $\mathcal{M}$ such that for all $d, t, m, k \in \omega$ with $t \leq d$, $m \leq 2^{d-t}$, $k < m$ and for all $a \in \mathbf{M}_d$ the following two statements are equivalent:*

(11) *$\mathbf{M}_d \models a = \eta(t, m, k)$*

(12) *for all $i \in 2^{d-t}$, if $i \equiv k \pmod m$ then $a[i, t] = 1$, otherwise $a[i, t] = 0$.*

Proof of Lemma 12. First we consider the special case $k = 0$. Let $a_0 \in \mathbf{M}_d$ the unique integer so that condition (12) is satisfied with $a{:=}\, a_0$ and $k = 0$. The integer a_0 can be expressed as the sum of a geometric sequence, that is,

$$a_0 = \sum_{j=0}^{\alpha(d,t,m)} 2^{jm2^t}$$

where $\alpha(d, t, m) = \lfloor (2^{d-t} - 1)/m \rfloor$. $\alpha(d, t, m)$ can be written in the form of $\div(2^{d-t} - \mathbf{1}, m)$, so it is a term of $\mathcal{M}$. Therefore Lemma 11 implies that there exists a term $\xi(x, y)$ of $\mathcal{M}$ such that for all $d \in \omega$, $\mathbf{M}_d \models a_0 = \xi(m, k)$.

Let h be a term of $\mathcal{M}$ such that for all $d \in \omega$ and for all a, b in $\mathbf{M}_d$, $a < b$ implies $\mathbf{M}_d \models h(a, b) = \mathbf{1}$ and $a \geq b$ implies $\mathbf{M}_d \models h(a, b) = \mathbf{0}$. Lemma 2 implies the existence of such a term.

Suppose now that $k \in m$ is arbitrary. We construct a term η_1 which works if $k + m\alpha(d, m, t) < 2^{d-t}$ and another term η_2 which works if $k + m\alpha(d, m, t) \geq 2^{d-t}$ and then we use Lemma 10 to get the term η.

Assume a satisfies condition (12) with a $k \in m$ such that $k + m\alpha(d, m, t) < 2^d$ and a_0 satisfies condition (12) with $k = 0$. Then $a = 2^{k2^t} a_0$, which gives the definition of η_1.

If $k + m\alpha(d, m, t) \geq 2^d$ then $a = 2^{k2^t}(a_0 - 2^{\alpha(d,m,t)2^t})$, which defines η_2. *Q.E.D.*(Lemma 12)

Lemma 13 *For all $d, t \in \omega$ with $t \leq d$, there exists a unique integer $e \in \mathbf{M}_d$, such that for all $i \in 2^{d-t}$, $e[i,t] = 1$. Moreover, for this integer e, we have $\mathbf{M}_d \models e = \div(-\mathbf{1}, \mathbf{q}(\mathbf{q}(t))-\mathbf{1})$.*

Proof of Lemma 13. The uniqueness follows for the facts that $e < 2^{2^d}$ and the first 2^{d-t}, 2^{2^t}-ary digits of e are given. Adding the geometric series representing e as it is done in the proof of Lemma 11 we get $\mathbf{M}_d \models e = \div(-\mathbf{1}, \mathbf{q}(\mathbf{q}(t)) - 1)$. *Q.E.D.*(Lemma 12)

Definition. For all $d, t \in \omega$ the unique element $e \in \mathbf{M}_d$ with the properties described in Lemma 13 will be denoted by $e_{d,t}$. The term $\div(-\mathbf{1}, \mathbf{q}(\mathbf{q}(x)) - 1)$ with the free variable x will be denoted by $\bar{e}(x)$. Therefore if $t \in \mathbf{M}_d$, $t \leq d$ then $\mathbf{M}_d \models \bar{e}(t) = e_{d,t}$ $\square$

In the following definitions we introduce new operations on the elements of $\mathbf{M}_d$. These operations will be defined in the following way. A natural number $t \leq d$ is given and for each $a \in \mathbf{M}_d$ we consider the vector whose coordinates are the 2^{2^t}-ary digits of a. The new operations will be defined as vector operations performed on vectors of this type. These operations and the way they can be uniformly defined in $\mathbf{M}$ (e.g., by a propositional formula of $\mathcal{M}$) will be important for the proofs of Circuit Simulation Lemma and the Vector Property.

Definition. 1. Assume that $d, t \in \omega$, $t \leq d$, $a \in \mathbf{M}_d$, and $\delta \in \{0, 1\}$. We define $(a)_{d,t,\delta}$ as the unique integer $b \in \mathbf{M}_d$ such that for all $k \in 2^{d-t}$, if $k \equiv \delta \pmod 2$) then $b[k,t] = a[k,t]$, otherwise $b[k,t] = 0$.

2. Suppose that $d, t \in \omega$ and $t \leq d$. We define an operation $a \oplus_{d,t} b$ on $\mathbf{M}_d$. For all $a, b, c \in \mathbf{M}_d$, $a \oplus_{d,t} b = c$ iff for all $k \in 2^{d-t}$, $a[k,t] + b[k,t] \equiv c[k,t] \pmod{2^{2^t}}$.

We define a binary operation $\odot_{d,t}$ on $\mathbf{M}_d$ if $d \in \omega$ and $t \in d+1$. For all $a, b \in \mathbf{M}_d$ $a \odot_{d,t} b$ is defined in the following way. If $a \notin \mathbf{M}_t = 2^{2^t}$ then $a \odot_{d,t} b = 0$. If $a \in \mathbf{M}_t$ then for all $c \in \mathbf{M}_d$, $a \odot_{d,t} b = c$ iff for all $k \in 2^{d-t}$, $a \cdot b[k,t] \equiv c[k,t]$, $\pmod{2^{2^t}}$, where the operation " $\cdot$ " is the multiplication between integers.

3. Suppose that $d, t \in \omega$ and $t \leq d$. We define a binary operation $\oslash_{d,t}$ on $\mathbf{M}_d$. For all $a, b \in \mathbf{M}_d$, $a \oslash_{d,t} b$ is defined in the following way. If $b = 0$ then $a \oslash_{d,t} b = 0$. If $b \neq 0$ then $a \oslash_{d,t} b$ is the unique element c of $\mathbf{M}_d$, such that for all $k \in 2^{d-t}$, $\lfloor a[k,t]/b \rfloor = c[k,t]$. $\square$

Remark. The operation $\oplus_{d,t}$ corresponds to the modulo 2^{2^t} addition of 2^{d-t} dimensional vectors. The operation $a \odot_{d,t} b$, if we restrict a to the set $\mathbf{M}_t$, corresponds the multiplication of 2^{d-t} dimensional vectors modulo 2^{2^t} by scalars from the set $\mathbf{M}_t = 2^{2^t}$. The operation $a \oslash b$ is the integer division of each component of a by the scalar b. In the case of $b = 0$ our definition is compatible with the interpretation of $\div$ in $\mathbf{M}_d$. More precisely we have the following. Suppose $d, t \in \omega$, $d \leq t$, $a, b \in \mathbf{M}_t$ and $c = a \oslash_{d,t} b$. Then for all $k \in \mathbf{M}_t \models \div(a[k,t], b) = c[k,t]$. (This holds even for $b = 0$.) If $b \in \mathbf{M}_d \backslash \mathbf{M}_t$, then $a \oslash b = 0$ $\square$

Lemma 14 *Each family of relations $R = \langle R^{(d)} \mid d \in \omega \rangle$ on $\mathbf{M}$, defined in the conditions below, is uniformly propositional on $\mathbf{M}$.*

(13) *$R^{(d)}$ is the unary relation on $\mathbf{M}_d$ defined by $R^{(d)}(t) \leftrightarrow d$ iff $t \leq d$,*

(14) *for each boolean function f with two variables, $R_f^{(d)}$ is the ternary relation on $\mathbf{M}_d$ defined by*

$$R_f^{(d)}(a,b,c) \leftrightarrow \forall k \in 2^d, f(a[k,0],b[k,0]) = c[k,0]$$

(15) *for each integer r, $R_r^{(d)}$ is the binary relation on $\mathbf{M}_d$ defined by $R_r^{(d)}(a,b)$ iff $\mathtt{shift}_{d,r}(a) = b$,*

(16) *$R^{(d)}$ is the binary binary relation on $\mathbf{M}_d$ defined by $R^{(d)}(a,t)$ iff $t \leq d$ and for all $i \in 2^{d-t}$, $a[i,t] = 1$,*

(17) *for each integer r, $R_r^{(d)}$ is the ternary relation on $\mathbf{M}_d$ defined by, $R_r^{(d)}(a,b,t)$ iff $t \leq d$ and $\mathtt{shift}_{d,t,r}(a) = b$,*

(18) *for each $\delta \in \{0,1\}$, $R^{(d)}$ is the ternary relation on $\mathbf{M}_d$ defined by, $R^{(d)}(a,b,t)$ iff $t \leq d$ and $(a)_{d,t,\delta} = b$,*

(19) *for each $\delta \in \{0,1\}$, $R^{(d)}$ is the binary relation on $\mathbf{M}_d$ defined by, $R^{(d)}(a,t)$ iff $t \leq d$ and $(2^{2^d}-1)_{d,t,\delta} = a$,*

(20) *$R^{(d)}$ is the quaternary relation on $\mathbf{M}_d$ defined by $R^{(d)}(a,b,c,t)$ iff $t \leq d$ and $a \oplus_{d,t} b = c$,*

(21) *$R^{(d)}$ is the quaternary relation on $\mathbf{M}_d$ defined by $R^{(d)}(a,b,c,t)$ iff $t \leq d$, and $a \odot_{d,t} b = c$,*

(22) *$R^{(d)}$ is the ternary relation on $\mathbf{M}_d$ defined by $R^{(d)}(a,b,t)$ iff $t \leq d$ and for all $k \in 2^{d-t}$, $a[k,t] \equiv -b[k,t] \pmod{2^{2^t}}$.*

Proof of Lemma 14. (13) For all $t \in \mathbf{M}_d$, $t \leq d$ iff $\mathbf{M}_d \models 2^t \leq \mathbf{n}$. Consequently $t \leq d$ is uniformly propositional on $\mathbf{M}$.

In some of the further statements of the lemma we use the assumption $t \leq d$. Since the conjunction of uniformly propositional families of relations on $\mathbf{M}$ are also uniformly propositional on $\mathbf{M}$, statement (13) that we may assume in all of these cases that $t \leq d$, that is, we prove the equivalence of the given relation and the relation defined by a propositional formula with the additional assumption $t \leq d$.

(15) and (17) are immediate consequences of Lemma 7.

(14). This is an immediate consequence of the following two facts (a) the function symbols $\cap$ and $\mathcal{N}$ are are interpreted as boolean vector operations $\wedge$ and $\neg$, on the sequences of binary bits $a[0,0], a[1,0], \ldots$ on the elements a of the structure $\mathbf{M}_d$, (b) each boolean function f can be obtained as a composition of the functions $\wedge$ and $\neg$.

(16). The statement follows from Lemma 13.

(19). We have $(2^{2^d}-1)[k,0] = 1$ for all $k \in 2^d$, and $\sum_{i=0}^{2^{t-1}} 2^i = 2^{2^t}-1$. Therefore

$$(2^{2^d}-1)_{d,t,0} = (2^{2^t}-1)\sum_{j=0}^{\lfloor (2^{d-t}-1)/2 \rfloor} 2^{2j2^t}$$

Consequently Lemma 11, and $\mathbf{M}_d \models 2^{d-t} = \div(\mathbf{n}, 2^t)$ implies the existence of the required term for $\delta = 0$. To get the term for $\delta = 1$ we use the equality $(2^{2^d} - 1)_{d,t,1} = \mathtt{shift}_{d,t,1}((2^{2^d} - 1)_{d,t,0})$ and the already proven statement (15).

(18). This is a consequence of (19) and the fact that $(a)_{d,t,\delta} = a \cap (2^{2^d} - 1)_{d,t,\delta}$, where $\cap$ is the operation defined in $\mathbf{M}_d$, that is, the vector operation $\wedge$ performed on the sequences of binary bits.

(20). Follows from $a \oplus_{d,t} b = ((a)_{d,t,0} + (b)_{d,t,0})_{d,t,0} + ((a)_{d,t,1} + (b)_{d,t,1})_{d,t,1}$

(21). We define $a \odot_{d,t}$ be separately for the cases $a \geq 2^{2^t}$ and $a < 2^{2^t}$. We will show that both definition is uniformly proposition, therefore Lemma 10 will imply our statement.

If $a \geq 2^{2^t}$ than $a \odot_{d,t} b = \mathbf{0}$ which gives a propositional definition.

Assume that $a < 2^{2^t}$. Then $a \odot_{d,t} b = (a(b)_{d,t,0})_{d,t,0} + (a(b)_{d,t,1})_{d,t,1}$. The already proven statement (18) implies that this is equivalent to a propositional formula.

(22) The condition "for all $k \in 2^{d-t}$, $a[k,t] \equiv -b[k,t] \pmod{2^{2^t}}$ " is equivalent to $a \oplus_{d,t} b = 0$, therefore our assertion is a consequence of statement (20). *Q.E.D.*(Lemma 14)

Lemma 15 *Assume that $k \in \omega$, $f(x_0, ..., x_{k-1})$ is a boolean function of k variables. Then there exists a term τ of $\mathcal{M}$, such that for all $d \in \omega$, and for all $a_0, ..., a_{k-1} \in \mathbf{M}_d$ we have that for all $i \in 2^d$,*

$$\mathbf{M}_d \models f(a_0[i,0], ..., a_{k-1}[i,0]) = \Big(\tau(a_0, ..., a_{k-1})\Big)[i,0]$$

Proof of Lemma 15. The boolean function f can be expressed using only the boolean operations $\wedge$, $\neg$. The corresponding expression in $\mathcal{M}$ using the operations $\cap$ and $\mathcal{N}$ will be τ. *Q.E.D.*(Lemma 15)

Lemma 16 *The family of ternary relations $\langle R^{(d)} \mid d \in \omega \rangle$, is uniformly propositional on $\mathbf{M}$, where*

(23) *$R^{(d)}$ is the ternary relation on $\mathbf{M}_d$ defined by $R^{d)}(a,b,c)$ iff $a + b = c$ among the integers.*

Proof of Lemma 16. For all $a, b, c \in \mathbf{M}_d$, $a + b = c$ (as integers) is equivalent to $\mathbf{M}_d \models a + b = c \wedge a \leq c \wedge b \leq c$. *Q.E.D.*(Lemma 16)

Remark. So far we have proved about some functions and relations, that we defined in terms of the 2^{2^t}-ary digits of integers, that they are propositional. In particular the operations $\oplus, \odot$ were among these functions. In the remaining part of this section we will consider relations that are also defined in terms of 2^{2^t}-ary bits of integers but now we will allow in the definitions statement which consider inequalities between the corresponding digits of two integers. For example such a relation is "$R^{(d)}(a,b,t)$ iff (for all $k \in 2^{d-t}$, $a[k,t] \leq b[k,t]$)" (see Lemma 21). We will show that this particular family of relations is uniformly existential, and we will state many similar results which will be useful later in proving the Circuit Simulation Lemma. □

Lemma 17 *The family of binary relations* $\langle R^{(d)} \mid d \in \omega \rangle$ *is uniformly propositional on* $\mathbf{M}$*, where*

(24) $R^{(d)}$ *is the binary relation defined on* $\mathbf{M}_d$ *by* $R^{(d)}(a,t)$ *iff* $t \leq d$ *and for all* $i \in 2^{d-t}$*,* $a[i,t]$ *is either* 0 *or* $2^{2^t}-1$*.*

Remark. 1. In this lemma the definition of the relation $R^{(d)}$ contains a universal quantification on the set 2^{d-t}. In spite of that, we have to show that the definition is equivalent to a propositional statement. We do this by showing that a vector of length 2^{d-t}, namely a vector consisting of the 2^{2^t}-ary digits of an integer depending on a is the 0 vector. We will use frequently this argument to eliminate of a universal quantifier (restricted to 2^{d-t}).

2. The condition "for all $i \in 2^{d-t}$, $a[i,t]$ is either 0 or $2^{2^t}-1$" is equivalent to the following: the sequence of first 2^d binary bits of a is formed from blocks of 0s and 1s each of length exactly 2^t, or equivalently the value $a[i,0]$ depends only on $\lfloor i/2^t \rfloor$ for all $i \in 2^{d-t}$. In the proof we will use the fact that if we consider the same blocks for the binary bits of the integer $e_{d,t}$ then the least significant bit in such a block is 1 and all of the other bits are zeros.

Proof of Lemma 17. The relation $R^{(d)}(a,t)$ is equivalent to the following: $t \leq d$ and for all $i \in 2^d$, if $i \not\equiv 0 \pmod{2^t}$ then the ith binary bit of a is the same as the $i-1$th binary bit of a (which is the ith bit of $2a$). Using the observation about $e_{d,t}$ in the previous remark we get the following. $R^{(d)}(a,t)$ holds iff $t \leq d$ and for all $i \in 2^d$, $A(i,t,a)$ holds, where $A(i,t,a) \equiv$ "if $e_{d,t}[i,0] \neq 1$ then $a[i,0] = (2a)[i,0]$". By Lemma 13 and Lemma 8 there exists terms η, ξ of $\mathcal{M}$ such that $e_{d,t}[i,0] = (\eta(i,t))_{\mathbf{M}_d}$ and $a[i,0] = (\xi(i,a))_{\mathbf{M}_d}$. Condition A can be expressed by boolean vector operations on the binary bits of the integers $e_{d,t}, a$ and $2a$, in the sense that A holds iff all of the components of the resulting vectors are 0s. Therefore Lemma 15 implies that the relation A is propositional. *Q.E.D.*(Lemma 17)

Definition. Assume that $t, a, i \in \omega$. We define a function $\mathtt{bit}_{a,t,i}$ on 2^t by $\mathtt{bit}_{a,t,i}(k) = (a[i,t])[k,0]$ for all $k \in 2^t$. According to this definition, $\mathtt{bit}_{a,t,i}(k)$ is the kth binary bit of the ith 2^{2^t}-ary digit of the integer a. We define another function $\mathtt{incr}_{a,t,i}(k)$, by $\mathtt{incr}_{a,t,i}(k) = \max_{j=0}^{k} \mathtt{bit}_{a,t,i}(k)$ for all $k \in 2^t$. For fixed a, t and i, $\mathtt{incr}_{a,t,i}(k)$ is monotone increasing in k and taking values in the set $0, 1$. The function $\mathtt{incr}_{a,t,i}$ can be also defined by recursion, namely, $\mathtt{incr}_{a,t,i}(0) = \mathtt{bit}_{a,t,i}(0)$ and for all $k \in 2^t - 1$, $\mathtt{incr}_{a,t,i}(k+1) = \max\{\mathtt{bit}_{a,t,i}(k+1), \mathtt{incr}_{a,t,i}(k)\}$. We define also a monotone decreasing function $\mathtt{decr}_{a,t,i}$ on 2^t by a similar recursion in the opposite direction $\mathtt{decr}_{a,t,i}(2^t-1) = \mathtt{bit}_{a,t,i}(2^t-1)$ and for all $k \in 2^t \backslash \{0\}$, $\mathtt{decr}_{a,t,i}(k-1) = \max\{\mathtt{bit}_{a,t,i}(k-1), \mathtt{decr}_{a,t,i}(k)\}$. Equivalently, for all $k \in 2^t$, $\mathtt{decr}_{a,t,i}(k) = \max_{j=k}^{2^t-1} \mathtt{bit}_{a,i,t}(j)$. For fixed a, i, t, the function $\mathtt{decr}_{a,t,i}(k)$ is monotone decreasing in k.

Lemma 18 *Each family of relations* $R = \langle R^{(d)} \mid d \in \omega \rangle$ *on* $\mathbf{M}$*, defined in one of the conditions below, is uniformly propositional on* $\mathbf{M}$*.*

(25) $R^{(d)}$ *is the ternary relation on* $\mathbf{M}_d$ *defined by* $R^{(d)}(a,t,b)$ *iff* $t \leq d$ *and for all* $i \in 2^{t-d}$*,* $k \in 2^t$ *we have* $\mathtt{bit}_{b,t,i}(k) = \mathtt{incr}_{a,t,i}(k)$*.*

(26) *$R^{(d)}$ is the ternary relation on $\mathbf{M}_d$ defined by $R^{(d)}(a,t,b)$ iff $t \leq d$ and for all $i \in 2^{t-d}$, $k \in 2^t$ we have $\mathtt{bit}_{b,t,i}(k) = \mathtt{decr}_{a,t,i}(k)$.*

Remark. The importance of this lemma is that the result of the recursive process contained in the definition of the function $\mathtt{incr}_{a,t,i}$ can be verified by a propositional statement. □

Proof of Lemma 18. We use similar reasoning in this proof as in the proof of Lemma 17. Consider first of condition (25). For given d, a, t clearly there exists a unique $b \in \mathbf{M}_d$ such that for all $i \in 2^{d-t}$ and $k \in 2^t$, $\mathtt{bit}_{b,t,i}(k) = \mathtt{incr}_{a,t,i}(k)$, since all the bits of b are determined. This integer b is also uniquely determined by the following condition: "for all $j \in 2^{d-t}$ if $e_{d,t}[j,0] = 1$, then $b[j,0] = a[j,0]$, if $e_{d,t}[j,0] = 0$ then $b[j,0] = \max\{a[j,0], b[j-1,0]\} = \max\{a[j,0], (2b)[j,0]\}$" using the same argument as in the case of Lemma 17 we get that the family $R^{(d)}$ is propositional. Statement (26) can be proved in a similar way. *Q.E.D.*(Lemma 17)

Definition. For all $d, t \in \omega$, $t \leq d$, we define two functions $\mathtt{Incr}_t^{(d)}$, $\mathtt{Decr}_t^{(d)}$ on $\mathbf{M}_d$ with values in $\mathbf{M}_d$. For each $a \in \mathbf{M}_d$, $\mathtt{Incr}_t^{(d)}(a)$ will be the unique integer $b \in \mathbf{M}_d$ such that for all $i \in 2^{d-t}$ and $k \in 2^t$, we have $\mathtt{bit}_{b,t,i}(k) = \mathtt{incr}_{a,t,i}(k)$. For each $a \in \mathbf{M}_d$, $\mathtt{Decr}_t^{(d)}(a)$ will be the unique integer $b \in \mathbf{M}_d$ such that for all $i \in 2^{d-t}$ and $k \in 2^t$, we have $\mathtt{bit}_{b,t,i}(k) = \mathtt{decr}_{a,t,i}(k)$.

Lemma 19 *The family of binary functions $f_0^{(d)}$, $f_1^{(d)}$, $d \in \omega$ defined below are uniformly propositional.*

(27) *For each $a, t \in \mathbf{M}_d$, if $t \leq d$ then $f_0^{(d)}(a,t) = \mathtt{Incr}_t^{(d)}(a)$, otherwise $f_0^{(d)}(a,t) = 0$.*

(28) *For each $a, t \in \mathbf{M}_d$, if $t \leq d$ then $f_1^{(d)}(a,t) = \mathtt{Decr}_t^{(d)}(a)$, otherwise $f_1^{(d)}(a,t) = 0$.*

Proof of Lemma 19. The lemma is an immediate consequence of Lemma *Q.E.D.*(Lemma 18)

Lemma 20 *Each family of ternary relations $\langle R^{(d)} \mid d \in \omega \rangle$ defined below is uniformly existential on $\mathbf{M}$, where*

(29) *$R^{(d)}$ is the ternary relation on $\mathbf{M}_d$ defined by $R^{(d)}(a,b,t)$ iff $t \leq d$ and for all $k \in 2^{d-t}$, $b[k,t] = 0$ if $a[k,t] = 0$, and $b[k,t] = e_{d,t}[k,t]$ otherwise.*

(30) *$R^{(d)}$ is the ternary relation on $\mathbf{M}_d$ defined by $R^{(d)}(a,b,t)$ iff $t \leq d$ and for all $k \in 2^{d-t}$, $b[k,t] = 0$ if $a[k,t] = 0$, and $b[k,t] = 1$ otherwise.*

Proof of Lemma 20. Statement (29). Assume that $t \leq d$. The definition of the relation $R^{(d)}$ implies that $R^{(d)}(a,b,t)$ holds iff for all $i \in 2^{d-t}$ either each binary bit of $b[i,t]$ is 1 or each binary bit of $b[i,t]$ is 0, (depending on whether $a[i,t]$ has a nonzero bit or not). Therefore the definitions of the functions $\mathtt{Incr}^{(d)}$ and $\mathtt{Decr}^{(d)}$ imply that $R^{(d)}(a,b,t)$

iff $b = \mathtt{Decr}_t^{(d)}(\mathtt{Incr}_t^{(d)}(a))$. Therefore $R^{(d)}(a,b,t)$ iff there exists a $c \in \mathbf{M}_d$ such that $b = \mathtt{Decr}_t^{(d)}(c)$ and $c = \mathtt{Incr}_t^{(d)}(a)$. By Lemma 19 the families of functions `Incr` and `Decr` are uniformly propositional therefore the family $R^{(d)}$, $d \in \omega$ is uniformly existential.

Statement (30) is a consequence of statement (29) of the present lemma and statement (14) of Lemma 14 and Lemma 13. Suppose that $t \leq d$ and let R_0 be the relation defined in condition (29), and let R be the relation defined in condition (30), then $R(a,b,t)$ holds iff there exists a $c \in \mathbf{M}_d$ such that $R_0(a,c,t)$ and for all $i \in 2^d$ we have that $e_{d,t}[i,0] = 1$ implies that $b[i,0] = c[i,0]$ and $e_{d,t}[i,0] = 0$ implies that $b[i,0] = 0$. By Lemma 13 $e_{d,t}$ is the value of a term, and by statement (14) of Lemma 14 the fact that a boolean relations holds between the ith bits of the integers b, c, and $e_{d,t}$ can be expressed by a propositional formula. *Q.E.D.*(Lemma 20)

Lemma 21 *The families of ternary relations* $\langle R_i^{(d)} \mid d \in \omega \rangle$, $i = 0, 1$ *defined below are uniformly existential on* $\mathbf{M}$, *where*

(31) $R_0^{(d)}$ *is the ternary relation on* $\mathbf{M}_d$ *defined by* $R_0^{(d)}(a,b,t)$ *iff* $t \leq d$ *and for all* $k \in 2^{d-t}$, $a[k,t] \neq b[k,t]$,

(32) $R_1^{(d)}$ *is the ternary relation on* $\mathbf{M}_d$ *defined by* $R_1^{(d)}(a,b,t)$ *iff* $t \leq d$ *and for all* $k \in 2^{d-t}$, $a[k,t] \leq b[k,t]$.

Proof of Lemma 21. According to statement (13) of Lemma 14 we may assume that $t \leq d$.

Statement (31). Let w be the unique element of $\mathbf{M}_d$ such that for all $i \in 2^d$, $w[i,0]$ is the exclusive or of $a[i,0]$ and $b[i,0]$, and let $w' = \mathtt{Decr}_t^{(d)}(Incr_t^{(d)})(a)$. Clearly $R_0^{(d)}(a,b,t)$ iff $w' = e_t$. Therefore Lemma 19 and Lemma 13 with $t = 0$ imply that the family $R_0^{(d)}$ is uniformly existential.

(32). We claim that

(33) $R_1^{(d)}(a,b,t)$ *iff* $\mathbf{M}_d \models a \leq b \wedge b = a \oplus_{d,t} (b - a)$.

According to statement (20) of Lemma 14 this implies our assertion. We prove now statement (33). If $R_1^{(d)}(a,b,t)$ holds then looking at the binary representations of a and b we get that $a \leq b$, and for all $k \in 2^{d-t}$, $b[k,t] = (b[k,t] - a[k,t]) + a[k,t]$, where both terms are nonnegative. Therefore the definition of the operation $\oplus_{d,t}$ implies that $\mathbf{M}_d \models a \leq b \wedge b = a \oplus_{d,t} (b - a)$ holds. Assume now that $\mathbf{M}_d \models a \leq b \wedge b = a \oplus_{d,t} (b - a)$ holds and let $c = b - a$. Since $a \leq b$ the integer operation and the operation in $\mathbf{M}_d$ gives the same value for c. We perform the integer addition $a + c$ in the 2^{2^t}-ary number system, starting from the least significant digits, $a[0,t], c[0,t]$. As long as there is no carryover the condition $b = a \oplus_{d,t} c$ implies that $a[k,t] \leq b[k,t]$ as required by $R_1^{(d)}(a,b,t)$. We claim that $\mathbf{M}_d \models a \leq b \wedge b = a \oplus_{d,t} (b - a)$ implies that there is no carryover at all. Assume that the first carryover occurs at the addition $a[k,t] + c[k,t]$ for some $k < 2^{d-t} - 1$. This implies that when we add $a[k+1,t] + c[k+1,t]$ we have to add the carryover 1. On the

other hand, because of $b = a \oplus_{d,t} c$, we have $a[k+1,t]+c[k+1,t] \equiv b[k+1,t] \pmod{2^{2^t}}$ so together with the carryover 1 we do not get $b[k+1,t]$ as the next digit, a contradiction. Assume now that the carryover occurs at $k = 2^{d-t} - 1$. This however, together with $b = a \oplus_{d,t} c$, contradicts the assumption $\mathbf{M}_d \models a \leq b$. *Q.E.D.*(Lemma 21)

Definition. Assume that $d, t \in \omega$, $d \geq t$. The set of all integers $a \in \mathbf{M}_d$ such that for all $j \in 2^{d-t}$, $a[j,t] \in \{0,1\}$. We will be called the zero-one set of $\mathbf{M}$ with parameters d, t and will be denoted by $\mathtt{zo}(d,t)$. □

Lemma 22 *For each $d \in \omega$, let $R^{(d)}(x,y)$ be the binary relation on $\mathbf{M}_d$ defined by: for each $a, t \in \mathbf{M}_d$, $R^{(d)}(a,t)$ iff $t \leq d$ and $a \in \mathtt{zo}(d,t)$. Then the family of binary relations $R = \langle R^{(d)} \mid d \in \omega \rangle$ is uniformly existential on $\mathbf{M}$.*

Proof of Lemma 22. Assume that $d, t \in \omega$, $d \leq t$. Recall that $e_{d,t}$ is the unique element of $\mathbf{M}_d$ such that for all $j \in 2^{d-t}$, $e_{d,t}[j,t] = 1$. For all $a \in \mathbf{M}_d$, we have $a \in \mathtt{zo}$ iff for all $j \in 2^{d-t}$, $a[j,t] \leq e_{d,t}[j,t]$. Therefore Lemma 13 and statement (31) of Lemma 21 imply the conclusion of the lemma. *Q.E.D.*(Lemma 22)

Lemma 23 *Assume that f is boolean function of two variables. Then the family of relations $R = \langle R^{(d)} \mid d \in \omega \rangle$, is uniformly existential on $\mathbf{M}$, where*

(34) *$R^{(d)}$ is the quaternary relation on $\mathbf{M}_d$ defined by $R^{(d)}(a,b,c,t)$ iff $t \leq d$, for all $k \in 2^{d-t}$, $a[k,t], b[k,t], c[k,t] \in \{0,1\}$, and $f(a[k,t], b[k,t]) = c[k,t]$.*

Proof of Lemma 23. Lemma 22 implies that the relation $\Phi(a,b,c,t) \equiv$"$t \leq d$ and $a[k,t], b[k,t], c[k,t] \in \{0,1\}$" is uniformly existential on $\mathbf{M}$. Assume now that for some $d \in \omega$ and $a, b, c, t \in \mathbf{M}_d$, and $\Phi(a,b,c,t)$ holds. Then, using statement (14) of Lemma 14 and the fact that for all $i \in 2^d$, $e_{d,t}[i,0] = 1$ if $i \equiv 0 \pmod{2^t}$ and $e_{d,t}[i,0] = 0$ otherwise, we may express $f(a[k,t], b[k,t]) = c[k,t]$ uniformly on $\mathbf{M}$ by a propositional formula of $\mathcal{M}$. *Q.E.D.*(Lemma 23)

Lemma 24 *Assume that $m \in \omega$ and $\mathcal{B}(X_0, ..., X_{m-1})$ is a boolean expression, where $X_0, ..., X_{m-1}$ are boolean variables. Then the family of $m+2$-ary relations $R = \langle R^{(d)} \mid d \in \omega \rangle$ on $\mathbf{M}$, is uniformly existential on $\mathbf{M}$, where*

(35) *$R^{(d)}$ is the $m+2$-ary relation on $\mathbf{M}_d$ defined by $R^{(d)}(a_0, ..., a_{m-1}, c, t)$ iff $t \leq d$, for all $k \in 2^{d-t}$, $a_0[k,t], ..., a_{m-1}[k,t], c[k,t] \in \{0,1\}$, and $\mathcal{B}(a_0[k,t], ..., a_{m-1}[k,t]) = c[k,t]$.*

Proof of Lemma 24. The lemma follows from Lemma 23 and Lemma 22. Let $\mathcal{B} = \mathcal{B}_0, \mathcal{B}_1, ..., \mathcal{B}_{s-1}, \mathcal{B}_s, ..., \mathcal{B}_{s+m-1}$ be the sequence of all subformulas of $\mathcal{B}$, where $\mathcal{B}_0, \mathcal{B}_1, ..., \mathcal{B}_{s-1}$ are not variables, and $\mathcal{B}_s, ..., \mathcal{B}_{s+m-1}$ are variables. Assume that for all $i \in s$, $\mathcal{B}_i = f_i(\mathcal{B}_{i_0}, \mathcal{B}_{i_1})$, where f_i is a boolean operation of two variables. Suppose that $t \leq d$ and for all $k \in 2^{d-t}$, $a_0[k,t], ..., a_{m-1}[k,t], c[k,t] \in \{0,1\}$. Then $\mathbf{M}_t \models R^{(d)}(a_0, ..., a_{m-1}, c, t)$ iff exists $u_0, ..., u_{s+m-1}$ such that for all $i = s, ..., s+m-1$ $a_i = u_i$, and for all $i \in s$ and $k \in 2^{d-t}$, $u_i[k,t] = f_i(u_{i_0}[k,t], u_{i_1}[k,t])$. Lemma 23 and

Lemma 22 imply that this condition can be expressed uniformly by an existential formula of $\mathcal{M}$. *Q.E.D.*(Lemma 24)

The following lemma implies the Vector Property (formulated in section 2) for the operations max and min.

Lemma 25 *The families of quaternary relations* $\langle R_i^{(d)} \mid d \in \omega \rangle$, $i = 0, 1$ *are uniformly existential on* $\mathbf{M}$, *where*

(36) $R_0^{(d)}$ *is the quaternary relation on* $\mathbf{M}_d$ *defined by* $R_0^{(d)}(a, b, u, t)$ *iff* $t \leq d$ *and for all* $k \in 2^{d-t}$, $u[k, t] = \min\{a[k, t], b[k, t]\}$, *and*

$R_1^{(d)}$ *is the quaternary relation on* $\mathbf{M}_d$ *defined by* $R_1^{(d)}(a, b, u, t)$ *iff* $t \leq d$ *and for all* $k \in 2^{d-t}$, $u[k, t] = \max\{a[k, t], b[k, t]\}$.

Remark. For the proof of Lemma 25 we need two other lemmas. In these lemmas we show that we can define in a uniformly existential way $0, 1$-valued functions on the set 2^{d-t} which select the values $k \in 2^{d-t}$ where $a[k, t] \neq b[k, t]$ or where $a[k, t] \leq b[k, t]$. In the proof of Lemma 25 these and similar $0, 1$-valued functions, which can be represented by a single element of $\mathbf{M}_d$, will be existentially quantified. □

Lemma 26 *The family of quaternary relations* $\langle R^{(d)} \mid d \in \omega \rangle$, *is uniformly existential on* $\mathbf{M}$, *where*

(37) $R^{(d)}$ *is the quaternary relation on* $\mathbf{M}_d$ *defined by* $R^{(d)}(a, b, w, t)$ *iff* $t \leq d$ *and for all* $k \in 2^{d-t}$, $a[k, t] = b[k, t] \rightarrow w[k, t] = 0$, *and* $a[k, t] \neq b[k, t] \rightarrow w[k, t] = 1$

Proof of Lemma 26. As in the previous lemmas we will assume that $t \leq d$. Let β be the unique element of $\mathbf{M}_d$ such that for all $k \in 2^{d-t}$, $\beta[k, t] \equiv -b[k, t] \pmod{2^{2^t}}$, and let $c = a \oplus_{d,t} \beta$. Conditions (22) and (20) of Lemma 14 imply that c has a uniform propositional definition, that is a propositional formula $P(x, y, z, s)$ such that $\mathbf{M}_d \models \forall x, P(x, a, b, t) \leftrightarrow x = c$, where P does not depend on d, t, a or b. Clearly for all $k \in 2^{d-t}$, $c[k, t] = 0 \rightarrow w[k, t] = 0$, and $c[k, t] \neq 0 \rightarrow w[k, t] = 1$ and so $R^{(d)}(a, b, w, t)$ iff

$$\mathbf{M}_d \models t \leq d \wedge \exists c, P(c, a, b, t) \wedge \forall k < 2^t, \Psi(c, w, k, t)$$

where

$$\Psi(c, w, k, t) \equiv (c[k, t] = 0 \rightarrow w[k, t] = 0) \wedge (c[k, t] \neq 0 \rightarrow w[k, t] = 1)$$

Therefore the statement of the lemma follows from condition (30) Lemma 20 with $a{:=}\, c$ and $b{:=}\, w$. *Q.E.D.*(Lemma 26)

Lemma 27 *The family of quaternary relations* $\langle R^{(d)} \mid d \in \omega \rangle$, *is uniformly existential on* $\mathbf{M}$, *where*

(38) $R^{(d)}$ *is the quaternary relation on* $\mathbf{M}_d$ *defined by* $R^{d)}(a, b, w, t)$ *iff* $t \leq d$ *and for all* $k \in 2^{d-t}$, $a[k, t] \leq b[k, t] \rightarrow w[k, t] = 0$, *and* $a[k, t] > b[k, t] \rightarrow w[k, t] = 1$.

Proof of Lemma 27. As in the previous proofs we may assume that $t \leq d$. First we prove the lemma for the modified relation $\bar{R}^{(d)}$ defined by,

(39) $\bar{R}^{(d)}(a,b,w,t)$ *iff* $R^{(d)}(a,b,w,t) \wedge (a = (a)_{d,t,0}) \wedge (b = (b)_{d,t,0})$.

Let c be the unique element of $\mathbf{M}_d$ such that $a \oplus_{d,t} c = b$. As we have seen in the proof of Lemma 26 the element c has a uniform propositional definition. It is a consequence of condition (39) and the definition of c that

(40) $a + c = b$ *(among the integers) iff for each even* $k \in 2^{d-t}$, $a[k,t] \leq b[k,t]$.

