Mathematical Institute
Slovak Academy of Sciences, Bratislava

Preprint 33/1996

Ivan Korec

A list of arithmetical structures strongest with respect to the first order definability

December 9, 1996
Revised January 29, 1997

PREPRINT SERIES

A LIST OF ARITHMETICAL STRUCTURES STRONGEST WITH RESPECT TO THE FIRST ORDER DEFINABILITY

Ivan Korec

Abstract. A structure with base set $\mathbb{N}$ is strongest with respect to the first order definability in the class of arithmetical structures if and only if the operations $+$, $\times$ are definable in it. A list of such structures is presented. Although structures with Pascal's triangles modulo n are preferred a little, an effort was made to collect as many simply formulated results as possible.

The author asks for further suggestions, comments, remarks, corrections, ...

1. Introduction

A list of (arithmetical) structures strongest with respect of the first order definability power (shortly: def-strongest structures) will be presented. Most of them have the base set $\mathbb{N}$ but also structures with some other universes are considered. (Formal definitions are given below.) The class of arithmetical structures can be quasi-ordered by first order definability power. After the usual factorization we obtain a partially ordered set, and def-strongest structures will form its greatest element. Of course, there are stronger structures (with respect to the first order definability) *outside* of the class of arithmetical structures. However, the class of arithmetical structures is rather natural and very important, and hence it has sense to investigate it.

Of course, the presented list of structures is influenced by the author's area of interest. For example, there is a lot of structures with generalized Pascal triangles (in particular, Pascal's triangles modulo n) in the list. However, an effort was made to include as many *simply formulated* results in this area as possible.

The author asks for help in making the list more complete (also including interesting items with "No:" or "??:") and in completing the bibliography. Also terminological and other corrections are invited; after a time, a revised version will be prepared. The author is grateful to D. Richard, P. Cegielski, S. Grigorieff, A. Bès and some others for their help in preparing the present version.

2. Definitions and technicalities

We shall use usual first order predicate calculus with equality. The symbols like $+$, $\times$, $<$, $|$ etc. will be used in their usual meaning (it usually depends only on the base set of the considered structure). The meaning of almost all symbols is explained when they are used (and also in the Index of symbols). Some operations

1991 *Mathematics Subject Classification.* Primary 03B10, 03C07 Secondary 11B65, 11U07.

Key words and phrases. Elementary definability, Pascal's triangle modulo n, Arithmetical structures, Undecidable theories.

This work is supported by Grant 2/1224 of Slovak Academy of Sciences

usually considered as partial ones are completed to total ones (e. g. by the value 0 for the argument 0). This is suitable from a purely technical reason: First order predicate calculus (usually) does not work with partial operations.

We shall sometimes use lambda notation to describe some operations. The notation $\lambda_{...}(T)$, where ... states instead of k (pairwise distinct) variables and T is a term, denotes the k-ary operation on the actual base set (or on the set written as a superscript of λ), whose values are determined by the term T. The subscript ... also determines the order of the arguments. In most cases here the base set will be $\mathbb{N}$, the set of nonnegative integers; if not it will be determined by the context. If the subscript ... is left it replaces all variables of the term T. (We may do that only if order of the variables is not substantial.) Analogously we shall use the notation $\rho_{...}(A)$ to describe relations; it is a little shorter and better readable than more complete notation $\{\langle\dots\rangle \in \mathbb{N}^k \mid A\}$.

We shall deal with the arithmetical structures defined as follows:

Definition 1. *A structure $\langle \mathbb{N}; X_1, \dots, X_k\rangle$ will be called arithmetical if all $X_1, \dots, X_k$ are arithmetical (i.e., first order definable in $\langle \mathbb{N}; +, \times\rangle$).*

We do not consider structures with infinite signature. Notice that every recursive structure is arithmetical; almost all structures below will be recursive.

Definition 2. *An arithmetical structure $\langle \mathbb{N}; X_1, \dots, X_k\rangle$ will be called strongest with respect to the first order definability (or shortly def-strongest) if the usual operations $+$, $\times$ are definable in it.*

Notice that the first order reinterpretability (of $\langle \mathbb{N}; + \times \rangle$) and undecidability are properties weaker than "to be def-strongest". (Roughly speaking, a structure $\mathcal{S}$ has reinterpretation property if A, $\oplus$, $\otimes$, $\equiv$ can be defined in $\mathcal{S}$ so that the factor structure $\langle A; \oplus, \otimes\rangle / \equiv$ is isomorphic with $\langle \mathbb{N}; +, \times\rangle$.)

The notion of def-strongest structure can be extended to arbitrary countably infinite structures as follows.

Definition 3. *Let X be a countably infinite set and let $f : \mathbb{N} \to X$ be a bijection.*

(i) *A relation $Y \subseteq X^2$ will be called (X, f)-arithmetical if there is an arithmetical set $R \subseteq \mathbb{N}^2$ such that $Y = \{(f(x), f(y)) \mid (x, y) \in R\}$. Similarly for relations of other arities and for the operations on X.*

(ii) *A structure $\langle X; X_1, \dots, X_k\rangle$ will be called (X, f)-arithmetical if all operations or relations $X_1, \dots, X_k$ are (X, f)-arithmetical.*

(iii) *An (X, f)-arithmetical structure $\langle X; X_1, \dots, X_k\rangle$ will be called strongest with respect to the first order definability (or (X, f)-def-strongest) if all (X, f)-arithmetical operations and relations are first-order definable in it.*

When no misunderstanding arises we shall delete "(X, f)" in the terms "(X,f)-arithmetical" and "(X, f)-def-strongest".

We shall use Definition 3 for X equal to $\mathbb{Z}$ (the set of integers), $\mathbb{Q}$ (the set of rational numbers), $\mathbb{G}$ (the set of Gaussian integers), and some other (concrete!) set of numbers. A suitable non-numerical universe can be Σ^*, the set of all words in a (fixed) alphabet Σ. Strictly speaking, for every considered set we ought to choose also a canonical bijection f, but in practice there is obviously a big freedom in its choice. Therefore we shall use the term def-strongest (without (X, f)) in all these cases.

Remarks. 1. In many cases $\mathbb{N}$ is a subset of the new universe X; however, we never use the insertion of $\mathbb{N}$ into X to transfer the notion of arithmetical relations or operations.

2. Of course, arithmetical structures on an universe X are isomorphic to some arithmetical structures on $\mathbb{N}$, hence formally it is unnecessary to consider them separately. However, in mathematical practice the new structure can be much more natural and more comfortable to work with.

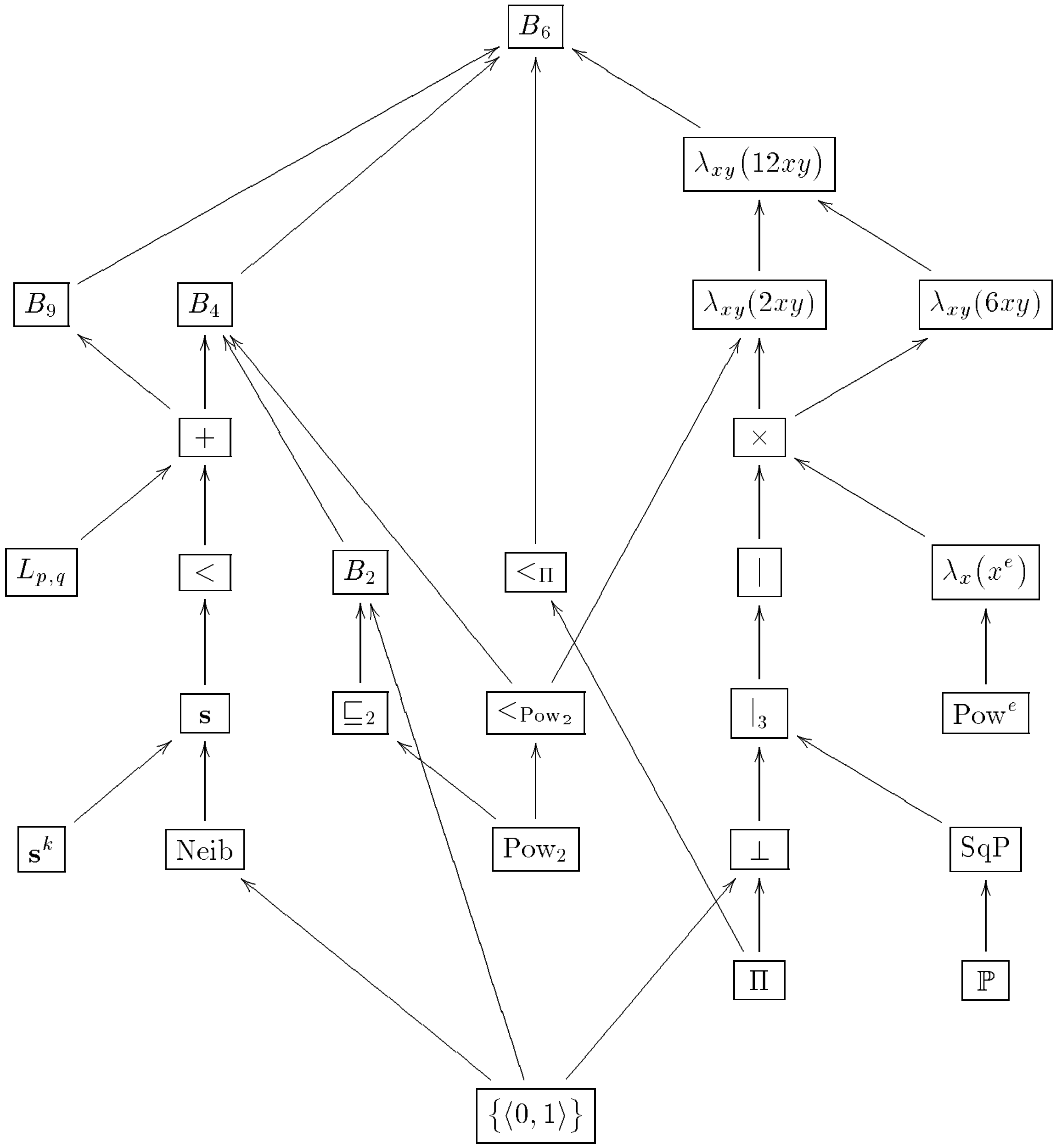

Figure 1. Definability power of some operations and relations on $\mathbb{N}$.

Figure 1 shows ordering of some symbols with respect to their definability power.

(More precisely, we ought to speak about the relations or functions associated to the symbols.) The considered base set is $\mathbb{N}$. An arrow from A to B means that B is (strictly) stronger than A. There are no distinct equivalent symbols in Figure 1, and hence it can be considered as the Hasse diagram of a partially ordered set. (It means that arrows which can be obtained by transitivity are not drawn.) The meaning of symbols can be found in the Index of symbols. Now only notice that B_n denotes Pascal's triangle modulo n, i.e. $B_n(x,y) = \binom{x+y}{x} \operatorname{MOD} n$. The symbol $|_3$ denotes one member of the infinite ascending chain of relations between coprimeness $\perp$ and divisibility $|$. The parameters e, p, q, k ought to be replaced by suitable numerical values (e.g., by integers ≥ 2).

The two left columns contain elements comparable with $+$ and incomparable with $\times$. The two right columns contain elements comparable with $\times$ and incomparable with $+$. The elements of the two central columns (except the top and the bottom one) are incomparable with both $+$, $\times$.

$\boxed{B_6,\ B_{10},\ B_{12},\ \ldots,\ \mathrm{EqB}_6,\ \mathrm{DIV},\ \mathrm{MOD},\ \beta,\ \exp,\ |_{\mathbf{s}},\ \lambda_{xy}(xy+1),\ \in,\ C_0,\ C_6}$

$\boxed{\lambda_{xy}(12xy),\ \lambda_{xy}(2^a 3^b x^m y)\ (a \neq b)}$ $\boxed{\lambda_{xy}(6xy),\ \lambda_{xy}(2^a 3^a x^m y)}$

$\boxed{\lambda_{xy}(2xy),\ \lambda_{xy}(2^a x^m y)}$ $\boxed{\times,\ \lambda_{xy}(x^m y^n)}$ $\boxed{|,\ \gcd,\ \mathrm{lcm}}$ $\boxed{\perp,\ |_1}$

$\boxed{B_{p^2}, B_{p^3}, B_{p^4}, \ldots\ (p \text{ fixed prime})}$ $\boxed{\sqsubseteq_2,\ \sqsubset_2,\ \sqcup_2,\ \sqcap_2,\ \mathrm{EqB}_2}$

$\boxed{+,\ \dot{-},\ \lambda_{xy}(|x-y|),\ \lambda_{xy}(ax+by),\ \lambda_{xy}(ax \dot{-} by)}$

$\boxed{<,\ >,\ \leq,\ \geq,\ \max,\ \min}$ $\boxed{\mathbf{s},\ \lambda_x(x \dot{-} 1)}$ $\boxed{\mathrm{Neib},\ \rho_{xy}(|x-y| \leq k)}$

Figure 2. Operations and relations on $\mathbb{N}$ with the same definability power.

The operation B_6 is stronger than both $+$, $\times$. If an arithmetical structure contains B_6 it is def-strongest, independently on presence of further operations or relations. Therefore the structures with B_6 and additional symbols are not listed. (Of course, the same holds for other operations or relations stronger than both $+$, $\times$; many examples can be found in the top rectangle of Figure 2.) Further, in any def-strongest structure we can replace any symbol by a stronger symbol, and we again obtain a def-strongest structure. Some structures which can be obtained in this way are not listed below. Analogously, the structures with $\leq$ or $\geq$ are not listed because these symbols are equivalent with $<$. Neither the symbol $=$ is explicitly listed because we consider the predicate calculus with equality (i.e. $=$ is considered as a logical symbol).

Figure 2 contains several lists of symbols equivalent to each other from definability point of view; every list is displayed in a rectangle. The parameters a, b, m, n, p run over positive integers (i.e. over $\mathbb{N} \setminus \{0\}$); further conditions on them are explicitly mentioned when necessary.

Now the structure of the further sections will be explained.

Section 3 contains the promised list of def-strongest structures itself. Classification of structures and their partitioning into subsections is based on:

- The number of basic operations and/or relations of a structure. We distinguish three possibilities: one; two; more than two. The constants are not counted here.
- In the case of two operations and/or relations, the relationship of their definability power to that of $+$, $\times$. For every of $+$, $\times$ we distinguish two cases: weaker (or equivalent); incomparable or strictly stronger.

Notice that only very few operations and relations are *simultaneously* weaker than both $+$, $\times$. (Conjecture: They are definable in the structure $\langle \mathbb{N}; 0, 1\rangle$.) We could join them to those weaker than $+$ only.

So we obtain six numbered sections for structures with the base set $\mathbb{N}$. All structures with base sets distinct from $\mathbb{N}$ are gathered into the 7-th section. Some of these sections are further divided into subsections denoted by letters. (Here the criteria are chosen ad hoc. E. g., sometimes presence of B_n is considered.) The details of the classifications are clear from the subheadings. When suitable, the last used letter corresponds to "none of the above, but in this section" (similarly to 99 in MR classification).

The list in Section 3 contains also information about some structures

- which are proved not to be def-strongest; they are introduced by "No:";
- which represent open problems yet; they are introduced by "??:".

They can show which new results can be looked for. A remark is made if a published result uses an unproved conjecture (e.g. Schinzel's hypothesis). However, applicability of such conjectures is not investigated in general.

