Electronic Colloquium on Computational Complexity, Report No. 102 (2011)

Determinism versus Nondeterminism with Arithmetic Tests and Computation

Miklós Ajtai
IBM Research, Almaden Research Center

July 30, 2011

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 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 $\lfloor x/y \rfloor$, $\max(x, y)$, $\min(x, y)$, 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 by a single instruction. We show that there exists 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 for all terms $G(y)$, which is also built up from the mentioned operations, the following holds. For infinitely many positive integers d, there exists an $a \in \mathbf{M}_d$ such that the following two statements are not equivalent: (i) $\mathbf{M}_d \models \exists x, F(x, a)$, (ii) $\mathbf{M}_d \models G(a) = 0$. In other words, the question whether an existential statement, depending on the parameter $a \in \mathbf{M}_d$ is true or not, cannot be decided by evaluating an algebraic expression at a.

We also show that this theorem remains true if we include the operation $\min\{x^y, 2^n - 1\}$ into the structure $\mathbf{M}_d$. A general theorem is proved as well which describes sufficient conditions for a set of operations on a sequence of structures $\mathbf{K}_d$, $d = 1, 2, ...$ which guarantees that the analogue of the mentioned theorem holds for the structure $\mathbf{K}_d$ too.

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.

ISSN 1433-8092

In this paper we consider the special case of this problem where both the test and the search consist of the evaluation of an algebraic expression. Assume that S is an algebraic structure with the operations $s_1, s_2, \ldots, s_k$. For example, S can be a field or a ring and $s_1, \ldots, s_k$ can be the field/ring operations. We also assume that the structure S has a distinguished element (defined as the value of a 0-ary operation s_i for some $i = 1, \ldots, k$) that we will denote by $\mathbf{0}$. In the case of a field/ring, $\mathbf{0}$ will be always the usual zero of the field/ring. Suppose further that $F(x, y)$ is an algebraic expression built up from the operations $s_1, \ldots, s_k$. Our search problem will depend on a parameter $a \in S$. If such an $a \in S$ is fixed, then we want to find $x \in S$ such that $F(x, a) = \mathbf{0}$. That is, the test T consists of checking whether for a given x we have $F(x, a) = \mathbf{0}$. We will say that the problem has an algebraic solution, if there exists an algebraic expression $G(y)$ built up from the operations $s_1, \ldots, s_k$ such that G depends only on F, and for all $a \in S$ the following two statements are equivalent: (i) there exists an $x \in S$ with $F(x, a) = \mathbf{0}$, and (ii) $F(G(a), a) = 0$. In other words if the equation $F(x, a)$ has a solution in x then $x = G(a)$ is such a solution.

Alternately we will also consider the problem of deciding whether the equation $F(x, a)$ has a solution in S. In this case we will say that the problem can be decided by an algebraic expression if there exists an algebraic expression $G(y)$ such that for all $a \in S$, the equation $F(x, a)$ has a solution in x iff $G(a) = \mathbf{0}$.

Several classical problems of mathematics can be formulate in this framework. For example, if S is the field of real numbers and $F(x, a) = x^2 - a$ then there is no $G(y)$ built up from the field operations so that for all $a \geq 0$, $x = G(a)$ is a solution of $F(x, a) = 0$. Indeed for a rational a the value of $G(a)$ is also rational while e.g., for $a = 2$ all of the solutions, namely $\pm\sqrt{2}$, are irrational. This was proved already by Pythagoras.

A more difficult problem if S is the field of complex numbers (or any other algebraically closed field), and the operations are the field operations and taking kth roots for each positive integer k. It is a consequence of Galois theory (see [6]) that there is an equation $F(x, a) = 0$ whose solution cannot be expressed by the given operation, so there is no algebraic expression $G(y)$ with the required properties. (Actually such an F can be constructed without using the "taking k-th root" operations.) Another example of similar nature is the problem of finding the antiderivative of an elementary function. We do not describe here the structure S, we just note that the basic results, that is, the existence of an elementary function whose antiderivative is not an elementary function (see e.g., [10]), can be also expressed in the present framework.

In this paper we consider the analogue questions in finite structures which, apart from the ring operations also contain other operations on integers which are used as instructions in random access machines. For each positive integer d we will consider a structure $\mathbf{M}_d$ whose universe is the set $\{0, 1, \ldots, 2^n - 1\}$, where $n = 2^d$. An element b of $\mathbf{M}_d$ is a natural number but sometimes we will consider it as a $0, 1$-sequence of length n, defined by the binary form of b. The operations on $\mathbf{M}_d$ will be, roughly speaking, the operations that a random access machine would be able to perform on nonnegative integers represented by n bits, where $n = 2^d$. Namely we assume that the operations of $\mathbf{M}_d$ are the following: (1) addition and multiplication modulo 2^n, (2) integer division, that is, the operation $\lfloor \frac{x}{y} \rfloor$, (3) $\max(x, y), \min(x, y)$, (4) an operation $\mathbf{p}(x)$ whose value is $\min\{2^x, 2^n - 1\}$, (5) pointwise boolean negation, AND, OR, on $0, 1$-sequences of length n. $\mathcal{M}$ will denote a firstorder language which contains for each of these operations a function symbol with the corresponding arity. Referring to this language the described operations will be called

$\mathcal{M}$-operations. (The results of this paper remain valid if we include a binary operation $\bar{\mathbf{p}}(x, y)$ whose value is $\min\{x^y, 2^n - 1\}$.)

The $\mathcal{M}$-operations that we have in addition to the ring operations, make the extension of the algebraic proofs on Galois theory to the structures $\mathbf{M}_d$ impossible. In spite of that we will show in Theorem 1, that there exists an algebraic expression $F(x, y)$ (built up from $\mathcal{M}$-operations) such that for all algebraic expression $G(y)$, (also built up from $\mathcal{M}$-operations), there exist infinitely many positive integers d such that for a suitably chosen $a \in \{0, 1, \ldots, 2^{2^d} - 1\}$, we have that the following two conditions are not equivalent: (i) $F(x, a)$ has a solution $x \in \mathbf{M}_d$, and (ii) $G(a) = \mathbf{0}$ in the structure $\mathbf{M}_d$.

The proof shows only that statements (i) and (ii) are not equivalent for infinitely many positive integers d, but it seems likely, that there exists an F such that for all sufficiently large integers d and a suitably chosen $a \in \{0, 1, \ldots, 2^{2^d} - 1\}$ they are not equivalent.

The mentioned result is about deciding whether an equation $F(x, a) = \mathbf{0}$ has a solution. However it is easy to see that the result remains valid for the search problem as well.

Of course the set of $\mathcal{M}$-operations is somewhat arbitrary. We may want to know which other operations can be added to $\mathcal{M}$ such that the mentioned theorem remains true. We prove a general theorem, Theorem 2 about a sequence of structures $\mathbf{K}_d$, $d = 1, 2, \ldots$, with $\mathtt{universe}(\mathbf{K}_d) = \{0, 1, \ldots, 2^n - 1\}$, $n = 2^d$ which describes conditions that are sufficient for an analogue of Theorem 1.

The proofs are based on a Gödel type diagonalization argument. Diagonalization has been used for the proof of several theorems about problems which are algorithmically undecidable. E.g., if S is the ring of integers and the operations are the ring operation, then the theorem of Matijasevic, Davis, Putnam, and Robinson about the unsolvability of diophantine equations (see [12], [9]), can be considered in some sense an infinite analogue of the present problem, and has been proved by the method of diagonalization.

Diagonalization has been used in complexity theory to prove various computational lower bounds. From the point of view of this paper the diagonalization method of Fortnow's proof (see [11]) of lower bounds about machines with limited amount of memory is the most relevant. At a very high level our proof has a similar structure: diagonalization which involves the collapse of a hierarchy. In the case of Fortnow's proof this is a hierarchy of certain alternating Turing machines, in the present case it is a hierarchy of firstorder formulas over the structure $\mathbf{M}_d$. The nature of the two problems and the technical details of their solutions, however, are quite different.

There as several theorems in complexity theory which says that in certain restricted computational models nondeterministic computation is much more efficient than deterministic computation. Such a separation has been made for example, for Turing machines (see [13]), and for certain classes of branching programs (see [2], [7], [8]).

A counterexample. In the last section we show that our main result does not hold if we replace the operations in $\mathbf{M}_d$ with arbitrary other operations. We show the following. Assume that a sequence of structures M_n, $n = 1, 2, \ldots$ are given with $\mathtt{universe}(M_n) = \{0, 1, ..., 2^n - 1\}$, where each M_n is an interpretation of a firstorder language $\mathcal{L}$ with equality and with a finite number of constant and functions symbols. We show that there exists an extension $\mathcal{L}'$ of $\mathcal{L}$ with a finite number of function symbols, and for each $n = 1, 2, \ldots$ there exists an interpretation M'_n of $\mathcal{L}'$ which is an extension of M_n on the same universe, such that for all terms $F(x, y)$ of $\mathcal{L}'$,

there exists a term $G(y)$ of $\mathcal{L}'$ with the property that for all sufficiently large $n \in \omega$, we have

$$M'_n \models \forall a, \Big(G(a) = \mathbf{0} \leftrightarrow \exists x, F(x,a) = \mathbf{0}\Big)$$

1.1.1 Further results

In this section we sketch some related results which are not proved in the present paper.

(i) The proof described in the present paper guarantees only the existence of an F, through an indirect argument, it does not tell how to get an explicit expression $F(x,y)$. In the case of the structures $\mathbf{M}_d$ (but *not* for the generalizations $\mathbf{K}_d$ described in Theorem 2), with some modification of the proof, that we do not describe in this paper, it is possible to give an explicit construction for F. This modified proof also extends the result for expressions $G(y)$ which may depend on d, provided that their lengths remain below $\ell(d)$, where $\ell(d)$ is an explicitly given slowly growing elementary function.

(ii) The theorem about $\mathbf{M}_d$ can be reformulated in a way that we replace the terms $F(x,y)$, $G(y)$ by constant time computation on a RAM R_d, whose each register contains a $0,1$ sequence of length $n = 2^d$. It is easy to see that evaluating the terms $F(x,y)$ and $G(y)$ can be equivalently formulated by constant time computation on the RAM R_d, whose arithmetic instructions are the functions of the structures $\mathbf{M}_d$. (E.g., we may eliminate the conditional instruction of a RAM as described in [4] and [3].) This way the result is that there exists a program P which can run on R_d, for each sufficiently large d, such that the following conditions are satisfied: (a) If the program P, working on machine R_d, gets the n bit words x and a as input, then, in constant time, P gives a $TRUE$ or $FALSE$ answer, and (b) there exists no program Q such that for all sufficiently large d, given an n-bit word a as an input Q is able to decide in constant time whether there exists an x with $P(x,a) \equiv TRUE$.

In other words if both the test and the decision process is constant time computation on RAMs, then we cannot get a correct decision each time. Using the results mentioned in (i), where the size of the term G may grow with d it is possible to prove the statement about the tests on RAMs even if Q is allowed to use time $\ell(d)$, where $\ell(d)$ is slowly growing explicitly given elementary function, even if P can use only constant time.

We will return to the questions described in (i) and (ii) in another paper, where we also show that there exists a term $F(x,y)$ over the structures $\mathbf{M}_d$ such that the following problem of size $n = 2^d$ is NP-complete: "for a given $a \in \mathbf{M}_d$ find an $x \in \mathbf{M}_d$ such that $\mathbf{M}_d \models F(x,a) = 0$".

1.2 The formulation of the main result

Notation. 1. ω will denote the set of all natural numbers, that is $\omega = \{0,1,2,,\ldots\}$. The natural number n will be considered as the set of all natural numbers less than n, that is, $n = \{0,1,\ldots,n-1\}$.

2. $\mathtt{coeff}_i(a,b)$ denotes the ith b-ary "bit" of a. More precisely, assume that $a,b \in \omega$, $b \geq 2$, and $a = \sum_{i=0}^{\infty} \alpha_i b^i$, where for all $i = \omega$, $\alpha_i \in \omega$. The integer α_i will be denoted by $\mathtt{coeff}_i(a,b)$.

3. The set of all functions defined on the set A with values in the set B will be denoted by $\mathtt{func}(A,B)$. The set of all k-ary functions defined on the set A with values in the set B will be denoted by $\mathtt{func}_k(A,B)$. If we say that $\varphi(x_0,\ldots,x_k)$ is a firstorder formula of a language $\mathcal{L}$ then we will always assume, unless we explicitly state otherwise, that all of the free variables of

the formula are among the variables $x_0, \ldots, x_k$. A firstorder statement with this notation would be $\varphi()$. If we say that ψ is a firstorder formula without indicating any of its variables then there is no restriction on the number of variables in ψ. We will use the same convention for indicating the free variables in terms as well.

Definition. If M is an interpretation of the firstorder language $\mathcal{L}$ and X is a relation, constant or function symbol of $\mathcal{L}$, then $(X)_M$ will denote the interpretation of X in the structure M. We extend this notations for terms as well, that is, if $t(x_0, \ldots, x_{k-1})$ is a term with the free variables $x_0, \ldots, x_{k-1}$, then $(t)_M$ will denote the k-ary function which is the interpretation of this term in M.

Definition. 1. $\mathcal{M}$ will denote a firstorder language with equation, 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 negation, $\mathbf{p}$ stands for "power").

Binary function symbols: $+$, $\times$, $\mathbf{p}$, $\div$, max, min, $\cap$.

2. 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 $z = \lfloor x/y \rfloor$
$(\mathbf{M}_d \models z = \mathbf{0})$ 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 $\mathcal{M}$.

3. Motivated by the definition of the standard interpretations we will use the following notation as well when we use the functions symbols of $\mathcal{M}$: $+(x, y) = x + y$, $\times(x, y) = x \times y$, $\mathbf{p}(x) = 2^x$, $\div(x, y) = x/y$. 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. □

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

Definition. 1. Assume that $\varphi(x)$, $\psi(x)$ are firstorder formulas of $\mathcal{M}$ with the only free variable x. We will say that $\varphi(x)$ and $\psi(x)$ are asymptotically equivalent with respect to the sequence $\langle \mathbf{M}_d \mid d \in \omega \rangle$, iff for all sufficiently large integers d, we have $\mathbf{M}_d \models \forall x, \varphi(x) \leftrightarrow \psi(x)$.

2. Assume that $F(x, y)$ is a term of $\mathcal{M}$ with the only free variables x, y. We say that the existence of a solution of the equation $F(x, y) = 0$ in x can be decided by a term of $\mathcal{M}$ with

respect to $\langle \mathbf{M}_d \mid d \in \omega \rangle$, if there exists a term $G(y)$ of $\mathcal{M}$ with the only free variable y, such that the formulas $\exists x, F(x,y) = 0$ and $G(y) = 0$ are asymptotically equivalent with respect to the sequence $\langle \mathbf{M}_d \mid d \in \omega \rangle$. □

Theorem 1 *There exists a term $F(x,y)$ of $\mathcal{M}$ with the only free variables x, y, such that the existence of a solution of the equation $F(x,y) = 0$ in x cannot be decided by a term of $\mathcal{M}$ with respect to $\langle \mathbf{M}_d \mid d \in \omega \rangle$.*

Definition. We define another language $\bar{\mathcal{M}}$ that we get from $\mathcal{M}$ by adding to it a new binary function symbol $\bar{\mathbf{p}}$. $\bar{\mathbf{M}}_d$ will denote the interpretation of $\bar{\mathcal{M}}$ which is the extension of the interpretation $\mathbf{M}_d$ (with the same universe) defined by $(\bar{\mathbf{M}}_d \models \bar{\mathbf{p}}(x,y) = z)$ iff $z = \min\{x^y, 2^n - 1\}$, where $n = 2^d$. □

Corollary 1 *Theorem 1 remains true if we substitute $\bar{\mathcal{M}}$ for $\mathcal{M}$ and $\bar{\mathbf{M}}_d$ for $\mathbf{M}_d$.*

The proof of the Corollary is almost identical to the proof of Theorem 1. At a few places however we need some additional arguments in the proof of the Corollary. We will describe these these extra steps during the proof of Theorem 1.

2 A generalization of Theorem 1

Definition. We will say that $\mathbf{K}$ is a $\mathcal{K}$-sequence if the following two conditions are satisfied:

(i) $\mathcal{K}$ is a firstorder language with equality, with a finite number of function symbols, and without relation symbols other than equality. (We will call the 0-ary function symbols constant symbols as well.)

(ii) $\mathbf{K} = \langle \mathbf{K}_d \mid d \in \omega \rangle$ is a sequence of interpretations of $\mathcal{K}$ with the property that for all $d \in \omega$, $\mathtt{universe}(\mathbf{K}_d) = 2^n$, where $n = 2^d$. □

Notation. 1. For the sake of brevity we will frequently write $a \in \mathbf{K}_d$ instead of $a \in \mathtt{universe}(\mathbf{K}_d)$.

2. If t is a term and R is a relation symbol of $\mathcal{K}$ then we will use the notation $t^{(d)} = (t)_{\mathbf{K}_d}$ and $R^{(d)} = (R)_{\mathbf{K}_d}$

In the following we will define several properties of a $\mathcal{K}$-sequence $\mathbf{K} = \langle \mathbf{K}_d \mid d \in \omega \rangle$ which together will imply that an analogue of Theorem 1 holds for $\mathbf{K}$. The first two properties regularity and projectivity, ensures that each $\mathbf{K}_d$ contains enough function so that certain elementary arguments or constructions which are available in $\mathbf{M}_d$ can be carried out in $\mathbf{K}_d$ as well.