Lemma 16 implies that "$a + c = b$ among the integers" is a uniformly propositional relation on $\mathbf{M}$ therefore "for each odd $k \in 2^{d-t}$, $a[k,t] \leq b[k,t]$"$\equiv \exists c, a+c = b$ is uniformly existential. This completes the proof for the family of relations $\bar{R}^{(d)}$. The same proof works also for the relation $\tilde{R}^{(d)}(a,b,w,t)$ iff $R^{d)}(a,b,w,t) \wedge (a = (a)_{d,t,1}) \wedge (b = (b)_{d,t,1})$. We have $a = (a)_{d,t,0} + (a)_{d,t,1}$, $b = (b)_{d,t,0} + (b)_{d,t,1}$. First we apply the already proven part of the lemma for the pair $(a)_{d,t,0}, (b)_{d,t,0}$ and get a uniformly existential definition for the corresponding element w that we will denote by $\bar{w}$. Using the pair $(a)_{d,t,1}, (b)_{d,t,1}$ in a similar way we get an existential definition for $\tilde{w}$. We have $R(a,b,w,t)$ iff $\mathbf{M}_d \models w = \bar{w} + \tilde{w}$ which together with the existential defintions of $\bar{w}$ and $\tilde{w}$ gives the existential formula for $R^{(d)}$. *Q.E.D.*(Lemma 27)

Proof of Lemma 25. As in the previous lemmas we may assume that $t \leq d$. We consider first the family of relations $R_0^{(d)}$. The existential formula defining the relation $R_0^{(d)}$ will be equivalent to the following statement.

There exists $v, w, w' \in \mathbf{M}_d$ *such that,*
(i) for all $k \in 2^{d-t}$, $a[k,t] \leq b[k,t] \rightarrow v[k,t] = 0$, *and* $a[k,t] > b[k,t] \rightarrow v[k,t] = 1$, *and*
(ii) for all $k \in 2^{d-t}$, $a[k,t] = u[k,t] \rightarrow w[k,t] = 0$, *and* $a[k,t] \neq u[k,t] \rightarrow w[k,t] = 1$, *and*
(iii) for all $k \in 2^{d-t}$, $b[k,t] = u[k,t] \rightarrow w'[k,t] = 0$, *and* $b[k,t] \neq u[k,t] \rightarrow w'[k,t] = 1$, *and*
(iv) for all $k \in 2^{d-t}$, $w[k,t] = 0 \rightarrow v[k,t] = 0$, *and* $w[k,t] = 1 \rightarrow (w'[k,t] = 0 \wedge v[k,t] = 1)$.

We claim that this statement is equivalent to $R_0(a,b,u,t)$. First we show that if $u[k,t] = \min\{a[k,t], b[k,t]\}$ for all $k \in 2^{d-t}$, then there exist $v, w, w' \in \mathbf{M}_d$ satisfying conditions (i),(ii),(iii) and (iv). We define for each fixed $k \in 2^{d-t}$, the integer $v[k,t] \in \{0,1\}$ by condition (i). This gives a $v \in \mathbf{M}_d$ satisfying condition (i). In a similar way we define the integer $w \in \mathbf{M}_d$ by condition (ii) and the integer $w' \in \mathbf{M}_d$ by condition (iii). We have to show that the integers v, w, w' defined this way satisfy condition (iv). Suppose that a $k \in 2^{d-t}$ is fixed.

If $w[k,t] = 0$ then by condition (ii) $a[k,t] = u[k,t] = \min\{a[k,t], b[k,t]\} \leq b[k,t]$ and therefore by condition (i) $v(k,t) = 0$.

If $w[k,t] = 1$ then by condition (ii) $a[k,t] \neq u[k,t] = \min\{a[k,t], b[k,t]\}$. Therefore $u[k,t] = b[k,t] < a[k,t]$. Condition (iii) and $u[k,t] = b[k,t]$ implies $w'[k,t] = 0$. Condition (i) and $b[k,t] < a[k,t]$ implies $v[k,t] = 1$, which completes the proof of condition (iv) and the fact that there exist integers v, w, w' satisfying conditions (i),(ii),(iii) and (iv).

Assume now that there exist integers $v, w, w' \in \mathbf{M}_d$ satisfying conditions (i),(ii),(iii) and (iv) and we show that for all $k \in 2^{d-t}$, $u[k,t] = \min\{a[k,t], b[k,t]\}$. Suppose that a $k \in 2^{d-t}$ is fixed. Statement (ii) implies that $w[k,t]$ is either 0 or 1. If $w[k,t] = 0$ then according to (iv) $v(k,t) = 0$ and by (ii) $u[k,t] = a[k,t]$. $v(k,t) = 0$ and (i) implies that $a[k,t] \leq b[k,t]$ and therefore $u[k,t] = \min\{a[k,t], b[k,t]\}$.

Assume now that $w[k,t] = 1$. According to (iv) $v(k,t) = 1$ and $w'(k,t) = 0$. Therefore by (i) $a[k,t] > b[k,t]$ and by (iii) $b[k,t] = u[k,t]$. Consequently $u[k,t] = \min\{a[k,t], b[k,t]\}$. This completes the proof of the fact that $R_0(a,b,u,t)$ holds iff there exist integers v, w, w' satisfying conditions (i),(ii),(iii) and (iv).

All of the four statements (i), (ii), (iii), and (iv) are uniformly existential on $\mathbf{M}$. This can be proved in each case separately using the following lemmas: statement (i): Lemma 27, statement (ii): Lemma 26, statement (iii): Lemma 26, statement (iv): Lemma 23.

The statement of the lemma for the family of relations $R_1^{(d)}$ can be proved in a similar way, or we may use the fact that $\mathbf{M}_d \models \forall x, y, \max(x,y) = -\min(-x,-y)$. *Q.E.D.*(Lemma 25)

Definition. 1. Let $\mathbf{f}$ be a k-ary function symbol of $\mathcal{M}$ for some $k \in \{0,1,2\}$. For all $d, t \in \omega$ with $d \geq t$, we define a k-ary function $\Upsilon_{\mathbf{f},d,t}$ on the universe $\mathbf{M}_d$ in the following way. Assume that $d, t \in \omega$ is fixed with $d \geq t$ and $a_0, ..., a_{k-1} \in \mathbf{M}_d$. Then $\Upsilon_{\mathbf{f},d,t}(a_0, ..., a_{k-1})$ is the unique element $b \in \mathbf{M}_d$ with the property that for all $i \in 2^{d-t}$, we have $\mathbf{M}_t \models \mathbf{f}(a_0[i,t], ..., a_{k-1}[i,t]) = b[i,t]$. The function $\Upsilon_{\mathbf{f},d,t}$ will be also called the parallel version of the operation $\mathbf{f}$. In the special cases $\mathbf{f} = +, \times$ we will use the notation $\Upsilon_{+,d,t} = \oplus_{d,t}$ $\Upsilon_{\times,d,t} = \otimes_{d,t}$. For the remaining function symbols $\mathbf{f}$ we will sometimes write $\mathbf{f}_{d,t}$ instead of $\Upsilon_{\mathbf{f},d,t}$, e.g. we may write $\dot{-}_{d,t}$, $\min_{d,t}$, $\cap_{d,t}$ etc.

2. Let $\mathbf{f}$ be a k-ary function symbol of $\mathcal{M}$ for some $k \in \{0,1,2\}$. We define a family of $k+2$-ary relations $\bar{\Upsilon}_{\mathbf{f}} = \langle \bar{\Upsilon}_{\mathbf{f}}^{(d)} \mid d \in \omega \rangle$ on $\mathbf{M}$. For all $d \in \omega$ and for all $a_0, ..., a_{k-1}, b, t \in \mathbf{M}_d$, $\bar{\Upsilon}^{(d)}(a_0, ..., a_{k-1}, b, t)$ iff $t \leq d$ and $\Upsilon_{\mathbf{f},d,t}(a_0, ..., a_{k-1}) = b$. We will say that the parallel $\mathbf{f}$ operation is uniformly existential on $\mathbf{M}$, if the family of relations $\bar{\Upsilon}_{\mathbf{f}}$ is uniformly existential on $\mathbf{M}$. □

Lemma 28 *Suppose that* $\mathbf{f}$ *is a function symbol of* $\mathcal{M}$ *such that* $\mathbf{f} \notin \{\times, \dot{-}, \mathbf{p}\}$. *Then the parallel* $\mathbf{f}$ *operation is uniformly existential on* $\mathbf{M}$.

Remark. 1. For some of the function symbol even more is true, in the sense that the family of relations $\bar{\Upsilon}_f$ is uniformly propositional. See e.g., statement (20) of Lemma 14 about the parallel version of addition, which was denoted by $\oplus_{d,t}$.

2. For the three the function symbols $\times, \dot{-}, \mathbf{p}$ we will be able to prove the lemma only in a weaker form, namely the existential formula defining the relation $\bar{\Upsilon}_{\mathbf{f},d,t}$ will not be considered in the structure $\mathbf{M}_d$ but in a larger structure $\mathbf{M}_{d+c(d-t)}$ for a sufficiently large constant $c \in \omega$. This generalized form of the lemma will have a crucial role in the proof of Theorem 3. □

Proof of Lemma 28. We show separately for each function symbols of $\mathcal{M}$, that the statement of the lemma is true.

Symbol $\mathbf{0}$. $\Upsilon_{\mathbf{0},d,t} = b$ is equivalent to $\mathbf{M}_d \models b = \mathbf{0}$.

Symbol $\mathbf{1}$. $\Upsilon_{\mathbf{1},d,t} = b$ is equivalent to $\mathbf{M}_d \models b = e_{d,t}$, therefore Lemma 13 implies our statement.

Symbol $-\mathbf{1}$. $\Upsilon_{-\mathbf{1},d,t} = b$ is equivalent to $\mathbf{M}_d \models b = -\mathbf{1}$. (Indeed for all $i \in 2^t$, $\mathbf{M}_t \models b[i,t] = -\mathbf{1}$ implies that all of the 2^t binary bits of $b[i,t]$ is 1.)

Symbol $+$. This follows from statement (20) of Lemma 14.

Symbol $\mathbf{n}$. $\Upsilon_{\mathbf{n},d,t} = b$ is equivalent to $b[i,t] = 2^t$ for all $i \in 2^{d-t}$, that is, $b = 2^t e_{d,t}$. Therefore our statement follows from Lemma 13.

Symbols $\mathcal{N}$ and $\cap$. The statement is an immediate consequence of the fact that these two operations are boolean vector operations performed on the binary forms of the arguments.

Symbols max and min. The statement is equivalent to Lemma 25. *Q.E.D.*(Lemma 28)

Definition. For all $d, t \in \omega$ with $d \geq t$, we define a binary relations $<_{d,t}$ on $\mathbf{M}_d$, by $a <_{d,t} b$ iff for all $i \in 2^{d-t}$, $a[i,t] < b[i,t]$. □

Lemma 29 *The family of ternary relations $Q = \langle Q_d \mid d \in \omega \rangle$ is uniformly existential, where for all $d \in \omega$ and for all $a, b, t \in \mathbf{M}_d$, we have $Q_d(a,b,t)$ iff "$d \geq t$ and $a <_{d,t} b$".*

Proof of Lemma 29. Let R be the quaternary family of relations defined in Lemma 27. Then for all $d \in \omega$ and for all $a, b, t \in \mathbf{M}_d$ we have $Q_d(a,b,t)$ iff $R_d(b, a, e_{d,t}, t)$. By Lemma 13, $e_{d,t}$ can be written as a 0-ary term, therefore Lemma 27 implies our statement. *Q.E.D.*(Lemma 29

Lemma 30 *For each boolean function $\delta(x,y)$ of two variables the family of quaternary relations $R = \langle R^{(d)} \mid d \in \omega \rangle$ is uniformly existential where for all $d \in \omega$ with $t \leq d$, and for all $a, b, c, t \in \mathbf{M}_d$, $R^{(d)}(a,b,c,t)$ iff $t \leq d$ and for all $i \in 2^{d-t}$, $c[i,t] = \delta(\min(a[i,t], 1), \min(b[i,t], 1))$.*

Proof of Lemma 30. Assuming that $t \leq d$, $R^{(d)}(a,b,c,t)$ is equivalent to the following.

(41) *There exists $a', b' \in \mathbf{M}_d$ such that $a' = \mathtt{Decr}_t^{(d)}(\mathtt{Incr}_t^{(d)}(a))$, $b' = \mathtt{Decr}_t^{(d)}(\mathtt{Incr}_t^{(d)}(a))$, and for all $i \in 2^d$, either "$e_{d,t}[i,0] = 1$ and $c[i,0] = \delta(a'[i,0], b'[i,0])$" or "$e_{d,t}[i,0] = 0$ and $c[i,0] = 0$".*

By Lemma 19 the definitions of a' and b' are uniformly propositional, by Lemma 13 $e_{d,t}$ is the value of a term, therefore statement (14) of Lemma 14 imply that the relation described in condition (41) is uniformly propositional. Consequently the family of relations $R^{(d)}$, $d \in \omega$ is uniformly existential. (We can get another proof by using Lemma 23 and the fact that the function $\min_{d,t}$ is uniformly existential, as stated in Lemma 28.) *Q.E.D.*(Lemma 30)

Lemma 31 *The family of quaternary relations $R^{(d)}$, $d \in \omega$ is uniformly existential, where for all $d, a, b, c, t \in \omega$, $R^{(d)}(a,b,c,t)$ holds iff $t \leq d$ and $a \oslash_{d,t} b = c$*

Proof of Lemma 31. We may assume that $t \leq d$. Then $a \oslash_{d,t} b = c$ iff either (($b > 2^{2^t}$ or $b = 0$) and $c = 0$) or "$b \leq 2^{2^t}$ and there exists a $w \in \mathbf{M}_d$, such that $w <_{d,t} b$ and $a = (b \odot_{d,t} c) \oplus_{d,t} w$". By statement (21) of Lemma 14 the relation $a = (b \odot_{d,t} c) \oplus_{d,t} w$ is uniformly existential, and by Lemma 29 the relation $w <_{d,t} b$ is also uniformly existential. This implies that the relation $a \oslash_{d,t} b = c$ is also uniformly existential. *Q.E.D.*(Lemma 31)

Lemma 32 *Assume that $k, m, l \in \omega$ and $f^{(j)} = \langle f_d^{(j)} \mid d \in \omega \rangle$ are families of k-ary function on $\mathbf{M}$, for $j = 0, 1, \ldots, m-1$ and $g = \langle g_d \mid d \in \omega \rangle$ is a family of m-ary functions on $\mathbf{M}$. Let h be the family of k-ary functions $h = \langle h_d \mid d \in \omega \rangle$ on $\mathbf{M}$ defined by $h_d(a_0, \ldots, a_{k-1}) = g_d(f_d^{(0)}(a_0, \ldots, a_{k-1}), \ldots, f_d^{(m-1)}(a_0, \ldots, a_{k-1}))$ for all $d \in \omega$, $a_0, \ldots, a_{k-1} \in \mathbf{M}_d$. Suppose further that each of the families $g, f^{(0)}, \ldots, f^{(m-1)}$ are uniformly existential on $\mathbf{M}$. Then the family h is also uniformly existential on $\mathbf{M}$.*

Proof of Lemma 32. We have that for all $d \in \omega$, and for all $a_0, ..., a_{k-1}, b \in \mathbf{M}_d$,

$$b = h(a_0, ..., a_{k-1}) \leftrightarrow \Psi(a_0, ..., x_{a-1}, b))$$

where $\Psi(x_0, ..., x_{k-1}, y)$ is the formula

$$\exists z_0, ..., z_{m-1},\ g(z_0, ..., z_{m-1}) = y \wedge \bigwedge_{i=0}^{m-1} z_i = f_i(x_0, ..., x_{k-1})$$

Writing the existential formulas defining the functions $g, f_0, ..., f_{m-1}$ into the formula Ψ we get the existential formula of $\mathcal{M}$ defining the function h. *Q.E.D.*(Lemma 32)

Definition. We will denote by $\mathcal{L}^{(=)}$ the first-order language with equality which contains the constant symbols $\mathbf{0}$, $\mathbf{1}$ and does not contain any other relation symbols, function symbols or constant symbols. For each $m \in \omega$, $\mathbf{N}_d$ will denote a model of $\mathcal{L}^{(=)}$ with $\mathtt{universe}(\mathbf{N}_m) = m$ and $(\mathbf{0})_{\mathbf{N}_m} = 0$, $(\mathbf{1})_{\mathbf{N}_m} = 1$. □

Lemma 33 *Let $k \in \omega$ and let $P(x_0, ..., x_{k-1})$ be a propositional formula of $\mathcal{L}^{(=)}$. Then the family of $k+1$-ary relations $R^{(P)} = \langle R_d^{(P)} \mid d \in \omega \rangle$ is uniformly existential, where for all $d \in \omega$, $a_0, ...a_{k-1}, u \in \mathbf{M}_d$, $R_d^{(P)}(a_0, ..., a_{k-1})$ holds iff $u \leq d$ and for all $i \in 2^{d-u}$,*

$$\mathbf{N}_{\bar{u}} \models P(a_0[i, u], ..., a_{k-1}[i, u])$$

where $\bar{u} = 2^{2^u}$

Proof of Lemma 33. Let $a_k = 0$, $a_{k+1} = e_{d,u}$, and $\kappa = k + 2$. For each $r, s \in \kappa$ let $b_{\kappa r+s} = \min_{d,u}(e_{d,u}, a_r - a_s)$. Lemma 13 implies that $e_{u,d}$ is a term of f and by Lemma 28 the operation $\min_{d,t}$ is uniformly existential. Therefore for each fixed r and s there exists a uniform existential definition for the integer $b_{\kappa r+s}$, consequently, there exists an existential formula $\psi(x_0, ..., x_{k-1}, y, z_0, ..., z_{\kappa^2-1})$ of $\mathcal{M}$ whose choice depends only on k,

such that $b_0, ..., b_{\kappa^2-1}$ is the unique sequence of length κ^2 from the elements of $\mathbf{M}_d$ such that

$$\mathbf{M}_d \models \psi(a_0, ..., a_{k-1}, u, b_0, ..., b_{k^2-1})$$

We have $a_k[i,u] = 0$ and $a_{k+1}[i,u] = 1$ for all $i \in 2^{d-u}$. Therefore for a fixed $i \in 2^{d-u}$ the sequence of $0,1$ values $b_0[i,u], ..., b_{\kappa^2-1}[i,u]$ determines the truth values of the following statements in $\mathbf{N}_{\bar{u}}$: $a_j[i,u] = 0$, $a_j[i,u] = 1$ for all $j \in k$, $a_r[i,u] = a_s[i,u]$ for all $r, s \in k$. Therefore there exists a boolean expression $\mathcal{B}(x_0, ..., x_{\kappa^2-1})$ such that "for all $i \in 2^{d-u}$ $\mathbf{N}_{\bar{u}} \models P(a_0[i,u], ..., a_{k-1}[i,u])$" iff

$$\forall i \in 2^{d-u} \mathcal{B}(b_0[i,u], ..., b_{\kappa^2-1}[i,u]) = 0$$

Lemma 24 implies that this property of the sequence b_i, $i \in \kappa_2$ can be expressed by an existential formula whose choice depends only on κ (and consequently only on k). This completes the proof since we have already seen that the sequence b_i is definable by such an existential formula. *Q.E.D.*(Lemma 33)

Definition. 1. We will denote by $\alpha \circ \beta$ the concatenation of the sequences α and β.

2. Assume that $u, a, i, l \in \omega$, and $\alpha = \langle \alpha_0, ..., \alpha_{l-1} \rangle$ is a sequence of natural numbers. The sequence $a[i + \alpha_0, u], ..., a[i + \alpha_{k-1}, u], a[i - \alpha_0, u], ..., a[i - \alpha_{k-1}, u]$ will be denoted by $\vec{a}[i \pm \alpha \wr u]$. □

Lemma 34 *Let $k, l \in \omega$ and let $P(x_0, ..., x_{2kl-1})$ be a propositional formula of $\mathcal{L}^{(=)}$. Then the family of $k+1$-ary relations $R^{(P)} = \langle R_d^{(P)} \mid d \in \omega \rangle$, is uniformly existential, where for all $d \in \omega$, $a_0, ...a_{k-1}, \alpha_0, ..., \alpha_{l-1}, u \in \mathbf{M}_d$, $\alpha = \langle \alpha_0, ..., \alpha_{l-1} \rangle$, $R_d^{(P)}(a_0, ..., a_{k-1})$ holds iff the following conditions are satisfied:*

(42) *$u \leq d$ and for all $j \in l$, $\alpha_j < 2^{d-u}$*

(43) *and for all $i \in 2^{d-u}$,*

$$\mathbf{N}_{\bar{u}} \models P\Big(\vec{a}_0[i \pm \alpha \wr u] \circ ... \circ a_{k-1}[i \pm \alpha \wr u]\Big)$$

where $\bar{u} = 2^{2^u}$.

Proof of Lemma 34. For each $j \in l$, $r \in k$ we choose an integer $b_{jk+r} \in \mathbf{M}_d$ such that

(44) $\mathbf{M}_d \models b_{jk+r} = 2^{\alpha_j 2^u} a_r$

and with the same j and r another integer that will be denoted by $b_{jl+r+kl}$ such that

(45) $\mathbf{M}_d \models b_{jk+r+lk} = \div(a_r, 2^{\alpha_j 2^u})$.

We apply now Lemma 33 with $k := 2kl$, $a_i := b_i$ for all $i \in 2kl$. Conditions (44) and (45) guarantee that all of the arguments of $P\Big(\vec{a}_0[i \pm \alpha \wr u] \circ ... \circ a_{k-1}[i \pm \alpha \wr u]\Big)$ of condition (43) is of the form $b_j[i,u]$ for a suitably chosen $j \in 2kl$, whose choice does not depend on i.

Therefore there exists a propositional formula $P'(x_0, ..., x_{2kl-1})$ of $\mathcal{L}^{(=)}$ such that for all $i \in 2^{d-u}$, $\mathbf{N}_{\bar{u}} \models P\Big(\vec{a}_0[i \pm \alpha \wr u] \circ ... \circ a_{k-1}[i \pm \alpha \wr u]\Big)$ is equivalent to $\mathbf{N}_{\bar{u}} \models P'(b_0, ..., b_{2kl-1})$, (where P, P' may differ only in the order of its variables.) Therefore Lemma 33 implies the conclusion of the present lemma. *Q.E.D.*(Lemma 34)

3.2 Extending existential formulas to larger structures

In section 3.1 we have proved about several families of relations R_d, $d \in \omega$ that there exists a single existential formula of φ which for each $d \in \omega$ defines the relation R_d in the structure $\mathbf{M}_d$. Sometimes we will need an existential definition for R_d not in the structure $\mathbf{M}_d$ but in another larger structure $\mathbf{M}_q$ with $q \geq d$. The results of this section will show that such an existential definition always exists provided that we can use in it d as a parameter. The following lemma considers the special case when the relation R_d is defined by a single function symbol of $\mathcal{M}$.

Lemma 35 *Suppose that $f(x_0, \ldots, x_{j-1})$ is a function symbol of $\mathcal{M}$. Then there exists a term $t(x_0, \ldots, x_{j-1}, y)$ of $\mathcal{M}$ such that for all $d, q \in \omega$ with $d \leq q$ and for all $a, b_0, \ldots, b_{j-1} \in \mathbf{M}_d$, we have $\mathbf{M}_d \models a = f(b_0, \ldots, b_{j-1})$ iff $\mathbf{M}_q \models a = t(b_0, \ldots, b_{j-1}, d)$.*

Proof Lemma 35. For the various function symbols f of $\mathcal{M}$ the choice of t is the following:

Constant symbols. Assume that f is one of the constant symbols $\mathbf{0}$ or $\mathbf{1}$. In these cases t is identical to the constant symbol f. If $f = -\mathbf{1}$ then $t(y) = 2^{2^y} - \mathbf{1}$. If $f = \mathbf{n}$ then $t(y) = 2^y$.

In the following definitions we will write $\mathrm{mod}(x, y)$ for the term $x - y\lfloor x/y \rfloor$

Unary function symbols. $f = \mathcal{N}$, $t(x_0, y) = \mathrm{mod}(\mathcal{N}(x_0), 2^{2^y})$. $f = \mathbf{p}$, $t(x_0, y) = \min(\mathbf{p}(x_0), 2^{2^y} - 1)$.

Binary function symbols. $f = +$, $t(x_0, x_1, y) = \mathrm{mod}(x_0 + x_1, 2^{2^y})$, $f = \times$, $t(x_0 x_1, y) = \mathrm{mod}(x_0 x_1, 2^{2^y})$, $f = \div$, $t(x_0, x_1, y) = \div(x_0, x_1)$, $f = \max$, $t(x_0, x_1, y) = \max(x_0, x_1)$, $f = \min$, $t(x_0, x_1, y) = \min(x_0, x_1)$, $f = \cap$, $t(x_0, x_1, y) = \mathrm{mod}(\cap(x_0, x_1), 2^{2^y})$. *Q.E.D.*(35).

If we consider instead of a function symbol f a term τ of $\mathcal{M}$ we may replace each function symbol in τ by the term whose existence is stated in 35. This way we get the following:

Corollary 9 *Let $\tau(x_0, \ldots, x_j)$ be a term of $\mathcal{M}$. Then there exists a term $t(x_0, \ldots, x_{j-1}, y)$ of $\mathcal{M}$ such that for all sufficiently large $d, q \in \omega$, with $d \leq q$, and for all $a, b_0, \ldots, b_{j-1} \in \mathbf{M}_q$, we have $\mathbf{M}_d \models a = \tau(b_0, \ldots, b_{j-1})$ iff $\mathbf{M}_q \models a = t(b_0, \ldots, b_{j-1}, d)$.*

Lemma 36 *For all $k \in \omega$ and for all propositional formulas $P(x_0, ..., x_{k-1})$ of $\mathcal{M}$, there exists a propositional formula $P'(x_0, ..., x_{k-1}, y)$ of $\mathcal{M}$ with the following property. Assume that $d, q \in \omega$, $d \leq q$. Then the following two conditions are satisfied:*

(46) *for all $a_0, ..., a_{k-1} \in \mathbf{M}_d$, $\mathbf{M}_d \models P(a_0, ..., a_{k-1})$ iff $\mathbf{M}_q \models P'(a_0, ..., a_{k-1}, d)$.*

(47) *for all $b_0, ..., b_{k-1} \in \mathbf{M}_q$, $\mathbf{M}_q \models P'(b_0, ..., b_{k-1}, d)$ implies $b_0, ..., b_{k-1} \in \mathbf{M}_d$.*

Proof of Lemma 36. The equality is the single relation symbol of the language $\mathcal{M}$. Consequently each atomic formula of $\mathcal{M}$ is of the form $\tau_1 = \tau_2$, where τ_1, τ_2 are terms of $\mathcal{M}$. We construct a propositional formula $P''(x_0, ..., x_{k-1})$ by substituting in P for each

atomic formula $\tau_1 = \tau_2$ the atomic formula $t_1 = t_2$, where t_i is the term whose existence is stated in Corollary 9 with $\tau := \tau_i$, for $i = 1, 2$. $P'(x_0, ..., x_{k-1}, y)$ will be the formula

$$P''(x_0, ..., x_{k-1}) \wedge \bigwedge_{i=0}^{k-1} x_i < 2^{2^y}$$

The statement of the lemma is an immediate consequence of Corollary 9 . *Q.E.D.*(Lemma 36)

As we have mentioned already in section 2 it is very important in the proof of the Collapsing statement that we are able to encode sequences formed from the elements of a structure $\mathbf{M}_d$ by a single element of a larger structure $\mathbf{M}_q$. Here we consider the implication of such an encoding for the number of existential quantifiers in an existential formula of $\mathcal{M}$. The following lemma states that if $\varphi(y_0, \ldots, y_{m-1})$ is an existential first-order formula of $\mathcal{M}$ containing k existential quantifiers, then there exists another existential formula $\psi(y_0, \ldots, y_{m-1})$ of $\mathcal{M}$ containing only a single existential quantifier such that for all $d \in \omega$, and for all $a_0, \ldots, a_{m-1} \in \mathbf{M}_d$, $\mathbf{M}_d \models \varphi(a_0, \ldots, a_{m-1})$ is equivalent to $\mathbf{M}_{d+p} \models \psi(a_0, \ldots, a_{m-1})$, where p depends only on k and the number of quantifiers in φ. Moreover the formula ψ can be given in the form of $\psi(y_0, \ldots, y_{m-1}) = \psi'(\pi(y_0, \ldots, y_{m-1}))$ where π is a term of $\mathcal{M}$ whose length is linear in m.

Lemma 37 *There exists a $c_0 \in \omega$, such that for all $m, k \in \omega$ there exist a $p \in \omega$ and a term $\pi(z_0, \ldots, z_{m-1}, w)$ of $\mathcal{M}$ of length at most $c_0 m$, such that for all propositional formulas $P(x_0 \ldots, x_{k-1}, y_0, \ldots, y_{m-1})$ of $\mathcal{M}$, there exists a propositional formula $Q(x, y)$ of $\mathcal{M}$ with the property that for all $d \in \omega$, if $q > d + p$, then the following holds:*

For all $a_0, \ldots, a_{m-1} \in \mathbf{M}_d$,

$$\mathbf{M}_d \models \exists x_0, \ldots, x_{k-1} P(x_0 \ldots, x_{k-1}, a_0, \ldots, a_{m-1}) \quad \leftrightarrow \quad \mathbf{M}_q \models \exists x, Q(x, \pi(a_0, \ldots, a_m, d))$$

Remark. In this lemma we replaced several existential quantifiers by a single one, and in the propositional part of the existential formula we replaced several parameters by a single one. These steps were needed since the indirect assumption in the proof of Theorem 3 is that a formula of the type $\exists x, F(x, y)$ is equivalent to a propositional formula. In order to apply this indirect assumption we need existential formulas with a single quantifier and a single parameter. The upper bounds on the integer q and on the size of the term π will be needed when by repeated use of the indirect assumption we will eliminate quantifiers from an arbitrary first-order formula of $\mathcal{M}$. In each step, the number of quantifiers in the formula will decrease, but the size of the structure where we interprete the formula will grow. The upper bounds are needed to keep this growth within reasonable limits. □

Proof of Lemma 37. We may assume that both k and m are powers of 2. (Otherwise we may add new variables to the formula P to make these numbers a power of 2.) Assume that $m = 2^s$, $k = 2^r$. We claim that the integer $p = r + s + 2$ meets the requirements of the lemma. The term $\pi(y_0, ..., y_{m-1}, z)$ is defined by $\pi(y_0, ..., y_{m-1}, z) = z 2^{\div(\mathbf{n},2)} + \sum_{i=0}^{m-1} y_i 2^{i 2^z}$. (Recall that $\mathbf{M}_q \models \mathbf{n} = 2^q$.)

If $a_0, ..., a_{k-1} \in \mathbf{M}_d$ then we have that $\mathbf{M}_q \models \pi(a_0, ..., a_{m-1}, d) = b = b_0 + b_1$, where $b_0 = d2^{2^{q-1}}$ and $b_1 = \sum_{i=0}^{m-1} a_i 2^{i2^d}$. Since $a_i < 2^{2^d}$ for $i \in m$ we have $b_1 < 2^{m2^d} < 2^{2^{d+s}}$. Therefore $q > d+s+2$ implies that $b_1 < 2^{2^{q-1}}$. As a consequence if $\pi_0(y) = \div(y, 2^{\div(\mathbf{n},2)})$, and $\pi_1(y) = y - \pi_0(y)2^{\div(\mathbf{n},2)}$, then, using that $\mathbf{M}_q \models 2^{\div(\mathbf{n},2)} = 2^{2^{q-1}}$, we get that

$$\mathbf{M}_q \models \pi_0(\pi(a_0, ..., a_{m-1}, d)) = d, \text{ and} \tag{48}$$
$$\mathbf{M}_q \models \pi_1(\pi(a_0, ..., a_{m-1}, d)) = \textstyle\sum_{i=0}^{m-1} a_i 2^{i2^d}$$

Motivated by these identities we define the propositional formula Q in the following way using the term $\sigma(x, y, z, w)$ that was defined in Lemma 8. Here it is used to extract a single term from the sum $\sum_{i=0}^{m-1} a_i 2^{i2^d}$ and from another sum of similar type. Our definition for $Q(x, y)$ is:

$$Q(x, y) \equiv P'(\kappa_1 \ldots, \kappa_{k-1}, \lambda_1, ..., \lambda_{k-1}, \pi_0(y))$$

where $\kappa_i = \sigma(x, i, i, \pi_0(y))$ for $i = 0, 1, ..., k-1$, $\lambda_j = \sigma(\pi_1(y), j, j, \pi_0(y))$, and where P' is the formula defined in Lemma 36 if we apply the lemma for the present formula P and $k{:=}\, k + l$. With this definition we get the truth value of $\mathbf{M}_q \models \exists x, Q(x, \pi(a_0, \ldots, a_m, d))$ in the following way. Condition (48) gives the values of $\mathbf{M}_q \models \pi_i(\pi(a_0, \ldots, a_m, d))$, for $i = 0, 1$. Putting this into the defining formula of Q and using Lemma 36, we get that $\mathbf{M}_q \models \exists x, Q(x, \pi(a_0, \ldots, a_m, d))$ is equivalent to $\mathbf{M}_q \models \exists x_0, \ldots, x_{k-1}, P'(x_0 \ldots, x_{k-1}, a_0, \ldots, a_{m-1}, d)$. Lemma 36 and the related choice of P' implies that the last expression is equivalent to $\mathbf{M}_d \models \exists x_0, \ldots, x_{k-1}, P(x_0 \ldots, x_{k-1}, a_0, \ldots, a_{m-1})$ as claimed in the present lemma. *Q.E.D.*(Lemma 37)

4 Existential definitions and turing machines

Definition. ∇ will denote the set of all pairs $\langle a_0, a_1\rangle$ with $a_0, a_1 \in \omega$ and $a_0 \geq a_1$. □

Definition. 1. Suppose that $k \in \omega$ and for all $\langle u, t\rangle \in \nabla$, $R_{u,t}$ is a k-ary relation defined on $\mathbf{M}_u$. We will say that the family of relations $R = \langle R_{u,t} \mid \langle u, t\rangle \in \nabla\rangle$ is polynomially existential in $\mathbf{M}$, if there exists an integer $c \in \omega$ and an existential first-order formula $\varphi(x_0, \ldots, x_{k-1}, y, z)$ of the language $\mathcal{M}$ such that

(49) *for all* $v, u, t \in \omega$, *if* $u \geq t$ *and* $v \geq c(u-t)+t$, *then for all* $a_0, \ldots, a_{k-1} \in \mathbf{M}_u$, $R_{u,t}(a_0, \ldots, a_{k-1})$ *holds iff* $\mathbf{M}_v \models \varphi(a_0, \ldots, a_{k-1}, u, t)$.

In this case we will say that the formula φ is a defining formula of the family of relations R. A family of k-ary functions $f_{u,t}$, $\langle u, t\rangle \in \nabla$ will be called polynomially existential if the family of relations $R_{u,t}$, $\langle u, t\rangle \in \nabla$ is polynomially existential, where for each $\langle u, t\rangle \in \nabla$, and $a, b_0, ..., b_{k-1} \in \mathbf{M}_u$, $R_{u,t}(a, b_0, ..., b_{k-1})$ iff $\mathbf{M}_u \models a = f_{u,t}(b_0, ..., b_{k-1})$.

2. Assume that $\mathbf{f}$ is a k-ary function symbol of $\mathcal{M}$. We will say that the function symbol $\mathbf{f}$ is polynomially existential if the family of relations $F_{\mathbf{f}} = \langle \mathbf{f}_{d,t} \mid \langle d, t\rangle \in \nabla\rangle$ is polynomially existential. □

Remark. The expression "polynomially existential" is motivated by the following facts. We may represent an element of $\mathbf{M}_u$ by the sequence of its 2^{2^t}-ary digits, that is, by a sequence of length 2^{u-t} whose elements are from $\mathbf{M}_t$, provided that $u \geq t$. In the existential formula defining the relation $R_{u,t}$ we can existentially quantify elements of $\mathbf{M}_v$ which also can be represented by the sequences of their 2^{2^t}-ary digits. For the smallest integer v satisfying condition (49) the length of such a sequence is $2^{c(u-t)}$. This number is a polynomial of 2^{u-t}, that is, for the definition of the relation $R_{u,t}$ it is enough to existentially quantify a sequence whose length is only a polynomial of the length of the sequences which represent the elements of $\mathbf{M}_u$. The next lemma shows that in the definition of a polynomially existential family of relations we may replace the assumption $v \geq c(u-t)+t$ by $v = c(u-t)+t$, and so considering only the smallest choice for the integer v is justified. □

Lemma 38 *The definition of a polynomially existential family of relations remains valid if we replace condition* (49) by the following condition

(50) *for all* $v, u, t \in \omega$, *if* $u \geq t$ *and* $v = c(u-t)+t$, *then for all* $a_0, \ldots, a_{k-1} \in \mathbf{M}_u$, $R_{u,t}(a_0, \ldots, a_{k-1})$ *holds iff* $\mathbf{M}_v \models \varphi(a_0, \ldots, a_{k-1}, u, t)$.

Proof of Lemma 38. The statement of the lemma is an immediate consequence of Lemma 37 *Q.E.D.*(Lemma 38)

Lemma 39 *Assume that* $k, m, l \in \omega$ *and* $f^{(j)} = \langle f^{(j)}_{d,u} \mid \langle d, u\rangle \in \nabla\rangle$ *are families of* k*-ary function on* $\mathbf{M}$, *for* $j = 0, 1, \ldots, m-1$ *and* $g = \langle g_{d,u} \mid \langle d, u\rangle \in \nabla\rangle$ *is a family of* m*-ary functions on* $\mathbf{M}$. *Let* h *be the family of* k*-ary functions* $h = \langle h_{d,u} \mid \langle d, u\rangle \in \nabla\rangle$ *on*

$\mathbf{M}$ *defined by* $h_{d,u}(a_0,\dots,a_{k-1}) = g_{d,u}(f^{(0)}_{d,u}(a_0,\dots,a_{k-1}),\dots,f^{(m-1)}_{d,u}(a_0,\dots,a_{k-1}))$ *for all* $\langle d,u\rangle \in \nabla$, $a_0,\dots,a_{k-1} \in \mathbf{M}_d$. *Suppose further that each of the families* $g, f^{(0)},\dots,f^{(m-1)}$ *are polynomially existential on* $\mathbf{M}$. *Then the family* h *is also polynomially existential on* $\mathbf{M}$.