The list contains mainly concrete structures (or parametrical items from which concrete structures can be obtained). However, sometimes only existence of a def-strongest structure in a class of structures is important, and description of a fixed example is complicated. In such cases only the class of structures (or: the requested properties of the example) are given. If an example can be constructed in two subsections we prefer the narrower one. (For example: "$\langle \mathbb{N}; f, g\rangle$, where f, g are suitable unary functions, f weaker than $\times$" is given in 3.4.b. Therefore "$\langle \mathbb{N}; f, g\rangle$, where f, g are suitable unary functions" is unnecessary in 3.5.)

In parametrical items the parameters runs over nonnegative integers (i.e. over the set $\mathbb{N}$). Additional conditions or another ranges are always explicitly mentioned.

Section 4 contains more details to items of Section 3, including sketches of some proofs. (They are not intended to replace complete proofs in separate papers.) It also contains more general comments, not associated strictly to one item. The symbol $\triangleright$ in an item of Section 3 shows that there is a further comment to it in Section 4. The subheadings and the order of items in both sections coincide (however, some items are omitted in Section 4). Moreover, the subsection 4.0 contains some remarks to Figure 1 and Figure 2.

Section 5 contains alphabetical and systematic index of symbols. The meaning of every symbol is shortly explained. The paper like this one obviously uses many notations. Although no formal system for notation is used (or planned), several rules were usually obeyed. In symbols consisting of several letters capitals are used only for the initial letters of the abbreviated words. Blackboard fonts are used for special number sets (e.g. $\mathbb{Z}$, $\mathbb{N}$). Slanted ($\approx$ italic) and bold letters are preferred for functional symbols, roman letters for predicate symbols. Some letters, e.g. F, f, X, R, have no fixed semantics; their meaning always must be found in the corresponding item. Analogously $\bullet$ has no fixed meaning, and will denote the actual binary operation (e.g., this one which will be contained in the just considered structure).

Bibliography contains not only cited items. The relationship of its items to the presented list of structures varies very much. Many references contain no directly used results but nevertheless they may be useful in further investigation in this area. Some of them are known to the author only indirectly, e.g. from another bibliographies or lists of references.

3. THE LIST OF DEF-STRONGEST STRUCTURES

3.1.a. *Structures with a unique polynomial*

$\langle \mathbb{N}; \lambda_{xy}(xy + x)\rangle$. This structure is contained in some items below. However, reduction to it is used in their proofs. $\triangleright$

$\langle \mathbb{N}; \lambda_{xy}(xy + ax + by + c)\rangle$, where $|a - b| = 1$. $\triangleright$

$\langle \mathbb{N}; \lambda_{xy}(xy + ax + c)\rangle$, where $a + c > 0$. $\triangleright$

$\langle \mathbb{N}; \lambda_{xy}(xy + ax + by)\rangle$, where $(a, b) \notin \{(0, 0), (1, 1)\}$. $\triangleright$

No: $\langle \mathbb{N}; \lambda_{xy}(xy + ax + ay + a^2 - a)\rangle$ for any nonnegative integer a. $\triangleright$

$\langle \mathbb{N}; \lambda_{xy}(xy + x + y + 1)\rangle$. $\triangleright$

$\langle \mathbb{N}; \lambda_{xy}(ax^2 + xy + cx + d)\rangle$, where $a + c + d > 0$. $\triangleright$

$\langle \mathbb{N}; \lambda_{xy}(ax^2 - bxy + cy^2)\rangle$, where $0 < b^2 \leq 4ac$ and $b \mid a$. $\triangleright$

$\langle \mathbb{N}; \lambda_{\dots}(x_1^2 + x_2^2 + x_3^2 + x_4^2 + x_5^2)\rangle$. Conjecture: Four squares suffice.

$\langle \mathbb{N}; \lambda_{xy}(x^n + by)\rangle$, where $n \geq 2$, $b > 0$. Connected with Waring's problem.

$\langle \mathbb{N}; \lambda_{xy}(x^n + y + c)\rangle$, where $n \geq 2$. Connected with Waring's problem.

??: $\langle \mathbb{N}; \mathbf{c}\rangle$, where $\mathbf{c}$ denotes Cantor's pairing function, $\mathbf{c}(x, y) = \frac{(x+y)(x+y+1)}{2} + x$ for all $x, y \in \mathbb{N}$. Conjecture: No (and the theory is decidable). $\triangleright$

No: $\langle \mathbb{N}; \overline{\mathbf{c}}\rangle$, where $\overline{\mathbf{c}}$ is defined by $\overline{\mathbf{c}}(x, y) = \frac{(x+y)(x+y+1)}{2} + x + 1$. Isomorphic with $\langle$ Pairs; $\boxed{\cdot}\rangle$ in 3.7.b. The theory is decidable by [Ma61]. $\triangleright$

3.1.b. *Structures with a unique (non-polynomial) operation*

$\langle \mathbb{N}; \mathrm{DIV}\rangle$, where DIV denotes the quotient by integer division. $\triangleright$

$\langle \mathbb{N}; \mathrm{MOD}\rangle$, where MOD denotes the rest by integer division. $\triangleright$

$\langle \mathbb{N}; \exp\rangle$, where $\exp(x, y) = x^y$. See P. CEGIELSKI [Ce96] where J.-P. PABION & D. RICHARD [PR81], and [Ri81], [Ri85] are mentioned. $\triangleright$

$\langle \mathbb{N}; \beta\rangle$, where $\beta(x, y, t) = x \,\mathrm{MOD}(1 + (y + 1)t)$ is the ternary Gödel beta function. See [Ce96], [PR81], [Ri81], [Ri85].

$\langle \mathbb{N}; C_0\rangle$, where $C_0(x, y) = \binom{x}{y}$ for $x \geq y$ and 0 otherwise. $\triangleright$

??: $\langle \mathbb{N}; B_0\rangle$, where $B_0(x, y) = \binom{x+y}{x}$. The operation B_0 is commutative, and we cannot use the ideas of the previous item.

$\langle \mathbb{N}; B_n\rangle$, where $n > 1$ is divisible by two distinct primes and $B_n(x, y) = \binom{x+y}{x} \,\mathrm{MOD}\, n$. See [Ko93a].

$\langle \mathbb{N}; C_n \rangle$, where $n > 1$ is divisible by two distinct primes and $C_n(x,y) = \binom{x}{y} \operatorname{MOD} n$.

$\langle \mathbb{N}; \lambda_{xy}(\gcd(x+1, y+1)) \rangle$. We can define $\mathbf{s}(x) = \gcd(x+1, x+1)$, then gcd and $|$.

$\langle \mathbb{N}; \lambda_{xy}(\gcd(x,y)+1) \rangle$. We can define $\mathbf{s}(x) = \gcd(x,x)+1$, then gcd and $|$.

$\langle \mathbb{N}; \lambda_{xy}(\operatorname{lcm}(x+1, y+1)) \rangle$. We can define $\mathbf{s}$, then lcm and $|$.

$\langle \mathbb{N}; \lambda_{xy}(\operatorname{lcm}(x,y)+1) \rangle$. We can define $\mathbf{s}$, then lcm and $|$.

$\langle \mathbb{N}; H \rangle$, where $H = \mathrm{GPT}(\mathcal{B}, 2)$ and $\mathcal{B} = \langle \{0,1,2\}, *, 2 \rangle$ is an algebra; GPT means generalized Pascal triangle. See [Ko94b]. $\triangleright$

$\langle \mathbb{N}; \bullet \rangle$, where $\bullet$ is a suitable pairing function (i.e., a bijection $\mathbb{N}^2 \to \mathbb{N}$). $\triangleright$

$\langle \mathbb{N}; \bullet \rangle$, where $\bullet$ is a suitable associative operation with the neutral element 0. (Hence $\langle \mathbb{N}; \bullet, 0 \rangle$ is a monoid; it cannot be free, compare $\langle \Sigma^*, \cdot \rangle$ in 3.7.b.)

3.1.c. *Structures with a unique relation*

$\langle \mathbb{N}; {}_{\mathbf{s}}| \rangle$, where $x \,{}_{\mathbf{s}}|\, y \iff \mathbf{s}(x) \,|\, y$ (in words: ${}_{\mathbf{s}}|$ is the composition of the graph of successor and the divisibility relation). Proof by reduction to $\langle \mathbb{N}; \mathbf{s}, | \rangle$. $\triangleright$

$\langle \mathbb{N}; |_{\mathbf{s}} \rangle$, where $x \,|_{\mathbf{s}}\, y \iff x \,|\, \mathbf{s}(y)$ (in words: $|_{\mathbf{s}}$ is the composition of the divisibility relation and the inverse of the graph of successor). Proof as above. $\triangleright$

$\langle \mathbb{N}; \rho_{xy}(x \,|\, y \vee y = \mathbf{s}(x)) \rangle$. $\triangleright$

$\langle \mathbb{N}; \rho_{xy}(x \,|\, y \vee x = \mathbf{s}(y)) \rangle$.

$\langle \mathbb{N}; \rho_{xy}(x \,|\, y \vee y = \mathbf{s}(x) \vee x = \mathbf{s}(y)) \rangle$.

No: $\langle \mathbb{N}; \rho_{xy}(x \,|\, y \vee y \,|\, x \vee y = \mathbf{s}(x) \vee x = \mathbf{s}(y)) \rangle$ because 0, 1 cannot be distinguished.

$\langle \mathbb{N}; \rho_{xyz}(x + y = z \vee xy = z) \rangle$.

??: $\langle \mathbb{N}; \rho_{xy}(f(x,y) = 0) \rangle$ for a suitable polynomial $f \in \mathbb{Z}[x,y]$. (For polynomials of 3 variables the answer is positive.)

$\langle \mathbb{N}; \in \rangle$, where $x \in y \iff y \operatorname{MOD} 2^{x+1} \geq 2^x$. A point of view: The elements of $\mathbb{N}$ are considered as hereditarily finite sets. $\triangleright$

??: $\langle \mathbb{N}; R \rangle$, where $R = \{(x,y) \mid \mathbf{p}_y \,|\, x\}$ (and $\mathbf{p}_y$ denotes the y-th prime). See [Ce96], [PR81], [Ri81].

$\langle \mathbb{N}; R, 0, 1, 2, 3 \rangle$, where $\langle \mathbb{N}; R \rangle$ is a suitable modular lattice of height 3. $\triangleright$

$\langle \mathbb{N}; R \rangle$, where R is a suitable lattice order of height 3. (Now the lattice need not be modular but no constants are used.) $\triangleright$

$\langle \mathbb{N}; R \rangle$, where R is a suitable irreflexive symmetric binary relation (so $\langle \mathbb{N}; R \rangle$ is a graph in the simplest sense). $\triangleright$

No: $\langle \mathbb{N}; R \rangle$, where R is any equivalence relation. Nevertheless, the theory of $\langle \mathbb{N}; R \rangle$ can be undecidable even for a recursive equivalence relation R. $\triangleright$

$\langle \mathbb{N}; \mathrm{EqB}_6 \rangle$, where $\mathrm{EqB}_6(x,y,u,v) \iff B_6(x,y) = B_6(u,v)$. $\triangleright$

??: $\langle \mathbb{N}; \mathrm{EqB}_n \rangle$, where $n > 1$ is divisible by two distinct primes and $\mathrm{EqB}_n(x,y,u,v) \iff B_n(x,y) = B_n(u,v)$. $\triangleright$

$\langle \mathbb{N}; \mathrm{EqH} \rangle$, where $\mathrm{EqH}(x,y,u,v) \iff H(x,y) = H(u,v)$ and H is defined in the item $\langle \mathbb{N}; H \rangle$ of 4.1.b.

3.2. *Structures with every of $+$, $\times$ replaced by a weaker operation or relation*

$\langle \mathbb{N}; +, \times \rangle$. By the definition.

$\langle \mathbb{N}; +, \mathrm{Sq} \rangle$, where Sq denotes the set of squares. See [Pu57]; a more general statement in **3.4**.

$\langle \mathbb{N}; \mathbf{s}, \times \rangle$, where $\mathbf{s}$ denotes successor; see JULIA ROBINSON [Ro49].

$\langle \mathbb{N}; \mathbf{s}, | \rangle$ where $|$ denotes divisibility; see [Ro49].

$\langle \mathbb{N}; \mathrm{Neib}, \times \rangle$, where Neib is the neighborhood relation: $\mathrm{Neib}(x, y) \iff |x-y| = 1$. See [Ko96a].

$\langle \mathbb{N}; \mathrm{Neib}, | \rangle$, where Neib is the neighborhood relation. See [Ko96a].

$\langle \mathbb{N}; \mathbf{s}^k, \times \rangle$, where k is a positive integer and $\mathbf{s}^k(x) = x + k$. ▷

$\langle \mathbb{N}; \mathbf{s}^k, | \rangle$, where k is a positive integer and $\mathbf{s}^k(x) = x + k$. ▷

$\langle \mathbb{N}; <, \perp \rangle$ where $x \perp y$ denotes "x, y are relatively prime"; see [Ce96] and A. R. WOODS [Wo81].

$\langle \mathbb{N}; <, \rho_{xy}(x \,|\, y \vee y \,|\, x) \rangle$.

??: $\langle \mathbb{N}; \mathbf{s}, \rho_{xy}(x \,|\, y \vee y \,|\, x) \rangle$.

??: $\langle \mathbb{N}; \mathbf{s}, \perp \rangle$, where $\perp$ denotes coprimeness. See [Wo81] or [Ce96] for connection with Erdös-Wood's conjecture. ▷

??: $\langle \mathbb{N}; \mathbf{s}, |_3 \rangle$, where $|_3$ is defined by $x \,|_3\, y \iff \bigwedge_{i \le 3} \forall z \big(\mathbb{P}(z) \wedge z^i \,|\, x \implies z^i \,|\, y\big)$. Interesting also for other constant instead of 3.

??: $\langle \mathbb{N}; \mathrm{Neib}, \perp \rangle$. Problem: Does Erdös-Wood's conjecture suffice for positive solution?

$\langle \mathbb{N}; L_{p,q}, \times \rangle$, where p, q are positive integers and $L_{p,q}(x) = px + q$ (a generalization of $\mathbf{s}^k$). ▷

??: $\langle \mathbb{N}; L_{p,q}, | \rangle$, where p, q are positive integers. Conjecture: The structure is def-strongest.

$\langle \mathbb{N}; +, \mathbb{P} \rangle$ where $\mathbb{P}$ is the set of primes. Proved assuming Schinzel's hypothesis. See P. T. BATEMAN & C. G. JOCKUSCH & A. R. WOODS [BJW93].

No: $\langle \mathbb{N}; <, \mathbb{P} \rangle$ assuming Schinzel's hypothesis. See [BJW93], where WMSO theory of the structure $\langle \mathbb{N}; \mathbf{s}, \mathbb{P} \rangle$ is shown to be decidable. ▷

??: $\langle \mathbb{N}; +, \Pi \rangle$, where Π is the set of prime powers.

3.3. *Structures with two operations or relations, one of them weaker than $+$*

$\langle \mathbb{N}; +, X \rangle$, where X is the range of any non-linear polynomial (of one variable) with nonnegative integer coefficients. See [Bü60].

$\langle \mathbb{N}; \mathbf{s}^k, \lambda_{xy}(xy + x + y) \rangle$, where k is a positive integer and $\mathbf{s}^k(x) = x + k$. ▷

??: $\langle \mathbb{N}; +, \varphi \rangle$, where $n > 1$ and φ denotes the Euler function.

$\langle \mathbb{N}; +, \tau \rangle$, where $n > 1$ and τ denotes the number of divisor function. See [Ko96]. Idea: $x \neq 0$ is a square if and only if $\tau(x)$ is odd.