We will say that a $\mathcal{K}$-sequence $\mathbf{K}_d$, $d \in \omega$ is regular if certain "basic" functions can be easily defined in $\mathbf{K}_d$. The expression "easily defined" means in certain cases that the functions are interpretations of suitably chosen terms of $\mathcal{K}$ while in other cases it means that the functions can be defined by firstorder formulas in the structure $\mathbf{K}_d$. The mentioned functions are, roughly speaking, (i) constant functions with values 0 and 1, (ii) boolean functions of two variables, (iii) characteristic function of the equality relation, (iv) all of the functions defined on $\{0, 1, \ldots, i-1\}$ with values in the same set, provided that d is sufficiently large with respect to i, (v) a function for forming pairs, provided that d is sufficiently large compared to the elements of the pairs.

Definition. Assume that $\mathbf{K} = \langle \mathbf{K}_d \mid d \in \omega \rangle$ is a $\mathcal{K}$-sequence. We say that $\mathbf{K}$ is regular if $\mathcal{K}$ contains the constant symbols $\mathbf{0}$, $\mathbf{1}$ and the following conditions are satisfied:

(1) *For each sufficiently large* $d \in \omega$, $(\mathbf{0})_{\mathbf{K}_d} = 0$, $(\mathbf{1})_{\mathbf{K}_d} = 1$

(2) *For each binary function* $f(x, y)$ *defined on the set* $\{\mathbf{0}, \mathbf{1}\}$ *and with values in* $\{\mathbf{0}, \mathbf{1}\}$, *there exists a term* $t(x, y)$ *of* $\mathcal{K}$, *such that for all* $a, b \in \{\mathbf{0}, \mathbf{1}\}$ *and for all sufficiently large* $d \in \omega$, *we have* $\mathbf{K}_d \models f(a, b) = t(a, b)$.

(3) *There exists a term* $\bar{t}(x, y)$ *of* $\mathcal{K}$, *so that for all sufficiently large* $d \in \omega$ *we have* $\mathbf{K}_d \models \forall x, y, (x = y \to \bar{t}(x, y) = \mathbf{0}) \wedge (x \neq y \to \bar{t}(x, y) = \mathbf{1})$.

(4) *for each* $k \in \omega$, *there exists a firstorder formula* $\varphi(x_0, \ldots, x_{k-1}, y, z)$ *of* $\mathcal{K}$ *such that for all* $i \in \omega$ *and for each* k*-ary function* $f(x_0, \ldots, x_{k-1}) \in \mathtt{func}_k(\{0, 1, \ldots, i-1\}, \{0, 1, \ldots, i-1\})$, *there exists a* $j \in \omega$, *such that for all sufficiently large* $d \in \omega$ *and for all* $a_0, \ldots, a_{k-1}, b \in i$ *we have that* $f(a_0, \ldots, a_{k-1}) = b$ *iff* $\mathbf{K}_d \models \varphi(a_0, \ldots, a_{k-1}, b, j)$.

(5) *There exists a firstorder formula* $\kappa(x, y, z)$ *of* $\mathcal{K}$ *with the following property. For each* $i, j \in \omega$ *there exists* $k \in \omega$ *such that for all sufficiently large* $d \in \omega$, $\mathbf{K}_d \models \forall x, y,\ \kappa(x, y, k) \leftrightarrow (x = i \wedge y = j)$. □

We define now another property of $\mathcal{K}$-sequence a $\mathbf{K} = \langle \mathbf{K}_d \mid d \in \omega \rangle$. If $\mathbf{K}$ has this property then the elements of the direct product of 2^c copies, of $\mathbf{K}_d$, can be encoded by single elements of $\mathbf{K}_{d+c}$ so that the encoding is done by a term of $\mathcal{K}$, and the projections of the direct product to its kth component can be defined by a firstorder formula Γ which contains k and c as parameters but otherwise the choice of Γ does not depend on k and c.

In the following definition we assume that the free variables of a firstorder formula or a term are among those which are explicitly shown.

Definition. Assume that $\mathbf{K} = \langle \mathbf{K}_d \mid d \in \omega \rangle$ is a $\mathcal{K}$-sequence. We say that $\mathbf{K}$ is projective if for all $c \in \omega$ and $k \in 2^c$, there exists a term $\pi_{c,k}$ of $\mathcal{K}$ so that the following conditions are satisfied.

(6) *for all* $c \in \omega$ *there exists a term* τ_c *of* $\mathcal{K}$ *such that if* $d \in \omega$ *is sufficiently large, and* $a_0, \ldots, a_{2^c-1} \in \mathbf{K}_d$, *then for all* $k = 0, 1, \ldots, 2^{c-1}$, *we have* $\mathbf{K}_{d+c} \models \pi_{c,k}(\tau_c(a_0, \ldots, a_{2^c-1})) = a_k$.

(7) *There exists a firstorder formula* $\Gamma(x, y, z, w)$ *of* $\mathcal{K}$ *such that for all* $c \in \omega$ *if* $d \in \omega$ *is sufficiently large and* $k \in 2^c$ *then*

$$\mathbf{K}_{d+c} \models \forall x, y, \Gamma(x, y, c, k) \leftrightarrow \pi_{c,k}(x) = y$$

□

Definition. Assume that $\mathbf{K} = \langle \mathbf{K}_d \mid d \in \omega \rangle$ is a $\mathcal{K}$-sequence. If $\mathbf{K}$ is both regular and projective then we will say that $\mathbf{K}$ is complete. □

Proposition 1 *Assume that* $\mathbf{K}^{(i)} = \langle \mathbf{K}^{(i)}_d \mid d \in \omega \rangle$ *is a* $\mathcal{K}^{(i)}$ *sequence for* $i = 0, 1$, *and* $\mathcal{K}^{(0)} \subseteq \mathcal{K}^{(1)}$, *that is, every symbol of* $\mathcal{K}_0$ *is also a symbol of* $\mathcal{K}_1$. *Suppose further that for all* $d \in \omega$, *the restriction of the model* $\mathbf{K}^{(1)}_d$ *of the language* $\mathcal{K}^{(1)}$ *to the language* $\mathcal{K}^{(0)}$ *is the model* $\mathbf{K}^{(0)}_d$. *Then we have that if the* $\mathcal{K}^{(0)}$ *sequence* $\mathbf{K}^{(0)}$ *is complete then the* $\mathcal{K}^{(1)}$*-sequence* $\mathbf{K}^{(1)}$ *is also complete.*

Proof. By the definition of a $\mathcal{K}$-sequence we have that $\mathtt{universe}(\mathbf{K}^{(0)}_d) = \mathtt{universe}(\mathbf{K}^{(1)}_d)$. The assumptions of the proposition imply that every function which is defined by a term in $\mathbf{K}^{(0)}_d$ is also defined in $\mathbf{K}^{(1)}_d$ by the same term, and every function which is defined by a firstorder formula in $\mathbf{K}^{(0)}_d$ is also defined in $\mathbf{K}^{(1)}_d$ by the same firstorder formula. The definitions of regularity and projectivity require only the existence of certain functions defined in the various structures $\mathbf{K}_d$, $d \in \omega$, by terms or firstorder formulas. Since the restriction of $\mathbf{K}^{(1)}_d$ to $\mathcal{K}^{(0)}$ is $\mathbf{K}^{(0)}_d$, the functions guaranteeing the regularity or projectivity of $\mathbf{K}^{(0)}$ will play the same role for $\mathbf{K}^{(1)}$. *Q.E.D.*Proposition 1

In the generalization of Theorem 1 we will speak about a $\mathcal{K}$ sequence $\mathbf{K} = \langle \mathbf{K}_d \mid d \in \omega \rangle$ which is complete and in addition to that it must be "retrospective" and "predictive" in the sense to be defined below. These properties establish connections between $\mathbf{K}_d$ and $\mathbf{K}_{d+c}$, where c is an arbitrary constant. Namely if we think that we construct the sequence $\mathbf{K}_0, \mathbf{K}_1, \ldots, \mathbf{K}_d, \ldots$ in this order then retrospectivity means that when we have $\mathbf{K}_d$ we are able using the functions defined in $\mathbf{K}_d$ to "look back" at $\mathbf{K}_{d-c}$ and decide the values of the functions defined in $\mathbf{K}_{d-c}$. Predictivity, in a similar way means, that using only functions defined in $\mathbf{K}_d$, we will be able to "predict", in some sense, what will be the values of the functions defined in $\mathbf{K}_{d+c}$.

The next definition describes the following property of a $\mathcal{K}$ sequence $\mathbf{K}_d$, $d \in \omega$. Assume that a g is function in $\mathbf{K}_{d-1}$ which is an interpretation of a function symbol of $\mathcal{K}$. Then, in the structure $\mathbf{K}_d$, g can be expressed by a term. If g is in $\mathbf{K}_{d-c}$, then in the structure $\mathbf{K}_d$, g can be expressed by a firstorder formula containing c as a parameter.

Definition. Assume that $\mathbf{K} = \langle \mathbf{K}_d \mid d \in \omega \rangle$ is a $\mathcal{K}$-sequence. We say that $\mathbf{K}$ is retrospective if it satisfies the following two conditions:

(8) *Let* $k \in \omega$ *and let* g *be a* k*-ary function symbol of* $\mathcal{K}$. *Then there exists a term* $t(x_0, \ldots, x_{k-1})$ *of* $\mathcal{K}$ *such that if* $d \in \omega$ *is sufficiently large and* $a_0, \ldots, a_{k-1}, b \in \mathbf{K}_{d-1}$ *then* $\mathbf{K}_{d-1} \models g(a_0, \ldots, a_{k-1}) = b$ *iff* $\mathbf{K}_d \models t(a_0, \ldots, a_{k-1}) = b$.

(9) *Let* $k \in \omega$ *and let* g, *be a* k*-ary function symbol of* $\mathcal{K}$. *Then there exists a firstorder formula* $\varphi(x_0, \ldots, x_{k-1}, y, z)$ *of* $\mathcal{K}$ *such that for all* $c \in \omega$, *if* $d \in \omega$ *is sufficiently large and* $a_0, \ldots, a_{k-1}, b \in \mathbf{K}_{d-c}$ *then*

$$\Big(\mathbf{K}_{d-c} \models g(a_0, \ldots, a_{k-1}) = b\Big) \leftrightarrow \mathbf{K}_d \models \varphi(a_0, \ldots, a_{k-1}, b, c)$$

□

In the next definition we will consider $\mathcal{K}$ sequnces $\mathbf{K}_d$, $d \in \omega$, where in the structure $\mathbf{K}_d$ we are able to decide in a first-order way whether a function f which is defined on $\mathtt{universe}(\mathbf{K}_{d+c})$, and which is an interpretation of a function symbol of $\mathcal{K}$, takes a certain value or not. More

precisely, we will consider only the case when the elements of $\mathbf{K}_{d+c}$ can be encoded by binary relations on $\mathbf{K}_d$ and the question whether the function f takes a value or not can be decided by a firstorder formula over $\mathbf{K}_d$, using these relations. (E.g., it is well-known that the addition and multiplication of the structure $\mathbf{M}_d$ have this property.) As we said earlier, if we consider the sequence of structures $\mathbf{K}_d$ as if they were constructed in time $d = 0, 1, \ldots$, then this property implies that at time d we will be able to predict the behavior of the functions that will be constructed at time $d + c$.

Definition. Assume that $\mathbf{K} = \langle \mathbf{K}_d \mid d \in \omega \rangle$ is a $\mathcal{K}$-sequence. We say that $\mathbf{K}$ is predictive if the following condition is satisfied

(10) *There exists a function assigning to each function symbol $f(x_0, \ldots, x_{k-1})$ of $\mathcal{K}$, (including the constant symbols for $k = 0$), a firstorder formula $\Phi_f(x, y, z, Y_0, \ldots, Y_{k-1})$ of $\mathcal{K}$, where x, y, z are free individual variables and $Y_0, \ldots, Y_{k-1}$ are free binary relation variables, such that the following holds. For all $c \in \omega$ if $d \in \omega$ is sufficiently large then there exists a map $\eta_{d,c}$ of* $\mathtt{universe}(\mathbf{K}_{d+c})$ *into the set of binary relations on* $\mathtt{universe}(\mathbf{K}_d)$ *with the following properties:*

(i) For each $a, u, v \in \mathbf{K}_d$, we have $(\eta_{d,c}(a))(u, v)$ iff "$u = 0$ and $v = a$".

(ii) Suppose that $f(x_0, \ldots, x_{k-1})$ is a k-ary function symbol of $\mathcal{K}$, for some $k = 0, 1, \ldots$ (including the constant symbols for $k = 0$) and $a_0, \ldots, a_{k-1} \in \mathbf{K}_{d+c}$. Then for all $u, v \in \mathbf{K}_d$, $(\eta_{d,c}(f^{(d+c)}(a_0, \ldots, a_{k-1}))(u, v)$ iff $\mathbf{K}_d \models \Phi_f(u, v, c, \eta_{d,c}(a_0), \ldots, \eta_{d,c}(a_{k-1}))$, where $f^{(d+c)} = (f)_{\mathbf{K}_{d+c}}$. □

Definition. 1. Assume that $\varphi(x)$, $\psi(x)$ are firstorder formulas of $\mathcal{M}$ with the only free variable x. We will say that $\varphi(x)$ and $\psi(x)$ are asymptotically equivalent with respect to the $\mathcal{K}$-sequence $\langle \mathbf{K}_d \mid d \in \omega \rangle$, iff for all sufficiently large integers d, we have $\mathbf{K}_d \models \forall x, \varphi(x) \leftrightarrow \psi(x)$.

2. Suppose that $\mathbf{K} = \langle \mathbf{K}_d,\ d \in \omega \rangle$ is a $\mathcal{K}$-sequence. Assume further that $F(x, y)$ is a term of $\mathcal{K}$ with the only free variables x, y. We say that the existence of a solution of the equation $F(x, y) = \mathbf{0}$, in the unknown x, can be decided by a term of $\mathcal{K}$, if there exists a term $G(y)$ of $\mathcal{K}$ with the only free variable y, such that the formulas $\exists x, F(x, y) = \mathbf{0}$ and $G(y) = \mathbf{0}$ are asymptotically equivalent with respect to $\mathbf{K}$. □

Theorem 2 *Assume that $\mathbf{K}$ is a $\mathcal{K}$-sequence, such that $\mathbf{K}$ is complete, retrospective, and predictive. Then there exists a term $F(x, y)$ of $\mathcal{K}$ with the only free variables x, y, such that the existence of a solution of the equation $F(x, y) = \mathbf{0}$ in the unknown x, cannot be decided by a term of $\mathcal{K}$.*

Sketch of the proof. Assume that the statement of the theorem is not true, namely it does not hold for the $\mathcal{K}$ sequence $\mathbf{K} = \langle \mathbf{K}_d \mid d \in \omega \rangle$, that is, $\mathbf{K}$ satisfies the assumptions of Theorem 2 and yet its conclusion does not hold. We will reach a contradiction by using Gödel's method of constructing a firstorder formula φ which expresses the statement that φ is false. Let $\mathtt{Form}(\mathcal{K}, k)$ be the set of all firstorder formulas of $\mathcal{K}$ with at most k free variables. We will show that there exists a function $\rho \in \mathtt{func}(\mathtt{Form}(\mathcal{K}, 1), \omega)$ and a firstorder formula $\psi(x, y)$ of $\mathcal{K}$ with the following property.

(11) *For all $\varphi \in \mathtt{Form}(\mathcal{K}, 1)$ if d is sufficiently large, then $\mathbf{K}_d \models \forall x, \varphi(x) \leftrightarrow \psi(x, \rho(\varphi))$*

This leads to a contradiction in the following way. Let $\varphi_0(x) = \neg\psi(x,x)$. Then condition (11) with $\varphi := \varphi_0$ implies that for all sufficiently large d we have $\mathbf{K}_d \models \forall x, \neg\psi(x,x) \leftrightarrow \psi(x,\rho(\varphi_0))$, and therefore $\mathbf{K}_d \models \psi(\rho(\varphi_0),\rho(\varphi_0)) \leftrightarrow \neg\psi(\rho(\varphi_0),\rho(\varphi_0))$ which is a contradiction. Note that in this argument we did not assume anything about the computability or definability of ρ. (Otherwise $\rho(\varphi)$ plays the role of the Gödel number of the formula φ.)

To get the formula ψ and the function ρ we start with an arbitrary $\varphi(x) \in \mathtt{Form}(\mathcal{K},1)$. First we note that we may assume that if the formula $\varphi(x)$ is in prenex form then its propositional part is of the form $t(x) = \mathbf{0}$ where t is a term. Since $\mathbf{K}$ is regular, conditions (2) and (3) of the definition of regularity implies that φ can be easily transformed into this form.