Proof of Lemma 39. Assume that $c \in \omega$ is an integer and $\varphi_0,...,\varphi_{m-1}$, γ are existential formulas of $\mathcal{M}$ such that for all $d,u \in \omega$ and for all $a_i, a_{i,0},...,a_{i,k-1} \in \mathbf{M}_d$, $i \in m$ and $b, b_0,...,b_{m-1} \in \mathbf{M}_d$ we have that for all $i \in m$, $\mathbf{M}_{u+c(d-u)} \models \varphi_i(a_i, a_{i,0},...,a_{i,k-1},d,u)$ iff $f^{(i)}_{d,u}(a_{i,0},...,a_{i,k-1}) = a_i$ and $\mathbf{M}_{u+c(d-u)} \models \gamma(b,b_0,...,b_{m-1},d,u)$ iff $g_{d,u}(b_0,...,b_{m-1}) = b$. Then we have that for all $x_0,...,x_{k-1},y \in \mathbf{M}_d$, $h_{d,u}(x_0,...,x_{k-1}) = y$ iff

$$\mathbf{M}_{u+c(d-u)} \models \exists z_0,...,z_{m-1}, \Psi_0 \wedge \Psi_1 \wedge \Psi_2$$

where $\Psi_0 \equiv \bigwedge_{i\in m} z_i < 2^{2^d}$, $\Psi_1 \equiv \bigwedge_{i\in m} \varphi_i(z_i,x_0,...,x_{k-1},d,u))$ and $\Psi_2 \equiv \gamma(y,z_0,...,z_{m-1},d,u)$. Therefore the existential formula $\exists z_0,...,z_{m-1}, \Psi_0 \wedge \Psi_1 \wedge \Psi_2$ shows that the family of functions h is polynomially existential. *Q.E.D.*(Lemma 39)

Definition. In the following a turing machine will mean a turing machine with a single tape and a single head, whose each cell contain a natural number less than 2^q for some fixed $q \in \omega$. We may also consider the contents of the cells as $0,1$-sequences $\delta_0,...,\delta_{q-1}$ of length q. If we say that $\mathcal{T}$ is a turing machine without specifying the value of q then we assume that $q = 2$, that is each cell contains a $0,1$ bit. The machine has always a finite number of cells, but as the machine works it can always open new cells. Since we will consider only polynomial time computation on this machine the exact way as the input and output is presented is not important. E.g. if the input consists of several integers we may give their binary bits in even numbered cells, while the bits in the odd numbered cells signal the start of a new input number and the end of the input. We will call this type of turing machines also unlimited turing machines when we want to distinguish them from another class of turing machine, the restricted turing machines that we will define later. (In a restricted turing machine the number of cells is fixed when the machine starts to work, and there are restrictions on the contents of the cells too.) □

Definition. Assume that $d,u \in \omega$, $d \geq u$ and $\chi \in \mathtt{zo}(d,u)$, that is, $\chi = \sum_{i=0}^{2^{d-u}-1} \delta_i 2^{i2^u}$, where $\delta_i \in \{0,1\}$ for all $i \in 2^{d-u}$. The the integer $\sum_{i=0}^{2^d-1} \delta_i 2^i$ will be denoted by $\mathtt{bin}(\chi)$, motivated by the fact the we interprete the 2^{2^u}-ary digits of a as *bin*ary bits. □

Lemma 40 *Suppose that* $c_0 \in \omega$ *and* $\mathcal{T}$ *is a turing machine such that for all* $n,j \in \omega$ *with* $j < n$, $h < 2^n$, *the machine* $\mathcal{T}$ *at an input* $\langle n,j,h\rangle$ *and at time* n^{c_0} *provides the output* $\lambda(n,j,h) \in n+1$. *Then the family of relations* $R_{d,u}$, $\langle d,u\rangle \in \nabla$ *is polynomially existential, where for all* $\langle d,u\rangle \in \nabla$, $R_{d,u}$ *is defined in the following way. Suppose that* $a,b,\chi \in \mathbf{M}_d$. *Then* $R_{d,u}(a,b,\chi)$ *iff the following holds*

(51) $\chi \in \mathtt{zo}(d,u)$ *and for all* $i \in 2^{d-u}$

$$b[i,u] = a[\lambda(2^{d-u}, i, \mathtt{bin}(\chi)), u]$$

In Lemma 40 we are speaking about polynomial time computation on turing machines so the exact parameters of the machine the number of tapes, etc. are irrelevant. From the point of view of our proof however these parameters are important so we give a more detailed definition of a turing machine. Before we start the proof of Lemma 40 we will prove another related result Lemma 42.

In the next definition we define a class of turing machines which will be called restricted turing machines or shortly r.-turing machines which will differ at the following points from the turing machines defined earlier:

(i) the number of cells are given when the machine starts to work, new cells cannot be opened,

(ii) each cell contains a $0,1$ sequence $\langle \delta_0, ..., \delta_{\mu-1} \rangle$ of length μ, for some fixed $\mu \in \omega$,

(iii) the contents of the cells where the head is located, determine in itself that the head is there and determines also the state of the automaton,

(iv) it is possible to tell in the knowledge of the content of a cell C whether C is at one of the two ends of the tape an if the answer is yes, it is possible to tell whether it is the first or the last cell.

Definition. We define a class of turing machines which will be called restricted turing machines or shortly r.-turing machines motivated by the fact that the length of the tape and the contents of the cells cannot be arbitrary, there are some *restrictions* on them. Such a machine $\mathcal{T}$ consists of a tape of length $\ell = \mathtt{tplength}(\mathcal{T})$. The cells are denoted by $\mathtt{cell}_0, ..., \mathtt{cell}_{\ell-1}$, they are given when the machine starts to work, new cells cannot be opened. Each cell at each time contains a $0,1$-sequence of length $\mu = \mathtt{Width}(\mathcal{T})$, where $\mu \in \omega$, $\mu > 3$. $\mu = \mathtt{Width}(\mathcal{T})$ will be also called the large width of the machine. If $\delta_0, ..., \delta_{\mu-1}$ is the content of cell j at time t, for some $j \in \ell$, $t \in \omega$, then for all $i \in \mu$ we will denote δ_i by $\mathtt{cont}_{t,j,i}$. A $k \in \omega$, $k < \mu - 3$ is fixed. The first k bits that is $\mathtt{cont}_{t,j,0}, ..., \mathtt{cont}_{t,j,k-1}$ will be called the work bits of $\mathtt{cell}_j$ at time t. They will play the role of the contents of the cells of a turing machine in the traditional sense the remaining bits, that is, $\mathtt{cont}_{t,j,k}, ..., \mathtt{cont}_{t,j,\mu-1}$ will contain information related to requirements (iii) and (iv) formulated before this definition. The integer k will be called the small width of the machine and denoted by $k = \mathtt{width}(\mathcal{T})$. We assume that the movement of the head and the changes of the contents of the cells from time t to time $t+1$ is directed by the finite automaton $\mathtt{aut}(\mathcal{T})$ with 2^ν states where $\nu = \mu - k - 3$. The states are identified with the natural numbers $0, 1, ..., 2^\nu - 1$. The state of the automaton $\mathtt{aut}(\mathcal{T})$ at time t will be denoted by $\mathtt{state}_t$. At time 0 the finite automaton is always in state 0.

At each time $t \in \omega$ the head of the machine is at one of the cells. If it is at $\mathtt{cell}_j$ then we will write $\mathtt{head}_t = j$. If $\mathtt{head}_t = j$ then $\mathtt{cont}_{t,j,k+\nu} = 1$, and the sequence $\mathtt{cont}_{t,j,k}, ..., \mathtt{cont}_{t,j,k+\nu-1}$ are the binary bits of $\mathtt{state}_t(\mathtt{aut}(\mathcal{T}))$, where $\mathtt{state}_t(\mathtt{aut}(\mathcal{T}))$ is the state of the automaton $\mathtt{aut}(\mathcal{T})$ at time t.

Finally the values $\mathtt{cont}_{t,j,k+\nu+1}$ and $\mathtt{cont}_{t,j,k+\nu+2}$ indicate whether $\mathtt{cell}_j$ is at an edge of the tape and if it is which one. Namely $\mathtt{cont}_{t,j,k+\nu+1} = 1$ iff $j = 0$ and $\mathtt{cont}_{t,j,k+\nu+2} = 1$ iff $j = \ell - 1$. We will call $\mathtt{cont}_{t,j,k+\nu+1}$ and $\mathtt{cont}_{t,j,k+\nu+2}$ the edge bits.

The change of the contents of the cells from time t to time $t+1$ is done in the following way. Assume that at time t the head is at $\mathtt{cell}_j$. Then the automaton $\mathtt{aut}(\mathcal{T})$ gets the the work bits of $\mathtt{cell}_j$ at time t, that is, the sequence, $\mathtt{cont}_{t,j,0}, ..., \mathtt{cont}_{t,j,k-1}$ as input and depending on this and its state at time t it provides an output which determines the following three things: (i) the work bits of $\mathtt{cell}_j$ at time $t+1$, (the work bits of the other cells remain unchanged), (ii) the state of $\mathtt{aut}(\mathcal{T})$ at time $t+1$, (iii) the movement of the head from time t to time $t+1$, that is, whether it stays where it is, or it attempts to move to the neighboring cell on the left or right (if it is at an edge of the tape where the desired movement is not possible then it stays where it is). Therefore (ii) and (iii) together with $\mathtt{head}_t$ determine $\mathtt{head}_{t+1}$ and $\mathtt{state}_{t+1}$. which uniquely determine $\mathtt{cont}_{t+1,j,i}$ for all $j \in \ell$, $i = k, k+1, ..., \mu - 1$.

For a fixed $t \in \omega, j \in \ell$ the sequence $\mathtt{cont}_{t,j,0}, ..., \mathtt{cont}_{t,j,\mu-1}$, will be denoted by $\vec{\mathtt{cont}}_{t,j}$. This definition does not define the symbols $\vec{\mathtt{cont}}_{t,-1}$, $\vec{\mathtt{cont}}_{t,\ell}$, however we will use these symbols to denote $0,1$-sequences of lengths μ, and on each occasion we will tell what are their values.

The advantage of using restricted turing machines is their property stated in the following lemma. This lemma will make it easy to define the history of a restricted turing machine by an existential formula of $\mathcal{M}$ in a suitably chosen structure $\mathbf{M}_v$.

Lemma 41 *Suppose that $\mathcal{T}$ is a restricted turing machine with $\mathtt{tplength}(\mathcal{T}) = \ell$, $\mathtt{Width}(\mathcal{T}) = \mu$, $\mathtt{width}(\mathcal{T}) = k$. Then there exist boolean functions $\mathcal{B}_i$, for all $i \in \mu$, with 3μ variables such that for all $t \in \omega$, $j \in \ell$, $i \in \mathtt{Width}(\mathcal{T})$, and for all possible values of the vectors $\vec{\mathtt{cont}}_{t+1,-1}, \vec{\mathtt{cont}}_{t,\ell} \in \{0,1\}^\mu$, we have*

$$\mathtt{cont}_{t+1,j,i} = \mathcal{B}_i(\vec{\mathtt{cont}}_{t,j-1} \circ \vec{\mathtt{cont}}_{t,j} \circ \vec{\mathtt{cont}}_{t,j+1})$$

Proof of Lemma 41. The values $\vec{\mathtt{cont}}_{t,j-1}, \vec{\mathtt{cont}}_{t,j}, \vec{\mathtt{cont}}_{t,j+1}$ determine the answer to the following questions.

(i) Is the head located at time t at one of the cells $\mathtt{cell}_{j-1}, \mathtt{cell}_j, \mathtt{cell}_{j+1}$ and if it is which one?

(ii) If the answer to question (i) is yes then what is $\mathtt{state}_t$ and the what are the contents of the cells $\mathtt{cell}_{j-1}, \mathtt{cell}_j, \mathtt{cell}_{j+1}$?

(iii) Is $\mathtt{cell}_j$ at the edge of the tape, or more precisely, which one of the following equations hold $j = 0$ or $j = \ell - 1$?

The answers to questions (i), (ii), and (iii) uniquely determine what is $\mathtt{cont}_{t+1,i,j}$. Moreover using the answer for question (iii) we can makes sure that the values $\vec{\mathtt{cont}}_{t,-1}$ and $\vec{\mathtt{cont}}_{t,\ell}$ are not used to answer any of these question even if they are present among the three sequences $\vec{\mathtt{cont}}_{t,j-1} \circ \vec{\mathtt{cont}}_{t,j} \circ \vec{\mathtt{cont}}_{t,j+1}$. *Q.E.D.*(Lemma 41)

Definition. Assume that $\mathcal{T}$ is restricted turing machine, $\mathtt{tplength}(\mathcal{T}) = \ell$, $\mathtt{Width}(\mathcal{T}) = \mu$, $\mathtt{width}(\mathcal{T}) = k$, and an $u \in \omega$ is fixed. The sequence of integers $a_0, ..., a_{k-1}$, will be called the u-based input for the machine $\mathcal{T}$, if for each $i \in k$, $a_i = \sum_{j=0}^{\ell-1} \mathtt{cont}_{0,j,i} 2^{j2^u}$. Our definition implies that the u-based input uniquely determines the complete history of the

machine that is all of the values $\mathtt{cont}_{t,j,i}$ for $t \in \omega$, $j \in \ell$, and $i \in \mu$. For all $i \in \mu$, $T \in \omega$ we define an integer $b_{i,T}$ by

$$b_{i,T} = \sum_{t=0}^{T-1} \sum_{j=0}^{\ell-1} \mathtt{cont}_{t,j,i} 2^{(t\ell+j)2^u}$$

The sequence $b_{0,T}, ..., b_{\mu-1,T}$ will be called the u-based history of the machine $\mathcal{T}$ till time T. □

Lemma 42 *Assume that $c_0, k, \mu, \in \omega$ and $\mathcal{A}$ is a finite automaton with $|\mathcal{A}| = 2^{\mu-k-3}$. Then there exists an existential formula ψ of $\mathcal{M}$ such that for all $d, u \in \omega$, with $d \geq u$ and for all $a_0, ..., a_{k-1} \in \mathbf{M}_d$, $b_0, ..., b_{\mu-1}, \in \mathbf{M}_v$, where $v = u + (c_0 + 1)(u - d)$ the following two conditions are equivalent:*

(52) $\mathbf{M}_v \models \psi(a_0, ..., a_{k-1}, b_0, ..., b_{\mu-1}, d, u)$

(53) *For all $i \in k$, $a_i \in \mathtt{zo}(d, u)$, and if $\mathcal{T}$ is a restricted turing machine with $\mathtt{aut}(\mathcal{T}) = \mathcal{A}$, $\mathtt{width}(\mathcal{T}) = k$, $\mathtt{tplength}(\mathcal{T}) = \ell = 2^{d-u}$, $\mathtt{Width}(\mathcal{T}) = \mu$, and with the u-based input $a_0, ..., a_{k-1}$, then its u-based history till time $T = \ell^{c_0}$ is $b_0, ..., b_{\mu-1}$.*

Proof. This lemma is a consequence of Lemma 34 and Lemma 41. We apply lemma 34 with $k{:=}\ k + \mu + 1$, $l{:=}\ 4$ $d{:=}\ v$ $a_0{:=}\ a_0, ..., a_{k-1}{:=}\ a_{k-1}$, $a_k{:=}\ b_0, ..., a_{k+\mu-1}{:=}\ b_{\mu-1}$, $a_{k+\mu}{:=}\ e_{d,u}$, $\alpha_0{:=}\ 0$ $\alpha_1{:=}\ \ell - 1$, $\alpha_2{:=}\ \ell$, $\alpha_3{:=}\ \ell + 1$.

In the formulation of the propositional statement P we follow the notation of the present lemma. The propositional formula P will say the following for all $r \in 2^{v-u}$: $\Big(e_{d,u}[r, u] = 1 \to \bigwedge_{i \in k}(b_r[i, u] = a_r[i, u])\Big)$ and if $e_{d,u}[r, u] = 0$, then

$$b_i[r, u] = \mathcal{B}_i(\vec{\beta}_{r-\ell-j-1} \circ \vec{\beta}_{r-\ell-j} \circ \vec{\beta}_{r-\ell-j+1})$$

where $\mathcal{B}_i$ is the boolean expression from Lemma 41 and $\vec{\beta}_r = \langle b_0[r, u], ..., b_{\mu-1}[r, u]\rangle$. Lemma 41 implies that if the the propositional formula P holds for all $r \in 2^{v-d}$ then $b_0, ..., b_{\mu-1}$ is the u-based history of the machine $\mathcal{T}$. Therefore Lemma 34 implies the existence of the existential formula ψ. *Q.E.D.*(Lemma 42)

Proof of Lemma 40. Suppose that $a, b, \chi \in \mathbf{M}_d$ and $R_{d,u}(a, b, h)$ holds, that is, for all $i \in 2^{d-u}$

$$b[i, u] = a[\lambda(2^{d-u}, i, \mathtt{bin}(\chi)), d]$$

This means we get the 2^{2^u}-ary digits of the integer b from the digits of the integer a in the following way. To get the ith digit $b[i, u]$, we have to compute, using the turing machine $\mathcal{T}$, the value of $\lambda_i = \lambda(2^{d-u}, i, \mathtt{bin}(\chi))$. If $\lambda_i < 2^{d-u}$ then $b[i, u] = a[\lambda_i, u]$ which is an element of 2^{2^u}. This is true also for the $\lambda_i = 2^{d-u}$ but, since $a \in \mathbf{M}_d$, we have $a[2^{d-u}, u] = 0$. Therefore each the 2^{2^u}-ary digit of b is either one of the first 2^{d-u} digits of a or it is 0.

Let S be the set of sequences of length s from the elements of $\mathbf{M}_u$, where $s = 2^{d-u}$. We define maps $\eta_{j,\iota}$, $j \in s - 1$, $\iota = 0, 1, 2$, that map S into itself. Suppose that $x = \langle x_0, ..., x_{s-1}\rangle \in S$, then

$\eta_{i,0}(x) = \langle y_0, ..., y_{s-1}\rangle$, where for all $j \in \{0, 1, ..., s-2\}\backslash\{i\}$, $y_j = x_j$, and $y_i = 0$. That is, we get $\eta_{i,0}(x)$ from x by replacing x_i with 0.

$\eta_{i,1}(x) = \langle y_0, ..., y_{s-1}\rangle$, where for all $j \in \{0, 1, ..., s-2\}\backslash\{i, i+1\}$, $y_j = x_j$, and $y_i = x_{i+1}$, $y_{i+1} = x_i$. That is, we get $\eta_{i,1}(x)$ from x by swapping x_i and x_{i+1}.

$\eta_{i,2}(x) = \langle y_0, ..., y_{s-1}\rangle$, where for all $j \in \{0, 1, ..., s-2\}\backslash\{i\}$, $y_j = x_j$, and $y_i = x_{i+1}$. That is, we get $\eta_{i,0}(x)$ from x by replacing x_i with x_{i+1}.

Clearly if d, u, a, χ, b are given as above then there exists a sequence $J = \langle \eta_{i_m,\iota_m} \mid m = 0, 1, ..., \kappa - 1$, where $\kappa < s^3$ such that

(54) *if* $A = \langle a[0, u], ..., a[s-1, u]\rangle$, $B = \langle b[0, u], ..., b[s-1, u]\rangle$, *then*

$$B = \eta_{i_0,\iota_0}(\eta_{i_1,\iota_1}(...\eta_{i_\kappa,\iota_\kappa}(A)...))$$

Since the function λ was computable by an (unlimited) turing machine $\mathcal{T}$ in time polynomial in s, the sequence $J = \langle\langle i_m, \iota_m\rangle \mid m = 0, 1, ..., \kappa - 1\rangle$ is polynomial time computable as well. So far we have assumed that $\mathcal{T}$ is an unlimited turing machine whose each cell contain a single $0, 1$ bit. The same computation can be performed by an unlimited turing $\mathcal{T}_1$ machine turing whose each cell contains two bits. The advantage of using such a machine is that the encoding of the input can be done in a form which is convenient for definitions by $\mathcal{M}$ formulas in a structure $\mathbf{M}_v$.

More precisely the assumptions of the lemma imply that there exists a constant $c_1 \in \omega$ and an unlimited turing machine $\mathcal{T}_1$ such that for each $j \in \omega$, $\mathtt{cell}_j$ at time t, contains two bits $\mathtt{cont}_{t,j,0}$ and $\mathtt{cont}_{t,j,1}$ and the machine in time s^{c_1} computes a sequence $\langle i_m, \iota_m \mid m = 0, 1, ..., \kappa - 1\rangle$ which satisfies condition (54). We will denote the time by t_m when the computation of the pair $\langle i_m, \iota_m\rangle$ has been completed. Moreover we also assume that the input χ is given at time 0 in the form $\mathtt{cont}_{0,j,0} = \chi[j, 2]$, for all $j < \lceil \log_2 \chi \rceil$, and $\mathtt{cont}_{0,j,i} = 0$ for all other values of $j, i \in \omega$, where $\mathtt{cont}_{0,j,i}$ is defined. (We may assume that at time 0 the length of the tape is determined by the length of the input, and when a new cell is opened its initial content is always $\langle 0, 0\rangle$.)

We define now a restricted turing machine $\mathcal{T}_2$ with $\mathtt{Width}(\mathcal{T}_2) = c_2$, $\mathtt{width}(\mathcal{T}_2) = k_0$ where $k_0, c_2 \in \omega$, $k_0 < c_2 - 3$ are constants that we will fix later and $\mathtt{tplength}(\mathcal{T}_2) = \ell = s^{c_1}$. When the machine starts to work $\mathtt{cont}_{0,j,i}$ is the same for $\mathcal{T}_1$ and $\mathcal{T}_2$ where both values are defined. If $\mathtt{cont}^{(\mathcal{T}_1)}_{0,j,i}$ is not defined and $i < c_2 - 3$ then $\mathtt{cont}^{(\mathcal{T}_2)}_{0,j,i} = 0$. (For $i = c_2 - 3, c_2 - 2, c_2 - 1$ $\mathtt{cont}^{(\mathcal{T}_2)}_{0,j,i}$ is determined by the definition of a restricted turing machine.)

We partition the first k_0 bits of each cell j at time t into subsets $X_{t,j}, Y_{t,j}, Z_{t,j}$. We will call the the X-bit, Y-bit and Z-bits. $X_{t,j}$ contain the first two bits (corresponding to the bits used by $\mathcal{T}_1$), $Y_{t,j}$ contains the next two bits and $Z_{t,j}$ contains the remaining work bits. The computation done by $\mathcal{T}_2$ will consist of κ consecutive time intervals $I_0, ..., I_{\kappa-1}$. Each interval I_m is further divided into four consecutive intervals J_m, K_m, L_m, M_m.

In the interval J_m, $m \in \kappa$, using only the X bits of its cells $\mathcal{T}_2$ simulates the computation done by $\mathcal{T}_1$ in the time interval $(t_{m-1}, t_m]$, (where $t_{-1} = -1$).

After that this simulation is suspended, and during the intervals K_m, L_m, M_m the X bits of the cells do not change, and consequently $\mathcal{T}_2$ will be able to continue the simulation of $\mathcal{T}_1$ in the time interval J_{m+1}.

In the interval K_m, $\mathcal{T}_2$ does the following, while it leaves the X bits and Y bits unchanged in each cell. $\mathcal{T}_2$ takes the head to $\mathtt{cell}_{i_m}$, where $\langle i_m, \iota_m \rangle$ is the pair computed by $\mathcal{T}_1$ by time t_m. For this no other work bits are used than the Z bits. Meanwhile $\mathtt{aut}(\mathcal{T}_2)$ "remembers" the value of ι_m, that is, it has enough states to use different ones depending on the value of ι_m.

During the whole interval L_m the head remains at $\mathtt{cell}_{i_m}$. When interval L_m starts say at $\mathcal{T}_2$-time t'_m, $\mathcal{T}_2$ writes the binary form of $\iota_m + 1$ into the two bits of the set Y_{t_m,i_m}. That is, $\mathtt{cont}_{t'_m,i_m,2} = (\iota_m + 1)[0,0]$ and $\mathtt{cont}_{t'_m,i_m,3} = (\iota_m + 1)[1,0]$. All of the other work bits remain unchanged

At time $t'_m + 1$ still in interval L_m, the head remains at $\mathtt{cell}_{i_m}$ and the bits in $Y_{t'_m+1,i_m}$ are changed into 0, that is, the $\mathtt{cont}_{t'_m+1,i_m,2} = 0$ and $\mathtt{cont}_{t'_m+1,i_m,3} = 0$. All of the other work bits remain unchanged.

In the interval M_m the head goes back to the position where it was at the end of interval K_m. During this the X and Y bits do not change. (The very last interval of the form M_m is exceptional in the sense that is has no end since according to our definition the machine cannot stop, so the head remains at the same place and the content of all of the cells remain unchanged.)

This completes the description of the computation done by $\mathcal{T}_2$. It is easy to see that there exists a finite automaton $\mathcal{A}$, such that if $\mathcal{A} = \mathtt{aut}(\mathcal{T}_2)$ then $\mathcal{T}_2$ will perform the described computation. $\mathtt{Width}(\mathcal{T}_2) = c_2$ and $\mathtt{width}(\mathcal{T}_2) = k_0$ are chosen in a way that is compatible with the described computation and the choice of $\mathcal{A}$.

Let t be a time according to $\mathcal{T}_2$ and let $j \in \ell$ such that at least on of the bits in $Y_{t,j}$ is not 0, equivalently $\mathtt{cont}_{t,j,2} \neq 0$ or $\mathtt{cont}_{t,j,3} \neq 0$. Then we will say that the integer j is a critical cell number at time t. We will need later the following immediate consequence of the definition of $\mathcal{T}_2$:

(55) *the machine $\mathcal{T}_2$ has the property that for each $t \in \omega$ there exists at most one integer $j \in \ell$ such that j is a critical cell number at time t. If j is a critical cell number at time t then then there exists a unique $m \in \kappa$ such that the machine $\mathcal{T}_2$ at time t, wrote the binary bits of $\iota_m + 1$ into the $Y_{t,j}$ bits. (In this case ι_m will be called the critical map-number at time t.)*

The total time needed for $\mathcal{T}_2$ to complete the described steps is at most $T = s^{c_3}$, where $c_3 \in \omega$ is sufficiently large with respect to c_1. We will write $\mathcal{T}_2^{(d,u)}$ instead of $\mathcal{T}_2$ if we want to emphasize its dependence on d and u. Applying Lemma 42 we get the following.

There exists an existential formula ψ of $\mathcal{M}$ such that for all $d, u \in \omega$ with $d \geq u$ for all $\chi \in \mathtt{zo}_{d,u}$ and for all $b_0, ..., b_{c_2-1} \in \mathbf{M}_v$, here $v = u + (c_3 + c_1)(d - u)$ the following two conditions are equivalent

(56) $\chi \in \mathtt{zo}_{d,u}$, *and the u-based history of the machine $\mathcal{T}_2^{(d,u)}$ with u-based input $\langle \chi, 0, ..., 0 \rangle$ is $b_0, ..., b_{c_2-1}$.*

(57) $\mathbf{M}_v \models \psi(b_0, ..., b_{c_2-1}, \chi, d, u)$

The next step is to give an existential formula φ of $\mathcal{M}$ such that for all $b_0, ..., b_{c_2-1} \in \mathtt{zo}(v, u)$ and for all $a, b, \chi \in \mathbf{M}_d$, $\mathbf{M}_v \models \varphi(b_0, ..., b_{c_2-1}, a, b, \chi, d, u)$ iff condition (51) of the lemma is satisfied. This together with the equivalence of conditions (56) and (57) clearly implies the conclusion of the Lemma 40, (we also need that according to Lemma 22 the conditions $b_0, ..., b_{c_2-1} \in \mathtt{zo}(v, u)$, $\chi \in \mathtt{zo}_{d,u}$ can be described by an existential formula in $\mathbf{M}_v$.)

We define an integer $\alpha \in \mathbf{M}_v$. We for each $j \in \ell, t \in T$, where $s = 2^{d-u}$, $\ell = s^{c_1}$, $T = s^{c_3}$, $\alpha_{t,j}$ will denote the integer $\alpha[t\ell + j, u]$. We define $\alpha_{t,j}$ by induction on t.

For $t = 0$, $\alpha_{0,j} = a[j, u]$. Assume that $\alpha_{t-1,j}$ has been defined for some $t \in \omega \backslash \{0\}$ and for all $j \in \ell$. If $j \geq s$ or there is no critical cell number at time t, then $\alpha_{t,j} = \alpha_{t-1,j}$. If there exists a critical cell number j_0 at time t and ι_m is the critical map-number at time t. Then we define $\alpha_{t,j}$ for all $j < s$, by

$$\langle \alpha_{t,0}, ..., \alpha_{t,s-1} \rangle = \eta_{j_0,\iota_m}\Big(\langle \alpha_{t-1,0}, ..., \alpha_{t-1,s-1} \rangle\Big)$$

and by $\alpha_{t,j} = 0$ for all $j \geq s$. This completes the definition of the integer α. The definition implies that we have $\alpha_{T,j} = b[j, u]$ for all $j \in s$. In the definition we treated separately the cases $j < s$ and $j \geq 0$. Later we will use the fact that the integer $w_{v,d,u} = e_{d,u} \sum_{i=0}^{T-1} 2^{i\ell 2^u}$, has the property that for all $j \in \ell$, $t \in T$, $w[t\ell + j, u] = 1$ if $j < s$ and and $w_{v,d,u}[t\ell + j, u] = 0$ otherwise. Moreover by Lemma 11 there exists a term σ of $\mathcal{M}$ whose choice does not depend on anything, such that $\mathbf{M}_v \models w_{v,d,u} = \sigma(v, u, d)$ and as a consequence w is definable by an existential formula in $\mathcal{M}$.

We show now that the integer α can be defined by an existential formula in $\mathbf{M}_v$ (using $b_0, ..., b_{c_2-1}, a, d, u$ as a parameters). We will denote by $\vec{\mathtt{cont}}_{t,j}$ the sequence $\mathtt{cont}_{t,j,0}, ..., \mathtt{cont}_{t,j,c_2-1}$ with respect to the machine $\mathcal{T}_2$. As earlier we use the symbols $\vec{\mathtt{cont}}_{t,-1}$ $\vec{\mathtt{cont}}_{t,\ell}$ to denote $0, 1$ sequences of length c_2, whose values will be decided later. In a similar way $\alpha_{t,-1}$, $\alpha_{t,\ell}$ will denote integers in $\mathbf{M}_u$ whose values will be decided later. The definition of the integers $\alpha_{t,j}$ implies the following:

(58) *There exists a propositional formula P of the language $\mathcal{L}^{(=)}$ such that for all $t \in s^{c_3}$, $j \in \ell$, $i \in c_2 = \mathtt{Width}(\mathcal{T}_2)$, and for all possible definitions of the vectors $\vec{\mathtt{cont}}_{t,-1}, \vec{\mathtt{cont}}_{t,\ell} \in \{0, 1\}^{c_2}$ and the integers $\alpha_{t,-1}, \alpha_{t,\ell} \in \mathbf{M}_u$, we have that $\alpha_{t+1,j}$ is the unique integer $A \in \mathbf{N}_{\bar{u}}$ such that*

$$\mathbf{N}_{\bar{u}} \models P(A, \alpha_{t-1,j}, \alpha_{t,j}, \alpha_{t+1,j}, \vec{\mathtt{cont}}_{t,j-1} \circ \vec{\mathtt{cont}}_{t,j} \circ \vec{\mathtt{cont}}_{t,j+1}, w_{v,d,u}[ts^{c_3} + j])$$

Now we use Lemma 34 and get that the α is definable by an existential formula in $\mathbf{M}_v$.

The definition of α implies that $\mathbf{M}_v \models b = \div(\alpha, 2^{\ell(T-1)2^u})$ and $a = \mathrm{mod}(\alpha, 2^{s2^u})$, that is, $\mathbf{M}_v \models a = \alpha - 2^{s2^u} \div (\alpha, 2^{s2^u})$, where $\mathrm{mod}(x, y)$ is the least nonnegative residue of x modulo y. *Q.E.D.*(Lemma 40)

Lemma 42 that we have formulated and proved earlier states that if $\mathcal{T}$ is a restricted turing machine $\mathcal{T}$ such that $\mathtt{width}(\mathcal{T})$ and $\mathtt{aut}(\mathcal{T})$ are constants, then its history can

be defined by an existential formula in $\mathbf{M}_v$, where v is large enough so that the u-based history can be presented as a sequence in $\mathcal{M}_v$. Now we formulate a consequence of the lemma which is dealing with not the whole history of $\mathcal{T}$ but only its input-output relation.

Lemma 43 *Assume that $c_0, c_1, k \in \omega$ and $\mathcal{A}$ is a finite automaton. Then the family of relations $\langle R_{d,u} \mid \langle d, u\rangle \in \nabla\rangle$ is polynomially existential, where for all $d, u \in \omega$, $d \geq u$, and for all $a_0, ..., a_{k-1}, b_0, ..., b_{k-1} \in \mathbf{M}_d$, $R_{d,u}(a_0, ..., a_{k-1}, b_0, ..., b_{k-1})$ holds iff there exists a restricted turing machine $\mathcal{T}$ with $\mathtt{width}(\mathcal{T}) = k$, $\mathtt{aut}(\mathcal{T}) = \mathcal{A}$, $\mathtt{tplength}(\mathcal{T}) = 2^{c_0(d-u)}$ such the the following holds:*

(59) *If the u-based input of the machine $\mathcal{T}$ is the sequence $a_0, ..., a_{k-1}$, and $T = 2^{c_1(d-u)} - 1$, then for all $i \in k$, $b_i = \sum_{j=0}^{2^{d-u}-1} \mathtt{cont}_{T,j,i} 2^{j2^u}$.*

Proof of Lemma 43. The statement of the lemma is an immediate consequence of Lemma 42, since we have to say only by an existential formula that there exists a history of $\mathcal{T}$ which is compatible with the given u-based input and the given contents of the cells at time T. *Q.E.D.*(Lemma 43)

5 Polynomially existential definition for parallel multiplication

In this section we prove the following

Lemma 44 *The function symbol $\times$ of $\mathcal{M}$ is polynomially existential in $\mathbf{M}$. Equivalently, the family of functions $\langle \otimes_{q,u} \mid \langle q,u\rangle \in \nabla\rangle$ is polynomially existential.*

As a first step of the proof we reformulate the statement of Lemma 44.

Lemma 45 *The following statement implies Lemma 44. Let $F = \langle F_{d,u} \mid \langle d,u\rangle \in \nabla\rangle$ be the the family of ternary functions defined in the following way. For all $d,u \in \omega$ with $d \geq u$, and for all $a,b,q \in \mathbf{M}_d$, $\mathbf{M}_d \models F_{d,u}(a,b,q) = a \otimes_{q,u} b$ if $a,b \in \mathbf{M}_u$, $q \geq u$ and $d \geq u + 2(q-u) + 2$, otherwise $F_{d,u}(a,b,q) = 0$. Then the family of function $F_{d,u}$ is polynomially existential.*

Proof of Lemma 45. Let Γ be the set of all triplets $\langle d,q,u\rangle \in \omega^3$, such that $d \geq q \geq u$ and $d \geq u+2(q-u)+2$. Suppose that the family functions F is polynomially existential. This implies that there exists an existential formula ψ of $\mathcal{M}$ and a $c_0 \in \omega$, such that for all $\langle d,q,u\rangle \in \Gamma$, and for all $a,b,c \in \mathbf{M}_q$, and for all $w \geq u + c_0(d-u)$ we have

(60) $\mathbf{M}_w \models \psi(a,b,c,q,d,u)$ *iff* $\mathbf{M}_q \models a \otimes_{q,u} b = c$.

Assume now that we choose $\langle q,u\rangle \in \nabla$ arbitrarily with the only restriction $q > u$, $a,b,c \in \mathbf{M}_u$, and we define d by $d = q + 2(q-u) + 2$, and so we have $\langle d,u,q\rangle \in \Gamma$. Let $c_1 \in \omega$ be a constant with $c_1 > c_0 + 6$. Then $u + c_1(q-u) \geq u + c_0(d-u)$ and therefore condition (60) implies that

(61) $\mathbf{M}_{u+c_1(q-u)} \models \psi(a,b,c,q,d,u)$ *iff* $\mathbf{M}_q \models a \otimes_{q,u} b = c$.

This holds for all $\langle q,u\rangle \in \nabla$, with $q > u$ and for all $a,b,c \in \mathbf{M}_q$. The $q = u$ case however is trivial since $\mathbf{M}_q \models a \otimes_{q,q} b = ab$. Therefore if we define another existential formula ψ' of $\mathcal{M}$ with $\psi'(a,b,c,q,u) \equiv (q = u \wedge ab = c) \vee \psi(a,b,c,q,q+2(q-u)+2,u)$, then we have that for all $\langle q,u\rangle \in \nabla$ and for all $a,b,c \in \mathbf{M}_q$

(62) $\mathbf{M}_{q+c_1(q-u)} \models \psi'(a,b,c,q,u)$ *iff* $\mathbf{M}_q \models a \otimes_{q,u} b = c$.

as required in the definition of a polynomially existential family of functions. *Q.E.D.*(Lemma 45)

Proof of Lemma 44. Let $F = \langle F_{d,u} \mid \langle d,u\rangle \in \nabla\rangle$ be the family of functions defined in Lemma 45. We will show that F is polynomially existential. We define four families of functions $F_i = \langle F_{d,u,i} \mid \langle d,u\rangle \in \nabla\rangle$ for $i = 0,1,2$ and $G = \langle F_{d,u,i} \mid \langle d,u\rangle \in \nabla\rangle$. The functions $F_{d,u,i}$, $i = 0,1,2$ will be binary functions and the functions $G_{d,u}$ will be ternary functions. For each fixed $\langle d,u\rangle \in \nabla$ we define a ternary function $F' = \langle F'_{d,u} \mid \langle d,u\rangle \in \nabla\rangle$. For all $a,b,q \in \mathbf{M}_{d,u}$,

$$F'_{d,u}(a,b,q) = F_{d,u,2}\Big(G_{d,u}\Big(F_{d,u,1}(a,q), F_{d,u,1}(a,q), q\Big), q\Big)$$

We will prove the following two statements.

(63) *The families of functions F_0, F_1, F_2, G, are all polynomially existential.*

(64) *For all $\langle d, u\rangle \in \nabla$ and for all $q \in \mathbf{M}_d$ and $a, b \in \mathbf{M}_q$, we have*

$$F'_{d,u}(a, b, q) = F_{d,u}(a, b, q)$$

According to Lemma 39 the composition of polynomially existential families is polynomially existential. The family F' was defined as a composition, therefore condition (63) implies that the family F' is polynomially existential. The fact that the family F' is polynomially existential and condition (64) together imply that the family F is also polynomially existential. (The functions $F'_{d,u}$ and $F_{d,u}$ are not necessarily identical on $\mathbf{M}_d$ since the equality in condition (64) is guaranteed only for $a, b \in \mathbf{M}_q$.) Indeed assume that ψ is an existential formula of $\mathcal{M}$ and $\mathbf{M}_{u+c_0(u-d)} \models \psi'(a, b, c, q, d, u)$ is equivalent to $F'_{d,u}(a, b, q) = c$, for all $a, b, c, q \in \mathbf{M}_d$. Let $\psi(a, b, c, q, d, u) \equiv ((a \geq 2^{2^q} \vee b \geq 2^{2^q}) \wedge c = 0) \vee \psi'(a, b, c, q, d, u)$. Then ψ' is an existential formula of $\mathcal{M}$, and $\mathbf{M}_{u+c_0(u-d)} \models \psi'(a, b, c, q, d, u)$ is equivalent to $F_{d,u}(a, b, q) = c$.