$\langle \mathbb{N}; +, \sigma \rangle$, where $n > 1$ and σ denotes the sum of divisor function. Idea: Odd x is a square if and only if $\sigma(x)$ is odd.

??: $\langle \mathbb{N}; +, \pi \rangle$, where $n > 1$ and π denotes the prime counting function $\pi(x) = \mathrm{card}\,\{p \in \mathbb{P} \mid p \le x\}$.

??: $\langle \mathbb{N}; +, \mathbf{p} \rangle$, where $\mathbf{p}$ denotes the list of primes ($\mathbf{p}(0) = 2$, $\mathbf{p}(1) = 3, \dots$).

No: $\langle \mathbb{N}; B_n, + \rangle$, if $n > 1$ is a prime power. The elementary theory is decidable.

$\langle \mathbb{N}; <, R \rangle$, where R is any arithmetical pattern-universal binary relation. See [Ko93] (also for the definition of "pattern-universal").

$\langle \mathbb{N}; +, R \rangle$, where R is any arithmetical pattern-universal unary relation. See [Ko93].

??: $\langle \mathbb{N}; \mathbf{s}, R \rangle$, where R is any arithmetical pattern-universal binary relation. See [Ko93].

??: $\langle \mathbb{N}; <, R \rangle$, where R is any arithmetical pattern-universal unary relation. See [Ko93].

3.4.a. *Structures with B_n and one operation or relation weaker than $\times$*

$\langle \mathbb{N}; B_n, \mathrm{Sq} \rangle$, where $n > 1$ and Sq is the set of squares. See [BK96] (and [Ko94] for $n = 2$).

$\langle \mathbb{N}; B_2, \mathrm{Pow}^e \rangle$, where e is odd, $3 \le e \le 19$ and $\mathrm{Pow}^e = \{x^e \mid x \in \mathbb{N}\}$. In particular, $\langle \mathbb{N}; B_2, \mathrm{Cub} \rangle$, where $\mathrm{Cub} = \mathrm{Pow}^3$ is the set of cubes. See [Ko96c]. $\triangleright$

$\langle \mathbb{N}; B_2, \mathrm{Pow}^e \rangle$, where e is odd, $3 \le e \le 19$ and $\mathrm{Pow}^e = \{x^e \mid x \in \mathbb{N}\}$.

$\langle \mathbb{N}; B_n, \mathrm{Pow}^e \rangle$, for all $3 \le n \le 20$, $2 \le e \le 20$ except $(n, e) = (3, 9)$ and $(3, 18)$. See [Ko96c]. $\triangleright$

No: $\langle \mathbb{N}; B_n, \mathrm{Pow}^e \rangle$, where n is a prime, and $e \ge 3$ is a multiple of $\frac{n^2 \cdot (n-1)}{2}$. Automorphism argument (with interchanging n^2, n^3); see [Ko96c]. $\triangleright$

$\langle \mathbb{N}; B_n, \times \rangle$ where $n > 1$. See [Ko95].

$\langle \mathbb{N}; B_n, | \rangle$, where $n > 1$. A corollary of the result with $\times$ instead of $|$ (and an obvious consequence of the result with $\perp$ instead of $|$).

$\langle \mathbb{N}; B_n, \perp \rangle$, where $n > 1$. See [BK96].

??: $\langle \mathbb{N}; B_2, \mathbb{P} \rangle$, where $\mathbb{P}$ is the set of primes.

??: $\langle \mathbb{N}; B_2, \mathrm{SqP} \rangle$, where $\mathrm{SqP} = \{(x, x^2) \mid x \in \mathbb{P}\}$ is the squaring of primes.

??: $\langle \mathbb{N}; B_2, \Pi \rangle$, where Π is the set of prime powers.

3.4.b. *Other structures with two operations or relations, one of them weaker than $\times$*

$\langle \mathbb{N}; L^{m,n}_{p,q}, \times \rangle$, where p, q, n are positive integers, $m \in \mathbb{N}$ and $L^{m,n}_{p,q}(x) = x^m \cdot (px+q)^n$ (a generalization of $L_{p,q}$). $\triangleright$

??: $\langle \mathbb{N}; L^{m,n}_{p,q}, | \rangle$, where p, q, n are positive integers and $m \in \mathbb{N}$.

$\langle \mathbb{N}; \lambda_x(x^2 \dot{-} 1), \times \rangle$. $\triangleright$

??: $\langle \mathbb{N}; \lambda_x(x^2 + 1), \times \rangle$.

??: $\langle \mathbb{N}; X, \times \rangle$, where $X = \{x^2 - x \mid x \in \mathbb{N}\}$.

No: $\langle \mathbb{N}; X, \times \rangle$, where $X = \{x^2 + 1 \mid x \in \mathbb{N}\}$. Automorphism argument; the primes of the form $4k + 3$ can be permuted.

??: $\langle \mathbb{N}; X, \times \rangle$, where $X = \{f(x) \mid x \in \mathbb{N}\}$ for a suitable polynomial $f(x) \in \mathbb{Z}[x]$. Conjecture: The polynomial $f(x) = x^5 \cdot (x + 1)^7$ is suitable here.

$\langle \mathbb{N}; \mathrm{Fac}, \times \rangle$, where $\mathrm{Fac} = \{x! \mid x \in \mathbb{N}\}$ is the set of factorials. Idea: We can define $<$ because $x \le y \iff x! \,|\, y!$ for positive x, y.

$\langle \mathbb{N}; |, <_\Pi \rangle$, where $<_\Pi$ is the restriction of $<$ to the set Π of prime powers. See the preprint [BR95] of A. Bès & D. Richard.

$\langle \mathbb{N}; \times, <_\Pi \rangle$; like the above.

??: $\langle \mathbb{N}; \times, \mathbf{p} \rangle$; where $\mathbf{p}$ denotes the list of primes ($\mathbf{p}(0) = 2$, $\mathbf{p}(1) = 3$, etc.)

No: $\langle \mathbb{N}; \times, \overline{\mathbf{p}} \rangle$; where $\overline{\mathbf{p}}$ is a slightly modified lost of primes: $\overline{\mathbf{p}}(0) = 5$, $\overline{\mathbf{p}}(1) = 7$, $\overline{\mathbf{p}}(2) = 3$, $\overline{\mathbf{p}}(3) = 2$ and $\overline{\mathbf{p}}(x) = \mathbf{p}(x)$ for $x \geq 4$. See [CMR96].

$\langle \mathbb{N}; f, g \rangle$, where f, g are unary functions and f is weaker than $\times$. ▹

$\langle \mathbb{N}; R_1, R_2 \rangle$, where R_1, R_2 are suitable equivalence relations on $\mathbb{N}$, and R_1 is weaker than $\times$. ▹

3.5. *Other structures with two operations or relations*

$\langle \mathbb{N}; B_n, \varphi \rangle$, where $n > 1$ and φ denotes the Euler function. See [Ko96].

$\langle \mathbb{N}; B_n, \sigma \rangle$, where $n > 1$ and σ denotes the sum of divisor function. See [Ko96].

$\langle \mathbb{N}; B_n, \tau \rangle$, where $n > 1$ and τ denotes the number of divisor function. See [Ko96].

$\langle \mathbb{N}; B_n, \lambda \rangle$, where $n > 1$ and λ denotes the Carmichael function. See [Ko96].

$\langle \mathbb{N}; B_n, \pi \rangle$, where $n > 1$ and π denotes the prime counting function, $\pi(x) = \operatorname{card}\{y \in \mathbb{P} \mid y \leq x\}$. See [Ko96].

??: $\langle \mathbb{N}; B_2, <_\mathbb{P} \rangle$, where $<_\mathbb{P}$ is the restriction of $<$ to the set of primes. Conjecture: The structure is def-strongest.

??: $\langle \mathbb{N}; B_2, \mathrm{Pow}_3 \rangle$, where Pow_3 is the set of powers of 3.

No: $\langle \mathbb{N}; B_n, \mathrm{SqPow}_n \rangle$, where n is a prime and SqPow_n denotes the squaring of powers of n. The elementary theory is decidable. See [BK96].

$\langle \mathbb{N}; B_n, \mathrm{SqPow}_n \rangle$, where n is composed. See [BK96]. Interesting only for n prime power (with exponent greater than 1).

$\langle \mathbb{N}; \sqsubseteq_p, \sqsubseteq_q \rangle$, where p, q are distinct primes and $\sqsubseteq_n$ denotes n-adic masking relation. See [BK93a].

??: $\langle \mathbb{N}; \sqsubseteq_m, \sqsubseteq_n \rangle$, where $m > 1$, $n > 1$ are multiplicatively independent. For m, n relatively prime the method of [Ko93a] can be used.

3.6. *Structures with more than two operations or relations*

$\langle \mathbb{N}; \mathbf{s}, \perp, R \rangle$, where $R(p, x)$ means "p is a prime and x is a quadratic residue modulo p". See [Ce96] and GRIGORIEFF & RICHARD [GR89].

$\langle \mathbb{N}; \mathbf{s}, \perp, R \rangle$, where $R(x, y)$ means "y is a power of x". See [Ce96], [GR89] and [Ri85c].

$\langle \mathbb{N}; \mathbf{s}, \perp, \mathrm{Add}_{\mathbb{PN}} \rangle$, where $\mathrm{Add}_{\mathbb{PN}} = \{(p, x, p + x) \mid p \in \mathbb{P}, x \in \mathbb{N}\}$ is a restriction of addition ($\mathbb{P}$ is the set of primes). See [Ce96], [GR89] and [Ri87].

$\langle \mathbb{N}; \mathbf{s}, \perp, \mathrm{Mult}_{\mathbb{PN}} \rangle$, where $\mathrm{Mult}_{\mathbb{PN}} = \{(p, x, px) \mid p \in \mathbb{P}, x \in \mathbb{N}\}$ is a restriction of multiplication. See [Ce96] and [GR89].

??: $\langle \mathbb{N}; B_2, +, \mathbb{P} \rangle$ without any hypothesis. (With Schinzel's hypothesis solved even without B_2. See 3.2.)

$\langle \mathbb{N}; +, V_m, V_n \rangle$,where m, n are multiplicatively independent and $V_n(x) =$ the greatest $d \in \mathrm{Pow}_n$ such than $d \mid x$; see R. VILLEMAIRE [Wi93].

$\langle \mathbb{N}; +, V_2, \mathrm{Pow}_3 \rangle$; see A. BÈS [Be95].

??: $\langle \mathbb{N}; +, \mathrm{Pow}_2, \mathrm{Pow}_3 \rangle$.

No: $\langle \mathbb{N}; <, \mathrm{Pow}_2, \mathrm{Pow}_3 \rangle$; the theory is decidable by SEMENOV [Se80].

??: $\langle \mathbb{N}; f_1, \ldots, f_m, g_1, \ldots g_n \rangle$, where all f_i, g_j are unary functions, all f_i are weaker than $+$ and all g_j are weaker than $\times$.

3.7.a. *Structures with other numerical universes*

$\langle \mathbb{N} \setminus \{0\}; +, \times \rangle$. A slight modification of the above. (Julia Robinson often used this base set.)

$\langle X; +, \times \rangle$, where X is an infinite subset of $\mathbb{N}$ closed under $+$, $\times$. (Such X are rather simple, e. g. they are definable in $\langle \mathbb{N}; + \rangle$.)

??: $\langle \mathbb{N} \setminus \{0\}; \rho_{xy}(x \mid y \vee y \mid x \vee y = \mathbf{s}(x) \vee x = \mathbf{s}(y)) \rangle$. (If it is def-strongest we can simplify the graph $\langle \mathbb{N}; R \rangle$ in 3.1.c.)

$\langle \mathbb{Z}; +, \times \rangle$ where $\mathbb{Z}$ denote the set of all integers. Proof by Four squares theorem.

No: $\langle \mathbb{Z}; +, | \rangle$ because of the automorphism $x \mapsto -x$. See [Ri85].

$\langle \mathbb{Z}; \mathbf{s}, | \rangle$. See [Ri89].

$\langle \mathbb{Z}; <, \perp \rangle$. See [Ri89].

$\langle \mathbb{Z}; \mathbf{s}, +, \perp \rangle$. See [Ri89].

No: $\langle \mathbb{Z}; \mathrm{Neib}, +, | \rangle$ because of the automorphism $x \mapsto -x$.

$\langle \mathbb{Z}; \mathbf{s}, \perp, F \rangle$, where $f(x) = 2^{|x|}$. See [Ri89].

$\langle \mathbb{Q}; +, \times \rangle$ where $\mathbb{Q}$ denotes the set of rational numbers. By [Ro49]; mentioned in [Ce96]. The most difficult part is to define $\mathbb{N}$ (or $\mathbb{Z}$).

No: $\langle \mathbb{Q}; <, \times \rangle$ by [RZ60] and [Ce90b]. The elementary theory is decidable.

$\langle \mathbb{Q}; \mathbf{s}, \times \rangle$ where $\mathbf{s}(x) = x + 1$. We can define $+$ because for $x \neq 0$ we have $x + y = x \times \mathbf{s}(x^{-1} \times y)$. Then we can consider $\langle \mathbb{Q}; +, \times \rangle$.

$\langle \mathbb{G}; +, \times, \mathrm{i}, \mathbb{N} \rangle$, where $\mathbb{G}$ denotes the set of Gaussian integers and i is the imaginary unity ($\mathrm{i}^2 = -1$).

??: $\langle \mathbb{G}; +, \times, \mathrm{i} \rangle$. (I have some ideas, but I do not know whether the result is known.)

No: $\langle \mathbb{G}; +, \times, \mathbb{N} \rangle$ because of the automorphism induced by $\mathrm{i} \mapsto -\mathrm{i}$.

3.7.b. *Structures with non-numerical universes*

No: $\langle \Sigma^*; \cdot \rangle$, where Σ^* is the set of all words in the alphabet Σ and $\cdot$ denotes concatenation. ▹

$\langle \Sigma^*; \cdot, w \rangle$, where Σ^*, $\cdot$ are as above, $\mathrm{card}\,\Sigma > 1$ and the word $w \in \Sigma^*$ contains occurrences of all letters from Σ except at most one.

$\langle P_\omega; \in \rangle$, where P_ω is the set of hereditarily finite sets and $\in$ is set-theoretical membership. ▹

??: $\langle P_\omega; \mathit{join} \rangle$, where P_ω is the set of hereditarily finite sets and *join* is joining of an element to a set: $\mathit{join}(x, y) = x \cup \{y\}$.