Our plan is the following. First, instead of expressing the truth value of φ in the structure $\mathbf{K}_d$, we express it in a larger structure $\mathbf{K}_{d+c}$ where c is a constant. More precisely we will show (in Lemma 4) that:

(12) *If Theorem 2 does not hold for* $\mathbf{K}$*, then there exists a term* $G(x,y)$ *of* $\mathcal{K}$*, and there exist functions* $s \in \mathtt{func}(\mathtt{Form}(\mathcal{K},1),\omega)$*,* $h \in \mathtt{func}(\omega,\omega)$ *with the following property. For all natural numbers* ℓ *and for all firstorder formulas* $\varphi(x)$ *of* $\mathcal{K}$ *with length at most* ℓ *we have that for all sufficiently large* $d \in \omega$ *and for all* $a \in \mathbf{K}_d$*,* $\mathbf{K}_d \models \varphi(a)$ *iff* $\mathbf{K}_{d+h(\ell)} \models G(a, s(\varphi,\ell)) = \mathbf{0}$

In other words the truth value of $\varphi(a)$, $a \in \mathbf{K}_d$ can be decided in the larger structure $\mathbf{K}_{d+h(\ell)}$ by evaluating a term. Although we have to use the structure $\mathbf{K}_{d+h(\ell)}$ instead of the structure $\mathbf{K}_d$, but if φ is fixed then $h(\ell)$ is a constant (while we change d). For a fixed φ, the parameter $s(\varphi,\ell)$ in the expression $G(a,s(\varphi,\ell))$ is also a constant. These facts will imply that using the predictivity of the $\mathcal{K}$-sequence $\mathbf{K}$ we will be able to express the truth value of $\mathbf{K}_d \models \varphi(a)$ by a formula $\psi(a,\rho(\varphi))$, where ψ does not depend on φ and this leads to a contradiction as described earlier.

In the step when we get the formula ψ from the term G, the predictivity of $\mathbf{K}$ is used in the following way. The term G describes operations in the structure $\mathbf{K}_{d+h(\ell)}$. The definition of predictivity implies that these operation can be performed in $\mathbf{K}_d$ by firstorder formulas acting on the binary relations which represent the elements of $\mathbf{K}_{d+h(\ell)}$ in $\mathbf{K}_d$.

Now we sketch the proof of statement (12). We reach the required equivalent form of $\mathbf{K}_d \models \varphi(a)$, for $a \in \mathbf{K}_d$ in three steps.

Step 1. We show (Lemma 2) that if Theorem 2 does not hold for the $\mathcal{K}$-sequence $\mathbf{K}$, then there exists a term G and a $c \in \omega$, both depending on φ, such that for all sufficiently large $d \in \omega$ we have that for all $a \in \mathbf{K}_d$, $\mathbf{K}_d \models \varphi(a)$ is equivalent to $\mathbf{K}_{d+c} \models G_1(a) = \mathbf{0}$.

This statement is similar to (12) but it is not the same since the term G may depend on φ. In fact the length of G will grow with the length of φ in the construction described in the proof of Step 1.

The proof of Step 1 is using the assumption that Theorem 2 is not true and therefore an existential statement of the type $\exists x, F(x,a) = \mathbf{0}$ is equivalent to a quantifier free statement of the form $G_1(a) = \mathbf{0}$. This suggests a process of quantifier elimination applied to the formula φ. To carry out the quantifier elimination we would need to eliminate quantifiers form statements of the type $\exists x, F(x,b_1,...,b_k,a) = \mathbf{0}$ where $b_1,...,b_k$ are fixed elements of $\mathbf{K}_d$. In other words we would need our indirect assumption for equations with more then one parameters. We do not have such an assumption, but we can reduce the many parameters to a single parameter

by considering the same statement not in $\mathbf{K}_d$ but in $\mathbf{K}_{d+c}$, where c is sufficiently large with respect to k. In this structure the $k+1$ parameters can be encoded by a single parameter, so the indirect assumption can be used. (We need the completeness and retrospectivity of $\mathbf{K}$ to prove the correctness of this step.)

Step 2. After Step 1 we have a statement of the type $\mathbf{K}_d \models G(a) = \mathbf{0}$ (with $d{:=}\, d+c$) where the the term G depends on φ, in particular it G can be arbitrarily large since we used the indirect assumption in its construction, which does not provide any limit on its size. In this step we show that (see Lemma 3)

(13) *There exists a firstorder formula $\xi(y,z)$ of $\mathcal{K}$ so that if $\mathbf{K} = \langle \mathbf{K}_d \mid d \in \omega \rangle$ is a $\mathcal{K}$-sequence, then for each term $G(y)$ of $\mathcal{K}$, and for each sufficiently large $c \in \omega$, there exists an $u_{c,G} \in \omega$, with the property that for all sufficiently large $d \in \omega$, and for all $a \in \mathbf{K}_d$, $\mathbf{K}_d \models G(a) = \mathbf{0}$ is equivalent to $\mathbf{K}_{d+c} \models \xi(y, u_{c,G})$.*

(We do not need the indirect assumption about $\mathbf{K}$ in this statement.) The important point in this statement is that the formula $\xi(x,y)$ does not depend on the term G. The dependence on G is only through a parameter of ξ. Applying Step 1 and then Step 2 we get that for all sufficiently large $d \in \omega$ and for all $a \in \mathbf{K}_d$, $\mathbf{K}_d \models \varphi(a)$ is equivalent to $\mathbf{K}_{d+c_1} \models \xi(a, c_2)$, where c_1 and c_2 depends only on φ (but not on d or a).

The proof of statement (13) is based on the observation that the evaluation of a term can be described by existentially quantifying the values of its subterms. If the integer c of statement (13) is sufficiently large with respect to G (which is allowed) then such an existential quantification is possible in $\mathbf{K}_{d+c}$.

Step 3. If we combine the first two steps we get, that for all sufficiently large $d \in \omega$, and for all $a \in \mathbf{K}_d$, $\mathbf{K}_d \models \varphi(a)$ is equivalent to $\mathbf{K}_{d+c_1} \models \xi(a, c_2)$, where the firstorder formula ξ does not depend on anything, and $c_1, c_2 \in \omega$ depend only on φ. Now we use the quantifier elimination, described in Step 1, again, and we get the term G whose existence is claimed in statement (12). Since ξ does not depend on φ the term G, that we gain at the end of the elimination process, will not depend on it either, the dependence on φ will be only through the parameters of G. *End of Sketch*

2.1 Proof of Theorem 2

Definition. Assume that $\mathbf{K} = \langle \mathbf{K}_d \mid d \in \omega \rangle$ is a $\mathcal{K}$-sequence with respect to the language $\mathcal{K}$ and $k \in \omega$. We will say that a family of k-ary functions $f^{(d)} \in \mathtt{func}_k(\mathtt{universe}(\mathbf{K}_d), \mathtt{universe}(\mathbf{K}_d))$, $d \in \omega$, is an external $\mathbf{K}$ family. The external $\mathbf{K}$ family of k-ary functions will be called a firstorder $\mathbf{K}$ family of k-ary functions, if there exists a firstorder formula $\varphi(x_0, \ldots, x_{k-1}, y)$ of $\mathcal{K}$, whose free variables are among $x_0, \ldots, x_{k-1}, y$, such that for all sufficiently large $d \in \omega$, and for all $a_0, \ldots, a_{k-1}, b \in \mathbf{K}_d$, we have $b = f(a_0, \ldots, a_{k-1})$ iff $\mathbf{K}_d \models \varphi(a_0, \ldots, a_{k-1}, b)$.

The external $\mathbf{K}$ family of k-ary functions will be called an internal $\mathbf{K}$ family of k-ary functions, if there exists a term $t(x_0, \ldots, x_{k-1})$ of $\mathcal{K}$ with k free variables, such that for all sufficiently large $d \in \omega$, and for all $a_0, \ldots, a_{k-1} \in \mathbf{K}_d$ we have $t^{(d)}(a_0, \ldots, a_{k-1}) = f(a_0, \ldots, a_{k-1})$, where $t^{(d)} = (t)_{\mathbf{K}_d}$. In this case the family of functions $f^{(d)}$ is called the family of functions induced by the term t. Sometimes we will say "$\mathbf{K}$ firstorder-family" instead of "firstorder $\mathbf{K}$ family of

functions" "**K** internal-family" instead of "internal **K** family of functions", and "**K** external-family" instead of "external **K** family of functions". □

Remark. It is important in the definition of a firstorder **K** family of function that in the formula $\varphi(x_0,\dots,x_{k-1},y)$ we do not allow any parameters. This makes the definition somewhat different from the usual definition of a firstorder definable function. □

Definition. 1. The set A is a co-finite subset of the set B, or $A \subseteq B$ is co-finite, if $A \subseteq B$ and $B\backslash A$ is finite.

2. Assume $\mathbf{K} = \langle \mathbf{K}_d \mid d \in \omega\rangle$ is a $\mathcal{K}$-sequence, with respect to the language $\mathcal{K}$, $A \subseteq \omega$ is co-finite and for all $d \in A$, $R_1^{(d)}, R_2^{(d)}$ are k-ary relations on the set $\mathtt{universe}(\mathbf{K}_d)$. We will say that the family of relations $R_1 = \langle R_1^{(d)} \mid d \in A\rangle$ and $R_2 = \langle R_2^{(d)} \mid d \in A\rangle$ are asymptotically equivalent iff for all sufficiently large $d \in \omega$, we have that $\forall a_0,\dots,a_{k-1} \in \mathbf{K}_d, R_1^{(d)}(a_0,\dots,a_{k-1}) \leftrightarrow R_2^{(d)}(a_0,\dots,a_{k-1})$. We will write $R_1 \sim R_2$ for "R_1 and R_2, are asymptotically equivalent".

3. Assume that $\varphi(x_0,\dots,x_{k-1})$ is a firstorder formula of $\mathcal{K}$, $j \in \omega$. For all $d \in \omega$, $\mathcal{R}_k^{(d)}[\varphi, j]$ will be the k-ary relation on $\mathtt{universe}(\mathbf{K}_d)$ defined by: "for all $a_0,\dots,a_{k-1} \in \mathbf{K}_d$, $(\mathcal{R}_k^{(d)}[\varphi,j])(a_0,\dots,a_{k-1})$ iff $\mathbf{K}_{d+j} \models \varphi(a_0,\dots,a_{k-1})$". The family of relations $\langle \mathcal{R}_k^{(d)}[\varphi,j] \mid d \in \omega\rangle$ will be denoted by $\mathcal{R}_k[\varphi,j]$. The relation $\mathcal{R}_k^{(d)}[\varphi,0]$ will be also denoted by $\mathcal{R}_k^{(d)}[\varphi]$. The corresponding family of relations will be denoted by $\mathcal{R}_k[\varphi]$.

4. If $F(x_0,\dots,x_{k-1})$ is a term of $\mathcal{K}$ and $j \in \omega$, $n = 1,2,\dots$ then the relation $\mathcal{R}_k^{(d)}[F(x_0,\dots,x_{k-1}) = \mathbf{0}, j]$ will be denoted by $\mathcal{R}_k^{(d)}[F,j]$, and for $j = 0$ by $\mathcal{R}_k^{(d)}[F]$ as well. The corresponding families of relations will be denoted by $\mathcal{R}_k[F,j]$ and $\mathcal{R}_k[F]$. □

Remark. According to these definitions the firstorder formulas $\varphi(x), \psi(x)$ are asymptotically equivalent iff the family of relations $\mathcal{R}_1^{(d)}[\varphi]$, $d \in \omega$ and $\mathcal{R}_1^{(d)}[\psi]$, $d \in \omega$ are asymptotically equivalent. □

Lemma 1 *Assume that* $\mathbf{K} = \langle \mathbf{K}_d \mid d \in \omega\rangle$ *is a regular* $\mathcal{K}$*-sequence. For each propositional formula* $P(x_1,\dots,x_k)$ *of* $\mathcal{K}$*, there exists a term* $T(x_1,\dots,x_k)$ *of* $\mathcal{K}$ *so that for all sufficiently large* $d \in \omega$*, we have* $\mathbf{K}_d \models \forall x_1,\dots,x_k, P(x_1,\dots,x_k) \leftrightarrow T(x_1,\dots,x_k) = \mathbf{0}$ *and* $\mathbf{K}_d \models \forall x_1,\dots,x_k, \neg P(x_1,\dots,x_k) \leftrightarrow T(x_1,\dots,x_n) = \mathbf{1}$*. Consequently for each propositional formula* $P(x_1\dots,x_k)$ *of* $\mathcal{K}$ *there exists a term* $T(x_1,\dots,x_k)$ *of* $\mathcal{K}$ *so that the family of relations* $\mathcal{R}_k^{(d)}[P]$*,* $d \in \omega$ *and* $\mathcal{R}_k^{(d)}[F]$*,* $d \in \omega$ *are asymptotically equivalent.*

Proof. Since the only relation symbol of the language $\mathcal{K}$ is the equality, we have that each atomic formula is of the form $t_1 = t_2$ where t_1 and t_2 are terms. By condition (3) of the definition of regularity $t_1 = t_2$ is equivalent to $\bar{t}(t_1,t_2) = \mathbf{0}$ and $\neg(t_1 = t_2)$ is equivalent to $\bar{t}(t_1,t_2) = \mathbf{1}$. Therefore using condition (2) for the various logical operations $\wedge, \vee, \neg$ etc. we can transform each propositional formula of $\mathcal{K}$ into a propositional formula into an equivalent propositional formula of the form $t = \mathbf{0}$, where t is a term. *Q.E.D.*(Lemma 1)

Notation. For an expression $x_0,\dots,x_{k-1}$ we will sometimes write $\underline{x}$ if the choice of k is clear from the context.

Proposition 2 *Assume that for each* $i = 0,1,2$*,* Φ_i *is a firstorder formula with* k *variables,* $u, v \in \omega$*, and we have* $\mathcal{R}_k[\Phi_0] \sim \mathcal{R}_k[\Phi_1, u]$ *and* $\mathcal{R}_k[\Phi_1] \sim \mathcal{R}_k[\Phi_2, v]$*. Then* $\mathcal{R}_k[\Phi_0] \sim \mathcal{R}_k[\Phi_2, u+v]$.

Proof. Assume $\underline{x} \in (\mathbf{K}_d)^k$, where d is sufficiently large. Then $\mathbf{K}_d \models \Phi_0(\underline{x})$ iff $\mathbf{K}_{d+u} \models \Phi_1(\underline{x})$ and $\mathbf{K}_{d+u} \models \Phi_1(\underline{x})$ iff $\mathbf{K}_{d+u+v} \models \Phi_2(\underline{x})$ which implies our statement. *Q.E.D.*(Proposition 2)

Remark. If $F_i(\underline{x})$ is a term, then we may apply Proposition 2 with $\Phi_i(\underline{x})$:= "$F_i(\underline{x}) = \mathbf{0}$". Therefore the proposition remains true if some of the Φ_is are not formulas but terms. □

Proposition 3 *Assume that* $\mathbf{K} = \langle \mathbf{K}_d \mid d \in \omega \rangle$ *is a retrospective and projective* $\mathcal{K}$*-sequence. Then the following condition is satisfied.*

(14) *Let* $k \in \omega$ *and let* $g^{(d)}$, $d \in \omega$ *be a* k*-ary* $\mathbf{K}$ *internal-family of functions. Then there exists a* $k+1$*-ary* $\mathbf{K}$ *firstorder-family of functions* $f^{(d)}$, $d \in \omega$ *such that for all* $c \in \omega$, *for all sufficiently large* $d \in \omega$, *and for all* $a_0, \dots, a_{k-1} \in \mathbf{K}_d$ *we have* $g^{(d)}(a_0, \dots, a_{k-1}) = f^{(d+c)}(a_0, \dots, a_{k-1}, c)$.

Proof of Proposition 3. The statement of the proposition requires a proof since the terms involved in $g^{(d)}$ are defined in $\mathbf{K}_d$, while the firstorder formula defining $f^{(d+c)}$ must be interpreted in $\mathbf{K}_{d+c}$.

The firstorder formula $\varphi(x_0, \dots, x_{k-1}, y)$ defining the function $f^{(d+c)}$ will say that $y \in \mathbf{K}_d$ and $g^{(d)}(x_0, \dots, x_{k-1}) = y$. By condition (6) of the definition of projectivity, $\mathtt{universe}(\mathbf{K}_d)$ is the image of the map $\pi^{(d)}_{c,0}$. Therefore $b \in \mathbf{K}_d$ iff $\mathbf{K}_{d+c} \models \exists a, \Gamma(a, b, d, c, 0)$, where Γ is the firstorder formula from condition (7) from the definition of projectivity. Consequently $y \in \mathbf{K}_d$ can be stated in $\mathbf{K}_{d+c}$ in a firstorder way and by condition (9) by the definition of a retrospective $\mathcal{K}$-sequence, $g^{(d)}(x_0, \dots, x_{k-1}) = y$ can be also defined in a firstorder way in $\mathbf{K}_{d+c}$. (We need the firstorder formula expressing $y \in \mathbf{K}_d$, since the formula guaranteed by condition (9) speaks only about the elements of $\mathbf{K}_d$ and not of $\mathbf{K}_{d+c}$.) *Q.E.D.*(Proposition 3)

Proposition 4 *Assume that* $\mathbf{K} = \langle \mathbf{K}_d \mid d \in \omega \rangle$ *is a retrospective and projective* $\mathcal{K}$*-sequence. Then the following condition is satisfied.*

(15) *Let* $k \in \omega$ *and let* $g(x_0, \dots, x_{k-1})$ *be a term of* $\mathcal{K}$ *with the only free variables* $x_0, \dots, x_{k-1}$. *Then for all* $c \in \omega$ *there exists a term* $h_{g,c}(x_0, \dots, x_{k-1})$ *of* $\mathcal{K}$ *with the only free variables* $x_0, \dots, x_{k-1}$ *such that for all sufficiently large* $d \in \omega$, *and for all* $a_0, \dots, a_{k-1} \in \mathbf{K}_d$ *we have* $g^{(d)}(a_0, \dots, a_{k-1}) = h^{(d+c)}_{g,c}(a_0, \dots, a_{k-1})$.