Therefore to complete the proof of Lemma 44 it is sufficient to show that there exists families of functions F_0, F_1, F_2, G, such that conditions (63) and (64) are satisfied. (In the latter one F' is defined as a composition F_0, F_1, F_2, G, as indicated earlier.)

Let Γ be the set of all triplets $\langle d, q, u\rangle \in \omega^3$, such that $d \geq q \geq u$ and $d \geq u+2(q-u)+2$.

We start the definition on the functions $F_{d,u,i}$, and G by defining their values in places that are not interesting for us. Suppose that $d, u, q \in \omega$, $d \geq u$, $q \in \mathbf{M}_d$ and $\langle d, q, u\rangle \notin \Gamma$. Then for all $x, y \in \mathbf{M}_u$, $F_{d,u,0}(x, q) = F_{d,u,0}(x, q) = F_{d,u,0}(x, q) = G(x, y, q) = 0$. Since $\langle d, q, u\rangle \notin \Gamma$ implies $F_{d,u}(x, y, q) = 0$ for all $x, y \in \mathbf{M}_u$ as well condition (64) is satisfied if $\langle d, q, u\rangle \notin \Gamma$. Therefore, starting from from this, point we consider only the $\langle d, q, u\rangle \in \Gamma$ case. Since $\langle d, q, u\rangle \in \Gamma$ is a propositional statement in $\mathbf{M}_d$, this is sufficient for our purposes.

The family of functions F_0 and F_1. Assume that a $\langle d, q, u\rangle \in \Gamma$ is fixed, $s = 2^{q-u}$ and $p \in 2^{s2^u} = \mathbf{M}_d$. If $p \notin \mathbf{M}_q$ then $F_{d,u,0}(p, q) = F_{d,u,1}(p, q) = 0$. Assume now that $p \in \mathbf{M}_q$. We define $F_{d,u,i}(p, q)$ for $i = 0, 1$. The integer p can be written in the form of

$$p = \sum_{i=0}^{s-1} \pi(i) 2^{i2^u}$$

where $\pi(i) \in 2^{2^u}$ for all $i \in s$. Our definitions are

$$F_{d,u,0}(p, q) = \sum_{i=0}^{s-1} \pi(i) 2^{2is2^u}, F_{d,u,1}(p, q) = \sum_{i=0}^{s-1} \pi(i) 2^{2i2^u},$$

that is, in both cases we got the 2^{2^d}-ary digits of $F_{d,u,i}(p, q)$ from the digits of p by moving the digits of p to different places and putting 0s in the remaining places. We have that $F_{d,u,0}(p, q)[j, u] = \pi(\frac{j}{2s})$ if $2s|j$ and $F_{d,u,0}(p, q)[j, u] = 0$ otherwise. We apply Lemma 40 with $n{:=}\ 2^{d-u}$, $\chi{:=}\ 2^{(q-u)2^u}$, $h = \mathtt{bin}(\chi) = 2^{q-u}$, and the function $\lambda(n, j, h)$ is defined in the following way: if $j = 2hi$ for some $i \in h$ then $\lambda(n, j, h) = i$ otherwise $\lambda(n, j, h) = n$.

Lemma 40 implies that the family F_0 is polynomially existential. We can show in a similar way that the family F_1 is also polynomially existential.

The family of functions G. Assume that $\langle d, q, u\rangle \in \nabla$ and $x, y \in \mathbf{M}_d$. Then $G_d(x, y) = xy$. Clearly the family of functions G is polynomially existential.

The definition of the function $F_{d,u,2}$. Assume that a $\gamma \in \langle d, q, u\rangle \in \Gamma$ is fixed and $p \in \mathbf{M}_d$ and $p[i, d] = \pi(i)$. Then $F_{d,u,2}(p) = \sum_{i=0}^{s-1} \pi(2si + 2i)2^{i2^u}$. In the same way as in the case of the family F_0 we can show using Lemma 40 that the family F_2 is polynomially existential.

This completes the definition of the families F_i and G and the proof of statement (63). Now we prove statement (64).

It is sufficient to show that for all $a, b \in \mathbf{M}_q$, and for all $i \in 2^{d-u}$,

$$F'_{d,u}(a, b, q)[i, u] = F_{d,u}(a, b, q)[i, u]$$

Since the values of d, u and q are fixed now, we will write $F_0(x)$ instead of $F_{d,u,0}(x, q)$, $F_2(x, y)$ instead of $F_{d,u,2}(x, y, q)$, etc.

Let $a = \sum_{j=0}^{s-1} a_j 2^{j2^u}$ and $b = \sum_{j=0}^{s-1} b_j 2^{j2^u}$, where $s = 2^{u-q}$. Then, by the definition of F and the definition of the operation $\otimes_{q,u}$ we have $F(a, b)[i, u] = (a_i b_i)_{\mathbf{M}_u}$, that is, $a_i b_i$ must be computed in $\mathbf{M}_u$.

If we compute F', according to its definition as a composition, we get the following. $F_0(a) = \sum_{j=0}^{s-1} a_j 4^{sj2^u}$ and $F_1(b) = \sum_{k=0}^{s-1} b_k 4^{k2^u}$. Therefore if we compute ab in the 4^{2^u}-ary numeral system then all of the products $a_j b_k$ will contribute to to a different digits of the product ab, since the sums $sj + k$, $j, k \in s$ are all different. Moreover $a_j, b_k \in \mathbf{M}_u$ imply that the product $a_j b_k$ as the product of integers is less than 4^{2^u}, therefore there is no carryover, and we have that

(65) $F_0(a)F_0(b) = \sum_{r=0}^{s^2-1} \alpha_r 4^{r2^r}$, *where* $\alpha_r = a_j b_k < 4^{2^u}$, *if* $r = sj + k$, *and* $j, k \in s$, *where every operation is performed as among integers.*

Moreover the assumptions $a, b \in \mathbf{M}_q$ and $d \geq u + 2(u - q) + 2$ imply that the product $F_0(a)F_0(b)$ among the integers is the same that in $\mathbf{M}_d$. Since $F_0(a)F_0(b) = G(F_0(a), F_0(b))$ we have that $F_2(F_0(a)F_0(b)) = F'(a, b)$. Let $h = F_0(a)F_1(b)$. Statement (65) imply that $h[2si + 2i, u] = (a_i b_i)_{\mathbf{M}_u}$, therefore, according to the definition of F_2, we get that $F'(a, b)[i, u] = (a_i b_i)_{\mathbf{M}_u}$, where $(a_i b_i)_{\mathbf{M}_u}$. This completes the proof of statement (64). *Q.E.D.*(Lemma 44)

6 The $\mathcal{M}$ operations are polynomially existential.

In this section we prove Theorem 7 which is equivalent to the following lemma.

Lemma 46 *For each function symbol* $\mathbf{f}$ *of* $\mathcal{M}$*, the parallel* $\mathbf{f}$ *operation is polynomially existential in* $\mathbf{M}$*. Equivalently, for each function symbol* $\mathbf{f}$ *the family of functions* $\langle \mathbf{f}_{d,t} \mid \langle d,t\rangle \in \nabla\rangle$ *is polynomially existential in* $\mathbf{M}$*.*

We will use the following three lemmas in the proof of Lemma 46.

Lemma 47 *Suppose that* $\tau(x_0,...,x_{k-1})$ *is a term of* $\mathcal{M}$*, such that for each function symbol* $\mathbf{f}$ *of* $\mathcal{M}$*, if* $\mathbf{f}$ *occurs in* τ *then* $\mathbf{f}$ *is polynomially existential. Then the family of* k*-ary relations* $R = \langle R_{d,t} \mid \langle d,t\rangle \in \nabla\rangle$ *is polynomially existential, where for all* $d,t \in \omega$ *with* $d \geq t$ *and for all* $a_0,...,a_{k-1} \in \mathbf{M}_d$*, we have* $R_{d,t}(a_0,...,a_{k-1})$ *iff for all* $i \in 2^{d-t}$*,* $\mathbf{M}_t \models \tau(a_0[i,t],...,a_{k-1}[i,t]) = \mathbf{0}$*.*

Assume now that for all of the function symbols $\mathbf{f}$ *in* τ*,* $\mathbf{f} \notin \{\times, \div, \mathbf{p}\}$*. Then the family of* $k+1$*-ary relations* $Q = \langle Q_d \mid d \in \omega\rangle$ *is uniformly existential, where for all* $d \in \omega$ *and for all* $a_0,...,a_{k-1},t \in \mathbf{M}_d$*,* $Q_d(a_0,...,a_{k-1},t)$ *iff* $t \leq d$ *and* $R_{d,t}(a_0,...,a_{k-1})$*.*

Proof of Lemma 47. To prove the first statement of the lemma we construct an existential formula ψ of $\mathcal{M}$ such that for all sufficiently large $c > 0$, for all $d,t \in \omega$ with $d \geq t$ and for all $a_0,...,a_{k-1} \in \mathbf{M}_d$, we have $R_{d,t}(a_0,...,a_{k-1})$ iff $\mathbf{M}_v \models \psi(a_0,...,a_{k-1},d,t)$, where $v = t + c(d-t)$.

Let $\mathbf{f}^{(0)},...,\mathbf{f}^{(l-1)}$ be the function symbols of $\mathcal{M}$ occurring in τ, and let $\tau_0,...,\tau_{r-1}$ be the sequence of all subterms of τ where $\tau_i = x_i$ for $i \in k$ and $\tau_{r-1} = \tau$. Assume that $\tau_i = \mathbf{f}^{(g_{i,0})}(\tau_{g_{i,1}}, \tau_{g_{i,2}})$, where $g_{i,0} \in l$ and $g_{i,1}, g_{i,2} \in r$. (If $\mathbf{f}^{(g_{i,0})}$ is not binary then one or both arguments of it may be missing). The formula ψ will say the following: there exists $b_0,...,b_{r-1} \in \mathbf{M}_d$, such that

$$\mathbf{M}_d \models b_{r-1} = \mathbf{0} \wedge \left(\bigwedge_{j\in k} b_j = a_j\right) \wedge \bigwedge_{i\in r} b_i = \mathbf{f}_{d,t}^{(g_{i,0})}(b_{g_{i,1}}, b_{g_{i,2}})$$

Our assumption that all of the function symbols $\mathbf{f}^{(i)}$, $i \in l$ are polynomially existential implies that this condition can be expressed by an existential formula in $\mathbf{M}_v$.

For the proof of the second statement of the lemma we note that by Lemma 28, $\mathbf{f} \notin \{\times, \div, \mathbf{p}\}$ implies that the parallel operation $\mathbf{f}$ is uniformly existential. Using this the the fact that family Q is uniformly existential can be proved in the same way as the first part of the lemma. *Q.E.D.*(Lemma 47)

Definition. Assume that $P(x_0,...,x_{k-1},y_0,...,y_{l-1})$ is a propositional formula of $\mathcal{M}$. We will say that P is k-sensitive, if the following three conditions are satisfied:

(i) for each occurrence $\times(\tau,\sigma)$ of the function symbol $\times$ of $\mathcal{M}$ in P, where τ,σ are terms of $\mathcal{M}$, there exists a $j \in l$ such that $\tau = y_j$,

(ii) for each occurrence $\div(\tau,\sigma)$ of the function symbol $\div$ of $\mathcal{M}$ in P, where τ,σ are terms of $\mathcal{M}$, there exists a $j \in l$ such that $\sigma = y_j$,

(iii) the formula P does not contain the function symbol $\mathbf{p}$ of $\mathcal{M}$. $\square$

Lemma 48 *Suppose that $P(x_0, ..., x_{k-1}, y_0, ..., y_{l-1})$ is a k-sensitive propositional formula of $\mathcal{M}$. Then the family of $k+l+1$-ary relations $R = \langle R_d \mid d \in \omega \rangle$ is uniformly existential, where for all $d \in \omega$, $a_0, ..., a_{k-1}, b_0, ..., b_{l-1}, t \in \mathbf{M}_d$, we have $R_d(a_0, ..., a_{k-1}, b_0, ..., b_{l-1}, t)$ iff $d \geq t$, $b_0, ..., b_{l-1} \in \mathbf{M}_t$ and for all $i \in 2^{d-t}$, $\mathbf{M}_t \models P(a_0[i,t], ..., a_{k-1}[i,t], b_0, ..., b_{l-1})$.*

Proof of Lemma 48. The proof of the lemma is the essentially the same as the proof of Lemma 47. (We have to use now, that according to Lemma 14, the family of relations $Q_d(a,b,c,t)$ is uniformly propositional, where for all $a, b, c, \in \mathbf{M}_d$, $Q_d(a,b,c,t)$ holds iff $d \leq t$ and $\odot_{d,t}(a,b) = c$.) *Q.E.D.*(Lemma 48)

Lemma 49 *Suppose that $P(x_0, ..., x_{3k-1}, y_0, ..., y_{l-1})$ is a $3k$-sensitive propositional formula of $\mathcal{M}$. Then the family of $k+l+1$-ary relations $R = \langle R_d \mid d \in \omega \rangle$ is uniformly existential, where for all $d \in \omega$, $a_0, ..., a_{k-1}, b_0, ..., b_{l-1}, t \in \mathbf{M}_d$, we have $R_d(a_0, ..., a_{k-1}, b_0, ..., b_{l-1}, t)$ iff $d \geq t$, $b_0, ..., b_{l-1} \in \mathbf{M}_t$ and for all $i \in 2^{d-t}$,*

$$\mathbf{M}_t \models P(\vec{A}_0, ..., \vec{A}_{k-1}, b_0, ..., b_{l-1})$$

where $\vec{A}_j$ stands for the sequence $a_j[i-1,t], a_j[i,t], a_j[i+1,t]$ for $j = 0, 1, ..., k-1$.

Proof of Lemma 49. We use Lemma 48 with $k{:=}\, 3k$. The statement $\mathbf{M}_t \models P(\vec{A}_0, ..., \vec{A}_{k-1}, b_0, ..., b_{l-1})$ is equivalent to

$$\mathbf{M}_t \models \exists g_0, ..., g_{k-1}, h_0, ..., h_{k-1}, \Phi \wedge \bigwedge_{i \in k} h_i = 2^{2^q} a_i \wedge g_i = \div(a_i, 2^{2^q})$$

where

$$\Phi \equiv P(\vec{B}_0, ..., \vec{B}_{k-1}, b_0, ..., b_{l-1})$$

and B_j stands for the sequence $g_j[i,q], a_j[i,q], h_j[i,q]$ for $j = 0, 1, ..., k-1$. Therefore applying Lemma 48 for the given propositional formula P we get the required existential formula. *Q.E.D.*(Lemma 49)

Lemma 50 *Assume that, $k, m \in \omega$ and P is a propositional formula of $\mathcal{M}$ with $3k+m+1$ free variables and σ does not contain any of the function symbols $\times, \div$ or $\mathbf{p}$. Then $R = \langle R_d \mid d \in \omega \rangle$ is a uniformly existential family of $k+m+1$-ary relations in $\mathbf{M}$, where for each $d \in \omega$, and for each $a_0, ..., a_{k-1}, w_0, ..., w_{m-1}, q \in \mathbf{M}_d$, $R_d(a_0, ...a_{k-1}, w_0, ..., w_{m-1}, q)$ holds iff $q \leq d$, $w_0, ..., w_{m-1} \in \mathbf{M}_q$ and for all $i \in 2^{d-q}$, $\mathbf{M}_q \models P(\vec{A}_0, ..., \vec{A}_{k-1}, w_0, ..., w_{m-1}, q)$, where $\vec{A}_j$ is the sequence $a_j[i-1,q], a_j[i,q], a_j[i+1,q]$, for all $j \in k$.*

Proof of Lemma 50. We may assume that P is of the form $\sigma(x_0, ..., x_{3k+m}) = \mathbf{0}$. We have

$$a_j[i-1,q] = (qa_j)[i,q] \wedge a_j[i+1,q] = (\lfloor a_j/q \rfloor)[i,q]$$

Therefore $R_d(a_0, ...a_{k-1}, w_0, ..., w_{m-1}, q)$ holds iff for all $i \in 2^{d-q}$,

$$\mathbf{M}_q \models \sigma(\vec{B}_0, ..., \vec{B}_{k-1}, w_0, ..., w_{m-1}, q) = \mathbf{0}$$

where $\vec{B}_j$ is the sequence $(qa_j)[i,q], a_j[i,q], (\lfloor a_j/q \rfloor)[i,q]$

Since the term σ does not contain the function symbols the second part of Lemma 47 implies the conclusion of lemma. *Q.E.D.*(Lemma 50)

Proof of Lemma 46. We know from Lemma 28 that the statement of the lemma holds if $\mathbf{f} \notin \{\times, \div, \mathbf{p}\}$. Lemma 44 implies the statement of the present lemma for $\mathbf{f} = \times$. Our next goal is to show that the function symbol $\div$ is existentially parallel. The operation $\div(a,b)$ has an existential definition among integers. Namely for all $a, b, c \in \omega$, $\div(a,b) = c$ iff "$(b = 0 \wedge c = 0)$ or ($b \neq 0$ and there exists an $r \in \omega$, with $a = cb + r$ and $r < b$)". This definition is not good if $a, b, c \in \mathbf{M}_d$ and we perform the arithmetic operations in $\mathbf{M}_d$, since there can be many different $c \in \mathbf{M}_d$ with $\mathbf{M}_d \models a - b < cb \leq a$ and for all of them $r := a - cb$ meets the requirement of the definition of $\div(a,b)$. Therefore we have to add the condition that the product cb computed among the integers is the same as the product cb in $\mathbf{M}_d$. The following Lemma says that the parallel version of this condition is polynomially existential.

Lemma 51 *The family of ternary relations $R = \langle R_{u,t} \mid \langle u,t \rangle \in \nabla \rangle$ is polynomially existential, where $R_{u,t}$ is defined in the following way.*

Assume that $u, t \in \omega$, $u \geq t$, and $a, b, w \in \mathbf{M}_u$. Then $R_{u,t}(a,b,w)$ holds iff for all $i \in 2^{u-t}$, $w[i,t] = 0$ implies that $a[i,t]b[i,t] < 2^{2^t}$, and $w[i,t] = 1$ implies that $a[i,t]b[i,t] \geq 2^{2^t}$

Proof of Lemma 51. For each fixed $t \in \omega$ we define two functions F_t, G_t on ω. Suppose that $a = \sum_{i=0}^{\infty} \alpha_i 2^{i2^t} \in \omega$, where $\alpha_i = a[i,t]$. Then $F_t(a) = \sum_{i=0}^{\infty} \alpha_i 2^{2i2^t} = \sum_{i=0}^{\infty} \alpha_i 2^{i2^{t+1}}$. This definition implies that every second 2^{2^t}- ary digits of $F_t(a)$ is 0 and between the 0s we have the digits of a. That is $F_t(a)$ "stretches" out the 2^{2^t}-ary form by a factor of 2, and puts 0s in the odd numbered places. We get the integer $G_t(a)$ from a by keeping only its 2^{2^t}-ary digits at the odd numbered places and then "compressing" this sequence by a factor of two. More precisely if $a \sum_{i=0}^{\infty} \alpha_i 2^{i2^t}$ then $G_t(a) = \sum_{j=0}^{\infty} \alpha_{2j+1} 2^{j2^t}$.

These functions has the following useful property.

Proposition 1 *Assume $u, t \in \omega$, $u \geq t$, $a, b \in \mathbf{M}_u$, and let*

$$h_{u,t}(a,b) = G_t\Big(F_t(a) \otimes_{u+1,t+1} F_t(b)\Big)$$

Then for all $i \in 2^{u-t}$, $a[i,t]b[i,t] < 2^{2^t}$ iff $h[i,t] = 0$.

Proof of Proposition 1. When we compute the parallel product $F_t(a) \otimes_{u+1,t+1} F_t(b)$ to get the ith component of the result we have to multiply $a[i,t]$ and $b[i,t]$ modulo $2^{2^{t+1}}$. Suppose that the result is $\mu_i 2^{2^t} + \lambda_i$, where $\mu_i, \lambda_i \in 2^{2^t}$. We have $F_t(a) \otimes_{u+1,t+1} F_t(b) = \sum_{i=0}^{2^{u-t}-1} (\mu_i 2^{2^t} + \lambda_i) 2^{i2^{t+1}}$. Therefore the definition of G_t implies that $G_t\Big(F_t(a) \otimes_{u+1,t+1} F_t(b)\Big) = \sum_{i=0}^{2^{u-t}-1} \mu_i 2^{2^t}$. We have $\mu_i = (h_{u,t}(a,b))[i,t]$ and so the definition of μ_i implies the statement of the proposition. *Q.E.D.*(Proposition 1)

Lemma 40 and Lemma 44 together imply that the family of functions $H = \langle h_{u,t} \mid \langle u,t \rangle \in \nabla \rangle$ is polynomially existential, where the function $h_{u,t}$ is defined in Proposition 1.

The relation $R_{u,t}(a,b,w)$ can be defined by "there exists a $\rho \in \mathbf{M}_u$ such that $\rho = h_{u,t}(a,b)$ and for all $i \in 2^{u-t}$, $w = \min_{u,t}(e_{u,t}, \rho)$". By Lemma 28 and Proposition 1 this shows that family $R_{u,t}$ is polynomially existential. *Q.E.D.*(Lemma 51)

Definition. We define a binary term $\mathtt{rem}(x,y)$ of $\mathcal{M}$ by $\mathtt{rem}(x,y) = x + (-\mathbf{1})y \div (x,y)$. (Suppose that $d \in \omega$, $a,m,b \in \mathbf{M}_d$, $m \neq 0$. Then $\mathbf{M}_d \models b = \mathtt{rem}(a,m)$ iff b is the least nonnegative residue of a modulo m.) For all $d,t \in \omega$ with $d \geq t$, $\mathtt{rem}_{d,t}$ will be the binary function defined on $\mathbf{M}_d$ in the following way. For all $a,m,b \in \mathbf{M}_d$, $\mathtt{rem}_{d,t}(a,m) = b$ iff for all $i \in 2^{d-t}$, $\mathtt{rem}(a[i,t], m[i,t]) = \mathtt{rem}(b[i,t])$. □

Lemma 52 *The function symbol $\div$ and the family of functions $\langle \mathtt{rem}_{d,t} \mid \langle d,t \rangle \in \nabla \rangle$ are polynomially existential in $\mathbf{M}$.*

Proof of Lemma 52. Let $R = \langle R_{u,t} \mid \langle u,t \rangle \in \nabla \rangle$ be the family of ternary relations defined in Lemma 51. For all $d \in \mathbf{M}_d$, and for all $q,a,b \in \mathbf{M}_d$, $\mathbf{M}_d \models q = \div_{d,t}(a,b)$ iff

$$R(b,q,e_{d,t}) \ \wedge \ \exists r \in \mathbf{M}_d, \Big(a = (q \otimes_{d,t} b) \oplus_{d,t} r \ \wedge \ r <_{d,t} q\Big)$$

We have already proved that $\mathbf{M}$ is existentially parallel with respect to multiplication and addition, and by Lemma 51 the relation R is polynomially existential, therefore this definition of $\div_{d,t}$ implies that the function symbol $\div$ is polynomially existential as well.

The family $\langle \mathtt{rem}_{d,t} \mid \langle d,t \rangle \in \nabla \rangle$ is polynomially existential since the function $\mathtt{rem}_{d,t}$ is defined by a term which is using on function symbols which are polynomially existential. *Q.E.D.*(Lemma 52).

Lemma 53 *The function symbol $\mathbf{p}$ of $\mathcal{M}$ is polynomially existential.*

Proof of Lemma 53. We have to construct an existential formula ψ such that if $c \in \omega$ is sufficiently large then for all $d,t \in \omega$ with $d \geq t$, and for all $a,b \in \mathbf{M}_d$, we have $\mathbf{p}_{d,t}(a) = b$ iff $\mathbf{M}_v \models \psi(a,b,d,t)$, where $v = t + c(d-t)$.

Suupose that $K \in \omega$ is a sufficiently large integer and c is sufficiently large with respect to K.

We will construct the formula ψ in the form of

$$\psi(a,b,d,t) \equiv (t \leq K \wedge \psi_0(a,b,d,t)) \vee (t > K \wedge \psi_1(a,b,d,t))$$

(Here we used a,b,d,t as variables to make the roles of the variables clear.)

The definition of ψ_0. For all integers $i \in [-2^K, 2^K]$ we define three elements of $\mathbf{M}_d$, a_i, t_i and M_i. If $i \geq 0$ then

$$\mathbf{M}_d \models a_i = 2^i a \ \wedge \ t_i = 2^i t \ \wedge \ M_i = 2^i e_{d,t}$$

If $i < 0$ then

$$\mathbf{M}_d \models a_i = \div(a, 2^i) \ \wedge \ t_i = \div(t, 2^i) \ \wedge \ M_i = \div(e_{d,t}, 2^i)$$

This definition implies that for each $i \in [-2^K, 2^K]$ there exist terms α_i, τ_i, μ_i of $\mathcal{M}$, depending only on i, such that for all choices of d, K, $t \in \omega$, $t \leq K$, $a \in \mathbf{M}_d$, we have

$$\mathbf{M}_d \models a_i = \alpha_i(a, d, t) \wedge t_i = \tau_i(a, d, t) \wedge M_i = \mu_i(a, d, t)$$

For each $j \in 2^d$, the three sequence of integers $\langle a_i[j, 0] \mid j \in [-2^K, 2^K]\rangle$, $\langle t_i[j, 0] \mid j \in [-2^K, 2^K]\rangle$, $\langle M_i[j, 0] \mid j \in [-2^K, 2^K]\rangle$, together uniquely determine the integers $a[j, t]$, t, and $\mathtt{rem}(j, 2^t)$.

Consequently there exists a boolean expression $\mathcal{B}$ with $3(2^{K+1} + 1)$ variables such that for all $j \in 2^{d-t}$ we have

$$(\mathbf{p}_{d,t}(a))[j, 0] = \mathcal{B}(\vec{a}_i[j, 0], \vec{t}_i[j, 0], \vec{M}_i[j, 0])$$

where $\vec{x}_i[j, 0]$, stands for the sequence $\langle x_i[j, 0] \mid i \in [-2^K, 2^K]\rangle$ for $x = a, t, M$. According to Lemma 15 this implies that there exists a term σ of $\mathcal{M}$ such that $\mathbf{M}_d \models \mathbf{p}_{d,t}(a) = \sigma(a, t)$. Based on that, using Corollary 9 of Lemma 35 we can define the formula ψ_0 with the required properties.

The definition of ψ_1. Assume that $d, t \in \omega$, $d \geq t > K$ and $a \in \mathbf{M}_d$. We define three integers $A_0, A_1, A_2 \in \mathbf{M}_d$, such that for all $i \in 2^{d-t}$ exactly on of the following two conditions are satisfied

(i) $A_0[i, t] = a[i, t] \geq 2^t$ and $A_1[i, t] = A_2[i, t] = 0$.

(ii) $A_0[i, t] = 0$, $a[i, t] < 2^t$, $a[i, t] = A_1[i, t]2^q + A_2[i, t]$, and $A_2[i, t] < 2^q$.

This property uniquely determines the integers $A_0, A_1, A_2 \in \mathbf{M}_d$, moreover Lemma 47 implies that that there exists an existential formula φ of $\mathcal{M}$ such that A_0, A_1, A_2 are the unique elements of $\mathbf{M}_d$ such that $\mathbf{M}_v \models \varphi(a, A_0, A_1, A_2, d, t)$, where $v = t + c(d - t)$.

Let $B_0 = \odot_{d,t}(2^{2^t-1}, \min_{d,t}(A_0, e_{d,t}))$. (That is $B_0[i, t] = 2^{2^{t-1}}$ if $A_0[i, t] \neq 0$, otherwise $B_0[i, t] = 0$.)

Then

$$\mathbf{p}_{d,t}(a) = \max_{d,t}\Big(B_0, \otimes_{d,t}\big(\mathbf{p}_{d,t}[\odot_{d,t}(2^q, A_1)], \mathbf{p}_{d,t}[A_2]\big)\Big)$$

We know already that the functions symbols max and $\times$ are polynomially existential, therefore it is sufficient to show that the following two families of relations relations are polynomially existential:

(66) $\Theta = \langle \Theta_{d,t} \mid \langle d, t\rangle \in \nabla\rangle$, *where for each* $d, t \in \omega$ *with* $d \geq t$ *and for each* $a, b \in \mathbf{M}_d$, $\Theta_{d,t}(a, b)$ *holds iff* $t > K$ *and for all* $i \in 2^{d-t}$, $a[i, t] < 2^t$ *and* $2^q | a[i, t]$ *and* $b = \mathbf{p}_{d,t}(\odot_{d,t}(2^q, a))$

(67) $\Phi = \langle \Phi_{d,t} \mid \langle d, t\rangle \in \nabla\rangle$, *where for each* $d, t \in \omega$ *with* $d \geq t$ *and for each* $a, b \in \mathbf{M}_d$, $\Phi_{d,t}(a, b)$ *holds iff* $t > K$ *and for all* $i \in 2^{d-t}$, $a[i, t] < 2^q$ *and* $b = \mathbf{p}_{d,t}(a)$

In other words, the original problem about the existential definability of $\mathbf{p}_{d,t}(a)$ has to be solved with some additional assumptions. The following lemma will be used to define the family Θ in an existential way.

Proposition 2 *The family of relations* Θ *defined in condition* (66) is uniformly existential.

Proof of Lemma 2. For each $d \in \omega$, let Θ'_d be the ternary relation on $\mathbf{M}_d$, defined by: for each $t, a, b \in \mathbf{M}_d$, $\Theta'_d(a, b, t)$ holds iff $t \leq d$ and $\Theta_{d,t}(a, b)$. We show that the family of relations $\Theta' = \langle \Theta'_d \mid d \in \omega \rangle$ is uniformly existential. This clearly implies the conclusion of the proposition.

By Lemma 49 it is sufficient to show that there exists $3k$-sensitive propositional formula $P(x_0, ..., x_{3k-1}, y_0, ..., y_{l-1})$ of $\mathcal{M}$ with $k = 3$ and $l = 1$ and with property.

(68) *For all* $d \in \omega$ *and for all* $t, q, a, b \in \mathbf{M}_d$, *we have* $\Theta'_d(a, b, t)$ *iff there exists* $a_0, ..., a_3, w_0 \in \mathbf{M}_d$ *such that* $a_0 = a$, $a_1 = b$, $a_2 = e_{d,t}$, $d \geq t$, $q = \lfloor \log_2 t \rfloor$, $w_0 = 2^q$ *and for all* $i \in 2^{d-q}$, $\mathbf{M}_q \models P(\vec{A}_0, ..., \vec{A}_3, w_0)$, *where* $\vec{A}_j$ *stands for the sequence* $a_j[i-1, q], a_j[i, q], a_j[i+1, q]$ *for* $j = 0, 1, 2, 3$.

The condition that there exists $a_0, ..., a_3, w_0 \in \mathbf{M}_d$ such that $a_0 = a$, $a_1 = b$, $a_2 = e_{d,t}$, $d \geq t$, $q = \lfloor \log_2 t \rfloor$, $w_0 = 2^q$ can be expressed by an existential formula χ in $\mathbf{M}_d$ since $q = \lfloor \log_2 t \rfloor$ is equivalent to $2^q \leq t < 2^{q+1}$. Therefore condition (68) implies that $\Theta'(d)(a, b, t)$ is equivalent to $\mathbf{M}_d \models \exists a_0, ..., a_3, w_0, \chi(a, b, t, a_0, ..., a_3, w_0)$ and for all $i \in 2^{d-q}$, $\mathbf{M}_q \models P(\vec{A}_0, ...\vec{A}_3, w_0)$, where χ is an existential formula of $\mathcal{M}$.

Lemma 49 implies that the condition "for all $i \in 2^{d-q}$, $\mathbf{M}_q \models P(\vec{A}_0, ..., \vec{A}_{k-1}, b_0, ..., b_{l-1})$" can be expressed by an existential formula of $\mathcal{M}$ in $\mathbf{M}_d$, therefore we only have to prove the existence of a 9-sensitive propositional formula P satisfying condition (68).

In the definition of P the variable a_3 will be denoted by h and for a_0, a_1, a_2 we will use the symbols $a, b, e_{d,t}$ indicated in condition (68). To make the formulas more understandable we rename the variables x_i in the following way: $x_{3j} = z_{j,-1}, x_{3j+1} = z_{j,0}, x_{3j+1} = z_{j,1}$. The advantage of this notation is that in condition (68) the variable $z_{j,\delta}$ takes the value $a_j[i + \delta]$ for $j = 0, 1, ..., k-1$, $\delta = -1, 0, 1$.

We define P by $P \equiv \bigwedge_{r \in 5} \Lambda_r$ where the propositional formulas Λ_r are defined below. First we write each formula Λ_r with the variables $z_{j,\delta}$, this is its definition, and then as a motivation, we write the formula Λ_r in the form that we get if the variables take the values indicated y condition (68) and by the abbreviation $h = a_3$.

$\Lambda_0 \equiv z_{2,0} = 1 \to z_{3,0} = z_{0,0}$

$e_{d,t}[i, q] = 1$ implies $h[i, q] = a[i, q]$

$\Lambda_1 \equiv (z_{2,0} = 0 \wedge z_{3,-1} \neq 0) \to z_{3,0} = z_{3,-1} - w_0$

$e_{d,t} = 0 \wedge h[i-1, q] \neq 0$ implies $h[i, q] = h[i-1, q] - 2^q$

$\Lambda_2 \equiv (z_{2,0} = 0 \wedge z_{3,-1} = 0) \to z_{3,0} = 0$

$e_{d,t}[i, q] = 0 \wedge h[i-1, q] = 0$ implies $h[i, q] = 0$

$\Lambda_3 \equiv z_{3,0} \neq w_0 \to z_{1,0} = 0$

$h[i, q] \neq 2^q$ implies $b[i, q] = 0$

$\Lambda_4 \equiv z_{3,0} = w_0 \to z_{1,0} = 1$

$h[i, q] = 2^q$ implies $b[i, q] = 1$

The meaning of these formulas is the following. Assume that an integer $i_0 \in 2^{d-q}$ is given with $e_{d,t}[i_0, q] = 1$. It means that $2^{i_0 2^q} = 2^{\nu 2^t}$ for some $\nu \in 2^{d-t}$, therefore $i_0 = \nu 2^{t-q}$. Because of the assumption $a[\nu, t] < 2^{2^q}$ have that $a[\nu, t] = a[i_0, q]$. We have to show that the described formulas together are equivalent to, $b[\nu, t] = 2^{a[i_0,q]2^q}$. Since $b[\nu, t]$ is a power of 2^{2^q}, its 2^{2^q}-ary form contains a single nonzero digit and this digit will be one.

The propositional formula P as we have defined it determines when $b[i, q] = 1$ in the following way. The value of $h[i_0, q]$ is $a[i_0, q]$, then as starting from $i = i_0$ each time we increase i with 1 the value of $h_{i,q}$ will decrease by 2^q. Therefore we will have $2^{i2^q} = 2^{a[\nu,t]2^q}$ when $h[i, q]$ becomes 0 so at that value of i we have $b[\nu, t] = 2^{i2^q}$. The propositional formula P defined above describes this definition of h and the connections between the values of a, b, h and $e_{d,t}$. The syntax of the formula shows that it is $3k$-sensitive, so it satisfies condition (68). *Q.E.D.*(Proposition 2)

Proposition 3 *The family of relations* Φ *defined in condition* (67) is uniformly existential.

Proof of Proposition 3. The proof is similar to the proof of Proposition 2. For each $d \in \omega$, let Φ'_d be the ternary relation on $\mathbf{M}_d$, defined by: for each $t, a, b \in \mathbf{M}_d$ $\Phi'_d(a, b, t)$ holds iff $t \leq d$ and $\Phi_{d,t}(a, b)$. We show that the family of relations $\Phi' = \langle \Phi'_d \mid d \in \omega \rangle$ is uniformly existential. This clearly implies the conclusion of the proposition.

By Lemma 49 it is sufficient to show that there exists $3k$-sensitive propositional formula $P(x_0, ..., x_{3k-1}, y_0, ..., y_{l-1})$ of $\mathcal{M}$ with $k = 7$ and $l = 0$ and with property.

(69) *For all* $d \in \omega$ *and for all* $t, q, a, b \in \mathbf{M}_d$, *we have* $\Phi'_d(a, b, t)$ *iff there exists* $a_0, ..., a_6 \in \mathbf{M}_d$ *such that* $a_0 = a$, $a_1 = b$, $a_2 = e_{d,t}$, $a_3 = e_{d,t}2^{(2^{t-q}-1)2^q}$, $a_4 = b2^{(2^{t-q}-1)2^q}$ $d \geq t$, $q = \lfloor \log_2 t \rfloor$, *and for all* $i \in 2^{d-q}$, $\mathbf{M}_q \models P(\vec{A}_0, ..., \vec{A}_4)$, *where* $\vec{A}_j$ *stands for the sequence* $a_j[i-1, q], a_j[i, q], a_j[i+1, q]$ *for* $j = 0, 1, ..., 6$.

The condition that there exists $a_0, ..., a_6 \in \mathbf{M}_d$ such that $a_0 = a$, $a_1 = b$, $a_2 = e_{d,t}$, $a_3 = e_{d,t}2^{(2^{t-q}-1)2^q}$, $a_4 = b2^{(2^{t-q}-1)2^q}$ $d \geq t$, $q = \lfloor \log_2 t \rfloor$, can be expressed by an existential formula χ in $\mathbf{M}_d$ since $q = \lfloor \log_2 t \rfloor$ is equivalent to $2^q \leq t < 2^{q+1}$. Therefore condition (69) implies that $\Phi'(d)(a, b, t)$ is equivalent to $\mathbf{M}_d \models \exists a_0, ..., a_6, \chi(a, b, t, a_0, ..., a_6)$ and for all $i \in 2^{d-q}$, $\mathbf{M}_q \models P(\vec{A}_0, ...\vec{A}_6)$, where χ is an existential formula of $\mathcal{M}$.