No: $\langle \mathrm{Pairs}; \boxed{\cdot} \rangle$, where $\boxed{\cdot}$ is the pairing function, $x \boxed{\cdot} y = \{\{x\}, \{x, y\}\}$, and Pairs is the smallest set which contains $\emptyset$ and is closed under $\boxed{\cdot}$. ▹

$\langle \mathrm{Pairs}; \boxed{\cdot}, \boxplus \rangle$, where Pairs, $\boxed{\cdot}$ are as above and $\boxplus$ denotes *concatenation of pairs*; $x \boxplus y$ arises from x by replacing the rightest $\emptyset$ by y. ▹

??: $\langle \mathrm{UPairs}; \mathit{upf} \rangle$, where *upf* is defined by $\mathit{upf}(x, y) = \{x, y\}$, and UPairs is the smallest set which contains $\emptyset$ and is closed under *upf*. ▹

??: $\langle \mathrm{HF}_k; \mathit{join}_k \rangle$, where HF_k is the smallest set containing $\emptyset$ and closed under join_k, and $\mathit{join}_k(x, y) = x \cup \{y\}$ if $\mathrm{card}(x) < k$ and $= x$ otherwise. ▹

4. Remarks and sketches of proofs

4.0. *Remarks to the figures in Section 2*

1. The items of the top rectangle (with B_6), and many further symbols which can be put into it, are considered in 3.1.a-c (and 4.1.a-c).
2. Let us consider the operation $\lambda_{xy}(kx^m y)$ where $k>0$, $m>0$; some cases with $m=1$ are contained in Figure 1. Let us use the symbol $\bullet$ for this operation. We can show $\times$ and k are definable from $\bullet$ (the converse also holds, and is trivial). Since $u\bullet v{=}1\bullet(u^m v)$ we can define $x=1 \iff \forall u,v\exists y(u\bullet v=x\bullet y)$. Then we can define multiplication by k (because $ky=1\bullet y$), and then the operations $\lambda_{xy}(x^m y)$ and $\lambda_x(x^m)$. The parameter m can be excluded similarly as k, and we obtain $\times$. When we have $\times$ and k we can find prime factors of k; if their exponents are distinct (like for $k=12$) we can distinguish (and define) them.
3. The operations gcd and lcm are the lattice operations to the partial order $|$. Hence these symbols are interdefinable.
4. To consider the symbols $\perp$ and $|_1$, exclude 0 from the further considerations, and denote (only here) the set of prime factors of x by $P(x)$. Then
$$x\perp y \iff P(x)\cap P(y)=\emptyset, \qquad x\,|_1\,y \iff P(x)\subseteq P(y).$$
(The above are not first order formulas!) Now we can use the relationship between the disjointness and the set inclusion.
5. The relation $|_2$ (not displayed in Figure 1) soffices to define $\mathbb{P}$ but it does not suffice to define SqP.
6. The symbol B_{p^k} (p prime, $k>1$) suffices to define both B_p and $+$, and these symbols suffice to define B_{p^k}.
7. In the rectangle containing $\sqsubseteq_2$ the subscripts 2 cannot be replaced by any odd prime. (However, they could be replaced by any integer $n>2$ if we delete the symbol EqB.)
8. To define $+$ from $\lambda_{xy}(|x-y|)$ we can use that for positive x, y, z
$$z=x+y \iff |x-z|=y\wedge|y-z|=x.$$
9. In the rectangle with $<$ parameters cannot be used as freely as in the rectangle with $+$. For example, $\rho_{xy}(x<2y)$ is strictly stronger than $<$.

4.1.a. *Structures with a unique polynomial*

$\langle\mathbb{N};\lambda_{xy}(xy+x)\rangle$. (Let us use the symbol $\bullet$ for the operation in the structure; similarly in the items below.) We can define 0 by $x=0 \iff x\bullet x=x$ and then 1 by
$$x=1 \iff \forall u,v\big(u\bullet v=0\vee\exists y(u\bullet v=x\bullet y)\big).$$
Then we can define $\mathbf{s}(x)=1\bullet x$, and finally $\times$. Now we can use the classical result about $\langle\mathbb{N};\mathbf{s},\times\rangle$, see 3.2.

$\langle\mathbb{N};\lambda_{xy}(xy+ax+by+c)\rangle$, where $|a-b|=1$. We may assume $a=b+1$. The substantial part is definition of $\mathbf{s}$. Here we use that $y=\mathbf{s}(x)$ if the sets $\{u\bullet y\mid u\in\mathbb{N}\}$, $\{x\bullet u\mid u\in\mathbb{N}\}$ differ in a unique element.

$\langle \mathbb{N}; \lambda_{xy}(xy+ax+c)\rangle$, where $a+c>0$. For $c=0$ we can define 0, then multiplication by a as $x \bullet 0$ and $\lambda_{xy}(xy+x)$ using $xy+x=(x\bullet(ay))/a$.

For $a=0$ we can define 0, 1 by

$$x=0 \iff \forall y,z(x\bullet y=x\bullet z), \qquad x=1 \iff \forall u,v\exists y(u\bullet v=x\bullet y),$$

Then we can define $\mathbf{s}^a(x)=x\bullet 1$, and using it $\times$. Now we can use the item $\langle \mathbb{N}; \mathbf{s}^k, \times\rangle$ from 3.2.

For $a>0$, $c>0$ we can define $\mathbf{s}^a$ (as $\mathbf{s}$ in the previous item), $\mathbf{s}^{a+c}$ (using $1\bullet x$) and then also $\mathbf{s}^c$. The last function can be used to reduction to the case $c=0$.

$\langle \mathbb{N}; \lambda_{xy}(xy+ax+by)\rangle$, where $(a,b)\notin\{(0,0),(1,1)\}$. We may assume $a>b$; then we can define $\mathbf{s}^{a-b}$. Further, we can define 0 by the property $0\bullet 0=0$, multiplication by a and by b, and then $\lambda_{xy}(xy+x)$. Further see 3.2, the structure $\langle \mathbb{N}; \mathbf{s}^k, \lambda_{xy}(xy+x)\rangle$.

No: $\langle \mathbb{N}; \lambda_{xy}(xy+ax+ay+a^2-a)\rangle$ for any nonnegative integer a. The structure is isomorphic with $\langle\{x\in\mathbb{N} \mid x\geq a\};\times\rangle$. (Notice that $(x\bullet y)+a=(x+a)\times(y+a)$.) Automorphisms are given by permutations of primes $\geq a$.

$\langle \mathbb{N}; \lambda_{xy}(xy+x+y+1)\rangle$. We can define 0 (it does not belong to the range of $\bullet$), then $\mathbf{s}(x)=0\bullet x$, and then $\times$.

$\langle \mathbb{N}; \lambda_{xy}(ax^2+xy+cx+d)\rangle$, where $a+c+d>0$. Here we can define divisibility by

$$x\,|\,y \iff y=0\vee\forall v\exists u(y\bullet v=x\bullet u).$$

Then we can define 1 and $\mathbf{s}^{a+c+d}(x)=1\bullet x$.

$\langle \mathbb{N}; \lambda_{xy}(ax^2-bxy+cy^2)\rangle$, where $0<b^2\leq 4ac$ and $b\,|\,a$. The substantial trick is that $x\bullet z=y\bullet z \iff x=y\vee a(x+y)=bz$ which enables us to define addition of distinct numbers, and then addition in general.

??: $\langle \mathbb{N}; \mathbf{c}\rangle$, where $\mathbf{c}$ denotes Cantor's pairing function, $\mathbf{c}(x,y)=\frac{(x+y)(x+y+1)}{2}+x$. P. CEGIELSKI and D. RICHARD (Warszawa, December 1996) claimed decidability. For many classical pairing functions instead of $\mathbf{c}$ we obtain an isomorphic structure. However, it is not true in general.

No: $\langle \mathbb{N}; \overline{\mathbf{c}}\rangle$, where $\overline{\mathbf{c}}$ is defined by $\overline{\mathbf{c}}(x,y)=\frac{(x+y)(x+y+1)}{2}+x+1$. Notice that $\overline{\mathbf{c}}$ is a bijection between $\mathbb{N}^2$ and $\mathbb{N}\setminus\{0\}$. The structure is a free groupoid with one generator 0 (i.e., an absolutely free algebra).

The author knows several further examples. However, up to now the results are not complete even for polynomials of degree 2 with two variables.

4.1.b. *Structures with a unique (non-polynomial) operation*

$\langle \mathbb{N}; \mathrm{DIV}\rangle$, where DIV denotes the quotient by integer division. We can define

$$x=0 \iff \forall y(y\,\mathrm{DIV}\,x=0), \qquad x<y \iff y\neq 0\wedge x\,\mathrm{DIV}\,y=0,$$
$$x\,|\,y \iff (\forall z<y)(z\,\mathrm{DIV}\,x<y\,\mathrm{DIV}\,x).$$

Now we can define $\mathbf{s}$, and use the result about $\langle \mathbb{N}; \mathbf{s}, |\rangle$ from 3.3.

See the remark in the next item.

$\langle \mathbb{N}; \mathrm{MOD}\,\rangle$, where MOD denotes the rest by integer division. We can define

$$x = 0 \iff \forall y (y \,\mathrm{MOD}\, x = y), \qquad x \mid y \iff y \,\mathrm{MOD}\, x = 0,$$
$$x < y \iff y \neq 0 \wedge x \,\mathrm{MOD}\, y = x,$$

and continue as above.

Remark: We have considered DIV, MOD as total functions, with the completion $x \,\mathrm{DIV}\, 0 = 0$, $x \,\mathrm{MOD}\, 0 = x$. However, this is only a technical detail. We can also consider them as partial functions where the results of integer division by 0 remain undefined (technically, then we will work with their graphs as ternary relations).

$\langle \mathbb{N}; \exp\,\rangle$, where $\exp(x, y) = x^y$. The definitions of $+$, $\times$ are

$$z = x \times y \iff \forall w \big(w^z = (w^x)^y\big), \qquad z = x + y \iff \forall w \big(w^z = w^x \times w^y\big).$$

$\langle \mathbb{N}; C_0 \rangle$, where $C_0(x, y) = \binom{x}{y}$ for $x \geq y$ and 0 otherwise. (The result was obtained in discussion of D. Richard, P. Cegielski and the author; Paris, July 1996.) We can start with the definition of 0 and $<$. Then we can determine parity of an integer x by the number of y for which $C_0(x, y)$ is maximal (there is unique such y if and only if x is even). Therefore we can define C_2 and then binary masking relation $\sqsubseteq_2$. Then we can define $+$, and since $f(x) = C_0(x, 2)$ is a quadratic polynomial we can define $\times$.

$\langle \mathbb{N}; H \rangle$, where $H = \mathrm{GPT}(\mathcal{B}, 2)$, where $\mathcal{B} = \big\langle \{0, 1, 2\}, *, 2 \big\rangle$ is an algebra of signature (2,0). (GPT: generalized Pascal triangle.) We shall define H directly, without defining $*$ and GPT. H is a binary operation on $\mathbb{N}$ defined by

$$H(x, y) = \begin{cases} 0 & \text{if } x = 0 \text{ or } y = 0, \\ H(x-1, y) & \text{if } x, y > 0 \text{ and } H(x, y-1) \neq 0, \\ (H(x-1, y) + 1) \,\mathrm{MOD}\, 3 & \text{if } x, y > 0 \text{ and } H(x, y-1) = 0. \end{cases}$$

The function H is a strictly $(3, 2)$-modular trellis if the sense of [CG86]; its structure resembles those of B_2 and B_3.

$\langle \mathbb{N}; \bullet \rangle$, where $\bullet$ is a suitable pairing function (i.e., a bijection $\mathbb{N}^2 \to \mathbb{N}$). For every $x \in \mathbb{N}$ we define $(4x+1) \bullet (4x) = 4x + 1$ and $(4x+2) \bullet (4x+3) = 4x + 3$. For all other cases we shall arrange $x \bullet y \notin \{x, y\}$. So we have $4 \mid x \iff \exists y (y \bullet x = y)$. The even values of $\bullet$ will be displaced so that they will code the relation $\in$ from the structure $\langle \mathbb{N}; \in \rangle$ in 3.1.c. Multiples of 4 will denote "true". We shall arrange $x \in y \iff 4 \,|(y \bullet x)$.

4.1.c. *Structures with a unique relation*

$\langle \mathbb{N}; {}_{\mathbf{s}}| \,\rangle$, where $x \,{}_{\mathbf{s}}|\, y \iff \mathbf{s}(x) \mid y$ (in words: ${}_{\mathbf{s}}|$ is the composition of the graph of successor and the divisibility relation). It suffices to define $|$ and $\mathbf{s}$, which can be done by:

$$x \mid y \iff \forall z \big(z \,{}_{\mathbf{s}}|\, x \implies z \,{}_{\mathbf{s}}|\, y\big), \qquad y = \mathbf{s}(x) \iff \forall z \big(y \mid z \iff x \,{}_{\mathbf{s}}|\, z\big).$$

$\langle \mathbb{N}; |_{\mathbf{s}} \rangle$, where $x \,|_{\mathbf{s}}\, y \iff x \,|\, \mathbf{s}(y)$ (in words: $|_{\mathbf{s}}$ is the composition of the divisibility relation and the inverse of the graph of successor). It suffices to define $|$ and $\mathbf{s}$, which can be done by:

$$x \,|\, y \iff \forall z\big(y \,|_{\mathbf{s}}\, z \implies x \,|_{\mathbf{s}}\, z\big), \qquad y = \mathbf{s}(x) \iff \forall z\big(z \,|\, y \iff z \,|_{\mathbf{s}}\, x\big).$$

$\langle \mathbb{N}; \rho_{xy}\big(x \,|\, y \vee y = \mathbf{s}(x)\big) \rangle$. Let R denote the relation from the structure. Using R we can define 0, 1, 2, and we can distinguish odd and even numbers. For odd y we have $y = \mathbf{s}(x)$ if and only if $R(x, y)$ and x is even. For even y (and odd x) we have to take some multiples of y into considerations. So we can define $\mathbf{s}$, and then also $|$, and use $\langle \mathbb{N}; \mathbf{s}, | \rangle$ from 3.2.a.

$\langle \mathbb{N}; \in \rangle$, where $x \in y \iff y \operatorname{MOD} 2^{x+1} \geq 2^x$. A classical result which is often used. Here the elements of $\mathbb{N}$ are considered as hereditarily finite sets (see $\langle \mathbb{N}; P_\omega; \in \rangle$ in 3.7.b and 4.7.b). Hence the whole structure can be considered as the standard model of the theory of finite sets. So we can use the classical von Neumann's construction of ordinals to define ω; the main idea is that every ordinal α is identified with the set of all ordinals smaller than α. Also the arithmetical operations on ω can be constructed. Of course, ω is distinct from the original $\mathbb{N}$. However, we can define a bijection between ω and $\mathbb{N}$, and use it to prove that the considered structure is def-strongest.

$\langle \mathbb{N}; R, 0, 1, 2, 3 \rangle$, where $\langle \mathbb{N}; R \rangle$ is a suitable modular lattice of height 3. (Height 3 means that the maximal chains contain 4 elements.) The considered lattice is isomorphic to the lattice L constructed as follows. Let us consider the extended affine plane $\mathcal{A}$ over the field $\mathbb{Q}$ of rational numbers, i.e. the projective plane over $\mathbb{Q}$ with distinguished ideal line (or: line in infinity). The lattice L will consist of the points and lines of $\mathcal{A}$ (including ideal ones), the whole plane $\mathcal{A}$ and the empty set. It will be partially ordered by inclusion.

Let the constants 0, 1, 2, 3 correspond to the four points $(0,0)$, $(1,0)$, $(0,1)$, and $(1,1)$; they determine the coordinate system, and also the ideal line. The lattice L is modular (we need the ideal elements here). To define R, we chose a bijection g between $\mathbb{N}$ and L which maps 0, 1, 2, 3 onto four mentioned points. Then we use g to transfer the order of L onto $\mathbb{N}$; the obtained order will be R. We can arrange that the relation R is recursive. It would be more comfortable to speak about the lattice L (with four distinguished elements) than about the structure $\langle \mathbb{N}; R, 0, 1, 2, 3 \rangle$.

We can identify any rational number x with the point $(x, 0)$, and then define the arithmetical operations "geometrically" (because, for example, we can speak about parallel lines: two lines (distinct from the ideal line) are parallel if and only if their intersection points with the ideal line coincide). Then we use that the structure $\langle \mathbb{Q}; +, \times \rangle$ is def-strongest (see 3.7.a). We can define a bijection between the elements of L and the new "rational numbers". Therefore L (with four distinguished elements) is def-strongest. Then the structure $\langle \mathbb{N}; R, 0, 1, 2, 3 \rangle$ is def-strongest, too.

Notice that the height 3 of the lattice $\langle \mathbb{N}; R \rangle$ (and of L) cannot be diminished.