Proof. We prove the proposition by induction on c. For $c = 1$ the statement of the proposition follows from condition (8) from the definition of retrospectivity. Assume that $c > 1$ and the proposition holds for all smaller values of c. We define $h_{g,c}$ by $h_{g,c}(x_0, \dots, x_{k-1}) = h_{h_{g,c-1},1}(x_0, \dots, x_{k-1})$. Assume that $a_0, \dots, a_{k-1} \in \mathbf{K}_d \subseteq \mathtt{universe}(\mathbf{K}_{d+c-1})$. We have $h^{(d+c)}_{g,c}(a_0, \dots, a_{k-1}) = h^{(d+c)}_{h_{g,c-1},1}(a_0, \dots, a_{k-1}) = h^{(d+c-1)}_{g,c-1}(a_0, \dots, a_{k-1}) = g^{(d)}(a_0, \dots, a_{k-1})$ as claimed in the conclusion of proposition. *Q.E.D.*(Proposition 4)

Proposition 5 *Assume that* $\mathbf{K}$ *is a projective* $\mathcal{K}$*-sequence and for all* $c \in \omega$, $k \in 2^c$ *let* $\pi_{c,k}$ *be the term whose existence is stated in the definition of projectivity. Then for all* $c \in \omega$ *and for all sufficiently large* $d \in \omega$, $\pi^{(d+c)}_{c,k}$ *is a map of* $\mathtt{universe}(\mathbf{K}_{d+c})$ *onto* $\mathtt{universe}(\mathbf{K}_d)$. *As a consequence, for each firstorder formula* $Q_0 x_0, \dots, Q_{k-1} x_{k-1}, P(x_0, \dots, x_{k-1})$ *of* $\mathcal{K}$, *where* $Q_0, \dots, Q_{k-1}$ *are quantifiers, the following two statements are equivalent*

(i) $\mathbf{K}_{d+c} \models Q_0 x_0, \dots, Q_{k-1} x_{k-1}, P(\pi_{c,0}(x_0), \dots, \pi_{c,0}(x_{k-1}))$

(ii) $Q_0 a_0 \in \mathbf{K}_d, \dots, Q_{k-1} a_{k-1} \in \mathbf{K}_d, \mathbf{K}_{d+c} \models P(a_0, \dots, a_{k-1})$

Proof. Condition (6) of the definition of projectivity implies that the image of $\pi^{(d)}_{c,k}$ is $\mathbf{K}_d$. (For the conclusions given in (i) and (ii) it is enough to use, for example, the map $\pi^{(d+c)}_{c,0}$.) *Q.E.D.*(Proposition 5)

Proposition 6 *Assume that* $\mathbf{K} = \langle \mathbf{K}_d \mid d \in \omega \rangle$ *is a* $\mathcal{K}$*-sequence,* $\langle f^{(d)} \mid d \in \omega \rangle$ *is a* k*-ary* $\mathbf{K}$ *internal-family of functions and for each* $j = 0, 1, \ldots, k-1$, $\langle g^{(d)}_j \mid d \in \omega \rangle$ *is an* l*-ary* $\mathbf{K}$ *intrernal-family of functions. For each* $d \in \omega$*, we define an* l*-ary function* $h^{(d)}$ *on* $\mathtt{universe}(\mathbf{K}_d)$ *by*

$$h^{(d)}(a_0, \ldots, a_{l-1}) = f^{(d)}(g^{(d)}_0(a_0, \ldots, a_{l-1}), \ldots, g^{(d)}_{k-1}(a_0, \ldots, a_{l-1}))$$

for all $a_0, \ldots, a_{k-1} \in \mathtt{universe}(\mathbf{K}_d)$*. Then* $h^{(d)}$ *is an* l*-ary* $\mathbf{K}$ *internal-family of functions.*

Proof. We get the term inducing the family $h^{(d)}$, by substituting the terms inducing the families $g^{(d)}_j$ into the corresponding term for $f^{(d)}$. *Q.E.D.*(Proposition 6)

Proposition 7 *Assume that* $\mathbf{K}$ *is a retrospective and projective* $\mathcal{K}$*-sequence, and for all* $c \in \omega$*,* τ_c *is the term of* $\mathcal{K}$ *whose existence was stated in condition* (6) of the definition of projectivity. Suppose further that $F(x, y_0, \ldots, y_{k-1})$ is a term of $\mathcal{K}$. Then for all $c \in \omega$ with $2^c \geq k$, there exists a term $G(x, z)$ of $\mathcal{K}$ so that for all sufficiently large $d \in \omega$ and for all $a, b_0, \ldots, b_{k-1} \in \mathbf{K}_d$ the following two statements are equivalent:
(i) $\mathbf{K}_d \models F(a, b_0, \ldots, b_{k-1}) = \mathbf{0}$,
(ii) $\mathbf{K}_{d+c} \models G(a, \tau_c(b_0, \ldots, b_{k-1}, \mathbf{0}, \ldots, \mathbf{0})) = \mathbf{0}$.

Proof. The term G is defined by $G(x, y) = h_{F,c}(x, \pi_{c,0}(y), \pi_{c,1}(y), \ldots, \pi_{c,k-1}(y))$, where the term $h_{F,c}$ is defined in Proposition 4 and the term $\pi_{c,i}$ is from condition (7) of the definition of projectivity. Proposition 4 and the definition of projectivity imply that statements (i) and (ii) are equivalent. *Q.E.D.*(Proposition 7)

As we said earlier if Theorem 2 is not true then there is a possibility for quantifier elimination. In the next lemma we show that this really can be done with a firstorder formula φ interpreted in $\mathbf{K}_d$, at the price of getting the equivalent quantifier free formula not in $\mathbf{K}_d$ but in $\mathbf{K}_{d+c}$, where the equivalence is valid for all sufficiently large d, and c depends only on φ.

Definition. Assume that $\mathbf{K} = \langle \mathbf{K}_d \mid d \in \omega \rangle$ is a complete, retrospective, and predictive $\mathcal{K}$-sequence such that the conclusion of Theorem 2 does not hold for $\mathbf{K}$. Then we will say that $\mathbf{K}$ is a counterexample for Theorem 2. □

Lemma 2 *Assume that Theorem 2 does not hold and* $\mathbf{K} = \langle \mathbf{K}_d \mid d \in \omega \rangle$ *is a counterexample for Theorem 2. Then for each firstorder formula* $\varphi(x_0, \ldots, x_{k-1})$ *of* $\mathcal{K}$*, there exist a* $c = c_\varphi \in \omega$ *and a term* $G(x_0, \ldots, x_{k-1}) = G_\varphi(x_0, \ldots, x_{k-1})$ *of* $\mathcal{K}$ *such that, the family of relations* $\mathcal{R}_k[\varphi(x_0, \ldots, x_{k-1})]$ *and* $\mathcal{R}_k[G(x_0, \ldots, x_{k-1}), c]$ *are asymptotically equivalent.*

Proof. Assume that $\varphi(\underline{x})$ has the following prenex from $\varphi(x) \equiv Q_0 z_0, \ldots, Q_{l-1} z_{l-1} P(\underline{z}, \underline{x})$, where $Q_0, \ldots, Q_{l-1}$ are quantifiers and P is a propositional formula. By Lemma 1 we may assume that P is of the form $F(\underline{z}, \underline{x}) = \mathbf{0}$ for a term F of $\mathcal{K}$. We prove the lemma in this form by induction on l, and by always assuming that the inductive assumption holds for all values

of k. For $l = 0$ the statement of the lemma trivially holds with $c = 0$, $G = F$. Assume now that the lemma is true for $l := l - 1$. Lemma 1 and condition (2) from the definition of a regular $\mathcal{K}$-sequence implies that the statement of the lemma is equivalent to the same statement with $\varphi := \neg\varphi$, therefore we may assume that Q_{l-1} is the quantifier $\exists$.

As we have noted earlier, Lemma 1 implies that there exists a term F_1 of $\mathcal{K}$ so that for each sufficiently large d and for each $a_0, \ldots, a_{l-2}, b_0, \ldots, b_{k-1} \in \mathbf{K}_d$, we have that $\mathbf{K}_d \models \exists z_{l-1} P(a_0, \ldots, a_{l-2}, z_{l-1}, b_0, \ldots, b_{k-1})$ is equivalent to $\mathbf{K}_d \models \Phi_1 \equiv \exists z_{l-1} F_1(a_0, \ldots, a_{l-2}, z_{l-1}, b_0, \ldots, b_{k-1}) = \mathbf{0}$. By Proposition 7, there exists a $c_1 \in \omega$, and a term $G_1(x, z)$ of $\mathcal{K}$ so that for all sufficiently large $d \in \omega$ and for all $a_0 \ldots, a_{l-2}, b_0, \ldots, b_{k-1} \in \mathbf{K}_d$, we have that $\mathbf{K}_d \models \Phi_1$ is equivalent to $\mathbf{K}_{d+c_1} \models \exists z_{l-1} G_1(z_{l-1}, \tau_{c_1}(a_0, \ldots, a_{l-2}, b_0, \ldots, b_{k-1}, \mathbf{0}, \ldots, \mathbf{0})) = \mathbf{0}$. We will denote the term $\tau_{c_1}(x_0, \ldots, x_{k+l-2}, \mathbf{0}, \ldots, \mathbf{0})$ by $\tau'_{c_1}(x_0, \ldots, x_{k+l-2})$. Using our assumption that Theorem 2 is not true with $F := G_1$, we get that there exists a term G_2, such that for all sufficiently large $d \in \omega$ and for all $a_0 \ldots, a_{l-2}, b_0, \ldots, b_{k-1} \in \mathbf{K}_d$ we have that $\mathbf{K}_{d+c_1} \models \exists z_{l-1}, G_1(z_{l-1}, \tau'_{c_1}(a_0, \ldots, a_{l-2}, b_0, \ldots, b_{k-1})) = \mathbf{0}$ is equivalent to $\mathbf{K}_{d+c_1} \models G_2(\tau'_{c_1}(a_0, \ldots, a_{l-2}, b_0, \ldots, b_{k-1})) = \mathbf{0}$.

We got that there exists a term G_2 of $\mathcal{K}$ such that for all sufficiently large d, and for all $a_0, \ldots, a_{l-2}, b_0, \ldots, b_{k-1} \in \mathbf{K}_d$, $\mathbf{K}_d \models \exists z_{l-1} P(a_0, \ldots, a_{l-2}, z_{l-1}, b_0, \ldots, b_{k-1})$ is equivalent to $\mathbf{K}_{d+c_1} \models G_2(\tau'_{c_1}(a_0, \ldots, a_{l-2}, b_0, \ldots, b_{k-1})) = \mathbf{0}$. Consequently, by using Proposition 5, we get that the statement $\mathbf{K}_d \models Q_0 z_0, \ldots, Q_{l-1} z_{l-2}, \exists z_{l-1} P(z_0, \ldots, z_{l-1}, b_0, \ldots, b_{k-1})$ is equivalent to $\mathbf{K}_{d+c_1} \models Q_0 z_0, \ldots, Q_{l-1} z_{l-2}, G_2(\tau'_{c_1}(\pi_{c_1,0}(z_0), \ldots, \pi_{c_1,0}(z_{l-2}), b_0, \ldots, b_{k-1})) = \mathbf{0})$, which can be written in the form of $\mathbf{K}_{d+c_1} \models \varphi_1(b_0, \ldots, b_{k-1})$, where φ_1 is a firstorder formula of $\mathcal{K}$ containing $l - 1$ quantifiers in its prenex form. Therefore we may apply the inductive assumption with $\varphi := \varphi_1$. We get that there exists a term G of $\mathcal{K}$ so that for all sufficiently large $d \in \omega$ and for all $b_0, \ldots, b_{k-1} \in \mathbf{K}_d$ we have that $\mathbf{K}_{d+c_1} \models Q_0 z_0, \ldots, Q_{l-1} z_{l-2}, G_2(\tau'_{c_1}(\pi_{c_1,0}(z_0), \ldots, \pi_{c_1,0}(z_{l-2}), b_0, \ldots, b_{k-1})) = \mathbf{0})$ is equivalent to $\mathbf{K}_{d+c_1+c_2} \models G(b_0, \ldots, b_{k-1})$, that is, $\mathbf{K}_d \models \varphi(b_0, \ldots, b_{k-1})$ iff $\mathbf{K}_{d+c_1+c_2} \models G(b_0, \ldots, b_{k-1})$. Since this is true for all choices of $b_0, \ldots, b_{k-1} \in \mathbf{K}_d$ we have that the family of relations $\mathcal{R}_k[\varphi(x_0, \ldots, x_{k-1})]$ and $\mathcal{R}_k[G(x_0, \ldots, x_{k-1}), c_1 + c_2]$ are asymptotically equivalent. *Q.E.D.*(Lemma 2)

Our next goal is to express the relation $G(y) = \mathbf{0}$ in $\mathbf{K}_d$, where G is a term of $\mathcal{K}$, with a firstorder formula $\xi(y, z)$ such that the dependence of G will be attained by substituting a parameter for z which depends on G. The formula $\xi(x, z)$ in itself will not depend on G. We will be able to do this if the formula ξ is interpreted in $\mathbf{K}_{d+c}$ where c is sufficiently large with respect to G (but it does not depend on d). We will get that for a suitably chosen $u_{c,G} \in \omega$, and for all sufficiently large $d \in \omega$, $\forall y \in \mathbf{K}_d$, $\mathbf{K}_d \models G(y) = \mathbf{0}$ iff $\mathbf{K}_{d+c} \models \xi(y, u_{c,G})$, where the parameter $u_{c,G}$ depends only on c and G. The importance of this is that we replaced an arbitrarily large term G with a firstorder formula ξ of fixed size. This is important since during the quantifier elimination described in Lemma 2 we have no control on the size of the term G. This is a consequence of the fact that in the proof of Lemma 2 we use the assumption that Theorem 2 is not true and this assumption implies the existence of a term but without any bound on its size.

In the following lemma the assumption "Theorem 2 does not hold" is *not* needed.

Lemma 3 *There exists a firstorder formula $\xi(y, z)$ of $\mathcal{K}$ so that if $\mathbf{K} = \langle \mathbf{K}_d \mid d \in \omega \rangle$ is a $\mathcal{K}$-*

sequence then for each term $G(y)$ of $\mathcal{K}$ and for each sufficiently large $c \in \omega$ there exists an $u_{c,G} \in \omega$ with the property that the family of relations $\mathcal{R}_1[G(y)]$ and $\mathcal{R}_1[\xi(y, u_{c,G}), c]$ are asymptotically equivalent.

Proof. We may assume that all of the function symbols of the language $\mathcal{K}$ has the same arity k, since for each $l < k$, an l-ary function $f(x_0, \dots, x_{l-1})$ can be considered as a k-ary function which does not depend on its last $k - l$ variables $x_k, \dots, x_{k-l-1}$. We will consider the constant symbols also as k-ary function symbols. Assume that all of the function symbols of $\mathcal{K}$, including the constant symbols, are $f_0, \dots, f_{\nu-1}$.

λ will denote the number of subterms of the term G. We claim that there exist functions $r \in \mathtt{func}(\lambda, \nu)$, $g \in \mathtt{func}(\lambda \times k, \lambda)$ so that for all sufficiently large $d \in \omega$ and for all $a \in \mathbf{K}_d$, the following two conditions are equivalent

(i) $\mathbf{K}_d \models G(a) = \mathbf{0}$

(ii) There exists $b_0, \dots, b_{\lambda-1} \in \mathbf{K}_d$ so that $b_0 = a$, $b_{\lambda-1} = 0$, and for all $i = 1, \dots, j$, $b_i = f^{(d)}_{r(i)}(b_{g(i,0)}, \dots, b_{g(i,k-1)})$.

We define the functions r, g in the following way. Let $t_0, \dots, t_{\lambda-1}$ be all of the subterms of $G(y)$, so that t_0 is the variable y, and $t_{\lambda-1}$ is the term G, and each subterm t' comes later in the sequence than any of its proper subterms. We choose the functions r and g such that $t_i = f_{r(i)}(t_{g(i,0)}, \dots, t_{g(i,k-1)})$ for $i = 1, \dots, \lambda - 1$. This completes the definition of r and g. Suppose now that condition (i) holds. Then we choose $b_i \in \mathbf{K}_d$ so that $\mathbf{K}_d \models b_i = t_i(a)$. The definitions of the functions r and g imply that condition (ii) is satisfied. Conversely assume that statement (ii) holds. Again by the definitions of the functions r and g, the sequence b_i gives the values of the terms of $t_i(a)$. Since $b_{\lambda-1} = 0$ we have $\mathbf{K}_d \models G(a) = \mathbf{0}$.