Lemma 49 implies that the condition "for all $i \in 2^{d-q}$, $\mathbf{M}_q \models P(\vec{A}_0, ..., \vec{A}_{k-1}, b_0, ..., b_{l-1})$" can be expressed by an existential formula of $\mathcal{M}$ in $\mathbf{M}_d$, therefore we only have to prove the existence of a k-sensitive propositional formula P satisfying condition (69). (In the present case $k = 7$ and $l = 0$.)

In the definition of P the integer a_5 will be denoted by h, and the integer a_6 by g and for a_0, a_1, a_2, a_3, a_4 we will use the expressions $a, b, e_{d,t}$, $e_{d,t}2^{(2^{t-q}-1)2^q}$, $b2^{(2^{t-q}-1)2^q}$ indicated in condition (69). To make the formulas more understandable we rename the variables x_i in the following way: $x_{3j} = z_{j,-1}, x_{3j+1} = z_{j,0}, x_{3j+1} = z_{j,1}$. The advantage of this notation is that in condition (69) the variable $z_{j,\delta}$ takes the value $a_j[i + \delta]$ for $j = 0, 1, ..., k-1$, $\delta = -1, 0, 1$.

We define P by $P \equiv \bigwedge_{r\in 8} \Lambda_r$ where the propositional formulas Λ_r are defined below. We write the formulas Λ_r, $r \in 8$ in the form when already $a_j[i+\delta, q]$ has been substituted for $z_{j,\delta}$. The formulas Λ_r with the variables $z_{j,\delta}$ (as in Proposition 2), can be derived from this by performing the reverse substitutions.

(70) $\Lambda_0 \equiv e_{d,t}[i,q] = 1 \to (h[i,q] = a \wedge g[i,q] = 1)$

(71) $\Lambda_1 \equiv (e_{d,t}[i,q] = 0 \wedge h[i-1,q] \neq 0) \to h[i,q] = h[i-1,q] - 1$
$\Lambda_2 \equiv (e_{d,t}[i,q] = 0 \wedge h[i-1,q] = 0) \to h[i,q] = 0$

(72) $\Lambda_3 \equiv (e_{d,t}[i,q] = 0 \wedge h[i,q] < h[i-1,q] = 0) \to g[i,q] = g[i-1,q] + g[i-1,q]$
$\Lambda_4 \equiv e_{d,t}[i,q] = 0 \wedge h[i,q] = h[i-1,q] \to g[i,q] = g[i-1,q]$

(73) $\Lambda_5 \equiv (e_{d,t}2^{(2^{t-q}-1)2^q})[i,q] = 1 \to (b2^{(2^{t-q}-1)2^q})[i,q] = g[i,q]$
$\Lambda_6 \equiv (e_{d,t}2^{(2^{t-q}-1)2^q})[i,q] = 0 \to (b2^{(2^{t-q}-1)2^q})[i,q] = 0$

The meaning of these formulas is the following. Assume that an integer $i_0 \in 2^{d-q}$ is given with $e_{d,t}[i_0, q] = 1$. It means that $2^{i_0 2^q} = 2^{\nu 2^t}$ for some $\nu \in 2^{d-t}$, therefore $i_0 = \nu 2^{t-q}$. Because of the assumption $a[\nu, t] < 2^q$ have that $a[\nu, t] = a[i_0, q]$. We have to show that the described formulas together are equivalent to, $b[\nu, t] = 2^{a[i_0,q]2^q}$. Since $b[\nu, t]$ is a power of 2^{2^q}, its 2^{2^q}-ary form contains a single nonzero digit and this digit will be one.

The propositional formula P as we have defined it determines when $b[i, q] = 1$ in the following way. We consider the sequence $h[i, q]$, for $i = 0, ..., 2^{t-q} - 1$. According to the definition of Λ_0 it starts with the integer a, and then, according to Λ_1 and Λ_2, each element of the sequence is smaller by 1 than the previous one, till it reaches the value 0 where it remains constant. Since $a < 2^q = 2^{\lceil \log_2 t \rceil} \log \leq 2t < 2^{t-q}$ the value 0 will be reached for some $i \in 2^{t-q}$. The sequence $g[i, q]$, $i = 0, 1, ...2^{t-q}$ starts with $g[0, q] = 1$ according to Λ_0 and it is increasing by a factor of 2 at each step where the sequence $h[i, q]$, $i = 0, 1, ..., 2^{t-q}$ is decreasing by 1, and then remains constant. Since the sequence $h[i, q]$, $i = 0, 1, ..., 2^{t-q}$ reaches the value 0 in a steps, the sequence $g[j, q]$ reaches the value 2^a in the same a steps and this will be its last value as well, that is, if i_1 is the largest integer with $i_0 + 2^{t-q} > i_1 > i_0$ then $g[i_1, q] = 2^a$. The integer i_1 is also the unique integer i in the interval $[i_0, i_0 + 2^{t-q} - 1]$ with the property that $(e_{d,t}2^{(2^{t-q}-1)2^q})[i, q] = 1$, so it can be used to identify i_1 in Λ_5 and Λ_6. *Q.E.D.*(Proposition 3) *Q.E.D.*(Lemma 53)

7 RAMs and polynomially existential functions, Proof of Theorem 8

Proof of Theorem 8. Assume that $F = \langle F_{d,u} \mid \langle d, u\rangle \in \nabla\rangle$ is a family of k-ary functions such that for each $d, u \in \omega$ with $d \geq u$, $F_{d,u}$ is a function defined on $\mathbf{M}_d$ with values in $\{0, 1\}$ and the family is polynomial time computable with respect to $\mathbf{M}$. We have to show that there exists a $c \in \omega$ and an existential formula φ_0 of $\mathcal{M}$ such that

(74) *for all* $d, u \in \omega$ *with* $d \geq u$ *and for all* $a_0, ..., a_{k-1} \in \mathbf{M}_d$, $b \in \{0, 1\}$ *we have* $F_{d,u}(a_0, ..., a_{k-1}) = b$ *iff* $\mathbf{M}_v \models \varphi_0(a_0, ..., a_{k-1}, b, d, u)$, *where* $v = u + c(d - u)$.

The assumption that the family F is polynomial time computable with respect to $\mathbf{M}$ implies that there exist a γ_1 and a program P such that the following holds

(75) *for all sufficiently large* $d \in \omega$, *for all* $u \in \omega$ *with* $d \geq u$, *and for all* $a_0, ..., a_{k-1} \in \mathbf{M}_d$, *machine* N_m *(a RAM with word length* m*), where* $m = 2^d$, *with program* P *and input* $k, d, u, a_0, ..., a_{k-1}$, *using only the first* $2^{\gamma_1(d-u)}$ *memory cells in time* $2^{\gamma_1(d-u)}$ *computes* $F_{d,u}(a_0, ..., a_{k-1})$.

We will choose the constant $c \in \omega$ later. We define now the existential formula φ_0 of $\mathcal{M}$. For this definition we will assume that each operation of $\mathcal{M}$ is binary. (The unary operations are considered binary operations which do not depend on their second argument and the constants are considered as binary operations which do not depend on any of their arguments.)

Let $m = 2^d$, $s = 2^{\gamma_1(d-u)}$. We will denote by $\mathcal{R}$ a random access with word length m, which has s memory cells. (That is we get $\mathcal{R}$ from N_m keeping only its first s memory cells.) Our assumption is that the machine $\mathcal{R}$ with program P and with input $k, d, u, a_0, ..., a_{k-1}$ in time s computes the value of $F_{d,u}(a_0, ..., a_{k-1})$. More precisely we assume the following.

Suppose that P is the sequence $p_0, ..., p_{c'-1}$, and at time 0 the content of $\mathtt{cell}_i$ is ρ_i for all $i \in s$. Then $\rho_i = p_i$ for all $i \in c'$, $\rho_{c'} = k$, $\rho_{c'+1} = d$, $\rho_{c'+2} = u$, $\rho_{c'+3+i} = \alpha_i$ for all $i \in k$, and $\rho_j = 0$ for all $j \in s$ with $j \geq c' + 3 + k$. Our assumption is that if the machine starts to work with this initial state then at time $s - 1$ the content of $\mathtt{cell}_0$ is $F_{d,u}(a_0, ..., a_{k-1})$.

Let $\rho = \sum_{i=0}^{s-1} \rho_i 2^{i2^u}$. With this notation at time 0 the content of $\mathtt{cell}_i$ is $\rho[i, u]$ for all $i \in s$. We will say that the integer ρ is the unified input of the machine $\mathcal{R}$. (The motivation for this expression is that ρ determines all of the integers in the input sequence and the program P as well.) It is important that

(76) *there exists a term* ξ_0 *of* $\mathcal{M}$ *depending only on* P *and* k *such that* $\mathbf{M}_v \models \rho = \xi_0(a_0, ..., a_{k-1}, d, u)$.

This implies that in the formula φ_0 to be defined we can use ρ as an argument.

Now we will use the following trivial fact. If M is a random access machine which works with ν memory cells till time ν then the output of M can be computed by a circuit

C of size ν^{c_3} where c_3 is a constant, and the circuit C is given independently of the contents of the memory cells at time 0. The gates of the circuit are performing the $\mathcal{M}$ operations. For each memory cell x of $\mathcal{M}$ there is an input node of C where the input is the content of cell x at time 0. Moreover the circuit C can be constructed by a turing machine with the input ν in time ν^{c_4}, where $c_4 \in \omega$ is a constant.

We apply this for the present situation with $M{:=}\,\mathcal{R}$, $\nu{:=}\,s$ and get the following, where $\mathbf{k}$ denotes the number of $\mathcal{M}$ operations.

Proposition 4 *There exists a sequence of triplets $T = \langle\langle \alpha_i, \kappa_i, \lambda_i\rangle \mid i \in s^{c_3}\rangle$ with the following properties:*

(77) *for all $i \in s$, $\alpha_i = \kappa_i = \lambda_i = 0$, and for all $i \in s^{c_3}\backslash s$, $\alpha_i \in \mathbf{k}$, $\kappa_i \in i$, $\lambda_i \in i$,*

(78) *there exists a turing machine $\mathcal{T}'$ such that if the machine $\mathcal{T}'$ gets s as input, then it computes in time s^{c_4}, the sequence $\langle \alpha_i, \kappa_i, \lambda_i\rangle$,*

(79) *if the sequence $\mathbf{b} = \langle \beta_i \mid i \in s^{c_3}\rangle$ satisfies conditions (i) and (ii), then it also satisfies condition (iii), where*

(i) for all $i \in s$, $\beta_i = \rho[i, u]$, that is, β_i is the content of $\mathtt{cell}_i$, at time 0 in the machine $\mathcal{R}$ with unified input ρ,

(ii) for all $i \in s^{c_3}\backslash s$, $\mathbf{M}_m \models \beta_i = \mathbf{f}_{\alpha_i}(\beta_{\kappa_i}, \beta_{\lambda_i})$,

(iii) $\beta_{s^{c_3}-1}$ is the output of $\mathcal{R}$ at time s^c at unified input ρ.

In other words the circuit C has a node x_i for each $i \in s^{c_3}$. The nodes $x_i, i \in s$ are the input nodes, the node $x_{s^{c_3}-1}$ is the output node, and for each $i \in s^{c_3}\backslash s$, at node x_i there is a gate performing the operation $\mathbf{f}_{\alpha_i}$ on the arguments which are the outputs of gates (or input nodes) at nodes x_{κ_i} and x_{λ_i}.

Assume now that a turing machine $\mathcal{T}'$ is fixed that determines a sequence T with the properties described above. The unified input ρ and the program P are also fixed. The formula φ_0 in $\mathbf{M}_v$ will be equivalent to the following: "there exists a sequence $B = \langle B_i \mid i \in s^{c_3}\rangle$ which satisfies conditions (i) and (ii) of Proposition 4 with $\beta_i{:=}\,B_i$ and for this sequence B we have $B_{s^{c_3}-1} = b$". For such a formula φ_0 we clearly have $F_{d,u}(a_0, ..., a_{k-1}) = b$ iff $\mathbf{M}_v \models \varphi_0(a_0, ..., a_{k-1}, b, d, u)$.

As a first step we reformulate the properties of (i) and (ii) of Proposition 4. The goal of this reformulation is to make these properties more easily expressible by existential formulas in $\mathbf{M}_v$. We will use the following notation: $s_0 = s^{c_3}$, $h = \lceil \log_2 \mathbf{k} \rceil$.

Proposition 5 *Assume that $B = \langle B_i \mid i \in s_0\rangle$ is a sequence with $B_i \in \mathbf{M}_m$. Then conditions (i) and (ii) of Proposition 4 are satisfied with $\mathbf{b}{:=}\,B$ iff there exist $2 + \mathbf{k} + h$ sequences K, L, $S^{(j)}$, $j \in \mathbf{k}$, $Q^{(r)}$, $r \in h$, all them of length s_0, satisfying the following conditions*

(80) *for all $i \in s$, B_i is the content of $\mathtt{cell}_i$ at time 0 in the machine $\mathcal{R}$ with program P and unified input input ρ,*

(81) *for all* $i \in s_0 \backslash s$, $K_i = B_{\kappa_i}$, $L_i = B_{\lambda_i}$, *and for all* $i \in s$, $K_i = L_i = 0$.

(82) *for all* $i \in s_0$, $r \in h$, $Q_i^{(r)} = \alpha_i[r, 2]$ *(and consequently* $Q^{(r)}(i) \in \{0, 1\}$*).*

(83) *for all* $i \in s_0$, $j \in \mathbf{k}$, $\mathbf{M}_m \models S_i^{(j)} = \mathbf{f}_j(K_i, L_i)$.

(84) *for all* $i \in s_0$, $B_i = S_i^{(j)}$, *where* j *is the unique integer with* $j \in \mathbf{k}$, *and* $\forall r \in h, j[r, s] = Q_i^{(r)}$.

Proof of Proposition 5 Since we fixed the turing machine $\mathcal{T}'$ the sequence $\langle\langle \alpha_i, \kappa_i, \lambda_i\rangle \mid i \in s^{c_3}\rangle$ is given. Assume first that $\mathbf{b}{:=}\ B$ satisfies conditions (i) and (ii) of property (79). Then the sequences $B = \langle \beta_i \mid i \in s^{c_3}\rangle$, $K = \langle \beta_{\kappa_i} \mid i \in s^{c_3}\rangle$, $L = \langle \beta_{\lambda_i} \mid i \in s^{c_3}\rangle$, obviously satisfy conditions (80) and (81). Condition (82) and (83) define the sequences $Q^{(r)}$ and $S^{(j)}$, $r \in h$, $j \in \mathbf{k}$, and condition condition (84) is the same as condition (ii) of property (79).

In the other direction assume that the sequences B, K, L, etc, satisfy conditions (80), (81), (82), (83), and we show that $\mathbf{b}{:=}\ B$ satisfies conditions (i),(ii) of property (79). Condition (80) imply condition (i). By condition (84) and (82) we have $B_i = S_i^{(\alpha_i)}$, and therefore by condition (83), $B_i = \mathbf{f}_{\alpha_i}(K_i, L_i)$ which implies condition (ii). *Q.E.D.*(Proposition 5)

Let $c \in \omega$ be constant sufficiently large with respect to $\gamma_1, k, \mathtt{length}(P), \mathbf{k}, c_3, c_4$, and let $v = u + c(d - u)$. We show that for each of the conditions (80),...,(84) there exists an existential formula ψ such that the condition holds iff $\mathbf{M}_v \models \psi(\bar{B}, \bar{K}, \bar{L}, \vec{\bar{S}}, \vec{\bar{Q}}, \rho, d, u)$, where for each sequence $A = \langle a_i \mid i \in s^{c_3}\rangle$, $\bar{A}$ is the integer $\sum_{i=0}^{s^{c_3}-1} a_i 2^{i2^u}$, and $\vec{\bar{S}} = \langle \bar{S}^{(0)}, ..., S^{(\mathbf{k}-1)}\rangle$, $\vec{\bar{Q}} = \langle \bar{Q}^{(0)}, ..., Q^{(h-1)}\rangle$.

Condition (80) is equivalent to $\mathbf{M}_v \models \overline{\mathrm{mod}}(\bar{B}, 2^{s^{c_3}} 2^u) = \rho(a_0, ..., a_{k-1}, d, u)$, where $\overline{\mathrm{mod}}(x, y)$ is a term of $\mathcal{M}$ such that for all $w \in \omega$ and for all $x, y, z \in w$ $\mathbf{M}_w \models z = \overline{\mathrm{mod}}(x, y)$ iff the least nonnegative residue of x modulo y is z, that is, $z = \mathrm{mod}(x, y)$.

To show that condition (82) is equivalent to an existential formula in $\mathbf{M}_v$ we use Lemma 43. We have that $\alpha_i \leq \mathbf{k}$, $\mathbf{k}$ is a constant and the turing machine $\mathcal{T}'$ computes the bits of α_i in time $2^{c_4(d-u)}$ where $c_4 \ll c$ (and $v = u + c(d - u)$). Lemma 43 is about restricted turing machines. $\mathcal{T}'$ is not restricted but can make a restricted machine from it with the definition $\mathtt{tplength}(\mathcal{T}') = 2^{c_4(d-u)}$. The integer $\bar{Q}$ is defined already in a way that Lemma 43 is applicable with $b_0{:=}\ \bar{Q}$. Therefore the existential formula whose existence is stated in Lemma 43 will describe condition (82).

The fact that condition (81) can be expressed by an existential formula is a consequence of Lemma 40. We get the sequences K_i, L_i form the sequence B_i by moving its elements to (possibly several) new places and inserting 0s. The destinations of the elements and the places of zeros are computed by a turing machine as required by Lemma 40.

The fact that condition (83) can be expressed by an existential formula in $\mathbf{M}_v$ is an immediate consequence of Lemma 46.

We show now that condition (84) can be described by an existential formula whose existence is guaranteed by Lemma 34. We have to show that the condition can be expressed

by a propositional formula $\mathcal{P}$ of $\mathcal{L}^{(=)}$. For each $j \in \mathbf{k}$, let $\mathcal{B}_j(x_0, ..., x_{h-1})$ be a boolean expression so that if $a_i = j[i, 2]$ that $\mathcal{B}_j(a_0, ..., a_{h-1}) = 1$, and otherwise $\mathcal{B}_j(a_0, ..., a_{h-1}) = 1$. We define the propositional formula $\mathcal{P}$ of $\mathcal{L}^{(=)}$, by

$$\mathcal{P}(X, Y_0, ..., Y_{\mathbf{k}-1}, Z_0, ..., Z_{h-1}) \equiv \bigwedge_{j \in \mathbf{k}} \mathcal{B}_j(Z_0, ..., Z_{h-1}) \rightarrow X = Y_j$$

Clearly for each $i \in s^{c_3}$, $\mathbf{N}_{\bar{u}} \models \mathcal{P}(B_i, S_i^{(0)}, ..., S_i^{(\mathbf{k}-1)}, Q^{(0)}, ..., Q^{(h-1)})$, where $\bar{u} = 2^{2^u}$, iff condition (84) holds for this particular integer i. Therefore by Lemma 34 there exists an existential formula which is true in $\mathbf{M}_v$ iff condition (84) is satisfied.

We define φ_0 as the conjunction of all of the existential formulas that expresses the various conditions and the formula $b \in \{0, 1\} \wedge B_{s^{c_3}-1} = b$, which can be written in $\mathbf{M}_v$ as $b = \min(\mathbf{1}, b) \wedge \dot{-}(\mathbf{B}, 2^{s^{c_3-1}2^u}) = b$. The formula φ_0 defined this way clearly meets all of our requirements. *Q.E.D.*(Theorem 8)

8 Circuits

In this section we will evaluate algebraic circuits by first-order existential formulas. We consider circuits whose gates are computing the functions of $\mathcal{M}$ in a structure $\mathbf{M}_t$, that is, the circuit evaluates a term μ of $\mathcal{M}$ in the structure $\mathbf{M}_t$.

Both the structure of the circuit computing the value of the term μ and the sequence of its inputs are encoded by elements of $\mathbf{M}_v$, where $v > t$. We show in Lemma 57 that there exists an existential formula φ, which do not depend on anything, and which decides whether an element of $\mathbf{M}_t$ is the output of the circuit, provided that $v > t + c\log(|C_\mu|)$, where C_μ is a circuit computing the value of the term μ, and c is a sufficiently large constant. This result will be used in section 9 where we formulate and prove the "collapsing statement" mentioned in the introduction. In fact the application of Lemma 57 will be the key step in that proof.

To give a rigorous formulation of the mentioned result we have to tell how the circuits computing the values of terms of $\mathcal{M}$ are encoded in $\mathbf{M}_v$. We also have to describe the method of encoding the sequence of inputs for such a circuit. This latter encoding is simpler. If the circuit has k inputs $a_0, ..., a_{k-1} \in \mathbf{M}_t$, then they will be represented by the unique 2^{2^t}-ary natural number whose 2^{2^t}-ary digits are $a_0, ..., a_{k-1}$. This natural number will be denoted by $\mathtt{enc}_{k,t}(a_0, ..., a_{k-1})$, that is, $\mathtt{enc}_{k,t}(a_0, ..., a_{k-1}) = \sum_{i=0}^{k-1} a_i 2^{i2^t}$.

This method of encoding a sequence by a single integer will be used in encoding a circuit. We consider a circuit as a directed acyclic graph with labelings on its vertices and edges which defines the gates and the flow of information in the circuit. The following definition describes the details of the encoding of such a circuit. After that we will describe some basic properties of the defined encoding and then formulate Lemma 57 and sketch of its proof.

Definition. We will always assume that all of the function symbols of $\mathcal{M}$ are $\mathbf{f}_0, ..., \mathbf{f}_{s-1}$. We include a new unary function symbol $\mathtt{id}$ among the function symbols of $\mathcal{M}$ whose interpretation is always the identity function, that is, for all $d \in \omega$, $a \in \mathbf{M}_d$, we have $\mathbf{M}_d \models \mathtt{id}(a) = a$. (This will correspond to a gate whose output is the same as its input which will be useful in circuit constructions.) We define the notion of a $\mathcal{M}$-circuit. (Essentially this will be a finite algebraic circuit whose each gate a is associated with one of the function symbols $\mathbf{f}_i$, say $\mathbf{f}_{i_a}$. If an interpretation $\mathbf{M}_t$ of $\mathcal{M}$ is fixed, then the gate a performs the operation $\mathbf{f}_{i_a}$) in the structure $\mathbf{M}_t$.

Suppose that $m \in \omega$. We will say that C is a $\mathcal{M}$-circuit of size m if C is a vertex-labeled and edge-labeled directed acyclic graph with multiple edges on the set of vertices $m = \{0, 1, \ldots, m-1\}$, satisfying the following conditions:

(i) Each node has either $0, 1$ *or* 2 *incoming edges, the nodes with* 0 *incoming edges will be called the input nodes. (The two incoming edges may have a common tail). The node* $m-1$ *will be called the output node.*

(ii) If a node has two incoming edges then exactly one of them is labeled by 0 *and the other is labeled by* 1*. If a node has a single incoming edge then this edge is labeled by* 0*.*

(iii) Each input node is labeled by the integer s*, and all of the other nodes are labeled by an element of the set* $\{0, 1, \ldots, s-1\}$*, where* s *is the number of function symbols in*

the language $\mathcal{M}$. If the label of the node a is i, where $i \in s$, then the arity of the function symbol $\mathbf{f}_i$ is identical to the number of incoming edges at node a.

(iv) The input nodes form an initial segment of the ordered set $\{0, 1, \ldots, m-1\}$.

We define an evaluation $\chi = \chi_C$ of the $\mathcal{M}$-circuit C in a structure $\mathbf{M}_t$ in the following way. A function g defined on the set of input nodes with values in $\mathbf{M}_t$ will be called an input. If an input g is given we assign an element $\chi^{(g)}(a)$ of $\mathbf{M}_t$ to each node a of the circuit in the following way. If a is an input node then $\chi^{(g)}(a) = g(a)$. Assume now that a is not an input node it is labeled by the integer $j \in s$ and there are two incoming edges at a, say, e_0 labeled by 0 and e_1 labeled by 1. This implies that the arity of $\mathbf{f}_j$ is 2. If e_i starts from the node b_i, for $i = 0, 1$, then we define $\chi^{(g)}(a)$ by $\mathbf{M}_t \models \chi^{(g)}(a) = \mathbf{f}_j(\chi^{(g)}(b_0), \chi^{(g)}(b_1))$. If there is exactly one incoming edge with tail b then the the arity of $\mathbf{f}_j$ is 1 and $\mathbf{M}_t \models \chi^{(g)}(a) = \mathbf{f}_j(\chi^{(g)}(b)))$. Finally, if the are no incoming edges at all then $\mathbf{f}_j$ is a constant symbol and $\mathbf{M}_t \models \chi^{(g)}(a) = \mathbf{f}_j^{(\tau)}$.

Our assumptions imply that, for a given input g, this defines a unique function $\chi^{(g)}$ on the set of nodes of the circuit C. The value of the function $\chi^{(g)}$ at the single output node $m-1$ is called the output of the circuit at input g. The function $\chi^{(g)}$ will be called the evaluation function of the circuit at input g.

For later use we define the depth of an element a of the circuit C as the largest natural number i such that there exists a path of length i starting at an input node and ending in a. Therefore the depth of each input node is 0, and the depths of all other nodes are positive integers. The set of all nodes with depth at most i will be denoted by $\mathtt{Start}_i(C)$. The restriction of the function $\chi^{(g)}$ to the set $\mathtt{Start}_i(C)$ will be denoted by $\chi^{(g,i)}$. If we want to make explicit the dependence of $\chi^{(g,i)}$ on the circuit C, we will write $\chi_C^{(g,i)}$.

Assume that C is a $\mathcal{M}$-circuit of size m. The circuit C is uniquely determined by the following three sequences each of length m:

(i) the sequence $\langle \alpha_{0,0}, \alpha_{0,1}, \ldots, \alpha_{0,m-1} \rangle$, where $\alpha_{0,i} \in m$ is the tail of the incoming edge labeled with 0, whose head is node i, provided that such an incoming edge exists, and $\alpha_{0,i} = i$ otherwise,

(ii) the sequence $\langle \alpha_{1,0}, \alpha_{1,1}, \ldots, \alpha_{1,m-1} \rangle$, where $\alpha_{1,i} \in m$ is the tail of the incoming edge labeled with 1, whose head is node i, provided that such an incoming edge exists, and $\alpha_{1,i} = i$ otherwise,

(iii) the sequence $\langle \alpha_{2,0}, \alpha_{2,1}, \ldots, \alpha_{2,m-1} \rangle$, where $\alpha_{2,i} \in s+1$ is the label of node i.

Our next goal is to encode an $\mathcal{M}$-circuit C of size m with an integer. The encoding will depend also on a parameter $d \in \omega$. So the circuit will be represented by a pair of integers. Suppose that a $d \in \omega$ is fixed with $m < 2^{2^d}$. We also assume that $s + 1 < m$ and therefore $\alpha_{i,j} < m < 2^{2^d}$ for all $i \in 3, j \in m$. For each $i = 0, 1, 2$, we define an integer $\bar{\alpha}_i^{(d)} = \sum_{j=0}^{m-1} \alpha_{i,j} 2^{j 2^d}$. Since $s + 1 < \alpha_{i,j} < m$ for all $i \in 3, j \in m$, we have that for $i = 0, 1, 2$, the integer $\bar{\alpha}_i^{(d)}$ uniquely determines the sequence $\langle \alpha_{i,0}, \ldots, \alpha_{i,m-1} \rangle$. In fact $\alpha_{i,j} = \bar{\alpha}_i^{(d)}[j, d]$ for all $i \in 3$, $j \in m$. We will write $\bar{\alpha}_i^{(d,C)}$ instead of $\bar{\alpha}_i^{(d)}$ if we want to make explicit the dependence of $\bar{\alpha}_i^{(d)}$ on C.

For a given $d \in \omega$ with $m < 2^{2^d}$, we encode the circuit C by a single inte-

ger $\mathtt{circode}_d(C)$ defined by $\mathtt{circode}_d(C) = 2^{2^d}(\sum_{i=0}^{2} \bar{\alpha}_i^{(d)} 2^{im2^d}) + m$. The inequalities $\bar{\alpha}_i^{(d)} < 2^{m2^d}$, $i \in 3$ and $m < 2^{2^d}$ imply that for a fixed language $\mathcal{M}$ and a fixed $d \in \omega$, $\mathtt{circode}_d(C)$ uniquely determines the circuit C. Indeed, m is the least nonnegative residue of $\mathtt{circode}_d(C)$ modulo 2^{2^d}. The $2^{2^{md}}$-ary digits of $\mathtt{circode}_s(C) - m$ give the integers $\bar{\alpha}_i^{(d)}$ for $i = 0, 1, 2$ and these determine the sequence $\alpha_{i,j}$, $i = 0, 1, 2$, $j \in m$.

The number of nodes in an $\mathcal{M}$-circuit C will be denoted by $|C|$. □

Definition. We define two functions $\mathtt{Circ}_0$ and $\mathtt{Circ}_1$ on the set of all $\mathcal{M}$-circuits. If C is an $\mathcal{M}$-circuit and d is the smallest natural number such that $|C| < 2^{2^d}$, then $|C| = d$ and $\mathtt{Circ}_1(C) = \mathtt{circode}_d(C)$. □

The following lemma says that from the integer $\mathtt{circode}_d(C)$ we can get back all of the elements of the circuit C by computing the values of a term τ in a suitably chosen structure $\mathbf{M}_u$.

Lemma 54 *There exist terms $\sigma(x, y), \tau(x, y, z, w), \kappa_i(x, y)$, $i = 0, 1, 2$ of $\mathcal{M}$ such that if $\mathcal{M}$ has s function symbols, $d, u \in \omega$, $d \leq u$, $s < m < 2^{2^d}$ and C is a $\mathcal{M}$-circuit with m nodes then $\mathtt{circode}_d(C) \in \mathbf{M}_u$ implies that $\mathbf{M}_u \models m = \sigma(\mathtt{circode}_d(C), d)$ and also implies that for all $i \in 3$, $j \in m$,*

$$\mathbf{M}_u \models \alpha_{i,j} = \tau(\mathtt{circode}_d(C), d, i, j) \wedge \bar{\alpha}_i^{(d,C)} = \kappa_i(\mathtt{circode}_d(C), d)$$

where the integers $\alpha_{i,j}$ are defined in the definition of $\mathtt{circode}_d(C)$. Moreover

$$|C| = \mathtt{circode}_d(C) - 2^{2^d} \lfloor \mathtt{circode}(C)/2^{2^d} \rfloor$$

Proof of Lemma 54. Clearly m is the least nonnegative residue of $\mathtt{circode}_d(C)$ modulo 2^{2^d} and so $m = \mathtt{circode}_d(C) - 2^{2^d} \lfloor \mathtt{circode}(C)/2^{2^d} \rfloor$. We also have $\bar{\alpha}_i^{(d)} = (\lfloor \mathtt{circode}_d(C)/2^{2^d} \rfloor)[i, d]$ for $i \in 3$. Therefore using Lemma 8 and the fact that $\alpha_{i,j} = \bar{\alpha}_i^{(d)}[j, d]$ for all $i \in 3$, $j \in m$ we get the term τ. *Q.E.D.*(Lemma 54)

Definition. If the number of input nodes of an $\mathcal{M}$-circuit C is k then we will say that C is a k-ary circuit. Assume that g is an input of the k-ary $\mathcal{M}$-circuit C evaluated according to the interpretation $\mathbf{M}_t$ of $\mathcal{M}$. By the definition of an input this means that g is a function with values in $\mathbf{M}_t$, and defined on the set of input nodes, that is, on the set k. In this case to express the fact that the output of the circuit C at input g is a we will write $\mathbf{M}_t \models a = C(g)$ or $\mathbf{M}_t \models a = C(g(0), \ldots, g(k-1))$.

Suppose that we evaluate the $\mathcal{M}$-circuit C in a structure $\mathbf{M}_t$. We will encode an input sequence $\langle g(0), \ldots, g(k-1) \rangle$ by the integer $\mathtt{enc}_{k,t}(g(0), \ldots, g(k-1)) = \sum_{i=0}^{k-1} 2^{i2^t} g(i)$. This number will be called an encoded input of the $\mathcal{M}$-circuit C with respect to the interpretation τ of $\mathcal{M}$. Clearly, for a given $\mathcal{M}$-circuit C, and a given interpretation $\mathbf{M}_t$ of $\mathcal{M}$, the encoded input uniquely determines the corresponding input sequence g. (This is a consequence of the fact that the length of the input k is uniquely determined by the circuit C, while the integer t is uniquely determined by the structure $\mathbf{M}_t$.) □

Lemma 55 *For all sufficiently large $m \in \omega$ if $t \in \omega$, if $t \in \omega$, $m < 2^{2^t}$, and C is a $\mathcal{M}$-circuit of size m, then $\mathtt{circode}_t(C) < m + 2^{(3m+1)2^t}$.*

Proof of Lemma 55. This is an immediate consequence of the definition of $\mathtt{circode}_t(C)$. *Q.E.D.*(55)

Definition. Suppose now that $k \in \omega$, $k \geq 1$ and $\tau(x_0, \ldots, x_{k-1})$ is a term of $\mathcal{M}$, where we allow that some of the variables x_i does not occur in τ (but all of the variables of τ is from the set $\{x_0, ..., x_{k-1}\}$). In this definition we will consider all of variables $x_0, ..., x_{k-1}$ as subterms of $\tau(x_0, \ldots, x_{k-1})$, even those variables which do not actually occur in τ. (For example, if $\tau(x_0, x_1)$ is the term x_0 then x_1 is a subterm of $\tau(x_0, x_1)$.) We construct an $\mathcal{M}$-circuit of C_τ based on τ. Let $\sigma = \langle \sigma_0, \ldots, \sigma_{m-1} \rangle$ be a sequence which consists of all of the pairwise distinct subterms of $\tau(x_0, \ldots, x_{k-1})$. A subterm with several occurrences in τ is represented only once in the sequence σ. We also assume that σ_{m-1} is the term τ, and for all $i \in k$, σ_i is the term x_i. The set of nodes of the circuit C_τ will be m, the label of each node $i \in m$ will be j if the outmost $\mathcal{M}$-operation of the term σ_i is $\mathbf{f}_j$. If such an operation does not exists, that is, τ is a variable then the label is s. The edges of C are defined in the following way. If i is labeled by j then we distinguish three cases according to the arity of the function symbol $\mathbf{f}_j$. If $\mathbf{f}_j$ is a binary function symbol and $\tau_i = \mathbf{f}_j(\tau_{i'}, \tau_{i''})$, then an edge labeled with 0 points from i' to i, and an edge labeled by 1 points from i'' to i. If $\mathbf{f}_j$ is a unary function symbol and $\tau_i = \mathbf{f}_j(\tau_{i'})$, then an edge points from i' to i, and it is labeled by 1. Finally if $\mathbf{f}_j$ is a constant symbol and $\tau_i = \mathbf{f}_j$ then are no edges ending at i.

The circuit C_τ will be called the circuit associated with the term τ. The size of the circuit C_τ, that is, m will be called the circuit size of τ and will be denoted by $\mathtt{csize}(\tau)$.

In this definition the order of the subterms in the sequence $\langle \sigma_0, ..., \sigma_{m-1} \rangle$ was arbitrary apart from the choices of $\sigma_0, ..., \sigma_{k-1}$ and σ_{m-1}. Therefore the circuit C_τ depends on an arbitrary choice in the definition. This choice however is important only for the order of the nodes.

The fact the we considered each x_i, $i \in k$ as a subterm of $\tau(x_0, ..., x_{k-1})$ implies that that the circuit C_τ has exactly k input nodes even if in the evaluation of the circuit C_τ the input provided at some of the nodes is not used.

We define the followng functions on the set of all $\mathcal{M}$-terms: $\mathtt{Circ}_0(\tau) = \mathtt{Circ}_0(C_\tau)$, $\mathtt{Circ}_1(\tau) = \mathtt{Circ}_1(C_\tau)$ and for all $d \in \omega$, $\mathtt{circode}_d(\tau) = \mathtt{circode}_d(C_\tau)$.

Suppose that C is an $\mathcal{M}$-circuit with k input nodes, and $\mu(x_0, ..., x_{k-1})$ is a term of $\mathcal{M}$. We say that the circuit C computes the term $\mathcal{M}$ iff for all $d \in \omega$, and for all $a_0, ..., a_{k-1} \in \mathbf{M}_d$ we have $\mathbf{M}_d \models \mu(a_0, ..., a_{k-1}) = C(a_0, ..., a_{k-1})$. □

In the next lemma logarithm means logarithm of base two.

Lemma 56 *Assume that C is an $\mathcal{M}$-circuit. Then*

$$\log\log|C| - 1 \leq \mathtt{Circ}_0(C) \leq \log\log|C|$$

and

$$\mathtt{Circ}_1(C) \leq |C|^{8|C|}$$

Proof of Lemma 56. By its definition $\mathtt{Circ}_0(C)$ is the smallest natural number d with $|C| < 2^{2^d}$. This implies the bounds on $\mathtt{Circ}_0(C)$. According to Lemma 55, if $\mathtt{Circ}_0(C) = t$

then $\mathtt{Circ}_1(C) = \mathtt{circode}_t(C) \leq |C| + 2^{(3|C|+1)2^t}$. Using the already proven upper bound on $t = \mathtt{Circ}_0(C)$ we get the claimed inequality. *Q.E.D.*(Lemma 56).

Lemma 57 *There exists an existential formula $\varphi(x_0, ..., x_4)$ of $\mathcal{M}$ with the following property. For all sufficiently large $c \in \omega$, for all $\mathcal{M}$-circuits C, and for all $t, v \in \omega$, if the number of inputs of C is k and $v > t + c \log |C|$ then for all $a_0, \ldots, a_k, b \in \mathbf{M}_t$, we have that $\mathtt{Circ}_0(C) \in \mathbf{M}_v$, $\mathtt{Circ}_1(C) \in \mathbf{M}_v$, $\mathtt{enc}_{k,t}(a_0, \ldots, a_{k-1}) = \sum_{i=0}^{k-1} a_i 2^{i2^t} \in \mathbf{M}_v$, and*

$$\mathbf{M}_t \models C(a_0, \ldots, a_{k-1}) = b \quad \leftrightarrow \quad \mathbf{M}_v \models \varphi(\mathtt{enc}_{k,t}(a_0, \ldots, a_{k-1}), b, t, \mathtt{Circ}_0(C), \mathtt{Circ}_1(C))$$

Proof of Lemma 57. Let $F = \langle F_{d,t} \mid d, t \in \nabla \rangle$ be the family of quaternary functions defined on $\mathbf{M}_d$ in the following way. Assume that $d, t \in \omega$, $d \geq t$, and $w, b, C_1, C_2 \in \mathbf{M}_d$. Then $F_{d,t}(w, b, C_0, C_1) \in \{0, 1\}$, and $F_{d,t}(w, b, C_0, C_1) = 1$ iff the following three conditions are satisfied:

(85) *there exists an $\mathcal{M}$-circuit C such that $d \geq \max(C_0, t)$, $\mathtt{Circ}_0(C) = C_0$, $\mathtt{Circ}_1(C) = C_1$, $2^{d-t} > |C|$,*

(86) *if condition* (85) holds and k is the number of input nodes of C, then there exists a sequence $a_0, ..., a_{k-1} \in \mathbf{M}_t$ such that $w = \mathtt{enc}_{k,t}(a_0, ..., a_{k-1}) = w$,

(87) *if both conditions* (85), (86) hold then $\mathbf{M}_t \models C(a_0, ..., a_{k-1}) = b$.