$\langle \mathbb{N}; R\rangle$, where R is a suitable lattice order of height 3 (the constructed lattice will not be modular). Let L be the lattice constructed as above from the rational lines and rational points of the affine plane over $\mathbb{Q}$; here we do not use the ideal line and its points. (Now distinct parallel lines are characterized by the property that their meet is $\emptyset$.) Since we cannot use constants we use additional elements to distinguish some points of L. We shall distinguish the points $(x,0)$ for $x \in \mathbb{N}$ and the point $(0,1)$; let $X \subseteq L$ be the set of distinguished points. (Four distinguished points, three from the above and $(3,0)$ instead of $(1,1)$, would suffice to determine the coordinate system; the point $(3,0)$ is used to distinguish the coordinate axes. However, the proof with X infinite is simpler. We need not use the most difficult result of [Ro49] because $\mathbb{N}$ will be given more directly.) Let the extension L' of the lattice L be constructed so that for every $x \in X$ we add a new element $x' > x$ into L; x' will be incomparable with all lines and all points distinct from x. So L' will be a lattice of height 3 (however, it will not be modular). We can use L' to construct R similarly as L was used above.

In L' we can define the set $X' = \{y' \mid y \in X\}$, and then the set X of distinguished points. Then we can define three points mentioned above as constants. (E.g., all elements of X except $(0,1)$ lie on a line; so $(0,1)$ can be defined. Further, $(0,0)$ is not the centre of any segment with endpoints in X, and $(1,0)$ is the centre of exactly one such segment.) Then we again can continue similarly as above.

$\langle \mathbb{N}; R\rangle$, where R is a suitable irreflexive symmetric binary relation (so $\langle \mathbb{N}; R\rangle$ is a graph in the simplest sense). The graph can be obtained from the Hasse diagram of the lattice L' from the item above; the greatest and the smallest elements will be deleted, and the directions of edges will be "forgotten". We can recognize the elements of X by its degree 1; the other elements have infinite degree. The lines and points can be recognized by their distances from the elements of X. Notice also that the graph is bipartite.

No: $\langle \mathbb{N}; R\rangle$, where R is an equivalence relation. We can define at most one constant in such structure, so it cannot be def-strongest.

For the construction of a recursive equivalence relation R with undecidable theory, consider a strictly increasing recursive function f, $f(0) = 0$, such that the difference set $\{f(z+1) - f(z) \mid z \in \mathbb{N}\}$ is not recursive. Let us define R by the formula

$$R(x,y) \iff \exists z\big(f(z) \le x \wedge x < f(z+1) \wedge f(z) \le y \wedge y < f(z+1)\big).$$

The sentences V_k ="some class of R has cardinality k" are expressible in the elementary theory of $\langle \mathbb{N}; R\rangle$. Since the set $\{k \mid V_k \text{ holds}\}$ is not recursive the theory of $\langle \mathbb{N}; R\rangle$ must be undecidable. (Maybe, for every $n \in \mathbb{N}$ the set of its closed formulas with at most n quantifiers is decidable.)

$\langle \mathbb{N}; \mathrm{EqB}_6\rangle$, where $\mathrm{EqB}_6(x,y,u,v) \iff B_6(x,y) = B_6(u,v)$. It is important that we can define six binary predicates $B_6(x,y) = k$ for $k = 0,1,\ldots,5$. For example, we can define $x = 0 \iff \forall y,z\, \mathrm{EqB}_6(x,y,x,z)$ and then

$$B_6(x,y) = 1 \iff \mathrm{EqB}_6(x,y,0,0).$$

Using these six predicates we can define the predicates $B_2(x,y)=0$ and $B_3(x,y)=0$, and then the masking relations $\sqsubseteq_2$, $\sqsubseteq_3$. Now we can use the result about $\langle \mathbb{N}; \sqsubseteq_p, \sqsubseteq_q \rangle$ for p, q distinct primes, see 3.7 and [Ko93a].

??: $\langle \mathbb{N}; \mathrm{EqB}_n \rangle$, where $n>1$ is divisible by two distinct primes and $\mathrm{EqB}_n(x,y,u,v) \iff B_n(x,y)=B_n(u,v)$. The substantial step is definition of n binary predicates $B_n(x,y)=k$ for $k=0,1,\dots,n-1$. This does not seem to be difficult for any concrete n. However, the problem is in the general method of the proof.

4.2. *Structures with every of $+$, $\times$ replaced by a weaker operation or relation*

$\langle \mathbb{N}; \mathbf{s}^k, \times \rangle$, where k is a positive integer and $\mathbf{s}^k(x)=x+k$. We can define the constant $k=\mathbf{s}^k(0)$ and then $\mathbf{s}$ by the formula

$$y=\mathbf{s}(x) \iff k\times y=\mathbf{s}^k(k\times x).$$

$\langle \mathbb{N}; \mathbf{s}^k, | \rangle$, where k is a positive integer and $\mathbf{s}^k(x)=x+k$. Multiplication by a (given or defined) constant is definable from divisibility. Therefore we can use the idea from the previous item.

$\langle \mathbb{N}; L_{p,q}, \times \rangle$, where p,q are positive integers and $L_{p,q}(x)=px+q$ (a generalization of $\mathbf{s}^k$). For $q=1$ we can generalize the classical Tarski-Robinson formula (for x, y, z positive) as follows :

$$x+y=z \iff (1+pxz)\cdot(1+pyz)=1+pz^2\cdot(1+pxy).$$

It can be rewritten as

$$x+y=z \iff L_{p,1}(xz)\cdot L_{p,1}(yz)=L_{p,1}\big(z^2\cdot L_{p,1}(xy)\big).$$

The cases with 0 can be considered separately.

The case $q>1$ can be reduced to the previous one by the definitions

$$q=L_{p,q}(0), \qquad y=L_{p,1}(x) \iff qy=L_{p,q}(qx).$$

??: $\langle \mathbb{N}; \mathbf{s}, \perp \rangle$, where $\perp$ denotes coprimeness. The structure is def-strongest if and only if the following Erdös—Woods conjecture holds:

There is a positive integer k such that for all $x,y\in\mathbb{N}$

$$x=y \iff (\forall i<k)(\forall p\in\mathbb{P})\big(p\,|\,x+i \iff p\,|\,y+i\big).$$

No: $\langle \mathbb{N}; <, \mathbb{P} \rangle$ assuming Schinzel's hypothesis. A. Bès claims (without Schinzel's hypothesis) that $+$ is not definable in any structure $\langle \mathbb{N}; <, X \rangle$ where $X\subseteq\mathbb{N}$ is a unary relation.

4.3. *Structures with two operations or relations, one of them weaker than $+$*

$\langle \mathbb{N}; \mathbf{s}^k, \lambda_{xy}(xy+x+y) \rangle$, where k is a positive integer and $\mathbf{s}^k(x)=x+k$. If $\bullet$ denotes the binary operation from the structure we have $x\bullet y+1=(x+1)(y+1)$. We can prove the following generalization of the classical Tarski-Robinson formula:

$$z=x+y+1 \iff \mathbf{s}^k(x\bullet z)\bullet\mathbf{s}^k(y\bullet z)=\mathbf{s}^{k^2}\big((z\bullet z)\bullet\mathbf{s}^k(x\bullet y)\big);$$

here $\mathbf{s}^{k^2}$ denotes $\mathbf{s}^k$ repeated k times. Indeed, for $x_1 = x+1$, $y_1 = y+1$, $z_1 = z+1$ we can transform the right side of the equivalence as follows:

$$\begin{aligned} 1 + (k + x \bullet z) \bullet (k + y \bullet z) &= k^2 + 1 + (z \bullet z) \bullet (k + x \bullet y) \\ (k + 1 + x \bullet z)(k + 1 + y \bullet z) &= k^2 + (1 + z \bullet z)(k + 1 + x \bullet y) \\ (k + x_1 z_1)(k + y_1 z_1) &= k^2 + z_1^2 (k + x_1 y_1) \\ k z_1 (x_1 + y_1) &= k z_1^2 \\ x_1 + y_1 &= z_1 \\ x + y + 1 &= z \end{aligned}$$

(We have used $k \neq 0$, $z_1 \neq 0$.) Now we can easily define $\mathbf{s}$, and then $+$, $\times$.

4.4.a. *Structures with B_n and one operation or relation weaker than $\times$*

For the case n divisible by two distinct primes see 3.1; only n prime power is interesting here.

$\langle \mathbb{N}; B_2, \mathrm{Pow}^e \rangle$, where e is odd, $3 \le e \le 19$ and $\mathrm{Pow}^e = \{x^e \mid x \in \mathbb{N}\}$. See the next item.

$\langle \mathbb{N}; B_n, \mathrm{Pow}^e \rangle$, for all $3 \le n \le 20$, $2 \le e \le 20$ except $(n, e) = (3, 9)$ and $(3, 18)$. If we can define $+$ then we can define $\times$ without further use of B_n. Therefore it is substantial how to define $+$ for the case when n is prime; it suffices to define $<_{\mathrm{Pow}_n}$ or $\mathit{nextpow}_n$. We can define the set Pow_n^e of powers of p^n using $\mathrm{Pow}_n^e = \mathrm{Pow}_n \cap \mathrm{Pow}^e$. Using properties of p-adic expansions of e-th powers we can define $<_{\mathrm{Pow}_n^e}$; this is done in [Ko96c] for all primes n and exponents $e > 1$. Further, we can define the function "nearest power of p^n" (we omit its exact definition here), and using it (and $<_{\mathrm{Pow}_n^e}$) we can compare those powers of p which are far from each other. Comparing of near powers of p can be reduced to a combinatorial question about the digits of p-adic expansions of e-th powers. This problem was solved for the above values in [Ko96c]. The list of pairs (n, e) can be extended without any principal difficulties.

Conjecture: For $n > 1$, $e > 1$ the structure $\langle \mathbb{N}; B_n, \mathrm{Pow}^e \rangle$ is def-strongest if and only if it has no nontrivial automorphism.

No: $\langle \mathbb{N}; B_n, \mathrm{Pow}^e \rangle$, where n is a prime, and $e \ge 3$ is a multiple of $\frac{n^2 \cdot (n-1)}{2}$. The condition is not necessary for the negative answer. An example not covered by this criterion: $n = 89$, $e = 89^2 \cdot 22$.

4.4.b. *Other structures with two operations or relations, one of them weaker than $\times$*

$\langle \mathbb{N}; L_{p,q}^{m,n}, \times \rangle$, where p, q, n are positive integers, $m \in \mathbb{N}$ and $L_{p,q}^{m,n}(x) = x^m \cdot (px+q)^n$ (a generalization of $L_{p,q}$). We shall reduce this case to that of $\langle \mathbb{N}; L_{p,q}, \times \rangle$ (see 4.2) if we define the function $L_{p,q} = L_{p,q}^{0,1}$. It holds

$$y = L_{p,q}(x) \iff x = 0 \wedge y = q \vee x \neq 0 \wedge x^m y^n = L_{p,q}^{m,n}(x).$$

(Powers must be written as repeated products.) It remains to define the constant q. It can be done by the formula

$$x = q \iff x \neq 0 \wedge x^{m+n} \mid L_{p,q}^{m,n}(x) \wedge \forall y \big(y \neq 0 \wedge y^{m+n} \mid L_{p,q}^{m,n}(y) \implies y \mid x\big).$$

In words: q is the $|$-greatest positive integer x such that $x^{m+n} \mid L_{p,q}^{m,n}(x)$. Indeed, the mentioned condition is (for $x \neq 0$) equivalent with $x^n \mid (px+q)^n$, hence with $x \mid px+q$ and finally with $x \mid q$.

Remark: The condition p, q, n positive is necessary. Otherwise $L_{p,q}^{m,n}$ is definable from $\times$ and a constant, and hence $+$ cannot be definable.

$\langle \mathbb{N}; \lambda_x(x^2 \dot- 1), \times \rangle$. Let us denote the unary operation by F. Let $\mathrm{Neib}_3(y,x,z)$ mean "y, x, z are three consecutive elements of $\mathbb{N}$" (in the ascending or descending order). We can define 0, $\mathbb{P}$ (the set of primes), 2 by the property "$F(2)$ is prime", $4 = 2 \times 2$, and finally

$$\begin{aligned}\mathrm{Neib}_3(y,x,z) \iff & x \neq 0 \wedge yz = F(x) \wedge \\ & \wedge \exists u, v\big(uv = F(2x) \wedge F(u) = 4xy \wedge F(v) = 4xz\big).\end{aligned}$$

Indeed, $\Longrightarrow$ is clear (if $y, z = x \pm 1$ then $u, v = 2x \pm 1$). To prove $\Leftarrow$, take $x \neq 0$, y, z, u, v for which all appropriate equalities hold, i.e.:

$$yz = x^2 - 1, \qquad uv = 4x^2 - 1, \qquad u^2 = 4xy + 1, \qquad v^2 = 4xz + 1.$$

(The second equation implies $u \neq 0$, $v \neq 0$, and this fact was used to obtain the last two equations.) From $(uv)^2 = u^2v^2$ we have

$$\begin{aligned}(4x^2-1)^2 &= 16x^2yz + 4xy + 4xz + 1 = 16x^2(x^2-1) + 4xy + 4xz + 1 \\ 16x^4 - 8x^2 + 1 &= 16x^4 - 16x^2 + 4xy + 4xz + 1 \\ 8x^2 &= 4xy + 4xz\end{aligned}$$

and since $x \neq 0$ we have $y + z = 2x$. This together with $yz = x^2 - 1$ give $y, z = x \pm 1$. Using Neib_3 we can define Neib, and then use the result about $\langle \mathbb{N}; \mathrm{Neib}, \times \rangle$.

$\langle \mathbb{N}; f, g \rangle$, where f, g are unary functions and f is weaker than $\times$. Let us take a recursive binary relation R such that the structure $\langle \mathbb{N}; R \rangle$ is def-strongest and both domains of R are equal to $\mathbb{N}$; such relations were presented in 3.1.c. The relation R can be defined by the formula

$$R(x,y) \iff \exists z\big(x = f(z) \wedge y = g(z)\big)$$

for suitable (recursive) unary function f, g; we may assume that f, g reach every value $x \in \mathbb{N}$ infinitely many times. (The conditions on the domains of R can be avoided by a modification of the defining formula.) Moreover, for every such f there is g such that the above formula holds.

Let $f(x) = y$ if $x = y^2 z$ for some $y \neq 0$ and a prime z, $f(x) = 0$ otherwise. The function f reaches every value infinitely many times, and is definable in $\langle \mathbb{N}; \times \rangle$ (i.e., weaker than $\times$). By the above we can find a unary (recursive) function g such that R is definable in $\langle \mathbb{N}; f, g \rangle$; then this structure is def-strongest.

$\langle \mathbb{N}; R_1, R_2 \rangle$, where R_1, R_2 are suitable equivalence relations on $\mathbb{N}$ and R_1 is weaker then $\times$. The equivalence relations R_1, R_2 can be constructed from the graph $\langle \mathbb{N}; R \rangle$ mentioned in 3.1.c and 4.1.c; the condition on R_1 will be arranged at the end. However, the construction is not direct; at first equivalence relations on $\mathbb{N} \cup R$ are constructed, and then a bijection between $\mathbb{N}$ and $\mathbb{N} \cup R$ is used.