Assume that $c \in \omega$ is sufficiently large. Our next task is to express condition (ii) by a firstorder formula in $\mathbf{K}_{d+c}$. First we note that the regularity of the $\mathcal{K}$-sequence $\mathbf{K}$ implies that there exist firstorder formulas $\eta_0, \eta_1, \eta_2, \eta_3, \eta_4$ such that for each term $G(y)$ of $\mathcal{K}$ there exists a natural number $u_{c,G}$ so that for all sufficiently large $d \in \omega$ the following requirements are met:

(a) for all $i \in \nu + 1$, $i = \nu$ iff $\mathbf{K}_d \models \eta_0(i, u_{c,G})$

(b) for all $i \in \lambda + 1$, $i = \lambda$ iff $\mathbf{K}_d \models \eta_1(i, u_{c,G})$

(c) for all $i \in \lambda, j \in \nu$, $r(i) = j$ iff $\mathbf{K}_d \models \eta_2(i, j, u_{c,G})$

(d) for all $i \in \lambda, j \in k, l \in \lambda$, $g(i, j) = l$ iff $\mathbf{K}_d \models \eta_3(i, j, l, u_{c,G})$

(e) for all $i \in c + 1$, $i = c$ iff $\mathbf{K}_d \models \eta_4(i, u_{c,G})$

These requirements say that the numbers ν, λ and the functions r, g must be definable in a firstorder way from the number $u_{c,G}$, which depends only on c, G but *not* on d, by formulas, which do *not* depend on either G or d. This means that we may speak about ν, λ, r and g in the structure $\mathbf{K}_{d+c}$ by a firstorder formula which does not depend on G or d if this firstorder formula contains $u_{c,G}$ as a parameter.

Condition (ii), that we want to express in $\mathbf{K}_{d+1}$, states the existence of a sequence $b_0, \dots, b_{\lambda-1} \in \mathbf{K}_d$ with certain properties. We will encode such a sequence with a single element of $\mathbf{K}_{d+c}$, so that, these properties will be expressible in a firstorder way. This will make it possible to state the existence of the sequence $b_0, \dots, b_{\lambda-1}$ by a single existential quantification in $\mathbf{K}_{d+c}$.

Since c is sufficiently large with respect to G we may assume that $2^c \geq \lambda$. Each sequence $b_0, \dots, b_{\lambda-1} \in \mathbf{K}_d$ will be represented by the element $w = \tau_c^{(d+c)}(b_0, \dots, b_{\lambda-1}, 0, \dots, 0) \in \mathbf{K}_{d+c}$

where τ_c is the term whose existence is stated in the definition of projectivity.

The definition projectivity imply that there exists a firstorder formula η_5 of $\mathcal{K}$ so that for all $i \in \lambda$, $b \in \mathbf{K}_{d+c}$ we have $b = b_i$ iff $\mathbf{K}_{d+c} \models \eta_5(w, b, i)$.

Finally we have to describe the equations $b_i = \bar{f}_{r(i)}(b_{g(i,0)}, \dots, b_{g(i,k-1)})$ by a firstorder formula in $\mathbf{K}_{d+c}$. $\mathbf{K}$ is retrospective, therefore condition (9) of the definition of a retrospective $\mathcal{K}$-sequence implies that this is possible using c as a parameter in the formula. Condition (e) of the definition of $u_{c,G}$ implies that c is definable from $u_{c,G}$ by a firstorder formula. We got that there exists a firstorder formula $\xi(y, z)$ of $\mathcal{K}$ such that for all $a \in \mathbf{K}_d$ condition (ii) is satisfied iff $\mathbf{K}_{d+c} \models \xi(a, u_{v,G})$. Since conditions (i) and (ii) are equivalent for each sufficiently large d this implies the statement of the lemma. *Q.E.D.*(Lemma 3)

Definition. The firstorder formula ξ whose existence is stated in Lemma 3 is not unique, but we assume that a choice for ξ has been fixed. The integer $u_{c,G}$ defined in the lemma will have the properties described there with this choice of ξ. The smallest integer $c \in \omega$ which satisfies the requirements of the Lemma 3 with ξ will be denoted by $c(G)$. □

Definition. Suppose that $\mathcal{L}$ is a firstorder language and $k \in \omega$. $\mathtt{Form}(\mathcal{L}, k)$ will denote the set of all firstorder formulas of $\mathcal{L}$ with at most k free variables. □

Lemma 4 *Assume that Theorem 2 does not hold and $\mathbf{K} = \langle \mathbf{K}_d \mid d \in \omega \rangle$ is a counter example for Theorem 2. Then there exists a term $G(y, z)$ of $\mathcal{K}$ and functions $h \in \mathtt{func}(\omega, \omega)$, $s \in \mathtt{func}(\mathtt{Form}(\mathcal{K}, 1) \times \omega, \omega)$ such that for all $\ell \in \omega$, and for all firstorder formulas $\varphi(y)$ of $\mathcal{K}$ with $\mathtt{length}(\varphi) \leq \ell$, the families of relations $\mathcal{R}_1[G(y, s(\varphi, \ell)), h(\ell)]$ and $\mathcal{R}_1[\varphi(y)]$ are asymptotically equivalent.*

Remark. This lemma states that the truth value of a firstorder formula $\varphi(y)$ as a function of y, for all formulas $\varphi(y)$ of length at most ℓ, can be determined by evaluating a term $G(y, u)$ in $\mathbf{K}_{d+v}$, where G does not depend on anything, v depends only on ℓ and u depends only on ℓ and φ. Therefore, in some sense, we reduced the question of determining the truth value of a firstorder formula to the evaluation of a term. On the other hand we have to do the evaluation of this term in a larger structure, than the one where the truth value of the formula is considered. □

Proof of Lemma 4. Let $\xi(y, z)$ be the firstorder formula whose existence was stated in Lemma 3. The binary term $G(y, z) = G_\xi(y, z)$ with the properties guaranteed by Lemma 2 will be also the term $G(y, z)$ whose existence is stated in the present lemma. Lemma 2, with $\varphi := \xi$, states the existence of an integer $c_\xi \in \omega$ that we will use later.

We have to define the functions h and s. Recall that if G is a term then $c(G)$ denotes the smallest $c \in \omega$ with the properties in Lemma 3. Let $c'' = \max\{c_\psi + c(G_\psi) \mid \psi \in \mathtt{Form}(\mathcal{K}, 2) \wedge \mathtt{length}(\psi) \leq \ell\}$, $c' = c'' - c_\varphi$, $h(\ell) = c'' + c_\xi$, and $s(\varphi, \ell) = u_{c', G_\varphi}$, where the $u_{c,G}$ is the integer whose existence is guaranteed by Lemma 3.

We prove now that for all $\ell \in \omega$, for all firstorder formulas $\varphi(y)$ of $\mathcal{K}$ with $\mathtt{length}(\varphi) \leq \ell$, for all sufficiently large $d \in \omega$, and for all $a \in \mathbf{K}_d$ we have

(16) $\mathbf{K}_d \models \varphi(a)$ *iff* $\mathbf{K}_{d+h(\ell)} \models G(a, s(\varphi, \ell)) = \mathbf{0}$.

According to Lemma 2, for all $a \in \mathbf{K}_d$, $\mathbf{K}_d \models \varphi(a)$ iff $\mathbf{K}_{d+c_\varphi} \models G_\varphi(a)$. The definitions of c'' and c' implies that $c' \geq c(G_\varphi)$. Therefore by Lemma 3 we have that for all $a \in \mathbf{K}_d$, $\mathbf{K}_{d+c_\varphi} \models G_\varphi(a)$ iff $\mathbf{K}_{d+c_\varphi+c'} \models \xi(a, u_{c',G_\varphi})$. Finally using Lemma 2 again with $k{:=}\ 2$, $\varphi{:=}\ \xi(x_0, x_1)$ we get that for all $a \in \mathbf{K}_d$, $\mathbf{K}_{d+c_\varphi+c'} \models \xi(a, u_{c',G_\varphi})$ iff $\mathbf{K}_{d+c_\varphi+c'+c_\xi} \models G(a, u_{c',G_\varphi})$. These equivalences together imply that for all $a \in \mathbf{K}_d$, $\mathbf{K}_d \models \varphi(a)$ iff $\mathbf{K}_{d+c_\varphi+c'+c_\xi} \models G(a, u_{c',G_\varphi})$, which by the definitions of h and s implies condition (16). *Q.E.D.*(Lemma 4)

Definition. A term $G(y, z)$ of $\mathcal{K}$ with the properties described in Lemma 4, will be called a universal term. We assume that for each universal term G of $\mathcal{K}$ a pair of functions, h, s is fixed with the properties given in Lemma 4. To indicate their dependency on G, we will denote these functions by h_G, s_G. □

Lemma 5 *Assume that* $\mathbf{K}$ *is a predictive* $\mathcal{K}$*-sequence and* $H(x_0, x_1)$ *is a term of* $\mathcal{K}$*. Then there exists a firstorder formula* $\Psi_H(x_0, x_1, w)$ *of* $\mathcal{K}$ *such that for all* $c \in \omega$ *the family of relations* $\mathcal{R}_2[H(x_0, x_1), c]$ *and* $\mathcal{R}_2[\Psi_H(x_0, x_1, c)]$ *are asymptotically equivalent.*

Proof. We will associate with each binary term $t(x_0, x_1)$ of $\mathcal{K}$ a firstorder formula $\Lambda_t(u, v, w, y_0, y_1)$. We want to define Λ_t such that for each fixed $c \in \omega$, if $d \in \omega$ is sufficiently large, then

(17) *for each fixed* $a_0, a_1, p, q \in \mathbf{K}_d$, $(\eta_{d,c}(t(a_0, a_1)))(p, q)$ *iff* $\mathbf{K}_d \models \Lambda_t(p, q, c, a_0, a_1)$,

where $\eta_{d,c}$ is the map described in the definition of predictivity.

We define Λ_t by recursion of the depth (maximal number of nested function symbols) of the term $t(x_0, x_1)$.

Assume first that $t(x_0, x_1)$ is the variable x_i for some $i \in \{0, 1\}$. In this case $\Lambda_t(u, v, w, y_0, y_1)$ is the formula $u = \mathbf{0} \wedge v = y_i$. Property (10)/(i) of the definition of a predictive $\mathcal{K}$-sequence implies that condition (17) is satisfied.

Suppose now that t is an individual constant symbol. Then $\Lambda_t(u, v, w, y_0, y_1) \equiv \Phi_t(u, v, w)$, where the firstorder formula Φ_t is defined in the definition of predictivity. Property (10)/(ii) of the definition of predictivity implies that Λ_t satisfies condition (17).

Let $t(x_0, x_1)$ be a term of the form $f(t_0, \ldots, t_{k-1})$, so that Λ_{t_i}, $i = 0, 1, \ldots, k-1$ has been already defined and it satisfies condition (17). Λ_t is defined by $\Lambda(u, v, w, y_0, y_1) \equiv \Phi(u, v, w, \Lambda_{t_0}(u, v, w, y_0, y_1), \ldots, \Lambda_{t_{k-1}}(u, v, w, y_0, y_1))$. Our inductive assumption implies that for all $i = 0, 1, \ldots, i-1$ condition (17) is satisfied by $t{:=}\ t_i$. Therefore property (10)/(ii) of the definition of predictivity implies that Λ_t satisfies condition (17) as well.

Finally we define the firstorder formula $\Psi_H(x_0, x_1, w)$ by $\Psi_H(x_0, x_1, w) \equiv \forall u, v, \Lambda_H(u, v, w, x_0, x_1) \leftrightarrow (u = \mathbf{0} \wedge v = \mathbf{0})$.

Let $\bar{H} = (H)_{\mathbf{K}_{d+c}}$. Condition (17) implies that for all $a_0, a_1 \in \mathbf{K}_d$, $\mathbf{K}_d \models \Psi_H(a_0, a_1, c)$ is equivalent to the statement that "for all $u, v \in \mathbf{K}_d$, $(\eta_{d,c}(\bar{H}(a_0, a_1)))(u, v)$ iff $(\eta_{d,c}(0))(u, v)$" and since the map $\eta_{d,c}$ is one-to-one, this is equivalent to the statement $\bar{H}(a_0, a_1) = 0$. We got that if $c \in \omega$ is fixed then for all sufficiently large $d \in \omega$ and for all for all $a_0, a_1 \in \mathbf{K}_d$, the following two statements are equivalent: $\mathbf{K}_d \models \Psi_H(a_0, a_1, c)$ and $\mathbf{K}_{d+c} \models H(a_0, a_1) = \mathbf{0}$ which is the statement of the lemma. *Q.E.D.*(Lemma 5)

Proof of Theorem 2. Let $\kappa(x, y, z)$ be the firstorder formula of $\mathcal{K}$ whose existence is stated in condition (5) of the definition of a regular $\mathcal{K}$-sequence. Assume that G is a universal term.

Let φ be the formula $\forall u, v, \kappa(u, v, y) \to \neg\Psi_G(u, v, y)$, where Ψ_G is the formula whose existence is stated in Lemma 5. Let $\ell = \mathtt{length}(\varphi)$, $w = s_G(\varphi, \ell)$, and $c = h_G(\ell)$. By condition (5) of the definition of a regular $\mathcal{K}$-sequence there exists an $r \in \omega$ such that for all sufficiently large $d \in \omega$ we have $\mathbf{K}_d \models \forall x, y,\ \kappa(x, y, r) \leftrightarrow (x = w \wedge y = c)$. Let $d \in \omega$ be sufficiently large. Then by Lemma 4, $\mathbf{K}_d \models \varphi(r)$ iff $\mathbf{K}_{d+c} \models G(r, w) = \mathbf{0}$, where $w = s(\varphi, \ell)$. On the other hand using $\ell = \mathtt{length}(\varphi) \geq \mathtt{length}(\Psi_G)$ and Lemma 5 with $c{:=}\ h(\ell)$ and $z{:=}\ s(\varphi, \ell)$, we get the following sequence of equivalent statements: $\mathbf{K}_d \models \varphi(r)$ iff $\mathbf{K}_d \models \forall u, v, \kappa(u, v, r) \to \neg\Psi_G(u, v, r)$ iff $\mathbf{K}_d \models \neg\Psi_G(w, c, r)$ iff $\mathbf{K}_{d+c} \models \neg G(r, w) = \mathbf{0}$. Consequently $\mathbf{K}_d \models \varphi(r)$ is equivalent to both $\mathbf{K}_{d+c} \models G(r, w) = \mathbf{0}$ and $\mathbf{K}_{d+c} \models \neg G(r, w) = \mathbf{0}$, that is, we reached a contradiction. *Q.E.D.*(Theorem 2).

3 Proof of Theorem 1

Proof of Theorem 1. Theorem 2 implies that it is sufficient to prove that $\mathbf{M} = \langle \mathbf{M}_d \mid d \in \omega \rangle$ is a complete, retrospective, and predictive $\mathcal{M}$-sequence.

The definition of the language $\mathcal{M}$ and $\mathtt{universe}(\mathcal{M}_d) = 2^d$, $d \in \omega$, implies that $\mathbf{M} = \langle \mathbf{M}_d \mid d \in \omega \rangle$ is an $\mathcal{M}$-sequence. We show that it is complete, retrospective, and predictive. For the completeness of $\mathbf{M}$ it is sufficient to prove that it is regular and projective.

$\mathbf{M}$ *is regular.* Condition (1) describes the interpretation of the symbols $\mathbf{0}$ and $\mathbf{1}$ as described in the definition of $\mathbf{M}_d$.

Condition (2). It is sufficient to show that the condition holds for $f(x, y) = \neg x$ and $f(x, y) = x \wedge y$ if we consider 0 and 1 as boolean values. For $f(x, y) = \neg x$ we have $t(x, y) = \mathbf{1} - x$, and for $f(x, y) = x \wedge y$ we have $t(x, y) = xy$.

Condition (3). $\bar{t}(x, y) = \min(\mathbf{1}, x - y)$ meets our requirements.

Condition (4). Such a formula can be easily constructed by using the techniques of Gödel numbering, using only the function symbols $\mathbf{0}, \mathbf{1}, -\mathbf{1}, +, \times, \max, \min$. (Not all of them are needed.)

Condition (5) We use the fact that the functions $\mathcal{F}_0(x) = x - \lfloor x^{\frac{1}{2}} \rfloor^2$, $\mathcal{F}_1(x) = \lfloor x^{\frac{1}{2}} \rfloor - \mathcal{F}_0(x)$ has the property that for each $y, z \in \omega$ there is an $x \in \omega$ with $\mathcal{F}_0(x) = y$ and $\mathcal{F}_1(x) = z$. Indeed, if $x = (y + z)^2 + y$, then $\mathcal{F}_0(x) = y$ and $\mathcal{F}_1(x) = z$. Based on this observation it is easy to see that the formula
$\kappa(x, y, z) \equiv (\max(y, x) = x) \wedge (\max(z, x) = x) \wedge$
$\wedge\, \exists u, (\max(u, x) = x) \wedge (\max(u^2, x) = x) \wedge (\max((u + 1)^2, x) \neq x) \wedge (y = x - u^2) \wedge (z = u - y)$
satisfies the requirements of this condition.

$\mathbf{M}$ *is retrospective.* Conditions (8) and (9). We prove condition (9) in the strong form where the formula $\varphi(x_0, \ldots, x_{k-1}, y, z)$ is of the form $t(x_0, \ldots, x_{k-1}, z) = y$, where t is a term of $\mathcal{K}$. Clearly this gives condition (8) with the term $t(x_0, \ldots, x_{k-1}, \mathbf{1})$.