We claim that the family of functions F is polynomial time computable with respect to $\mathbf{M}$. Let $\gamma_1 \in \omega$ be a sufficiently large constant. We will show that there exists a program P such that the following statement, needed for polynomial time computability with respect to $\mathbf{M}$, is true (note that the variable k of that definition has the value 4 now):

(88) *for all sufficiently large $d \in \omega$, for all $t \in \omega$ with $d \geq t$, and for all $w, b, C_0, C_1 \in \mathbf{M}_d$, the following holds. The machine N_m (a RAM with word length m), where $m = 2^d$, with program P and input $4, d, t, w, b, C_0, C_1$, using only the first $2^{\gamma_1(d-t)}$ memory cells in time $2^{\gamma_1(d-t)}$ computes $F_{d,t}(w, b, C_0, C_1)$.*

First assume that there exists a circuit C satisfying conditions (85) and (86). Then the assumption $2^{d-t} > |C|$ implies that machine N_m can determine the underlying directed graph of C, and the labellings of its nodes and edges in time polynomial in 2^{d-t}. The assumption $m = 2^d$ implies that each $\mathcal{M}$-operation in $\mathbf{M}_t$ can be performed in constant time on N_m and since the number of nodes of C is at most 2^{d-t}, P can determine the integers $a_i \in \mathbf{M}_t$, $i \in k$ and can evaluate the circuit C time polynomial in 2^{d-t}, and comparing the output to b can determine the value of $F_{d,t}(w, b, C_0, C_1)$ in polynomial time.

The same computation can be performed also by P on an arbitrary input. If the construction of the graph of C does not terminate in time, or the result contradicts to conditions (85), or (86) then the value of $F_{d,t}$ is 0, otherwise the machine gets the value

of $F_{d,t}$ as described above. This completes the proof of the fact that the family F is polynomial time computable with respect to $\mathbf{M}$.

Theorem 8 implies that the family F is polynomially existential, that is, there exists a there exists a $c_0 \in \omega$ and an existential formula φ of $\mathcal{M}$ such that

(89) *for all* $d, t \in \omega$ *with* $d \geq t$ *and for all* $w, b, C_0, C_1 \in \mathbf{M}_d$ *and for all* $v \geq t + c_0(d-t)$ *we have* $F_{d,t}(w, b, C_0, C_1) = 1$ *iff* $\mathbf{M}_v \models \varphi(w, b, C_0, C_1, d, t)$.

We define an existential formula $\psi(x_0, x_1, y_0, y_1, w)$ of $\mathcal{M}$ by

$$\psi(x_0, x_1, y_0, y_1, w) \equiv \varphi(x_0, x_1, y_0, y_1, w + c_2\mathbf{p}(y_0), w)$$

where c_2 is a sufficiently large constant. (The meaning of the expression $w+c_2\mathbf{p}(y_0)$ is that we want to define d, in order to choose a member $F_{d,t}$ of the family F, by $d = t + c_2 2^{C_0}$.)

Assume now that $t \in \omega$, C is an $\mathcal{M}$-circuit, with k inputs, $a_0, ..., a_{k-1}, b \in \mathbf{M}_t$, $\mathtt{enc}_{k,t}(a_0, ..., a_{k-1}) = w$, and let c_1 be sufficiently large with respect to c_0. We claim that for all $v > t + c_1 \log |C|$, $\mathbf{M}_t \models C(a_0, ..., a_{k-1}) = b$ iff $\mathbf{M}_v \models \psi(w, b, C_0, C_1, t)$.

Let $d = t + c_2 2^{C_0}$. First we show that $w, b, C_0, C_1 \in \mathbf{M}_d$. By the definition of the function $\mathtt{enc}_{k,t}$ we have $w \leq 2^{|C|2^t}$, therefore it is sufficient to show that $|C|2^t < 2^d$, or equivalently $\log |C| + t < d$. By Lemma 56 $\frac{1}{2} \log |C| \leq 2^{C_0}$, and so the definition of d implies the claimed inequality.

Since $b \in \mathbf{M}_t$ and $t \leq d$ we have $b \in \mathbf{M}_t$. $C_0 \leq d$ and so $C_0 \in \mathbf{M}_d$. Finally by Lemma 56 $C_1 < |C|^{8|C|}$, therefore it is sufficient to show that $\log\log(|C|^{8|C|}) < d$. We have $\log\log(|C|^{8|C|}) = 3 + \log |C| + \log\log |C|$. According Lemma 56 $\log |C| \leq 2^{C_0+1}$ so if c_2 is a sufficiently large constant then $C_1 \in \mathbf{M}_d$.

Since $w, b, C_0, C_1 \in \mathbf{M}_d$, the definition of the function $F_{d,t}$ implies that $\mathbf{M}_t \models C(a_0, ..., a_{k-1}) = b$ iff $F_{d,t}(w, b, C_0, C_1) = 1$

Condition (89) implies that if $v \geq t + c_0(d-t)$ then $\mathbf{M}_t \models C(a_0, ..., a_{k-1}) = b$ iff $\mathbf{M}_v \models \varphi(w, b, C_0, C_1, d, t)$ which is equivalent to $\mathbf{M}_v \models \psi(w, b, C_0, C_1, t)$.

This is true if $v \geq t + c_0(d-t)$. Assume now that we know only that $v > t + c \log |C|$, as required in the present lemma, where $c \in \omega$ is sufficiently large with respect to c_0 and c_2. We have that $d - t = c_2 2^{C_0}$, and so by Lemma 56 $d - t \leq c_2 \log |C|$ and therefore $t+c_0(d-t) \leq t+c \log |C|$ and consequently for all $v \geq t+c \log |C|$, $\mathbf{M}_t \models C(a_0, ..., a_{k-1}) = b$ iff $\mathbf{M}_v \models \psi(w, b, C_0, C_1, t)$. *Q.E.D.*(Lemma 57)

9 Collapsing and Predictivity

Notation. In this section log will always mean logarithm with base 2 unless we explicitly state it otherwise.

9.1 Expressing the truth value with terms

This section contains the "collapsing" argument. We show that if Theorem 3 is not true then the hierarchy of first-order formulas of $\mathcal{M}$, interpreted in the structures $\mathbf{M}_d$, collapses in a quantitative sense. For each $d \in \omega$ we define a class of first-order formulas Θ_d by giving some bounds on the number of their quantifiers, which may depend on d. We also define a function $\mathbf{g}$ on Θ_d with values in $\mathbf{M}_d$, and a term τ of $\mathcal{M}$ with an upper bound on its size, also depending on d, such that if q is about $d + \log d$, then for each formula $\varphi \in \Theta_d$ and for each $xa \in \mathbf{M}_d$ we have

$$\mathbf{M}_d \models \varphi(a) \leftrightarrow \mathbf{M}_q \models \tau(a, \mathbf{g}(\varphi)) = \mathbf{0}$$

That is, our indirect assumption implies that we are able to express the truth value of a not too large first-order formula in $\mathbf{M}_d$ as the value of a term in $\mathbf{M}_q$, where q is not very much larger then d. This will lead, in the following sections, to the final diagonalization argument after we also prove the "simulation statement ", namely, that each not too large term in $\mathbf{M}_q$ can be evaluated by a first-order formula ψ in $\mathbf{M}_d$, moreover these formulas can be chosen from the class Θ_d.

The situation will be slightly more complicated than the picture given in the preceding, paragraphs, since the class Θ_d will depend on other parameters as well, which will make it easier to choose the first-order formula mentioned above in a way that it meets all of our requirements.

We give now a rigorous formulation of the collapsing statement as outlined above and then we will sketch its proof.

Definition. 1. Suppose that $\varphi(x_0, \dots, x_{k-1}) = Q_0 x_0, \dots, Q_{k-1} x_{k-1}, P(x_0, \dots, x_{k-1})$ is a first-order prefix formula of $\mathcal{M}$, where $P(x_0, \dots, x_{k-1})$ is a propositional formula and Q_i, $i \in k$ are quantifiers. In this section if we say that φ is a prefix formula of $\mathcal{M}$ we will always assume, unless we explicitly state it otherwise, that $P(x_0, \dots, x_{k-1})$ is of the form $t(x_0, \dots, x_{k-1}) = \mathbf{0}$, where t is a term. (It is easy to see that there exists a $c > 0$, such that for each $k \in \omega$, and for each propositional formula $P(x_0, \dots, x_{k-1})$, there exists a term $t(x_0, \dots, x_{k-1})$ such that $\mathtt{length}(t) \leq c\mathtt{length}(P)$, and for all $d \in \omega$, and for all $a_0, \dots a_{,k-1} \in \mathbf{M}_d$, $\mathbf{M}_d \models P(x_0, \dots, x_{k-1}) \leftrightarrow t(x_0, \dots, x_{k-1}) = \mathbf{0}$.) Suppose that $\varphi(x_0, \dots, x_{k-1}) \equiv Q_0 x_0, \dots, Q_{k-1} x_{k-1}, t(x_0, \dots, x_{k-1}) = \mathbf{0}$. Then $\mathtt{term}(\varphi)$ will denote the term $t(x_0, \dots, x_{k-1})$.

2. If $\varphi(x_0, \dots, x_{k-1}) \equiv Q_0 x_0, \dots, Q_{k-1} x_{k-1}, t(x_0, \dots, x_{k-1}) = \mathbf{0}$ is a first-order formula of $\mathcal{M}$, then the $\mathcal{M}$-circuit C_t associated with the term t will be also denoted by C_φ. □

Definition. Assume that $\mathcal{L}$ is a first-order language and $\mathcal{L}'$ is the second-order extension of $\mathcal{L}$. The set of all second-order formulas Ψ of $\mathcal{L}'$ which satisfies the following conditions will be denoted by $\mathtt{SForm}(\mathcal{L})$:

(i) Ψ does not contain second-order quantifiers.

(ii) the only second-order variables that may be contained in Ψ are variables for k-ary relations for some $k \in \omega$. (Such a variable represents a k-ary relation between the elements of the universe.)

Usually we will write such a formula Ψ in the form of $\Psi(x_0, \ldots, x_{k-1}, Y_0, \ldots, Y_{l-1})$ where $x_0, \ldots, x_{k-1}$ are all of the first-order variables contained in Ψ, and $Y_0, \ldots, Y_{l-1}$ are all of the second-order variables contained in Ψ. According to our definition the variables $x_0, \ldots, x_{k-1}$ represent elements of the universe and the variables $Y_0, \ldots, Y_{l-1}$ represent $k_0, \ldots, k_{l-1}$-ary relations on the universe. □

We formulate below a statement that we will call the $\mathcal{D}$-quantifier elimination assumption, where $\mathcal{D}$ can be a real-valued function defined on ω. In the case $\mathcal{D}(x) = \varepsilon(\log x)^{\frac{1}{2}}$ the $\mathcal{D}$-quantifier elimination assumption follows from the assumption that Theorem 3 is not true.

Definition. 1. Assume that $\mathcal{D}$ is a function. The conjunction of the following two conditions will be called the $\mathcal{D}$-quantifier elimination assumption for $\mathbf{M}$ or shortly $\mathcal{D}$-elimination assumption:

(90) *$\mathcal{D}$ is a monotone increasing function defined on an interval $[r, \infty)$ of the real numbers with positive real values for a suitably chosen $r \geq 0$,*

(91) *for all propositional formulas $P(x, y)$ of $\mathcal{M}$ and for all sufficiently large $d \in \omega$, there exists a term τ of $\mathcal{M}$, such that $\mathtt{depth}(\tau) \leq \mathcal{D}(d)$, and for all $a \in \mathbf{M}_d$, $\mathbf{M}_d \models \exists x, P(x, a)$ iff $\mathbf{M}_d \models \tau(a) = \mathbf{0}$.* □

Definition. Suppose that φ is a prenex first-order formula of $\mathcal{M}$. The total number of quantifiers, both existential and universal in φ will be denoted by $\mathtt{quant}(\varphi)$.□

Notation. In a first-order formula if a sequence of quantifiers of the same type occurs for example $\exists z_0, \ldots, \exists z_{k-1}$ then, sometimes, we will abbreviate it by writing $\exists \vec{z}$, where $\vec{z}$ is the sequence of variables $z_0, \ldots, z_{k-1}$.

Definition. Assume that φ is a first-order prenex formula of $\mathcal{M}$, and $\langle j_m, ..., j_1 \rangle$ is a sequence of positive integers. We will say that the quantifier pattern of φ is $\langle j_m, ..., j_1 \rangle$ if the following conditions are satisfied.

(92) *$\varphi \equiv Q_m \vec{x}_m, \ldots, Q_1 \vec{x}_1, P(\vec{x}_1, \ldots, \vec{x}_m)$, $\vec{x}_i$ is a sequence $x_{i,0}, \ldots, x_{i,j_i-1}$ of variables of $\mathcal{M}$, and Q_i is a quantifier binding the variables in $\vec{x}_i$.*

(93) *There exists a $\delta \in \{0, 1\}$ such that, for each for $i = 1, ..., m$, Q_i is universal iff $i \equiv \delta \pmod 2$.*

We will refer to the expression $Q_i \vec{x}_i$ in the formula φ as a block or as a block of quantifiers. We define the notion of quantifier pattern in the same way for prenex formulas

in $\mathtt{SForm}(\mathcal{M})$ as well. Since these formulas contain only first-order quantification the definition remains unchanged. □

Remark. We write in the quantifier pattern $\langle j_m, \ldots, j_1 \rangle$ the elements of the sequence $j_1, ..., j_m$ in reverse order since we will have an inductive proof about formulas with a given quantifier pattern which starts with eliminating the innermost block of quantifiers. This will simplify the notation in the inductive proof.

Definition. Assume that $M, j_1, \ldots, j_m$ are positive integers. $\mathtt{Form}(M, j_m, \ldots, j_1)$ denotes the set of all prenex first-order formulas φ of $\mathcal{M}$ such that $\mathtt{csize}(\varphi) \leq M$ and the quantifier pattern of φ is $\langle j_m, \ldots, j_1 \rangle$. □

The main result of section 9.1 is the following Lemma 58 which is the "collapsing" statement. The remaining part of this section contains the proof of Lemma 58.

Lemma 58 *For all $c \in \omega \backslash \{0\}$, if $\varepsilon > 0$ is sufficiently small with respect c then the following holds. Assume that*

(94) *the $\mathcal{D}$-quantifier elimination assumption holds for $\mathbf{M}$, where $\mathcal{D}(x) = \varepsilon(\log x)^{\frac{1}{2}}$,*

(95) *$d \in \omega$ is sufficiently large with respect to ε,*

(96) *$\delta = \lfloor \mathcal{D}(d + \log d) \rfloor = \lfloor \varepsilon(\log(d + \log d))^{\frac{1}{2}} \rfloor$, $m \in \omega$, $m \leq c\delta$, and $\iota_m, ..., \iota_1$ are positive integers with $\iota_m + \ldots + \iota_1 \leq c^\delta$, $\iota_m \leq c\delta$.*

Then there exists a function $\mathbf{g}$ which assigns to each prenex formula

$$\varphi \in \mathtt{Form}(c^\delta, \iota_m, \ldots, \iota_1)$$

a natural number $\mathbf{g}(\varphi) < 2^{2^{d-1}}$, and there exists a term $\tau(x, y)$ of $\mathcal{M}$ such that the following conditions are satisfied:

(97) $\mathtt{csize}(\tau) \leq 3 \cdot 2^{d + \log d}$

(98) *for each prenex formula $\varphi \in \mathtt{Form}(c^\delta, \iota_m, \ldots, \iota_1)$ and for each $a \in \mathbf{M}_d$, if $q = d + m\lfloor \frac{\log d}{m} \rfloor$ then*

$$\mathbf{M}_d \models \varphi(a) \ \leftrightarrow \ \mathbf{M}_q \models \tau(a, \mathbf{g}(\varphi)) = \mathbf{0}$$

Remark. The function $\mathbf{g}$ plays the role of Gödel numbering in our proof. Apart from the upper bound given in the Lemma we do not need □

Sketch of the proof of Lemma 58. The $\mathcal{D}$-quantifier elimination says that for each first-order formula $\exists x, P(x, y)$, of $\mathcal{M}$, where P is propositional, and for each $d \in \omega$, there exists a τ with $\mathtt{depth}(\tau) < d$ such that for all $a \in \mathbf{M}_d$, $\mathbf{M}_d \models \exists x, P(x, y)$ iff $\mathbf{M}_d \models \tau(a) = \mathbf{0}$. In in Lemma 58 instead of the formula $\exists x, P(x, y) = 0$ which does not depend on d we have an arbitrary first-order formula φ whose size may grow with d. We reach a similar conclusion, namely $\mathbf{M}_d \models \varphi(a) \ \leftrightarrow \ \mathbf{M}_q \models \tau(a, \mathbf{g}(\varphi)) = \mathbf{0}$. It will help in finding such a

term τ that, (a) the structure $\mathbf{M}_q$ is may be somewhat larger than $\mathbf{M}_d$, and (b) τ may contain a parameter $\mathbf{g}(\varphi)$ which encodes the formula φ by an integer in $\mathbf{M}_d$.

The structure of the proof is the following. First we try to eliminate the innermost block of quantifiers in $\varphi \equiv Q_m\vec{x}_m, \ldots, Q_1\vec{x}_1, P(\vec{x}_1, \ldots, \vec{x}_m)$, namely the block $Q_1\vec{x}_1$. We may assume without the loss of generality that Q_1 is existential (otherwise we work with formula $\neg\varphi$). We want to accomplish the quantifier elimination by using the $\mathcal{D}$-elimination assumption. We consider the formula without the other quantifiers namely the formula $\psi \equiv \exists\vec{x}_1, P(\vec{x}_1, \vec{x}_2, \ldots, \vec{x}_m)$. Here the $\vec{x}_2, \ldots, \vec{x}_m$ are free variables their role is the same that the role of the variable y in the formula $\exists x, P(x, y)$. If we can show that ψ is equivalent to a propositional formula $\tau(\vec{x}_2, \ldots, \vec{x}_m) = 0$, in the sense that they are equivalent for all choices of the values of the variables $\vec{x}_2, \ldots, \vec{x}_m$, then we may replace the original formula φ by the simpler formula $Q_m\vec{x}_m, \ldots, Q_2\vec{x}_2, \tau(\vec{x}_2, \ldots, \vec{x}_m) = \mathbf{0}$ and continue the elimination with the next block of quantifiers.

As a first step we consider only the elimination of the first block of quantifiers $Q_1\vec{x}_1$. There are three problems that prevents us from using directly the $\mathcal{D}$-uantifier elimination assumption.

(i) In the $\mathcal{D}$-elimination assumption there is only one parameter the variable y in the formula $P(x, y)$, while we now we have all of the variables $\vec{x}_2, \ldots, \vec{x}_m$

(ii) In the $\mathcal{D}$-elimination assumption there is only one existential quantifier, the quantifier $\exists x$, while now we have the whole block $\exists\vec{x}_1$, where the number of variables may even depend on d.

(iii) In the $\mathcal{D}$-elimination assumption the propositional formula $P(x, y)$ does not depend on d while now $P(\vec{x}_1, \ldots, \vec{x}_m)$ may depend on d

What may help in overcoming the problems caused by this changes is that the assumptions of the lemma imply upper bounds on the number of parameters, the number of existential qauntifiers, and the size of the formula P. These upper bounds are in condition (96) and in the assumption $\varphi \in \mathtt{Form}(c^\delta, \iota_m, ..., \iota_1)$.

We will be able to reduce all of the numbers mentioned in problems (i),(ii), and (iii) to one (the value needed in the $\mathcal{D}$-elimination assumption) by considering the formula φ not in the structure $\mathbf{M}_d$ but in a larger structure $\mathbf{M}_v$. In such a larger structure $\mathbf{M}_v$ we may encode a sequence of elements of $\mathbf{M}_d$ by a single integer of $\mathbf{M}_v$. (The same way as it was done in [2].) This encoding will solve problem (i) and problem (ii). For the solution of problem (iii) we use Lemma 57 about the evaluation of circuits with existential formulas. The propositional formula $P(\vec{x}_1, \ldots, \vec{x}_m)$ can be written in the form of $\xi(\vec{x}_1, \ldots, \vec{x}_m) = \mathbf{0}$, where ξ is a term of $\mathcal{M}$. We may consider the algebraic circuit corresponding to ξ. As Lemma 57 states, this circuit defined over $\mathbf{M}_v$, can be evaluated by a first-order formula in a structure $\mathbf{M}_{v'}$, where $v' > v$, provided that its input is encoded by a single integer, and the circuit itself is also encoded by two integers. Lemma 57 also gives an upper bound v'.

This way we will be able to substitute the propositional formula P in problem (iii) by an existential formula of constant size. (See Lemma 59 later in this section.) The new existential quantifiers can be merged by the already existing existential quantifiers mentioned in problem (i) and all of them can be reduced to a single quantifier by going

to a larger structure.

This quantifier elimination that we described for the first block of quantifiers, can be recursively repeated and gradually eliminate all of the quantifiers while we have to evaluate the formulas in larger and larger structures. Later we will sketch further details of the proof as we are getting to the definitions and lemmas which describe the specific parts of the proof. *End of Sketch*

Definition. Let τ be a term of $\mathcal{M}$. We will say that τ is a $0,1$-term if for all $d \in \omega$ and for all $a \in a$ we have $\mathbf{M}_d \models \tau(a) = \mathbf{0} \vee \tau(a) = \mathbf{1}$ $\square$

In the following definition, starting with a formula $\varphi \equiv Q_m \vec{x}_m, \ldots, Q_1 \vec{x}_1, P(\vec{x}_1, \ldots, \vec{x}_m, x)$ that we have at the beginning of the inductive proof of Lemma 58, we describe the sequence of formulas that we derive from φ as we eliminate its blocks of quantifiers one-by-one.

Definition. Assume that $m \in \omega \backslash \{0,1\}$, $j_m, \ldots, j_1$ are positive integers, $\vec{x}_i$ is the sequence of variables $x_{i,0}, \ldots, x_{i,j_i}$ of $\mathcal{M}$, and φ is a first-order prenex formula of $\mathcal{M}$, $\varphi \equiv Q_m \vec{x}_m, \ldots, Q_1 \vec{x}_1, P(\vec{x}_1, \ldots, \vec{x}_m, x)$, with quantifier pattern $\langle j_m, \ldots, j_1 \rangle$, where P is a propositional formula of $\mathcal{M}$, moreover Q_i is the universal quantifier for all even $i \in \{1, \ldots, m\}$, and Q_i is the existential quantifier for all odd $i \in \{1, \ldots, m\}$.

We define a sequence of formulas φ_i of $\mathcal{M}$ for $i = 0, 1, \ldots, m$, by recursion on i. The free variables of the formula φ_i will be $\vec{x}_{i+1}, \ldots, \vec{x}_m, x$. For $i = 0$, $\varphi_0(\vec{x}_1, \ldots, \vec{x}_m, x) \equiv \neg P(\vec{x}_1, \ldots, \vec{x}_m, x)$. Assume that $\varphi_{i-1}(\vec{x}_i, \ldots, \vec{x}_m, x)$ has been already defined for some $i = 1, \ldots, m$. Then φ_i is defined by $\varphi_i(\vec{x}_{i+1}, \ldots, \vec{x}_m, x) \equiv \exists \vec{x}_i, \neg \varphi_{i-1}(\vec{x}_i, \vec{x}_{i+1}, \ldots, \vec{x}_m, x)$. The formula φ_i defined this way will be called the ith segment of the formula φ.

Clearly if m is odd then $\varphi_m \equiv \varphi$, and if m is even, then $\varphi_m \equiv \neg\varphi$. (We get this by replacing the quantifiers $\forall \vec{x}_i, (\ldots)$ in the definition of φ by $\neg\exists \vec{x}_i, \neg(\ldots)$ for all even $i \in [1, m]$.) $\square$

Definition. Suppose that $\mathcal{D}$ is a function so that the $\mathcal{D}$-quantifier elimination assumption holds for $\mathbf{M}$. Then $\mathcal{S} = \mathcal{S}_{\mathcal{D}}$ will denote the function $2^{\mathcal{D}}$. $\square$

Remark. The functions $\mathcal{S}_{\mathcal{D}}$ will be useful for us since for every term τ of $\mathcal{M}$ if $\mathtt{depth}(\tau) \leq \mathcal{D}(d)$ for some $d \in \omega$, then $\mathtt{csize}(\tau) \leq 2\mathcal{S}_{\mathcal{D}}(d)$. This is a consequence of the fact that the arities of the function symbols of $\mathcal{M}$ are at most two. $\square$

The following Lemma 59 solves the problems (i), (ii), and (iii) mentioned in the sketch of the proof of Lemma 58. (The remaining problem, reducing the number of existential quantifiers from a constant to one, will be solved Lemma 61.) Lemma 59 will be used in the inductive proof of Lemma 58. Applying Lemma 59 we will be able to eliminate a block of quantifiers in the inductive step.

Lemma 59 *For all sufficiently large $c \in \omega$ the following holds. Assume that*

(99) *$\mathcal{D}$ is a function and the $\mathcal{D}$-quantifier elimination assumption holds,*

(100) *ψ is an existential formula of $\mathcal{M}$ of the form*

$$\psi \equiv \exists x_0, \ldots, x_{k-1}, \xi(x_0, \ldots, x_{k-1}, y_0, \ldots, y_{l-1}) = \mathbf{0}$$

where ξ is a $0,1$-term of $\mathcal{M}$,

(101) *$r, v \in \omega$ and $v \geq r + c\lceil \log(\mathtt{csize}(\xi)) \rceil$.*

Then there exists a $0,1$-term $\eta(x_0, \dots, x_{l-1}, w_0, w_1, w_2)$ of $\mathcal{M}$ such that the following conditions are satisfied:

(102) $\mathtt{csize}(\eta) \leq 2^{\mathcal{D}(v)} + c(k+l)$

(103) *for all $a_0, \dots, a_{l-1} \in \mathbf{M}_r$,*

$$\mathbf{M}_r \models \psi(a_0, \dots, a_{l-1}) \quad \leftrightarrow \quad \mathbf{M}_v \models \eta(a_0, \dots, a_{l-1}, \mathtt{Circ}_0(\xi), \mathtt{Circ}_1(\xi), r) = \mathbf{0}$$

We will prove the lemma in three steps. First, in Lemma 60 instead of the propositional statement $\eta = \mathbf{0}$ we will have an existential statement of constant size, but with possibly more than one existential quantifiers. In lemma 61 we reduce the number of existential quantifiers to one. Then, using the $\mathcal{D}$-quantifier elimination assumption, we complete the proof of Lemma 59.

Proof of Lemma 59. Assume that $\mathcal{D}$, are fixed satisfying condition (99) of the lemma. Sometimes we will write $\mathcal{S}(x)$ instead of $2^{\mathcal{D}(x)}$. As a first step we prove the following Lemma 60 (without the assumption of $\mathcal{D}$ quantifier elimination). In this lemma is a similar statement to Lemma 59 but now we express the truth value of $\mathbf{M}_r \models \psi$, not by a term η in $\mathbf{M}_v$ but by constant size first-order existential formula φ in $\mathbf{M}_v$. So we are saying less because because φ has quantifiers, but at the same time also saying more since φ is of constant size.

Lemma 60 *There exists an existential first-order formula $\varphi(x_0, \dots, x_5)$ of $\mathcal{M}$ such that for all sufficiently large $c_1 > 0$ and for all integers k, l, for all formulas ψ and terms ξ of $\mathcal{M}$ satisfying condition* (100) of Lemma, 59, and for all $r, v' \in \omega$ with $v' \geq r + c_1\lceil \log(\mathtt{csize}(\xi)) \rceil$, we have

(104) *for all $a_0, \dots, a_{l-1} \in \mathbf{M}_r$,*

$$\mathbf{M}_r \models \psi(a_0, \dots, a_{l-1}) \quad \leftrightarrow \quad \mathbf{M}_{v'} \models \varphi(A, r, \mathtt{Circ}_0(\xi), \mathtt{Circ}_1(\xi), k, l)$$

where $A = \mathtt{enc}_{l,r}(a_0, \dots, a_{l-1})$.

Remark. The important point in this lemma is that the formula φ does not depend on anything. Therefore we replaced the formula ψ of arbitrary size with a fixed formula φ of constant size, while k, l, ξ, r can be arbitrarily large. □

Proof of Lemma 60. First we describe the formula φ as a mathematical statement, and then we show using Lemma 57 that this statement can be expressed by an existential formula φ of $\mathcal{M}$, as required by the lemma.

The formula φ will say the following:

(105) *there exists an element* $u \in \mathbf{M}_{v'}$, *with* $u < 2^{k2^r}$ *such that if* $u_i = u[i,r]$, *for* $i = 0, ..., k-1$, *then* $\xi(u_0, ..., u_{k-1}, a_0, ..., a_{l-1}) = 0$

If we describe the statement in (105) as it is by a first-order formula of $\mathcal{M}$, then the size of the formula will depend on k and l so it is not suitable for our purposes. Lemma 57 however provides an existential first-order formula of constant size which decides whether a term μ in the structure $\mathbf{M}_t$ takes a given value b, at a given evaluation of the variables of the term μ. The evaluation of the variables is given by a single integer, and the term μ is given by the two integers $\mathtt{Circ}_0(\mu)$ and $\mathtt{Circ}_1(\mu)$. Lemma 57 is applicable for the present case with $\mu{:=}\ \xi$, $k{:=}\ k+l$, $t{:=}\ r$, $v{:=}\ v'$, $a_i{:=}\ a_i$, for $i = 0, 1, ..., l-1$ and $a_{l+j}{:=}\ u_j$ for $j = 0, 1, ..., k-1$, $b{:=}\ 0$. Let $\varphi'(y_0, ..., y_4)$ be the existential formula whose existence is guaranteed by lemma 57 with this choices of the parameters. The definition of the function $\mathtt{enc}$ implies that $\mathtt{enc}_{k+l,r}(a_0, ..., a_{l-1}, u_0, ..., u_{l-1}) = \mathtt{enc}_{l,r}(a_0, ..., a_{l-1}) + u2^{l2^r} = A + u2^{l2^r}$. Therefore the formula $\varphi(x_0, ..., x_5) \equiv \exists u, \varphi'(x_0 u 2^{x_5 2^{x_1}}, x_1, x_3, x_4)$ meets our requirements, since with $x_0{:=}\ A$, $x_1{:=}\ r$ $x_2{:=}\ \mathtt{Circ}_0(\xi)$, $x_3{:=}\ \mathtt{Circ}_0(\xi), x_4{:=}\ k$, $x_5{:=}\ l$ we get that

$\mathbf{M}_{v'} \models \varphi(\mathtt{enc}_{l,r}(A, r, \mathtt{Circ}_0(\xi), \mathtt{Circ}_1(\xi), k, l)$ iff there "exists an $u = \sum_{i=0}^{k} u_i 2^{i2^r} < 2^{k2^r} \in \mathbf{M}_{v'}$ with $\mathbf{M}_{v'} \models \varphi'(A + u2^{lr}, \mathbf{0}, r, \mathtt{Circ}_0(\xi), \mathtt{Circ}_1(\xi))$". This last statement by Lemma 57 is equivalent to condition (105). Therefore the formula φ our requirements. *Q.E.D.*(Lemma 60)

The existential formula φ in Lemma 60 may have more than one existential quantifier. Suppose that $\varphi \equiv \exists y_0, ..., y_{s-1}, P(y_0, ..., y_{s-1}, x_0, ..., x_5)$, where P is a propositional formula of $\mathcal{M}$. To reduce the number of existential quantifiers in the formula φ to one, and also to replace the six parameters $A, r, \mathtt{Circ}_0(\xi), \mathtt{Circ}_1(\xi), k, l$ of φ by a single parameter, we use Lemma 37 with the propositional formula P occurring in φ. We get the following stronger version of Lemma 60.

Lemma 61 *There exists a term* $\pi(x_0, \ldots, x_5)$ *of* $\mathcal{M}$ *and there exists an existential first-order formula* $\varphi(x)$ *of* $\mathcal{M}$, *containing a single existential quantifier, such that for all sufficiently large* $c_1 > 0$, *and for all integers* k, l, *for all formulas* ψ *and terms* ξ *satisfying condition* (100) of Lemma 59, and for all $r, v \in \omega$ with $v \geq r + c_1 \lceil \log(\mathtt{csize}(\xi)) \rceil$, we have that

(106) *for all* $a_0, \ldots, a_{l-1} \in \mathbf{M}_r$,

$$\mathbf{M}_r \models \psi(a_0, \ldots, a_{l-1}) \quad \leftrightarrow \quad \mathbf{M}_{v'} \models \varphi(\pi(A, r, \mathtt{Circ}_0(\mu), \mathtt{Circ}_1(\mu), k, l))$$

where $A = \mathtt{enc}_{l,r}(a_0, \ldots, a_{l-1})$.

Proof of Lemma 61. With the choice $v = v' + c_2$ where v' is the integer whose existence is stated in Lemma 60 the statement of the present lemma is an immediate consequence of Lemma 37 and Lemma 60. *Q.E.D.*(Lemma 61)

To complete the proof of Lemma 59 we use the $\mathcal{D}$-quantifier elimination assumption with the existential formula φ whose existence is stated in Lemma 61. We get that there exists a term η' of $\mathcal{M}$ with $\mathtt{csize}(\eta') \leq 2^{\mathcal{D}(v)}$ such that

(107) *for all* $a_0, \ldots, a_{l-1} \in \mathbf{M}_r$,

$$\mathbf{M}_r \models \psi(a_0, \ldots, a_{l-1}) \quad \leftrightarrow \quad \mathbf{M}_v \models \eta'(\pi(A, r, \mathtt{Circ}_0(\mu), \mathtt{Circ}_1(\mu), k, l)) = 0$$

where $A = \mathtt{enc}_{l,r}(a_0, \ldots, a_{l-1})$.

The definition of A implies that there exists a term σ of $\mathcal{M}$ with length at most $c_2 l$, where c_2 is a constant, such that $\mathbf{M}_v \models A = \sigma(a_0, \ldots, a_{l-1})$. There exist also terms σ', σ'' (without any free variables) of $\mathcal{M}$ of lengths at most $c_2(k+l)$ such that $\mathbf{M}_v \models k = \sigma' \wedge l = \sigma''$. Therefore the term $\eta = \eta'(\pi(\sigma(x_0, \ldots, x_{l-1}), w_0, w_1, w_2, \sigma', \sigma''))$ meets our requirements. *Q.E.D.*(Lemma 59)

Lemma 62 *Assume that* $k, m \in \omega$, $m \geq k$, $\langle j_k, ..., j_1 \rangle$, $\langle \iota_m, ..., \iota_1 \rangle$ *are sequences of positive integers,* $j_{k-i} \leq \iota_{m-i}$ *for all* $i = 0, ..., k-1$, *and* φ *is a prenex formula of* $\mathcal{M}$, *with quantifier pattern* $\langle j_m, ..., j_1 \rangle$. *Then there exists a prenex formula* ψ *of* $\mathcal{M}$ *with quantifier pattern* $\langle \iota_m, ..., \iota_1 \rangle$ *such that the propositional parts of* φ *and* ψ *are identical, and* $\vdash \varphi \leftrightarrow \psi$.

Proof of Lemma 62. We may add new quantified variables to φ which do not occur in the propositional part of φ. By "padding" φ with such new variables and quantifiers we may change its quantifier pattern into $\langle \iota_m, ..., \iota_1 \rangle$ in a way that the obtained prenex formula remains logically equivalent to φ. *Q.E.D.*(Lemma 62)

With Lemma 59 and 61 we have everything that we need to carry out the inductive step in the proof of Lemma 58. The following Lemma 63 says exactly what we have to prove at an inductive step, in terms of the quantitative bounds on the various parameters. It also defines integers denoted by $\gamma_{i,j}$ in Lemma 63 that will be used to define the "Gödel numbers" $\mathbf{g}(\varphi)$. The role of the sequence $\rho_0 < ... < \rho_m$ to be defined in Lemma 63 will be that at the ith step in the inductive proof we will show that $\mathbf{M}_d \models \varphi_i(...)$ is equivalent to $\mathbf{M}_{\rho_i} \models \tau_i(...) = \mathbf{0}$, where φ_i is the $i$the segment of the formula φ as defined earlier. After the proof of Lemma 63 we will return to the proof of Lemma 58.