To explain some details we come back to the geometrical terminology. Remember that we have constructed a def-strongest graph $\langle L \cup P \cup X; R\rangle$, where L is the set of *lines* (in $\mathbb{Q}^2$), P is the set of *points* and X is the set of elements used to distinguish some points; the elements of X will be called *pseudo-lines* (remember that in the lattice constructed above they have the same height as lines). R was in essential the incidence relation between the lines and points, and every pseudo-line was connected by R with exactly one point. We shall call the elements of R *edges*, and we shall consider them as two-element subsets of $L \cup P \cup X$. We may assume that the sets L, P, X, R are pairwise disjoint.

Now we shall construct a structure with the universe $M = L \cup P \cup X \cup R$. We shall define two equivalence relations E_b, E_r ("blue" and "red") on the set M. In the blue equivalence E_b every point will be isolated, and every line or pseudo-line will be connected with all edges containing it. ("Isolated" is understood to form a one-element class of the equivalence.) In the red equivalence E_r every line or pseudo-line will be isolated, and every point will be connected with all edges containing it.

In the structure $\langle M; E_b, E_r\rangle$ we can distinguish edges as the elements which are isolated neither in E_b nor in E_r. Therefore we can define the sets $L \cup P \cup X$ and R (as unary relations). Then we can define the relation R^* which corresponds to the original relation R of the graph:

$$\begin{aligned} R^*(x,y) \iff & x \notin R \wedge y \notin R \wedge x \neq y \wedge \\ & \wedge (\exists z \in R)\big((E_b(x,z) \vee E_r(x,z)) \wedge (E_b(y,z) \vee E_r(y,z))\big). \end{aligned}$$

(We only expressed the idea; technical details concerning symbols must be changed.) So we have interpreted a def-strongest structure, namely the graph $\langle L \cup P \cup X; R\rangle$, in the structure $\langle M; E_b, E_r\rangle$. Now it remains to define a bijection between $L \cup P \cup X$ and M, which is rather tedious, but possible. Then we shall know that the structure $\langle M; E_b, E_r\rangle$ is def-strongest.

Let a structure $\langle \mathbb{N}; R_1, R_2\rangle$ isomorphic to $\langle M; E_b, E_r\rangle$ have been constructed; we may arrange that the relations R_1, R_2 are recursive (even: if we do not spoil that on purpose, they will be recursive). The equivalence relation R_1 has infinitely many classes of every of the cardinalities 1, 2, $\aleph_0$, and no classes of other cardinalities. This property determines $\langle \mathbb{N}; R_1\rangle$ up to isomorphism. We can find an equivalence S_1 on $\mathbb{N}$ with the same property, and weaker than $\times$. (The classes of S_1 can be of the forms $\{p\}$, $\{p^2, p^3\}$ and $\{p^i \mid i > 3\}$ for every prime p, and all other $x \in \mathbb{N}$ can form the further class.) We can find another equivalence relation S_2 such that $\langle \mathbb{N}; S_1, S_2\rangle$ will be isomorphic with $\langle \mathbb{N}; R_1, R_2\rangle$.

4.5. *Other structures with two operations or relations*

No additional remarks.

4.6. *Structures with more than two operations or relations*

The first four mentioned structures are obviously related to the structure $\langle \mathbb{N}; \mathbf{s}, \perp \rangle$, see 3.2.

4.7.a. *Structures with other numerical universes*

No additional remarks.

4.7.b. *Structures with other numerical universes*

No: $\langle \Sigma^*; \cdot \rangle$, where Σ^* is the set of all words in the alphabet Σ and $\cdot$ denotes concatenation. For $\operatorname{card}\Sigma = 1$ the structure (isomorphic to $\langle \mathbb{N}; + \rangle$) has decidable theory. If $\operatorname{card}\Sigma > 1$ then the structure has nontrivial automorphisms (induced by the permutations of Σ).

$\langle P_\omega; \in \rangle$, where P_ω is the set of hereditarily finite sets and $\in$ is set-theoretical membership. (The structure is the standard model of the theory of finite sets.) The set P_ω can be defined as $\bigcup_{n\in\mathbb{N}} P_n$, where $P_0 = \emptyset$ and for every $n \in \mathbb{N}$ the set P_{n+1} is the powerset (i.e. the set of all subsets) of P_n. The mentioned example is isomorphic with $\langle \mathbb{N}; \in \rangle$ from 3.2.

No: $\langle \text{Pairs}; \boxed{,} \rangle$, where $\boxed{,}$ is the pairing function, $x \boxed{,} y = \langle x, y \rangle$ $(= \{\{x\}, \{x, y\}\})$ and Pairs is the smallest set which contains $\emptyset$ and is closed under forming ordered pairs (i.e., the function $\boxed{,}$). Of course, $\text{Pairs} \subseteq P_\omega$.

The operation $\boxed{,}$ was intensively studied by P. J. Voda (without restriction to first order properties); this and the next item were consulted with him. Among other notions he uses *head* and *tail* operations which (together) form an inverse of $\boxed{,}$ in the obvious sense. (Technically, P. J. Voda deals with $\mathbb{N}$ instead of Pairs, 0 instead of $\emptyset$, and he uses only comma ',' instead of $\boxed{,}$. It was not suitable here.) The substantial properties of $\boxed{,}$ are that

(i) $\boxed{,}$ is injective;
(ii) exactly one element of Pairs does not belong to the range of $\boxed{,}$;
(iii) if $X \subseteq \text{Pairs}$ contains $\emptyset$ and is closed under $\boxed{,}$ then $X = \text{Pairs}$.

We can also imagine elements of Pairs as (finite) rooted binary trees such that all their vertices except leaves have both sons.

From the point of view of general algebra, we can say that $\langle \text{Pairs}; \boxed{,} \rangle$ is free groupoid with the generator $\emptyset$ (i.e. an absolutely free algebra). Therefore by [Ma61] its theory is decidable.

$\langle \text{Pairs}; \boxed{,}, \boxplus \rangle$, where Pairs, $\boxed{,}$ are as above and $\boxplus$ is *concatenation of pairs*. To explain the meaning of $\boxplus$ it is suitable to imagine x, y as rooted binary trees (all their vertices except leaves must have both sons). Then $x \boxplus y$ is obtained if we put y instead of the rightest leaf of x. The following identities hold:

$$\emptyset \boxplus y = y, \qquad y \boxplus \emptyset = y, \qquad (v \boxed{,} w) \boxplus y = v \boxed{,} (w \boxplus y).$$

It is possible to transform some inductive definitions into usual first order definitions. We shall show that at the following definition of the operation RT ("right tree"):

$$RT(\emptyset) = \emptyset, \qquad RT(x, y) = \emptyset \boxed{,} RT(x \boxplus y);$$

in the tree terminology, $RT(x)$ is the binary tree (like above) which has as many vertices as x, and in which every left son is a leave. We can define:

$$
\begin{aligned}
y = RT(x) \iff \exists t, t_1 \Big(t = (x \boxed{,} y) \boxed{,} t_1 \wedge \forall u, v, a, b \Big(t = v \boxplus ((a \boxed{,} b) \boxed{,} w) \implies \\
\implies a = \emptyset \wedge b = \emptyset \wedge w = \emptyset \vee \\
\vee \exists a_1, a_2, b_2, w_2 \big(a = a_1 \boxed{,} a_2 \wedge b = \emptyset \boxed{,} b_2 \wedge \\
\wedge a = \big((a_1 \boxplus a_2) \boxed{,} b_2 \big) \boxed{,} w_2)) \Big) \Big).
\end{aligned}
$$

Using RT we can express "x has at most as many vertices as y" by the formula $\exists u \big(RT(x) \boxplus u = RT(y) \big)$. This is a substantial step to define an order (of type ω) on Pairs, etc. (We must convert many inductive definitions into the usual ones.)

The considered structure was used in [Vo92] and [Vo94] as a basis for theory of programming and computability.

??: $\langle \text{UPairs}; \mathit{upf} \rangle$, where *upf* is the operation of forming unordered pairs, $\mathit{upf}(x, y) = \{x, y\}$, and UPairs is the smallest set which contains $\emptyset$ and is closed under the operation *upf*. We can see Pairs $\subseteq$ UPairs $\subseteq P_\omega$. This structure is interesting mainly because of their relationship to the two items above. Notice that the operation $\boxed{,}$ (extended to the whole UPairs) can be easily defined in it. It is not clear whether Pairs and $\boxplus$ are definable (Of course, they are definable if the structure is def-strongest.) It is even not clear how to replace $\boxplus$ in a natural way.

??: $\langle \mathrm{HF}_k; \mathit{join}_k \rangle$, where HF_k is the smallest set containing $\emptyset$ and closed under join_k, and $\mathit{join}_k(x, y) = x \cup \{y\}$ if $\mathrm{card}(x) < k$, $\mathit{join}_k(x, y) = x$ otherwise. The set HF_k consists of all "hereditarily at most k-element sets". For example, $\mathrm{HF}_2 =$ UPairs, and join_2, *upf* are interdefinable.

5. Index of symbols

In the first part of the index the symbols are alphabetically ordered. For symbols containing letters the letters are considered at first; In sorting only letters are considered, and latin letters precedes the greek letters. Symbols without letters are put at the end. The parameters e, k, m, n, p, q, X (which are replaced by numerical values or sets in concrete applications) are not considered by sorting.

The second part contains the same symbols sorted systematically; the system is clear from the subheadings.

Remarks. 1. The index does not contain some widely used symbols, if the denoted notions are only used, and not investigated. It concerns e.g. $=$, logical connectives and quantifiers, set-theoretic symbols $\subseteq$, $\in$ (also a special meaning!), etc.

2. Distinguish the fonts; e.g. $\mathbf{p}_n$ denotes the n-th prime, while p_n is a variable (which can denote, e.g., arbitrary prime).

5.1. Alphabetically Sorted Index

$\mathbf{p}$ ... the list of primes (as a unary operation); $\mathbf{p}(0) = 2$, $\mathbf{p}(1) = 3, \dots$; we write also $\mathbf{p}_x$ instead of $\mathbf{p}(x)$
P_ω ... the set of hereditarily finite sets
Pairs ... the smallest set which contains $\emptyset$ and is closed under $\boxed{,}$
Pow^e ... the set of e-th powers; $\mathrm{Pow}^e = \{x^e \mid x \in \mathbb{N}\}$
Pow_n ... the set of powers of n; $\mathrm{Pow}_n = \{n^x \mid x \in \mathbb{N}\}$
Pow_n^e ... the set of powers of n^e; $\mathrm{Pow}_n = \{n^{ex} \mid x \in \mathbb{N}\}$
$\leq_{\mathrm{Pow}_n}$ ... the restriction of $\leq$ to the set Pow_n
$\mathbb{Q}$ ... the set of rational numbers
RT ... "right tree" operation on special binary trees; $RT(x)$ has as many vertices as x, and every its left son is a leaf
$\mathbf{s}$ ... successor function $\mathbf{s}(x) = x + 1$ (also on $\mathbb{Z}$, $\mathbb{Q}$ etc.)
$\mathbf{s}^n$ ... $\mathbf{s}^n(x) = x + n$ (also on $\mathbb{Z}$, $\mathbb{Q}$ etc.)
$_{\mathbf{s}}|$ ... composition of the graph of $\mathbf{s}$ and $|$; $x\ _{\mathbf{s}}|\ y \iff \mathbf{s}(x) \mid y$;
$|_{\mathbf{s}}$ ... composition of $|$ and the inverse of the graph of $\mathbf{s}$; $x \mid_{\mathbf{s}} y \iff x \mid \mathbf{s}(y)$
Sq ... the set of squares
SqP ... squaring of primes; $\mathrm{SqP} = \{(p, p^2) \mid p \in \mathbb{P}\}$
SqPow_n ... squaring of powers of n; $\mathrm{SqPow}_n = \{(n^i, n^{2i}) \mid i \in \mathbb{N}\}$
UPairs ... the smallest set which contains $\emptyset$ and is closed under *upf*
upf ... unordered pairing function, $upf(x, y) = \{x, y\}$
V_n ... $V_n(x) =$ the greatest $d \in \mathrm{Pow}_n$ such than $d \mid x$ (but $V_n(0) = 0$)
$\mathbb{Z}$ ... the set of integers
λ ... Carmichael function: $\lambda(x) =$ the smallest $e > 0$ such that $y^e \equiv 1 \pmod{x}$ whenever x, y are relatively prime (but $\lambda(0) = 0$)
$\lambda_{\dots}()$ ... lambda notation; e.g. $\lambda_{xy}(T)$ denotes the binary operation (on the actual base set, usually $\mathbb{N}$) given by the term T
Π ... the set of prime powers
$\leq_\Pi$ ... usual order on the set of prime powers
π ... $\pi(x) =$ the number of primes not exceeding x; e.g. $\pi(3) = 2$
$\rho_{\dots}()$ ... a notation for relations; e.g. $\rho_{xy}(A)$ denotes the binary relation (on the actual base set, usually $\mathbb{N}$) given by the formula A
σ ... sum of (positive) divisors; $\sigma(0) = 0$
τ ... the number of (positive) divisors; $\tau(0) = 0$
φ ... Euler function; $\varphi(n) = \mathrm{card}\{x < n \mid x \perp n\}$
Σ^* ... the set of all words in the alphabet Σ
$\cdot$ ... concatenation of words (sometimes also multiplication)
$\boxplus$ ... VODA's concatenation of pairs; $x \boxplus y$ arises from x by replacing the rightest $\emptyset$ by y
$\boxed{,}$ ... pairing function, $x \boxed{,} y = \{\{x\}, \{x, y\}\}$
$+$, $\times$ ... addition and multiplication (on $\mathbb{N}$ or other number set)
$\dot{-}$ ... $x \dot{-} y = x - y$ for $x \geq y$ and $x \dot{-} y = 0$ otherwise
$\leq$, $<$ ... usual order and strict order
$\leq_X$ ... usual order restricted to the set X
$|$ ... divisibility (on $\mathbb{N}$ or other set)
$|_n$ ... defined by $x \mid_n y \iff \bigwedge_{i \leq n} \forall z (\mathbb{P}(z) \wedge z^i \mid x \implies z^i \mid y)$
$||$ ... (ternary relation!) $x^y || z \iff x^y \mid z \wedge x^{y+1} \nmid z$

$\perp$ ... coprimeness (on $\mathbb{N}$ or other set)
$[a_k \dots a_0]_n$ ... n-adic expansion (a_i ... n-adic digits); $[a_k \dots a_0]_n = \sum_{i=0}^{k} a_i n^i$
$\sqsubseteq_n$ ... n-adic masking relation; $x \sqsubseteq_n y \iff$ the n-adic digits of x do not exceed the corresponding n-adic digits of y
$\sqsubset_n$ ... $x \sqsubset_n y \iff x \sqsubseteq_n y \wedge x \neq y$
$\sqcup_n$, $\sqcap_n$ ... lattice operations derived from $\sqsubseteq_n$
$\in$ ... $x \in y \iff y \,\mathrm{MOD}\, 2^{x+1} \geq 2^x$ (also set-theoretical membership)
$\bullet$ ... actual binary operation (hence no general fixed meaning)

5.2. *Systematical Index of Notations*

Number sets

Cub ... the set of cubes
Fac ... the set of factorials; $\mathrm{Fac} = \{x! \mid x \in \mathbb{N}\}$
$\mathbb{G}$ ... the set of Gaussian integers
$\mathbb{N}$ ... the set of nonnegative integers
$\mathbb{P}$ ... the set of primes
Pow^e ... the set of e-th powers; $\mathrm{Pow}^e = \{x^e \mid x \in \mathbb{N}\}$
Pow_n ... the set of powers of n; $\mathrm{Pow}_n = \{n^x \mid x \in \mathbb{N}\}$
Pow_n^e ... the set of powers of n^e; $\mathrm{Pow}_n = \{n^{ex} \mid x \in \mathbb{N}\}$
$\mathbb{Q}$ ... the set of rational numbers
Sq ... the set of squares
$\mathbb{Z}$ ... the set of integers
Π ... the set of prime powers