We consider separately the various possible choices for the function symbol g and in each case we describe the required term t. The term $\mathbf{p}(\div(\mathbf{n}, \mathbf{p}(2, c)))$ will be denoted by $2^{2^{-c}\mathbf{n}}$. $g = \mathbf{1}$, $t = \mathbf{1}$; $g = \mathbf{0}$, $t = \mathbf{0}$; $g = \mathbf{n}$, $t = \div(\mathbf{n}, \mathbf{p}(2, c))$; $g = -\mathbf{1}$, $t = 2^{2^{-c}\mathbf{n}} - \mathbf{1}$; $g = xy$, $t = xy - \div(xy, 2^{2^{-c}\mathbf{n}}))2^{2^{-c}\mathbf{n}}$, $g = x + y$, $t = x + y - \div(x + y, 2^{2^{-c}\mathbf{n}})2^{2^{-c}\mathbf{n}}$; $g = \mathbf{p}(y)$, $t = \min(\mathbf{p}(y), 2^{2^{-c}\mathbf{n}} - \mathbf{1})$; $g = \div(x, y)$, $t = \div(x, y)$; $g = \min(x, y)$, $t = \min(x, y)$; $g = \max(x, y)$, $t = \max(x, y)$; $g = x \cap y$, $t = x \cap y$; $g = \mathcal{N}(x)$, $t = \mathcal{N}(x)$.

In the proof of the Corollary we will have the following: $g = \bar{\mathbf{p}}(x, y)$, $t = \min(\bar{\mathbf{p}}(x, y), 2^{2^{-c}\mathbf{n}} - \mathbf{1})$

Definition. Assume that $a, m \in \omega$, $m > 0$. The least nonnegative residue of a modulo m will be denoted by $\mathtt{res}(a, m)$. □

Proposition 8 *Assume that* $u, v, a, b, m, i \in \omega$, $b \geq 2$, $a < b^m$, $i < m$. *Then* $\mathtt{res}(u, v) = u - v\lfloor \frac{u}{v} \rfloor$ *and*

$$\mathtt{coeff}_i(a, b) = b^{-(m-1)}\mathtt{res}\Big(b^{m-1}\Big\lfloor \frac{a}{b^i} \Big\rfloor, b^m\Big)$$

Proof. $a = a_{m-1}b^{m-1} + \ldots + a_i b^i + \ldots + a_0$, where $a_j = \mathtt{coeff}_j(a, b)$ for $j = 0, 1, \ldots, m-1$. Therefore $a/b^i = a_{m-1}b^{m-1-i} + \ldots a_{i+1}b + a_i + a_{i-1}b^{-1} + \ldots + a_0 b^{-i}$ and consequently $\lfloor a/b^i \rfloor = a_{m-1}b^{m-1-i} + \ldots + a_{i+1}b + a_i$. Multiplying both sides of the last equation by b^{m-1} we get $b^{m-1}\lfloor a/b_i \rfloor = a_{m-1}b^{m-1-i+(m-1)} + \ldots + a_{i+1}b^{1+(m-1)} + a_i b^{m-1} = Mb^m + a_i b^{m-1}$, where M is an integer. The statement of the proposition is an immediate consequence of this equation. *Q.E.D.*(Proposition 8)

$\mathbf{M}$ *is projective.* We will use in this proof that $\mathbf{n}^{(d+c)} = 2^c\mathbf{n}^{(d)}$ and so $2^d = \mathbf{n}^{(d+c)} \div 2^c$. We want to define the terms τ_c and $\pi_{c,k}$ such that if $c \in \omega$, $2^c = \nu$, $k \in \{0, 1, \ldots, \nu - 1\}$, and $d \in \omega$, $2^d = n$ is sufficiently large then for all $a_0, a_1, \ldots, a_{\nu-1} \in \mathbf{M}_d$ we have $\tau_c^{(d)}(a_0, a_1, \ldots, a_{\nu-1}) = \sum_{k=0}^{\nu-1} a_k(2^{2^d})^k$, and for each $a \in \mathbf{M}_{d+c}$, $\pi_{c,k}^{(d+c)}(a) = \mathtt{coeff}_k(a, 2^{2^d})$. Clearly if this holds then the terms $\tau_c, \pi_{c,k}$ satisfy condition (6) of the definition of projectivity.

The definition of τ_c is simply the arithmetic expression $\sum_{k=0}^{\nu-1} a_k(2^{2^d})^k$ written with the function symbols of $\mathcal{M}$. Since τ_c may depend on c we may express c in the form $c = \mathbf{1} + \ldots + \mathbf{1}$. All of the partial results in the expression $\sum_{k=0}^{\nu-1} a_k(2^{2^d})^k$ does not exceed the bound $2^{2^{d+c}} - 1$ so the arithmetic operations occurring in it work the same way in $\mathbf{M}_{d+c}$ as among the integers.

To define the term $\pi_{c,k}$ it is sufficient to show that $\mathtt{coeff}_k(a, 2^{2^d})$ can be computed by a term in $\mathbf{M}_{d+c}$. This is however an immediate consequence of Proposition 8 with $a{:=}\ a$, $b{:=}\ 2^{2^d}$, $m{:=}\ 2^c$. Here we used the fact that the operation $x \times y$ in $\mathbf{M}_{d+c}$ is the least nonnegative residue of xy (computed by the multiplication among integers) modulo 2^{d+c}.

The firstorder formula Γ of condition (7) describes the computation of $\pi_{c,k}$ by the term defined above, but it uses c and k directly as parameters.

$\mathbf{M}$ *is predictive.* Assume that $c \in \omega$ and d is sufficiently large. First we define the map $\eta_{d,c}$ whose existence is required by the definition of predictivity. To make our notation more concise we will write $\eta_{d,c}^{(a)}$ instead of $\eta_{d,c}(a)$.

Assume that $a \in \mathbf{M}_{d+c}$, $2^d = n$, $\nu = 2^c$. Let $a_i = \mathtt{coeff}_i(a, 2^n)$ for $i = 0, 1, \ldots, \nu - 1$. We define $\eta_{d,c}$ by: "for all $u, v \in \mathbf{M}_d$, $\eta_{d,c}^{(a)}(u, v)$ iff $u \in \nu$ and $v = a_u$". This definition implies that if $a \in \mathbf{M}_d$ then for all $u, v \in \mathbf{M}_d$, $\eta_{d,c}^{(a)}(u, v)$ iff $u = 0$ and $v = a$, that is, our definition satisfies condition (10)/(i) from the definition of predictivity.

We define now the firstorder formula $\Phi_f(x, y, z, Y_0, \ldots, Y_{k-1})$ for each function symbol f of $\mathcal{M}$.

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 $\eta_{d,c}$, the formula $\Phi_{\mathbf{c}}$ satisfies condition (10)/(ii) from the definition of predictivity, for all constant symbols $\mathbf{c}$ of $\mathcal{M}$.

We will not use the relation $\eta^{(a)}_{d,c}$ directly in the definition of Φ_f, for the remaining function symbols f of $\mathcal{M}$, but we first define another binary relation $\xi^{(a)}_{d,c}$ 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 $\sum\{2^{u\wr_n} \mid u \in \mathbf{M}_d^k \wedge R(u)\}$. 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 $\mathtt{integer}_k^{-1}(R)$. □

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 $u = \langle u_0, \ldots, u_{k-1}\rangle \in \mathbf{M}_d^k$, $R(u_0, \ldots, u_{k-1})$ implies that for all $i = 0, 1, \ldots, k-1$ with $u_i \in n$.

2. Assume that d, c are positive integers and $a < 2^{n^2}$. Then $\xi^{(a)}_{d,c}$ is the unique binary relation on $\mathbf{M}_d$ which satisfies the following two conditions: (a) The relation $\xi^{(a)}_{d,c}$ is n-restricted, and (b) $\mathtt{integer}_2(\xi^{(a)}_{d,c}) = a$. □

Proposition 9 *There exists a firstorder 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 proposition follows from Proposition 8. *Q.E.D.*(Proposition 9)

The following Proposition states that the relations $\xi^{(a)}_{d,c}$ and $\eta^{(a)}_{d,c}$ can be defined from each other in a firstorder way. It is important that for the definition of the value $\xi^{(a)}_{d,c}(u, v)$ for a fixed pair u, v we may need the values $\eta^{(a)}_{d,c}(x, y)$ for all $x, y \in \mathbf{M}_d$ and vice versa.

Proposition 10 *There exist firstorder formulas $\Psi_i(x, y, z, Z)$, $i = 0, 1$, where x, y, z are individual variables and Z is a variable for a binary relation such that for all $c \in \omega$, for all sufficiently large $d \in \omega$, and for all $a \in \mathbf{M}_{d+c}$ the following holds: $\mathbf{M}_d \models \forall u, v, [\xi^{(a)}_{d,c}(u, v) \leftrightarrow \Psi_0(u, v, c, \eta^{(a)}_{d,c})]$ and $\mathbf{M}_d \models \forall u, v, [\eta^{(a)}_{d,c}(u, v) \leftrightarrow \Psi_1(u, v, c, \xi^{(a)}_{d,c})]$*

Proof. Assume $a \in 2^{2^{d+c}}$ and $a = \sum_{i=0}^{(\nu-1)} a_i(2^{2^d})^\nu$. 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 $\eta^{(a)}_{d,c}$ we can define a_u in a firstorder way in $\mathbf{M}_d$, namely $x = a_u$ iff $\mathbf{M}_d \models \eta^{(a)}_{d,c}(u, x)$. If a_u is given then, by Proposition 9, $\mathtt{coeff}_v(a_u, 2)$ has a firstorder definition in $\mathbf{M}_d$. This completes the definition of Ψ_0. In the firstorder formula Ψ_1 we have to define a_u form its binary coefficients which can be done by using again Proposition 9. *Q.E.D.*(Proposition 10)

Proposition 10 implies that it is sufficient to prove that condition (10) of the definition of predictivity holds in the following modified form. (For the sake of notational simplicity we consider here $\mathbf{p}$ and $\mathcal{N}$ as a binary function symbols whose interpretation in each $\mathbf{M}_d$ is a binary function which depends only in its first variable.)

(18) *Suppose that f is one of the function symbols $+, \times, \mathbf{p}, \div, \max, \min, \cap, \mathcal{N}$ of $\mathcal{M}$ then there exists a firstorder formula $\Phi'_f(x, y, z, Y_0, Y_1)$ where x, y, z are individual 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 $a, b \in \mathbf{M}_{d+c}$, and for all $u, v \in \mathbf{M}_d$, $\xi_{d,c}^{(f^{(d+c)}(a,b))}(u, v)$ is true iff $\mathbf{M}_d \models \Phi'_f(u, v, c, \xi_{d,c}(a), \xi_{d,c}(b))$, where $f^{(d+c)} = (f)_{\mathbf{M}_{d+c}}$.*

In other words given the binary bits of $a, b \in 2^{2^{d+c}}$, each by a binary relation on $\mathtt{universe}(\mathbf{M}_d)$, we have to define in $\mathbf{M}_d$ in a firstorder way the binary bits of $a + b, ab, a \div b = \lfloor a/b \rfloor, 2^a$, $\min(a, b)$, $\max(a, b)$, $a \cap b$, and $\mathcal{N}(a)$ where the operations are defined in the structure $\mathbf{M}_{d+c}$. Since $a \cap b$ and $\mathcal{N}(a)$ are defined by bitwise operations this obviously can be easily accomplished for these two operations so from now on we consider only the remaining ones.

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 firstorder 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 firstorder definable family function or a s.f.d.-family in $\mathbf{M}$ if there exists a firstorder formula $\Gamma(x_0, \dots, x_{w_1-1}, Z)$, where x_i, $i = 0, 1, \dots, w_1 - 1$ 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 $u_0, \dots, u_{w_1-1} \in n$, $\mathtt{relation}_{b,n}(u_0, \dots, u_{w_{1-1}})$ iff $\mathbf{M}_d \models \Gamma(u_0, \dots, u_{w_1-1}, \mathtt{relation}_{a,n})$. □

We prove now that condition (18) is satisfied by each function symbol of $\mathcal{M}$. As we mentioned already this statement trivially holds for the function symbols $\cap$ and $\mathcal{N}$ since the corresponding pointwise boolean operation can be executed on the relations representing the elements of $\mathbf{M}_{d+c}$. For the remaining operations we show now that the corresponding families of functions are are strongly firstorder 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 firstorder 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 firstorder 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 firstorder formulas, that we need for our present purposes, over a structure containing the arithmetic operations. Firstorder formulas describing addition and multiplication in this sense were used in [5]. To make the paper more self-contained we prove all the relevant facts about the firstorder definability of sums of sequences of integers.

Definition. If b is a finite sequence of integers then $\mathbf{S}b$ will denote the sum of its elements. □

Lemma 6 *Assume that $c_0, c_1 \in \omega$. Then there exists a strongly firstorder 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 $\mathbf{S}a = f^{(d)}(a)$.*

Proof or Lemma 6. During the proof we will use the notation $n = 2^d$, $m = 2^n$, and we will always assume that d is sufficiently large with respect to c_0, c_1. We assume that $\langle a_0, \dots, a_{j-1} \rangle \in \mathtt{seq}(j, 2^{n^{c_1}})$ and we will define the binary bits of $\mathbf{S}a$ using the bits of the integers a_i, $a = 0, 1, \dots, j-1$. While describing this definition which goes through several steps, we will indicate the reasons why the definition can be told in $\mathbf{M}_d$ in a firstorder way. We prove the lemma through a sequence of special cases. Throughout the proof when we say that something can be defined by a firstorder formula in $\mathbf{M}_d$ we will always mean a firstorder formula of the type which was used in the definition of a strongly firstorder definable family of functions.

Proposition 11 *Lemma 6 holds with the additional assumption $j = 2$.*

Proof of Proposition 11. We have $a = a_0 + a_1$ and we have to determine the binary bits of $a_0 + a_1$. Assume that $a_0 = \sum_{i=0}^{n^k-1} \alpha_i 2^i$, $a_1 = \sum_{i=0}^{n^k-1} \beta_i 2^i$, and $u + v = \sum_{i=0}^{n^k} \gamma_i 2^i$, where $\alpha_i, \beta_i, \gamma_i \in \{0, 1\}$. Then for all $i = 0, 1, \ldots, n^k$ we define γ_i in the following way. If there exists a $t \in \{0, 1, \ldots, i-1\}$ such that $\alpha_t = \beta_t = 1$ and for all k, with $t < k < i$, $\alpha_k + \beta_k \geq 1$, then $\gamma_i = \alpha_i + \beta_i + 1$. If such a t does not exists then $\gamma_i = \alpha_i + \beta_i$.

This definition of γ_i can be stated in $\mathbf{M}_d$ in a firstorder way, since it requires quantification only on the set of integers $\{0, 1, \ldots, n^{c_0}\}$, while $\mathtt{universe}(\mathbf{M}_d) = 0, 1, \ldots, 2^n - 1$. We have used the ordering of the set $\{0, 1, \ldots, n^{c_0}\}$ which is also available since the operations $\max(x, y)$, $\min(x, y)$ define the natural ordering of $\mathtt{universe}(\mathbf{M}_d)$. *Q.E.D.*(Proposition AR1.1)

Proposition 12 *Lemma 6 holds in the special case when* $j \leq \sqrt{n}$ *and* $\max_{i=0}^{j-1} a_i \leq 2^{\sqrt{n}}$, *where* $a = \langle a_0, \ldots, a_{j-1} \rangle$.

Let $s_0 = 0$, $s_\nu = \sum_{i=0}^{\nu-1} a_i$, for $\nu = 1, \ldots, j$. Each s_ν has at most $\log_2(\sum_{i=0}^{\nu-1} a_i) \leq \log_2(j \max_{i=0}^{j-1} a_i) \leq n^{\frac{1}{2}} + \log_2 j \leq 2n^{\frac{1}{2}}$ bits, so the total number of bits in the sequence $s_1, \ldots, s_j$ is at most $2jn^{\frac{1}{2}} \leq 2n$. In $\mathbf{M}_d$ with a single existential quantifier we may talk about the existence of n-bits, so in $\mathbf{M}_d$ we can define the rth bit γ_r of $\mathbf{S}a$ by saying that: $\gamma_r = 1$ if there exists a sequence $s_0, \ldots, s_j$, and a $b \in 2^n$, such that $s_0 = 0, s_j = b$, for all $i = 1, \ldots, j$, $s_j = a_{j-1} + s_j$ and the rth bit of b is 1. *Q.E.D.*(Proposition 12)

Proposition 13 *Lemma 6 holds in the special case* $j \leq n^{1/2}$

Proof of Proposition 13. Assume that $a = \langle a_0, \ldots, a_{j-1} \rangle$ and for each $i = 0, \ldots, j-1$, $a_i = \sum_{s=0}^{l-1} \alpha_{s,i} 2^s$, where $l = 2n^k$. We partition the interval $[0, l-1]$ into subintervals $I_1, ..., I_r$ each of lengths $\frac{1}{2}n$. For $\delta = 0, 1$, let

$$J_\delta = \bigcup \{I_\nu \mid \nu \in [1, r] \wedge \nu \equiv \delta \pmod 2\}$$

For each $i = 0, 1, \ldots, j-1$ we define two integers $u_{0,i}, v_{1,i} \in [0, 2^l - 1]$ by $u_{\delta,i} = \sum\{\alpha_{s,i} 2^s \mid s \in J_\delta\}$. Proposition 12 implies that for $\nu \in [0, l-1]$ and $\delta \in \{0, 1\}$, the integer $v_\delta^{(\nu)} = \sum\{\alpha_{s,i} 2^s \mid i \in [0, l-1], \nu \in J_\delta \cap I_\nu\}$ is firstorder definable in $\mathbf{M}_d$. For fixed ν, $\mathtt{coeff}_s(v_\delta^{(\nu)}, 2) \neq 0$ implies that $s \in I_\nu \cup I_{\nu+1}$, therefore for a fixed δ if we add the numbers $v_\delta^{(\nu)}$, for example, for all even integers ν, there will be no "carry over" and so the binary bits of v_δ are firstorder definable in $\mathbf{M}_d$. Finally by Proposition 6 the binary bits of their sum $\mathbf{S}a = v_0 + v_1$ are also firstorder definable in $\mathbf{M}_d$. *Q.E.D.*(Proposition 13)

We may complete the proof of the lemma in the following way. We may use Proposition 13 iteratively first adding blocks of size $n^{\frac{1}{2}}$ in the sum $\sum_{i=0}^{j-1} a_i$, and then repeating this for the resulting shorter sum etc. *Q.E.D.*(Lemma 6)

We prove condition (18) 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 (18) for the function symbol $\div$ and (in the proof of the Corollary) for function symbol $\bar{\mathbf{p}}$.