Definition. The expression "β is sufficiently large with respect to α" will be written as $\alpha \ll \beta$. □

Lemma 63 *For all* $c, \alpha_0 \in \omega \backslash \{0\}$, *and for* $\varepsilon > 0$, *if* $c \ll \alpha_0 \ll \frac{1}{\varepsilon}$ *then the following holds. Assume that*

(108) *the* $\mathcal{D}$ *quantifier elimination assumption holds, where* $\mathcal{D}(x) = \varepsilon(\log x)^{\frac{1}{2}}$,

(109) $d \in \omega$ *is sufficiently large with respect to* ε,

(110) $\delta = \lfloor \mathcal{D}(d + \log d) \rfloor$, $m \in \omega$, $m \leq c\delta$, *and* $\iota_m, ..., \iota_1$ *are positive integers with* $\iota_m + \ldots \iota_1 \leq c^\delta$, $\iota_m \leq c\delta$,

(111) $\rho_0, \ldots, \rho_m$ *is a sequence of natural numbers defined by* $\rho_i = d + iD$, *for* $i = 0, 1, ..., m$, *where* $D = \lfloor \frac{\log d}{m} \rfloor$,

(112) $\varphi \equiv Q_m \vec{x}_m, \ldots, Q_1 \vec{x}_1, \mu(\vec{x}_1, \ldots, \vec{x}_m, x) = \mathbf{0}$ *is a prenex first-order formula of* $\mathcal{M}$*, with quantifier pattern* $\langle \iota_m, \ldots, \iota_1 \rangle$ *of* $\mathcal{M}$*, where* μ *is a* $0,1$*-term of* $\mathcal{M}$ *with* $\mathtt{csize}(\mu) \leq c^\delta$*,* $\vec{x}_i$ *is the sequence of variables* $x_{i,0}, \ldots, x_{i,\iota_i - 1}$*, and* Q_1 *is an existential quantifier.*

Then there exist $3(m+1)$ *natural numbers* $\gamma_{i,j}$*,* $i \in m+1$*,* $j \in 3$*, and there exists a sequence of terms* $\langle \tau_0, \ldots, \tau_m \rangle$ *of* $\mathcal{M}$ *such that for each* $i \in m+1$ *the following conditions are satisfied:*

(113) $\gamma_{i,0} = \mathtt{Circ}_0(\tau_i)$*,* $\gamma_{i,1} = \mathtt{Circ}_1(\tau_i)$*,* $\gamma_{i,2} = \rho_i$ *and* $\max\{\gamma_{i,0}, \gamma_{i,1}, \gamma_{i,2}\} < 2^d$*,*

(114) τ_i *has arity* $1 + 3i + \sum_{j=i+1}^{m} \iota_j$*,*

(115) $\mathtt{csize}(\tau_m) \leq \mathcal{S}(\rho_m)$*, and if* $i > 0$ *then* $\mathtt{csize}(\tau_i) \leq (\mathcal{S}(\rho_m))^{\alpha_0}$*,*

(116) *for all* $\vec{a}_{i+1} \in (\mathbf{M}_d)^{\iota_{i+1}}, \ldots, \vec{a}_m \in (\mathbf{M}_d)^{\iota_m}, a \in \mathbf{M}_d$*,*

$$\mathbf{M}_d \models \varphi_0(\vec{a}_{i+1}, \ldots, \vec{a}_m, a) \;\leftrightarrow\; \mathbf{M}_{\rho_0} \models \tau_0(\vec{a}_{i+1}, \ldots, \vec{a}_m, a) = \mathbf{0}$$

and if $i > 0$ *then*

$$\mathbf{M}_d \models \varphi_i(\vec{a}_{i+1}, \ldots, \vec{a}_m, a) \;\leftrightarrow\; \mathbf{M}_{\rho_i} \models \tau_i(\vec{a}_{i+1}, \ldots, \vec{a}_m, a, \vec{\gamma}_0, \ldots, \vec{\gamma}_i) = \mathbf{0}$$

where the formula φ_i *is the* i*th segment of the formula* φ*, and* $\vec{\gamma}_r$ *is the sequence* $\gamma_{r,0}, \gamma_{r,1}, \gamma_{r,2}$ *for all* $r \in m$*.*

Proof of Lemma 63. Assume that $c \ll \frac{1}{\varepsilon}$ and $d, \mathcal{S}, m, \nu, \iota_0, \ldots, \iota_m, \varphi$ are given and they satisfy conditions (108),...,(112) of the lemma. We construct the sequences τ_i, $\vec{\gamma}_i$, $i = 0, 1, \ldots, m$ by recursion on i and at the same time we prove their required properties by induction on i.

$i = 0$. We define the term τ_0 by $\tau_0 = \mu$. The sequence $\vec{\gamma}_0 = \langle \gamma_{0,0}, \gamma_{0,1}, \gamma_{0,2} \rangle$ is defined by condition (113) of the lemma. We check all of the conditions that must be satisfied.

Condition (113). The first three equalities follows from the definition of $\vec{\gamma}_0$.

The upper bound on the integer $\gamma_{0,2}$ holds, since $\gamma_{0,2} = \rho_0 \leq \rho_m \leq d + \log d < 2^d$. According to Lemma 56 we have $\gamma_{0,0} = \mathtt{Circ}_0(\mu) \leq \log\log(c^\delta) < 2^d$ and $\gamma_{0,1} = \mathtt{Circ}_{0,1}(\mu) \leq (c^\delta)^{8c^\delta} = 2^{8\delta c^\delta \log c}$. Since $\delta = \lfloor \mathcal{D} + \log d \rfloor \leq 2\varepsilon(\log d)^{\frac{1}{2}}$ we have that $\mathtt{Circ}_1(\mu) < 2^d$.

Condition (114). The arity of μ is $1 + \sum_{j=1}^{m} \iota_i$.

Condition (115). For $i = 0$ this does not state anything.

Condition (116). Since $\rho_0 = d$ and $\tau_0 = \mu$ the two statements whose equivalence is claimed are identical.

$i > 0$. Assume that $\tau_0, \ldots, \tau_{i-1}$, $\vec{\gamma}_0, \ldots, \vec{\gamma}_{i-1}$ has been already defined and they meet the requirements of the lemma with $i := i - 1$. For the definition of τ_i we use Lemma 59 with $k := \iota_i$, $l := 1 + 3i + \sum_{j=i+1}^{m} \iota_j$, $\xi := \mathbf{1} - \tau_{i-1}$, $\psi := \exists \vec{x}_i, \mathbf{1} - \tau_{i-1}(\vec{x}_i, \vec{x}_{i+1}, \ldots, \vec{x}_m, x, \vec{y}_0, \ldots, \vec{y}_{i-1}) = \mathbf{0}$, where $\vec{x}_j$ is the sequence of variables $x_{j,0}, \ldots, x_{j,\iota_j - 1}$, for $j = i-1, \ldots, m$ and $\vec{y}_j$ is the sequence of variables $y_{j,0}, y_{j,1}, y_{j,2}$, $r := \rho_{i-1}$, $v := \rho_i$. We assume that $\frac{1}{\varepsilon}$ is sufficiently large with respect to the constant c

of Lemma 59. We have to check that the assumption of Lemma 59 are satisfied by this choice of its parameters. Conditions (99) and (100) are immediate consequences of the definitions and the assumptions of Lemma 63.

Condition (101) of Lemma 59. Here we separately consider the $i = 1$ and the $i > 1$ case. Assume first that $i = 1$. Then $\xi = \mathbf{1} - \tau_0 = \mathbf{1} - \mu$. We have $\mathtt{csize}(\mu) \leq c^\delta$, $r = \rho_0$, $v = \rho_1$, and by the definition of the sequence ρ_j, $\rho_1 \geq \rho_0 + \frac{\log d}{m}$, where $m \leq c\delta$, $\delta = \lfloor \mathcal{D}(d + \log d) \rfloor \leq \varepsilon(\log(d + \log d))^{\frac{1}{2}}$. (We denote the constant c of Lemma 59 by c'.) Therefore $r + c' \log(\mathtt{size}(\xi)) = \rho_0 + c' \log(c^\delta) \leq \rho_0 + c'\delta \log c$. Since $\varepsilon > 0$ is sufficiently small with respect to both c and c', $m \leq c\delta$, we have $c'\varepsilon\delta \log c < \frac{\log d}{m}$ and therefore $r + c' \log(\mathtt{size}(\xi)) \leq \rho_1 = v$ as required.

In the $i > 1$ case (of condition (101) of Lemma 59) the upper bound on $\mathtt{csize}(\xi) = \mathtt{csize}(\tau_{i-1})$ follows from conditions (115), namely $\mathtt{csize}(\tau_{i-1}) \leq (\mathcal{S}(\rho_m))^{\alpha_0}$. Therefore $\log(\mathtt{csize}(\tau_{i-1})) \leq \alpha_0\varepsilon(\log(d + \log d))^{\frac{1}{2}}$. This differs from the same upper bound in the $i = 1$ case only by a constant factor which is sufficiently small with respect to $1/\varepsilon$, so we may complete the proof in the same way as in the $i = 1$ case. This completes the proof of the fact that the assumptions of Lemma 59 hold, and we continue the definitions in the inductive proof of Lemma 63 in the $i > 0$ case.

We define τ_i by $\tau_i = \eta$, where η is the term whose existence is guaranteed by Lemma 59. $\vec{\gamma}_i$ is defined by (113). We show now that the sequences $\tau_0, \ldots, \tau_i$, $\vec{\gamma}_0, \ldots, \vec{\gamma}_i$ satisfy conditions (113), (114), (115), (116) of Lemma 63.

Condition (113). The first three equalities are the definitions of $\gamma_{i,j}$, $j \in 3$. We get the upper bounds on $\gamma_{i,j}$, $j = 0, 1, 2$ in the same way as in the $i = 0$ case.

Condition (114). The arity of η in Lemma 59 is the number of free variables of ψ plus 3. The number of free variables of the formula $\exists \vec{x}_i, \tau_{i-1}(\vec{x}_i, \vec{x}_{i+1}, \ldots, \vec{x}_m, x, \vec{y}_0, \ldots, \vec{y}_{i-1})$ is $1 + 3(i-1) + \sum_{j=i+1}^{m} \iota_j$. Increasing it by three we get the value claimed in condition (114).

Condition (115). In this proof we will use the following trivial inequality containing the function $\mathcal{D}(x) = \varepsilon(\log x)^{\frac{1}{2}}$:

$$\mathcal{D}(d + \log d) \leq 2\mathcal{D}\Big(d + m\Big\lfloor \frac{\log d}{m} \Big\rfloor\Big) = 2\mathcal{D}(\rho_m)$$

According to condition (102) of Lemma 59 $\mathtt{csize}(\tau_i) = \mathtt{csize}(\eta) \leq \mathcal{S}(v) + c'(k + l) = \mathcal{S}(\rho_i) + c'(\iota_i + 1 + 3i + \sum_{j=i+1}^{m} \iota_j) \leq \mathcal{S}(\rho_i) + c'c^\delta + 1 + 3c\delta + c^\delta \leq c''\mathcal{S}(\rho_m)c^\delta$, where c'' is a suitably chosen constant. (We used here the inequality $\mathcal{S}(\rho_i) \leq \mathcal{S}(\rho_m)$.) The definition of δ implies that $c^\delta \leq 2^{\mathcal{D}(d+\log d)\log c} \leq 2^{2\mathcal{D}(\rho_m)\log c} = (\mathcal{S}(\rho_m))^{2\log c}$. Since $c \ll \alpha_0$ this implies $\mathtt{csize}(\tau_i) \leq \mathcal{S}(\rho_m)^{\alpha_0}$

In the $i = m$ case we use that fact that the values k and l from Lemma 59 are smaller than in the general case. Namely $k = \iota_m$ and $l = 1 + 3m$. Therefore by (110) $\mathtt{csize}(\tau_m) \leq \mathcal{S}(\rho_m) + c'(c\delta + 1 + 3c\delta) \leq \mathcal{S}(\rho_m) + 4cc' \log(\mathcal{S}(\rho_m)) \leq 2\mathcal{S}(\rho_m)$.

Condition (116). According to the inductive assumption for all $\vec{a}_i \in (\mathbf{M}_d)^{\iota_{i+1}}, \ldots, \vec{a}_m \in (\mathbf{M}_d)^{\iota_m}, a \in \mathbf{M}_d$, $\mathbf{M}_d \models \varphi_{i-1}(\vec{a}_i, \ldots, \vec{a}_m, a)$ is equivalent to $\tau_i(\vec{a}_i, \ldots, \vec{a}_m, a, \vec{\gamma}_0, \ldots, \vec{\gamma}_{i-1}) = \mathbf{0}$. This fact, the definition of φ_i, and Lemma 59 imply that for all $\vec{a}_{i+1} \in (\mathbf{M}_d)^{\iota_{i+1}}, \ldots, \vec{a}_m \in (\mathbf{M}_d)^{\iota_m}, a \in \mathbf{M}_d$, the following statements are equivalent

$\mathbf{M}_d \models \varphi_i(\vec{a}_{i+1}, \ldots, \vec{a}_m, a)$

$\mathbf{M}_d \models \exists \vec{x}_i, \neg\varphi_{i-1}(\vec{x}_i, \vec{a}_{i+1} \ldots, \vec{a}_m, a)$
$\mathbf{M}_{\rho_{i-1}} \models \exists \vec{x}_i,\ \mathbf{1} - \tau_{i-1}(\vec{x}_i, \vec{a}_{i+1}, \ldots, \vec{a}_m, a, \vec{\gamma}_0, \ldots, \vec{\gamma}_{i-1}) = \mathbf{0}$.
$\mathbf{M}_{\rho_{i-1}} \models \exists \vec{x}_i, \xi(\vec{x}_i, \vec{a}_{i+1}, \ldots, \vec{a}_m, a, \vec{\gamma}_0, \ldots, \vec{\gamma}_{i-1}) = \mathbf{0}$
$\mathbf{M}_{\rho_i} \models \eta(\vec{a}_{i+1}, \ldots, \vec{a}_m, a, \vec{\gamma}_0, \ldots, \vec{\gamma}_{i-1}, \gamma_i) = \mathbf{0}$
$\mathbf{M}_{\rho_i} \models \tau_i(\vec{a}_{i+1}, \ldots, \vec{a}_m, a, \vec{\gamma}_0, \ldots, \vec{\gamma}_{i-1}, \gamma_i) = \mathbf{0}$
The equivalence of the first and last statements of this sequence is claimed in condition (116) of the present lemma. *Q.E.D.*(Lemma 63)

Proof of Lemma 58. Assume that $\mathcal{S}, d, m, \delta, \iota_1, \ldots, \iota_m,\ \rho_0, \ldots, \rho_m$ are fixed with the properties described in the assumptions of Lemma 63. We define first the function $\mathbf{g}$.

Assume that a first-order formula $\varphi \in \mathtt{Form}(\mathcal{S}(\rho_m), \iota_1, \ldots, \iota_m)$ is is given. We apply now Lemma 63 for φ with the given values of the parameters. Let $\gamma_{i,j}$, $i \in m, j \in 3$ be the natural numbers and let $\tau_0, \ldots, \tau_m$ be the terms whose existence is guaranteed by Lemma 63. We define now $\mathbf{g}(\varphi)$ by

$$\mathbf{g}(\varphi) = d2^{\rho_m} + 2^{2\rho_m} \sum_{i=0}^{m} \sum_{j=0}^{2} \gamma_{i,j} 2^{(3i+j)d}$$

By condition (110), $m \leq c\delta \leq \log d$ and according to condition (113) $\max\{\gamma_{i,j} | i \in m+1, j \in 3\} < 2^d$, so we have that $\mathbf{g}(\varphi) < 2^{2^{d-1}}$ as stated in the lemma. We also claim that

(117) $\mathbf{g}(\varphi)$ *uniquely determines all of the integers* $\gamma_{i,j}$.

This is true since $d2^{\rho_m}$ is the residue of $\mathbf{g}(\varphi)$ divided by $2^{2\rho_m}$. This uniquely determines both d and $\sum_{i=0}^{m} \sum_{j=0}^{2} \gamma_{i,j} 2^{(3i+j)d}$. According to (113) $\gamma_{i,j} < 2^d$, therefore this sum uniquely determines all of the integers $\gamma_{i,j}$, $i \in m+1, j \in 3$.

This process as we got the integers $\gamma_{i,j}$ for $\mathbf{g}(\varphi)$ can be implemented by a term of $\mathcal{M}$, which is evaluated in $\mathbf{M}_{\rho_m}$. Indeed we have $\mathbf{M}_{\rho_m} \models \div(\mathbf{g}(\varphi), \mathbf{n}) = b$, where $b = \sum_{i=0}^{m} \sum_{j=0}^{2} \gamma_{i,j} 2^{(3i+j)d}$ and $\mathbf{M}_{\rho_m} \models d = \div(\mathbf{g}(\varphi) - b, \mathbf{n})$. Finally from b and d we can compute each $\gamma_{i,j}$ using Lemma 5. This implies that there exist a term $\chi(x, y, z, w)$, of $\mathcal{M}$ (which does not depend on anything so its length is a constant c_1), such that for each possible choice of φ with the described properties we have that for all $i \in m$, $j \in 3$, $\mathbf{M}_{\rho_m} \models \gamma_{i,j} = \chi(\mathbf{g}(\varphi), m, i, j)$, for $i \in m, j \in 3$.

We want to define the term τ such that for all $a, b \in \mathbf{M}_{\rho_m}$,

$$\mathbf{M}_{\rho_m} \models \tau(a, b) = \tau_m\Big(a, \vec{\chi}(b, m_0, 0), \vec{\chi}(b, m_0, 1), \ldots, \vec{\chi}(b, m_0, m-1)\Big)$$

where $\vec{\chi}(b, m_0, i)$ is the sequence $\chi(b, m_0, i, 0), \chi(b, m_0, i, 1), \chi(b, m_0, i, 2)$ for $i = 0, 1, \ldots, m-1$. We can achieve this by a term τ whose circuit-size is at most $\mathtt{csize}(\tau_m) + c'm$, where $c' \in \omega$ is a constant. We prove the existence of such a term τ by constructing first an $\mathcal{M}$-circuit C, which computes the same function that is expected from τ. The $\mathcal{M}$-circuit at the input a, b will compute first the numbers $0, ..., m-1$ using m nodes. For each fixed $i \in m$, $j \in 3$ there will be at most c_1 nodes in the circuit C to evaluate $\chi(a, b, i, j)$ and finally C contains $\mathtt{csize}(\tau_m)$ nodes to evaluate τ_m at the

input $a, \vec{\chi}(b, m_0, 0), \vec{\chi}(b, m_0, 1), \ldots, \vec{\chi}(b, m_0, m-1)$. The term τ whose existence is stated in the lemma will be a term of $\mathcal{M}$ which computes the same value at each input as the circuit C constructed above.

We show now that the function $\mathbf{g}$, and the term τ satisfies conditions (97) and (98) of the lemma.

Condition (97). The definition of the term τ implies that $\mathtt{csize}(\tau) \leq \mathtt{csize}(\tau_m) + c'm$ for some constant c'. Therefore $m \leq c\delta$ and the upper bound on $\mathtt{csize}(\tau_m)$ given in (115) implies that $\mathtt{csize}(\tau) \leq 3\mathcal{S}(d + \log d)$.

Condition (98). The definition of the formula τ and the terms $\chi_{i,j}$ implies that $\mathbf{M}_{\rho_m} \models \tau(a, \mathbf{g}(\varphi)) = \tau_m(a, \vec{\gamma}_0, \ldots, \vec{\gamma}_m)$ and therefore condition (116) with $i = m$ implies our statement. *Q.E.D.*(Lemma 58)

9.2 The predictivity of M

Definition. 1. The set of functions symbols of $\mathcal{M}$ (including the constant symbols) will be denoted by $\mathtt{fsymb}(\mathcal{M})$

2. Let $\mathcal{J}$ be a function. We will say that $\mathbf{M}$ is $\mathcal{J}$-predictive if the following conditions are satisfied.

(118) *The function $\mathcal{J}$ is a monotone increasing function defined on ω and with values in ω.*

(119) *For all sufficiently large $d \in \omega$, $\mathcal{J}(d) \in \mathbf{M}_d$ and $\mathcal{J}(d) > d$.*

(120) *There exists a function defined on $\mathtt{fsymb}(\mathcal{M})$ assigning to each function symbol $f(x_0, \dots, x_{k-1})$ of $\mathcal{M}$, a formula $\Phi_f(x, y, z, Y_0, \dots, Y_{k-1}) \in \mathtt{SForm}(\mathcal{M})$, where x, y, z are free first-order variables and $Y_0, \dots, Y_{k-1}$ are free variables for binary relations, such that the following holds. For all $d, r \in \omega$ with $d + r \leq \mathcal{J}(d)$ there exists a map $\eta_{d,r}$ of $\mathtt{universe}(\mathbf{M}_{d+r})$ into the set of binary relations on $\mathtt{universe}(\mathbf{M}_d)$ with the following properties:*

(i) For each $a, u, v \in \mathbf{M}_d$, we have $(\eta_{d,r}(a))(u, v)$ iff "$u = 0$ and $v = a$".

(ii) Suppose that $f(x_0, \dots, x_{k-1})$ is a k-ary function symbol of $\mathcal{M}$, for some $k = 0, 1, 2$ (including the constant symbols for $k = 0$) and $a_0, \dots, a_{k-1} \in \mathbf{M}_{d+r}$. Then for all $u, v \in \mathbf{M}_d$, $(\eta_{d,r}(f^{(d+r)}(a_0, \dots, a_{k-1}))(u, v)$ iff $\mathbf{M}_d \models \Phi_f(u, v, r, \eta_{d,r}(a_0), \dots, \eta_{d,r}(a_{k-1}))$, where $f^{(d+r)} = (f)_{\mathbf{M}_{d+r}}$. □

Lemma 64 *Assume that $c > 0$ is a real, and $\mathcal{J}(x) = \lfloor x + c \log x \rfloor$. Then $\mathbf{M}$ is $\mathcal{J}$ predictive.*

Proof. In [6] a weaker result of similar nature is proved which implies that there exists a function $g(x)$ with $\lim_{x\to\infty} g(x) = \infty$, such that if $\mathcal{J}_0 = x + g(x)$ then $\mathbf{M}$ is $\mathcal{J}_0$-predictive. Some of the partial results of the proof given there were stronger than what was needed for the theorem formulated in [6]. We get Lemma 64 by using the full strength of these partial results in particular about the first-order definability of the bits of the results of multiplication and division between large numbers.

Here we give only the outline of the proof together with with those details that has to be changed for the present purposes.

We define the function $\mathcal{J}$ by $\mathcal{J}(x) = \lfloor x + c \log x \rfloor$. Assume that $d \in \omega$ is sufficiently large $\chi \in \omega$ and $d + \chi \leq \mathcal{J}(d)$. First we define the map $\eta_{d,\chi}$ whose existence is required by the definition of predictivity. To make our notation more concise we will write $\eta^{(a)}_{d,\chi}$ instead of $\eta_{d,\chi}(a)$.

Assume that $a \in \mathbf{M}_{d+\chi}$, $2^d = n$, $\nu = 2^\chi$. Let $a_i = \mathtt{coeff}_i(a, 2^n)$ for $i = 0, 1, \dots, \nu - 1$. We define $\eta_{d,\chi}$ by: "for all $u, v \in \mathbf{M}_d$, $\eta^{(a)}_{d,\chi}(u, v)$ iff $u \in \nu$ and $v = a_u$". This definition

implies that if $a \in \mathbf{M}_d$ then for all $u, v \in \mathbf{M}_d$, $\eta^{(a)}_{d,\chi}(u,v)$ iff $u = 0$ and $v = a$, that is, our definition satisfies condition (120)/(i) from the definition of predictivity.

We define now the formula $\Phi_f(x, y, z, Y_0, \ldots, Y_{k-1})$ for each function symbol f of $\mathcal{M}$. (According to the definition of $\mathcal{J}$-predictivity the formula Φ_f cannot depend on the choices of d or χ.)

If $f = \mathbf{c}$ is a constant symbol of $\mathcal{M}$ then $\Phi_{\mathbf{c}} \equiv x = \mathbf{0} \wedge y = \mathbf{c}$. By the definition of $\eta_{d,\chi}$, the formula $\Phi_{\mathbf{c}}$ satisfies condition (120)/(ii) from the definition of predictivity, for all constant symbols $\mathbf{c}$ of $\mathcal{M}$.

We will not use the relation $\eta^{(a)}_{d,\chi}$ directly in the definition of Φ_f, for the remaining function symbols f of $\mathcal{M}$, but we first define another binary relation $\xi^{(a)}_{d,\chi}$ on $\mathbf{M}_d$ and use this relation.

Definition. 1. For each positive integer k and $u = \langle u_0, \ldots, u_{k-1}\rangle \in (\mathbf{M}_d)^k$, $u\wr_n$ will denote the integer $u_{k-1}n^{k-1} + u_{k-2}n^{k-2} + \ldots + u_1 n + u_0$.

2. Assume that R is a k-ary relation on the set $n = \{0, 1, \ldots, n-1\}$, where $n = 2^d$. $\mathtt{integer}_k(R)$ will denote the integer $\sum\{2^{u\wr_n} \mid u \in \mathbf{M}^k_d \wedge R(u)\}$. Clearly $R \to \mathtt{integer}_k(R)$ is a one-to-one map from the set of all k-ary relation on n to the set of all natural numbers less then 2^{n^k}. If $a \in [0, 2^{n^k} - 1]$ is a natural number then the unique k-ary relation R on n with $\mathtt{integer}_k(R) = a$ will be denoted by $\mathtt{integer}^{-1}_k(R)$. □

Definition. 1. Suppose that R is a k-ary relation on $\mathbf{M}_d$. We will say that the relation R is n-restricted if for all $u = \langle u_0, \ldots, u_{k-1}\rangle \in \mathbf{M}^k_d$, $R(u_0, \ldots, u_{k-1})$ implies that for all $i = 0, 1, \ldots, k-1$ with $u_i \in n$.

2. Assume that d, χ are positive integers and $a < 2^{n^2}$. Then $\xi^{(a)}_d$ is the unique binary relation on $\mathbf{M}_d$ which satisfies the following two conditions: (a) The relation $\xi^{(a)}_d$ is n-restricted, and (b) $\mathtt{integer}_2(\xi^{(a)}_d) = a$. □

Lemma 65 *There exists a first-order formula $\varphi(x, y, z)$ of $\mathcal{M}$ such that for all $d \in \omega$ and for all $a, b \in 2^{2^d}$ and $i \in 2^d$ we have that $b = \mathtt{coeff}_i(a, 2)$ iff $\mathbf{M}_d \models \varphi(a, b, i)$.*

Proof. The statement of the lemma follows from Lemma 8, *Q.E.D.*(Lemma 65)

The following Lemma states that the relations $\xi^{(a)}_d$ and $\eta^{(a)}_{d,\chi}$ can be defined from each other in a first-order way. It is important that for the definition of the value $\xi^{(a)}_d(u, v)$ for a fixed pair u, v we may need the values $\eta^{(a)}_{d,\chi}(x, y)$ for all $x, y \in \mathbf{M}_d$ and vice versa.

Lemma 66 *There exist formulas $\Psi_i(x, y, z, Z) \in \mathtt{SForm}(\mathcal{M})$, $i = 0, 1$, where x, y, z are first-order variables and Z is a variable for a binary relation such that for all for all sufficiently large $d \in \omega$, for all $\chi \in 2^d$ and for all $a \in \mathbf{M}_{d+\chi}$ the following holds: $\mathbf{M}_d \models \forall u, v, [\xi^{(a)}_d(u, v) \leftrightarrow \Psi_0(u, v, \chi, \eta^{(a)}_{d,\chi})]$ and $\mathbf{M}_d \models \forall u, v, [\eta^{(a)}_{d,\chi}(u, v) \leftrightarrow \Psi_1(u, v, \chi, \xi^{(a)}_d)]$*

Proof. Assume $a \in 2^{2^{d+\chi}}$ and $a = \sum^{(\nu-1)}_{i=0} a_i (2^{2^d})^\nu$. The formula Ψ_1 have to express the statement $u \leq \nu \wedge v \leq n \wedge \mathtt{coeff}_{un+v}(a, 2) = 1$. $\mathtt{coeff}_{un+v}(a, 2) = 1$ is equivalent to $\mathtt{coeff}_v(a_u, 2) = 1$. Using the relation $\eta^{(a)}_{d,\chi}$ we can define a_u in a first-order way in $\mathbf{M}_d$,

namely $x = a_u$ iff $\mathbf{M}_d \models \eta^{(a)}_{d,\chi}(u,x)$. If a_u is given then, by Lemma 65, $\mathtt{coeff}_v(a_u,2)$ has a first-order definition in $\mathbf{M}_d$. This completes the definition of Ψ_0. In the first-order formula Ψ_1 we have to define a_u form its binary coefficients which can be done by using again Lemma 65. *Q.E.D.*(Lemma 66)

Lemma 66 implies that it is sufficient to prove that condition (120) of the definition of predictivity holds in the following modified form. For the sake of notational simplicity we consider here all of the function symbols of $\mathbf{M}$ as binary function symbols. In the case of the constant symbols $\mathbf{0}, \mathbf{1}, -\mathbf{1}$, and $\mathbf{n}$ the interpretation of these symbols is a binary function which does not depend on its variables. For the unary functions symbols $\mathcal{N}$ and $\mathbf{p}$ their interpretation is a binary function which depends only on its first variable.

(121) *Suppose that f is one of the function symbols $\mathbf{0}, \mathbf{1}, -\mathbf{1}$, $\mathbf{n}, \cap, \mathcal{N}$, $+, \times, \mathbf{p}, \div$, $\max, \min, \cap, \mathcal{N}$ of $\mathcal{M}$. Then there exists a formula $\Phi'_f(x,y,z,Y_0,Y_1) \in \mathtt{SForm}(\mathcal{M})$, where x,y,z are first-order variables and Y_0, Y_1 are variables for binary relations such that for all $c \in \omega$, for all sufficiently large $d \in \omega$, and for all $a, b \in \mathbf{M}_{d+\chi}$, and for all $u, v \in \mathbf{M}_d$, $\xi_d^{(f^{(d+\chi)}(a,b))}(u,v)$ is true iff $\mathbf{M}_d \models \Phi'_f(u,v,\chi,\xi_d^{(a)},\xi_d^{(b)})$, where $f^{(d+\chi)} = (f)_{\mathbf{M}_{d+\chi}}$.*

In other words given the binary bits of $a, b \in 2^{2^{d+\chi}}$, each by a binary relation on $\mathtt{universe}(\mathbf{M}_d)$, we have to define in $\mathbf{M}_d$ in a first-order way the binary bits of $0, 1, 2^{2^{d+\chi}}-1$, $d+\chi, 2^a, \mathcal{N}(a)$, $a+b, ab, a \div b = \lfloor a/b \rfloor$,, $\min(a,b)$, $\max(a,b)$, $a \cap b$, where the operations are defined in the structure $\mathbf{M}_{d+\chi}$. The task is trivial for 0 and 1. In the case of $2^{2^{d+\chi}}-1$ all of the $2^{d+\chi}$ bits are 1s. We get the bits of $d+\chi$ by computing $d+\chi$ with an addition in $\mathbf{M}_d$, where d can be defined by a first-order formula using the constant symbol $\mathbf{n}$. Since $a \cap b$ and $\mathcal{N}(a)$ are defined by bitwise operations Φ_f obviously can be easily defined for these two operations. Therefore we have to prove that condition (121) holds only for the remaining function symbols.

Using the function $\mathtt{integer}_k^{-1}$ we can represent natural numbers from the interval $[0, 2^{n^k}-1]$ by k-ary relations on n. Our next goal is to represent sequences of natural numbers by relation on n, (where we have a bound both on the length of the sequence and the sizes of its elements).

Definition. 1. The set of all sequences of length i, whose elements are from the set A will be denoted by, $\mathtt{seq}(i,A)$. For example the set of all sequences of length n^l whose elements are integers in the interval $[0, 2^{n^k}-1]$ is $\mathtt{seq}(n^l, 2^{n^k})$.

2. Assume that $a = \langle a_0, \ldots, a_{j-1} \rangle \in \mathtt{seq}(n^l, 2^{n^k})$. We will represent this sequence by a $k+l$-ary relation $R^{(a)}$ on n defined in the following way. For all $i \leq j-1$, and for all $u_0, \ldots, u_{k-1}, v_0, \ldots, v_{l-1} \in n$, $R^{(a)}(u_0, \ldots, u_{k-1}, v_0, \ldots, v_{l-1})$ iff $(\mathtt{integer}_k^{(-1)}(a_t))(u_0, \ldots, u_{k-1})$, where $t = \sum_{i=0}^{l-1} v_i n^i$. Since in this representation the length of the sequence cannot be arbitrarily chosen it must be n^l, for some $l \in \omega$, we will call this representation a representation of the sequence without its length.

3. The definition above provides representation only for sequences with exactly n^l elements for some natural number l. A sequence $a = \langle a_0, \ldots, a_{j-1} \rangle$ where $j < n^l$, $a_i \in$

$[0, 2^{n^k} - 1]$ will be represented in the following way. We attach the number j as the first element to the sequence a and attach a sequence of 0s to its end, so that the total length of the sequence $a' = \langle j, a_0, \ldots, a_{j-1}, 0, \ldots, 0\rangle$ obtained this way is n^l. The representation of the sequence a together with its length will be the same as the representation of the sequence a' without its length, as defined earlier. In the following the representation of a sequence will always mean a representation of the sequence together with its length unless we explicitly state otherwise.

4. Assume that d is a positive integer and $n = 2^d$. We will say that the set X is $\mathbf{M}_d$-representable if there exists natural numbers k, l such that either $X = \{0, 1, \ldots, 2^{n^k} - 1\}$ or $X = \mathtt{seq}_n(n^l, 2^{n^k})$. If X is an $\mathbf{M}_d$ representable set and $X = \{0, 1, \ldots, 2^{n^k} - 1\}$ then we define its weight by $\mathtt{weight}(X) = k$, if $X = \mathtt{seq}_n(n^l, 2^{n^k})$ then we define its weight by $\mathtt{weight}(X) = k + l$. If $a \in X$, where X is an $\mathbf{M}_d$ representable set, then $\mathtt{relation}_{a,n}$ will denote the k-ary or $k + l$-ary relation on n representing the element a. □

We will consider now families of functions $f^{(d)}$, $d \in \omega$ so that for each $d \in \omega$, $f^{(d)} \in \mathtt{func}(X^{(d)}, Y^{(d)})$ where both $X^{(d)}$ and $Y^{(d)}$ are $\mathbf{M}_d$-representable sets with weight less then w for a constant w. We are interested in the case when such a family of functions can be defined by a first-order formula in $\mathbf{M}_d$ without using any parameters. The world "strongly" that we will use in the definition below refers to mentioned the lack of parameters.

Definition. 1. Assume that $w_i \in \omega$ for $i = 0, 1$ and for all $d \in \omega$, $A_i^{(d)}$ are $\mathbf{M}_d$ representable sets of weight w_i for $i = 0, 1$, and $f^{(d)} \in \mathtt{func}(A_0^{(d)}, A_1^{(d)})$. We will say that the family of functions $f^{(d)}$ is a strongly first-order definable family function or a s.f.d.-family in $\mathbf{M}$ if there exists a formula $\Gamma(x_0, \ldots, x_{w_1-1}, Z) \in \mathtt{SForm}$, where x_i, $i = 0, 1, \ldots, w_1 - 1$ are individual variables and Z is a variable for k_0-ary relations such that for all sufficiently large $d \in \omega$ and for all $a \in A_0^{(d)}$, and $b \in A_1^{(d)}$ with $f(a) = b$, we have that for all $u_0, \ldots, u_{w_1-1} \in n$, $\mathtt{relation}_{b,n}(u_0, \ldots, u_{w_{1-1}})$ iff $\mathbf{M}_d \models \Gamma(u_0, \ldots, u_{w_1-1}, \mathtt{relation}_{a,n})$. □

We prove now that condition (121) is satisfied by each function symbol of $\mathcal{M}$. As we mentioned already this statement trivially holds for some of the function symbols. For the remaining ones we show now that the corresponding families of functions are are strongly first-order definable in $\mathbf{M}$.

For $f = \min$ and $f = \max$ the statement is trivial since $a \leq b$ iff $\mathtt{integer}_2^{-1}(a) \leq \mathtt{integer}_2^{-1}(b)$ according to the lexicographic ordering which clearly can be defined in $\mathbf{M}_d$ in a first-order way.

The function symbol $f =$ " $+$ ". If two integers are given in binary form each with m bits then the bits of their sum can be defined by a simple well-known constant depth circuit whose size is linear in m. This circuit is defined in a uniform way which makes it possible to translate it into a first-order formula interpreted in $\mathbf{M}_d$. For later use we also consider now the case where we have to add a sequence of integers. This question has been also studied for circuits, and it is known that if we have at most $(\log m)^{c_0}$ integers with m^{c_1} binary bits then their sum can be computed by an unlimited fan-in boolean circuit with size m^{c_2} and depth c_3, where c_2, c_3 depend only on c_0 and c_1, see [1]. The

construction of the circuit is uniform, in this case too, and can be translated into a first-order formulas, that we need for our present purposes, over a structure containing the arithmetic operations.

Definition. If b is a finite sequence of integers then $\mathbf{S}b$ will denote the sum of its elements. □

The following Lemma is proved in [6]

Lemma 67 *Assume that $c_0, c_1 \in \omega$. Then there exists a strongly first-order definable family of functions $f^{(d)}$, $d \in \omega$, such that for all sufficiently large d if $n = 2^d$, $j \leq n^{c_0}$ and a is sequence of length j, from elements of the set 2^{n^k}, that is, $a \in \mathtt{seq}(j, 2^{n^k})$, then $\mathbf{S}a = f^{(d)}(a)$.*

We prove condition (121) for $f = \times$ in a more general form then needed, namely we will consider products with more than two factors. This will be useful in the proof of (121).

Definition. Assume that $a = \langle a_0, a_1, \ldots, a_{j-1} \rangle$ is a sequence of integers. Then $\mathbf{P}a$ will denote the number $\prod_{i=0}^{j-1} a_i$. □

Definition. Assume that $\alpha(x), \beta(x)$ are functions defined on ω with real values. We will say that the pair $\langle \alpha(x), \beta(x) \rangle$ is acceptable if there exists a strongly first-order definable family of functions $f^{(d)}$, $d \in \omega$, such that for all sufficiently large integers $d \in \omega$, for all nonnegative integers $j \leq \alpha(d)$, and for all $a \in \mathtt{seq}(j, 2^{\beta(d)})$, we have $\mathbf{P}a = f^{(d)}(a)$. □

The following two lemmas are proved in [6]. The second lemma is a special case of the first one.

Lemma 68 *For each fixed $c > 0, \varepsilon > 0$ the pair $\alpha(x) = x^c$, $\beta(x) = 2^{x+x^{1-\varepsilon}}$ is acceptable.*

Lemma 69 *For all $\varepsilon > 0$ there exists a family of functions $f^{(d)}$, $d \in \omega$, such that, for all sufficiently large $d \in \omega$ if $a = \langle a_0, a_1 \rangle \in \mathtt{seq}(2, 2^{2^{d+d^{1-\varepsilon}}})$, then $a_0 a_1 = f^{(d)}(a)$.*

Using Lemma 69 we can show that condition (121) is satisfied by $f = \times$. If d is sufficiently large and $d + \chi \leq \mathcal{J}(d) \leq d + c \log\log d$ then $d + d^{\frac{1}{2}} > d + \chi$ and therefor Lemma 69 implies that, multiplication in $\mathbf{M}_{d+\chi}$ can be defined in $\mathbf{M}_d$ in the sense of (121). This completes the proof of (121) for $f = \times$.

Now we prove condition (121) for $f = \div$. We follow the technique used by Beame, Cook, and Hoover (see [9]) for performing integer division by small depth circuits. Namely, we reduce integer division to multiplication and addition by approximating the function $\frac{1}{1-x}$ with an initial segment of its Taylor series.

Assume that d is sufficiently large, $d + \chi \leq \mathcal{J}(d) \leq d + c \log\log d$, $a, b \in \mathbf{M}_{d+\chi}$, and we want to define $\lfloor a/b \rfloor$ in $\mathbf{M}_d$ in a first-order way. First we describe a way, using general mathematical language, to compute $\lfloor a/b \rfloor$ and then we show that this can be translated into the formula Φ'_f required in (121). We will use the notation $2^d = n$ and $2^\chi = \nu$.

(i) First we note that it is sufficient to find integers t, l such that $\frac{1}{b} - t2^l < 2^{-\nu n-1}$. The reason for this is that in the possession of the integers t, l we can compute $\alpha = at2^l$ and $|\alpha - \lfloor a/b \rfloor| < a2^{-\nu n-1} < 2^{\nu n}2^{-\nu n-1} \leq \frac{1}{2}$ so we get $\lfloor a/b \rfloor$ by rounding.