Unary operations

$L_{p,q}$ ... unary operation $L_{p,q}(x) = px + q$
$L_{p,q}^{m,n}$ ... unary operation $L_{p,q}^{m,n}(x) = x^m \cdot (px+q)^n$
$nextpow_n$ ... next power of n; $nextpow_n(x) = nx$, if $\mathrm{Pow}_n(x)$, 0 otherwise
$\mathbf{p}$ ... the list of primes; $\mathbf{p}(0) = 2$, $\mathbf{p}(1) = 3$, ... ; we write also $\mathbf{p}_x$ instead of $\mathbf{p}(x)$
RT ... "right tree" operation on special binary trees; $RT(x)$ has as many vertices as x, and every its left son is a leaf
$\mathbf{s}$ ... successor function $\mathbf{s}(x) = x + 1$ (also on $\mathbb{Z}$, $\mathbb{Q}$ etc.)
$\mathbf{s}^n$ ... $\mathbf{s}^n(x) = x + n$ (also on $\mathbb{Z}$, $\mathbb{Q}$ etc.)
V_n ... $V_n(x) =$ the greatest $d \in \mathrm{Pow}_n$ such than $d \mid x$ (but $V_n(0) = 0$)
λ ... Carmichael function: $\lambda(x) =$ the smallest $e > 0$ such that $y^e \equiv 1 \pmod{x}$ whenever x, y are relatively prime (but $\lambda(0) = 0$)
π ... $\pi(x) =$ the number of primes not exceeding x; e.g. $\pi(3) = 2$
σ ... sum of (positive) divisors; $\sigma(0) = 0$
τ ... the number of (positive) divisors; $\tau(0) = 0$
φ ... Euler function; $\varphi(n) = \mathrm{card}\,\{x < n \mid x \perp n\}$

Binary operations

B_n ... Pascal triangle modulo n; $B_n(x,y) = \binom{x+y}{x} \,\mathrm{MOD}\, n$
$\mathbf{c}$ ... Cantor's pairing function; $\mathbf{c}(x,y) = \frac{(x+y)(x+y+1)}{2} + x$
$\overline{\mathbf{c}}$ ... the bijection between $\mathbb{N} \times \mathbb{N}$ and $\mathbb{N} \setminus \{0\}$ defined by $\overline{\mathbf{c}}(x,y) = \mathbf{c}(x,y) + 1 = \frac{(x+y)(x+y+1)}{2} + x + 1$
C_n ... "skewed" Pascal triangle modulo n: $C_n(x,y) = \binom{x}{y} \,\mathrm{MOD}\, n$

DIV	...	quotient by integer division; completed by $x\,\mathrm{DIV}\,0=0$.
exp	...	exponential function; $\exp(x,y)=x^y$
gcd	...	greatest common divisor
H	...	a special mapping $\mathbb{N}^2\to\{0,1,2\}$; defined in 4.1.b, item $\langle\mathbb{N};H\rangle$
join	...	joining an element to a set; $join(x,y)=x\cup\{y\}$
$join_k$	...	$join_k(x,y)=x\cup\{y\}$ if $\mathrm{card}(x)<k$, $join_k(x,y)=x$ otherwise
lcm	...	least common multiple
MOD	...	rest by integer division; completed by $x\,\mathrm{MOD}\,0=x$
upf	...	unordered pairing function, $upf(x,y)=\{x,y\}$
$\cdot$	...	concatenation of words (sometimes also multiplication)
$\boxplus$	...	Voda's concatenation of pairs; $x\boxplus y$ arises from x by replacing the rightest $\emptyset$ by y
$+,\ \times$	...	addition and multiplication (on $\mathbb{N}$ or other set)
$\dot{-}$	...	$x\dot{-}y=x-y$ for $x\geq y$ and $x\dot{-}y=0$ otherwise
$\sqcup_n,\ \sqcap_n$	...	lattice operations derived from $\sqsubseteq_n$
$\boxed{,}$	...	pairing function, $x\boxed{,}y=\{\{x\},\{x,y\}\}$
$\bullet$	...	actual binary operation (hence no general fixed meaning)

Binary relations

Neib	...	neighborhood relation; $\mathrm{Neib}(x,y)\iff|x-y|=1$
SqP	...	squaring of primes; $\mathrm{SqP}=\{(p,p^2)\mid p\in\mathbb{P}\}$
SqPow_n	...	squaring of powers of n; $\mathrm{SqPow}_n=\{(n^i,n^{2i})\mid i\in\mathbb{N}\}$
$\leq,\ <$	...	usual order and strict order
$\leq_{\mathbb{P}},\ \leq_{\Pi}$	...	the restrictions of $\leq$ to the set of primes and to the set of prime powers, respectively
$\leq_{\mathrm{Pow}_n}$	...	the restriction of $\leq$ to the set Pow_n
$\sqsubseteq_n$	...	n-adic masking relation; $x\sqsubseteq_n y\iff$ the n-adic digits of x do not exceed the corresponding n-adic digits of y
$\sqsubset_n$	...	$x\sqsubset_n y\iff x\sqsubseteq_n y\wedge x\neq y$
$\in$	...	$x\in y\iff y\,\mathrm{MOD}\,2^{x+1}\geq 2^x$ (also set-theoretical membership)
$\mid$	...	divisibility (on $\mathbb{N}$ or other set)
$\mid_n$	...	defined by $x\mid_n y\iff\bigwedge_{i\leq n}\forall z(\mathbb{P}(z)\wedge z^i\mid x\implies z^i\mid y)$
$_{\mathbf{s}}\mid$	...	composition of the graph of $\mathbf{s}$ and $\mid$; $x\,{_{\mathbf{s}}\mid}\,y\iff\mathbf{s}(x)\mid y$
$\mid_{\mathbf{s}}$	...	composition of $\mid$ and the inverse of the graph of $\mathbf{s}$; $x\mid_{\mathbf{s}}y\iff x\mid\mathbf{s}(y)$
$\perp$	...	coprimeness (on $\mathbb{N}$ or other set)

Ternary and 4-ary relations

$\mathrm{Add}_{\mathbb{PN}}$	...	$=\rho_{xyz}(\mathbb{P}(x)\wedge x+y=z)$
EqB_n	...	$=\rho_{xyzw}(B_n(x,y)=B_n(z,w))$
EqH	...	$=\rho_{xyzw}(H(x,y)=H(z,w))$
$\mathrm{Mult}_{\mathbb{PN}}$	...	$=\rho_{xyz}(\mathbb{P}(x)\wedge xy=z)$
$\Vert$	...	(ternary relation!) $x^y\Vert z\iff x^y\mid z\wedge x^{y+1}\nmid z$

Other notations

card	...	cardinality (of a set)
GPT	...	generalized Pascal triangle (defined e.g. in [Ko94])
HF_k	...	the smallest set containing $\emptyset$ and closed under $join_k$
Pairs	...	the smallest set which contains $\emptyset$ and is closed under $\boxed{,}$

P_ω	...	the set of hereditarily finite sets
UPairs	...	the smallest set which contains $\emptyset$ and is closed under *upf*
Σ^*	...	the set of all words in the alphabet Σ
$\lambda_{\dots}()$	...	lambda notation; e.g. $\lambda_{xy}(T)$ denotes the binary operation (on the actual base set, usually $\mathbb{N}$) given by the term T
$\rho_{\dots}()$	...	a notation for relations; e.g. $\rho_{xy}(A)$ denotes the binary relation (on the actual base set, usually $\mathbb{N}$) given by the formula A
$[a_k \dots a_0]_n$	...	n-adic expansion (a_i ... n-adic digits); $[a_k \dots a_0]_n = \sum_{i=0}^k a_i n^i$

BIBLIOGRAPHY

[Ax68] J. Ax, *The elementary theory of finite fields*, Ann. Math. **88** (1968), 239–271.

[BJW93] P. T. Bateman — C. G. Jockusch — A. R. Woods, *Decidability and undecidability of theories with a predicate for the primes*, Journal of Symbolic Logic **58** (1953), no. 2, 672–687.

[Be94] A. Bès, *On Pascal triangles modulo a prime power*, Proceedings Logic Colloquium'94 (Annals of Pure and Applied Logic) (submitted 1994), 15pp.

[Be95] ———, *Undecidable extensions of Büchi arithmetic and Cobham-Semenov theorem*, Journal of Symbolic Logic (submitted 1995), 17pp.

[Be96] ———, *An extension of the Cobham-Semënov theorem*, A preprint (1996), 10pp.

[Be96a] ———, *Problèmes de dèfinissabilitè arithmétique: triagles de Pascal, arithmétique de Presburger et arithmétique de Skolem*, Ph.D. thesis, Université Paris VII, 1996.

[BK96] A. Bès — I. Korec, *Definability within structures related to Pascal triangles modulo an integer*, A manuscript (1996), 17pp.

[BR94] A. Bès — D. Richard, *Undecidable extensions of Skolem arithmetic*, Journal of Symbolic Logic (submitted 1994), 22pp, also Preprint 42 of LLAIC.

[Bh53] E. W. Beth, *On PADOA's method in the theory of definition*, Indagationes mathematicae **15** (1953), 330–339.

[Bo90] B. A. Bondarenko, *Generalized Pascal triangles and pyramids, their fractals, graphs and applications (in Russian)*, "Fan", Tashkent, 1990.

[Bü60] J. R. Büchi, *Weak second-order arithmetic and finite automata*, Zeitschrift für Math. Logik Grundlagen Math. **6** (1960), 66–92.

[Bü60a] ———, *On a decision method in restricted second order arithmetic*, Logic, Methodology, and Philosophy of Science. Proceedings of the1960 Congress, Stanford University Press, California, 1960, pp. 1–11.

[BL69] J. R. Büchi — L. Landweber, *Definability in the monadic second-order theory of successor*, Journal for Symbolic Logic **34** (1969), 166–170.

[Ce81] P. Cegielski, *La théorie élémentaire de la multiplication*, Model Theory and Arithmetic (Berline, McAloon, Ressayre, eds.), Springer Lecture Notes in Math. 890, 1981, pp. 44–89.

[Ce84] ———, *La théorie élémentaire de la divisibilité est finiment axiomatisable*, C. R. Acad. Sc. Paris, Série I **299** (1984), 367–369.

[Ce89] ———, *The elementary theory of the natural lattice is finitely axiomatizable*, Notre Dame Journal of Formal Logic **30** (1989), 138–150.

[Ce90] ———, *La théorie de corps réel-clos inductifs est une extension conservative de l'Arithmétique de Peano*, Comptes Rendus de l'Académie des Sciences. Série I. Mathématique **310** (1990), no. 5, 239–242.

[Ce90a] ———, *Quelques contributions a l'etude des arithmetiques faibles (Thèse), LITP 90.77*, Octobre 1990.

[Ce90b] ———, *Julia Robinson definability forty years later*, Seminaire du LLAIC, Vol. I, Université d'Auvergne – Clermont 1, 1989–1990, pp. 32–45.

[Ce96] ———, *Definability, decidability and complexity*, Annals of Mathematics on Artificial Intelligence **16** (1996), 311–341.

[CMR96] P. Cegielski — Y. Matiyasevich — D. Richard, *Definability and decidability issues in extensions of the integers with the divisibility predicate*, Journal of Symbolic Logic **61** (1996), no. 2, 515–540.

[CR92] P. Cegielski — D. Richard, *Indécidabilité de la théorie des entiers naturels munis d'un eénumération des premiers et de la divisibilité*, C. R. Acad. Sc. Paris, Série I **315** (1992), 1431–1434, also Seminaire du LLAIC, Université d'Auvergne – Clermont 1, Vol. IV (1992–1993), 17–23.

[CR93] P. Cegielski — D. Richard, *Une application de la complexitè à la non-définassibilité*, Seminaire du LLAIC, Vol. IV, Université d'Auvergne – Clermont 1, 1992–1993, pp. 25–31.

[CG86] A. Černý, J. Gruska, *Modular trellises*, Acta Informaticae **9** (1986), 253–282.

[Co69] A. Cobham, *On the base dependence of sets of numbers recognizable by finite automata*, Math. System Theory **3** (1969), 186–192.

[Co72] ______, *Uniform tag sequences*, Math. System Theory **6** (1972), 164–192.

[El61] C. C. Elgot, *Decision problems of finite automata design and related arithmetics*, Trans. Amer. Math. Soc. **98** (1961), 21–52.

[ER66] C. C. Elgot – M. O. Rabin, *Decidability and undecidability of second (first) order theory of (generalized) successor*, J. Symbolic Logic **31** (1966), 169–181.

[Er80] P. Erdös, *How many pairs of products of consecutive integers have the same prime factors?*, Amer. Math. Monthly **87** (1980), 391–392.

[Gr91] S. Grigorieff, *Décidabilité et complexité des thèories logiques*, Logique et Informatique: Une Introduction (B. Courcelle — M. Nivat, eds.), I.N.R.I.A., Rocquancourt – France, 1991, pp. 92pp.

[GR89] S. Grigorieff — D. Richard, *Contibution à l'ètude d'une conjecture de théorie des nombres par le codage ZBV*, L'Enseignement mathématique, 2° série **35** (1989), 125–189.

[Ko85] I. Korec, *Multiples of an integer in the Pascal triangle*, Acta Math. Univ. Comen. **46–47** (1985), 83–91.

[Ko89] ______, *Generalized Pascal triangles*, K. Halkowska – B. Stawski (Editors) : Proceedings of the V Universal Algebra Symposium, Turawa, Poland, 3-7 May 1988, World Scientific, Singapore, 1989, pp. 198–218.

[Ko90] ______, *Pascal triangles modulo n and modular trellises*, Computers and Artificial Intelligence **9** (1990), 105–113.

[Ko93] ______, *Definability of arithmetic operations from the order and a random relation*, Fundamenta Informaticae **18** (1993), no. 2,3,4, 287–296.

[Ko93a] ______, *Definability of arithmetic operations in Pascal triangle modulo an integer divisible by two primes*, Grazer Matematische Berichte **318** (1993), 53–62.

[Ko94] ______, *Generalized Pascal triangles, their relation to cellular automata and their elementary theories*, Development in theoretical computer science, Proceedings of the 7th IMYCS, Smolenice 92, November 16–20, 1992 (Dassow, J. — Kelemenová,A., eds.), Gordon and Breach Science, 1994, pp. 59–70.

[Ko94a] ______, *Structures related to Pascal's triangle modulo* 2 *and their elementary theories*, Mathematica Slovaca **44** (1994), no. 5, 531–554.

[Ko94b] ______, *Substantially different theories of two structures associated to the same generalized Pascal triangle*, Summer School on General Algebra and Ordered Sets, Horní Lipová, September 1994 (I. Chajda, F. Halaš, F. Krutský, eds.), Palacký University, Olomouc, 1994, pp. 63–78.

[Ko94c] ______, *Theories of generalized Pascal triangles* (Proceedings of the Logic Colloquium'94, Clermont-Ferrand, July 21–30, 1994), Annals of Pure and Applied Logic (submitted July 1994), 1-7.

[Ko95] ______, *Elementary theories of structures containing generalized Pascal triangles modulo a prime*, Discrete Mathematics and Applications, Blagoevgrad/Predel, Sept. 12–16, 1994 (S. Shtrakov and Iv. Mirchev, eds.), Blagoevgrad, 1995, pp. 91–102.