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 firstorder 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 $\mathbf{P}a = f^{(d)}(a)$. $\square$

Lemma 7 *For each fixed $c > 0, \varepsilon > 0$ the pair $\alpha(x) = x^c$, $\beta(x) = 2^{x+x^{1-\varepsilon}}$ is acceptable.*

We prove the lemma by showing how can we create acceptable pairs of functions, possibly by using other acceptable pairs. These constructions are described in the following propositions. In the remaining of the paper if we say that a family of functions is firstorder definable we will mean that it is strongly firstorder definable.

Proposition 14 *Assume that $\langle \alpha(x), \beta(x) \rangle$ is an acceptable pair and $\bar{\alpha}(x), \bar{\beta}(x)$ are functions defined on ω with real values so that for all sufficiently large $d \in \omega$, $\bar{\alpha}(d) \leq \alpha(d)$ and $\bar{\beta}(d) \leq \beta(d)$. Then the pair $\langle \bar{\alpha}(x), \bar{\beta}(x) \rangle$ is also acceptable*

Proof. The statement of the proposition is an immediate consequence of the definition of acceptability.

Proposition 15 *For all $c > 0$ the following pair of function is acceptable: $\alpha(x) = 2$, $\beta(x) = 2^{2^{cx}}$.*

Proof. This is a consequence of Lemma 6, since the multiplication of two l bit integers can be performed as the addition of l integers each with $2l$ bits if we follow the standard method of computing a product. *Q.E.D.*(Proposition 15)

Proposition 16 *Assume that α, β are real valued functions defined on ω, $c > 0$, and for all sufficiently large $d \in \omega$ we have $(\alpha(d))^2 \beta(d) \leq cn$, where $n = 2^d$. Then the pair $\alpha(x), \beta(x)$ is acceptable.*

Proof of Proposition 15. Assume that $a = \langle a_0, \ldots, a_{j-1} \rangle$, and for all $i = 0, 1 \ldots, j$ let $p_i = \prod_{r=1}^{i-1} a_i$. Clearly $p_0 = 1$ and $p_j = \mathbf{P}a$. The integer p_i has at most $i\beta(d) \leq j\beta(d) \leq \alpha(d)\beta(d)$ binary bits. Therefore the total number of bits in the sequence $\langle p_1, \ldots, p_j \rangle$ is at most $j\alpha(d)\beta(d)$ $\leq (\alpha(d))^2 \beta(d) \leq cn$. This implies that we are able to speak about the existence of such a sequence $\langle p_0, \ldots, p_j \rangle$ in a firstorder way. As a consequence, $\mathbf{P}a = x$ will be equivalent to the following firstorder formula in $\mathbf{M}_d$: "there exists a sequence $p_0, \ldots, p_{j-1}$, such that $p_0 = 0$, and for all $i = 1, \ldots, j$, $p_i = a_{i-1}p_{i-1}$ and $p_j = x$". *Q.E.D.*Proposition 16

Proposition 17 *Assume that $\langle \alpha(x), \beta(x) \rangle$ is a pair of acceptable functions, $c > 0$ and $t(x) \in \mathtt{func}(\omega, \omega)$, such that for all sufficiently large $d \in \omega$ we have $(t(d))^{\alpha(d)} \leq 2^{cd}$. Then the pair $\langle \alpha(x), t(x)\beta(x) \rangle$ is also acceptable.*

Proof. Assume that $d \in \omega$ is sufficiently large and $a = \langle a_0, a_1, \ldots, a_{j-1} \rangle \in \mathtt{seq}(\alpha(d), t(d)\beta(d))$. Let $h = \lfloor \beta(d) \rfloor$. For all $i = 0, 1, \ldots, j-1$, $k = 0, 1, \ldots, t(d)$ let $b_{i,k} = \mathtt{coeff}_k(a_i, 2^h)$, that is, $a_i = \sum_{k=0}^{t(d)-1} b_{i,k} 2^{kh}$. Proposition 8 implies that the coefficients $b_{i,k}$ are firstorder definable in $\mathbf{M}_d$.

If we compute the product $\prod_{i=0}^{j-1} a_i$ using $a_i = \sum_{k=0}^{t(d)-1} b_{i,k} 2^{kh}$ and distributivity then we get $(t(d))^j \leq (t(d))^{\alpha(d)} \leq n^c$ terms. Each of these terms is uniquely determined by a function $\lambda \in \mathtt{func}(t(d), j)$, namely the term determined by such a function is $\prod_{i=0}^{j-1} \mathtt{coeff}_{\lambda(i)}(a_i, 2^h) 2^{\lambda(i)h}$. If we separate the powers of 2 in this product we can write it in the form of $2^{h\sum_{i=0}^{j-1}\lambda(i)} \prod_{i=0}^{j-1} \mathtt{coeff}_{\lambda(i)}(a, 2^h)$. We have $\mathtt{coeff}_{\lambda(i)}(a, 2^h) \leq 2^h \leq 2^{\beta(d)}$, and $j \leq \alpha(d)$, therefore the acceptability of the pair $\langle \alpha(x), \beta(x) \rangle$ implies that $\prod_{i=0}^{j-1} \mathtt{coeff}_{\lambda(i)}(a, 2^h)$ is firstorder definable in $\mathbf{M}_d$. By Lemma 6, $\sum_{i=0}^{j-1} \lambda(i)$ is also firstorder definable in $\mathbf{M}_d$. Since the total number of choices for the function $\lambda(i)$ is at most n^c, Lemma 6 implies that the sum that is $\mathbf{P}a$ is also firstorder definable in $\mathbf{M}_d$. *Q.E.D.*(Proposition 17)

Proposition 18 *Assume that $\alpha(x), \beta(x), \gamma(x)$ are functions defined on ω with real values in the interval $[1, \infty)$ and the pairs $\langle \alpha(x), \beta(x)\gamma(x) \rangle$, $\langle \gamma(x), \beta(x) \rangle$ are both acceptable. Then $\langle \alpha(x)\gamma(x), \beta(x) \rangle$ is also acceptable.*

Proof. Assume that $d \in \omega$ is sufficiently large and $a = \langle a_0, \ldots, a_{j-1} \rangle \in \mathtt{seq}(\alpha(d)\gamma(d), 2^{\beta(d)})$. We partition the interval $[0, j-1]$ into at most $\alpha(d)$ intervals $I_0, \ldots, I_{r-1}$ each of size at most $\gamma(d)$. The pair $\langle \gamma(x), \beta(x) \rangle$ is acceptable $\gamma(x) \geq 1$ therefore we can define the products $P_k = \prod_{i \in I_k} a_i$, $k = 0, 1, \ldots, r-1$ in a firstorder way in $\mathbf{M}_d$. Moreover the value of each of these products will be at most $(2^{\beta(d)})^{\gamma(d)} = 2^{\beta(d)\gamma(d)}$. Since the pair $\langle \alpha(x), \beta(x)\gamma(x) \rangle$ is acceptable we are also able to define $\prod_{k=0}^{r-1} P_k = \mathbf{P}a$ in a firstorder way in $\mathbf{M}_d$. *Q.E.D.*(Proposition AR6)

Proof of Lemma 7. Assume that a $\tau \in (0, 1)$ is given. We claim that

(19) *the pair $\langle x^\tau, 2^{x - x^{1-\tau}} \rangle$ is acceptable.*

This is a consequence of Proposition 16 and of the fact that for all sufficiently large $d \in \omega$, we have $d^{2\tau} 2^{d - d^{(1-\tau)}} \leq 2^d$. Suppose that for some integer s the pair $(x^\tau, 2^{x + sx^{(1-\tau)}})$ is acceptable. We can apply Proposition 17 with $\alpha(x) := x^\tau, \beta(x) := 2^{x + sx^{1-\tau}}, t(x) := 2^{x^{1-\tau}}$. Using the fact that $(t(d))^{\alpha(d)} = 2^{d^{1-\tau} d^\tau} = 2^d$, we get that the pair $\langle x^\tau, 2^{x + (s+1)x^{1-\tau}} \rangle$ is also acceptable. With the help of this fact and condition (19), we can show by induction on s, starting with $s = -1$, that the following holds:

(20) *for all $\tau \in (0, 1)$, and for all integers s, the pair $(x^\tau, 2^{x + sx^{1-\tau}})$ is acceptable.*

We want to show that

(21) *for all $\tau \in (0, 1)$ and for all $k, s \in \omega$ the pair $(x^{\tau + \frac{k}{2}}, 2^{x + sx^{1-\tau}})$ is acceptable.*

We prove this statement by induction on k, where the inductive assumption is that the statement holds for a fixed k, with every possible choices of τ and s. For $k = 0$ this is condition (20). Assume now that the statement holds for a fixed $k \in \omega$.

We apply Proposition 18 with $\alpha(x) := x^{\tau + \frac{k}{2}}$, $\gamma(x) := x^{\frac{1}{2}}$ and $\beta(x) := 2^{x + sx^{1-\tau}}$. The first assumption of Proposition 18 is that the pair $A_1 = (\alpha(x), \beta(x)\gamma(x)) = (x^{\tau + \frac{k}{2}}, x^{\frac{1}{2}} 2^{x + sx^{1-\tau}})$ is acceptable. Since $x^{\frac{1}{2}} 2^{x + sx^{1-\tau}} = 2^{x + sx^{1-\tau} + \frac{1}{2}\log_2 x} \leq 2^{x + (s+1)x^{1-\tau}}$ the inductive assumption with $s := s + 1$ and Proposition 14 implies that the pair A_1 is acceptable.

The second assumption is that the pair $A_2 = (\gamma(x), \beta(x)) = (x^{\frac{1}{2}}, 2^{x+sx^{1-\tau}})$ is acceptable. This follows directly from condition (20). Therefore by Proposition 18 the pair $(\alpha(x)\gamma(x), \beta(x)) = (x^{\tau+\frac{k+1}{2}}, 2^{x+sx^{1-\tau}})$ is acceptable which completes the proof of (21). This and Proposition 14 together imply the statement of the lemma. *Q.E.D.*(Lemma 7)

Proposition 19 *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 $a_0 a_1 = f^{(d)}(a)$.*

Proof. The proposition is a special case of Lemma 7.

Using Proposition 19 we can show that condition (18) is satisfied by $f = \times$. Since for each fixed $c > 0$ if d is sufficiently large then $d + d^{\frac{1}{2}} > d + c$, we get that multiplication in $\mathbf{M}_{d+c}$ can be defined in $\mathbf{M}_d$ in the sense of (18). This completes the proof of (18) for $f = \times$.

Proposition 20 *For all $c > 1, c' > 1$, there exists a strongly firstorder definable family of functions $f^{(d)}$, $d \in \omega$, such that for all sufficiently large $d \in \omega$, if $a = \langle a_0, \ldots, a_{j-1}\rangle$ is a sequence of natural numbers such that $a_i \leq 2^{c^i}$ for all $i = 0, 1, \ldots, j-1$ and $c^j \leq 2^{c'd}$, then $\mathbf{P}a = f^{(d)}(a)$.*

Proof. Let $p_i = \prod_{s=0}^{i-1} a_s$. Clearly $p_0 = 1$ and $p_j = \mathbf{P}a$. The number of binary bits in a_i is at most c^i, therefore the total number of bits in p_i is at most $\frac{c^i-1}{c-1}$ and the total number of bits in the sequence $p_1, \ldots, p_j$ is at most $(c-1)^2 c^{j+2} \leq (c-1)^2 c^2 2^{c'd} \leq 2^{(c'+1)d}$. Consequently in $\mathbf{M}_d$ we may speak about the existence of a sequence $p_1, \ldots, p_j$ in a firstorder way. Therefore, $\mathbf{P}a = x$ will be equivalent to the following firstorder formula in $\mathbf{M}_d$: "there exists a sequence $p_0, \ldots, p_{j-1}$, such that $p_0 = 0$, and for all $i = 1, \ldots, j$, $p_i = a_{i-1}p_{i-1}$ and $p_j = x$". *Q.E.D.*Proposition 20

Now we show that condition (18) is satisfied by $f = \mathbf{p}$ and, for the proof of the Corollary, we show that it is satisfied by $f = \bar{\mathbf{p}}$. Since the proof for $f = \bar{\mathbf{p}}$ can be easily converted into a proof for $f = \mathbf{p}$ we describe here only the $f = \bar{\mathbf{p}}$ case.

Proposition 21 *There exist strongly firstorder definable families $f_q^{(d)}$, $d \in \omega$, $q = 0, 1, 2$ such that for all sufficiently large d the following holds, where $n = 2^d$:*

(i) if $a < 2^n$, then $f_0^{(d)}(a)$ is the sequence $u = \langle u_0, \ldots, u_{j(a)-1}\rangle$, where $u_i = a^{2^i}$, and $j(a)$ is the smallest natural number with $a^{2^{j(a)}} \geq 2^n$, and $f_1^{(d)}(a) = j(a)$.

(ii) if $a < 2^n$ and $b < j(a)$, then $f_2(\langle a, b\rangle) = a^b$.

Proof. Statement (i) is an immediate consequence of Proposition 20. To prove statement (ii) assume that $d \in \omega$ is sufficiently large $a < 2^n$, $b < j(a)$. We have $b = \sum_{i=0}^{j(a)} \mathtt{coeff}_i(b, 2)2^i$. Proposition 8 implies that $\alpha_i = \mathtt{coeff}_i(b_2)$ is firstorder definable in $\mathbf{M}_d$. We may write a^b as the product $\prod_{i=0}^{j(a)} a^{\alpha_i 2^i}$. Statement (i) and Proposition 20 together imply that a^b is firstorder definable in $\mathbf{M}_d$. *Q.E.D.*(Proposition 21)

The integer a^b can be written in the form of $a^b = (a^{j(a)})^k a^t$, where $t < j(a)$. Assume that $a^b \leq 2^{2^{cd}}$. Then $a^{j(a)} > 2^d = n$ implies that $k \leq c$ therefore according to Lemma 7 and Proposition 21 $a^{j(a)}$ and a^t both can be defined in $\mathbf{M}_d$, and then again by Proposition (20) their product is also firstorder definable in $\mathbf{M}_d$. This completes the proof of condition (18) for $f = \bar{\mathbf{p}}$ and $f = \mathbf{p}$.

Now we prove condition (18) for $f = \div$. Assume that $a, b \in \mathbf{M}_{cd}$ is given and we want to define $\lfloor a/b \rfloor$ in $\mathbf{M}_d$ in a firstorder way. First we describe a way, using general mathematical language, to compute $\lfloor a/b \rfloor$ and then we show that it can be translated into a firstorder formula of $\mathcal{M}$ over $\mathbf{M}_d$.

(i) First we note that it is sufficient to find integers t, l such that $\frac{1}{b} - t2^l < 2^{-cn-1}$. The reason for this is that in the possession of the integers t, l we can compute $\alpha = at2^l$ and $|\alpha - \lfloor a/b \rfloor| < \frac{1}{2}$ 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 $4c$ terms of this geometric series. Clearly $w = \frac{1}{zb} + R_1$, where $|R_1| < 2^{-3n}$. Consequently $\frac{1}{b} = z\frac{1}{zb} = z(w - R_1) = zw + R_2$, where $|R_2| < 2^{-2cn}$.

Now we show the all the quantities in this computation can be defined in a firstorder way in $\mathbf{M}_d$.

Stage (i). The definition of t and l will be described later. However if we have t and l Proposition 19 implies that we may define the product $at2^l$ in a firstorder way in $\mathbf{M}_d$. The rounding also can be done in a firstorder 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 firstorder definable in $\mathbf{M}_d$.

Stage (iii). Proposition 19 implies that the product zb can be defined in $\mathbf{M}_d$. Using Lemma 6 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. Lemma 7 implies that such a product can be defined in $\mathbf{M}_d$ and by Lemma 6 the sum of the first $4c$ terms can be defined as well. Therefore we defined w and by Proposition 19 we can define zw as well. This completes the proof of the fact that condition (18) is satisfied by $f = \div$, and also the proof of predictivity of $\mathbf{M}$. *Q.E.D.*(Theorem 1)

4 A counterexample related to Theorem 2

In this section we give an example for a $\mathcal{K}$-sequence $\mathbf{K}$ where the conclusion of Theorem 2 does not hold. (Naturally some of the assumptions of the theorem do not hold either.)