(ii) Let k be an integer so that $1 > 2^{-k}b > 1/2$. If there exists no integer with this property then the problem is trivial, since we can get the binary bits of $\lfloor a/b \rfloor$ form the bits of a simply by shift and the erasure of a block of consecutive bits. Let $u = 2^{-k}b$. Since $1 > u > \frac{1}{2}$, we have $1 < \frac{1}{u} < 2$. We may write $\frac{1}{u}$ in the form of $v2^{-(n+2)} + R$, where $v \in [0, 2^{n+2}]$ is an integer and $0 \leq R < 2^{-n-1}$. (v will be determined by the first $n+1$ bits of $\frac{1}{u}$, and R is what remains from $\frac{1}{u}$ after erasing these bits.) Let $z = v2^{-(n+2)}$. The definition of v implies that $0 \leq z \leq 2$.

(iii) We have $zb = 1 + Rz = 1 + r$, where $|r| < 2^{-n+1}$. We consider the series $\frac{1}{zb} = \frac{1}{1-(1-zb)} = \frac{1}{1-(-r)} = 1 - r + r^2 - r^3 + \ldots$. Let w be the sum of the first 4ν terms of this geometric series. Clearly $w = \frac{1}{zb} + R_1$, where $|R_1| < 2^{-3\nu n}$. Consequently $\frac{1}{b} = z\frac{1}{zb} = z(w - R_1) = zw + R_2$, where $|R_2| < 2^{-2\nu n}$.

Now we show that all of the quantities in this computation can be defined in a first-order way in $\mathbf{M}_d$.

Stage (i). The definition of t and l will be described later. However if we have t and l Lemma 69 implies that we may define the product $at2^l$ in a first-order way in $\mathbf{M}_d$. The rounding also can be done in a first-order way.

Stage (ii). The integer v has only $n+2$ bits. In $\mathbf{M}_d$ we can quantify n bits with a single existential quantifier, therefore v with the given property is first-order definable in $\mathbf{M}_d$.

Stage (iii). Lemma 69 implies that the product zb can be defined in $\mathbf{M}_d$. Using Lemma 67 we get that r can be defined as well. Each needed terms of the geometric series can be defined in $\mathbf{M}_d$, we define the ith term as a product with i factors. Since $\nu = 2^\chi \leq 2^{c \log\log n} \leq (\log n)^c$, Lemma 68 implies that the bits of such a product can be defined in $\mathbf{M}_d$ and by Lemma 67 the bits of the sum of the first 4ν terms can be defined as well. Therefore we defined w and by Lemma 69 we can define zw as well. This completes the proof of the fact that condition (121) is satisfied by $f = \div$, and also the proof of $\mathcal{J}$-predictivity of $\mathbf{M}$. *Q.E.D.*(Lemma 64)

10 The Conclusion of the Proof of Theorem 3

Definition. 1. Assume that α, k are positive integers. The geometric sequence $\langle \alpha, \alpha^2, \ldots, \alpha^k \rangle$ will be denoted by $\mathtt{gseq}(k, \alpha)$.

2. Assume that $M, j_m, ..., j_1$ are positive integers. The set of all prenex first-order formulas φ of $\mathcal{M}$ satisfying the following two conditions will be denoted by $\mathbf{L}(M, j_m, ..., j_1)$.

(122) *if the quantifier pattern of φ is $\langle \iota_k, ..., \iota_1 \rangle$ then $k \leq m$ and $\iota_{k-i} \leq j_{m-i}$ for all i=0,...,k-1.*

(123) *if $\varphi \equiv Q_r x_r, ..., Q_1 x_1 P(x_r, ..., x_1)$, where $Q_r, ..., Q_1$ are quantifiers and P is a propositional formula of $\mathcal{M}$ then $\mathtt{length}(P(x_1, ..., x_r)) \leq M$*

The set of all prenex formulas $\varphi \in \mathtt{SForm}(\mathcal{M})$ satisfying these two conditions will be denoted by $\bar{\mathbf{L}}(M, j_m, ..., j_1)$ □

Remark. The definitions of sets $\mathtt{Form}(M, j_m, ..., j_1)$ and $\mathbf{L}(M, j_m, ..., j_1)$ are similar but they are not the same. The set $\mathtt{Form}(M, j_m, ..., j_1)$ contains prenex formulas φ whose quantifier pattern is exactly $\langle j_m, ..., j_1 \rangle$, while in the case of $\mathbf{L}(M, j_m, ..., j_1)$, the sequence $\langle j_m, ..., j_1 \rangle$ is only an upper bound, in some sense, on the quantifier pattern of φ. Apart from that, in the case of $\mathtt{Form}$, M is an upper bound on the circuit size of the propositional part of φ, and in the case of $\mathbf{L}$ it is an upper bound on the length of the propositional part.

Lemma 70 *There exists a $c > 0$ such that if Φ_0, Φ_1 are prenex first-order formulas of $\mathcal{M}$, $m \in \omega$, $M \geq 1$, $\beta \geq 2$, $\Phi_0, \Phi_1 \in \mathbf{L}(M, \mathtt{gseq}(r, \beta))$ and φ is one of the formulas formulas $\Phi_0 \wedge \Phi_1$, $\Phi_0 \vee \Phi_1$, $\neg \Phi_0$ then there exists a prenex first-order formula $\psi \in \mathbf{L}(2M+c, \mathtt{gseq}(r+4, \beta))$ such that $\vdash \varphi \leftrightarrow \psi$.*

Proof of Lemma 70. We consider only the $\varphi \equiv \Phi_0 \wedge \Phi_1$ case, the other logical connectives can be handled in a similar way. Assume that for $i = 0, 1$,

$$\Phi_i \equiv Q_{m_i,i} \vec{x}_{m_i,i}, ..., Q_1 \vec{x}_{1,i}, P(\vec{x}_{m_i,i}, ..., \vec{x}_{1,i})$$

where $\vec{x}_{j,i}$, $j = m_i, ..., 1$ is sequence of variables, and $Q_{k,i}$ are quantifiers for $k = m_i, ..., 1$. The length of the sequence of variables $\vec{x}_{j,i}$ will be denoted by $l_{i,j}$.

Our assumptions imply that $l_{i,j} \leq \beta^{m_i - j + 1}$ for $i = 0, 1$, $j \in m_i, ..., 1$. First we choose a $c' \in \{1, 2\}$ such that for all integers $j \in \omega$, if $Q_{j,0}$ and $Q_{j+c',1}$ are defined, then they are quantifiers of the same type. When forming the prenex form of $\Phi_0 \wedge \Phi_1$, we will combine the quantifiers $Q_{j,0}$ and $Q_{j+c',1}$ and the variables bound by them into a single block for all $j \in \omega$, provided that both blocks are defined. If one of these blocks is not defined then we use the other block alone. The assumption $\beta \geq 2$ implies that if the prenex form Φ of $\Phi_0 \wedge \Phi_1$ constructed this way has a quantifier pattern $j_m, ..., j_1$, then $\mathtt{length}(\Phi) \leq 2M + c$ and $j_{m-r} \leq \beta^r$ for $r = 0, ..., m-1$. *Q.E.D.*(Lemma 70)

Lemma 71 *For all $\alpha, \beta \in \omega$ there exists a $\gamma \in \omega$ such that the following holds. Assume that*

(124) $\Phi(x_0, \ldots, x_{k-1}, Y_0, \ldots, Y_{l-1}) \in \mathtt{SForm}(\mathcal{M})$, *with* $\mathtt{length}(\Phi) \leq \alpha$, *where $x_0, \ldots, x_{k-1}$, are first-order variables, and $Y_0, \ldots, Y_{l-1}$ are second-order variables, for k-ary relations,*

(125) $m, r \in \omega$, $m > 0$, *and* $\Psi_0(x_0, \ldots, x_{k-1}), \ldots, \Psi_{l-1}(x_0, \ldots, x_{k-1}) \in \mathbf{L}(m, \mathtt{gseq}(r, \beta))$,

Then there exists a first-order prenex formula $\Theta(x_0, ..., x_{k-1}) \in \mathbf{L}(\gamma m, \mathtt{gseq}(r+\gamma, \beta))$. of $\mathcal{M}$ such that

(126) $\Theta(x_0, \ldots, x_{k-1})$ *is logically equivalent to the formula that we get from Φ by substituting Ψ_i for Y_i for all $i \in l$, that is,*

$$\vdash \Theta \leftrightarrow \Phi(x_0, \ldots, x_{k-1}, \Psi_0(x_0, \ldots, x_{k-1}), \ldots, \Psi_{l-1}(x_0, \ldots, x_{k-1}))$$

Proof of Lemma 71. Assume that $\Phi(x_0, ..., x_{k-1}, Y_0, ..., Y_{l-1}) \equiv Q_0 y_0, ..., Q_{t-1} y_t, P(y_0, ..., y_{t-1}, x_0, ..., x_{k-1}, Y_0, ..., Y_{l-1})$, where $Q_0, ..., Q_{t-1}$ are quantifiers, P is a propositional formula, and $t \leq \alpha$. It is sufficient to show that

(127) *there exists a prenex formula Θ' with*

$$\vdash \Theta' \leftrightarrow P(y_0, ..., y_{t-1}, x_0, \ldots, x_{k-1}, \Psi_0, \ldots, \Psi_{l-1})$$

such that $\Theta' \in \mathbf{L}(\gamma' m, \mathtt{gseq}(r+\gamma', \beta))$ for a suitably chosen $\gamma' \in \omega$ which depends only on α and β.

We prove condition (127) by induction on the depth d of the formula P. We will denote by γ'_d the integer γ' which satisfies condition (127) if the depth of P is d. (Since $d \leq \alpha$, the integer γ_d remains below a bound depending only on α and β.) Assume that our statement is true for formulas of depth at most $d-1$, and for example, $P(\vec{y}, \vec{x}, \vec{Y}) \equiv P_0(\vec{y}, \vec{x}, \vec{Y}) \wedge P_1(\vec{y}, \vec{x}, \vec{Y})$, and Θ'_i, is a prenex form of $P_i(\vec{y}, \vec{x}, \Psi_0, \ldots, \Psi_{l-1})$ for $i = 0, 1$, where $\Theta_i \in \mathbf{L}(\gamma'_{d-1} m, \mathtt{gseq}(r+\gamma_{d-1}, \beta))$. Lemma 70 implies that $P_i(\vec{y}, \vec{x}, \Psi_0, \ldots, \Psi_{l-1})$ has a prenex form Θ with $\Theta \in \mathbf{L}(2\gamma_{d-1} m + c, \mathtt{gseq}(r + \gamma_{d-1} + 4, \beta)) \subseteq \Theta \in \mathbf{L}(\gamma_d m, \mathtt{gseq}(r + \gamma_d, \beta))$, where $\gamma_d = 2c\gamma_{d-1} + 4$. The recursive definition of γ starting with $\gamma_0 = 1$ implies that $\gamma_d \leq 2^{c_1 d}$ for a suitable chosen constant $c_1 \in \omega$. Since d remains below a bound depending only on α, condition (127) is satisfied by $\gamma' = \gamma_d$. *Q.E.D.*(Lemma 71)

Lemma 72 *Assume that $\mathcal{J}$ is a function, and $\mathbf{M}$ is $\mathcal{J}$-predictive. For all sufficiently large $c_3, c_4 \in \omega$, if $d \in \omega$ is sufficiently large, $r, k \in \omega$, $d \leq r \leq \mathcal{J}(d)$ and $\tau(x_0, \ldots, x_{k-1})$ is a term of $\mathcal{M}$, and $\delta = \mathtt{depth}(\tau)$, then there exists a first-order formula*

$$\lambda(x_0, \ldots, x_{k-1}, y, z) \in \mathbf{L}\Big(c_4^{\delta}, \mathtt{gseq}(c_3\delta, c_4)\Big)$$

with the property that for all $a_0, \ldots, a_{k-1}, b \in \mathbf{M}_d$,

$$\mathbf{M}_r \models b = \tau(a_0, \ldots, a_{k-1}) \quad \leftrightarrow \quad \mathbf{M}_d \models \lambda(a_0, \ldots, a_{k-1}, b, r)$$

To make an inductive proof possible we prove the lemma in a slightly stronger form stated in the following lemma. That lemma says that the terms of $\mathcal{M}$ has the property which was formulated only for the operations of $\mathcal{M}$ in the definition of predictivity. Moreover we also state an upper bound on the quantifier patterns of the formulas involved in this property.

Lemma 73 *Assume that $\mathcal{J}$ is a function, and $\mathbf{M}$ is $\mathcal{J}$-predictive. Then for all sufficiently large $c_3, c_4 \in \omega$ the following holds. Suppose that $d, r, k \in \omega$ with $d \leq r \leq \mathcal{J}(d)$, $\eta_{d,r}$ is the function whose existence is stated in the definition of $\mathcal{J}$-predictivity, and $\tau(x_0, \dots, x_{k-1})$ is a term of $\mathcal{M}$ with $\mathtt{depth}(\tau) = \delta$. Then there exists a formula $\Psi_\tau(x, y, z, Z_0, \dots, Z_{k-1}) \in \mathtt{SForm}(\mathcal{M})$, where x, y, z are free first-order variables and $Z_0, \dots, Z_{k-1}$ are free variables for binary relations, such that*

$$\Psi_\tau(x, y, z, Z_0, \dots, Z_{k-1}) \in \bar{\mathbf{L}}\Big(c_4^\delta, \mathtt{gseq}(c_3\delta, c_4)\Big)$$

and the following condition is satisfied:

(128) *for all $a_0, \dots, a_{k-1}, u, v \in \mathbf{M}_d$, the following two statements are equivalent:*
(i) $(\eta_{d,r}(b))(u, v)$, *where b is the unique element of $\mathbf{M}_r$ with $\mathbf{M}_r \models b = \tau(a_0, \dots, a_{k-1})$,*
(ii) $\mathbf{M}_d \models \Psi_\tau(u, v, r, \eta_{d,r}(a_0), \dots, \eta_{d,r}(a_{k-1}))$.

Proof of Lemma 73. We prove the lemma by induction on $\mathtt{depth}(\tau)$. If $\mathtt{depth}(\tau) = 0$, then τ is either a constant symbol $\mathbf{c}$ or a variable x_i for some $i \in k$. In the former case the formula Ψ_τ is identical to the formula $\Phi_{\mathbf{c}}$ whose existence is guaranteed in the definition of $\mathcal{J}$-predictivity. If $\tau = x_i$ then $\Psi_\tau(x, y, z, Z_0, \dots, Z_{k-1}) \equiv Z_i(x, y)$.

Assume now that $i > 0$ and the Lemma is true if the depth of τ is at most $i-1$. We may assume that all of the function symbols of $\mathcal{M}$ are binary (e.g., a unary function symbol can be replaced by a binary which does not depend on its second variable). Suppose that the term τ is of the form $\mathbf{f}(\tau_0(x_0, \dots, x_k), \tau_1(x_0, \dots, x_k))$, where $\mathbf{f}$ is a binary function symbol of $\mathcal{M}$. Then $\Psi_\tau(x, y, z, Z_0, \dots, Z_{k-1})$ is defined in the following way. We will use the notation $\Phi_{\mathbf{f}}$ from the definition of $\mathcal{J}$-predictivity, if $\mathbf{f}$ is a function symbol of $\mathcal{M}$. For all $i = 0, 1$, the relation symbol Y_i may occur in the formula $\Phi_{\mathbf{f}}(x, y, z, Y_0, Y_1)$ several times. Assume that the jth occurrence of the variable Y_i is contained in a subformula of the form $Y_i(\sigma_{j,0}, \sigma_{j,1})$, where $\sigma_{j,0}, \sigma_{j,1}$ are terms of $\mathcal{M}$. We replace each subformula $Y_i(\sigma_{j,0}, \sigma_{j,1})$ of $\Phi_{\mathbf{f}}(x, y, z, Y_0, Y_1)$ by the formula $\Psi_{\tau_i}(\sigma_{j,0}, \sigma_{j,1}, z, Z_0, \dots, Z_{k-1})$. The formula obtained this way will be $\Psi_\tau(x, y, z, Z_0, \dots, Z_{k-1})$. The definition of the formula $\Phi_{\mathbf{f}}$ and the inductive assumption together imply that the formula Ψ_τ satisfy condition (128). The property $\Psi_\tau(x, y, z, Z_0, \dots, Z_{k-1}) \in \bar{\mathbf{L}}\Big(c_4^\delta, \mathtt{gseq}(c_3\delta, c_4)\Big)$ follows from the inductive assumption and Lemma 71. *Q.E.D.*(Lemma 73)

Proof of Lemma 72. The lemma is a consequence of Lemma 73. In the conclusion (128) of Lemma 73 we have the formula $\Psi_\tau(u, v, r, \eta_{d,r}(a_0), \dots, \eta_{d,r}(a_{k-1}))$. Since $a_i \in \mathbf{M}_d$ for $i \in k$, the definition of $\mathcal{J}$-predictivity implies that $\eta_{d,r}(a_i)(x, y) \equiv x = \mathbf{0} \wedge y = a_i$. Therefore we have a first-order formula ψ_τ of $\mathcal{M}$ such that for all $a_0), \dots, a_{k-1} \in \mathbf{M}_d$,

(129) *for all* $u, v \in \mathbf{M}_d$,

$$\Big(\eta_{d,r}\big(\tau(a_0,\dots,a_{k-1})\big)\Big)(u,v) \quad \leftrightarrow \quad \mathbf{M}_d \models \psi_\tau(u,v,r,a_0,\dots,a_{k-1})$$

Therefore $\lambda(x_0,\dots,x_{k-1},y,z) \equiv \forall u,v,\psi_\tau(u,v,z,x_0,\dots,x_{k-1}) \leftrightarrow (u = 0 \wedge v = y)$ meets the requirements of Lemma 72. *Q.E.D.*(Lemma 72)

Lemma 74 *For all sufficiently small* $\varepsilon > 0$ *if* $\mathcal{D}$ *is the function defined by* $\mathcal{D}(x) = \varepsilon(\log x)^{\frac{1}{2}}$ *for all* $x > 0$*, then the* $\mathcal{D}$ *quantifier elimination assumption does not hold for* $\mathbf{M}$.

Proof of Lemma 74. Let $\mathcal{J}$ be the function $\lfloor x + \log x \rfloor$. According to Lemma 64, $\mathbf{M}$ is $\mathcal{J}$-predictive. Therefore Lemma 72 is applicable for the function $\mathcal{J}$. Let $c, \alpha_0 \in \omega$, such that $1 \ll c \ll \alpha_0 \ll \frac{1}{\varepsilon}$. We may suppose that statement of Lemma 72 holds with a choice of c_3 and c_4 such that $c_3, c_4 \ll c$. We may also assume that Lemma 58 holds with the present choice of c, ε and α_0.

Assume that contrary to the statement of the present lemma the $\mathcal{D}$ quantifier elimination assumption holds for $\mathbf{M}$. Then condition (94) of Lemma 58 is satisfied. We choose a $d \in \omega$ such that $\frac{1}{\varepsilon} \ll d$, that is, condition (95) of Lemma 58 is also satisfied by the present choices of the parameters. Let $\delta = \lfloor \mathcal{D}(d + \log d) \rfloor$, $m = \lfloor c\delta \rfloor$, $\iota_{m-i} = c^i$ if $i < \lfloor \delta/2 \rfloor$ and $\iota_{m-i} = c^{\lfloor \delta/2 \rfloor}$ otherwise. Clearly these choices satisfy condition (96) of Lemma 58.

Since all of the assumptions of Lemma 58 are valid for the present choices of the parameters, its conclusion also holds. Let $\mathbf{g}$ be the function and let $\tau(x,y)$ be the term whose existence is stated in Lemma 58.

We have that if $\varphi \in \mathtt{Form}(c^\delta, \iota_m, ..., \iota_1)$ and $q = \rho_m$ then

(130) *for all* $a \in \mathbf{M}_d$,

$$\mathbf{M}_d \models \varphi(a) \quad \leftrightarrow \quad \mathbf{M}_q \models \tau(a, \mathbf{g}(\varphi)) = \mathbf{0}$$

We apply now Lemma 72 with d, $c_3 = c_4 \ll c$, $r{:=}\, q$, $k{:=}\, 2$, $\tau(x_0,\dots,x_{k-1}){:=}\, \tau(x_0,x_1)$. Let $\lambda(x_0,x_1,y,z)$ be the first-order formula whose existence is guaranteed by Lemma 72. The conclusion of Lemma 72 and condition (130) imply that

(131) *for all* $a \in \mathbf{M}_d$,

$$\mathbf{M}_d \models \varphi(a) \quad \leftrightarrow \mathbf{M}_d \models \lambda(a, \mathbf{g}(\varphi), \mathbf{0}, q)$$

Let $\sigma_0(x)$, $\sigma_1(x)$ be terms of $\mathcal{M}$ such that for all $h \in \mathbf{M}_d$ we have

$$\mathbf{M}_d \models \max(\sigma_0(h), \sigma_1(h)) < 2^{2^{d-1}} \wedge \sigma_0(h) + \sigma_1(h) 2^{2^{d-1}} = h$$

For example the terms $\sigma_0(x) = \div(x, 2^{2^{d-1}})$, $\sigma_1(x) = x - \sigma_0(x)$ meet this requirement.

Let $\mu(x,y) \equiv \lambda(x, \sigma_0(y), \mathbf{0}, \sigma_1(y))$. Recall that φ was an arbitrary element of the set $H = \mathtt{Form}(c^\delta, \iota_m, ..., \iota_1)$. For each and $\varphi \in H$ let $\mathbf{G}(\varphi) = \mathbf{g}(\varphi) + q 2^{2^{d-1}}$. According to the definition of the function $\mathbf{g}$ in Lemma 58 $\mathbf{g}(\varphi) < 2^{2^{d-1}}$. Since $q \leq d + \log d$ we have $\mathbf{G}(\varphi) \in \mathbf{M}_d$. Condition (131) and the definition of $\mathbf{G}$ imply that

(132) *for all* $\varphi \in H$ *and for all* $a \in \mathbf{M}_d$,

$$\mathbf{M}_d \models \varphi(a) \quad \leftrightarrow \quad \mathbf{M}_d \models \mu(a, \mathbf{G}(\varphi))$$

Let $\psi(x)$ be the formula of $\mathcal{M}$ defined by $\psi(x) \equiv \neg\mu(x,x)$. We claim that the formula ψ is in the set H. Indeed according to Lemma 72 $\lambda(x_0, x_1, y, z) \in \mathbf{L}\Big(c_4^\delta, \mathtt{gseq}(c_3\delta, c_4)\Big)$ and therefore $\psi(x) \equiv \neg\mu(x,x) \in \mathbf{L}\Big(c_4^\delta + c_5, \mathtt{gseq}(c_3\delta, c_4)\Big)$ where $c_5 \in \omega$ is an absolute constant. The upper bound $c_3 = c_4 \ll c$, and the definition of the integers $\iota_m, ..., \iota_m$, implies that $c_4^k < \iota_{m-k+1}$ for $k = 1, ..., c_3\delta$. Therefore Lemma 62 implies that $\mathbf{L}\Big(c_4^\delta + c_5, \mathtt{gseq}(c_3\delta, c_4)\Big) \subseteq \mathtt{Form}(c^\delta, \iota_m, ..., \iota_1)$. (Here we also used that $\mathtt{csize}(\kappa) \leq \mathtt{length}(\kappa)$ if κ is a term of $\mathcal{M}$.)

The fact $\psi \in H$ and condition (132) leads to a contradiction using Gödel's diagonalization argument. Namely, we have by the definition of ψ that $\mathbf{M}_d \models \psi(\mathbf{G}(\psi)) \leftrightarrow \neg\mu(\mathbf{G}(\psi), \mathbf{G}(\psi))$. On the other hand condition (132) with $\varphi{:=}\,\psi$, and $a{:=}\,\mathbf{G}(\psi)$ yields $\mathbf{M}_d \models \psi(\mathbf{G}(\psi)) \leftrightarrow \mu(\mathbf{G}(\psi), \mathbf{G}(\psi))$, that is we have $\mathbf{M}_d \models \mu(\mathbf{G}(\psi), \mathbf{G}(\psi)) \leftrightarrow \neg\mu(\mathbf{G}(\psi), \mathbf{G}(\psi))$ a contradiction. *Q.E.D.*(Lemma 74)

Proof of Theorem 3. Assume that the statement of the theorem is not true. This implies that for all $\varepsilon > 0$, and for all terms $F(x,y)$ of $\mathcal{M}$ there exists a sequence of terms $G = \langle G_d(y) \mid y \in \omega \rangle$ such that G decides whether there exists a solution for F and the depth of G_d is smaller than $\varepsilon(\log d)^{\frac{1}{2}}$ for all sufficiently large $d \in \omega$. Since for each propositional formula $P(x,y)$ of $\mathcal{M}$ there exists a term $F(x,y)$ of calm such that for all $d \in \omega$, $\mathbf{M}_d \models \forall x, y, P(x,y) \leftrightarrow F(x,y) = 0$ we get that for all $\varepsilon > 0$ if $\mathcal{D}(x) = \varepsilon(\log d)^{\frac{1}{2}}$ then the $\mathcal{D}$ quantifier elimination assumption holds for $\mathbf{M}$. This however contradicts to Lemma 74. *Q.E.D.*(Theorem 3)

11 Random Access Machines

A detailed description of the random access machines N_n is given in [5].

Proofs of Theorems 1 and 2. Theorems 1 and 2 are simple consequences of Theorem 3. We describe here the proof Theorem 1 and indicate the only place where it has to be changed to get a proof of Theorem 2. In this description if $d \in \omega$ the symbol n always will denote the integer 2^d even if we do not say it explicitly. We assume that Theorem 1 is not true and show that Theorem 3 cannot be true either.

We will consider programs R running on N_n which get only k integers in 2^n as input, where $k = 1$ or $k = 2$. For the sake of simplicity we assume that these integers are already given as the contents of memory cells $\bar{c}$ and (possibly) $\bar{c} + 1$ at time 0 when the machine start working, where $\bar{c}$ is a constant.

Assume that $F(x, y)$ is an arbitrary term of $\mathcal{M}$ and $\varepsilon > 0$. Using the assumption that Theorem 1 is not true, we construct a sequence of terms $G = \langle G_d \mid d \in \omega \rangle$, such that G decides whether there exists a solution for F, and for all sufficiently large $d \in \omega$, $\mathtt{depth}(G_d) \leq \varepsilon(\log d)^{\frac{1}{2}}$.

The definitions of the $\mathcal{M}$ operations in the structures $\mathbf{M}_d$ imply that there exists a $c > 0$ and c-size binary test P, with time requirement c on each machine N_n, such that for all $d \in \omega$, and $a, b \in 2^n$, $P_n(b, a) = 0$ if $\mathbf{M}_d \models F(a, b) = 0$, and $P_n(b, a) = 1$ otherwise. (The program P computes the value of $F(a, b)$ and checks whether it is 0.) If Theorem 1 is not true then there exists a $c' \in \omega$, and a c'-size unary test Q such that for all sufficiently large $d \in \omega$, the time requirement of Q on N_n is at most $\varepsilon'(\log d)^{\frac{1}{2}}(\log d)^{-1}$, and for all sufficiently large $d \in \omega$, $Q_n(a) = 0$ iff $\exists x \in 2^n, P_n(x, a) = 0$, where $\varepsilon' > 0$ is a sufficiently small constant with respect to ε. We construct, for each sufficiently large $d \in \omega$, an $\mathcal{M}$-circuit C_d such that at the input a, C_d gives the same output as the program Q on N_n, and the depth of C_d is at most $c_1\varepsilon(\log d)^{\frac{1}{2}}$, where c_1 is a constant which does not depend on ε or ε'. The existence of such an $\mathcal{M}$ circuit C_d implies a term G_d with the same depth which meets our requirements. (Each $\mathcal{M}$ circuit can be transformed into a functionally equivalent $\mathcal{M}$ term without an increase in the depth, of course the size of the term may be much larger than the size of the circuit). For the construction of C_d first we replace Q by another program Q' which has the same input-output behavior as Q and satisfies the following condition. There exists a $c_2 \in \omega$ such that for all $n \in N$:

(a) the size of Q' is less than c_2,

(b) if Q', while running on N_n, executes an instruction I which involves the memory cell i for some $i \geq c_2$, then instruction I is either a write instruction or a read instruction. (A memory cell is involved an an instruction if either its content influences what happens when the instruction is executed or its content may change when the instruction is executed.)

(c) the time requirements of Q' on N_n is larger that the time requirement of Q on N_n at most by a factor of c_2.

It is easy to see, using only the definition of a RAM, that such a program Q' exists. (In the case of Theorem 2 the program Q is of length l, where the integer l may depend on n. In this case we substitute first Q by a program Q_0 of constant length which gets an

input of length l which is written in the memory at time 0.) We claim now that if $n = 2^d$ and the time requirement of Q' on N_n is t_n then we can simulate Q' running on N_n, by an $\mathcal{M}$ circuit of C_d of depth at most $O(t_n \log t_n)$, whose gates perform operations in $\mathbf{M}_d$.

The set of nodes of the $\mathcal{M}$-circuit C_d will be denoted by $\mathcal{Q}$. For a given input a of the circuit C_d, we may evaluate the circuit, and this evaluation assigns a value $\chi(a, u)$ for each node u of $\mathcal{Q}$, which is the value computed by the gate at node u if the input is a. For each $s \in t_n$ and $i \in c_2$ the set $\mathcal{Q}$ will have an element $u_{s,i}$, and for each $\delta \in \{0, 1, 2\}$ and $s \in t_n$ the set $\mathcal{Q}$ will have an element $v_{s,\delta}$. (The set $\mathcal{Q}$ will have other elements as well.) We will define the circuit in a way that if at input a and at time $s \leq t_n$, while Q' is running on N_n, the content of cell i for some $i < c_2$ is w then $\chi(a, u_{s,i}) = w$. The nodes $v_{s,\delta}$ for $i > c_2$, $s \in t_n$ will be used in the following way. If at time s while Q' is running on N_n, the machine performs a write write instruction, and it writes the integer x in cell j then $\chi(a, v_{s,0}) = x$, $\chi(a, v_{s,1}) = j$, and $\chi(a, v_{s,2}) = 1$. If at time s the machine does not perform a write instruction then $\chi(a, v_{s,0})) = \chi(a, v_{s,1}) = \chi(a, v_{s,2}) = 0$.

First we note that the existence of a circuit C_d with these properties and the required bound on its depth implies the theorem. Indeed since at the nodes $u_{s,i}$ we have the contents of the first c_2 memory cells at each time, we have the output of the program Q' as well.

We claim that for all $s \in t_n$ there exists an $\mathcal{M}$ circuit D_s of depth at most $O(t_n \log t_n)$ such that given $\chi(a, u_{s,i})$, $\chi(a, v_{r,\delta})$, $i \in c_2, r \in [0, s]$, $\delta \in \{0, 1, 2\}$ as input the circuit gives as output the values $\chi(a, u_{s+1,i})$, $\chi(a, v_{s+1,\delta})$, $i \in c_2$, $\delta \in \{0, 1, 2\}$. Clearly the existence of such circuits D_s imply the existence of the circuit C_d with the required properties.

Assume that at time s instruction I is executed. We distinguish two cases according to whether I is a read instruction or not.

(i) if I is not a read instruction then it is easy to see that condition (b) implies that for each fixed $i \in c_2$, $\delta \in \{0, 1, 2\}$ the earlier specified values of $\chi(a, u_{s+1,i})$ and $\chi(a, v_{s+1,\delta})$ can be computed by a constant depth $\mathcal{M}$ circuit $B_{s,i,\delta}$ from the input $\chi(a, u_{s,i})$. $i \in c_2$, $\delta \in \{0, 1, 2\}$.

(ii) if I is a read instruction which reads the content of cell j then we need a circuit which determines which is the largest integer $r \leq s$ such that $\chi(a, v_{r,1}) = j$, $\chi(a, v_{s,2}) = 1$, and for this integer r, $\chi(a, v_{r,1})$ will be the current content of cell j. (If there is no such r then it will be the content of cell j at time 0). Since the total number of nodes needed for this is at most $O(t_n)$, this can be done by a circuit of depth at most $O(\log t)$. The circuits in case (i) and case (ii) can be combined into a single circuit which first checks whether I is a read instruction. According to condition (b) this can be done in constant depth.

Since the number of possible values for s is at most t_n this construction gives the required circuit with depth $O(t_n \log t_n)$. *Q.E.D.*(Theorem 1 and Theorem 2)

12 NP-completeness, proof of Theorem 5

Proof of Theorem 5. The theorem is a consequence of Lemma 43. The following problem is clearly NP-complete with a suitable choice of the finite automaton $\mathcal{A}$. The size of the problem is m. Let $u = \lfloor \log_2(m/3) \rfloor$, $d = u$. Let $\mathcal{T}$ be a restricted turing machine with $\mathtt{aut}(\mathcal{T}) = \mathcal{A}$, $\mathtt{width}(\mathcal{T}) = 1$, $\mathtt{tplength}(\mathcal{T}) = 2^u$.

Suppose that an $b \in 2^{2^d-1}$ is given, decide whether there exists an $a \in 2^{2^d-1}$ such that the a is a possible u-based input for the turing machine $\mathcal{T}$ and if restricted turing machine $\mathcal{T} = \langle A, 2^t \rangle$ starts to work with u-based input a, then $b = \sum_{j=0}^{2^{d-u}-1} \mathtt{cont}_{T,j,0} 2^{j2^u}$, where $T = 2^{d-u}$. (That is, the machine with the input described by a reaches a state described by b at time T.)

Lemma 43 implies that there exists an existential formula ψ of $\mathcal{M}$ such that for all $u \in \omega$, and for all $b \in 2^{2^d-1}$ the problem described above has a solution iff $\mathbf{M}_{c'u} \models \psi(b, u)$, where $c' \in \omega$ is a sufficiently large constant. The condition $\mathbf{M}_{c'u} \models \psi(b, u)$ is equivalent to $\mathbf{M}_{c'u} \models \exists x, 2^x = \mathbf{n} \wedge \psi(b, \dot{-}(x, c'))$. Therefore there exists an existential formula ψ' of $\mathcal{M}$ such that for all $u \in \omega$, and for all $b \in 2^{2^d-1}$ the problem described above has a solutioniff $\mathbf{M}_{c'u} \models \psi'(b)$.

The formula ψ' may have more than one existential quantifiers. However Lemma 37 implies that there exists an existential formula φ of $\mathcal{M}$ with a single existential quantifier such that if $c = 2c'$, then $\mathbf{M}_{c'u}\psi'(b)$ is equivalent to $\mathbf{M}_{cu} \models \varphi(b)$. Therefore for a suitable chosen term τ of $\mathcal{M}$ this can be written in the form of $\mathbf{M}_{cu} \models \exists x, \tau(x, b)$. Therefore we have reduced our the NP-complete problem about turing machines to an instance of the problem that we called "the solution of the equation $\tau(x, b) = 0$ in x". Moreover, since we are looking for a solution in $\mathbf{M}_{cu}$ the size of the problem is $2^{cu} \leq 2^{c \log_2 m} = m^c$. *Q.E.D.*(Theorem 5)

References

[1] A.V. Aho, J.E. Hopcroft, J.D. Ullman, *The Design and Analysis of Computer Algorithms*, Addison-Wesley, 1974.

[2] M. Ajtai. *Detreminism versus Nondeterminism with Arithmetic Tests and Computation*, Proceedings of the 44th ACM Symposium on Theory of Computing, STOC 2012, New York, NY, USA, June 2012, pages 249-268 ACM, 2012.

[3] M. Ajtai, *Determinism versus Nondeterminism for Linear Time RAMs with Memory Restrictions*, Journal of Computer and Systems Science, 65(1): 2-37, (2002)

[4] M. Ajtai, *Oblivious RAMs without cryptographic assumptions*, Electronic Colloquium on Computational Complexity (ECCC), 17:28, 2010.

[5] M. Ajtai. *Oblivious RAMs without cryptographic assumptions*, Proceedings of the 42nd ACM Symposium on Theory of Computing, STOC 2010, Cambridge, Massachusetts, USA, 5-8 June 2010, pages 181–190. ACM, 2010.

[6] M. Ajtai. *Determinism versus Nondeterminism with Arithmetic Tests and Computation*, Proceedings of the 44nd ACM Symposium on Theory of Computing, STOC 2012, New York, NY, USA, May 2012, pages 249-268. ACM, 1012.

[7] M. Ajtai, Y. Gurevich, *Monotone versus positive*, Journal of the ACM (JACM), Vol. 34, Issue 4, Oct. 1987, pp. 1004-1015.

[8] E. Artin. *Galois Theory*, Dover Publications, 1998. (Reprinting of second revised edition of 1944, The University of Notre Dame Press).

[9] P. Beame, S. A. Cook, and H. J. Hoover, Log Depth Circuits for Division and Related Problems, SIAM Journal on Computing, 15(4):994-1003, November 1986.

[10] P. Beame, T. S. Jayram, M. Sacks, *Time-space tradeoffs for branching programs*, Journal of Computer and Systems Science, 63(4):542-572, December 2001.

[11] P. Beame, M. Sacks, Xiadong Sun, E. Vee, *Time-space trade-off lower bounds for randomized computation of decision problems*, Journal of ACM, 50(2):154-195, 2003.

[12] M. Davis, H. Putnam and J. Robinson, *The decision problem for exponential diophantine equations*, Ann. of Math. (2) 74 (1961), 425-436.

[13] J.E. Hopcroft, W. Paul, L. Valiant. *On Time versus Space.* Journal of ACM, Vol. 24 Issue 2, April 1977, pp. 332-337.

[14] A. Magid, *Differential Galois theory*, Notices of the American Mathematical Society 46 (9): 1999.

[15] L. Fortnow, *Time-space tradoffs for satisfiability*, Journal of Computer and System Sciences, 60:337-353, 2000.

[16] Ju. V. Matijasevic, *Enumerable sets are diophantine*, Dokl. Akad. Nauk SSSR 191 (1970), 279-282. English transi.: Soviet Math. Doklady 11 (1970), 354-358.

[17] W. Paul, N. Pippenger, E. Szemerédi, and W. Trotter. *On determinism versus non-determinism and related problems*, In Proceedings of the 24th IEEE Symposium on Foundations of Computer Science, pages 429-438. IEEE, New York, 1983.

[18] G. Takeuti, *Proof Theory*, North-Holland, Studies in Logic and the Foundations of Mathematics, Vol. 81, Second edition, 1987.

[19] A. Yao *Separating the polynomial time hierarchy by oracles*, Proc. 26th Annu. IEEE Symp. Found. Comp. Sci. 1-10 (1985).

ECCC ISSN 1433-8092

http://eccc.hpi-web.de