[Ko95a] ______, *Decidable and undecidable theories of generalized Pascal triangles*, General Algebra and Discrete Mathematics, Potsdam, Sept. 27 – Okt. 1, 1993 (K. Denecke, O. Lüders, eds.), Heldermann-Verlag, Berlin, 1995, pp. 169–179.

[Ko95b] ______, *Undecidable elementary theories of classes of generalized Pascal triangles*, Tatra Mountains Mathematical Publications **5** (1995), 151–168.

[Ko95c] ______, *Undecidability and uniform definability in classes of structures related to Pascal triangles modulo n*, Tatra Mountains Mathematical Publications (submitted December 1995), 12pp, also Preprint 18/1996 of Math. Institute SAV Bratislava.

[Ko95d] ______, *Theories of generalized Pascal triangles (Abstract)*, Bulletin of the Association for Symbolic Logic **1** (1995), no. 2, 214–215.

[Ko96] ______, *Definability of arithmetical operations from Pascal's triangle modulo n and arithmetical functions*, Preprint 19/1996 of Math. Institute SAV Bratislava, 8pp.

[Ko96a] ______, *Definability of addition from multiplication and neighborhood relation and some related results*, Preprint 23/1996 of Math. Institute SAV Bratislava, 8pp.

[Ko96b] ______, *Definability of Pascal's triangles modulo* 4 *and* 6 *and some other binary operations from their associated equivalence relations*, Preprint 32/1996 of Math. Inst. Slovak Acad. Sci. Bratislava, 12pp.

[Ko96c] ______, *Elementary definability from Pascal's triangle modulo p and and the set of e-th powers*, Proceeddings of Number Theory Conference Eger 1996 (submétted December 1996), 23pp, also Preprint 2/1997 of Math. Inst. Slovak Acad. Sci. Bratislava.

[KPR74] I. Korec — N. G. Peretiatkin. — W. Rautenberg, *Definability in structures of finite valency*, Fundamenta Mathematicae **81** (1974), 173–181.

[KR76] I. Korec — W. Rautenberg, *Model-interpretability into trees and applications*, Archiv für math. Logik und Grundlagenforschung **17** (1976), 97–104.

[CR92a] A. Kościelski, *Borel determinacy, weak set theories and higher order arithmetics*, Seminaire du LLAIC, Vol. IV, Université d'Auvergne – Clermont 1, 1992–1993, pp. 144–196.

[La92] M. Langevin, *Approximations diophantiennes et nombres transcendants*, Luminy 1990 (Philippon, Patrice, eds.), de Gruyter, Berlin, 1992, pp. 203–214.

[Lä68] H. Läuchli, *A decision procedure for the weak second order theory of linear order*, K. Schütte (Ed.): Contributions to mathematical logic, North Holand, Amsterdam, 1968, pp. 189–197.

[Ma61] A. I. Mal'cev, *Elementary theories of locally free universal algebras* (Russian), Dokl. Akad. Nauk SSSR **138** (1961), 1009–1012.

[Ma87] F. Marko, *The divisibility of the binomial coefficients near a half-line and in convex sets*, Acta Math. Univ. Comen **50–51** (1987), 267–275.

[Mc78] McAloon, Kenneth, *Completeness theorems, incompleteness theorems and models of arithmetic*, Transactions of the American Mathematical Society **239** (1978), no. 5, 253–277.

[Me64] E. Mendelson, *Introduction to mathematical logic*, Van Nostrand, 1964, 3^{rd} ed. 1987, Wadsworth, California, X+342 p.

[Mil81] P. Michel, *Borne supérieure de la complexité de la théorie de N muni de la relation de divisibilité*, Model Theory and Arithmetic (Berline, McAloon, Ressayre, eds.), Springer Lecture Notes in Mathematics 890, 1981, pp. 242–250.

[Mo76] J. D. Monk, *Mathematical logic*, Springer Verlag, New York, 1976.

[Mr92] M. More, *Images de spectres binaires par des polynômes*, C. R. Acad. Sci. Paris, Série I **315** (1992), 343–348.

[Ms52] A. Mostowski, *On direct products of theories*, Jornal of Symbolic Logic **17** (1952), no. 1, 1–31, also in Foundational studies Selected works Vol. 2, North Holland 1979.

[PR81] J.-P. Pabion — D. Richard, *Synonymy and re-interpretation for some sublanguages of Peano arithmetic*, Open days in model theory and set theory, Jadwisin (Poland) September 1981 (W. Guzicki, W. Marek, A. Pelc, C. Rauszer, eds.), Leeds University Press, 1981.

[Pa01] A. Padoa, *Essai d'une théorie algébrique des nombres entiers, précédé d'une introduction logiqueá une théorie déductive quelconque*, Bibliothèque du Congrès international de philosophie, Paris, 1900, vol. 3, Armand Colin, 1901, pp. 309–365, Engl. translation in van Heijenoort, From Frege to Gödel, Harvard University Press 1967, 118–123.

[Pe73] Yu. G. Penzin, *Razreshimost' teorii celych chisel so slozheniem, porjadkom i umnozheniem na proizvol'noe chislo*, Matematicheskie Zametki **13** (1973), no. 5, 667–675, Translated in: Mathematical Notes 13(5):401–405, 1973.

[Pe74] ______, *Undecidability of the theory of the integers with addition and the predicate of coprimality (in russian)*, Third All-Union Conf. Math. Logic Novosibirsk, 1974, (information: [Ce90a]).

[Pe76] ———, *Undecidability of a theory of the integers with addition and predicate mutually disjoint (in russian)*, Algeb. Systemy (Irkutsk 1976), 149–153.

[Pe78] ———, *Nerazreshimye teorii kol'ca nepreryvnych funkcij*, Algoritmicheskie voprosy algebraicheskich sistem, Irkutsk, 1978, pp. 142–147.

[Pe79] ———, *Problema bliznecov v formal'noj arifmetike*, Matematicheskie Zametki **26** (1979), no. 4, 505–511, Translated in: Mathematical Notes 26(3-4):743-746, 1979.

[Po85] B. Poizat, *Cours de théorie des modèles*, Offilib, Paris, 1985.

[Pu57] H. Putnam, *Decidability and essential undecidability*, Journal of Symbolic Logic **22** (1957), 39–54.

[Ra69] O. Rabin, *Decidability of second-order theories and automata on infinite trees*, Transactions Amer. Math. Society **141** (1969), 1–35.

[Ri81] D. Richard, *De la structure additive a la saturation des modeles de Peano et a la classification des sous-languages de l'Arithmetique*, Model Theory and Arithmetic (Berline, McAloon, Ressayre, eds.), Springer Lecture Notes in Math. 890, 1981, pp. 270–296.

[Ri84] ———, *The arithmetics as theories of two orders*, Annals of Discrete Mathematics **23** (1984), 287–312.

[Ri85] ———, *Answer to a problem raised by J. Robinson: the arithmetic of positive or negative integers is definable from successor and divisibility*, Journal of Symbolic Logic **50** (1985), 927–935.

[Ri85a] ———, *All arithmetical sets of powers of primes are first order definable in terms of the successor and the coprimeness predicate*, Discrete Mathematics **53** (1985), 221-247.

[Ri85b] ———, *Définissabilité en arithmétique et méthode de codage Z.B.V. appliquéeà des langages avec successeurs et coprimarité*, 1985, Thèse de doctorat d'état, Université de Lyon-I.

[Ri85c] ———, *Définissabilité de lárithmétique et par successeurs, coprimarité et puissance*, C. R. Acad. Sc. Paris Série I **300** (1985), no. 13, 415–418.

[Ri87] ———, *Définissabilité de lárithmétique par coprimarité et restrictions de l'addition ou de la multiplication*, C. R. Acad. Sc. Paris Série I **305** (1987), 665–668.

[Ri88] ———, *Equivalence of some questions in mathematical logic with some conjectures in number theory*, Number Theory and Applications (R. Mollin, eds.), 1988, pp. 529–545.

[Ri89] ———, *Definability in terms of the successor function and the coprimeness predicate in the set of arbitrary integers*, Journal of Symbolic Logic **54** (1989), no. 4, 1253-1287.

[Ro49] J. Robinson, *Definability and decision problems in arithmetic*, Journal of Symbolic Logic **14** (1949), 98–114.

[Ro52] ———, *Existential definability in arithmetic*, Transactions of the American Mathematical Society **72** (1952), no. 3, 437–449.

[Ro60] ———, *The indecidability of algebraic rings and fields*, Proc. of A.M.S. **10** (1960).

[Ro65] ———, *The decision problem for fields*, The theory of models (Addison, Henkin, Tarski, eds.), North Holland, 1965, pp. 299–311.

[Ro96] ———, *Collected papers* (S. Feferman, ed.), AMS Publications, 1996, probably contains the four items above.

[RZ60] A. Robinson — E. Zakon, *Elementary properties of ordered Abelian groups*, Transactions A.M.S. **96** (1960), 222–236.

[Se77] A. L. Semenov, *The Presburger nature of predicates that are regular in two number systems (in Russian)*, Siberian Math. Journal **18** (1977), no. 2, 289–299.

[Se80] ———, *On certain extensions of the arithmetic of addition of natural numbers*, Mathematics of the USSR — Izvestiya **15** (1980), 401–419.

[Se82] ———, *On definability of arithmetic in their fragments (in Russian)*, Doklady Akad. nauk SSSR **263** (1982), no. 1, 44–47.

[Se83] ———, *Logical theories of one-place functions on the set of natural numbers*, Izvestiya Akademii nauk SSSR Serija Matematicheskaya **47** (1983), 623-658, English translation: Mathematics of the USSR — Izvestiya 22 (1984), 162–175.

[Se84] ———, *Decidability of monadic theories* (1984), Springer, Lecture Notes in Computer Science 176, 401-419.

[Sf70] D. Siefkes, *Büchi's monadic second order successor arithmetics*, Springer, Lecture Notes in Math. 120, 1970.

[Sn74] D. Singmaster, *Notes on binomial coefficients III — Any integer divides almost all binomial coefficients*, J. London Math. Soc. **(2) 8** (1974), 555-560.

[Th75] W. Thomas, *A note on undecidable extensions of monadic second-order successor arithmetic*, Arch. math. Logik **17** (1975), 43–44.

[Th78] ______, *The theory of successor with an extra predicate*, Mathematische Annalen **227** (1978), 121–132.

[Th80] ______, *On the bounded monadic theory of well-ordered structures*, Journal of Symbolic Logic **45** (1980), 334–338.

[Th81] ______, *A combinatorial approach to the theory of ω-automata*, Information and Control **48** (1981), 261–283.

[Vi92] R. Villemaire, *Joining k- and l-recognizable sets of natural numbers*, Proceedings STACS'92, Springer Lecture Notes in Computer Science **577**, 1986, pp. 458–466.

[Vi93] R. Villemaire, $\langle \mathbb{N}, +, V_k, V_l \rangle$ *is undecidable*, Theor. Comput. Sci **106** (1993), 337–349.

[Vo92] P. J. Voda, *Basis for a feasible programming language*, Computer Science Logic CSL'94, Springer Lecture Notes in Computer Science **933**, 1995, pp. 324–338.

[Vo96] P. J. Voda, *Programming by Logic & Logic by Programming (Volume 1. Computability)*, In preparation.

[Wo81] A. R. Woods, *Some problems in logic and number theory, and their connection*, Ph.D. thesis, University of Manchester, 1981.

[Ye80] Yu. L. Yershow, *Decidability problems and constructive models* (Russian), "Nauka", Moscow, 1980.

MATHEMATICAL INSTITUTE, SLOVAK ACADEMY OF SCIENCES,
ŠTEFÁNIKOVA 49, 81473 BRATISLAVA, SLOVAKIA
E-mail address: korec@savba.sk

This preprint series was founded in 1996. Its purpose is to present manuscripts of submitted or unpublished papers and reports of fellows of the Mathematical Institute of the Slovak Academy of Sciences in Bratislava and its Košice branch. The authors are fully responsible for the content of the preprints. Postal addresses:

Mathematical Institute
Slovak Academy of Sciences
Štefánikova 49
SK–814 73 Bratislava
SLOVAKIA

Tel./Fax (+421 7) 5249 7316

Mathematical Institute
Slovak Academy of Sciences
Grešákova 6
SK–040 01 Košice
SLOVAKIA

Tel./Fax (+421 95) 6228291

PostScript files of preprints are available at WWW address:
`http://www.mat.savba.sk/preprints`

Latest preprints of the series:

33/1996 *Ivan Korec*: A list of arithmetical structures strongest with respect to the first order definability

32/1996 *Ivan Korec*: Definability of Pascal's triangles modulo 4 and 6 and some other binary operations from their associated equivalence relations

31/1996 *Anatolij Dvurečenskij*: Measures and states on BCK-algebras

30/1996 *Ján Haluška*: Uncertainty and tuning in music

29/1996 *Ján Haluška*: On numbers 256/243, 25/24, 16/15

28/1996 *Ján Haluška*: COMMA 32 805/32 768

27/1996 *Beloslav Riečan*: On the sum of observables in MV algebras of fuzzy sets

26/1996 *Beloslav Riečan*: On the strong law of large numbers for weak observables in MV algebras

25/1996 *Ivan Korec*: Algebraical constructions of reversible generalized Pascal triangles and one–dimensional cellular automata

24/1996 *Peter Vojtáš*: Uncertain reasoning with floating connectives

23/1996 *Ivan Korec*: Definability of addition from multiplication and neighbourhood relation and some related results

22/1996 *Ivan Korec*: Open problems more or less related to generalized Pascal triangles

21/1996 *Sylvia Pulmannová*: On connections among some orthomodular structures

20/1996 *Pekka Lahti, Sylvia Pulmannová*: Coexistent observables and effects in quantum mechanics

19/1996 *Ivan Korec*: Definability of arithmetical operations from Pascal's triangle modulo n and arithmetical functions

18/1996 *Ivan Korec*: Undecidability and uniform definability in classes of structures related to Pascal's triangles modulo n

17/1996 *Beloslav Riečan*: Probability theory on some ordered structures

16/1996 *Beloslav Riečan*: Weak observables in MV algebras

15/1996 *Anatolij Dvurečenskij, Hee Sik Kim*: On connections between BCK-algebras and difference posets

14/1996 *Anatolij Dvurečenskij, Karl Svozil*: Product of partition logics, orthoalgebras and automata

13/1996 *Robin L. Hudson, Sylvia Pulmannová*: Chaotic expansion of elements of the universal enveloping algebra of a Lie algebra associated with a quantum stochastic calculus

12/1996 *Sylvia Pulmannová*: Congruences in partial abelian semigroups

(continued on inside back cover)

11/1996 *Karol Nemoga, Štefan Schwarz*: An explicit description of the set of all normal bases generators of a finite field

10/1996 *Ján Jakubík*: Subdirect product decompositions of MV-algebras

9/1996 *Ivan Korec*: Reversibility in generalized Pascal triangles and binary reversibility in one-dimensional cellular automata

8/1996 *Jozef Bobok, Milan Kuchta*: X-minimal patterns and generalization of Sharkovskiĭ's theorem

7/1996 *Jarmila Hedlíková, Sylvia Pulmannová*: Generalized difference posets and orthoalgebras

6/1996 *Ján Borsík, Roman Frič*: Pointwise convergence fails to be strict

5/1996 *Miroslav Ploščica*: Affine completions of distributive lattices

4/1996 *Ján Haluška*: Equal temperament and Pythagorean tuning: a geometrical interpretation in the plane

3/1996 *Winfried Just, Peter Vojtáš*: On matrix rapid filters

2/1996 *Anatolij Dvurerečenskij*: Fuzzy set representations of some quantum structures

1/1996 *Miloslav Duchoň, Beloslav Riečan*: On the product of semigroup valued measures