Lemma 8 *Assume that $\mathcal{L}$ is a firstorder language with equality, with no relation symbols other than equality, and with a finite number of constant and function symbols, among them the constant symbol $\mathbf{0}$. Then there exists an extension $\mathcal{L}'$ of $\mathcal{L}$ with a finite number of function symbols, and there exists a function which assigns to each term $F(x, y)$ of $\mathcal{L}'$ a term $G_F(x)$ of $\mathcal{L}'$ so that the following holds.*

Assume that for all $n \in \omega$, M_n is an interpretation of $\mathcal{L}$ with $\mathtt{universe}(M_n) = 2^n$ *and with* $(\mathbf{0})_{M_n} = 0$. *Then for all $n \in \omega$, there exists an interpretation M'_n of $\mathcal{L}'$ so that* $\mathtt{universe}(M'_n) = \mathtt{universe}(M_n)$, *$M'_n$ is an extension of M_n and the sequence M'_n, $n \in \omega$ has the following property. For all terms $F(x, y)$ of $\mathcal{L}'$ and for all sufficiently large $n \in \omega$, we have*

$$M'_n \models \forall a, \Big(G_F(a) = \mathbf{0} \leftrightarrow \exists x, F(x, a) = \mathbf{0}\Big)$$

Proof. First we describe the language $\mathcal{L}'$ and the interpretations of some of its function symbols. Then we will sketch the the main ideas of proof. Assume that $f_0, \ldots, f_{k-1}$ are function symbols of a firstorder language $\mathcal{L}_1$ each with arity r. We will say that the sequence $f = \langle f_0, \ldots, f_{k-1} \rangle$ is a k-dimensional function symbol vector of $\mathcal{L}_1$ with arity r. If it does not cause any misunderstanding we will write M_n instead of $\mathtt{universe}(M_n)$.

The definition of $\mathcal{L}'$. We get $\mathcal{L}'$ by extending $\mathcal{L}$ with

(i) a unary function symbol $\mathbf{a}$,

(ii) a function symbol h with arity four, and

(iii) with a four dimensional function symbol vector $g = \langle g_0, g_1, g_2, g_3 \rangle$ with arity six.

We will interpret $\mathbf{a}$ in the following way, for each n, if, $u, v \in 2^n$ and $u + 1 \equiv v \pmod{2^n}$, then $M_n \models \mathbf{a}(u) = v$. That is $(\mathbf{a})_{M_n}$ is the function adding 1 mod 2^n. For each $b \in \omega$, $\tilde{b}$ will denote the term $\mathbf{a}(\ldots \mathbf{a}(\mathbf{0}))$ containing exactly b copies of $\mathbf{a}$. Clearly if $2^n > b$ then $M_n \models \tilde{b} = b$.

Let $T_0(x, y), T_1(x, y), \ldots$ be an enumeration of all binary terms of $\mathcal{L}'$, each may contain only the free variables x, y. We assume that if $i \leq j$ then $\mathtt{length}(T_i) \leq \mathtt{length}(T_j)$.

We fix a function $\vartheta(n)$, $n \in \omega$ so that $\vartheta(n)$ tends to infinity very slowly, in the sense that in the proof we will require several times that n is sufficiently large with respect to $\vartheta(n)$. These requirements will define the needed growth rate of ϑ.

Assume that $F(x, y) = T_b(x, y)$ is a term of $\mathcal{L}'$. We define the term $G_F(z)$ in the following way. First we define a sequence of four dimensional vector terms which may contain only the free variables x, y (a vector term of dimension d is a sequence consisting of d terms). The sequence $s_0(x, y), s_1(a, b), \ldots, s_i(a, b), \ldots$ of four dimensional vector terms is defined by recursion on i. $s_0(x, y) = \langle x, x, y, y \rangle$. Assume that $s_i(x, y)$ has been already defined. Then $s_{i+1}(x, y) = g(s_i(x, y), x, y)$. (This is well-defined since g has arity six and $s_i(x, y)$ is a four dimensional vector.) We define the term $G_F(z)$ by $G_F(z) = h(s_{\vartheta(n)}(z, \tilde{b}))$.

Now we define M'_n. We have already defined $(\mathbf{a})_{M'_n}$. We define now $g^{(n)} = (g)_{M'_n}$ the interpretation of g on the structure M'_n. We define $g^{(n)}$ in the following way. For each fixed $a, b \in M_n$ we the define the function $g_{a,b}(x) = g^{(n)}(x, a, b)$, $x \in M_n^4$. The function $g_{a,b}$ mapping M_n^4 into itself is chosen with uniform distribution from the set of all permutations of M_n^4, which has exactly one cycle. Moreover these random selections of $g_{a,b}$ are mutually independent for all of the possible values of n and a, b.

For the definition of $h^{(n)} = (h)_{M'_n}$ we define another interpretation M''_n of $\mathcal{L}'$. Let $\chi^{(n)}$ be the identically 0 function on M_n^4. M''_n will be an interpretation of $\mathcal{L}'$ on 2^n such that it is an extension of M_n, and $(g)_{M''_n} = g^{(n)}$ and $(h)_{M''_n} = \chi^{(n)}$. (We reserve the notation $h^{(n)}$ for the interpretation of the function symbol h in the structure M'_n.)

$h^{(n)}(x)$, $x \in M_n^4$ is defined in the following way. If there exists exactly one pair $a, b \in M_n$ so that $b \leq \vartheta(\vartheta(n))$, $M'_n \models x = s_{\vartheta(n)}(a, b)$, and for this pair a, b we have $M''_n \models \exists y, T_b(y, a) = \mathbf{0}$, then $h^{(n)}(x) = 1$. Otherwise $h^{(n)}(x) = \chi^{(n)}(x) = 0$. This completes the definition of the

interpretation M'_n. (Note that the term s_i does not contain the function symbol h therefore $M'_n \models x = s_{\vartheta(n)}(a,b)$ is equivalent to $M''_n \models x = s_{\vartheta(n)}(a,b)$.)

We show that with a probability 1 for the randomizations in the definition of the sequence M'_n, $n \in \omega$, the structures M'_n, $n \in \omega$ satisfy the requirements of the lemma. For the proof of this fact we need the following.

Let $V_i(x,y)$ be the set of all four dimensional term vectors $S(x,y) = \langle S_j(x,y) \mid j = 0,1,2,3\rangle$ of the language $\mathcal{L}'$, which may contain only the free variables x, y, such that $\mathtt{length}(S_j(x,y)) \leq i$ for all $j = 0,1,2,3$. For each $a, u \in M_n$, we define a subset $\mathcal{V}_i(a,u)$ of M_n^4 by $\mathcal{V}_i(a,u) = \{(S(a,u))_{M_{n'}} \mid S(x,y) \in V_i(x,y)\}$. Clearly $|\mathcal{V}_i(a,u)| \leq c_1^i$, where $c_1 > 1$ depends only on the language $\mathcal{L}$.

Proposition 22 *For each fixed $i \in \omega$ if n is sufficiently large, $a, b, u \in M_n$, $b \leq \vartheta(\vartheta(n))$ then the probability of $s_{\vartheta(n)}(a,b) \in \mathcal{V}_i(a,u)$ is at most $c_2^i \vartheta(n)|M_n|^{-4}$, where $c_2 > 1$ depends only on $\mathcal{L}$.*

This proposition will guarantee that changing the value of h on $\alpha = s_{\vartheta(n)}(a,b)$ does not change the fact whether $x = u$ is a solution of the equation $F(x,a) = \mathbf{0}$ or not, since α is not among the elements which are of the form $T(a,u)$ where T is a term of length at most $i = \mathtt{length}(F)$. According to the proposition with high probability this will be true simultaneously for all $u \in M_n$.

Proof. For the determination of the set $\mathcal{V}_i(a,u)$ we do not need to know the function $(h)_{M_n}$ since it may take only the values 0 and 1 which are also the values of the terms $\mathbf{0}$ and $\mathbf{a}(\mathbf{0})$. Therefore we may exclude from the definition of the set $\mathcal{V}_i$ the function symbol h. On the other hand we have to know some values of $g^{(n)}$. We start constructing the set $\mathcal{V}_i$ by recursion on i. If we have $\mathcal{V}_i$ already, then to get $\mathcal{V}_{i+1}$ we have to apply all of the M'_n interpretations of the function symbols in $\mathcal{L}'$ (with the exception of h) to the r-tuples of $\mathcal{V}_i$, where r always takes the value of the arity of the corresponding function. Each of these functions, with the exception of $g^{(n)}$, is fixed. The function $g^{(n)}$ however had a probabilistic definition. When we need a value of $g^{(n)}$ in this process then we will randomize it. Since there are only a finite number of functions symbols in $\mathcal{L}'$, we have that $|\mathcal{V}_{i+1}| \leq c_1|\mathcal{V}_i|$ for all $i = 0,1,\ldots$, where c_1 is a suitably chosen constant. Assume now an $i \in \omega$ is fixed and n is sufficiently large. After we have constructed $\mathcal{V}_i$ in the described way, while choosing some values of $g^{(n)}$ as well, we continue the randomization of the values of $g^{(n)}(x,a,b)$, which are needed for for getting the values of $x = s_j(a,b)$, $j = 0,1,\ldots,\vartheta(n)$.

Since n is sufficiently large with respect to i, $\vartheta(n)$ is also sufficiently large with respect to i. $g(x,a,b)$ is a permutation of M_n^4 with one cycle, therefore there exists an $j = 1,\ldots,\vartheta(n)$ such that $s_j(a,b) \notin \mathcal{V}_j(a,u)$. Since the permutation is chosen with uniform distribution with the mentioned property, the probability that there exists a $j' \in [j+1, \vartheta(n)]$, such that $s_{j'}(a,b) \in \mathcal{V}_i(a,u))$ is at most $|\mathcal{V}_i(a,u)|^2\vartheta(n)|M_n|^{-4}$, and so $|\mathcal{V}_i(a,u)| \leq c_1^i$ implies the conclusion of the proposition. *Q.E.D.*(Proposition 22)

Proposition 23 *with a probability of at least $1 - 2^{-n}$ with respect to the randomization of the function $g^{(n)}$ the following conditions are satisfied:*

(22) *for each fixed $x \in M_n^4$, there exists at most one pair $a, b \in M_n$ such that $b \leq \vartheta(n)$ and $M'_n \models x = s_{\vartheta_n}(a,b)$*

(23) *for all* $x \in M_n^4$, $h^{(n)}(x) \neq 0$ *implies that* $x \notin \bigcup\{\mathcal{V}_i(a,u)\}a,u \in M_n, i \in [0,\vartheta(\vartheta(n))]$.

Proof. First we show that condition (22) is satisfied. Assume that we randomize all of the values of $g^{(n)}$ involved in the computation of all of the values $s_i(a,b)$ with $0 \leq i \leq \vartheta(n)$, $0 \leq b \leq \vartheta_n$, $a \in M_n$. This is altogether no more then $(\vartheta(n))^2|M_n| = (\vartheta(n))^2 2^n$ values out of the total $|M_n^4| = 2^{4n}$. Assume that we randomize these values of $g^{(n)}$ sequentially, fixing first a,b and then we randomize the values of $g^{(n)}$ which is needed to determine $s_i(a,b)$ for $i = 0,1,\ldots,\vartheta(b)$. At the time when we have to choose $s_{\vartheta_b}(a,b)$ and the corresponding value of $g^{(n)}$ we have already chosen at most $(\vartheta(n))^2 2^n$ values of the cyclic permutation $g_{a,b}$. Therefore the probability that we will choose a value which already occurred in the process as a value of $g^{(n)}$ is at most $(\vartheta(n))^2 2^{-3n}$. Therefore the probability that this will happen for some a,b and i with the given restrictions is at most $(\vartheta(n))^4 2^{-2n} \leq 2^{-2n}$.

Condition (23) Assume that an $x \in M_n^4$ is fixed with $h^{(n)}(x) \neq 0$. For each fixed $a,u \in M_n$, $i \in [0,\vartheta(\vartheta(n))]$ we give an upper bound on $p_{a,u,i}$, the probability of the event $x \in \bigcup\{\mathcal{V}_i(a,u)\}a,u \in M_n, i \in [0,\vartheta(\vartheta(n))]$

By the definition of $h^{(n)}$, $h^{(n)}(x) \neq 0$ implies that $x = s_{\vartheta(n)}(a,b)$ for suitably chosen a and b. Therefore Proposition 22 implies that $p_{a,u,i} \leq c_2\vartheta(n)|M_n|^{-4}$. Adding the $p_{a,u,i}$ for all possible values for a,u,i we get that the probability that (23) does not hold is at most $\vartheta(n)|M_n|^{-2} \leq |M_n|^{-1} = 2^{-n}$. *Q.E.D.*(Proposition 23).

Proposition 24 *For all terms* $F(x,y)$ *of* $\mathcal{L}'$, *for all sufficiently large* $n \in \omega$, *with a probability of at least* $1 - 2^n$ *the following holds:*

(24) *for all* $a \in M_n$, $M_n' \models \exists x, \Phi(x,a)$ *iff* $M_n'' \models \exists x, \Phi(x,a)$

Proof. Clearly it is sufficient to show that conditions (22) and (23) of Proposition 23 imply condition (24) of this proposition. Assume that $u \in M_n$. Let W be the set of all elements w of M_n such that there is a subterm t of F with $t(u,a) = w$. Since n is sufficiently large we may assume that $\vartheta(\vartheta(n)) > \texttt{length}(F)$. Therefore condition (23) implies that $h^{(n)}(w) = 0$ for all $w \in W$, and we have by definition $(h)_{M_n''}(\mathrm{w})=0$, for all $w \in W$. Since for all other function symbols f of $\mathcal{L}'$, $(f)_{M_n'} = (f)_{M_{n''}}$, we can prove by induction of the depth of a subterm t of F that $(t(u,a))_{M_n'} = (t(u,a))_{M_n''}$, and therefore $(F(u,a))_{M_n'} = (F(u,a))_{M_n''}$. Since this is true for all $u \in M_n$ we get the equivalence of $M_n' \models \exists x, \Phi(x,a)$ and $M_n'' \models \exists x, \Phi(x,a)$. *Q.E.D.*(Proposition 24)

We return now to the proof of Lemma 8. Let $F(x,y)$ be a term of $\mathcal{L}'$, and suppose that n is sufficiently large with respect to $\texttt{length}(F)$. We show that with a probability of at least $p_n = 2^{-n+1}$ we have that for all $a \in M_n$,

(25) $M_n' \models G_F(a) = \mathbf{0} \leftrightarrow \exists x, F(x,a) = \mathbf{0}$

Since $\sum_{n=0}^{\infty} p_n < \infty$ this will imply that with a probability 1 condition (25) holds for each sufficiently large n, that is the conclusion of Lemma 8 holds.

Proposition 23 and Proposition 24 imply that it is sufficient to prove that if all the three conditions (22), (23), and are satisfied by the structure M_n' then condition (25) is also satisfied by M_n. Assume now that the requirements of conditions (22), (23), and are met. Condition

(22) and the definition of $h^{(n)}$ implies that By definition by the definition of G_F we have $M'_n \models G_F(a) = 1 - h(s_{\vartheta(n)}(a,b))$, where $F(x,y) = T_b(x,y)$. Condition (22) and the definition of $h^{(n)}$ implies that $h(s_\vartheta(n)(a,b)) = 1$ iff $M''_n \models \exists x, F(x,a)$. By condition (24) this is equivalent to $M'_n \models \exists x, F(x,a)$ which completes the proof of condition (25).

References

[1] A.V. Aho, J.E. Hopcroft, J.D. Ullman, *The Design and Analysis of Computer Algorithms*, Addison-Wesley, 1974.

[2] M. Ajtai, *Determinism versus Nondeterminism for Linear Time RAMs with Memory Restrictions*, Journal of Computer and Systems Science, 65(1): 2-37, (2002)

[3] M. Ajtai, *Oblivious RAMs without cryptographic assumptions*, Electronic Colloquium on Computational Complexity (ECCC), 17:28, 2010.

[4] 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.

[5] M. Ajtai, Y. Gurevich, *Monotone versus positive*, Journal of the ACM (JACM), Vol. 34, Issue 4, Oct. 1987, pp. 1004-1015.

[6] E. Artin. *Galois Theory*, Dover Publications, 1998. (Reprinting of second revised edition of 1944, The University of Notre Dame Press).

[7] 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.

[8] 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.

[9] M. Davis, H. Putnam and J. Robinson, *The decision problem for exponential diophantine equations*, Ann. of Math. (2) 74 (1961), 425-436. 3. J. P. Jones, Three universal representations of r.e. sets, J. Symbolic Logic 43 (1978), 335-351.

[10] A. Magid, *Differential Galois theory*, Notices of the American Mathematical Society 46 (9): 1999.

[11] L. Fortnow, *Time-space tradoffs for satisfiability*, Journal of Computer and System Sciences, 60:337-353, 2000.

[12] Ju. V. Matijasevic, *Enumerable sets are diophantine*, Dokl. Akad. Nauk SSSR 191 (1970), 279-282. English transi.: Soviet Math. Doklady 11 (1970), 354-358.

[13] W. Paul, N. Pippenger, E. Szemerédi, and W. Trotter. *On determinism versus nondeterminism and related problems*, In Proceedings of the 24th IEEE Symposium on Foundations of Computer Science, pages 429-438. IEEE, New York, 1983.

[14] G. Takeuti, *Proof Theory*, North-Holland, Studies in Logic and the Foundations of Mathematics, Vol. 81, Second edition, 1987.

[15] 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